Web Application Report

This report includes important security information about your web application.

Security Report

This report was created by IBM Security AppScan Standard 9.0.3.12, Rules: 17339
Scan started: 5/7/2024 11:22:49 AM

Table of Contents

Introduction

Summary

Issues Sorted by Issue Type

Introduction

This report contains the results of a web application security scan performed by IBM Security AppScan Standard.

Medium severity issues:	1
Low severity issues:	30
Informational severity issues:	59
Total security issues included in the report:	90
Total security issues discovered in the scan:	90

General Information

Scan file name: MCIT_LifeRay

Scan started: 5/7/2024 11:22:49 AM

Test policy: Default

Host	mcit-liferayqc.linkdev.com
Port	443
Operating system:	Unknown
Web server:	Unknown
Application server:	JavaAppServer

Login Settings

Login method:	Recorded login
Concurrent logins:	Enabled
JavaScript execution:	Disabled
In-session detection:	Enabled
In-session pattern:	
Tracked or session ID cookies:	
Tracked or session ID parameters:	
Login sequence:	

Summary

Issue Types 15

TOC

	Issue Type	Number of Issues
M	Missing Secure Attribute in Encrypted Session (SSL) Cookie	1
L	Autocomplete HTML Attribute Not Disabled for Password Field	1
L	Cacheable SSL Page Found	15
L	Check for SRI (Subresource Integrity) support	1
L	Missing or insecure "Content-Security-Policy" header	2
L	Missing or insecure "X-XSS-Protection" header	2
L	Missing or insecure HTTP Strict-Transport-Security Header	2
L	Unsafe third-party link (target="_blank")	7
I	Application Error	35
I	Application Test Script Detected	1
I	Email Address Pattern Found	1
I	Integer Overflow	6
I	Internal IP Disclosure Pattern Found	6
I	SHA-1 cipher suites were detected	1
I	Unsanitized user input reflected in JSON	9

Vulnerable URLs 23

TOC

	URL	Number of Issues
M	https://mcit-liferayqc.linkdev.com/c	2
L	https://mcit-liferayqc.linkdev.com/web/guest/home	5
L	https://mcit-liferayqc.linkdev.com/account-type	3
L	https://mcit-liferayqc.linkdev.com/documents/d/guest/mcit-forgot-password-ar	1
L	https://mcit-liferayqc.linkdev.com/documents/d/guest/mcit-home-newsletter-ar	1

L	https://mcit-liferayqc.linkdev.com/documents/d/guest/mcit-individual-registration-ar	1
L	https://mcit-liferayqc.linkdev.com/documents/d/guest/mcit-recruitment-ar	1
L	https://mcit-liferayqc.linkdev.com/home	3
L	https://mcit-liferayqc.linkdev.com/individual-registeration	2
L	https://mcit-liferayqc.linkdev.com/o/frontend-js-loader-modules-extender/loader.js	1
L	https://mcit-liferayqc.linkdev.com/o/js_resolve_modules	6
L	https://mcit-liferayqc.linkdev.com/o/mcit-theme/fonts/Bukra-Medium.otf	1
L	https://mcit-liferayqc.linkdev.com/o/mcit-theme/js/main.js	1
L	https://mcit-liferayqc.linkdev.com/o/mcit-theme/manifest.json	4
L	https://mcit-liferayqc.linkdev.com/recruitment	3
L	https://mcit-liferayqc.linkdev.com/web/guest/recruitment-options	3
L	https://mcit-liferayqc.linkdev.com/c/portal/login	1
I	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/	37
I	https://mcit-liferayqc.linkdev.com/o/mcit-common-apis/v1.0/uploadFile	1
I	https://mcit-liferayqc.linkdev.com/o/mcit-registration/v1.0/individualRegistration	7
I	https://mcit-liferayqc.linkdev.com/web/	1
I	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplicationtypes	3
I	https://mcit-liferayqc.linkdev.com/o/mcit-forgot-password/v1.0/forgot-password	2

Fix Recommendations 14

TOC

	Remediation Task	Number of Issues
M	Add the 'Secure' attribute to all sensitive cookies	1
L	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"	7
L	Add to each third-party script/link element support to SRI(Subresource Integrity).	1
L	Change server's supported ciphersuites	1
L	Config your server to use the "Content-Security-Policy" header with secure policies	2
L	Config your server to use the "X-XSS-Protection" header with value '1' (enabled)	2
L	Correctly set the "autocomplete" attribute to "off"	1
L	Implement the HTTP Strict-Transport-Security policy with a long "max-age"	2
L	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.	15

L	Remove e-mail addresses from the website	1	
L	Remove internal IP addresses from your website	6	
L	Remove test scripts from the server	1	
L	Review possible solutions for hazardous character injection	9	
L	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions	41	

Security Risks 8

TOC

	Risk	Number of Issues	
M	It may be possible to steal user and session information (cookies) that was sent during an encrypted session	1	
L	It may be possible to bypass the web application's authentication mechanism	1	
L	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations	28	
L	In case the third-party server is compromised, the content/behavior of the site will change	1	
L	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.	13	
I	It is possible to gather sensitive debugging information	41	
I	It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords	1	
I	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user	10	

Causes 10

TOC

	Cause	Number of Issues	
M	The web application sends non-secure cookies over SSL	1	
L	Insecure web application programming or configuration	14	
L	Sensitive information might have been cached by your browser	15	
L	There is no support to Subresource Integrity.	1	
L	The rel attribute in the link element is not set to "noopener noreferrer".	7	
I	Proper bounds checking were not performed on incoming parameter values	41	

I	No validation was done in order to make sure that user input matches the data type expected	41	
I	Temporary files were left in production environment	1	
I	The web server or application server are configured in an insecure way	1	
I	Sanitation of hazardous characters was not performed correctly on user input	9	

WASC Threat Classification

TOC

Threat	Number of Issues	
Abuse of Functionality	7	
Cross-site Scripting	9	
Information Leakage	65	
Integer Overflows	6	
Predictable Resource Location	1	
Remote File Inclusion	1	
Server Misconfiguration	1	

Issues Sorted by Issue Type

M Missing Secure Attribute in Encrypted Session (SSL) Cookie 1 TOC

Issue 1 of 1 TOC

Missing Secure Attribute in Encrypted Session (SSL) Cookie	
Severity:	Medium
CVSS Score:	6.4
URL:	https://mcit-liferayqc.linkdev.com/c
Entity:	LiferayJWTToken (Cookie)
Risk:	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Causes:	The web application sends non-secure cookies over SSL
Fix:	Add the 'Secure' attribute to all sensitive cookies

Reasoning: AppScan found that an encrypted session (SSL) is using a cookie without the "secure" attribute.

Test Requests and Responses:

```
GET /c HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/web/guest/home?
p_p_id=com_liferay_login_web_portlet_LoginPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=vi
ew&_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName=%2Flogin%2Flogin&saveLastPath
=false
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0; COOKIE_SUPPORT=true;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
ID=78692f674d56476771344b754c46314878394f5043513d3d; GUEST_LANGUAGE_ID=ar_SA;
_ga=GA1.1.128297136.1599395143; _ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0;
LFR_SESSION_STATE_20099=1715073020896; JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF;
COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Upgrade-Insecure-Requests: 1
Sec-Fetch-Mode: navigate
```

```
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Cache-Control: max-age=0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.7
Sec-Fetch-User: ?1
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: document


HTTP/1.1 302
Location: https://mcit-liferayqc.linkdev.com/c/portal/layout
Connection: keep-alive
Liferay-Portal: Liferay Digital Experience Platform
Content-Length: 0
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Set-Cookie: JSESSIONID=5C030282C0E25C8DBA7507BC4319F8B4; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 10:31:33 GMT



GET /c/portal/layout HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/c
Cookie: _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0; COOKIE_SUPPORT=true;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
_ga=GA1.1.128297136.1599395143; GUEST_LANGUAGE_ID=ar_SA;
ID=78692f674d56476771344b754c46314878394f5043513d3d;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_20099=1715073020896;
JSESSIONID=5C030282C0E25C8DBA7507BC4319F8B4; COMPANY_ID=20096
Connection: Keep-Alive
Host: mcit-liferayqc.linkdev.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 302
Location: https://mcit-liferayqc.linkdev.com/web/guest/home
Connection: keep-alive
Liferay-Portal: Liferay Digital Experience Platform
Content-Length: 0
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Date: Tue, 07 May 2024 09:55:03 GMT
Content-Type: text/html;charset=UTF-8



GET /web/guest/home HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/c/portal/layout
Cookie: _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0; COOKIE_SUPPORT=true;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
_ga=GA1.1.128297136.1599395143; GUEST_LANGUAGE_ID=ar_SA;
ID=78692f674d56476771344b754c46314878394f5043513d3d;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_20099=1715073020896;
JSESSIONID=5C030282C0E25C8DBA7507BC4319F8B4; COMPANY_ID=20096
Connection: Keep-Alive
Host: mcit-liferayqc.linkdev.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Liferay-Portal: Liferay Digital Experience Platform
X-Content-Type-Options: nosniff
```

```
Keep-Alive: timeout=20
Cache-Control: private
Date: Tue, 07 May 2024 10:31:38 GMT
Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>
```

```
<html class="rtl" dir="rtl" lang="ar-SA">

<head>
 <title>       وزارة الاتصالات وتقنية المعلومات - الرئيسية</title>
  <meta name="viewport" content="width=device-width, width=device-width" />
  <meta name="description" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية " />
  <meta name="keywords" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية">
  <meta name="format-detection" content="telephone=no">
  <meta property="og:url" content="/web/guest/home" />
  <meta property="og:type" content="Webs
...
...
...
```

Issue 1 of 1

TOC

Autocomplete HTML Attribute Not Disabled for Password Field

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/web/guest/home
Entity:	home (Page)
Risk:	It may be possible to bypass the web application's authentication mechanism
Causes:	Insecure web application programming or configuration
Fix:	Correctly set the "autocomplete" attribute to "off"

Reasoning: AppScan has found that a password field does not enforce the disabling of the autocomplete feature.

Test Requests and Responses:

```
GET /web/guest/home?
p_p_id=com_liferay_login_web_portlet_LoginPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=vi
ew&_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName=%2Flogin%2Flogin&saveLastPath
=false HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/c/portal/login?p_l_id=129
Cookie: COOKIE_SUPPORT=true; GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: Keep-Alive
Host: mcit-liferayqc.linkdev.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Liferay-Portal: Liferay Digital Experience Platform
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Set-Cookie: JSESSIONID=D665878CFE4205F850A8E9C7B1AF8D24; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 10:06:08 GMT
Content-Type: text/html;charset=UTF-8
```

```
<!DOCTYPE html>
```

```
<html class="rtl" dir="rtl" lang="ar-SA">

<head>
 <title>       وزارة الاتصالات وتقنية المعلومات - الرئيسية</title>
  <meta name="viewport" content="width=device-width, width=device-width" />
  <meta name="description" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية " />
  <meta name="keywords" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية">
  <meta name="format-detection" content="telephone=no">
  <meta property="og:url" content="/web/guest/home?
p_p_id=com_liferay_login_web_portlet_LoginPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=vi
ew&_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName=%2Flogin%2Flogin&saveLastPath
=false" />
  <meta property="og:type" content="Website" />
  <meta property="og:title" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية " />
  <meta property="og:description" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية " />
  <meta property="og:image" content="https://mcit-liferayqc.linkdev.com/o/mcit-theme/images/logo-
share.png" />
  <meta property="og:image:secure_url" content="https://mcit-liferayqc.linkdev.com/o/mcit-
theme/images/logo-share.png" />

  <link rel="manifest" href="/o/mcit-theme/manifest.json">

<meta content="text/html; charset=UTF-8" http-equiv="content-type" />

<script type="importmap">{"imports":{"react-dom":"/o/frontend-js-react-
web/__liferay__/exports/react-dom.js","@clayui/breadcrumb":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$breadcrumb.js","@clayui/form":"/o/frontend-taglib-
```

```
clay/__liferay__/exports/@clayui$form.js","@clayui/popover":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$popover.js","@clayui/charts":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$charts.js","@clayui/shared":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$shared.js","@clayui/localized-input":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$localized-input.js","@clayui/modal":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$modal.js","@clayui/empty-state":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$empty-state.js","react":"/o/frontend-js-react-
web/__liferay__/exports/react.js","@clayui/color-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$color-picker.js","@clayui/navigation-bar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$navigation-bar.js","@clayui/pagination":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$pagination.js","@clayui/icon":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$icon.js","@clayui/table":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$table.js","@clayui/autocomplete":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$autocomplete.js","@clayui/slider":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$slider.js","@clayui/management-toolbar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$management-toolbar.js","@clayui/multi-select":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$multi-select.js","@clayui/nav":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$nav.js","@clayui/time-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$time-picker.js","@clayui/provider":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$provider.js","@clayui/upper-toolbar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$upper-toolbar.js","@clayui/loading-indicator":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$loading-indicator.js","@clayui/panel":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$panel.j
...
...
...



<input  class="field form-control"
id="_com_liferay_login_web_portlet_LoginPortlet_mcit-login-password"
name="_com_liferay_login_web_portlet_LoginPortlet_password"    title="كلمة المرور" type="password"
value=""   />


...
...
...
```

L Cacheable SSL Page Found 15

TOC

Issue 1 of 15

TOC

Cacheable SSL Page Found	
Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/o/js_resolve_modules
Entity:	js_resolve_modules (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /o/js_resolve_modules?modules=frontend-js-spa-web%405.0.44%2Finit HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/web/guest/home?
p_p_id=com_liferay_login_web_portlet_LoginPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=vi
ew&_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName=%2Flogin%2Flogin&saveLastPath
=false
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715070788022;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; COOKIE_SUPPORT=true;
GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Accept: */*
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty


HTTP/1.1 200
Connection: keep-alive
Content-Length: 6078
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Cache-Control: no-cache
ETag: W/"d18b97c3-14f5-489a-90fa-791afa57880a"
Set-Cookie: JSESSIONID=FA891FCD20C9A147073C2593CC3ED7A0; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 09:26:50 GMT
Content-Type: application/json;charset=UTF-8

{
 "pathMap": {
         "frontend-js-spa-web@5.0.44\/screen\/ActionURLScreen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/ActionURLScreen",
         "frontend-js-spa-web@5.0.44\/screen\/RenderURLScreen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/RenderURLScreen",
         "frontend-js-spa-web@5.0.44\/surface\/Surface": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/surface\/Surface",
         "frontend-js-spa-web@5.0.44\/cacheable\/Cacheable": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/cacheable\/Cacheable",
         "frontend-js-spa-web@5.0.44\/app\/LiferayApp": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/app\/LiferayApp",
         "frontend-js-spa-web@5.0.44\/app\/App": "\/o\/js\/resolved-module\/frontend-js-
spa-web@5.0.44\/app\/App",
         "frontend-js-spa-web@5.0.44\/screen\/EventScreen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/EventScreen",
         "frontend-js-web@5.0.97\/index": "\/o\/js\/resolved-module\/frontend-js-
web@5.0.97\/index",
         "frontend-js-spa-web@5.0.44\/route\/Route": "\/o\/js\/resolved-module\/frontend-
js-spa-web@5.0.44\/route\/Route",
         "frontend-js-spa-web@5.0.44\/util\/utils": "\/o\/js\/resolved-module\/frontend-
js-spa-web@5.0.44\/util\/utils",
         "frontend-js-spa-web@5.0.44\/util\/pathParser": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/util\/pathParser",
         "frontend-js-spa-web@5.0.44\/screen\/HtmlScreen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/HtmlScreen",
         "frontend-js-spa-web@5.0.44\/init": "\/o\/js\/resolved-module\/frontend-js-spa-
web@5.0.44\/init",
         "frontend-js-spa-web@5.0.44\/screen\/Screen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/Screen",
         "frontend-js-spa-web@5.0.44\/screen\/RequestScreen": "\/o\/js\/resolved-
```

```
module\/frontend-js-spa-web@5.0.44\/screen\/RequestScreen"
 },
 "configMap": {

 },
 "resolvedModules": [
        "frontend-js-web@5.0.97\/index",
        "frontend-js-spa-web@5.0.44\/surface\/Surface",
        "frontend-js-spa-web@5.0.44\/util\/utils",
        "frontend-js-spa-web@5.0.44\/util\/pathParser",
        "frontend-js-spa-web@5.0.44\/route\/Route",
        "frontend-js-spa-web@5.0.44\/cacheable\/Cacheable",
        "frontend-js-spa-web@5.0.44\/screen\/Screen",
        "frontend-js-spa-web@5.0.44\/app\/App",
        "frontend-js-spa-web@5.0.44\/app\/LiferayApp",
        "frontend-js-spa-web@5.0.44\/screen\/RequestScreen",
        "frontend-js-spa-web@5.0.44\/screen\/HtmlScreen",
        "frontend-js-spa-web@5.0.44\/screen\/EventScreen",
        "frontend-js-spa-web@5.0.44\/screen\/ActionURLScreen",
        "frontend-js-spa-web@5.0.44\/screen\/RenderURLScreen",
        "frontend-js-spa-web@5.0.44\/init"
 ],
 "moduleMap": {
        "frontend-js-spa-web@5.0.44\/screen\/ActionURLScreen": {
                ".\/EventScreen": "frontend-js-spa-web@5.0.44\/screen\/EventScreen",
                "..\/util\/utils": "frontend-js-spa-web@5.0.44\/util\/utils"
        }       ,
        "frontend-js-spa-web@5.0.44\/screen\/RenderURLScreen": {
                ".\/EventScreen": "frontend-js-spa-web@5.0.44\/screen\/EventScreen"
        }       ,
        "frontend-js-spa-web@5.0.44\/surface\/Surface": {
                "frontend-js-web": "frontend-js-web@5.0.97\/index"
        }       ,
        "frontend-js-spa-web@5.0.44\/cacheable\/Cacheable": {
                "frontend-js-web": "frontend-js-web@5.0.97\/index"
        }       ,
        "frontend-js-spa-web@5.0.44\/app\/LiferayApp": {
                "..\/surfac
...
...
...
```


Issue 2 of 15

TOC

Cacheable SSL Page Found

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/o/mcit-theme/manifest.json
Entity:	manifest.json (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /o/mcit-theme/manifest.json HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/home/
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Accept: */*
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: manifest


HTTP/1.1 200
Last-Modified: Thu, 02 May 2024 04:58:18 GMT
Connection: keep-alive
Content-Length: 100
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
ETag: W/"100-1714625898000"
Set-Cookie: JSESSIONID=E90AC3E46AEB1D8C025F1F93120E5B4A; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 09:26:51 GMT
Content-Type: application/json

{

"name": "MCIT",

"Short_name": "MCIT",

"display": "fullscreen",

"scope": "/"

}
```

Issue 3 of 15

TOC

Cacheable SSL Page Found

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/o/mcit-theme/fonts/Bukra-Medium.otf
Entity:	Bukra-Medium.otf (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma:

no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
This request/response contains binary content, which is not included in generated reports.
```

Issue 4 of 15

TOC

Cacheable SSL Page Found

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/home
Entity:	home (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /home HTTP/1.1
Sec-Fetch-Site: none
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; _ga=GA1.1.128297136.1599395143;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Upgrade-Insecure-Requests: 1
Sec-Fetch-Mode: navigate
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.7
Sec-Fetch-User: ?1
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: document


HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Liferay-Portal: Liferay Digital Experience Platform
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
```

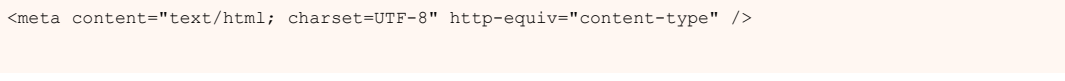
```
Set-Cookie: JSESSIONID=635B598C22E03A9CFB3F7DDDFCEC1274; Path=/; Secure; HttpOnly
Set-Cookie: COOKIE_SUPPORT=true; Max-Age=31536000; Expires=Wed, 07 May 2025 09:26:52 GMT; Path=/;
Secure; HttpOnly
Set-Cookie: GUEST_LANGUAGE_ID=ar_SA; Max-Age=31536000; Expires=Wed, 07 May 2025 09:26:52 GMT;
Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 09:26:54 GMT
Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>
```

```
<html class="rtl" dir="rtl" lang="ar-SA">

<head>
 <title>       وزارة الاتصالات وتقنية المعلومات - الرئيسية</title>
  <meta name="viewport" content="width=device-width, width=device-width" />
  <meta name="description" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية " />
  <meta name="keywords" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية">
  <meta name="format-detection" content="telephone=no">
  <meta property="og:url" content="/home" />
  <meta property="og:type" content="Website" />
  <meta property="og:title" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية " />
  <meta property="og:description" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية " />
  <meta property="og:image" content="https://mcit-liferayqc.linkdev.com/o/mcit-theme/images/logo-
share.png" />
  <meta property="og:image:secure_url" content="https://mcit-liferayqc.linkdev.com/o/mcit-
theme/images/logo-share.png" />

  <link rel="manifest" href="/o/mcit-theme/manifest.json">
```



```
<meta content="text/html; charset=UTF-8" http-equiv="content-type" />
```

```
<script type="importmap">{"imports":{"react-dom":"/o/frontend-js-react-
web/__liferay__/exports/react-dom.js","@clayui/breadcrumb":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$breadcrumb.js","@clayui/form":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$form.js","@clayui/popover":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$popover.js","@clayui/charts":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$charts.js","@clayui/shared":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$shared.js","@clayui/localized-input":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$localized-input.js","@clayui/modal":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$modal.js","@clayui/empty-state":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$empty-state.js","react":"/o/frontend-js-react-
web/__liferay__/exports/react.js","@clayui/color-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$color-picker.js","@clayui/navigation-bar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$navigation-bar.js","@clayui/pagination":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$pagination.js","@clayui/icon":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$icon.js","@clayui/table":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$table.js","@clayui/autocomplete":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$autocomplete.js","@clayui/slider":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$slider.js","@clayui/management-toolbar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$management-toolbar.js","@clayui/multi-select":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$multi-select.js","@clayui/nav":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$nav.js","@clayui/time-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$time-picker.js","@clayui/provider":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$provider.js","@clayui/upper-toolbar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$upper-toolbar.js","@clayui/loading-indicator":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$loading-indicator.js","@clayui/panel":"/o/frontend-
...
...
...
```

Issue 5 of 15

TOC

Cacheable SSL Page Found

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/documents/d/guest/mcit-home-newsletter-ar
Entity:	mcit-home-newsletter-ar (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /documents/d/guest/mcit-home-newsletter-ar HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/home
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0; _ga=GA1.1.128297136.1599395143;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0; COOKIE_SUPPORT=true;
GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty


HTTP/1.1 200
Last-Modified: Thu, 28 Mar 2024 09:09:12 GMT
Connection: keep-alive
Content-Length: 949
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Cache-Control: private
Content-Disposition: attachment; filename="mcit-home-newsletter-ar.json"
Set-Cookie: JSESSIONID=3247456FD5648D779BFC8C996BCF4BAD; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 09:26:51 GMT
Content-Type: application/json

{

"subscribe": "اشترك",

"now": "الآن",

"email": "البريد الإلكتروني",

"enterYourEmail": "أدخل بريدك الإلكتروني",

"subscriptionParagraph": "للتعرف على أحدث المعلومات عن وزارة الاتصالات وتكنولوجيا المعلومات وكافة الجهات
التابعة لها",

"subscribedSuccessfully": "لقد اشتركت في النشرة الإخبارية لدينا بنجاح",

"serverError": "خطأ في الخادم الداخلي",

"Subscribe Now": "اشترك الآن",

"subscribed": "مشترك",

"Thanks for subscribing": "شكرا على الإشتراك",

"email-already-in-use-in-newsletter": "هذا البريد الألكتروني قيد الأستخدام بالفعل. يرجى إدخال بريد
الكتروني فريد",

"emailValidation": "الرجاء إدخال عنوان بريد إلكتروني صالح"

}
```

Issue 6 of 15

TOC

Cacheable SSL Page Found

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/documents/d/guest/mcit-individual-registration-ar
Entity:	mcit-individual-registration-ar (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /documents/d/guest/mcit-individual-registration-ar HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/individual-registeration
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: __gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-
ZDNGS8OTIECFDg; _ga=GA1.1.128297136.1599395143;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0; LFR_SESSION_STATE_20099=1715071585564;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0; COOKIE_SUPPORT=true;
GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty


HTTP/1.1 200
Last-Modified: Mon, 29 Apr 2024 16:36:20 GMT
Connection: keep-alive
Content-Length: 5097
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Cache-Control: private
Content-Disposition: attachment; filename="mcit-individual-registration-ar.json"
Set-Cookie: JSESSIONID=40CF2C04CD055BC7D70572C46789956B; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 09:31:39 GMT
Content-Type: application/json

{

"createAcc": "إنشاء حساب",

"fieldsValidationWarning": "جميع الحقول التي تحمل علامة النجمة",

"mandatory": "إلزامية",

"basicInfo": "معلومات اساسية",

"contactInfo": "معلومات الاتصال",
```

```
"fullNameEn": "(الاسم الكامل (باللغة الإنجليزية)",
"fullNameAr": "(الاسم الكامل (باللغة العربية)",
"firstName": "الاسم الأول",
"lastName": "الاسم الأخير",
"english": "(الإنجليزية)",
"arabic": "(العربية)",
"dateOfBirth": "تاريخ الميلاد",
"gender": "الجنس",
"male": "ذكر",
"female": "انثى",
"nationality": "الجنسية",
"countryOfResidence": "دولة الإقامة الحالية",
"city": "المدينة",
"passportIdResidenceNumber": "رقم جواز السفر / الإقامة / الهوية",
"next": "التالى",
"cancel": "إلغاء",
"email": "البريد الإلكتروني",
"verify": "تأكيد",
"username": "اسم المستخدم",
"password": "كلمة المرور",
"retypePassword": "تأكيد كلمة المرور",
"mobileNum": "رقم الجوال",
"previous": "السابق",
"success": "نجاح",
"accountSuccess": "لقد تم إنشاء حسابك بنجاح",
"goToHomepage": "انتقل إلى الصفحة الرئيسية",
"otpEmailTitle": "الرجاء إدخال كلمة المرور لمرة واحدة للتحقق من بريدك الإلكتروني",
"otpMobileTitle": "يتم إرسال رسالة نصية قصيرة تحتوي على كلمة مرور لمرة واحدة إلى رقم هاتفك المحمول",
"oneTimePass": "تم إرسال كلمة المرور لمرة واحدة إلى",
"codeValidity": "الكود صالح ل",
"minute": "دقيقة",
"validate": "التحقق",
"resendPassword": "إعادة إرسال كلمة المرور لمرة واحدة",
"wrongEmail": "أدخلت بريدا إلكترونيا خاطئا؟",
"submit": "سجل",
"select": "أختر",
"retriesExpired": "انتهت صلاحية محاولات التحقق من الرمز",
"codeError": "رمز التحقق غير صالح.",
"serverError": "هناك خطأ ما.",
```

```
"timeExpired": "انتهى الوقت برجاء إعادة إرسال رمز التحقق",

"tryAgain": "حاول مرة أخرى",

"verifyEmail": "يرجى التحقق من البريد الإلكتروني الخاص بك",

"verifyMobile": "يرجى التحقق من رقم هاتفك المحمول.",

"invalid-english-names": "يجب عليك إدخال الاسم الأول واسم العائلة باللغة الإنجليزية",

"invalid-arabic-names": "يجب عليك إدخال الاسم الأول واسم العائلة باللغة العربية",

"mobile-phone-exist": "الهاتف المحمول الذي أدخلته موجود بالفعل",

"Identity-number-exist": "رقم الهوية الذي قمت بإدخاله موجود بالفعل",

"not-same-password": "تأكيد كلمة المرور التي أدخلتها لا يتطابق مع كلمة المرور",

"email-exist": "البريد الإلكتروني الذي أدخلته موجود بالفعل",

"token-expired": "لقد وصلت إلى الحد اليومي.",

"server-error": "هناك خطأ ما.",

"firstNameLastNameErrorEn": "يرجى التأكد من إدخال الاسم الأول واسم العائلة باللغة الإنجليزية",

"LastNameArError": "يرجى التأكد من إدخال اسم العائلة باللغة العربية",

"firstNameArError": "يرجى التأكد من إدخال الاسم الأول باللغة العربية",

"firstNameLastNameError": "الرجاء إدخال الاسم الأول واسم العائلة على الأقل بأي لغة",

"LastNameEnError": "يرجى التأكد من إدخال اسم العائلة باللغة الانجليزية",

"firstNameEnError": "يرجى التأكد من إدخال الاسم الأول باللغة الانجليزية",

"confirmation-password-must-be-the-same-as-the-password": "تأكيد كلمة المرور يجب أن تكون هي نفس كلمة
المرور.",

"passwordPattern": "يجب أن تتكون من 6 إلى 20 حرفًا. يجب أن تحتوي على أحرف و أرقام و رموز",

"pleaseVerify": "برجاء التحقق",

"arabicPattern": "الرجاء ادخال حروف عربية فقط",

"englishPattern": "الرجاء ادخال حروف انجليزية فقط",

"failure": "خطاء",

"emailValidation": "الرجاء إدخال عنوان بريد إلكتروني صالح",

"required": "هذا الحقل مطلوب",

"phoneValida
...
...
...
```

Cacheable SSL Page Found

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/individual-registeration
Entity:	individual-registeration (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /individual-registeration HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/client
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: __gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-
ZDNGS8OTIECFDg; _ga=GA1.1.128297136.1599395143;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0; LFR_SESSION_STATE_20099=1715071579366;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0; COOKIE_SUPPORT=true;
GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
x-csrf-token: VIjAd6Jf
x-requested-with: XMLHttpRequest
sec-ch-ua-mobile: ?0
x-pjax: true
Accept: */*
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty


HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Liferay-Portal: Liferay Digital Experience Platform
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Set-Cookie: JSESSIONID=B2653273E5210639E1A1EE82BA4C2114; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 09:30:25 GMT
Content-Type: text/html;charset=UTF-8
```

```
<!DOCTYPE html>
```

```
<html class="rtl" dir="rtl" lang="ar-SA">

<head>
 <title>       وزارة الاتصالات وتقنية المعلومات - تسجيل الأفراد</title>
  <meta name="viewport" content="width=device-width, width=device-width" />
  <meta name="description" content="تسجيل الأفراد - وزارة الاتصالات وتقنية المعلومات" />
  <meta name="keywords" content="تسجيل الأفراد - وزارة الاتصالات وتقنية المعلومات">
  <meta name="format-detection" content="telephone=no">
  <meta property="og:url" content="/individual-registeration" />
  <meta property="og:type" content="Website" />
  <meta property="og:title" content="تسجيل الأفراد - وزارة الاتصالات وتقنية المعلومات" />
  <meta property="og:description" content="تسجيل الأفراد - وزارة الاتصالات وتقنية المعلومات" />
  <meta property="og:image" content="https://mcit-liferayqc.linkdev.com/o/mcit-theme/images/logo-
share.png" />
  <meta property="og:image:secure_url" content="https://mcit-liferayqc.linkdev.com/o/mcit-
theme/images/logo-share.png" />

  <link rel="manifest" href="/o/mcit-theme/manifest.json">

<meta content="text/html; charset=UTF-8" http-equiv="content-type" />

<script type="importmap">{"imports":{"react-dom":"/o/frontend-js-react-
web/__liferay__/exports/react-dom.js","@clayui/breadcrumb":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$breadcrumb.js","@clayui/form":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$form.js","@clayui/popover":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$popover.js","@clayui/charts":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$charts.js","@clayui/shared":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$shared.js","@clayui/localized-input":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$localized-input.js","@clayui/modal":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$modal.js","@clayui/empty-state":"/o/frontend-taglib-
```

```
clay/__liferay__/exports/@clayui$empty-state.js","react":"/o/frontend-js-react-
web/__liferay__/exports/react.js","@clayui/color-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$color-picker.js","@clayui/navigation-bar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$navigation-bar.js","@clayui/pagination":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$pagination.js","@clayui/icon":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$icon.js","@clayui/table":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$table.js","@clayui/autocomplete":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$autocomplete.js","@clayui/slider":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$slider.js","@clayui/management-toolbar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$management-toolbar.js","@clayui/multi-select":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$multi-select.js","@clayui/nav":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$nav.js","@clayui/time-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$time-picker.js","@clayui/provider":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$provider.js","@clayui/upper-toolbar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$upper-toolbar.js","@clayui/loading-indicator":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$loading-indicator.js","@clayui/panel":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$panel.js","@clayui/drop-down":"/o/frontend-taglib-
clay/__li
...
...
...
```

Issue 8 of 15

TOC

Cacheable SSL Page Found

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/account-type
Entity:	account-type (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /account-type HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/web/guest/home?
p_p_id=com_liferay_login_web_portlet_LoginPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=vi
ew&_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName=%2Flogin%2Flogin&saveLastPath
=false
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
LFR_SESSION_STATE_20099=1715071553037; _ga=GA1.1.128297136.1599395143;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0; COOKIE_SUPPORT=true;
GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: keep-alive
```

```
Host: mcit-liferayqc.linkdev.com
Upgrade-Insecure-Requests: 1
Sec-Fetch-Mode: navigate
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.7
Sec-Fetch-User: ?1
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: document


HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Liferay-Portal: Liferay Digital Experience Platform
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Set-Cookie: JSESSIONID=BBEB3B653EB0A4BF373F5C5EF8C77970; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 09:28:41 GMT
Content-Type: text/html;charset=UTF-8
```

```
<!DOCTYPE html>
```

```
<html class="rtl" dir="rtl" lang="ar-SA">

<head>
 <title>       اختيارات التسجيل - وزارة الاتصالات وتقنية المعلومات</title>
  <meta name="viewport" content="width=device-width, width=device-width" />
  <meta name="description" content="اختيارات التسجيل - وزارة الاتصالات وتقنية المعلومات" />
  <meta name="keywords" content="اختيارات التسجيل - وزارة الاتصالات وتقنية المعلومات">
  <meta name="format-detection" content="telephone=no">
  <meta property="og:url" content="/account-type" />
  <meta property="og:type" content="Website" />
  <meta property="og:title" content="اختيارات التسجيل - وزارة الاتصالات وتقنية المعلومات" />
  <meta property="og:description" content="اختيارات التسجيل - وزارة الاتصالات وتقنية المعلومات" />
  <meta property="og:image" content="https://mcit-liferayqc.linkdev.com/o/mcit-theme/images/logo-
share.png" />
  <meta property="og:image:secure_url" content="https://mcit-liferayqc.linkdev.com/o/mcit-
theme/images/logo-share.png" />

  <link rel="manifest" href="/o/mcit-theme/manifest.json">
```

```
<meta content="text/html; charset=UTF-8" http-equiv="content-type" />
```

```
<script type="importmap">{"imports":{"react-dom":"/o/frontend-js-react-
web/__liferay__/exports/react-dom.js","@clayui/breadcrumb":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$breadcrumb.js","@clayui/form":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$form.js","@clayui/popover":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$popover.js","@clayui/charts":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$charts.js","@clayui/shared":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$shared.js","@clayui/localized-input":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$localized-input.js","@clayui/modal":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$modal.js","@clayui/empty-state":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$empty-state.js","react":"/o/frontend-js-react-
web/__liferay__/exports/react.js","@clayui/color-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$color-picker.js","@clayui/navigation-bar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$navigation-bar.js","@clayui/pagination":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$pagination.js","@clayui/icon":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$icon.js","@clayui/table":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$table.js","@clayui/autocomplete":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$autocomplete.js","@clayui/slider":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$slider.js","@clayui/management-toolbar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$management-toolbar.js","@clayui/multi-select":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$multi-select.js","@clayui/nav":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$nav.js","@clayui/time-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$time-picker.js","@clayui/provider":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$provider.js","@clayui/
...
...
...
```

Cacheable SSL Page Found

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/web/guest/recruitment-options
Entity:	recruitment-options (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /web/guest/recruitment-options HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/home/client
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
LFR_SESSION_STATE_20099=1715073020896; _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073077970;
_ga=GA1.1.128297136.1599395143;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
ID=78692f674d56476771344b754c46314878394f5043513d3d; COMPANY_ID=20096; COOKIE_SUPPORT=true;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; GUEST_LANGUAGE_ID=ar_SA
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
x-csrf-token: MEQeGkLB
x-requested-with: XMLHttpRequest
sec-ch-ua-mobile: ?0
x-pjax: true
Accept: */*
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty


HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Liferay-Portal: Liferay Digital Experience Platform
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Set-Cookie: JSESSIONID=F5FEF704BF4BA09031B6F515D64F384F; Path=/; Secure; HttpOnly
```

```
Date: Tue, 07 May 2024 09:55:26 GMT
Content-Type: text/html;charset=UTF-8
```

```
<!DOCTYPE html>
```

```
<html class="rtl" dir="rtl" lang="ar-SA">

<head>
 <title>       التوظيف - وزارة الاتصالات وتقنية المعلومات</title>
  <meta name="viewport" content="width=device-width, width=device-width" />
  <meta name="description" content="التوظيف - وزارة الاتصالات وتقنية المعلومات" />
  <meta name="keywords" content="التوظيف - وزارة الاتصالات وتقنية المعلومات">
  <meta name="format-detection" content="telephone=no">
  <meta property="og:url" content="/web/guest/recruitment-options" />
  <meta property="og:type" content="Website" />
  <meta property="og:title" content="التوظيف - وزارة الاتصالات وتقنية المعلومات" />
  <meta property="og:description" content="التوظيف - وزارة الاتصالات وتقنية المعلومات" />
  <meta property="og:image" content="https://mcit-liferayqc.linkdev.com/o/mcit-theme/images/logo-
share.png" />
  <meta property="og:image:secure_url" content="https://mcit-liferayqc.linkdev.com/o/mcit-
theme/images/logo-share.png" />

  <link rel="manifest" href="/o/mcit-theme/manifest.json">
```

```
<meta content="text/html; charset=UTF-8" http-equiv="content-type" />
```

```
<script type="importmap">{"imports":{"react-dom":"/o/frontend-js-react-
web/__liferay__/exports/react-dom.js","@clayui/breadcrumb":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$breadcrumb.js","@clayui/form":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$form.js","@clayui/popover":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$popover.js","@clayui/charts":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$charts.js","@clayui/shared":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$shared.js","@clayui/localized-input":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$localized-input.js","@clayui/modal":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$modal.js","@clayui/empty-state":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$empty-state.js","react":"/o/frontend-js-react-
web/__liferay__/exports/react.js","@clayui/color-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$color-picker.js","@clayui/navigation-bar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$navigation-bar.js","@clayui/pagination":
...
...
...
```

Issue 10 of 15

TOC

Cacheable SSL Page Found

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/documents/d/guest/mcit-forgot-password-ar
Entity:	mcit-forgot-password-ar (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /documents/d/guest/mcit-forgot-password-ar HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/forgot-password
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0; _ga=GA1.1.128297136.1599395143;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
LFR_SESSION_STATE_20099=1715072841895; COOKIE_SUPPORT=true; GUEST_LANGUAGE_ID=ar_SA;
JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
```

```
sec-ch-ua-mobile: ?0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty


HTTP/1.1 200
Last-Modified: Wed, 24 Apr 2024 13:27:31 GMT
Connection: keep-alive
Content-Length: 2235
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Cache-Control: private
Content-Disposition: attachment; filename="mcit-forgot-password-ar.json"
Set-Cookie: JSESSIONID=0F0DFD74A77BBD676A494719AB589010; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 09:52:24 GMT
Content-Type: application/json

{

"forgotPassword": "هل نسيت كلمة السر",

"fieldsValidationWarning": "أحد الحقول",

"mandatory": "إلزامية",

"passportIdResidenceNumber": "رقم جواز السفر/الإقامة/الهوية",

"passportIdResidenceCommercialNumber": "رقم جواز السفر/الإقامة/رقم السجل",

"individual": "فرد",

"corporate": "شركة",

"chooseBetweenIndividualOrCorporate": "اختر بين فرد أو شركة",

"cancel": "إلغاء",

"email": "البريد الإلكتروني",

"username": "اسم المستخدم",

"mobileNum": "رقم الجوال",

"success": "نجاح",

"accountSuccess": "تم إرسال بريد إلكتروني إليك، يرجى التحقق من بريدك.",

"goToHomepage": "انتقل إلى الصفحة الرئيسية",

"submit": "سجل",

"failure": "فشل",

"tryAgain": "حاول مرة أخرى",

"captchaError": "ادخل رمز التحقق",

"recaptcha-is-not-valid": "الرمز غير محقق",

"please-provide-your-data": "ارجوا ادخال البيانات",

"invalid-user-email": "البريد الالكترونى غير صحيح",

"email-does-not-match-commercial-number": "البريد الإلكتروني غير مطابق للرقم السجل.",

"no-information-stored-this-user": "لا توجد معلومات مخزنة لهذا المستخدم.",

"email-does-not-match-identity-number": "البريد الإلكتروني لا يطابق رقم الهوية.",

"invalid-corpRegister-Number-or-individualId": "رقم الهوية / رقم التسجيل غير صحيح",

"serverError": "خطأ في الخادم الداخلي",

"searchCountry": "أبحث عن البلد",

"invalidFormErrorMsg": "الرجاء إدخال قيمة واحدة على الأقل من المدخلات التالية: البريد الإلكتروني أو رقم
```

```
جواز السفر/الإقامة/الهوية/رقم السجل",

"mcit-logo": "وزارة الاتصالات وتقنية المعلومات",

"password-should-not-equal-old-password": "كلمة المرور الجديدة يجب ألا تكون نفس كلمة المرور القديمة"

}
```


Issue 11 of 15

TOC

Cacheable SSL Page Found

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/documents/d/guest/mcit-recruitment-ar
Entity:	mcit-recruitment-ar (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:


```
GET /documents/d/guest/mcit-recruitment-ar HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
LFR_SESSION_STATE_20099=1715073020896; _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073208993;
_ga=GA1.1.128297136.1599395143; _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25Ecjlzbmxl ZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEalliOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
```

```
sec-ch-ua-mobile: ?0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty


HTTP/1.1 200
Last-Modified: Wed, 01 May 2024 09:19:12 GMT
Connection: keep-alive
Content-Length: 3364
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Cache-Control: private
Content-Disposition: attachment; filename="mcit-recruitment-ar.json"
Set-Cookie: JSESSIONID=A5CBB5C122EF39975B08A91BF0654E96; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 09:58:30 GMT
Content-Type: application/json

{

"fullNameEn": "(الاسم الكامل (باللغة الإنجليزية",

"fullNameAr": "(الاسم الكامل (باللغة العربية",

"dateOfBirth": "تاريخ الميلاد",

"nationality": "الجنسية",

"countryOfResidence": "دولة الإقامة الحالية",

"city": "المدينة",

"gender": "الجنس",

"male": "ذكر",

"female": "انثى",

"noDataFound": "لا يوجد بيانات",

"passportIdResidenceNumber": "رقم جواز السفر / الإقامة / الهوية",

"educationQualification": "المؤهلات التعليمية",

"anotherEducationQualification": "مؤهل دراسي آخر",

"Qualification": "المؤهل الدراسى",

"QualificationFrom": "من",

"graduationDate": "سنة التخرج",

"universityName": "اسم الجامعة",

"specialization": "التخصص",

"average": "المعدل",

"add": "أضف",

"delete": "مسح",

"listOfExperience": "مجال الخبرة",

"professionalExperience": "الخبرة العملية",

"anotherExperienceQualification": "خبرة عملية أخرى",

"jobTitle": "المسمى الوظيفى",

"employer": "جهة العمل الحالية",

"dateFrom": "التاريخ من",

"dateTo": "التاريخ الى",

"experienceYears": "عدد سنوات الخبرة",
```

```
"dateRangeError": "التاريخ الى يجب ان يكون أكبر من التاريخ من",
"currentJob": "الوظيفة الحالية",
"personalInfo": "المعلومات الشخصية",
"contactInfo": "معلومات التواصل",
"email": "البريد الإلكتروني",
"countryCode": "مفتاح الدولة",
"mobile": "رقم الجوال",
"emailValidation": "يرجى إدخال البريد الإلكتروني الصحيح.",
"address": "عنوان السكن",
"fieldOfInterest": "مجال الاهتمام",
"SubmissionData": "بيانات التقديم",
"other": "أخرى",
"alreadyRegistered": "هل أنت مسجل في نظام المؤسسة العامة للتأمينات الاجتماعية؟",
"acknowledgment": "الإقرار بالتعهد والشروط؟ ",
"captchaError": "ادخل رمز التحقق",
"submit": "سجل",
"identityType": "نوع الهوية",
"arabicFieldHint": "يرجى كتابة الحروف العربية فقط",
"englishFieldHint": "يرجى كتابة الرسالة الإنجليزية فقط",
"serverError": "عفوا.. حدث خطأ فني",
"cvError": "الرجاء ارفاق ملف السير الذاتية",
"cv": "السيرة الذاتية",
"nameHint": "الاسم يجب أن يتطابق مع الهوية أو جواز السفر",
"tryAgain": "حاول مرة أخرى",
"accountSuccess": "تم تقديم طلبك بنجاح",
"goToHomepage": "انتقل إلى الصفحة الرئيسية",
"success": "نجاح",
"failure": "خطاء",
"select": "أختر",
"cvMaxSizeError": "يرجى
...
...
...
```


Issue 12 of 15

TOC

Cacheable SSL Page Found

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/o/mcit-theme/js/main.js
Entity:	main.js (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /o/mcit-theme/js/main.js?browserId=chrome&minifierType=js&languageId=ar_SA&t=1714625928000
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/home
Cookie: COOKIE_SUPPORT=true; GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: Keep-Alive
Host: mcit-liferayqc.linkdev.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Connection: keep-alive
Content-Length: 27499
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private, no-cache
ETag: "kFgoIi/8sb1shEv9SFvX5UtoQwQ="
Set-Cookie: JSESSIONID=8FA23E6882610B947A206F3B8C14EA7E; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 10:00:59 GMT
Content-Type: text/javascript

/*1714625900000*/
AUI().ready("liferay-sign-in-modal", function () {

  //Header
  if ($(".header").length) {
    $(window).on("scroll", function () {
      // sticky header
      let stickyheader = $(window).scrollTop();

      if (stickyheader > 0) {
        $(".header").addClass("is-fixed");
      } else {
        $(".header").removeClass("is-fixed");
      }
    });
    if(window.scrollY > 0) {
      $(".header").addClass("is-fixed");
    } else {
      $(".header").removeClass("is-fixed");
    }
    function signIn(){
      if($(".sign-in").length){
        $(".header .navbar-nav:last-child .navbar-nav-item,.header .navbar-nav .nav-
item").addClass("navbar-nav-item-sperate")
```

```
      }
    }
      if (window.innerWidth >= 1200) {
          signIn();
      }
      $(window).resize(function(){
        if ($(window).width() >= 1200){
          signIn();
        }
      });

  }

  // Control Menu
  if($(".cadmin .control-menu-nav").length){
    $(".header").addClass("header-dropdown");
  }
  // language selector
  if ($(".language-selector").length) {

    $(".language-selector").each(function () {
      let languageText = $(this).find("a.language-entry-long-text").text();
      $(this).attr("title", languageText);
      if($("html").attr("dir") == "rtl"){
        $(this).attr("title","English");
      }
    });
  }
  if ($(".img-download").length) {
    $('.btn.btn-primary.mr-auto.text-decoration-none, .img-download').off('click');
}

if ($(".img-download").length) {
    $('.btn.btn-primary.mr-auto.text-decoration-none, .img-download').on('click', function
(event) {
        event.preventDefault();
        var fileUrls = []; // Array to store all image URLs
        // Iterate through each .img-download element and extract the href attribute
        $(".img-download").each(function () {
          var fileUrl = $(this).attr('href');
          fileUrls.push(fileUrl); // Push each URL to the array
        });

        // Create and click download anchor for each URL in the array
        fileUrls.forEach(function (fileUrl) {
          var anchor = document.createElement('a');
          anchor.href = fileUrl;
          anchor.download = '';
          document.body.appendChild(anchor);
          anchor.click();
          document.body.removeChild(anchor);
        });
    });
}

if ($(".img-download2").length) {
  $('.img-download2').off('click');
}

if ($(".img-download2").length) {
  $('.img-download2').on('click', function (event) {
      event.preventDefault();
      var fileUrls = []; // Array to store all image URLs

      // Iterate through each .img-download element and extract the href attribute
      $(".img-download2").each(function () {
          var fileUrl = $(this).attr('href');
          fileUrls.push(fileUrl); // Push each URL to the array
      });

      // Create and click download anchor for each URL in the array
      fileUrls.forEach(function (fileUrl) {
          var anchor = document.createElement('a');
          anchor.href = fileUrl;
          anchor.download = '';
          document.body.appendChild(anchor);
          anchor.click();
          document.body.removeChild(anchor);
```

```
        });
    });
}
    //user control
    if ($(".user-control").length) {
      $(".user-control .personal-menu-dropdown button")
        .html(`<span class="icon-login"></span>`)
        .removeAttr("title");
    }
    //breadcrumb
    if($(".breadcrumb-banner").length){
        $("footer").addClass("footer-inners");
        if($(".breadcrumb-text-truncate").length){
          let breadcrumbText = $(".breadcrumb-text-truncate").text();
          $(".breadcrumb-text-truncate").attr("title",breadcrumbText);
        }
        $(".breadcrumb-banner .breadcrumb-item:nth-child(2).first a").each(function(){
            $(this).attr("href",".");
        });
        $(".breadcrumb-banner .breadcrumb-item a[href='.']").on("click",function(event){
            event.preventDefault();
      });

...
...
...
```

Issue 13 of 15

TOC

Cacheable SSL Page Found

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/o/frontend-js-loader-modules-extender/loader.js
Entity:	loader.js (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /o/frontend-js-loader-modules-extender/loader.js?
mac=9WaMmhziBCkScHZwrrVcOR7VZF4=&browserId=chrome&languageId=ar_SA&minifierType=js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/home
Cookie: COOKIE_SUPPORT=true; GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: Keep-Alive
Host: mcit-liferayqc.linkdev.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
```

```
HTTP/1.1 200
Connection: keep-alive
Content-Length: 24414
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private, no-cache
ETag: "UeHU783LuYBJeOHynIKoUxHoBjk="
Set-Cookie: JSESSIONID=8A531D1BD14FED57D78D89F3EFFD7DEF; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 09:59:39 GMT
Content-Type: text/javascript

/*1708528392000*/
(()=>{"use strict";(()=>{var e=function e(){throw function(e,t){if(!(e instanceof t))throw new
TypeError("Cannot call a class as a function")}(this,e),new Error("Don't construct
ResolvablePromise objects directly: rely on ResolvablePromise.new() instead")};function t(e)
{if(e.fulfilled)throw new Error("Promise already fulfilled")}function n(e,t){for(var
n=0;n<t.length;n++){var r=t[n];r.enumerable=r.enumerable||!1,r.configurable=!0,"value"in r&&
(r.writable=!0),Object.defineProperty(e,r.key,r)}}e.new=function(){var e={},n=new
Promise((function(t,n){e._resolve=t,e._reject=n}));return Object.assign(n,e,
{fulfilled:!1,rejected:!1,rejection:void 0,resolution:void 0,resolved:!1}),n.resolve=function(e)
{return function(e,n){t(e),e.fulfilled=!0,e.resolved=!0,e.resolution=n,e._resolve(n)}
(n,e)},n.reject=function(e){return function(e,n)
{t(e),e.fulfilled=!0,e.rejected=!0,e.rejection=n,e._reject(n)}(n,e)},"undefined"!=typeof
jest&&n.catch((function(){})),n};var r=function(){function t(n){!function(e,t){if(!(e instanceof
t))throw new TypeError("Cannot call a class as a function")}
(this,t),this._name=n,this._dependencies=void 0,this._factory=void 0,this._implementation=
{},this._useESM=!1,this._map=void 0,this._state=
{_define:e.new(),_fetch:e.new(),_implement:e.new()}}var r,o;return r=t,(o=
[{key:"name",get:function(){return this._name},set:function(e){throw new Error("Name of module
".concat(this.name," is read-only"))}},{key:"dependencies",get:function(){return
this._dependencies},set:function(e){if(this._dependencies)throw new Error("Dependencies of module
".concat(this.name," already set"));this._dependencies=e}},{key:"factory",get:function(){return
this._factory},set:function(e){if(this._factory)throw new Error("Factory of module
".concat(this.name," already set"));this._factory=e}},{key:"implementation",get:function(){return
this._implementation},set:function(e){this._implementation=e}},{key:"map",get:function(){return
this._map},set:function(e){if(this._map)throw new Error("Local module map of module
".concat(this.name," already set"));this._map=e}},{key:"esModule",get:function(){return
this._implementation.__esModule},set:function(e)
{Object.defineProperty(this._implementation,"__esModule",
{configurable:!0,value:e,writable:!0})}},{key:"fetch",get:function(){return this._state._fetch}},
{key:"fetched",get:function(){return this.fetch.resolved}},{key:"define",get:function(){return
this._state._define}},{key:"defined",get:function(){return this.define.resolved}},
{key:"implement",get:function(){return this._state._implement}},{key:"implemented",get:function()
{return this.implement.resolved}},{key:"useESM",get:function(){return
this._useESM},set:function(e){this._useESM=e}}])&&n(r.prototype,o),t}();function o(e)
{return(o="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(e){return typeof
e}:function(e){return e&&"function"==typeof
Symbol&&e.constructor===Symbol&&e!==Symbol.prototype?"symbol":typeof e})(e)}function i(e,t)
{return function(e){if(Array.isArray(e))return e}(e)||function(e,t){var n=null==e?
null:"undefined"!=typeof Symbol&&e[Symbol.iterator]||e["@@iterator"];if(null!=n){var r,o,i=
[],a=!0,l=!1;try{for(n=n.call(e);!(a=(r=n.next()).done)&&
(i.push(r.value),!t||i.length!==t);a=!0);}catch(e)
{l=!0,o=e}finally{try{a||null==n.return||n.return()}finally{if(l)throw o}}return i}}
(e,t)||function(e,t){if(e){if("string"==typeof e)return a(e,t);var
n=Object.prototype.toString.call(e).slice(8,-1);return"Object"===n&&e.constructor&&
(n=e.constructor.name),"Map"===n||"Set"===n?
Array.from(e):"Arguments"===n||/^(?:Ui|I)nt(?:8|16|32)(?:Clamped)?Array$/.test(n)?a(e,t):void 0}}
(e,t)||function(){throw new TypeError("Invalid attempt to destructure non-iterable instance.\nIn
order to be iterable, non-array objects must have a [Symbol.iterator]() method.")}()}function
a(e,t){(null==t||t>e.length)&&(t=e.length);for(var n=0,r=new Array(t);n<t;n++)r[n]=e[n];return
r}function l(e,t){if(!(e instanceof t))throw new TypeError("Cannot call a class as a
function")}functi
...
...
...
```

Cacheable SSL Page Found

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/recruitment
Entity:	recruitment (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /recruitment?isFresh=true HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/c
Cookie: COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: Keep-Alive
Host: mcit-liferayqc.linkdev.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Liferay-Portal: Liferay Digital Experience Platform
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Set-Cookie: JSESSIONID=05290F490FA0F0E6888471823A352D11; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 10:04:44 GMT
Content-Type: text/html;charset=UTF-8
```

```
<!DOCTYPE html>
```

```
<html class="rtl" dir="rtl" lang="ar-SA">

<head>
 <title>       وزارة الاتصالات وتقنية المعلومات - التوظيف</title>
  <meta name="viewport" content="width=device-width, width=device-width" />
  <meta name="description" content="وزارة الاتصالات وتقنية المعلومات - التوظيف " />
  <meta name="keywords" content="وزارة الاتصالات وتقنية المعلومات - التوظيف">
  <meta name="format-detection" content="telephone=no">
```

```
  <meta property="og:url" content="/recruitment?isFresh=true" />
  <meta property="og:type" content="Website" />
  <meta property="og:title" content="التوظيف - وزارة الاتصالات وتقنية المعلومات" />
  <meta property="og:description" content="التوظيف - وزارة الاتصالات وتقنية المعلومات" />
  <meta property="og:image" content="https://mcit-liferayqc.linkdev.com/o/mcit-theme/images/logo-
share.png" />
  <meta property="og:image:secure_url" content="https://mcit-liferayqc.linkdev.com/o/mcit-
theme/images/logo-share.png" />

  <link rel="manifest" href="/o/mcit-theme/manifest.json">
```

```
<meta content="text/html; charset=UTF-8" http-equiv="content-type" />
```

```
<script type="importmap">{"imports":{"react-dom":"/o/frontend-js-react-
web/__liferay__/exports/react-dom.js","@clayui/breadcrumb":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$breadcrumb.js","@clayui/form":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$form.js","@clayui/popover":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$popover.js","@clayui/charts":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$charts.js","@clayui/shared":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$shared.js","@clayui/localized-input":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$localized-input.js","@clayui/modal":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$modal.js","@clayui/empty-state":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$empty-state.js","react":"/o/frontend-js-react-
web/__liferay__/exports/react.js","@clayui/color-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$color-picker.js","@clayui/navigation-bar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$navigation-bar.js","@clayui/pagination":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$pagination.js","@clayui/icon":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$icon.js","@clayui/table":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$table.js","@clayui/autocomplete":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$autocomplete.js","@clayui/slider":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$slider.js","@clayui/management-toolbar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$management-toolbar.js","@clayui/multi-select":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$multi-select.js","@clayui/nav":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$nav.js","@clayui/time-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$time-picker.js","@clayui/provider":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$provider.js","@clayui/upper-toolbar":"/o/frontend-taglib-
```

```
clay/__liferay__/exports/@clayui$upper-toolbar.js","@clayui/loading-indicator":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$loading-indicator.js","@clayui/panel":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$panel.js","@clayui/drop-down":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$drop-down.js","@clayui/list":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$list.js","@clayui/date-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$date-picker.js","@clayui/label":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$label.js","@clayui/data-provider":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$data-provider.js","@liferay/frontend-js-api/data-
set":"/o/frontend-js-dependencies-web/__liferay__/exports/@liferay$js-api$data-
set.js","@clayui/core":"/o/frontend-taglib-clay/__liferay__/exports/@clayui$core.
...
...
...
```

Issue 15 of 15

TOC

Cacheable SSL Page Found

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/web/guest/home
Entity:	home (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /web/guest/home?
p_p_id=com_liferay_login_web_portlet_LoginPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=vi
ew&_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName=%2Flogin%2Flogin&saveLastPath
=false HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/c/portal/login?p_l_id=129
Cookie: COOKIE_SUPPORT=true; GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: Keep-Alive
Host: mcit-liferayqc.linkdev.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Liferay-Portal: Liferay Digital Experience Platform
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Set-Cookie: JSESSIONID=83F99BB5369AC6AA3CDC7BA3BC14493D; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 10:04:14 GMT
Content-Type: text/html;charset=UTF-8
```

```
<!DOCTYPE html>
```

```
<html class="rtl" dir="rtl" lang="ar-SA">

<head>
 <title>       وزارة الاتصالات وتقنية المعلومات - الرئيسية</title>
  <meta name="viewport" content="width=device-width, width=device-width" />
  <meta name="description" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية " />
  <meta name="keywords" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية">
  <meta name="format-detection" content="telephone=no">
  <meta property="og:url" content="/web/guest/home?
p_p_id=com_liferay_login_web_portlet_LoginPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=vi
ew&_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName=%2Flogin%2Flogin&saveLastPath
=false" />
  <meta property="og:type" content="Website" />
  <meta property="og:title" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية " />
  <meta property="og:description" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية " />
  <meta property="og:image" content="https://mcit-liferayqc.linkdev.com/o/mcit-theme/images/logo-
share.png" />
  <meta property="og:image:secure_url" content="https://mcit-liferayqc.linkdev.com/o/mcit-
theme/images/logo-share.png" />

  <link rel="manifest" href="/o/mcit-theme/manifest.json">
```

```
<meta content="text/html; charset=UTF-8" http-equiv="content-type" />
```

```
<script type="importmap">{"imports":{"react-dom":"/o/frontend-js-react-
web/__liferay__/exports/react-dom.js","@clayui/breadcrumb":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$breadcrumb.js","@clayui/form":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$form.js","@clayui/popover":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$popover.js","@clayui/charts":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$charts.js","@clayui/shared":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$shared.js","@clayui/localized-input":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$localized-input.js","@clayui/modal":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$modal.js","@clayui/empty-state":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$empty-state.js","react":"/o/frontend-js-react-
web/__liferay__/exports/react.js","@clayui/color-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$color-picker.js","@clayui/navigation-bar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$navigation-bar.js","@clayui/pagination":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$pagination.js","@clayui/icon":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$icon.js","@clayui/table":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$table.js","@clayui/autocomplete":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$autocomplete.js","@clayui/slider":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$slider.js","@clayui/management-toolbar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$management-toolbar.js","@clayui/multi-select":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$multi-select.js","@clayui/nav":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$nav.js","@clayui/time-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$time-picker.js","@clayui/provider":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$provider.js","@clayui/upper-toolbar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$upper-toolbar.js","@clayui/loading-indicator":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$loading-indicator.js","@clayui/panel":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$panel.js","@clayui/drop-down":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$drop-down.js","@clayui/list":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$list.js","@clayui/date-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$date-picker.js","@clayui/label":"/o/front
...
...
...
```


L Check for SRI (Subresource Integrity) support 1

TOC

Issue 1 of 1

TOC

Check for SRI (Subresource Integrity) support	
Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/web/guest/home
Entity:	home (Page)
Risk:	In case the third-party server is compromised, the content/behavior of the site will change
Causes:	There is no support to Subresource Integrity.
Fix:	Add to each third-party script/link element support to SRI(Subresource Integrity).

Reasoning: The third-party links/scripts don't have integrity attribute for the browser to confirm they

didn't compromised

Test Requests and Responses:

```
GET /web/guest/home?
p_p_id=com_liferay_login_web_portlet_LoginPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=vi
ew&_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName=%2Flogin%2Flogin&saveLastPath
=false HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/c/portal/login?p_l_id=129
Cookie: COOKIE_SUPPORT=true; GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: Keep-Alive
Host: mcit-liferayqc.linkdev.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Liferay-Portal: Liferay Digital Experience Platform
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Set-Cookie: JSESSIONID=E5B8F8EFB128E107E25B1803A25A2CCD; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 10:06:04 GMT
Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>
```

```
<html class="rtl" dir="rtl" lang="ar-SA">

<head>
 <title>       وزارة الاتصالات وتقنية المعلومات - الرئيسية</title>
  <meta name="viewport" content="width=device-width, width=device-width" />
  <meta name="description" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية " />
  <meta name="keywords" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية">
  <meta name="format-detection" content="telephone=no">
  <meta property="og:url" content="/web/guest/home?
p_p_id=com_liferay_login_web_portlet_LoginPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=vi
ew&_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName=%2Flogin%2Flogin&saveLastPath
=false" />
  <meta property="og:type" content="Website" />
  <meta property="og:title" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية " />
  <meta property="og:description" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية " />
  <meta property="og:image" content="https://mcit-liferayqc.linkdev.com/o/mcit-theme/images/logo-
share.png" />
  <meta property="og:image:secure_url" content="https://mcit-liferayqc.linkdev.com/o/mcit-
theme/images/logo-share.png" />

  <link rel="manifest" href="/o/mcit-theme/manifest.json">
```

```
<meta content="text/html; charset=UTF-8" http-equiv="content-type" />
```

```
<script type="importmap">{"imports":{"react-dom":"/o/frontend-js-react-
web/__liferay__/exports/react-dom.js","@clayui/breadcrumb":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$breadcrumb.js","@clayui/form":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$form.js","@clayui/popover":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$popover.js","@clayui/charts":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$charts.js","@clayui/shared":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$shared.js","@clayui/localized-input":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$localized-input.js","@clayui/modal":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$modal.js","@clayui/empty-state":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$empty-state.js","react":"/o/frontend-js-react-
web/__liferay__/exports/react.js","@clayui/color-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$color-picker.js","@clayui/navigation-bar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$navigation-bar.js","@clayui/pagination":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$pagination.js","@clayui/icon":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$icon.js","@clayui/table":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$table.js","@clayui/autocomplete":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$autocomplete.js","@clayui/slider":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$slider.js","@clayui/management-toolbar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$management-toolbar.js","@clayui/multi-select":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$multi-select.js","@clayui/nav":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$nav.js","@clayui/time-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$time-picker.js","@clayui/provider":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$provider.js","@clayui/upper-toolbar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$upper-toolbar.js","@clayui/loading-indicator":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$loading-indicator.js","@clayui/panel":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$panel.js","@clayui/drop-down":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$drop-down.js","@clayui/list":"/o/frontend-taglib-
clay/__liferay__/exp
...
...
...

 <script src="       https://www.google.com/recaptcha/api.js?hl=ar" type="text/javascript">
</script>
...
...
...
```

Issue 1 of 2

TOC

Missing or insecure "Content-Security-Policy" header

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/o/js_resolve_modules
Entity:	js_resolve_modules (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header with secure policies

Reasoning: AppScan detected that the Content-Security-Policy response header is missing or with an insecure policy, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET /o/js_resolve_modules?modules=frontend-js-spa-web%405.0.44%2Finit HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/web/guest/home?
p_p_id=com_liferay_login_web_portlet_LoginPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=vi
ew&_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName=%2Flogin%2Flogin&saveLastPath
=false
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715070788022;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; COOKIE_SUPPORT=true;
GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Accept: */*
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty


HTTP/1.1 200
Connection: keep-alive
Content-Length: 6078
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Cache-Control: no-cache
ETag: W/"d18b97c3-14f5-489a-90fa-791afa57880a"
Set-Cookie: JSESSIONID=FA891FCD20C9A147073C2593CC3ED7A0; Path=/; Secure; HttpOnly
```

```
Date: Tue, 07 May 2024 09:26:50 GMT
Content-Type: application/json;charset=UTF-8

{
 "pathMap": {
         "frontend-js-spa-web@5.0.44\/screen\/ActionURLScreen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/ActionURLScreen",
         "frontend-js-spa-web@5.0.44\/screen\/RenderURLScreen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/RenderURLScreen",
         "frontend-js-spa-web@5.0.44\/surface\/Surface": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/surface\/Surface",
         "frontend-js-spa-web@5.0.44\/cacheable\/Cacheable": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/cacheable\/Cacheable",
         "frontend-js-spa-web@5.0.44\/app\/LiferayApp": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/app\/LiferayApp",
         "frontend-js-spa-web@5.0.44\/app\/App": "\/o\/js\/resolved-module\/frontend-js-
spa-web@5.0.44\/app\/App",
         "frontend-js-spa-web@5.0.44\/screen\/EventScreen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/EventScreen",
         "frontend-js-web@5.0.97\/index": "\/o\/js\/resolved-module\/frontend-js-
web@5.0.97\/index",
         "frontend-js-spa-web@5.0.44\/route\/Route": "\/o\/js\/resolved-module\/frontend-
js-spa-web@5.0.44\/route\/Route",
         "frontend-js-spa-web@5.0.44\/util\/utils": "\/o\/js\/resolved-module\/frontend-
js-spa-web@5.0.44\/util\/utils",
         "frontend-js-spa-web@5.0.44\/util\/pathParser": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/util\/pathParser",
         "frontend-js-spa-web@5.0.44\/screen\/HtmlScreen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/HtmlScreen",
         "frontend-js-spa-web@5.0.44\/init": "\/o\/js\/resolved-module\/frontend-js-spa-
web@5.0.44\/init",
         "frontend-js-spa-web@5.0.44\/screen\/Screen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/Screen",
         "frontend-js-spa-web@5.0.44\/screen\/RequestScreen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/RequestScreen"
 },
 "configMap": {

 },
 "resolvedModules": [
         "frontend-js-web@5.0.97\/index",
         "frontend-js-spa-web@5.0.44\/surface\/Surface",
         "frontend-js-spa-web@5.0.44\/util\/utils",
         "frontend-js-spa-web@5.0.44\/util\/pathParser",
         "frontend-js-spa-web@5.0.44\/route\/Route",
         "frontend-js-spa-web@5.0.44\/cacheable\/Cacheable",
         "frontend-js-spa-web@5.0.44\/screen\/Screen",
         "frontend-js-spa-web@5.0.44\/app\/App",
         "frontend-js-spa-web@5.0.44\/app\/LiferayApp",
         "frontend-js-spa-web@5.0.44\/screen\/RequestScreen",
         "frontend-js-spa-web@5.0.44\/screen\/HtmlScreen",
         "frontend-js-spa-web@5.0.44\/screen\/EventScreen",
         "frontend-js-spa-web@5.0.44\/screen\/ActionURLScreen",
         "frontend-js-spa-web@5.0.44\/screen\/RenderURLScreen",
         "frontend-js-spa-web@5.0.44\/init"
 ],
 "moduleMap": {
         "frontend-js-spa-web@5.0.44\/screen\/ActionURLScreen": {
                 ".\/EventScreen": "frontend-js-spa-web@5.0.44\/screen\/EventScreen",
                 "..\/util\/utils": "frontend-js-spa-web@5.0.44\/util\/utils"
         }       ,
         "frontend-js-spa-web@5.0.44\/screen\/RenderURLScreen": {
                 ".\/EventScreen": "frontend-js-spa-web@5.0.44\/screen\/EventScreen"
         }       ,
         "frontend-js-spa-web@5.0.44\/surface\/Surface": {
                 "frontend-js-web": "frontend-js-web@5.0.97\/index"
         }       ,
         "frontend-js-spa-web@5.0.44\/cacheable\/Cacheable": {
                 "frontend-js-web": "frontend-js-web@5.0.97\/index"
         }       ,
         "frontend-js-spa-web@5.0.44\/app\/LiferayApp": {
                 "..\/surfac
...
...
...
```

Issue 2 of 2

TOC

Missing or insecure "Content-Security-Policy" header

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/o/mcit-theme/manifest.json
Entity:	manifest.json (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header with secure policies

Reasoning: AppScan detected that the Content-Security-Policy response header is missing or with an insecure policy, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET /o/mcit-theme/manifest.json HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/home/
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Accept: */*
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: manifest


HTTP/1.1 200
Last-Modified: Thu, 02 May 2024 04:58:18 GMT
Connection: keep-alive
Content-Length: 100
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
ETag: W/"100-1714625898000"
Set-Cookie: JSESSIONID=E90AC3E46AEB1D8C025F1F93120E5B4A; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 09:26:51 GMT
Content-Type: application/json

{

"name": "MCIT",

"Short_name": "MCIT",

"display": "fullscreen",

"scope": "/"

}
```

Issue 1 of 2

TOC

Missing or insecure "X-XSS-Protection" header

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/o/js_resolve_modules
Entity:	js_resolve_modules (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-XSS-Protection" header with value '1' (enabled)

Reasoning: AppScan detected that the X-XSS-Protection response header is missing or with an insecure value, which may allow Cross-Site Scripting attacks

Test Requests and Responses:

```
GET /o/js_resolve_modules?modules=frontend-js-spa-web%405.0.44%2Finit HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/web/guest/home?
p_p_id=com_liferay_login_web_portlet_LoginPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=vi
ew&_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName=%2Flogin%2Flogin&saveLastPath
=false
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715070788022;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; COOKIE_SUPPORT=true;
GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Accept: */*
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty


HTTP/1.1 200
Connection: keep-alive
Content-Length: 6078
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
```

```
Cache-Control: private
Cache-Control: no-cache
ETag: W/"d18b97c3-14f5-489a-90fa-791afa57880a"
Set-Cookie: JSESSIONID=FA891FCD20C9A147073C2593CC3ED7A0; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 09:26:50 GMT
Content-Type: application/json;charset=UTF-8

{
 "pathMap": {
         "frontend-js-spa-web@5.0.44\/screen\/ActionURLScreen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/ActionURLScreen",
         "frontend-js-spa-web@5.0.44\/screen\/RenderURLScreen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/RenderURLScreen",
         "frontend-js-spa-web@5.0.44\/surface\/Surface": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/surface\/Surface",
         "frontend-js-spa-web@5.0.44\/cacheable\/Cacheable": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/cacheable\/Cacheable",
         "frontend-js-spa-web@5.0.44\/app\/LiferayApp": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/app\/LiferayApp",
         "frontend-js-spa-web@5.0.44\/app\/App": "\/o\/js\/resolved-module\/frontend-js-
spa-web@5.0.44\/app\/App",
         "frontend-js-spa-web@5.0.44\/screen\/EventScreen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/EventScreen",
         "frontend-js-web@5.0.97\/index": "\/o\/js\/resolved-module\/frontend-js-
web@5.0.97\/index",
         "frontend-js-spa-web@5.0.44\/route\/Route": "\/o\/js\/resolved-module\/frontend-
js-spa-web@5.0.44\/route\/Route",
         "frontend-js-spa-web@5.0.44\/util\/utils": "\/o\/js\/resolved-module\/frontend-
js-spa-web@5.0.44\/util\/utils",
         "frontend-js-spa-web@5.0.44\/util\/pathParser": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/util\/pathParser",
         "frontend-js-spa-web@5.0.44\/screen\/HtmlScreen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/HtmlScreen",
         "frontend-js-spa-web@5.0.44\/init": "\/o\/js\/resolved-module\/frontend-js-spa-
web@5.0.44\/init",
         "frontend-js-spa-web@5.0.44\/screen\/Screen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/Screen",
         "frontend-js-spa-web@5.0.44\/screen\/RequestScreen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/RequestScreen"
 },
 "configMap": {

 },
 "resolvedModules": [
         "frontend-js-web@5.0.97\/index",
         "frontend-js-spa-web@5.0.44\/surface\/Surface",
         "frontend-js-spa-web@5.0.44\/util\/utils",
         "frontend-js-spa-web@5.0.44\/util\/pathParser",
         "frontend-js-spa-web@5.0.44\/route\/Route",
         "frontend-js-spa-web@5.0.44\/cacheable\/Cacheable",
         "frontend-js-spa-web@5.0.44\/screen\/Screen",
         "frontend-js-spa-web@5.0.44\/app\/App",
         "frontend-js-spa-web@5.0.44\/app\/LiferayApp",
         "frontend-js-spa-web@5.0.44\/screen\/RequestScreen",
         "frontend-js-spa-web@5.0.44\/screen\/HtmlScreen",
         "frontend-js-spa-web@5.0.44\/screen\/EventScreen",
         "frontend-js-spa-web@5.0.44\/screen\/ActionURLScreen",
         "frontend-js-spa-web@5.0.44\/screen\/RenderURLScreen",
         "frontend-js-spa-web@5.0.44\/init"
 ],
 "moduleMap": {
         "frontend-js-spa-web@5.0.44\/screen\/ActionURLScreen": {
                 ".\/EventScreen": "frontend-js-spa-web@5.0.44\/screen\/EventScreen",
                 "..\/util\/utils": "frontend-js-spa-web@5.0.44\/util\/utils"
         }       ,
         "frontend-js-spa-web@5.0.44\/screen\/RenderURLScreen": {
                 ".\/EventScreen": "frontend-js-spa-web@5.0.44\/screen\/EventScreen"
         }       ,
         "frontend-js-spa-web@5.0.44\/surface\/Surface": {
                 "frontend-js-web": "frontend-js-web@5.0.97\/index"
         }       ,
         "frontend-js-spa-web@5.0.44\/cacheable\/Cacheable": {
                 "frontend-js-web": "frontend-js-web@5.0.97\/index"
         }       ,
         "frontend-js-spa-web@5.0.44\/app\/LiferayApp": {
                 "..\/surfac
...
...
```

```
...
```

Issue 2 of 2

TOC

Missing or insecure "X-XSS-Protection" header	
Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/o/mcit-theme/manifest.json
Entity:	manifest.json (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-XSS-Protection" header with value '1' (enabled)

Reasoning: AppScan detected that the X-XSS-Protection response header is missing or with an insecure value, which may allow Cross-Site Scripting attacks

Test Requests and Responses:

```
GET /o/mcit-theme/manifest.json HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/home/
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Accept: */*
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: manifest


HTTP/1.1 200
Last-Modified: Thu, 02 May 2024 04:58:18 GMT
Connection: keep-alive
Content-Length: 100
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
ETag: W/"100-1714625898000"
Set-Cookie: JSESSIONID=E90AC3E46AEB1D8C025F1F93120E5B4A; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 09:26:51 GMT
Content-Type: application/json

{

"name": "MCIT",

"Short_name": "MCIT",

"display": "fullscreen",

"scope": "/"
```

```
}
```

L Missing or insecure HTTP Strict-Transport-Security Header 2 TOC

Issue 1 of 2 TOC

Missing or insecure HTTP Strict-Transport-Security Header	
Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/o/js_resolve_modules
Entity:	js_resolve_modules (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Implement the HTTP Strict-Transport-Security policy with a long "max-age"

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing or with insufficient "max-age"

Test Requests and Responses:

```
GET /o/js_resolve_modules?modules=frontend-js-spa-web%405.0.44%2Finit HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/web/guest/home?
p_p_id=com_liferay_login_web_portlet_LoginPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=vi
ew&_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName=%2Flogin%2Flogin&saveLastPath
=false
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715070788022;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; COOKIE_SUPPORT=true;
GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Accept: */*
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty


HTTP/1.1 200
```

```
Connection: keep-alive
Content-Length: 6078
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Cache-Control: no-cache
ETag: W/"d18b97c3-14f5-489a-90fa-791afa57880a"
Set-Cookie: JSESSIONID=FA891FCD20C9A147073C2593CC3ED7A0; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 09:26:50 GMT
Content-Type: application/json;charset=UTF-8

{
 "pathMap": {
         "frontend-js-spa-web@5.0.44\/screen\/ActionURLScreen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/ActionURLScreen",
         "frontend-js-spa-web@5.0.44\/screen\/RenderURLScreen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/RenderURLScreen",
         "frontend-js-spa-web@5.0.44\/surface\/Surface": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/surface\/Surface",
         "frontend-js-spa-web@5.0.44\/cacheable\/Cacheable": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/cacheable\/Cacheable",
         "frontend-js-spa-web@5.0.44\/app\/LiferayApp": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/app\/LiferayApp",
         "frontend-js-spa-web@5.0.44\/app\/App": "\/o\/js\/resolved-module\/frontend-js-
spa-web@5.0.44\/app\/App",
         "frontend-js-spa-web@5.0.44\/screen\/EventScreen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/EventScreen",
         "frontend-js-web@5.0.97\/index": "\/o\/js\/resolved-module\/frontend-js-
web@5.0.97\/index",
         "frontend-js-spa-web@5.0.44\/route\/Route": "\/o\/js\/resolved-module\/frontend-
js-spa-web@5.0.44\/route\/Route",
         "frontend-js-spa-web@5.0.44\/util\/utils": "\/o\/js\/resolved-module\/frontend-
js-spa-web@5.0.44\/util\/utils",
         "frontend-js-spa-web@5.0.44\/util\/pathParser": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/util\/pathParser",
         "frontend-js-spa-web@5.0.44\/screen\/HtmlScreen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/HtmlScreen",
         "frontend-js-spa-web@5.0.44\/init": "\/o\/js\/resolved-module\/frontend-js-spa-
web@5.0.44\/init",
         "frontend-js-spa-web@5.0.44\/screen\/Screen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/Screen",
         "frontend-js-spa-web@5.0.44\/screen\/RequestScreen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/RequestScreen"
 },
 "configMap": {

 },
 "resolvedModules": [
         "frontend-js-web@5.0.97\/index",
         "frontend-js-spa-web@5.0.44\/surface\/Surface",
         "frontend-js-spa-web@5.0.44\/util\/utils",
         "frontend-js-spa-web@5.0.44\/util\/pathParser",
         "frontend-js-spa-web@5.0.44\/route\/Route",
         "frontend-js-spa-web@5.0.44\/cacheable\/Cacheable",
         "frontend-js-spa-web@5.0.44\/screen\/Screen",
         "frontend-js-spa-web@5.0.44\/app\/App",
         "frontend-js-spa-web@5.0.44\/app\/LiferayApp",
         "frontend-js-spa-web@5.0.44\/screen\/RequestScreen",
         "frontend-js-spa-web@5.0.44\/screen\/HtmlScreen",
         "frontend-js-spa-web@5.0.44\/screen\/EventScreen",
         "frontend-js-spa-web@5.0.44\/screen\/ActionURLScreen",
         "frontend-js-spa-web@5.0.44\/screen\/RenderURLScreen",
         "frontend-js-spa-web@5.0.44\/init"
 ],
 "moduleMap": {
         "frontend-js-spa-web@5.0.44\/screen\/ActionURLScreen": {
                 ".\/EventScreen": "frontend-js-spa-web@5.0.44\/screen\/EventScreen",
                 "..\/util\/utils": "frontend-js-spa-web@5.0.44\/util\/utils"
         }       ,
         "frontend-js-spa-web@5.0.44\/screen\/RenderURLScreen": {
                 ".\/EventScreen": "frontend-js-spa-web@5.0.44\/screen\/EventScreen"
         }       ,
         "frontend-js-spa-web@5.0.44\/surface\/Surface": {
                 "frontend-js-web": "frontend-js-web@5.0.97\/index"
         }       ,
         "frontend-js-spa-web@5.0.44\/cacheable\/Cacheable": {
                 "frontend-js-web": "frontend-js-web@5.0.97\/index"
         }       ,
```

```
          "frontend-js-spa-web@5.0.44\/app\/LiferayApp": {
                 "..\/surface\/Surface": "frontend-js-spa-web@5.0.44\/su
...
...
...
```

Issue 2 of 2

TOC

Missing or insecure HTTP Strict-Transport-Security Header

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/o/mcit-theme/manifest.json
Entity:	manifest.json (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Implement the HTTP Strict-Transport-Security policy with a long "max-age"

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing or with insufficient "max-age"

Test Requests and Responses:

```
GET /o/mcit-theme/manifest.json HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/home/
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Accept: */*
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: manifest


HTTP/1.1 200
Last-Modified: Thu, 02 May 2024 04:58:18 GMT
Connection: keep-alive
Content-Length: 100
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
ETag: W/"100-1714625898000"
Set-Cookie: JSESSIONID=E90AC3E46AEB1D8C025F1F93120E5B4A; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 09:26:51 GMT
Content-Type: application/json

{

"name": "MCIT",

"Short_name": "MCIT",
```

```
"display": "fullscreen",

"scope": "/"

}
```

L Unsafe third-party link (target="_blank") 7 TOC

Issue 1 of 7 TOC

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/home
Entity:	home (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /home HTTP/1.1
Sec-Fetch-Site: none
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; _ga=GA1.1.128297136.1599395143;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Upgrade-Insecure-Requests: 1
Sec-Fetch-Mode: navigate
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.7
Sec-Fetch-User: ?1
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: document


...
```

```
...
...
          <div class="overflow-hidden">
          <p class="sub-title" title="دعم العمل الحر عن طريق تأهيل وتمكين العاملين المستقلين ومخصص
للمتفرغين للعمل والباحثين عن عمل والعاملين بشكل جزئي.">دعم العمل الحر عن طريق تأهيل وتمكين العاملين
المستقلين ومخصص للمتفرغين للعمل والباحثين عن عمل والعاملين بشكل جزئي.</p>
          </div>
          <div class="overflow-hidden"><a class="btn btn-sm btn-outline-light"
href="https://www.google.com/" target="_blank" title="اقرأ المزيد">اقرأ المزيد</a>
          </div>
          </div>
          </div>
          </div>
...
...
...

          <div class="overflow-hidden">
          <p class="sub-title" title="تتضمن الاستراتيجية، خطة عمل طموحة تقوم على استقطاب الشركات
الدولية الرائدة في المجالات ذات الأولوية الخاصة بالتقنيات الناشئة.">تتضمن الاستراتيجية، خطة عمل طموحة تقوم
على استقطاب الشركات الدولية الرائدة في المجالات ذات الأولوية الخاصة بالتقنيات الناشئة.</p>
          </div>
          <div class="overflow-hidden"><a class="btn btn-sm btn-outline-light"
href="https://www.google.com/" target="_blank" title="اقرأ المزيد">اقرأ المزيد</a>
          </div>
          </div>
          </div>
          </div>
...
...
...

          <div class="overflow-hidden">
          <p class="sub-title" title="دعم العمل الحر عن طريق تأهيل وتمكين العاملين المستقلين ومخصص
للمتفرغين للعمل والباحثين عن عمل والعاملين بشكل جزئي.">دعم العمل الحر عن طريق تأهيل وتمكين العاملين
المستقلين ومخصص للمتفرغين للعمل والباحثين عن عمل والعاملين بشكل جزئي.</p>
          </div>
          <div class="overflow-hidden"><a class="btn btn-sm btn-outline-light"
href="https://www.google.com/" target="_blank" title="اقرأ المزيد">اقرأ المزيد</a>
          </div>
          </div>
          </div>
          </div>
...
...
...

          <div class="card-col d-flex flex-column h-100">
          <div class="card-info d-flex align-items-center">
          <div class="status d-flex align-items-baseline"><span class="icon-status d-sm-inline-
block d-none"></span> <span title="مكتمل">مكتمل</span>
          </div>
          <div class="location d-flex align-items-baseline"><span class="icon-location d-sm-
inline-block d-none"></span> <a href="https://www.google.com/" title="افتراضي"
target="_blank">افتراضي</a> <a href="https://www.google.com/" title="حضوري"
target="_blank">حضوري</a>
          </div>
          </div>
          <div class="card-head">
          <h4 title="2 اليوم العالمي للتطوع السعودي">2 اليوم العالمي للتطوع السعودي</h4>
...
...
...

          <div class="card-col d-flex flex-column h-100">
          <div class="card-info d-flex align-items-center">
          <div class="status d-flex align-items-baseline"><span class="icon-status d-sm-inline-
block d-none"></span> <span title="مكتمل">مكتمل</span>
          </div>
          <div class="location d-flex align-items-baseline"><span class="icon-location d-sm-
inline-block d-none"></span> <a href="https://www.google.com/" title="افتراضي"
target="_blank">افتراضي</a> <a href="https://www.google.com/" title="حضوري"
target="_blank">حضوري</a>
          </div>
          </div>
          <div class="card-head">
          <h4 title="2 اليوم العالمي للتطوع السعودي">2 اليوم العالمي للتطوع السعودي</h4>
...
```

```
...
...

          <div class="card-col d-flex flex-column h-100">
          <div class="card-info d-flex align-items-center">
          <div class="status d-flex align-items-baseline"><span class="icon-status d-sm-inline-
block d-none"></span> <span title="مكتمل">مكتمل</span>
          </div>
          <div class="location d-flex align-items-baseline"><span class="icon-location d-sm-
inline-block d-none"></span> <a href="https://www.google.com/" title="حضوري"
target="_blank">حضوري</a>
          </div>
          </div>
          <div class="card-head">
          <h4 title="اليوم العالمي للتطوع السعودي 1">اليوم العالمي للتطوع السعودي 1</h4>
...
...
...

          <div class="card-col d-flex flex-column h-100">
          <div class="card-info d-flex align-items-center">
          <div class="status d-flex align-items-baseline"><span class="icon-status d-sm-inline-
block d-none"></span> <span title="مكتمل">مكتمل</span>
          </div>
          <div class="location d-flex align-items-baseline"><span class="icon-location d-sm-
inline-block d-none"></span> <a href="https://www.google.com/" title="افتراضي"
target="_blank">افتراضي</a>
          </div>
          </div>
          <div class="card-head">
          <h4 title="اليوم العالمي للتطوع السعودي 2">اليوم العالمي للتطوع السعودي 2</h4>
...
...
...

          <div class="card-col d-flex flex-column h-100">
          <div class="card-info d-flex align-items-center">
          <div class="status d-flex align-items-baseline"><span class="icon-status d-sm-inline-
block d-none"></span> <span title="مكتمل">مكتمل</span>
          </div>
          <div class="location d-flex align-items-baseline"><span class="icon-location d-sm-
inline-block d-none"></span> <a href="https://www.google.com/" title="افتراضي"
target="_blank">افتراضي</a>
          </div>
          </div>
          <div class="card-head">
          <h4 title="اليوم العالمي للتطوع السعودي 2">اليوم العالمي للتطوع السعودي 2</h4>
...
...
...

          <div class="card-col d-flex flex-column h-100">
          <div class="card-info d-flex align-items-center">
          <div class="status d-flex align-items-baseline"><span class="icon-status d-sm-inline-
block d-none"></span> <span title="مكتمل">مكتمل</span>
          </div>
          <div class="location d-flex align-items-baseline"><span class="icon-location d-sm-
inline-block d-none"></span> <a href="https://www.google.com/" title="افتراضي"
target="_blank">افتراضي</a>
          </div>
          </div>
          <div class="card-head">
          <h4 title="اليوم العالمي للتطوع السعودي 2">اليوم العالمي للتطوع السعودي 2</h4>
...
...
...

          </div>
          <div class="container">
          <div class="owl-carousel owl-theme owl-home-partners">
          <div class="item h-auto">
          <div class="journal-content-article " data-analytics-asset-id="35686" data-analytics-
asset-title="المركز الوطني لتنمية القطاع غير الربحي" data-analytics-asset-type="web-content"><a
href="https://ncnp.gov.sa/en" class="image-slide d-flex justify-content-center align-items-center
h-100" title="المركز الوطني لتنمية القطاع غير الربحي" target="_blank">
          <picture data-fileentryid="40666">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/40666/Thumbnail-
300x300/NAPS+%281%29.png?t=1702746299256">
```

```
          <source media="(max-width:414px) and (min-width:300px)" srcset="/o/adaptive-
media/image/40666/Preview-1000x0/NAPS+%281%29.png?t=1702746299256">
...
...
...

          </div>
          </div>
          <div class="item h-auto">
          <div class="journal-content-article " data-analytics-asset-id="35674" data-analytics-
asset-title="التحول الرقمي والحلول المعتمدة على الذكاء الاصطناعي" data-analytics-asset-type="web-
content"><a href="https://thinktechnow.com/" class="image-slide d-flex justify-content-center
align-items-center h-100" title="التحول الرقمي والحلول المعتمدة على الذكاء الاصطناعي" target="_blank">
          <picture data-fileentryid="40561">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/40561/Thumbnail-
300x300/thinktech+%281%29.png?t=1702745963237">
          <source media="(max-width:354px) and (min-width:300px)" srcset="/o/adaptive-
media/image/40561/Preview-1000x0/thinktech+%281%29.png?t=1702745963237">
...
...
...

          </picture> </a>
          </div>
          </div>
          <div class="item h-auto">
          <div class="journal-content-article " data-analytics-asset-id="35656" data-analytics-
asset-title="مبادرة العطاء الرقمي" data-analytics-asset-type="web-content"><a
href="https://attaa.sa/" class="image-slide d-flex justify-content-center align-items-center h-
100" title="مبادرة العطاء الرقمي" target="_blank">
          <picture data-fileentryid="40698">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/40698/Thumbnail-
300x300/Atta-Digital+%281%29.png?t=1702746406364">
          <source media="(max-width:414px) and (min-width:300px)" srcset="/o/adaptive-
media/image/40698/Preview-1000x0/Atta-Digital+%281%29.png?t=1702746406364">
          <picture data-fileentryid="40698">
...
...
...

          </picture> </a>
          </div>
          </div>
          <div class="item h-auto">
          <div class="journal-content-article " data-analytics-asset-id="35582" data-analytics-
asset-title="المركز الوطني لتنمية القطاع غير الربحي" data-analytics-asset-type="web-content"><a
href="https://ncnp.gov.sa/en" class="image-slide d-flex justify-content-center align-items-center
h-100" title="المركز الوطني لتنمية القطاع غير الربحي" target="_blank">
          <picture data-fileentryid="40666">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/40666/Thumbnail-
300x300/NAPS+%281%29.png?t=1702746299256">
          <source media="(max-width:414px) and (min-width:300px)" srcset="/o/adaptive-
media/image/40666/Preview-1000x0/NAPS+%281%29.png?t=1702746299256">
...
...
...

          </picture> </a>
          </div>
          </div>
          <div class="item h-auto">
          <div class="journal-content-article " data-analytics-asset-id="35549" data-analytics-
asset-title="المرصد الوطني للعمل" data-analytics-asset-type="web-content"><a
href="https://nlo.gov.sa/" class="image-slide d-flex justify-content-center align-items-center h-
100" title="المرصد الوطني للعمل" target="_blank">
          <picture data-fileentryid="40634">
          <source media="(max-width:168px)" srcset="/o/adaptive-media/image/40634/Preview-
1000x0/NAO+%281%29.png?t=1702746200592">
          <source media="(max-width:168px) and (min-width:168px)" srcset="/o/adaptive-
media/image/40634/Thumbnail-300x300/NAO+%281%29.png?t=1702746200592">
          <picture data-fileentryid="40634">
...
...
...

          </picture> </a>
          </div>
          </div>
```

```
          <div class="item h-auto">
          <div class="journal-content-article " data-analytics-asset-id="35519" data-analytics-
asset-title="الأكاديمية السعودية الرقمية" data-analytics-asset-type="web-content"><a
href="https://sda.edu.sa/" class="image-slide d-flex justify-content-center align-items-center h-
100" title="الأكاديمية السعودية الرقمية" target="_blank"><a href="https://thinktechnow.com/"
class="image-slide d-flex justify-content-center align-items-center h-100" title="التحول الرقمي
والحلول المعتمدة على الذكاء الاصطناعي" target="_blank">--end_highlight_tag--
          <picture data-fileentryid="40561">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/40561/Thumbnail-
300x300/thinktech+%281%29.png?t=1702745963237">
          <source media="(max-width:354px) and (min-width:300px)" srcset="/o/adaptive-
media/image/40561/Preview-1000x0/thinktech+%281%29.png?t=1702745963237">
...
...
...

          <li class="d-block">
          <div class="social-media-links"><span title="تابعنا على">تابعنا على</span>
          <ul>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84409" data-analytics-
asset-title="Facebook" data-analytics-asset-type="web-content">
          <picture data-fileentryid="40561">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/40561/Thumbnail-
300x300/thinktech+%281%29.png?t=1702745963237">
          <source media="(max-width:354px) and (min-width:300px)" srcset="/o/adaptive-
media/image/40561/Preview-1000x0/thinktech+%281%29.png?t=1702745963237">
...
...
...

          <li class="d-block">
          <div class="social-media-links"><span title="تابعنا على">تابعنا على</span>
          <ul>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84409" data-analytics-
asset-title="Facebook" data-analytics-asset-type="web-content">--begin_highlight_tag--<a
href="https://www.facebook.com/McitGovSa/" title="facebook" target="_blank"><a
href="https://www.facebook.com/McitGovSa/" title="facebook" target="_blank">--end_highlight_tag--
<span class="icon-facebook"></span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84452" data-analytics-
asset-title="Twitter" data-analytics-asset-type="web-content"> <span class="icon-facebook">
</span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84452" data-analytics-
asset-title="Twitter" data-analytics-asset-type="web-content">--begin_highlight_tag--<a
href="https://twitter.com/mcitgovsa?s=11" title="twitter" target="_blank"><a
href="https://twitter.com/mcitgovsa?s=11" title="twitter" target="_blank">--end_highlight_tag--
<span class="icon-twitter"></span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84442" data-analytics-
asset-title="Instagram" data-analytics-asset-type="web-content"> <span class="icon-twitter">
</span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84442" data-analytics-
asset-title="Instagram" data-analytics-asset-type="web-content">--begin_highlight_tag--<a
href="https://www.instagram.com/p/CiIYfgYMhFy/" title="instagram" target="_blank"><a
href="https://www.instagram.com/p/CiIYfgYMhFy/" title="instagram" target="_blank">--
end_highlight_tag-- <span class="icon-instagram"></span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84419" data-analytics-
asset-title="Linkedin" data-analytics-asset-type="web-content"> <span class="icon-instagram">
</span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84419" data-analytics-
asset-title="Linkedin" data-analytics-asset-type="web-content">--begin_highlight_tag--<a
href="https://www.linkedin.com/company/mcitgovsa/" title="linkedin" target="_blank"><a
href="https://www.linkedin.com/company/mcitgovsa/" title="linkedin" target="_blank">--
end_highlight_tag-- <span class="icon-linkedin"></span> </a>
          </div></li>
          <li>
```

```
          <div class="journal-content-article " data-analytics-asset-id="84475" data-analytics-
asset-title="youtube" data-analytics-asset-type="web-content"> <span class="icon-linkedin">
</span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84475" data-analytics-
asset-title="youtube" data-analytics-asset-type="web-content">--begin_highlight_tag--<a
href="https://www.youtube.com/@Mcitgovsa" title="youtube" target="_blank"><a
href="https://www.youtube.com/@Mcitgovsa" title="youtube" target="_blank">--end_highlight_tag--
<span class="icon-youtube"></span> </a>
          </div></li>
          </ul>
          </div></li>
          <li class="d-none d-lg-block">
...
...
...

          <section class="footer-mcit-ecosystem">
          <div class="container">
          <div class="row justify-content-center align-items-center">
          <div class="col-sm-3 h-auto">
          <div class="journal-content-article " data-analytics-asset-id="47025" data-analytics-
asset-title="وحدة التحول الرقمي" data-analytics-asset-type="web-content"> <span class="icon-
youtube"></span> </a>
          </div></li>
          </ul>
          </div></li>
          <li class="d-none d-lg-block">
...
...
...

          <section class="footer-mcit-ecosystem">
          <div class="container">
          <div class="row justify-content-center align-items-center">
          <div class="col-sm-3 h-auto">
          <div class="journal-content-article " data-analytics-asset-id="47025" data-analytics-
asset-title="وحدة التحول الرقمي" data-analytics-asset-type="web-content">--begin_highlight_tag--<a
href="https://ndu.gov.sa/" class="image-slide d-block" title="وحدة التحول الرقمي"
target="_blank"><a href="https://ndu.gov.sa/" class="image-slide d-block" title="وحدة التحول
الرقمي" target="_blank">--end_highlight_tag--
          <picture data-fileentryid="47007">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/47007/Thumbnail-
300x300/national-img.png?t=1704710148114">
          <source media="(max-width:442px) and (min-width:300px)" srcset="/o/adaptive-
media/image/47007/Preview-1000x0/national-img.png?t=1704710148114">
          <picture data-fileentryid="47007">
...
...
...

          </picture> </a>
          </div>
          </div>
          <div class="col-sm-3 h-auto">
          <div class="journal-content-article " data-analytics-asset-id="47060" data-analytics-
asset-title="هيئة الحكومة الرقمية" data-analytics-asset-type="web-content">
          <picture data-fileentryid="47007">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/47007/Thumbnail-
300x300/national-img.png?t=1704710148114">
          <source media="(max-width:442px) and (min-width:300px)" srcset="/o/adaptive-
media/image/47007/Preview-1000x0/national-img.png?t=1704710148114">
          <picture data-fileentryid="47007">
...
...
...

          </picture> </a>
          </div>
          </div>
          <div class="col-sm-3 h-auto">
          <div class="journal-content-article " data-analytics-asset-id="47060" data-analytics-
asset-title="هيئة الحكومة الرقمية" data-analytics-asset-type="web-content">--begin_highlight_tag--
<a href="https://dga.gov.sa/en" class="image-slide d-block" title="هيئة الحكومة الرقمية"
target="_blank"><a href="https://dga.gov.sa/en" class="image-slide d-block" title="هيئة الحكومة
الرقمية" target="_blank">--end_highlight_tag--
          <picture data-fileentryid="47048">
```

```
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/47048/Thumbnail-
300x300/digital-img.png?t=1704710370519">
          <source media="(max-width:405px) and (min-width:300px)" srcset="/o/adaptive-
media/image/47048/Preview-1000x0/digital-img.png?t=1704710370519">
          <picture data-fileentryid="47048">
...
...
...

          </picture> </a>
          </div>
          </div>
          <div class="col-sm-3 h-auto">
          <div class="journal-content-article " data-analytics-asset-id="47095" data-analytics-
asset-title="هيئة الاتصالات و الفضاء و التقنية" data-analytics-asset-type="web-content">
          <picture data-fileentryid="47048">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/47048/Thumbnail-
300x300/digital-img.png?t=1704710370519">
          <source media="(max-width:405px) and (min-width:300px)" srcset="/o/adaptive-
media/image/47048/Preview-1000x0/digital-img.png?t=1704710370519">
          <picture data-fileentryid="47048">
...
...
...

          </picture> </a>
          </div>
          </div>
          <div class="col-sm-3 h-auto">
          <div class="journal-content-article " data-analytics-asset-id="47095" data-analytics-
asset-title="هيئة الاتصالات و الفضاء و التقنية" data-analytics-asset-type="web-content">--
begin_highlight_tag--<a href="https://www.cst.gov.sa/en/Pages/default.aspx" class="image-slide d-
block" title="هيئة الاتصالات و الفضاء و التقنية" target="_blank"><a
href="https://www.cst.gov.sa/en/Pages/default.aspx" class="image-slide d-block" title="هيئة
الاتصالات و الفضاء و التقنية" target="_blank">--end_highlight_tag--
          <picture data-fileentryid="47083">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/47083/Thumbnail-
300x300/space-img.png?t=1704710540062">
          <source media="(max-width:493px) and (min-width:300px)" srcset="/o/adaptive-
media/image/47083/Preview-1000x0/space-img.png?t=1704710540062">
          <picture data-fileentryid="47083">
...
...
...
```

Issue 2 of 7

TOC

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/c/portal/login
Entity:	login (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /c/portal/login?p_l_id=129 HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/home/
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_20099=1715070788022;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0; _ga=GA1.1.128297136.1599395143;
COOKIE_SUPPORT=true; GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Upgrade-Insecure-Requests: 1
Sec-Fetch-Mode: navigate
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.7
Sec-Fetch-User: ?1
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: document


HTTP/1.1 302
Location: https://mcit-liferayqc.linkdev.com/web/guest/home?
p_p_id=com_liferay_login_web_portlet_LoginPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=vi
ew&_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName=%2Flogin%2Flogin&saveLastPath
=false
Connection: keep-alive
Liferay-Portal: Liferay Digital Experience Platform
Content-Length: 0
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Set-Cookie: JSESSIONID=BE2EA0A70C370B8DA403A7C238190E79; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 09:26:51 GMT
Content-Type: text/html;charset=UTF-8



GET /web/guest/home?
p_p_id=com_liferay_login_web_portlet_LoginPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=vi
ew&_com_liferay_login_web_portlet_LoginPo
...
...
...
                        <a href="https://www.facebook.com/McitGovSa/" title="facebook"
target="_blank">
    <span class="icon-facebook"></span>
  </a>
...
...
...
                        <a href="https://twitter.com/mcitgovsa?s=11" title="twitter"
target="_blank">
    <span class="icon-twitter"></span>
  </a>
...
...
...
                        <a href="https://www.instagram.com/p/CiIYfgYMhFy/" title="instagram"
target="_blank">
    <span class="icon-instagram"></span>
  </a>
...
...
...
                        <a href="https://www.linkedin.com/company/mcitgovsa/" title="linkedin"
target="_blank">
    <span class="icon-linkedin"></span>
  </a>
```

```
...
...
...
                        <a href="https://www.youtube.com/@Mcitgovsa" title="youtube"
target="_blank">
    <span class="icon-youtube"></span>
  </a>
...
...
...
                                <a href="https://ndu.gov.sa/" class="image-slide d-block"
title="وحدة التحول الرقمي" target="_blank">
        <picture data-fileentryid="47007"><source media="(max-width:300px)"
srcset="/o/adaptive-media/image/47007/Thumbnail-300x300/national-img.png?t=1704710148114"><source
media="(max-width:442px) and (min-width:300px)" srcset="/o/adaptive-media/image/47007/Preview-
1000x0/national-img.png?t=1704710148114"><img src="https://mcit-
liferayqc.linkdev.com/documents/20119/0/national-img.png/b870b8f9-21ef-9a9d-e990-a1925bb37594?
t=1704710148114" data-fileentryid="47007" title="وحدة التحول الرقمي" alt="وحدة التحول الرقمي">
</picture>
   </a>
...
...
...
                                <a href="https://dga.gov.sa/en" class="image-slide d-block"
title="هيئة الحكومة الرقمية" target="_blank">
        <picture data-fileentryid="47048"><source media="(max-width:300px)"
srcset="/o/adaptive-media/image/47048/Thumbnail-300x300/digital-img.png?t=1704710370519"><source
media="(max-width:405px) and (min-width:300px)" srcset="/o/adaptive-media/image/47048/Preview-
1000x0/digital-img.png?t=1704710370519"><img src="https://mcit-
liferayqc.linkdev.com/documents/20119/0/digital-img.png/89d76923-dd22-fb7a-ef3d-d02eaf504f00?
t=1704710370519" data-fileentryid="47048" title="هيئة الحكومة الرقمية" alt="هيئة الحكومة الرقمية">
</picture>
   </a>
...
...
...
                                <a href="https://www.cst.gov.sa/en/Pages/default.aspx"
class="image-slide d-block" title="هيئة الاتصالات و الفضاء و التقنية" target="_blank">
        <picture data-fileentryid="47083"><source media="(max-width:300px)"
srcset="/o/adaptive-media/image/47083/Thumbnail-300x300/space-img.png?t=1704710540062"><source
media="(max-width:493px) and (min-width:300px)" srcset="/o/adaptive-media/image/47083/Preview-
1000x0/space-img.png?t=1704710540062"><img src="https://mcit-
liferayqc.linkdev.com/documents/20119/0/space-img.png/672e4b1c-d12a-dba4-c0e5-4b7310c97b8e?
t=1704710540062" data-fileentryid="47083" title="هيئة الاتصالات و الفضاء و التقنية" alt="هيئة الاتصالات و
الفضاء و التقنية"></picture>
   </a>
...
...
...
```

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/account-type
Entity:	account-type (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /account-type HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/web/guest/home?
p_p_id=com_liferay_login_web_portlet_LoginPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=vi
ew&_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName=%2Flogin%2Flogin&saveLastPath
=false
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
LFR_SESSION_STATE_20099=1715071553037; _ga=GA1.1.128297136.1599395143;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0; COOKIE_SUPPORT=true;
GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Upgrade-Insecure-Requests: 1
Sec-Fetch-Mode: navigate
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.7
Sec-Fetch-User: ?1
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: document


...
...
...
          <li class="d-block">
          <div class="social-media-links"><span title="تابعنا على">تابعنا على</span>
          <ul>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84409" data-analytics-
asset-title="Facebook" data-analytics-asset-type="web-content"><a
href="https://www.facebook.com/McitGovSa/" title="facebook" target="_blank"> <span class="icon-
facebook"></span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84452" data-analytics-
asset-title="Twitter" data-analytics-asset-type="web-content"><a
href="https://twitter.com/mcitgovsa?s=11" title="twitter" target="_blank"> <span class="icon-
twitter"></span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84442" data-analytics-
asset-title="Instagram" data-analytics-asset-type="web-content"><a
```

```
href="https://www.instagram.com/p/CiIYfgYMhFy/" title="instagram" target="_blank"> <span
class="icon-instagram"></span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84419" data-analytics-
asset-title="Linkedin" data-analytics-asset-type="web-content"><a
href="https://www.linkedin.com/company/mcitgovsa/" title="linkedin" target="_blank"> <span
class="icon-linkedin"></span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84475" data-analytics-
asset-title="youtube" data-analytics-asset-type="web-content"><a
href="https://www.youtube.com/@Mcitgovsa" title="youtube" target="_blank"> <span class="icon-
youtube"></span> </a>
          </div></li>
          </ul>
          </div></li>
          <li class="d-none d-lg-block">
...
...
...

          <section class="footer-mcit-ecosystem">
          <div class="container">
          <div class="row justify-content-center align-items-center">
          <div class="col-sm-3 h-auto">
          <div class="journal-content-article " data-analytics-asset-id="47025" data-analytics-
asset-title="وحدة التحول الرقمي" data-analytics-asset-type="web-content"><a
href="https://ndu.gov.sa/" class="image-slide d-block" title="وحدة التحول الرقمي" target="_blank">
          <picture data-fileentryid="47007">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/47007/Thumbnail-
300x300/national-img.png?t=1704710148114">
          <source media="(max-width:442px) and (min-width:300px)" srcset="/o/adaptive-
media/image/47007/Preview-1000x0/national-img.png?t=1704710148114">
          <picture data-fileentryid="47007">
...
...
...

          </picture> </a>
          </div>
          </div>
          <div class="col-sm-3 h-auto">
          <div class="journal-content-article " data-analytics-asset-id="47060" data-analytics-
asset-title="هيئة الحكومة الرقمية" data-analytics-asset-type="web-content"><a
href="https://dga.gov.sa/en" class="image-slide d-block" title="هيئة الحكومة الرقمية"
target="_blank">
          <picture data-fileentryid="47048">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/47048/Thumbnail-
300x300/digital-img.png?t=1704710370519">
          <source media="(max-width:405px) and (min-width:300px)" srcset="/o/adaptive-
media/image/47048/Preview-1000x0/digital-img.png?t=1704710370519">
          <picture data-fileentryid="47048">
...
...
...

          </picture> </a>
          </div>
          </div>
          <div class="col-sm-3 h-auto">
          <div class="journal-content-article " data-analytics-asset-id="47095" data-analytics-
asset-title="هيئة الاتصالات و الفضاء و التقنية" data-analytics-asset-type="web-content"><a
href="https://www.cst.gov.sa/en/Pages/default.aspx" class="image-slide d-block" title="هيئة
الاتصالات و الفضاء و التقنية" target="_blank">
          <picture data-fileentryid="47083">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/47083/Thumbnail-
300x300/space-img.png?t=1704710540062">
          <source media="(max-width:493px) and (min-width:300px)" srcset="/o/adaptive-
media/image/47083/Preview-1000x0/space-img.png?t=1704710540062">
          <picture data-fileentryid="47083">
...
...
...
```

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/recruitment
Entity:	recruitment (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /recruitment?isFresh=true HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/c
Cookie: COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: Keep-Alive
Host: mcit-liferayqc.linkdev.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


...
...
...
          <li class="d-block">
          <div class="social-media-links"><span title="تابعنا على"><تابعنا على</span>
          <ul>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84409" data-analytics-
asset-title="Facebook" data-analytics-asset-type="web-content"><a
href="https://www.facebook.com/McitGovSa/" title="facebook" target="_blank"> <span class="icon-
facebook"></span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84452" data-analytics-
asset-title="Twitter" data-analytics-asset-type="web-content"><a
href="https://twitter.com/mcitgovsa?s=11" title="twitter" target="_blank"> <span class="icon-
twitter"></span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84442" data-analytics-
asset-title="Instagram" data-analytics-asset-type="web-content"><a
href="https://www.instagram.com/p/CiIYfgYMhFy/" title="instagram" target="_blank"> <span
class="icon-instagram"></span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84419" data-analytics-
asset-title="Linkedin" data-analytics-asset-type="web-content"><a
href="https://www.linkedin.com/company/mcitgovsa/" title="linkedin" target="_blank"> <span
class="icon-linkedin"></span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84475" data-analytics-
asset-title="youtube" data-analytics-asset-type="web-content"><a
```

```
href="https://www.youtube.com/@Mcitgovsa" title="youtube" target="_blank"> <span class="icon-
youtube"></span> </a>
          </div></li>
          </ul>
          </div></li>
          <li class="d-none d-lg-block">
...
...
...

          <section class="footer-mcit-ecosystem">
          <div class="container">
          <div class="row justify-content-center align-items-center">
          <div class="col-sm-3 h-auto">
          <div class="journal-content-article " data-analytics-asset-id="47025" data-analytics-
asset-title="وحدة التحول الرقمي" data-analytics-asset-type="web-content"><a
href="https://ndu.gov.sa/" class="image-slide d-block" title="وحدة التحول الرقمي" target="_blank">
          <picture data-fileentryid="47007">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/47007/Thumbnail-
300x300/national-img.png?t=1704710148114">
          <source media="(max-width:442px) and (min-width:300px)" srcset="/o/adaptive-
media/image/47007/Preview-1000x0/national-img.png?t=1704710148114">
          <picture data-fileentryid="47007">
...
...
...

          </picture> </a>
          </div>
          </div>
          <div class="col-sm-3 h-auto">
          <div class="journal-content-article " data-analytics-asset-id="47060" data-analytics-
asset-title="هيئة الحكومة الرقمية" data-analytics-asset-type="web-content"><a
href="https://dga.gov.sa/en" class="image-slide d-block" title="هيئة الحكومة الرقمية"
target="_blank">
          <picture data-fileentryid="47048">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/47048/Thumbnail-
300x300/digital-img.png?t=1704710370519">
          <source media="(max-width:405px) and (min-width:300px)" srcset="/o/adaptive-
media/image/47048/Preview-1000x0/digital-img.png?t=1704710370519">
          <picture data-fileentryid="47048">
...
...
...

          </picture> </a>
          </div>
          </div>
          <div class="col-sm-3 h-auto">
          <div class="journal-content-article " data-analytics-asset-id="47095" data-analytics-
asset-title="هيئة الاتصالات و الفضاء و التقنية" data-analytics-asset-type="web-content"><a
href="https://www.cst.gov.sa/en/Pages/default.aspx" class="image-slide d-block" title="هيئة
الاتصالات و الفضاء و التقنية" target="_blank">
          <picture data-fileentryid="47083">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/47083/Thumbnail-
300x300/space-img.png?t=1704710540062">
          <source media="(max-width:493px) and (min-width:300px)" srcset="/o/adaptive-
media/image/47083/Preview-1000x0/space-img.png?t=1704710540062">
          <picture data-fileentryid="47083">
...
...
...
```

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/c
Entity:	c (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /c HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/web/guest/home?
p_p_id=com_liferay_login_web_portlet_LoginPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=vi
ew&_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName=%2Flogin%2Flogin&saveLastPath
=false
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0; COOKIE_SUPPORT=true;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
ID=78692f674d56476771344b754c46314878394f5043513d3d; GUEST_LANGUAGE_ID=ar_SA;
_ga=GA1.1.128297136.1599395143; _ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0;
LFR_SESSION_STATE_20099=1715073020896; JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF;
COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Upgrade-Insecure-Requests: 1
Sec-Fetch-Mode: navigate
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Cache-Control: max-age=0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.7
Sec-Fetch-User: ?1
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: document


...
...
...
          <div class="overflow-hidden">
          <p class="sub-title" title="دعم العمل الحر عن طريق تأهيل وتمكين العاملين المستقلين ومخصص
للمتفرغين للعمل والباحثين عن عمل والعاملين بشكل جزئي.">دعم العمل الحر عن طريق تأهيل وتمكين العاملين
المستقلين ومخصص للمتفرغين للعمل والباحثين عن عمل والعاملين بشكل جزئي.</p>
          </div>
          <div class="overflow-hidden"><a class="btn btn-sm btn-outline-light"
href="https://www.google.com/" target="_blank" title="اقرأ المزيد">اقرأ المزيد</a>
          </div>
          </div>
          </div>
          </div>
...
...
...

          <div class="overflow-hidden">
```

```
          <p class="sub-title" title="تتضمن الاستراتيجية، خطة عمل طموحة تقوم على استقطاب الشركات
الدولية الرائدة في المجالات ذات الأولوية الخاصة بالتقنيات الناشئة.">تتضمن الاستراتيجية، خطة عمل طموحة تقوم
على استقطاب الشركات الدولية الرائدة في المجالات ذات الأولوية الخاصة بالتقنيات الناشئة.</p>
          </div>
          <div class="overflow-hidden"><a class="btn btn-sm btn-outline-light"
href="https://www.google.com/" target="_blank" title="اقرأ المزيد">اقرأ المزيد</a>
          </div>
          </div>
          </div>
          </div>
...
...
...

          <div class="overflow-hidden">
          <p class="sub-title" title="دعم العمل الحر عن طريق تأهيل وتمكين العاملين المستقلين ومخصص
للمتفرغين للعمل والباحثين عن عمل والعاملين بشكل جزئي.">دعم العمل الحر عن طريق تأهيل وتمكين العاملين
المستقلين ومخصص للمتفرغين للعمل والباحثين عن عمل والعاملين بشكل جزئي.</p>
          </div>
          <div class="overflow-hidden"><a class="btn btn-sm btn-outline-light"
href="https://www.google.com/" target="_blank" title="اقرأ المزيد">اقرأ المزيد</a>
          </div>
          </div>
          </div>
          </div>
...
...
...

          <div class="card-col d-flex flex-column h-100">
          <div class="card-info d-flex align-items-center">
          <div class="status d-flex align-items-baseline"><span class="icon-status d-sm-inline-
block d-none"></span> <span title="مكتمل">مكتمل</span>
          </div>
          <div class="location d-flex align-items-baseline"><span class="icon-location d-sm-
inline-block d-none"></span> <a href="https://www.google.com/" title="افتراضي"
target="_blank">افتراضي</a> <a href="https://www.google.com/" title="حضوري"
target="_blank">حضوري</a>
          </div>
          </div>
          <div class="card-head">
          <h4 title="2 اليوم العالمي للتطوع السعودي">اليوم العالمي للتطوع السعودي 2</h4>
...
...
...

          <div class="card-col d-flex flex-column h-100">
          <div class="card-info d-flex align-items-center">
          <div class="status d-flex align-items-baseline"><span class="icon-status d-sm-inline-
block d-none"></span> <span title="مكتمل">مكتمل</span>
          </div>
          <div class="location d-flex align-items-baseline"><span class="icon-location d-sm-
inline-block d-none"></span> <a href="https://www.google.com/" title="افتراضي"
target="_blank">افتراضي</a> <a href="https://www.google.com/" title="حضوري"
target="_blank">حضوري</a>
          </div>
          </div>
          <div class="card-head">
          <h4 title="2 اليوم العالمي للتطوع السعودي">اليوم العالمي للتطوع السعودي 2</h4>
...
...
...

          <div class="card-col d-flex flex-column h-100">
          <div class="card-info d-flex align-items-center">
          <div class="status d-flex align-items-baseline"><span class="icon-status d-sm-inline-
block d-none"></span> <span title="مكتمل">مكتمل</span>
          </div>
          <div class="location d-flex align-items-baseline"><span class="icon-location d-sm-
inline-block d-none"></span> <a href="https://www.google.com/" title="حضوري"
target="_blank">حضوري</a>
          </div>
          </div>
          <div class="card-head">
          <h4 title="1 اليوم العالمي للتطوع السعودي">اليوم العالمي للتطوع السعودي 1</h4>
...
...
...
```

```
          <div class="card-col d-flex flex-column h-100">
          <div class="card-info d-flex align-items-center">
          <div class="status d-flex align-items-baseline"><span class="icon-status d-sm-inline-
block d-none"></span> <span title="مكتمل">مكتمل</span>
          </div>
          <div class="location d-flex align-items-baseline"><span class="icon-location d-sm-
inline-block d-none"></span> <a href="https://www.google.com/" title="افتراضي"
target="_blank">افتراضي</a>
          </div>
          </div>
          <div class="card-head">
          <h4 title="اليوم العالمي للتطوع السعودي 2">اليوم العالمي للتطوع السعودي 2</h4>
...
...
...

          <div class="card-col d-flex flex-column h-100">
          <div class="card-info d-flex align-items-center">
          <div class="status d-flex align-items-baseline"><span class="icon-status d-sm-inline-
block d-none"></span> <span title="مكتمل">مكتمل</span>
          </div>
          <div class="location d-flex align-items-baseline"><span class="icon-location d-sm-
inline-block d-none"></span> <a href="https://www.google.com/" title="افتراضي"
target="_blank">افتراضي</a>
          </div>
          </div>
          <div class="card-head">
          <h4 title="اليوم العالمي للتطوع السعودي 2">اليوم العالمي للتطوع السعودي 2</h4>
...
...
...

          <div class="card-col d-flex flex-column h-100">
          <div class="card-info d-flex align-items-center">
          <div class="status d-flex align-items-baseline"><span class="icon-status d-sm-inline-
block d-none"></span> <span title="مكتمل">مكتمل</span>
          </div>
          <div class="location d-flex align-items-baseline"><span class="icon-location d-sm-
inline-block d-none"></span> <a href="https://www.google.com/" title="افتراضي"
target="_blank">افتراضي</a>
          </div>
          </div>
          <div class="card-head">
          <h4 title="اليوم العالمي للتطوع السعودي 2">اليوم العالمي للتطوع السعودي 2</h4>
...
...
...

          </div>
          <div class="container">
          <div class="owl-carousel owl-theme owl-home-partners">
          <div class="item h-auto">
          <div class="journal-content-article " data-analytics-asset-id="35686" data-analytics-
asset-title="المركز الوطني لتنمية القطاع غير الربحي" data-analytics-asset-type="web-content"><a
href="https://ncnp.gov.sa/en" class="image-slide d-flex justify-content-center align-items-center
h-100" title="المركز الوطني لتنمية القطاع غير الربحي" target="_blank">
          <picture data-fileentryid="40666">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/40666/Thumbnail-
300x300/NAPS+%281%29.png?t=1702746299256">
          <source media="(max-width:414px) and (min-width:300px)" srcset="/o/adaptive-
media/image/40666/Preview-1000x0/NAPS+%281%29.png?t=1702746299256">
...
...
...

          </div>
          </div>
          <div class="item h-auto">
          <div class="journal-content-article " data-analytics-asset-id="35674" data-analytics-
asset-title="التحول الرقمي والحلول المعتمدة على الذكاء الاصطناعي" data-analytics-asset-type="web-
content"><a href="https://thinktechnow.com/" class="image-slide d-flex justify-content-center
align-items-center h-100" title="التحول الرقمي والحلول المعتمدة على الذكاء الاصطناعي" target="_blank">
          <picture data-fileentryid="40561">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/40561/Thumbnail-
300x300/thinktech+%281%29.png?t=1702745963237">
          <source media="(max-width:354px) and (min-width:300px)" srcset="/o/adaptive-
media/image/40561/Preview-1000x0/thinktech+%281%29.png?t=1702745963237">
```

```
...
...
...

          </picture> </a>
          </div>
          </div>
          <div class="item h-auto">
          <div class="journal-content-article " data-analytics-asset-id="35656" data-analytics-
asset-title="مبادرة العطاء الرقمي" data-analytics-asset-type="web-content"><a
href="https://attaa.sa/" class="image-slide d-flex justify-content-center align-items-center h-
100" title="مبادرة العطاء الرقمي" target="_blank">
          <picture data-fileentryid="40698">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/40698/Thumbnail-
300x300/Atta-Digital+%281%29.png?t=1702746406364">
          <source media="(max-width:414px) and (min-width:300px)" srcset="/o/adaptive-
media/image/40698/Preview-1000x0/Atta-Digital+%281%29.png?t=1702746406364">
          <picture data-fileentryid="40698">
...
...
...

          </picture> </a>
          </div>
          </div>
          <div class="item h-auto">
          <div class="journal-content-article " data-analytics-asset-id="35582" data-analytics-
asset-title="المركز الوطني لتنمية القطاع غير الربحي" data-analytics-asset-type="web-content"><a
href="https://ncnp.gov.sa/en" class="image-slide d-flex justify-content-center align-items-center
h-100" title="المركز الوطني لتنمية القطاع غير الربحي" target="_blank">
          <picture data-fileentryid="40666">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/40666/Thumbnail-
300x300/NAPS+%281%29.png?t=1702746299256">
          <source media="(max-width:414px) and (min-width:300px)" srcset="/o/adaptive-
media/image/40666/Preview-1000x0/NAPS+%281%29.png?t=1702746299256">
...
...
...

          </picture> </a>
          </div>
          </div>
          <div class="item h-auto">
          <div class="journal-content-article " data-analytics-asset-id="35549" data-analytics-
asset-title="المرصد الوطني للعمل" data-analytics-asset-type="web-content"><a
href="https://nlo.gov.sa/" class="image-slide d-flex justify-content-center align-items-center h-
100" title="المرصد الوطني للعمل" target="_blank">
          <picture data-fileentryid="40634">
          <source media="(max-width:168px)" srcset="/o/adaptive-media/image/40634/Preview-
1000x0/NAO+%281%29.png?t=1702746200592">
          <source media="(max-width:168px) and (min-width:168px)" srcset="/o/adaptive-
media/image/40634/Thumbnail-300x300/NAO+%281%29.png?t=1702746200592">
          <picture data-fileentryid="40634">
...
...
...

          </picture> </a>
          </div>
          </div>
          <div class="item h-auto">
          <div class="journal-content-article " data-analytics-asset-id="35519" data-analytics-
asset-title="الأكاديمية السعودية الرقمية" data-analytics-asset-type="web-content"><a
href="https://sda.edu.sa/" class="image-slide d-flex justify-content-center align-items-center h-
100" title="الأكاديمية السعودية الرقمية" target="_blank"><a href="https://thinktechnow.com/"
class="image-slide d-flex justify-content-center align-items-center h-100" title="التحول الرقمي
والحلول المعتمدة على الذكاء الاصطناعي" target="_blank">--end_highlight_tag--
          <picture data-fileentryid="40561">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/40561/Thumbnail-
300x300/thinktech+%281%29.png?t=1702745963237">
          <source media="(max-width:354px) and (min-width:300px)" srcset="/o/adaptive-
media/image/40561/Preview-1000x0/thinktech+%281%29.png?t=1702745963237">
...
...
...

          <li class="d-block">
          <div class="social-media-links"><span title="تابعنا على">تابعنا على</span>
```

```
          <ul>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84409" data-analytics-
asset-title="Facebook" data-analytics-asset-type="web-content">
          <picture data-fileentryid="40561">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/40561/Thumbnail-
300x300/thinktech+%281%29.png?t=1702745963237">
          <source media="(max-width:354px) and (min-width:300px)" srcset="/o/adaptive-
media/image/40561/Preview-1000x0/thinktech+%281%29.png?t=1702745963237">
...
...
...

          <li class="d-block">
          <div class="social-media-links"><span title="تابعنا على">تابعنا على</span>
          <ul>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84409" data-analytics-
asset-title="Facebook" data-analytics-asset-type="web-content">--begin_highlight_tag--<a
href="https://www.facebook.com/McitGovSa/" title="facebook" target="_blank"><a
href="https://www.facebook.com/McitGovSa/" title="facebook" target="_blank">--end_highlight_tag--
<span class="icon-facebook"></span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84452" data-analytics-
asset-title="Twitter" data-analytics-asset-type="web-content"> <span class="icon-facebook">
</span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84452" data-analytics-
asset-title="Twitter" data-analytics-asset-type="web-content">--begin_highlight_tag--<a
href="https://twitter.com/mcitgovsa?s=11" title="twitter" target="_blank"><a
href="https://twitter.com/mcitgovsa?s=11" title="twitter" target="_blank">--end_highlight_tag--
<span class="icon-twitter"></span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84442" data-analytics-
asset-title="Instagram" data-analytics-asset-type="web-content"> <span class="icon-twitter">
</span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84442" data-analytics-
asset-title="Instagram" data-analytics-asset-type="web-content">--begin_highlight_tag--<a
href="https://www.instagram.com/p/CiIYfgYMhFy/" title="instagram" target="_blank"><a
href="https://www.instagram.com/p/CiIYfgYMhFy/" title="instagram" target="_blank">--
end_highlight_tag-- <span class="icon-instagram"></span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84419" data-analytics-
asset-title="Linkedin" data-analytics-asset-type="web-content"> <span class="icon-instagram">
</span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84419" data-analytics-
asset-title="Linkedin" data-analytics-asset-type="web-content">--begin_highlight_tag--<a
href="https://www.linkedin.com/company/mcitgovsa/" title="linkedin" target="_blank"><a
href="https://www.linkedin.com/company/mcitgovsa/" title="linkedin" target="_blank">--
end_highlight_tag-- <span class="icon-linkedin"></span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84475" data-analytics-
asset-title="youtube" data-analytics-asset-type="web-content"> <span class="icon-linkedin">
</span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84475" data-analytics-
asset-title="youtube" data-analytics-asset-type="web-content">--begin_highlight_tag--<a
href="https://www.youtube.com/@Mcitgovsa" title="youtube" target="_blank"><a
href="https://www.youtube.com/@Mcitgovsa" title="youtube" target="_blank">--end_highlight_tag--
<span class="icon-youtube"></span> </a>
          </div></li>
          </ul>
          </div></li>
          <li class="d-none d-lg-block">
...
...
...
```

```
          <section class="footer-mcit-ecosystem">
          <div class="container">
          <div class="row justify-content-center align-items-center">
          <div class="col-sm-3 h-auto">
          <div class="journal-content-article " data-analytics-asset-id="47025" data-analytics-
asset-title="وحدة التحول الرقمي" data-analytics-asset-type="web-content"> <span class="icon-
youtube"></span> </a>
          </div></li>
          </ul>
          </div></li>
          <li class="d-none d-lg-block">
...
...
...

          <section class="footer-mcit-ecosystem">
          <div class="container">
          <div class="row justify-content-center align-items-center">
          <div class="col-sm-3 h-auto">
          <div class="journal-content-article " data-analytics-asset-id="47025" data-analytics-
asset-title="وحدة التحول الرقمي" data-analytics-asset-type="web-content">--begin_highlight_tag--<a
href="https://ndu.gov.sa/" class="image-slide d-block" title="وحدة التحول الرقمي"
target="_blank"><a href="https://ndu.gov.sa/" class="image-slide d-block" title="وحدة التحول
الرقمي" target="_blank">--end_highlight_tag--
          <picture data-fileentryid="47007">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/47007/Thumbnail-
300x300/national-img.png?t=1704710148114">
          <source media="(max-width:442px) and (min-width:300px)" srcset="/o/adaptive-
media/image/47007/Preview-1000x0/national-img.png?t=1704710148114">
          <picture data-fileentryid="47007">
...
...
...

          </picture> </a>
          </div>
          </div>
          <div class="col-sm-3 h-auto">
          <div class="journal-content-article " data-analytics-asset-id="47060" data-analytics-
asset-title="هيئة الحكومة الرقمية" data-analytics-asset-type="web-content">
          <picture data-fileentryid="47007">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/47007/Thumbnail-
300x300/national-img.png?t=1704710148114">
          <source media="(max-width:442px) and (min-width:300px)" srcset="/o/adaptive-
media/image/47007/Preview-1000x0/national-img.png?t=1704710148114">
          <picture data-fileentryid="47007">
...
...
...

          </picture> </a>
          </div>
          </div>
          <div class="col-sm-3 h-auto">
          <div class="journal-content-article " data-analytics-asset-id="47060" data-analytics-
asset-title="هيئة الحكومة الرقمية" data-analytics-asset-type="web-content">--begin_highlight_tag--
<a href="https://dga.gov.sa/en" class="image-slide d-block" title="هيئة الحكومة الرقمية"
target="_blank"><a href="https://dga.gov.sa/en" class="image-slide d-block" title="هيئة الحكومة
الرقمية" target="_blank">--end_highlight_tag--
          <picture data-fileentryid="47048">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/47048/Thumbnail-
300x300/digital-img.png?t=1704710370519">
          <source media="(max-width:405px) and (min-width:300px)" srcset="/o/adaptive-
media/image/47048/Preview-1000x0/digital-img.png?t=1704710370519">
          <picture data-fileentryid="47048">
...
...
...

          </picture> </a>
          </div>
          </div>
          <div class="col-sm-3 h-auto">
          <div class="journal-content-article " data-analytics-asset-id="47095" data-analytics-
asset-title="هيئة الاتصالات و الفضاء و التقنية" data-analytics-asset-type="web-content">
          <picture data-fileentryid="47048">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/47048/Thumbnail-
300x300/digital-img.png?t=1704710370519">
```

```
          <source media="(max-width:405px) and (min-width:300px)" srcset="/o/adaptive-
media/image/47048/Preview-1000x0/digital-img.png?t=1704710370519">
          <picture data-fileentryid="47048">
...
...
...

          </picture> </a>
          </div>
          </div>
          <div class="col-sm-3 h-auto">
          <div class="journal-content-article " data-analytics-asset-id="47095" data-analytics-
asset-title="هيئة الاتصالات و الفضاء و التقنية" data-analytics-asset-type="web-content">--
begin_highlight_tag--<a href="https://www.cst.gov.sa/en/Pages/default.aspx" class="image-slide d-
block" title="هيئة الاتصالات و الفضاء و التقنية" target="_blank"><a
href="https://www.cst.gov.sa/en/Pages/default.aspx" class="image-slide d-block" title="هيئة
الاتصالات و الفضاء و التقنية" target="_blank">--end_highlight_tag--
          <picture data-fileentryid="47083">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/47083/Thumbnail-
300x300/space-img.png?t=1704710540062">
          <source media="(max-width:493px) and (min-width:300px)" srcset="/o/adaptive-
media/image/47083/Preview-1000x0/space-img.png?t=1704710540062">
          <picture data-fileentryid="47083">
...
...
...
```

Issue 6 of 7

TOC

Unsafe third-party link (target="_blank")	
Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/web/guest/recruitment-options
Entity:	recruitment-options (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /web/guest/recruitment-options HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/home/client
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
LFR_SESSION_STATE_20099=1715073020896; _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073077970;
_ga=GA1.1.128297136.1599395143;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
ID=78692f674d56476771344b754c46314878394f5043513d3d; COMPANY_ID=20096; COOKIE_SUPPORT=true;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
```

```
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; GUEST_LANGUAGE_ID=ar_SA
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
x-csrf-token: MEQeGkLB
x-requested-with: XMLHttpRequest
sec-ch-ua-mobile: ?0
x-pjax: true
Accept: */*
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty


...
...
...
          <li class="d-block">
          <div class="social-media-links"><span title="تابعنا على">تابعنا على</span>
          <ul>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84409" data-analytics-
asset-title="Facebook" data-analytics-asset-type="web-content"><a
href="https://www.facebook.com/McitGovSa/" title="facebook" target="_blank"> <span class="icon-
facebook"></span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84452" data-analytics-
asset-title="Twitter" data-analytics-asset-type="web-content"><a
href="https://twitter.com/mcitgovsa?s=11" title="twitter" target="_blank"> <span class="icon-
twitter"></span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84442" data-analytics-
asset-title="Instagram" data-analytics-asset-type="web-content"><a
href="https://www.instagram.com/p/CiIYfgYMhFy/" title="instagram" target="_blank"> <span
class="icon-instagram"></span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84419" data-analytics-
asset-title="Linkedin" data-analytics-asset-type="web-content"><a
href="https://www.linkedin.com/company/mcitgovsa/" title="linkedin" target="_blank"> <span
class="icon-linkedin"></span> </a>
          </div></li>
          <li>
          <div class="journal-content-article " data-analytics-asset-id="84475" data-analytics-
asset-title="youtube" data-analytics-asset-type="web-content"><a
href="https://www.youtube.com/@Mcitgovsa" title="youtube" target="_blank"> <span class="icon-
youtube"></span> </a>
          </div></li>
          </ul>
          </div></li>
          <li class="d-none d-lg-block">
...
...
...

          <section class="footer-mcit-ecosystem">
          <div class="container">
          <div class="row justify-content-center align-items-center">
          <div class="col-sm-3 h-auto">
          <div class="journal-content-article " data-analytics-asset-id="47025" data-analytics-
asset-title="وحدة التحول الرقمي" data-analytics-asset-type="web-content"><a
href="https://ndu.gov.sa/" class="image-slide d-block" title="وحدة التحول الرقمي" target="_blank">
          <picture data-fileentryid="47007">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/47007/Thumbnail-
```

```
300x300/national-img.png?t=1704710148114">
          <source media="(max-width:442px) and (min-width:300px)" srcset="/o/adaptive-
media/image/47007/Preview-1000x0/national-img.png?t=1704710148114">
          <picture data-fileentryid="47007">
...
...
...

          </picture> </a>
          </div>
          </div>
          <div class="col-sm-3 h-auto">
          <div class="journal-content-article " data-analytics-asset-id="47060" data-analytics-
asset-title="هيئة الحكومة الرقمية" data-analytics-asset-type="web-content"><a
href="https://dga.gov.sa/en" class="image-slide d-block" title="هيئة الحكومة الرقمية"
target="_blank">
          <picture data-fileentryid="47048">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/47048/Thumbnail-
300x300/digital-img.png?t=1704710370519">
          <source media="(max-width:405px) and (min-width:300px)" srcset="/o/adaptive-
media/image/47048/Preview-1000x0/digital-img.png?t=1704710370519">
          <picture data-fileentryid="47048">
...
...
...

          </picture> </a>
          </div>
          </div>
          <div class="col-sm-3 h-auto">
          <div class="journal-content-article " data-analytics-asset-id="47095" data-analytics-
asset-title="هيئة الاتصالات و الفضاء و التقنية" data-analytics-asset-type="web-content"><a
href="https://www.cst.gov.sa/en/Pages/default.aspx" class="image-slide d-block" title="هيئة
الاتصالات و الفضاء و التقنية" target="_blank">
          <picture data-fileentryid="47083">
          <source media="(max-width:300px)" srcset="/o/adaptive-media/image/47083/Thumbnail-
300x300/space-img.png?t=1704710540062">
          <source media="(max-width:493px) and (min-width:300px)" srcset="/o/adaptive-
media/image/47083/Preview-1000x0/space-img.png?t=1704710540062">
          <picture data-fileentryid="47083">
...
...
...
```

Issue 7 of 7

TOC

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://mcit-liferayqc.linkdev.com/web/guest/home
Entity:	home (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /web/guest/home?
p_p_id=com_liferay_login_web_portlet_LoginPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=vi
ew&_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName=%2Flogin%2Flogin&saveLastPath
=false HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/c/portal/login?p_l_id=129
Cookie: COOKIE_SUPPORT=true; GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: Keep-Alive
Host: mcit-liferayqc.linkdev.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Liferay-Portal: Liferay Digital Experience Platform
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Set-Cookie: JSESSIONID=83F99BB5369AC6AA3CDC7BA3BC14493D; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 10:04:14 GMT
Content-Type: text/html;charset=UTF-8









<!DOCTYPE html>
```

```
<html class="rtl" dir="rtl" lang="ar-SA">

<head>
 <title>       وزارة الاتصالات وتقنية المعلومات - الرئيسية</title>
  <meta name="viewport" content="width=device-width, width=device-width" />
  <meta name="description" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية " />
  <meta name="keywords" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية">
  <meta name="format-detection" content="telephone=no">
  <meta property="og:url" content="/web/guest/home?
p_p_id=com_liferay_login_web_portlet_LoginPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=vi
ew&_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName=%2Flogin%2Flogin&saveLastPath
=false" />
  <meta property="og:type" content="Website" />
  <meta property="og:title" conte
...
...
...

                            <a href="https://www.facebook.com/McitGovSa/" title="facebook"
target="_blank">
    <span class="icon-facebook"></span>
  </a>
...
...
...
                            <a href="https://twitter.com/mcitgovsa?s=11" title="twitter"
target="_blank">
    <span class="icon-twitter"></span>
  </a>
...
...
...
                            <a href="https://www.instagram.com/p/CiIYfgYMhFy/" title="instagram"
```

```
target="_blank">
    <span class="icon-instagram"></span>
  </a>
...
...
...
                        <a href="https://www.linkedin.com/company/mcitgovsa/" title="linkedin"
target="_blank">
    <span class="icon-linkedin"></span>
  </a>
...
...
...
                        <a href="https://www.youtube.com/@Mcitgovsa" title="youtube"
target="_blank">
    <span class="icon-youtube"></span>
  </a>
...
...
...
                            <a href="https://ndu.gov.sa/" class="image-slide d-block"
title="وحدة التحول الرقمي" target="_blank">
        <picture data-fileentryid="47007"><source media="(max-width:300px)"
srcset="/o/adaptive-media/image/47007/Thumbnail-300x300/national-img.png?t=1704710148114"><source
media="(max-width:442px) and (min-width:300px)" srcset="/o/adaptive-media/image/47007/Preview-
1000x0/national-img.png?t=1704710148114"><img src="https://mcit-
liferayqc.linkdev.com/documents/20119/0/national-img.png/b870b8f9-21ef-9a9d-e990-a1925bb37594?
t=1704710148114" data-fileentryid="47007" title="وحدة التحول الرقمي " alt="وحدة التحول الرقمي">
</picture>
   </a>
...
...
...
                            <a href="https://dga.gov.sa/en" class="image-slide d-block"
title="هيئة الحكومة الرقمية" target="_blank">
        <picture data-fileentryid="47048"><source media="(max-width:300px)"
srcset="/o/adaptive-media/image/47048/Thumbnail-300x300/digital-img.png?t=1704710370519"><source
media="(max-width:405px) and (min-width:300px)" srcset="/o/adaptive-media/image/47048/Preview-
1000x0/digital-img.png?t=1704710370519"><img src="https://mcit-
liferayqc.linkdev.com/documents/20119/0/digital-img.png/89d76923-dd22-fb7a-ef3d-d02eaf504f00?
t=1704710370519" data-fileentryid="47048" title="هيئة الحكومة الرقمية " alt="هيئة الحكومة الرقمية">
</picture>
   </a>
...
...
...
                            <a href="https://www.cst.gov.sa/en/Pages/default.aspx"
class="image-slide d-block" title="هيئة الاتصالات و الفضاء و التقنية" target="_blank">
        <picture data-fileentryid="47083"><source media="(max-width:300px)"
srcset="/o/adaptive-media/image/47083/Thumbnail-300x300/space-img.png?t=1704710540062"><source
media="(max-width:493px) and (min-width:300px)" srcset="/o/adaptive-media/image/47083/Preview-
1000x0/space-img.png?t=1704710540062"><img src="https://mcit-
liferayqc.linkdev.com/documents/20119/0/space-img.png/672e4b1c-d12a-dba4-c0e5-4b7310c97b8e?
t=1704710540062" data-fileentryid="47083" title="هيئة الاتصالات و الفضاء و التقنية " alt="هيئة الاتصالات و
الفضاء و التقنية"></picture>
   </a>
...
...
...
```

Issue 1 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/mcit-registration/v1.0/individualRegistration
Entity:	->"gender" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/mcit-registration/v1.0/individualRegistration HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/individual-registeration/
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0; _ga=GA1.1.128297136.1599395143;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_20099=1715072401645;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0; COOKIE_SUPPORT=true;
GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1238
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "firstName": "appscan",
 "firstNameAr": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "lastNameAr": "\u062a\u0633\u062a",
 "lastName": "test",
 "birthDate": "05-01-2024",
```

```
 "gender": "",
 "nationalityCode": "7",
 "currentCountryCode": "a5850948-fc7e-ee11-a46d-000d3a2df947",
 "cityCode": "",
 "identityId": "11122324",
 "identityType": 753240002,
 "userType": 1,
 "recaptchaResponse":
"03AFcWeA5mBel1XrnrT8saLAPe3vE167CAe3LvbRrPeWbWd0d8fLJaLv_V4RcbyjlHWuPSMV1Kpu_lgxM9hIXpZlypL55qZR
y-PCv1pd8mOwWAVF0FqepBF2DNPHyaut01vfREz1cZOyblEI2jOVfSLmVku2fNkVzR-
xCUsh8cd7RegyCD1RR2lLcXbyreZDXwt0lUjDn5w2L9BHTclNmCmlv751IBkU04Fu8GRlCtEjQM9VGfgs_VuHUuXnBqB570Gx
nFMB84MYSF8_-ZDDAFQEa5nCrAJ6jm5ny_djdkz47R4PKFqS4SCLp9mZ_-8bllp-
AOX73ZpwEWMug8uhm4bDLlQNJnnpH0KfShzxrLMArkmfbCVndFFTqzBIg2qRj0RKl2sZbVbDx97Rcz44HDn_N84zbUi6U5S2n
Ms1fFwOnONy12Me00AvNNGfApEofZhrjOUwIA02N8a5_32eQebu3LJtyW9ro3qwOVHtLEOjsYZrY3rgLgVdtsgeC6jucda1Nk
jRM6A5DJYrg2HBCLliWqXwddiTewpsbNr9ULk6kdTgms65DUxjERTwz0vIi7zOlup_bAlmJntJvKBuZ-9WV-
PFbdJO9vZqFnOSEtbD_37m2XlvlF-ukTm66FGrKwy3ggdIXwRbpCOK39ek2of7LGZdqh50205PS_E-
tSWz4BPfqEkYsyiuztBeyCJq-6EBJaqbvL3sn_fEkPolRjUFDPWm3Ke7ylOw",
 "password": "P@ssw0rd",
 "re-password": "P@ssw0rd",
 "isNafazAccount": false,
 "email": "vepapi2863@rehezb.com",
 "mobilePhone": "+966 11 888 6660",
 "locale": "ar_SA"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=9FA787F78941CC54AABB0CFFF5868925; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 10:34:47 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Error"

}
```


Issue 2 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"applicationQualifications"[0]->"universityName" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1842
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
         "key": "residence",
         "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                         "key": "4",
                         "name": "4"
                 }       ,
                 "qualification": {
                         "key": "masters",
                         "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": ""
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
```

```
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
         "key": "key2",
         "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
         "value": "",
         "disable": true
 },
 "fieldOfInterest": {
         "key": "facilitiesSecurityAndSafety",
         "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
         "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=D70C81AD4913DB0DF6AE9EBA6F1FD8C0; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 10:55:19 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Error"
...
...
...
```


Issue 3 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/mcit-registration/v1.0/individualRegistration
Entity:	->"userType" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/mcit-registration/v1.0/individualRegistration HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/individual-registeration/
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0; _ga=GA1.1.128297136.1599395143;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_20099=1715072401645;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0; COOKIE_SUPPORT=true;
GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1241
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "firstName": "appscan",
 "firstNameAr": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "lastNameAr": "\u062a\u0633\u062a",
 "lastName": "test",
 "birthDate": "05-01-2024",
 "gender": true,
 "nationalityCode": "7",
 "currentCountryCode": "a5850948-fc7e-ee11-a46d-000d3a2df947",
 "cityCode": "",
 "identityId": "11122324",
 "identityType": 753240002,
 "userType": "",
 "recaptchaResponse":
"03AFcWeA5mBel1XrnrT8saLAPe3vE167CAe3LvbRrPeWbWd0d8fLJaLv_V4RcbyjlHWuPSMV1Kpu_lgxM9hIXpZlypL55qZR
y-PCv1pd8mOwWAVF0FqepBF2DNPHyaut01vfREz1cZOyblEI2jOVfSLmVku2fNkVzR-
xCUsh8cd7RegyCD1RR2lLcXbyreZDXwt0lUjDn5w2L9BHTclNmCmlv751IBkU04Fu8GRlCtEjQM9VGfgs_VuHUuXnBqB570Gx
nFMB84MYSF8_-ZDDAFQEa5nCrAJ6jm5ny_djdkz47R4PKFqS4SCLp9mZ_-8bllp-
AOX73ZpwEWMug8uhm4bDLlQNJnnpH0KfShzxrLMArkmfbCVndFFTqzBIg2qRj0RKl2sZbVbDx97Rcz44HDn_N84zbUi6U5S2n
Ms1fFwOnONy12Me00AvNNGfApEofZhrjOUwIA02N8a5_32eQebu3LJtyW9ro3qwOVHtLEOjsYZrY3rgLgVdtsgeC6jucda1Nk
jRM6A5DJYrg2HBCLliWqXwddiTewpsbNr9ULk6kdTgms65DUxjERTwz0vIi7zOlup_bAlmJntJvKBuZ-9WV-
PFbdJO9vZqFnOSEtbD_37m2XlvlF-ukTm66FGrKwy3ggdIXwRbpCOK39ek2of7LGZdqh50205PS_E-
tSWz4BPfqEkYsyiuztBeyCJq-6EBJaqbvL3sn_fEkPolRjUFDPWm3Ke7ylOw",
 "password": "P@ssw0rd",
 "re-password": "P@ssw0rd",
 "isNafazAccount": false,
```

```
 "email": "vepapi2863@rehezb.com",
 "mobilePhone": "+966 11 888 6660",
 "locale": "ar_SA"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=0AD5C665CFC4735D190C4A9A48678884; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 10:35:47 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Error"

}
```

Issue 4 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/mcit-registration/v1.0/individualRegistration
Entity:	->"isNafazAccount" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/mcit-registration/v1.0/individualRegistration HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/individual-registeration/
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0; _ga=GA1.1.128297136.1599395143;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_20099=1715072401645;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0; COOKIE_SUPPORT=true;
GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
```

```
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1237
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "firstName": "appscan",
 "firstNameAr": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "lastNameAr": "\u062a\u0633\u062a",
 "lastName": "test",
 "birthDate": "05-01-2024",
 "gender": true,
 "nationalityCode": "7",
 "currentCountryCode": "a5850948-fc7e-ee11-a46d-000d3a2df947",
 "cityCode": "",
 "identityId": "11122324",
 "identityType": 753240002,
 "userType": 1,
 "recaptchaResponse":
"03AFcWeA5mBe11XrnrT8saLAPe3vE167CAe3LvbRrPeWbWd0d8fLJaLv_V4RcbyjlHWuPSMV1Kpu_lgxM9hIXpZlypL55qZR
y-PCv1pd8mOwWAVF0FqepBF2DNPHyaut01vfREz1cZOyblEI2jOVfSLmVku2fNkVzR-
xCUsh8cd7RegyCD1RR2lLcXbyreZDXwt0lUjDn5w2L9BHTclNmCmlv751IBkU04Fu8GRlCtEjQM9VGfgs_VuHUuXnBqB570Gx
nFMB84MYSF8_-ZDDAFQEa5nCrAJ6jm5ny_djdkz47R4PKFqS4SCLp9mZ_-8bllp-
AOX73ZpwEWMug8uhm4bDLlQNJnnpH0KfShzxrLMArkmfbCVndFFTqzBIg2qRj0RKl2sZbVbDx97Rcz44HDn_N84zbUi6U5S2n
Ms1fFwOnONy12Me00AvNNGfApEofZhrjOUwIA02N8a5_32eQebu3LJtyW9ro3qwOVHtLEOjsYZrY3rgLgVdtsgeC6jucda1Nk
jRM6A5DJYrg2HBCLliWqXwddiTewpsbNr9ULk6kdTgms65DUxjERTwz0vIi7zOlup_bAlmJntJvKBuZ-9WV-
PFbdJO9vZqFnOSEtbD_37m2XlvlF-ukTm66FGrKwy3ggdIXwRbpCOK39ek2of7LGZdqh50205PS_E-
tSWz4BPfqEkYsyiuztBeyCJq-6EBJaqbvL3sn_fEkPolRjUFDPWm3Ke7y1Ow",
 "password": "P@ssw0rd",
 "re-password": "P@ssw0rd",
 "isNafazAccount": "",
 "email": "vepapi2863@rehezb.com",
 "mobilePhone": "+966 11 888 6660",
 "locale": "ar_SA"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=BF3380984F1E67F1B85CBF32DB9305CA; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 10:36:11 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Error"

}
```

Issue 5 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"alreadyRegistered" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEalliOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1850
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
        "key": "residence",
        "name": "\u0625\u0642\u0627\u0645\u0629"
 },
```

```
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                         "key": "4",
                         "name": "4"
                 }       ,
                 "qualification": {
                         "key": "masters",
                         "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
         "key": "key2",
         "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
         "value": "",
         "disable": true
 },
 "fieldOfInterest": {
         "key": "facilitiesSecurityAndSafety",
         "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": "\u0000",
 "cv": {
         "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=53649BB535805675C7F80D111B3EFE43; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 10:55:02 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server
...
...
...
```

Issue 6 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"identityType"->"key" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21lNTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEalliOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1847
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json
```

```
{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
        "key.": "residence",
        "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                        "key": "4",
                        "name": "4"
                 }       ,
                 "qualification": {
                        "key": "masters",
                        "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
        "key": "key2",
        "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
        "value": "",
        "disable": true
 },
 "fieldOfInterest": {
        "key": "facilitiesSecurityAndSafety",
        "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
        "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}
```


```
HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=DA492DBC5B15D6C300976248188D5C0C; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 10:57:47 GMT
```

```
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Er
...
...
...
```

Issue 7 of 35

TOC

Application Error	
Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"birthDate" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25Ecjlzbmxl ZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
```

```
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1836
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
        "key": "residence",
        "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                        "key": "4",
                        "name": "4"
                 }       ,
                 "qualification": {
                        "key": "masters",
                        "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
        "key": "key2",
        "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
        "value": "",
        "disable": true
 },
 "fieldOfInterest": {
        "key": "facilitiesSecurityAndSafety",
        "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
        "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}
```

```
HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=BCCABF873F5A075981868D61670FD925; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:02:24 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Error"

}
```

Issue 8 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"applicationQualifications"[0]->"graduationDate" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
```

```
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1847
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
         "key": "residence",
         "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate.": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                         "key": "4",
                         "name": "4"
                 }       ,
                 "qualification": {
                         "key": "masters",
                         "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
         "key": "key2",
         "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
         "value": "",
         "disable": true
 },
 "fieldOfInterest": {
         "key": "facilitiesSecurityAndSafety",
         "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
         "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
```

```
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=08234D0D66F72B7F6D3CBFD92E471238; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 10:57:14 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Er
...
...
...
```

Issue 9 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/mcit-common-apis/v1.0/uploadFile
Entity:	->"mimeType" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/mcit-common-apis/v1.0/uploadFile HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga=GA1.1.128297136.1599395143; _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
```

```
LFR_SESSION_STATE_116486=1715073214368; _ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
LFR_SESSION_STATE_20099=1715073020896; COOKIE_SUPPORT=true;
ID=78692f674d56476771344b754c46314878394f5043513d3d; GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 12199
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "file":
"/9j/4AAQSkZJRgABAQEAeAB4AAD/2wBDAAIBAQIBAQICAgICAgICAwUDAwMDAwYEBAMFBwYHBwcGBwcICQsJCAgKCAcHCg0K
CgsMDAwMBwkODw0MDgsMDAz/2wBDAQICAgMDAwYDAwYMCAcIDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMD
AwMDAwMDAwMDAwMDAz/wAARCAGXAmMDASIAAhEBAxEB/8QAHwAAAQUBAQEBAQEAAAAAAAAAAAECAwQFBgcICQoL/8QAtRAAAg
EDAwIEAwUFBAQAAAF9AQIDAAQRBRIhMUEGE1FhByJxFDKBkaEII0KxwRVS0fAkM2JyggkKFhcYGRolJicoKSo0NTY3ODk6Q0R
FRkdISUpTVFVWV1hZWmNkZWZnaGlqc3R1dnd4eXqDhIWGh4iJipKTlJWWl5iZmqKjpKWmp6ipqrKztLW2t7i5usLDxMXGx8jJ
ytLT1NXW19jZ2uHi4+Tl5ufo6erx8vP09fb3+Pn6/8QAHwEAAwEBAQEBAQEBAQAAAAAAAAECAwQFBgcICQoL/8QAtREAAgECB
AQDBAcFBAQAAQJ3AAECAxEEBSExBhJBUQdhcRMiMoEIFEKRobHBCSMzUvAVYnLRChYkNOEl8RcYGRomJygpKjU2Nzg5OkNERU
ZHSElKU1RVVldYWVpjZGVmZ2hpanN0dXZ3eHl6goOEhYaHiImKkpOUlZaXmJmaoqOkpaanqKmqsrO0tba3uLm6wsPExcbHyMn
K0tPU1dbX2Nna4uPk5ebn6Onq8vP09fb3+Pn6/9oADAMBAAIRAxEAPwD9/KKKKACiiigAooooAKKKKACiiigAooooAKKKKACi
iigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACii
igAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiii
gAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiig
AooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigA
ooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAo
oooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACiiigAooooAKDwDRQRkUAFFF
FABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFF
ABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFA
BRRRQAUdKKOtABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRR
QAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQ
AUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQA
UUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAU
UUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUU
UUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUU
UAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUU
AFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFF
...
...
...

 "fileName": "cit (3).jpg",
 "mimeType": "'"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
...
...
...
```

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"nationality" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEalliOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1847
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
```

```
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality.": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
        "key": "residence",
        "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                        "key": "4",
                        "name": "4"
                 }       ,
                 "qualification": {
                        "key": "masters",
                        "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
        "key": "key2",
        "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
        "value": "",
        "disable": true
 },
 "fieldOfInterest": {
        "key": "facilitiesSecurityAndSafety",
        "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
        "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}
```


```
HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=DE84A4B0392A832EA292762869B472B4; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:02:58 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json
```

```
{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Er
...
...
...
```

Issue 11 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"countryKey"->"name" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
```

```
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1847
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
         "key": "residence",
         "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                         "key": "4",
                         "name": "4"
                 }       ,
                 "qualification": {
                         "key": "masters",
                         "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
         "key": "key2",
         "name.": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
         "value": "",
         "disable": true
 },
 "fieldOfInterest": {
         "key": "facilitiesSecurityAndSafety",
         "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
         "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
```

```
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=421470E8D06CFB9A34B966E242F0187C; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:03:12 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Er
...
...
...
```

Issue 12 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"fieldOfInterest"->"key" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
```

```
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1819
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
         "key": "residence",
         "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                         "key": "4",
                         "name": "4"
                 }       ,
                 "qualification": {
                         "key": "masters",
                         "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
         "key": "key2",
         "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
         "value": "",
         "disable": true
 },
 "fieldOfInterest": {
         "key": "",
         "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
         "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
```

```
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=73DFBC2FBF30577A777DE3100C01CB1E; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:02:26 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Error"

}
```

Issue 13 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"isMale" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
```

```
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1847
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
         "key": "residence",
         "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale.": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                         "key": "4",
                         "name": "4"
                 }       ,
                 "qualification": {
                         "key": "masters",
                         "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
         "key": "key2",
         "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
         "value": "",
         "disable": true
 },
 "fieldOfInterest": {
         "key": "facilitiesSecurityAndSafety",
         "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
```

```
 "alreadyRegistered": true,
 "cv": {
        "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=ACDF49849BCBDBBEE8D8E43B73FA219D; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:02:29 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Er
...
...
...
```

Issue 14 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"reCaptcheCheck" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_NlTBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1847
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
        "key": "residence",
        "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                        "key": "4",
                        "name": "4"
                 }       ,
                 "qualification": {
                        "key": "masters",
                        "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
        "key": "key2",
        "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
```

```
 "mobile": "+96611666",
 "city": {
        "value": "",
        "disable": true
 },
 "fieldOfInterest": {
        "key": "facilitiesSecurityAndSafety",
        "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
        "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck.":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=0616E541D8D2AE5DF548929430D2C821; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:02:32 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Er
...
...
...
```


Issue 15 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"identityNumber" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEalliOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1849
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
        "key": "residence",
        "name": "\u0625\u0642\u0627\u0645\u0629"
 },
```

```
 "identityNumber": "       11122324XYZ",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                         "key": "4",
                         "name": "4"
                 }       ,
                 "qualification": {
                         "key": "masters",
                         "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
         "key": "key2",
         "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
         "value": "",
         "disable": true
 },
 "fieldOfInterest": {
         "key": "facilitiesSecurityAndSafety",
         "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
         "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=AE796294F6B950B26ADABCF8641D6266; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:04:10 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERRO
...
...
...
```

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"r_applicationType_c_recruitmentApplicationTypeId" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEalliOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1851
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
```

```
"fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
"fullNameEnglish": "appscan",
"r_applicationType_c_recruitmentApplicationTypeId": "       89319XYZ",
"birthDate": "05-23-2001",
"nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
"identityType": {
        "key": "residence",
        "name": "\u0625\u0642\u0627\u0645\u0629"
},
"identityNumber": "11122324",
"isMale": true,
"applicationQualifications": [
               {
                "average": "4",
                "graduationDate": "2023-12-31T22:00:00.000Z",
                "qualificationFrom": {
                        "key": "4",
                        "name": "4"
                }       ,
                "qualification": {
                        "key": "masters",
                        "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                }       ,
                "specialization": "ECE",
                "universityName": "MUST"
               }
],
"applicationExperiences": [

],
"email": "vepapi2863@rehezb.com",
"country": "\u0623\u0646\u062f\u0648\u0631\u0627",
"countryKey": {
        "key": "key2",
        "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
},
"mobile": "+96611666",
"city": {
        "value": "",
        "disable": true
},
"fieldOfInterest": {
        "key": "facilitiesSecurityAndSafety",
        "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
},
"other": "",
"alreadyRegistered": true,
"cv": {
        "id": "116508"
},
"acceptance": true,
"reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=1DF9CB501E88924F4B1D937E108EFA01; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:02:49 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json
```

```
{

"status": "INTERNAL_SERVER_ER
...
...
...
```

Issue 17 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"applicationQualifications"[0]->"qualificationFrom"->"name" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEalliOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
```

```
sec-ch-ua-mobile: ?0
Content-Length: 1849
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
         "key": "residence",
         "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                         "key": "4",
                         "name": "       4XYZ"
                 }       ,
                 "qualification": {
                         "key": "masters",
                         "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
         "key": "key2",
         "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
         "value": "",
         "disable": true
 },
 "fieldOfInterest": {
         "key": "facilitiesSecurityAndSafety",
         "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
         "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
```

```
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=0E5E8163AF2F37D63369552E2BEE47FB; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:04:12 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERRO
...
...
...
```

Issue 18 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"applicationQualifications"[0]->"average" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEalliOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
```

```
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1847
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
        "key": "residence",
        "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average.": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                        "key": "4",
                        "name": "4"
                 }       ,
                 "qualification": {
                        "key": "masters",
                        "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
        "key": "key2",
        "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
        "value": "",
        "disable": true
 },
 "fieldOfInterest": {
        "key": "facilitiesSecurityAndSafety",
        "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
        "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
```

```
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=0426E6433AE174F59A9C8B911ED779AA; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:04:18 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Er
...
...
...
```

Issue 19 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"applicationQualifications"[0]->"qualification"->"key" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
```

```
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1847
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
        "key": "residence",
        "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                        "key": "4",
                        "name": "4"
                 }       ,
                 "qualification": {
                        "key.": "masters",
                        "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
        "key": "key2",
        "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
        "value": "",
        "disable": true
 },
 "fieldOfInterest": {
        "key": "facilitiesSecurityAndSafety",
        "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
```

```
        "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=FC29D952EA43E9E98E36D5023762459E; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:04:16 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Er
...
...
...
```

Issue 20 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"applicationQualifications"[0]->"qualificationFrom"->"key" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
```

```
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1845
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
        "key": "residence",
        "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                        "key": "",
                        "name": "4"
                 }       ,
                 "qualification": {
                        "key": "masters",
                        "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
        "key": "key2",
        "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
```

```
          "value": "",
          "disable": true
 },
 "fieldOfInterest": {
          "key": "facilitiesSecurityAndSafety",
          "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
          "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=9F87A9C9C7B33A922750B1C57004050A; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:05:11 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Erro
...
...
...
```


Issue 21 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"countryKey"->"key" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEalliOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1847
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
        "key": "residence",
        "name": "\u0625\u0642\u0627\u0645\u0629"
 },
```

```
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                         "key": "4",
                         "name": "4"
                 }       ,
                 "qualification": {
                         "key": "masters",
                         "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
         "key.": "key2",
         "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
         "value": "",
         "disable": true
 },
 "fieldOfInterest": {
         "key": "facilitiesSecurityAndSafety",
         "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
         "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=C4D57157B9070990ADE02D609E2BA200; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:05:30 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Er
...
...
...
```

Issue 22 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"other" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21lNTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEalliOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1847
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json
```

```
{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
        "key": "residence",
        "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                        "key": "4",
                        "name": "4"
                 }       ,
                 "qualification": {
                        "key": "masters",
                        "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
        "key": "key2",
        "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
        "value": "",
        "disable": true
 },
 "fieldOfInterest": {
        "key": "facilitiesSecurityAndSafety",
        "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other.": "",
 "alreadyRegistered": true,
 "cv": {
        "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}
```


```
HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=01FA80EAA8F238E389AF81C1B5B6B201; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:04:18 GMT
```

```
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Er
...
...
...
```

Issue 23 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"applicationQualifications"[0]->"qualification"->"name" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25Ecjlzbmxl ZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
```

```
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1847
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
        "key": "residence",
        "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                        "key": "4",
                        "name": "4"
                 }       ,
                 "qualification": {
                        "key": "masters",
                        "name.": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
        "key": "key2",
        "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
        "value": "",
        "disable": true
 },
 "fieldOfInterest": {
        "key": "facilitiesSecurityAndSafety",
        "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
        "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}
```

```
HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=8A3E67BF97E914164DE86449C291FCC2; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:04:22 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Er
...
...
...
```

Issue 24 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"fullNameArabic" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
```

```
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1847
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic.": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
        "key": "residence",
        "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                        "key": "4",
                        "name": "4"
                 }       ,
                 "qualification": {
                        "key": "masters",
                        "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
        "key": "key2",
        "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
        "value": "",
        "disable": true
 },
 "fieldOfInterest": {
        "key": "facilitiesSecurityAndSafety",
        "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
        "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
```

```
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=26AF188EEFA3380700273A54DAB0801D; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:04:24 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Er
...
...
...
```

Issue 25 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"acceptance" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
```

```
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEalliOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1847
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
        "key": "residence",
        "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                        "key": "4",
                        "name": "4"
                 }       ,
                 "qualification": {
                        "key": "masters",
                        "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
        "key": "key2",
        "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
        "value": "",
        "disable": true
 },
 "fieldOfInterest": {
        "key": "facilitiesSecurityAndSafety",
```

```
          "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
         "id": "116508"
 },
 "acceptance.": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=B8477CE30647AA75BF72C88390DD0A40; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:04:30 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Er
...
...
...
```


Issue 26 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"fieldOfInterest"->"name" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that

may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1847
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
         "key": "residence",
         "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                         "key": "4",
                         "name": "4"
                 }       ,
                 "qualification": {
                         "key": "masters",
                         "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
```

```
 "countryKey": {
        "key": "key2",
        "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
        "value": "",
        "disable": true
 },
 "fieldOfInterest": {
        "key": "facilitiesSecurityAndSafety",
        "name.": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
        "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=E0D69810980C16A8A17CDAABAE645DF1; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:04:30 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Er
...
...
...
```


Issue 27 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"mobile" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEalliOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1837
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
        "key": "residence",
        "name": "\u0625\u0642\u0627\u0645\u0629"
 },
```

```
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                         "key": "4",
                         "name": "4"
                 }       ,
                 "qualification": {
                         "key": "masters",
                         "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
         "key": "key2",
         "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "",
 "city": {
         "value": "",
         "disable": true
 },
 "fieldOfInterest": {
         "key": "facilitiesSecurityAndSafety",
         "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
         "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=4DF123F2135EDA45459E43B5C5B5B6EA; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:05:04 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Error"

}
```

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"applicationQualifications"[0]->"specialization" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEalliOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1847
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json
```

```
{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
        "key": "residence",
        "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                        "key": "4",
                        "name": "4"
                 }       ,
                 "qualification": {
                        "key": "masters",
                        "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization.": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
        "key": "key2",
        "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
        "value": "",
        "disable": true
 },
 "fieldOfInterest": {
        "key": "facilitiesSecurityAndSafety",
        "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
        "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}
```



```
HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=868D683BFE936F455E76556551CF8509; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:05:32 GMT
Access-Control-Allow-Methods: *
```

```
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Er
...
...
...
```

Issue 29 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"email" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
```

```
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1847
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
         "key": "residence",
         "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                         "key": "4",
                         "name": "4"
                 }       ,
                 "qualification": {
                         "key": "masters",
                         "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email.": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
         "key": "key2",
         "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
         "value": "",
         "disable": true
 },
 "fieldOfInterest": {
         "key": "facilitiesSecurityAndSafety",
         "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
         "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}
```

```
HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=F4EC73DC8711F485A3788B056D0343EB; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:05:13 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Er
...
...
...
```

Issue 30 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"identityType"->"name" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
```

```
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1822
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
         "key": "residence",
         "name": "\u0000"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                         "key": "4",
                         "name": "4"
                 }       ,
                 "qualification": {
                         "key": "masters",
                         "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
         "key": "key2",
         "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
         "value": "",
         "disable": true
 },
 "fieldOfInterest": {
         "key": "facilitiesSecurityAndSafety",
         "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
         "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
```

```
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=E48FDBFC904D81AF0EFBE8C01AA16A5A; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:05:25 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Error"

}
```

Issue 31 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"fullNameEnglish" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
```

```
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1847
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish.": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
         "key": "residence",
         "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                         "key": "4",
                         "name": "4"
                 }       ,
                 "qualification": {
                         "key": "masters",
                         "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
         "key": "key2",
         "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
         "value": "",
         "disable": true
 },
 "fieldOfInterest": {
         "key": "facilitiesSecurityAndSafety",
         "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
```

```
  },
  "other": "",
  "alreadyRegistered": true,
  "cv": {
          "id": "116508"
  },
  "acceptance": true,
  "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=A24EAF164C5A46B2D69B079B49F4E33D; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:05:44 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Er
...
...
...
```


Issue 32 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"country" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEalliOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1810
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
        "key": "residence",
        "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                        "key": "4",
                        "name": "4"
                 }       ,
                 "qualification": {
                        "key": "masters",
                        "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "",
 "countryKey": {
        "key": "key2",
```

```
        "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
        "value": "",
        "disable": true
 },
 "fieldOfInterest": {
        "key": "facilitiesSecurityAndSafety",
        "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
        "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=51052D41240BF6908B5200A1FC204291; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:05:44 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Error"

}
```


Issue 33 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"cv"->"id" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEalliOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1849
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
        "key": "residence",
        "name": "\u0625\u0642\u0627\u0645\u0629"
 },
```

```
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                         "key": "4",
                         "name": "4"
                 }       ,
                 "qualification": {
                         "key": "masters",
                         "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
         "key": "key2",
         "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
         "value": "",
         "disable": true
 },
 "fieldOfInterest": {
         "key": "facilitiesSecurityAndSafety",
         "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
         "id": "       116508XYZ"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=CBF3AA180E4A5A650F3ABC18F965F991; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:05:51 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERRO
...
...
...
```

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"city"->"disable" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEalliOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1847
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
```

```
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
         "key": "residence",
         "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                         "key": "4",
                         "name": "4"
                 }       ,
                 "qualification": {
                         "key": "masters",
                         "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
         "key": "key2",
         "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
         "value": "",
         "disable.": true
 },
 "fieldOfInterest": {
         "key": "facilitiesSecurityAndSafety",
         "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
         "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=65E3AABAD6600E3B98F9C6D4A4A09F7A; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:07:39 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json
```

```
{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Er
...
...
...
```

Issue 35 of 35

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"city"->"value" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRUZBQU9DQVE4QU1JSUJDZ0tDQVFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEalliOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
```

```
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1847
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
        "key": "residence",
        "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                        "key": "4",
                        "name": "4"
                 }       ,
                 "qualification": {
                        "key": "masters",
                        "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
        "key": "key2",
        "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
        "value.": "",
        "disable": true
 },
 "fieldOfInterest": {
        "key": "facilitiesSecurityAndSafety",
        "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
        "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
```

```
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=B91CA906C04E39AF234AD1891506460A; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:05:53 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SERVER_ERROR",

"title": "Internal Server Er
...
...
...
```

I Application Test Script Detected 1 TOC

Issue 1 of 1 TOC

Application Test Script Detected

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/web/
Entity:	test (Page)
Risk:	It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords
Causes:	Temporary files were left in production environment
Fix:	Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Requests and Responses:

```
GET /web/test?
p_p_id=com_liferay_login_web_portlet_LoginPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=vi
ew&_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName=%2Flogin%2Flogin&saveLastPath
=false HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/c/portal/login?p_l_id=129
Cookie: COOKIE_SUPPORT=true; GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: Keep-Alive
Host: mcit-liferayqc.linkdev.com
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Liferay-Portal: Liferay Digital Experience Platform
X-Content-Type-Options: nosniff
...
...
...

<script data-senna-track="permanent" src="/combo?
browserId=chrome&minifierType=js&languageId=ar_SA&t=1715103903840&/o/frontend-js-jquery-
web/jquery/jquery.min.js&/o/frontend-js-jquery-web/jquery/init.js&/o/frontend-js-jquery-
web/jquery/ajax.js&/o/frontend-js-jquery-web/jquery/bootstrap.bundle.min.js&/o/frontend-js-
jquery-web/jquery/collapsible_search.js&/o/frontend-js-jquery-web/jquery/fm.js&/o/frontend-js-
jquery-web/jquery/form.js&/o/frontend-js-jquery-web/jquery/popper.min.js&/o/frontend-js-jquery-
web/jquery/side_navigation.js" type="text/javascript"></script>
<script data-senna-track="permanent" type="text/javascript">window.Liferay = window.Liferay ||
{}; window.Liferay.CSP = {nonce: ''};</script>
<link data-senna-track="temporary" href="https://mcit-liferayqc.linkdev.com/web/test"
rel="canonical" />
<link data-senna-track="temporary" href="https://mcit-liferayqc.linkdev.com/web/test"
hreflang="ar-SA" rel="alternate" />
<link data-senna-track="temporary" href="https://mcit-liferayqc.linkdev.com/en/web/test"
hreflang="en-US" rel="alternate" />
<link data-senna-track="temporary" href="https://mcit-liferayqc.linkdev.com/web/test"
hreflang="x-default" rel="alternate" />

<meta property="og:locale" content="ar_SA">
<meta property="og:locale:alternate" content="ar_SA">
<meta property="og:locale:alternate" content="en_US">
<meta property="og:site_name" content="Admin Ar Admin En">
<meta property="og:title" content="My Profile - Admin Ar Admin En - Ministry of Communications
and Information Technology">
<meta property="og:type" content="website">
<meta property="og:url" content="https://mcit-liferayqc.linkdev.com/web/test">
...
...
...
        Liferay.Browser = {
                acceptsGzip:        function() {
                        return false;
                }       ,
...
...
...
                getMajorVersion:        function() {
                        return 124.0;
                }       ,
...
...
...
                getRevision:        function() {
                        return '537.36';
                }       ,
                getVersion:        function() {
                        return '124.0';
                }       ,
...
...
...
                isAir:        function() {
                        return false;
                }       ,
                isChrome:        function() {
                        return true;
                }       ,
                isEdge:        function() {
                        return false;
                }       ,
                isFirefox:        function() {
                        return false;
                }       ,
                isGecko:        function() {
                        return true;
```

```
                }       ,
                isIe:           function() {
                        return false;
                }       ,
                isIphone:         function() {
                        return false;
                }       ,
                isLinux:         function() {
                        return false;
                }       ,
                isMac:          function() {
                        return false;
                }       ,
                isMobile:         function() {
                        return false;
                }       ,
                isMozilla:          function() {
                        return false;
                }       ,
                isOpera:         function() {
                        return false;
                }       ,
                isRtf:          function() {
                        return true;
                }       ,
                isSafari:         function() {
                        return true;
                }       ,
                isSun:          function() {
                        return false;
                }       ,
                isWebKit:         function() {
                        return true;
                }       ,
                isWindows:          function() {
                        return true;
                       }
        }       ;
...
...
...
        Liferay.Data.isCustomizationView =          function() {
                return false;
        }       ;
...
...
...
               (function () {
                var available = {};
...
...
...
                Liferay.Language = {
                        available,
                        direction,
                        get:          function(key) {
                                return key;
                               }
                }       ;
        })();
...
...
...

                        getLayoutId:          function() {
                                return '1';
                        }       ,
...
...
...
                        getLayoutRelativeControlPanelURL:          function() {
                                return '/user/       test/~/control_panel/manage?
p_p_id=com_liferay_login_web_portlet_LoginPortlet';
                        }       ,
...
...
...
                        getLayoutRelativeURL:          function() {
```

```
                                return '/web/       test/home';
                        }       ,
                        getLayoutURL:        function() {
                                return 'https://mcit-
liferayqc.linkdev.com/web/test/home';
                        }       ,
                        getParentLayoutId:        function() {
                                return '0';
                        }       ,
                        isControlPanel:        function() {
                                return false;
                        }       ,
                        isPrivateLayout:        function() {
                                return 'false';
                        }       ,
                        isVirtualLayout:        function() {
                                return false;
                        }       ,

...
...
...
                getBCP47LanguageId:        function() {
                        return 'ar-SA';
                }       ,
                getCanonicalURL:        function() {
...
...
...
                        return 'https\x3a\x2f\x2fmcit-
liferayqc\x2elinkdev\x2ecom\x2fweb\x2ftest';
                }       ,
                getCDNBaseURL:        function() {
                        return 'https://mcit-liferayqc.linkdev.com';
                }       ,
                getCDNDynamicResourcesHost:        function() {
                        return '';
                }       ,
                getCDNHost:        function() {
                        return '';
                }       ,
                getCompanyGroupId:        function() {
                        return '20121';
                }       ,
                getCompanyId:        function() {
                        return '20096';
                }       ,
                getDefaultLanguageId:        function() {
                        return 'ar_SA';
                }       ,
                getDoAsUserIdEncoded:        function() {
                        return '';
                }       ,
                getLanguageId:        function() {
                        return 'ar_SA';
                }       ,
                getParentGroupId:        function() {
                        return '20125';
                }       ,
                getPathContext:        function() {
                        return '';
                }       ,
                getPathImage:        function() {
                        return '/image';
                }       ,
                getPathJavaScript:        function() {
                        return '/o/frontend-js-web';
                }       ,
                getPathMain:        function() {
                        return '/c';
                }       ,
                getPathThemeImages:        function() {
                        return 'https://mcit-liferayqc.linkdev.com/o/classic-
theme/images';
                }       ,
                getPathThemeRoot:        function() {
                        return '/o/classic-theme';
                }       ,
```

```
                getPlid:        function() {
                        return '13';
                }       ,
                getPortalURL:       function() {
                        return 'https://mcit-liferayqc.linkdev.com';
                }       ,
                getRealUserId:        function() {
                        return '20099';
                }       ,
                getRemoteAddr:        function() {
                        return '10.100.30.154';
                }       ,
                getRemoteHost:        function() {
                        return '10.100.30.154';
                }       ,
                getScopeGroupId:        function() {
                        return '20125';
                }       ,
                getScopeGroupIdOrLiveGroupId:        function() {
                        return '20125';
                }       ,
                getSessionId:       function() {
                        return '';
                }       ,
                getSiteAdminURL:        function() {
                        return 'https://mcit-
liferayqc.linkdev.com/group/test/~/control_panel/manage?
p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view';
                }       ,
                getSiteGroupId:        function() {
                        return '20125';
                }       ,
                getURLControlPanel:       function() {
                        return '/group/control_panel?refererPlid=13';
                }       ,
                getURLHome:       function() {
                        return 'https\x3a\x2f\x2fmcit-
liferayqc\x2elinkdev\x2ecom\x2fhome';
                }       ,
                getUserEmailAddress:        function() {
                        return '';
                }       ,
                getUserId:        function() {
                        return '20099';
                }       ,
                getUserName:        function() {
                        return '';
                }       ,
                isAddSessionIdToURL:        function() {
                        return false;
                }       ,
                isImpersonated:       function() {
                        return false;
                }       ,
                isSignedIn:       function() {
                        return false;
                }       ,
...
...
...
                isStagedPortlet:        function() {


                                        return true;

...
...
...

                isStateExclusive:        function() {
                        return false;
                }       ,
                isStateMaximized:        function() {
                        return true;
                }       ,
                isStatePopUp:       function() {
                        return false;
                       }
```

```
        }       ;
...
...
...
                getCombine:         function() {
                        return true;
                }       ,
                getComboPath:         function() {
                        return '/combo/?
browserId=chrome&minifierType=&languageId=ar_SA&t=1713966024674&';
                }       ,
                getDateFormat:         function() {
                        return '%d/%m/%Y';
                }       ,
                getEditorCKEditorPath:         function() {
                        return '/o/frontend-editor-ckeditor-web';
                }       ,
                getFilter:         function() {
                        var filter = 'raw';
...
...
...
                        return filter;
                }       ,
                getFilterConfig:         function() {
                        var instance = this;
...
...
...
                        return filterConfig;
                }       ,
                getJavaScriptRootPath:         function() {
                        return '/o/frontend-js-web';
                }       ,
                getPortletRootPath:         function() {
                        return '/html/portlet';
                }       ,
                getStaticResourceURLParams:         function() {
                        return '?
browserId=chrome&minifierType=&languageId=ar_SA&t=1713966024674';
                       }
        }       ;
...
...
...
        Liferay.currentURL =
'\x2fweb\x2ftest\x3fp_p_id\x3dcom_liferay_login_web_portlet_LoginPortlet\x26p_p_lifecycle\x3d0\x2
6p_p_state\x3dmaximized\x26p_p_mode\x3dview\x26_com_liferay_login_web_portlet_LoginPortlet_mvcRen
derCommandName\x3d\x252Flogin\x252Flogin\x26saveLastPath\x3dfalse';
        Liferay.currentURLEncoded =
'\x252Fweb\x252Ftest\x253Fp_p_id\x253Dcom_liferay_login_web_portlet_LoginPortlet\x2526p_p_lifecyc
le\x253D0\x2526p_p_state\x253Dmaximized\x2526p_p_mode\x253Dview\x2526_com_liferay_login_web_portl
et_LoginPortlet_mvcRenderCommandName\x253D\x25252Flogin\x25252Flogin\x2526saveLastPath\x253Dfalse
';
 // ]]>
</script>
...
...
...attribute-observable/attribute-observable-min.js&/o/frontend-js-aui-web/aui/attribute-
extras/attribute-extras-min.js&/o/frontend-js-aui-web/aui/event-custom-base/event-custom-base-
min.js&/o/frontend-js-aui-web/aui/event-custom-complex/event-custom-complex-min.js&/o/frontend-
js-aui-web/aui/oop/oop-min.js&/o/frontend-js-aui-web/aui/aui-base-lang/aui-base-lang-
min.js&/o/frontend-js-aui-web/liferay/dependency.js&/o/frontend-js-aui-
web/liferay/util.js&/o/oauth2-provider-web/js/liferay.js&/o/frontend-js-
web/liferay/dom_task_runner.js&/o/frontend-js-web/liferay/events.js&/o/frontend-js-
web/liferay/lazy_load.js&/o/frontend-js-web/liferay/liferay.js&/o/frontend-js-
web/liferay/global.bundle.js&/o/frontend-js-web/liferay/portlet.js&/o/frontend-js-
web/liferay/workflow.js" type="text/javascript"></script>
<script data-senna-track="temporary" type="text/javascript">window.Liferay = Liferay || {};
window.Liferay.OAuth2 = {getAuthorizeURL: function() {return 'https://mcit-
liferayqc.linkdev.com/o/oauth2/authorize';}, getBuiltInRedirectURL: function() {return
'https://mcit-liferayqc.linkdev.com/o/oauth2/redirect';}, getIntrospectURL: function() { return
'https://mcit-liferayqc.linkdev.com/o/oauth2/introspect';}, getTokenURL: function() {return
'https://mcit-liferayqc.linkdev.com/o/oauth2/token';}, getUserAgentApplication:
function(externalReferenceCode) {return
Liferay.OAuth2._userAgentApplications[externalReferenceCode];}, _userAgentApplications: {}}
</script><script data-senna-track="temporary" type="text/javascript">try {var
MODULE_MAIN='staging-taglib@8.0.2/index';var MODULE_PATH='/o/staging-
```

```
taglib';AUI().applyConfig({groups:{stagingTaglib:
{base:MODULE_PATH+"/",combine:Liferay.AUI.getCombine(),filter:Liferay.AUI.getFilterConfig(),modul
es:{"liferay-export-import-management-bar-button":
{path:"export_import_entity_management_bar_button/js/main.js",requires:["aui-component","liferay-
search-container","liferay-search-container-select"]}},root:MODULE_PATH+"/"}}});
} catch(error) {console.error(error);}try {var MODULE_MAIN='staging-processes-
web@5.0.54/index';var MODULE_PATH='/o/staging-processes-web';AUI().applyConfig({groups:
{stagingprocessesweb:{base:MODULE_P
...
...
...
base","timers"]},"liferay-alloy-editor-source":{path:"alloyeditor_source.js",requires:["aui-
debounce","liferay-fullscreen-source-editor","liferay-source-
editor","plugin"]}},root:MODULE_PATH+"/js/"}});
} catch(error) {console.error(error);}try {var MODULE_MAIN='exportimport-web@5.0.81/index';var
MODULE_PATH='/o/exportimport-web';AUI().applyConfig({groups:{exportimportweb:
{base:MODULE_PATH+"/",combine:Liferay.AUI.getCombine(),filter:Liferay.AUI.getFilterConfig(),modul
es:{"liferay-export-import-export-import":{path:"js/main.js",requires:["aui-datatype","aui-
dialog-iframe-deprecated","aui-modal","aui-parse-content","aui-toggler","liferay-portlet-
base","liferay-util-window"]}},root:MODULE_PATH+"/"}});
} catch(error) {console.error(error);}try {var MODULE_MAIN='dynamic-data-mapping-
web@5.0.97/index';var MODULE_PATH='/o/dynamic-data-mapping-web';!function(){const
a=Liferay.AUI;AUI().applyConfig({groups:{ddm:
{base:MODULE_PATH+"/js/",combine:Liferay.AUI.getCombine(),filter:a.getFilterConfig(),modules:
{"liferay-ddm-form":{path:"ddm_form.js",requires:["aui-base","aui-datatable","aui-datatype","aui-
image-viewer","aui-parse-content","aui-set","aui-sortable-list","json","liferay-form","liferay-
map-base","liferay-translation-manager","liferay-util-window"]},"liferay-portlet-dynamic-data-
mapping":{condition:{trigger:"liferay-document-library"},path:"main.js",requires:
["arraysort","aui-form-builder-deprecated","aui-form-validator","aui-map","aui-text-
unicode","json","liferay-menu","liferay-translation-manager","liferay-util-
window","text"]},"liferay-portlet-dynamic-data-mapping-custom-fields":{condition:
{trigger:"liferay-document-library"},path:"custom_fields.js",requires:["liferay-portlet-dynamic-
data-mapping"]}},root:MODULE_PATH+"/js/"}})}();
...
...
...

</style>
<script>
Liferay.Loader.require(
'@liferay/frontend-js-state-web@1.0.19',
function(FrontendJsState) {
try {
} catch (err) {
 console.error(err);
}
...
...
...

</script><script>
Liferay.Loader.require(
'frontend-js-spa-web@5.0.44/init',
function(frontendJsSpaWebInit) {
try {
(function() {
frontendJsSpaWebInit.default({"navigationExceptionSelectors":":not([target=\"_blank\"]):not([data
-senna-off]):not([data-resource-href]):not([data-cke-saved-href]):not([data-cke-saved-
href])","cacheExpirationTime":-1,"clearScreensCache":false,"portletsBlacklist":
["com_liferay_nested_portlets_web_portlet_NestedPortletsPortlet","com_liferay_site_navigation_dir
ectory_web_portlet_SitesDirectoryPortlet","com_liferay_questions_web_internal_portlet_QuestionsPo
rtlet","com_liferay_account_admin_web_internal_portlet_AccountUsersRegistrationPortlet","com_life
ray_portal_language_override_web_internal_portlet_PLOPortlet","com_liferay_login_web_portlet_Logi
nPortlet","com_liferay_login_web_portlet_FastLoginPortlet"],"excludedTargetPortlets":
["com_liferay_users_admin_web_portlet_UsersAdminPortlet","com_lifera
...
...
...

<script type="text/javascript">
Liferay.on(
 'ddmFieldBlur',        function(event) {
        if (window.Analytics) {
                Analytics.send(
                        'fieldBlurred',
                        'Form',
...
...
```

```
...

Liferay.on(
 'ddmFieldFocus',        function(event) {
        if (window.Analytics) {
                Analytics.send(
                        'fieldFocused',
                        'Form',
...
...
...

Liferay.on(
 'ddmFormPageShow',        function(event) {
        if (window.Analytics) {
                Analytics.send(
                        'pageViewed',
                        'Form',
...
...
...

Liferay.on(
 'ddmFormSubmit',        function(event) {
        if (window.Analytics) {
                Analytics.send(
                        'formSubmitted',
                        'Form',
...
...
...

Liferay.on(
 'ddmFormView',        function(event) {
        if (window.Analytics) {
                Analytics.send(
                        'formViewed',
                        'Form',
...
...
...

                <header id="banner">
                        <div class="navbar navbar-classic navbar-top py-3">
                                <div class="container-fluid container-fluid-max-xl user-
personal-bar">
                                        <div class="align-items-center autofit-row">
                                                <a class="logo custom-logo align-items-
center d-md-inline-flex d-sm-none d-none logo-md" href="https://mcit-
liferayqc.linkdev.com/web/test" title="إلى انتقال Admin Ar Admin En">
                                                <img alt="" class="mr-2" height="56"
src="/image/company_logo?img_id=108768&amp;t=1715103867656" />
...
...
...
                        <div class="navbar navbar-classic navbar-expand-md navbar-light
pb-3">
                                <div class="container-fluid container-fluid-max-xl">
                                        <a class="logo custom-logo align-items-center d-
inline-flex d-md-none logo-xs" href="https://mcit-liferayqc.linkdev.com/web/test" rel="nofollow">
                                                <img alt="" class="mr-2" height="56"
src="/image/company_logo?img_id=108768&amp;t=1715103867656" />
...
...
...
                                <li class="lfr-nav-item nav-item selected active"
id="layout_com_liferay_site_navigation_menu_web_portlet_SiteNavigationMenuPortlet_1"
role="presentation">
                                        <a  class="nav-link text-truncate"
href='https://mcit-liferayqc.linkdev.com/web/test/home'  role="menuitem">
                                                <span class="text-truncate"> My Profile
</span>
                                        </a       >
...
...
...
<script>
AUI().use(
```

```
  'liferay-navigation-interaction',
function(A) {
(function() {
var $ = AUI.$;var _ = AUI._;            var navigation =
A.one('#navbar_com_liferay_site_navigation_menu_web_portlet_SiteNavigationMenuPortlet');
...
...
...
                <div class="autofit-float autofit-row portlet-header">
                                <div class="autofit-col">
                                        <div class="autofit-section">
                                                <a class="icon-monospaced portlet-icon-
back text-default" href="https://mcit-liferayqc.linkdev.com/web/test/home?
p_p_id=com_liferay_login_web_portlet_LoginPortlet&amp;p_p_lifecycle=1&amp;p_p_state=normal&amp;p_
p_state_rcv=1&amp;p_auth=He2Dg8EQ" title="العودة للصفحة الكاملة">
...
...
...
<form action="https://mcit-liferayqc.linkdev.com/web/test/home?
p_p_id=com_liferay_login_web_portlet_LoginPortlet&amp;p_p_lifecycle=1&amp;p_p_state=maximized&amp
;p_p_mode=view&amp;_com_liferay_login_web_portlet_LoginPortlet_javax.portlet.action=%2Flogin%2Flo
gin&amp;_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName=%2Flogin%2Flogin&amp;p_a
uth=He2Dg8EQ" class="form sign-in-form w-100 " data-fm-
namespace="_com_liferay_login_web_portlet_LoginPortlet_"
id="_com_liferay_login_web_portlet_LoginPortlet_loginForm" method="post"
name="_com_liferay_login_web_portlet_LoginPortlet_loginForm" autocomplete="on" >

...
...
...

        Liferay.currentURL =
'\x2fweb\x2ftest\x3fp_p_id\x3dcom_liferay_login_web_portlet_LoginPortlet\x26p_p_lifecycle\x3d0\x2
6p_p_state\x3dmaximized\x26p_p_mode\x3dview\x26_com_liferay_login_web_portlet_LoginPortlet_mvcRen
derCommandName\x3d\x252Flogin\x252Flogin\x26saveLastPath\x3dfalse';
        Liferay.currentURLEncoded =
'\x252Fweb\x252Ftest\x253Fp_p_id\x253Dcom_liferay_login_web_portlet_LoginPortlet\x2526p_p_lifecyc
le\x253D0\x2526p_p_state\x253Dmaximized\x2526p_p_mode\x253Dview\x2526_com_liferay_login_web_portl
et_LoginPortlet_mvcRenderCommandName\x253D\x25252Flogin\x25252Flogin\x2526saveLastPath\x253Dfalse
';
...
...
...
<script type="text/javascript">
(function() {var $ = AUI.$;var _ = AUI._;
 var onDestroyPortlet =        function () {
        Liferay.detach('messagePosted', onMessagePosted);
        Liferay.detach('destroyPortlet', onDestroyPortlet);
 };
...
...
...
 var onMessagePosted =        function (event) {
        if (window.Analytics) {
                const eventProperties = {
                        className: event.className,
                        classPK: event.classPK,
                                commentId: event.commentId,
                        text: event.text,
                }       ;
...
...
...
                Analytics.send('posted', '       Comment', eventProperties);
               }
 };
...
...
...
        function getValueByAttribute(node, attr) {
         return (
                node.dataset[attr] ||
                (node.parentElement && node.parentElement.dataset[attr])
         )       ;
...
...
...
```

```
        function sendAnalyticsEvent(anchor) {
         var fileEntryId = getValueByAttribute(anchor, 'analyticsFileEntryId');
         var title = getValueByAttribute(anchor, 'analyticsFileEntryTitle');
         var version = getValueByAttribute(anchor, 'analyticsFileEntryVersion');
...
...
...
        function handleDownloadClick(event) {
         if (window.Analytics) {
                if (event.target.nodeName.toLowerCase() === 'a') {
                        sendAnalyticsEvent(event.target);
                       }
...
...
...

(function() {var $ = AUI.$;var _ = AUI._;
 var onVote =        function (event) {
         if (window.Analytics) {
                let title = event.contentTitle;
...
...
...
 var onDestroyPortlet =        function () {
         Liferay.detach('ratings:vote', onVote);
         Liferay.detach('destroyPortlet', onDestroyPortlet);
 };
...
...
...
 Liferay.on('ratings:vote', onVote);
 Liferay.on('destroyPortlet', onDestroyPortlet);
})();
(function() {var $ = AUI.$;var _ = AUI._;
 var onShare =        function (data) {
         if (window.Analytics) {
                Analytics.send('shared', 'SocialBookmarks', {
                        className: data.className,
                        classPK: data.classPK,
...
...
...

 var onDestroyPortlet =        function () {
         Liferay.detach('socialBookmarks:share', onShare);
         Liferay.detach('destroyPortlet', onDestroyPortlet);
 };
...
...
...
 if (window.svg4everybody && Liferay.Data.ICONS_INLINE_SVG) {
         svg4everybody(
                       {
                        polyfill: true,
                        validate:        function (src, svg, use) {
                                return !src || !src.startsWith('#');
                               }
                       }
         )       ;
...
...
...

(function() {var $ = AUI.$;var _ = AUI._;
                var form =
document.getElementById('_com_liferay_login_web_portlet_LoginPortlet_loginForm');

                if (form) {
                        form.addEventListener('submit', (event) => {
...
...
...

                isStatic: 'end',
                namespacedId: 'p_p_id_com_liferay_login_web_portlet_LoginPortlet_',
                portletId: 'com_liferay_login_web_portlet_LoginPortlet',
                refreshURL:
'\x2fc\x2fportal\x2frender_portlet\x3fp_l_id\x3d13\x26p_p_id\x3dcom_liferay_login_web_portlet_Log
```

```
inPortlet\x26p_p_lifecycle\x3d0\x26p_t_lifecycle\x3d0\x26p_p_state\x3dmaximized\x26p_p_mode\x3dvi
ew\x26p_p_col_id\x3dnull\x26p_p_col_pos\x3dnull\x26p_p_col_count\x3dnull\x26p_p_isolated\x3d1\x26
currentURL\x3d\x252Fweb\x252Ftest\x253Fp_p_id\x253Dcom_liferay_login_web_portlet_LoginPortlet\x25
26p_p_lifecycle\x253D0\x2526p_p_state\x253Dmaximized\x2526p_p_mode\x253Dview\x2526_com_liferay_lo
gin_web_portlet_LoginPortlet_mvcRenderCommandName\x253D\x25252Flogin\x25252Flogin\x2526saveLastPa
th\x253Dfalse',
                refreshURLData:
{"_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName":["\/login\/login"]}
              }
 );
...
...
...
                namespacedId:
'p_p_id_com_liferay_product_navigation_user_personal_bar_web_portlet_ProductNavigationUserPersona
lBarPortlet_',
                portletId:
'com_liferay_product_navigation_user_personal_bar_web_portlet_ProductNavigationUserPersonalBarPor
tlet',
                refreshURL:
'\x2fc\x2fportal\x2frender_portlet\x3fp_l_id\x3d13\x26p_p_id\x3dcom_liferay_product_navigation_us
er_personal_bar_web_portlet_ProductNavigationUserPersonalBarPortlet\x26p_p_lifecycle\x3d0\x26p_t_
lifecycle\x3d0\x26p_p_state\x3dnormal\x26p_p_mode\x3dview\x26p_p_col_id\x3dnull\x26p_p_col_pos\x3
dnull\x26p_p_col_count\x3dnull\x26p_p_static\x3d1\x26p_p_isolated\x3d1\x26currentURL\x3d\x252Fweb
\x252Ftest\x253Fp_p_id\x253Dcom_liferay_login_web_portlet_LoginPortlet\x2526p_p_lifecycle\x253D0\
x2526p_p_state\x253Dmaximized\x2526p_p_mode\x253Dview\x2526_com_liferay_login_web_portlet_LoginPo
rtlet_mvcRenderCommandName\x253D\x25252Flogin\x25252Flogin\x2526saveLastPath\x253Dfalse',
                refreshURLData: {}
              }
 );
...
...
...
                isStatic: 'end',
                namespacedId:
'p_p_id_com_liferay_portal_search_web_search_bar_portlet_SearchBarPortlet_INSTANCE_templateSearch
_',
                portletId:
'com_liferay_portal_search_web_search_bar_portlet_SearchBarPortlet_INSTANCE_templateSearch',
                refreshURL:
'\x2fc\x2fportal\x2frender_portlet\x3fp_l_id\x3d13\x26p_p_id\x3dcom_liferay_portal_search_web_sea
rch_bar_portlet_SearchBarPortlet_INSTANCE_templateSearch\x26p_p_lifecycle\x3d0\x26p_t_lifecycle\x
3d0\x26p_p_state\x3dnormal\x26p_p_mode\x3dview\x26p_p_col_id\x3dnull\x26p_p_col_pos\x3dnull\x26p_
p_col_count\x3dnull\x26p_p_static\x3d1\x26p_p_isolated\x3d1\x26currentURL\x3d\x252Fweb\x252Ftest\
x253Fp_p_id\x253Dcom_liferay_login_web_portlet_LoginPortlet\x2526p_p_lifecycle\x253D0\x2526p_p_st
ate\x253Dmaximized\x2526p_p_mode\x253Dview\x2526_com_liferay_login_web_portlet_LoginPortlet_mvcRe
nderCommandName\x253D\x25252Flogin\x25252Flogin\x2526saveLastPath\x253Dfalse',
                refreshURLData: {}
              }
 );
...
...
...
                isStatic: 'end',
                namespacedId:
'p_p_id_com_liferay_site_navigation_menu_web_portlet_SiteNavigationMenuPortlet_',
                portletId:
'com_liferay_site_navigation_menu_web_portlet_SiteNavigationMenuPortlet',
                refreshURL:
'\x2fc\x2fportal\x2frender_portlet\x3fp_l_id\x3d13\x26p_p_id\x3dcom_liferay_site_navigation_menu_
web_portlet_SiteNavigationMenuPortlet\x26p_p_lifecycle\x3d0\x26p_t_lifecycle\x3d0\x26p_p_state\x3
dnormal\x26p_p_mode\x3dview\x26p_p_col_id\x3dnull\x26p_p_col_pos\x3dnull\x26p_p_col_count\x3dnull
\x26p_p_static\x3d1\x26p_p_isolated\x3d1\x26currentURL\x3d\x252Fweb\x252Ftest\x253Fp_p_id\x253Dco
m_liferay_login_web_portlet_LoginPortlet\x2526p_p_lifecycle\x253D0\x2526p_p_state\x253Dmaximized\
x2526p_p_mode\x253Dview\x2526_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName\x25
3D\x25252Flogin\x25252Flogin\x2526saveLastPath\x253Dfalse',
                refreshURLData: {}
              }
 );
...
...
...
</script><script>
Liferay.Loader.require(
'layout-taglib@16.1.4/render_layout_structure/js/InfoItemActionHandler',
'frontend-js-web/index',
function(InfoItemActionHandler, frontendJsWeb) {
try {
```

```
AUI().use(
  'liferay-menu',
  'liferay-form',
function(A) {
(function() {
Liferay.component('infoItemActionComponent', new
InfoItemActionHandler.default({"executeInfoItemActionURL":"https:\/\/mcit-
liferayqc.linkdev.com\/c\/portal\/execute_info_item_action?
p_l_mode=view&plid=13","namespace":"","spritemap":"https:\/\/mcit-
liferayqc.linkdev.com\/o\/classic-theme\/images\/clay\/icons.svg"}), { destroyOnNavigate: true,
portletId: ''});
})();
(function() {
var $ = AUI.$;var _ = AUI._;
 var {delegate} = frontendJsWeb;
...
...
...
 delegate(
         document,
         'focusin',
         '.portlet',
                function(event) {
                 event.delegateTarget.closest('.portlet').classList.add('open');
                }
 );
...
...
...
 delegate(
         document,
         'focusout',
         '.portlet',
                function(event) {
                 event.delegateTarget.closest('.portlet').classList.remove('open');
                }
 );
})();
(function() {
var $ = AUI.$;var _ = AUI._;
 new Liferay.Menu();
...
...
...
})();
(function() {
var $ = AUI.$;var _ = AUI._;
         var {openToast} = frontendJsWeb;
...
...
...
         AUI().use(
                 'liferay-session',
                        function() {
                         Liferay.Session = new Liferay.SessionBase(
                                        {
                                         autoExtend: true,
                                         redirectOnExpire: false,
...
...
...

                        }
         )       ;

})();
(function() {
var $ = AUI.$;var _ = AUI._;
 Liferay.Form.register(
                {
                 id: '_com_liferay_login_web_portlet_LoginPortlet_loginForm'
...
...
...

                         , onSubmit:        function(event) {
                                 event.preventDefault();
                                }
```

```
...
...
...
 var onDestroyPortlet =        function(event) {
         if (event.portletId === 'com_liferay_login_web_portlet_LoginPortlet') {
                 delete
Liferay.Form._INSTANCES['_com_liferay_login_web_portlet_LoginPortlet_loginForm'];
                }
 };
...
...
...
<script>
Liferay.Loader.require(
'frontend-js-tooltip-support-web@4.0.23/index',
function(TooltipSupport) {
try {
(function() {
TooltipSupport.default()
})();
} catch (err) {
 console.error(err);
...
...
...

</script><script>
Liferay.Loader.require(
'frontend-js-dropdown-support-web@2.0.14/index',
function(DropdownProvider) {
try {
(function() {
DropdownProvider.default()
})();
} catch (err) {
 console.error(err);
...
...
...

</script><script>
Liferay.Loader.require(
'frontend-js-tabs-support-web@2.0.15/index',
function(TabsProvider) {
try {
(function() {
TabsProvider.default()
})();
} catch (err) {
 console.error(err);
...
...
...

</script><script>
Liferay.Loader.require(
'frontend-js-alert-support-web@2.0.13/index',
function(AlertProvider) {
try {
(function() {
AlertProvider.default()
})();
} catch (err) {
 console.error(err);
...
...
...

</script><script>
Liferay.Loader.require(
'frontend-js-collapse-support-web@2.0.18/index',
function(CollapseProvider) {
try {
(function() {
CollapseProvider.default()
})();
} catch (err) {
```

```
 console.error(err);
...
...
...
```

I Email Address Pattern Found 1

TOC

Issue 1 of 1

TOC

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplicationtypes
Entity:	recruitmentapplicationtypes (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Reasoning: The response contains an e-mail address that may be private.

Test Requests and Responses:

```
GET /o/c/recruitmentapplicationtypes?restrictFields=creator,actions&pageSize=100000 HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
LFR_SESSION_STATE_116486=1715073208993; _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
LFR_SESSION_STATE_20099=1715073020896; _ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0;
_ga=GA1.1.128297136.1599395143; _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
```

```
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty


HTTP/1.1 200
Connection: keep-alive
Content-Length: 1480
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: no-cache, no-store
Set-Cookie: JSESSIONID=0BA931A9B3CBE2D68B4F16D2A19DFEBB; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 09:57:33 GMT
Content-Type: application/json

{

"actions": {

 },

"facets": [

 ],

"items": [
                {

"dateCreated": "2024-04-02T09:17:23Z",

"dateModified": "2024-04-02T09:17:45Z",

"externalReferenceCode": "c84d9da4-0962-c1fe-d44a-0aeb28fa6523",

"id": 89317,

"keywords": [

                ]       ,

"status": {

"code": 0,

"label": "approved",

"label_i18n": "Approved"

                }       ,

"taxonomyCategoryBriefs": [

                ]       ,

"name": "المتخصصين وذوي الخبرات",

"email": "Experience@linkdev.com"

         }       ,
                {

"dateCreated": "2024-04-02T09:18:18Z",

"dateModified": "2024-04-02T09:18:18Z",

"externalReferenceCode": "38c0731e-c877-294d-e41e-a3fba6d35fcd",

"id": 89319,

"keywords": [

                ]       ,

"status": {
```

```
"code": 0,
"label": "approved",
"label_i18n": "Approved"
                }       ,
"taxonomyCategoryBriefs": [
                ]       ,
"name": "حديثي التخرج",
"email": "Fresh@linkdev.com"
        }       ,
               {
"dateCreated": "2024-04-02T09:18:46Z",
"dateModified": "2024-04-02T09:18:46Z",
"externalReferenceCode": "00507bb0-2e7b-9592-fe23-7eac7bca5954",
"id": 89322,
"keywords": [
                ]       ,
"status": {
"code": 0,
"label": "approved",
"label_i18n": "Approved"
                }       ,
"taxonomyCategoryBriefs": [
                ]       ,
"name": "برنامج التدريب التعاوني",
"email": " Training@linkdev.com"
               }
 ],
"lastPage": 1,
"page": 1,
"pageSize": 500,
"totalCount": 3
}
```


I Integer Overflow 6 TOC

Integer Overflow

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"r_applicationType_c_recruitmentApplicationTypeId" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1862
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId":        -99999999999999999999,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
```

```
 "identityType": {
        "key": "residence",
        "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
               {
                "average": "4",
                "graduationDate": "2023-12-31T22:00:00.000Z",
                "qualificationFrom": {
                        "key": "4",
                        "name": "4"
                },
                "qualification": {
                        "key": "masters",
                        "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                },
                "specialization": "ECE",
                "universityName": "MUST"
               }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
        "key": "key2",
        "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
        "value": "",
        "disable": true
 },
 "fieldOfInterest": {
        "key": "facilitiesSecurityAndSafety",
        "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
        "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=9E71CAAD85B4B4C58E8979C4EB327A25; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:01:35 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNA
...
```

```
...
...
```

Issue 2 of 6

TOC

Integer Overflow

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"identityNumber" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEalliOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1858
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
```

```
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
         "key": "residence",
         "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "       9999999999999999999",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                         "key": "4",
                         "name": "4"
                 }       ,
                 "qualification": {
                         "key": "masters",
                         "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
         "key": "key2",
         "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
         "value": "",
         "disable": true
 },
 "fieldOfInterest": {
         "key": "facilitiesSecurityAndSafety",
         "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
         "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
```

```
Set-Cookie: JSESSIONID=84951C06CFFEAF0A5DD17464DBE896BB; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:03:35 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_SE
...
...
...
```

Issue 3 of 6

TOC

Integer Overflow

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"cv"->"id" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25Ecjlzbmxl ZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
```

```
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1860
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
        "key": "residence",
        "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                        "key": "4",
                        "name": "4"
                 }       ,
                 "qualification": {
                        "key": "masters",
                        "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
        "key": "key2",
        "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
        "value": "",
        "disable": true
 },
 "fieldOfInterest": {
        "key": "facilitiesSecurityAndSafety",
        "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
        "id": "       99999999999999999999"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}
```

```
HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=86CF75ADED5A89FBDA7791F3BAF471A9; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:05:09 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTERNAL_
...
...
...
```

Issue 4 of 6

TOC

Integer Overflow

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"applicationQualifications"[0]->"qualificationFrom"->"name" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_NlTBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
```

```
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1865
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
         "key": "residence",
         "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                         "key": "4",
                         "name": "       99999999999999999999"
                 }       ,
                 "qualification": {
                         "key": "masters",
                         "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
         "key": "key2",
         "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
         "value": "",
         "disable": true
 },
 "fieldOfInterest": {
         "key": "facilitiesSecurityAndSafety",
         "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
         "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
```

```
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=E215D8C1314D1463F28A97FD97F957FF; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:03:37 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTE
...
...
...
```

Issue 5 of 6

TOC

Integer Overflow

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"applicationQualifications"[0]->"average" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
```

```
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1865
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
         "key": "residence",
         "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "       99999999999999999999",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                         "key": "4",
                         "name": "4"
                 }       ,
                 "qualification": {
                         "key": "masters",
                         "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
         "key": "key2",
         "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
         "value": "",
         "disable": true
 },
 "fieldOfInterest": {
         "key": "facilitiesSecurityAndSafety",
         "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
```

```
 "alreadyRegistered": true,
 "cv": {
        "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=8A3076984DDB8DD26B48D80150EDB1CD; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:03:51 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTE
...
...
...
```

Issue 6 of 6

TOC

Integer Overflow

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplications/
Entity:	->"applicationQualifications"[0]->"qualificationFrom"->"key" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /o/c/recruitmentapplications/ HTTP/1.1
```

```
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment/?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073214368;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715073020896;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1865
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "fullNameArabic": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "fullNameEnglish": "appscan",
 "r_applicationType_c_recruitmentApplicationTypeId": 89319,
 "birthDate": "05-23-2001",
 "nationality": "\u0623\u0645\u0631\u064a\u0643\u064a",
 "identityType": {
         "key": "residence",
         "name": "\u0625\u0642\u0627\u0645\u0629"
 },
 "identityNumber": "11122324",
 "isMale": true,
 "applicationQualifications": [
                {
                 "average": "4",
                 "graduationDate": "2023-12-31T22:00:00.000Z",
                 "qualificationFrom": {
                         "key": "       99999999999999999999",
                         "name": "4"
                 }       ,
                 "qualification": {
                         "key": "masters",
                         "name": "\u0645\u0627\u062c\u0633\u062a\u064a\u0631"
                 }       ,
                 "specialization": "ECE",
                 "universityName": "MUST"
                }
 ],
 "applicationExperiences": [

 ],
 "email": "vepapi2863@rehezb.com",
 "country": "\u0623\u0646\u062f\u0648\u0631\u0627",
 "countryKey": {
         "key": "key2",
         "name": "\u0645\u0641\u062a\u0627\u062d \u0627\u0644\u062f\u0648\u0644\u0629 2"
 },
 "mobile": "+96611666",
 "city": {
```

```
        "value": "",
        "disable": true
 },
 "fieldOfInterest": {
        "key": "facilitiesSecurityAndSafety",
        "name": "\u0645\u0631\u0627\u0641\u0642 \u0648\u0623\u0645\u0646
\u0648\u0633\u0644\u0627\u0645\u0629"
 },
 "other": "",
 "alreadyRegistered": true,
 "cv": {
        "id": "116508"
 },
 "acceptance": true,
 "reCaptcheCheck":
"03AFcWeA6BLvmZsRqoPRJy8VCy5EB3B6twBuS8yHQjX_tqKU7PDXzbotcwZORoeQEOuSzBiXdC13EBhPjfcmFh8f_kzngDbe
0qbvVfq5T2K-
f9MB5AodbUjGaI6iJ7aMTnZzbxfh_qDdPpJ03OGLgA8YLwgEKzTnzahITM3msf4tLplQt9T0FU_wagw1MS9LPVFbCY85hn53j
JybFxJJ6PPIlPBKNi1BovJS7YBa04yvJTqWY4cxdEDpsAWKYidGbmGga5xFujE9nk1qs5zk055TjYESX3n7hGCm9l7uljJXF2
ItvGBF0b1f-kMefnGctk1RCyMrAmg2dPP0a8w5tmeWVQZaomDSUToP-
RMUMusnUkq3aIO6R5YD5LXLiMVZHGy0fF5VKaA6NBXz8CL-
tInHQ_a90nfJkQNNElOyYvO3TtZlP5LM3XsfE6J6vwDb0PgAq9xUm4X0dMs94Uz1aYCfCu9O6CqXvKmYjm4bReMazH0StULII
c-R05Fd2SKt2fJV-
dZUTn6Ky3DXpi3mPtzvOJDLD70z28vSecmQTMjCNlr2dCTTYoHG6rqLZN5e1FI1vUhuGSUppW4mkucKw_E8vsAsialTZsVwn5
Lj539EVXTg6RZk44OQp85YWW7e5VDVw2G1KvhWfjA98OWt5G2jVUN3Adjpv2bLPMrzuYiB11m5vgXC6M2iFotZ5w2B7hyr9T2
rj_yeaF"
}

HTTP/1.1 500
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 80
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=553586EC5A34FA588A7C29A4040D18B4; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 11:04:40 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"status": "INTE
...
...
...
```


I Internal IP Disclosure Pattern Found 6

TOC

Issue 1 of 6

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/account-type
Entity:	account-type (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove internal IP addresses from your website

Reasoning: AppScan discovered what looks like an internal IP address in the response.

Test Requests and Responses:

```
GET /account-type HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/web/guest/home?
p_p_id=com_liferay_login_web_portlet_LoginPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=vi
ew&_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName=%2Flogin%2Flogin&saveLastPath
=false
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
LFR_SESSION_STATE_20099=1715071553037; _ga=GA1.1.128297136.1599395143;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0; COOKIE_SUPPORT=true;
GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Upgrade-Insecure-Requests: 1
Sec-Fetch-Mode: navigate
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.7
Sec-Fetch-User: ?1
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: document


HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Liferay-Portal: Liferay Digital Experience Platform
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Set-Cookie: JSESSIONID=BBEB3B653EB0A4BF373F5C5EF8C77970; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 09:28:41 GMT
Content-Type: text/html;charset=UTF-8
```

```
<!DOCTYPE html>
```

```
<html class="rtl" dir="rtl" lang="ar-SA">

<head>
 <title>       وزارة الاتصالات وتقنية المعلومات - اختيارات التسجيل</title>
  <meta name="viewport" content="width=device-width, width=device-width" />
  <meta name="description" content="اختيارات التسجيل - وزارة الاتصالات وتقنية المعلومات " />
  <meta name="keywords" content="اختيارات التسجيل - وزارة الاتصالات وتقنية المعلومات">
  <meta name="format-detection" content="telephone=no">
  <meta property="og:url" content="/account-type" />
  <meta property="og:type" content="Website" />
  <meta property="og:title" content="اختيارات التسجيل - وزارة الاتصالات وتقنية المعلومات " />
  <meta property="og:description" content="اختيارات التسجيل - وزارة الاتصالات وتقنية المعلومات " />
  <meta property="og:image" content="https://mcit-liferayqc.linkdev.com/o/mcit-theme/images/logo-
share.png" />
  <meta property="og:image:secure_url" content="https://mcit-liferayqc.linkdev.com/o/mcit-
theme/images/logo-share.png" />

  <link rel="manifest" href="/o/mcit-theme/manifest.json">

<meta content="text/html; charset=UTF-8" http-equiv="content-type" />

<script type="importmap">{"imports":{"react-dom":"/o/frontend-js-react-
web/__liferay__/exports/react-dom.js","@clayui/breadcrumb":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$breadcrumb.js","@clayui/form":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$form.js","@clayui/popover":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$popover.js","@clayui/charts":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$charts.js","@clayui/shared":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$shared.js","@clayui/localized-input":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$localized-input.js","@clayui/modal":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$modal.js","@clayui/empty-state":"/o/frontend-taglib-
```

```
clay/__liferay__/exports/@clayui$empty-state.js","react":"/o/frontend-js-react-
web/__liferay__/exports/react.js","@clayui/color-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$color-picker.js","@clayui/navigation-bar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$navigation-bar.js","@clayui/pagination":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$pagination.js","@clayui/icon":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$icon.js","@clayui/table":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$table.js","@clayui/autocomplete":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$autocomplete.js","@clayui/slider":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$slider.js","@clayui/management-toolbar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$management-toolbar.js","@clayui/multi-sele
...
...
...

                getRealUserId: function() {
                        return '20099';
                }       ,
                getRemoteAddr: function() {
                        return '       10.100.30.154';
                }       ,
                getRemoteHost: function() {
                        return '       10.100.30.154';
                }       ,
                getScopeGroupId: function() {
                        return '20119';
                }       ,
...
...
...
```

Issue 2 of 6

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/home
Entity:	home (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove internal IP addresses from your website

Reasoning: AppScan discovered what looks like an internal IP address in the response.

Test Requests and Responses:

```
GET /home HTTP/1.1
Sec-Fetch-Site: none
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; _ga=GA1.1.128297136.1599395143;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
```

```
Upgrade-Insecure-Requests: 1
Sec-Fetch-Mode: navigate
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.7
Sec-Fetch-User: ?1
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: document


HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Liferay-Portal: Liferay Digital Experience Platform
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Set-Cookie: JSESSIONID=635B598C22E03A9CFB3F7DDDFCEC1274; Path=/; Secure; HttpOnly
Set-Cookie: COOKIE_SUPPORT=true; Max-Age=31536000; Expires=Wed, 07 May 2025 09:26:52 GMT; Path=/;
Secure; HttpOnly
Set-Cookie: GUEST_LANGUAGE_ID=ar_SA; Max-Age=31536000; Expires=Wed, 07 May 2025 09:26:52 GMT;
Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 09:26:54 GMT
Content-Type: text/html;charset=UTF-8









                <!DOCTYPE html>
```

```
<html class="rtl" dir="rtl" lang="ar-SA">

<head>
 <title>       وزارة الاتصالات وتقنية المعلومات - الرئيسية</title>
  <meta name="viewport" content="width=device-width, width=device-width" />
  <meta name="description" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية " />
  <meta name="keywords" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية">
  <meta name="format-detection" content="telephone=no">
  <meta property="og:url" content="/home" />
  <meta property="og:type" content="Website" />
  <meta property="og:title" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية " />
  <meta property="og:description" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية " />
  <meta property="og:image" content="https://mcit-liferayqc.linkdev.com/o/mcit-theme/images/logo-
share.png" />
  <meta property="og:image:secure_url" content="https://mcit-liferayqc.linkdev.com/o/mcit-
theme/images/logo-share.png" />

  <link rel="manifest" href="/o/mcit-theme/manifest.json">
```

```
<meta content="text/html; charset=UTF-8" http-equiv="content-type" />
```

```
<script type="importmap">{"imports":{"react-dom":"/o/frontend-js-react-
web/__liferay__/exports/react-dom.js","@clayui/breadcrumb":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$breadcrumb.js","@clayui/form":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$form.js","@clayui/popover":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$popover.js","@clayui/charts":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$charts.js","@clayui/shared":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$shared.js","@clayui/localized-input":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$localized-input.js","@clayui/modal":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$modal.js","@clayui/empty-state":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$empty-state.js","react":"/o/frontend-js-react-
web/__liferay__/exports/react.js","@clayui/color-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$color-picker.js","@clayui/navigation-bar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$navigation-bar.js","@clayui/pagination":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$pagination.js","@clayui/icon":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$icon.js","@clayui/table":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$table.js","@clayui/autocomplete":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$autocomplete.js","@clayui/slider":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$slider.js","@clayui/management-toolbar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$management-toolbar.js","@clayui/multi-select":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$multi-select.js","@clayui/nav":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$nav.js","@clayui/time-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@c
...
...
...
```

```
                getRealUserId: function() {
                        return '20099';
                }       ,
                getRemoteAddr: function() {
                        return '       10.100.30.154';
                }       ,
                getRemoteHost: function() {
                        return '       10.100.30.154';
                }       ,
                getScopeGroupId: function() {
                        return '20119';
                }       ,
...
...
...
```

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/individual-registeration
Entity:	individual-registeration (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove internal IP addresses from your website

Reasoning: AppScan discovered what looks like an internal IP address in the response.

Test Requests and Responses:

```
GET /individual-registeration HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/client
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: __gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-
ZDNGS8OTIECFDg; _ga=GA1.1.128297136.1599395143;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0; LFR_SESSION_STATE_20099=1715071579366;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0; COOKIE_SUPPORT=true;
GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
x-csrf-token: VIjAd6Jf
x-requested-with: XMLHttpRequest
sec-ch-ua-mobile: ?0
x-pjax: true
Accept: */*
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty


HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Liferay-Portal: Liferay Digital Experience Platform
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Set-Cookie: JSESSIONID=B2653273E5210639E1A1EE82BA4C2114; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 09:30:25 GMT
Content-Type: text/html;charset=UTF-8
```

```
<!DOCTYPE html>
```

<html class="rtl" dir="rtl" lang="ar-SA">

<head>
 <title>تسجيل الأفراد - وزارة الاتصالات وتقنية المعلومات</title>
  <meta name="viewport" content="width=device-width, width=device-width" />
  <meta name="description" content="تسجيل الأفراد - وزارة الاتصالات وتقنية المعلومات" />
  <meta name="keywords" content="تسجيل الأفراد - وزارة الاتصالات وتقنية المعلومات">
  <meta name="format-detection" content="telephone=no">
  <meta property="og:url" content="/individual-registeration" />
  <meta property="og:type" content="Website" />
  <meta property="og:title" content="تسجيل الأفراد - وزارة الاتصالات وتقنية المعلومات" />
  <meta property="og:description" content="تسجيل الأفراد - وزارة الاتصالات وتقنية المعلومات" />
  <meta property="og:image" content="https://mcit-liferayqc.linkdev.com/o/mcit-theme/images/logo-share.png" />
  <meta property="og:image:secure_url" content="https://mcit-liferayqc.linkdev.com/o/mcit-theme/images/logo-share.png" />

  <link rel="manifest" href="/o/mcit-theme/manifest.json">

<meta content="text/html; charset=UTF-8" http-equiv="content-type" />

<script type="importmap">{"imports":{"react-dom":"/o/frontend-js-react-web/__liferay__/exports/react-dom.js","@clayui/breadcrumb":"/o/frontend-taglib-clay/__liferay__/exports/@clayui$breadcrumb.js","@clayui/form":"/o/frontend-taglib-clay/__liferay__/exports/@clayui$form.js","@clayui/popover":"/o/frontend-taglib-clay/__liferay__/exports/@clayui$popover.js","@clayui/charts":"/o/frontend-taglib-clay/__liferay__/exports/@clayui$charts.js","@clayui/shared":"/o/frontend-taglib-clay/__liferay__/exports/@clayui$shared.js","@clayui/localized-input":"/o/frontend-taglib-clay/__liferay__/exports/@clayui$localized-input.js","@clayui/modal":"/o/frontend-taglib-clay/__liferay__/exports/@clayui$modal.js","@clayui/empty-state":"/o/frontend-taglib-clay/__liferay__/exports/@clayui$empty-state.js","react":"/o/frontend-js-react-

```
web/__liferay__/exports/react.js","@clayui/color-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$color-picker.js","@clayui/navigation-bar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$navigation-bar.js","@clayui/pagination":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$pagination.js","@clayui/icon":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$icon.js","@clayui/table":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$table.js","@clayui/autocomplete":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$autocomplete.js","@clayui/slider":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$slider.js","@clayui/management-toolbar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$management-toolbar.js","@clayui/multi-select":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$multi-select.js","@clayui/nav":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$nav.js","@clayui/time-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$time-picker.js","@clayui/provider":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$provi
...
...
...

                getRealUserId: function() {
                        return '20099';
                }       ,
                getRemoteAddr: function() {
                        return '       10.100.30.154';
                }       ,
                getRemoteHost: function() {
                        return '       10.100.30.154';
                }       ,
                getScopeGroupId: function() {
                        return '20119';
                }       ,
...
...
...
```

Issue 4 of 6

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/web/guest/recruitment-options
Entity:	recruitment-options (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove internal IP addresses from your website

Reasoning: AppScan discovered what looks like an internal IP address in the response.

Test Requests and Responses:

```
GET /web/guest/recruitment-options HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/home/client
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
LFR_SESSION_STATE_20099=1715073020896; _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
```

```
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_116486=1715073077970;
_ga=GA1.1.128297136.1599395143;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
ID=78692f674d56476771344b754c46314878394f5043513d3d; COMPANY_ID=20096; COOKIE_SUPPORT=true;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; GUEST_LANGUAGE_ID=ar_SA
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
x-csrf-token: MEQeGkLB
x-requested-with: XMLHttpRequest
sec-ch-ua-mobile: ?0
x-pjax: true
Accept: */*
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty


HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Liferay-Portal: Liferay Digital Experience Platform
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Set-Cookie: JSESSIONID=F5FEF704BF4BA09031B6F515D64F384F; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 09:55:26 GMT
Content-Type: text/html;charset=UTF-8

                    <!DOCTYPE html>
```

```
<html class="rtl" dir="rtl" lang="ar-SA">

<head>
 <title>       وزارة الاتصالات وتقنية المعلومات - التوظيف</title>
  <meta name="viewport" content="width=device-width, width=device-width" />
  <meta name="description" content="وزارة الاتصالات وتقنية المعلومات - التوظيف " />
  <meta name="keywords" content="وزارة الاتصالات وتقنية المعلومات - التوظيف">
  <meta name="format-detection" content="telephone=no">
  <meta property="og:url" content="/web/guest/recruitment-options" />
  <meta property="og:type" content="Website" />
  <meta property="og:title" content="وزارة الاتصالات وتقنية المعلومات - التوظيف " />
  <meta property="og:description" content="وزارة الاتصالات وتقنية المعلومات - التوظيف " />
  <meta property="og:image" content="https://mcit-liferayqc.linkdev.com/o/mcit-theme/images/logo-
share.png" />
  <meta property="og:image:secure_url" content="https://mcit-liferayqc.linkdev.com/o/mcit-
theme/images/logo-share.png" />

  <link rel="manifest" href="/o/mcit-theme/manifest.json">
```

```
<meta content="text/html; charset=UTF-8" http-equiv="content-type" />
```

```
<script type="importmap">{"imports":{"react-dom":"/o/frontend-js-react-
web/__liferay__/exports/react-dom.js","@clayui/breadcrumb":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$breadcrumb.js","@clayui/form":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$form.js","@clayui/popover":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$popover.js","@clayui/charts":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$charts.js","@clayui/shared":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$shared.js","@clayui/localized-input":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$localized-input.js","@clayui/modal":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$modal.js","@clayui/empty-state":"/o/fronte
...
...
...

                getRealUserId: function() {
                        return '20099';
                }       ,
                getRemoteAddr: function() {
                        return '       10.100.30.154';
                }       ,
                getRemoteHost: function() {
                        return '       10.100.30.154';
                }       ,
                getScopeGroupId: function() {
                        return '20119';
                }       ,
...
...
...
```

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/web/guest/home
Entity:	home (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove internal IP addresses from your website

Reasoning: AppScan discovered what looks like an internal IP address in the response.

Test Requests and Responses:

```
GET /web/guest/home?
p_p_id=com_liferay_login_web_portlet_LoginPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=vi
ew&_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName=%2Flogin%2Flogin&saveLastPath
=false HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/c/portal/login?p_l_id=129
Cookie: COOKIE_SUPPORT=true; GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: Keep-Alive
Host: mcit-liferayqc.linkdev.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Liferay-Portal: Liferay Digital Experience Platform
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Set-Cookie: JSESSIONID=83F99BB5369AC6AA3CDC7BA3BC14493D; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 10:04:14 GMT
Content-Type: text/html;charset=UTF-8
```

```
<!DOCTYPE html>
```

```
<html class="rtl" dir="rtl" lang="ar-SA">

<head>
 <title>       وزارة الاتصالات وتقنية المعلومات - الرئيسية</title>
  <meta name="viewport" content="width=device-width, width=device-width" />
  <meta name="description" content="وزارة الاتصالات وتقنية المعلومات - الرئيسية " />
```

```
  <meta name="keywords" content="الرئيسية - وزارة الاتصالات وتقنية المعلومات">
  <meta name="format-detection" content="telephone=no">
  <meta property="og:url" content="/web/guest/home?
p_p_id=com_liferay_login_web_portlet_LoginPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=vi
ew&_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName=%2Flogin%2Flogin&saveLastPath
=false" />
  <meta property="og:type" content="Website" />
  <meta property="og:title" content="الرئيسية - وزارة الاتصالات وتقنية المعلومات" />
  <meta property="og:description" content="الرئيسية - وزارة الاتصالات وتقنية المعلومات" />
  <meta property="og:image" content="https://mcit-liferayqc.linkdev.com/o/mcit-theme/images/logo-
share.png" />
  <meta property="og:image:secure_url" content="https://mcit-liferayqc.linkdev.com/o/mcit-
theme/images/logo-share.png" />

  <link rel="manifest" href="/o/mcit-theme/manifest.json">
```

```
<meta content="text/html; charset=UTF-8" http-equiv="content-type" />
```

```
<script type="importmap">{"imports":{"react-dom":"/o/frontend-js-react-
web/__liferay__/exports/react-dom.js","@clayui/breadcrumb":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$breadcrumb.js","@clayui/form":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$form.js","@clayui/popover":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$popover.js","@clayui/charts":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$charts.js","@clayui/shared":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$shared.js","@clayui/localized-input":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$localized-input.js","@clayui/modal":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$modal.js","@clayui/empty-state":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$empty-state.js","react":"/o/frontend-js-react-
web/__liferay__/exports/react.js","@clayui/color-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$color-picker.js","@clayui/navigation-bar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$navigation-bar.js","@clayui/pagination":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$pagination.js","@clayui/icon":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$icon.js","@clayui/table":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$table.js","@clayui/autocomplete":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$autocomplete.js","@clayui/slider":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$slider.js","@clayui/management-toolbar":"/o/frontend-taglib-
```

```
clay/__liferay__/exports/@clayui$management-toolbar.js","@clayui/multi-select":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$multi-select.js","@clayui/nav":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$nav.js","@clayui/time-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$time-picker.js","@clayui/provider":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$provider.js","@clayui/upper-toolbar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$upper-toolbar.js","@clayui/loading-indicator":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$loading-indicator.js","@clayui/panel":"/o/front
...
...
...

                getRealUserId: function() {
                        return '20099';
                }       ,
                getRemoteAddr: function() {
                        return '       10.100.30.154';
                }       ,
                getRemoteHost: function() {
                        return '       10.100.30.154';
                }       ,
                getScopeGroupId: function() {
                        return '20119';
                }       ,
...
...
...
```

Issue 6 of 6

TOC

Internal IP Disclosure Pattern Found	
Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/recruitment
Entity:	recruitment (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove internal IP addresses from your website

Reasoning: AppScan discovered what looks like an internal IP address in the response.

Test Requests and Responses:

```
GET /recruitment?isFresh=true HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/c
Cookie: COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: Keep-Alive
Host: mcit-liferayqc.linkdev.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
```

```
Liferay-Portal: Liferay Digital Experience Platform
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Set-Cookie: JSESSIONID=05290F490FA0F0E6888471823A352D11; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 10:04:44 GMT
Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>
```

```
<html class="rtl" dir="rtl" lang="ar-SA">

<head>
 <title>       التوظيف - وزارة الاتصالات وتقنية المعلومات</title>
  <meta name="viewport" content="width=device-width, width=device-width" />
  <meta name="description" content="التوظيف - وزارة الاتصالات وتقنية المعلومات" />
  <meta name="keywords" content="التوظيف - وزارة الاتصالات وتقنية المعلومات">
  <meta name="format-detection" content="telephone=no">
  <meta property="og:url" content="/recruitment?isFresh=true" />
  <meta property="og:type" content="Website" />
  <meta property="og:title" content="التوظيف - وزارة الاتصالات وتقنية المعلومات" />
  <meta property="og:description" content="التوظيف - وزارة الاتصالات وتقنية المعلومات" />
  <meta property="og:image" content="https://mcit-liferayqc.linkdev.com/o/mcit-theme/images/logo-
share.png" />
  <meta property="og:image:secure_url" content="https://mcit-liferayqc.linkdev.com/o/mcit-
theme/images/logo-share.png" />

  <link rel="manifest" href="/o/mcit-theme/manifest.json">

<meta content="text/html; charset=UTF-8" http-equiv="content-type" />
```

```
<script type="importmap">{"imports":{"react-dom":"/o/frontend-js-react-
web/__liferay__/exports/react-dom.js","@clayui/breadcrumb":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$breadcrumb.js","@clayui/form":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$form.js","@clayui/popover":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$popover.js","@clayui/charts":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$charts.js","@clayui/shared":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$shared.js","@clayui/localized-input":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$localized-input.js","@clayui/modal":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$modal.js","@clayui/empty-state":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$empty-state.js","react":"/o/frontend-js-react-
web/__liferay__/exports/react.js","@clayui/color-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$color-picker.js","@clayui/navigation-bar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$navigation-bar.js","@clayui/pagination":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$pagination.js","@clayui/icon":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$icon.js","@clayui/table":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$table.js","@clayui/autocomplete":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$autocomplete.js","@clayui/slider":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$slider.js","@clayui/management-toolbar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$management-toolbar.js","@clayui/multi-select":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$multi-select.js","@clayui/nav":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$nav.js","@clayui/time-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$time-picker.js","@clayui/provider":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$provider.js","@clayui/upper-toolbar":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$upper-toolbar.js","@clayui/loading-indicator":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$loading-indicator.js","@clayui/panel":"/o/frontend-
taglib-clay/__liferay__/exports/@clayui$panel.js","@clayui/drop-down":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$drop-down.js","@clayui/list":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$list.js","@clayui/date-picker":"/o/frontend-taglib-
clay/__liferay__/exports/@clayui$date-picker.js","@clayui/label":"/o/frontend-ta
...
...
...

                getRealUserId: function() {
                        return '20099';
                }       ,
                getRemoteAddr: function() {
                        return '       10.100.30.154';
                }       ,
                getRemoteHost: function() {
                        return '       10.100.30.154';
                }       ,
                getScopeGroupId: function() {
                        return '20119';
                }       ,
...
...
...
```

I SHA-1 cipher suites were detected 1

TOC

Issue 1 of 1

TOC

SHA-1 cipher suites were detected

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/js_resolve_modules
Entity:	mcit-liferayqc.linkdev.com (Page)
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	The web server or application server are configured in an insecure way
Fix:	Change server's supported ciphersuites

Reasoning: AppScan determined that the site uses weak cipher suites by successfully creating SSL connections using each of the weak cipher suites listed here.

Test Requests and Responses:

```
GET /o/js_resolve_modules?modules=frontend-js-spa-web%405.0.44%2Finit HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/home
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: __gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-
ZDNGS8OTIECFDg; _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga=GA1.1.128297136.1599395143; _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF; COOKIE_SUPPORT=true; GUEST_LANGUAGE_ID=ar_SA
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Accept: */*
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty


HTTP/1.1 200
Connection: keep-alive
Content-Length: 6078
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Cache-Control: no-cache
ETag: W/"d18b97c3-14f5-489a-90fa-791afa57880a"
Date: Tue, 07 May 2024 08:19:12 GMT
Content-Type: application/json;charset=UTF-8

{
 "pathMap": {
         "frontend-js-spa-web@5.0.44\/screen\/ActionURLScreen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/ActionURLScreen",
         "frontend-js-spa-web@5.0.44\/screen\/RenderURLScreen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/RenderURLScreen",
         "frontend-js-spa-web@5.0.44\/surface\/Surface": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/surface\/Surface",
         "frontend-js-spa-web@5.0.44\/cacheable\/Cacheable": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/cacheable\/Cacheable",
         "frontend-js-spa-web@5.0.44\/app\/LiferayApp": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/app\/LiferayApp",
         "frontend-js-spa-web@5.0.44\/app\/App": "\/o\/js\/resolved-module\/frontend-js-
spa-web@5.0.44\/app\/App",
         "frontend-js-spa-web@5.0.44\/screen\/EventScreen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/EventScreen",
         "frontend-js-web@5.0.97\/index": "\/o\/js\/resolved-module\/frontend-js-
```

```
web@5.0.97\/index",
        "frontend-js-spa-web@5.0.44\/route\/Route": "\/o\/js\/resolved-module\/frontend-
js-spa-web@5.0.44\/route\/Route",
        "frontend-js-spa-web@5.0.44\/util\/utils": "\/o\/js\/resolved-module\/frontend-
js-spa-web@5.0.44\/util\/utils",
        "frontend-js-spa-web@5.0.44\/util\/pathParser": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/util\/pathParser",
        "frontend-js-spa-web@5.0.44\/screen\/HtmlScreen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/HtmlScreen",
        "frontend-js-spa-web@5.0.44\/init": "\/o\/js\/resolved-module\/frontend-js-spa-
web@5.0.44\/init",
        "frontend-js-spa-web@5.0.44\/screen\/Screen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/Screen",
        "frontend-js-spa-web@5.0.44\/screen\/RequestScreen": "\/o\/js\/resolved-
module\/frontend-js-spa-web@5.0.44\/screen\/RequestScreen"
 },
 "configMap": {

 },
 "resolvedModules": [
        "frontend-js-web@5.0.97\/index",
        "frontend-js-spa-web@5.0.44\/surface\/Surface",
        "frontend-js-spa-web@5.0.44\/util\/utils",
        "frontend-js-spa-web@5.0.44\/util\/pathParser",
        "frontend-js-spa-web@5.0.44\/route\/Route",
        "frontend-js-spa-web@5.0.44\/cacheable\/Cacheable",
        "frontend-js-spa-web@5.0.44\/screen\/Screen",
        "frontend-js-spa-web@5.0.44\/app\/App",
        "frontend-js-spa-web@5.0.44\/app\/LiferayApp",
        "frontend-js-spa-web@5.0.44\/screen\/RequestScreen",
        "frontend-js-spa-web@5.0.44\/screen\/HtmlScreen",
        "frontend-js-spa-web@5.0.44\/screen\/EventScreen",
        "frontend-js-spa-web@5.0.44\/screen\/ActionURLScreen",
        "frontend-js-spa-web@5.0.44\/screen\/RenderURLScreen",
        "frontend-js-spa-web@5.0.44\/init"
 ],
 "moduleMap": {
        "frontend-js-spa-web@5.0.44\/screen\/ActionURLScreen": {
                ".\/EventScreen": "frontend-js-spa-web@5.0.44\/screen\/EventScreen",
                "..\/util\/utils": "frontend-js-spa-web@5.0.44\/util\/utils"
        }       ,
        "frontend-js-spa-web@5.0.44\/screen\/RenderURLScreen": {
                ".\/EventScreen": "frontend-js-spa-web@5.0.44\/screen\/EventScreen"
        }       ,
        "frontend-js-spa-web@5.0.44\/surface\/Surface": {
                "frontend-js-web": "frontend-js-web@5.0.97\/index"
        }       ,
        "frontend-js-spa-web@5.0.44\/cacheable\/Cacheable": {
                "frontend-js-web": "frontend-js-web@5.0.97\/index"
        }       ,
        "frontend-js-spa-web@5.0.44\/app\/LiferayApp": {
                "..\/surface\/Surface": "frontend-js-spa-web@5.0.44\/surface\/Surface",
                "frontend-js-web": "frontend-js-web@5.0.97\/index",
                "..\/util\/utils": "frontend-js-spa-web@5.0.44\/util\/utils",
                ".\/App": "frontend-js-spa-web@5.0.44\/app\/App"
        }       ,
        "frontend-js-spa-web@5.0.44\/app\/App": {
                "..\/route\/Route": "frontend-js-spa-web@5.0.44\/route\/Route",
                "..\/surface\/Surf
...
...
...
```


Verify that the site uses the cryptographically weak cipher suites listed here.

The following weak cipher suites are supported by the server:

Id	Name	SSL Version
51	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLS 1.2
57	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLS 1.2

49171	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLS 1.2
49172	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLS 1.2

I Unsanitized user input reflected in JSON 9

TOC

Issue 1 of 9

TOC

Unsanitized user input reflected in JSON

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/mcit-forgot-password/v1.0/forgot-password
Entity:	forgot-password (Global)
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Reasoning: The test result seems to indicate a vulnerability because the Global Validation feature found an embedded script in the response, which was probably injected by a previous test.

Test Requests and Responses:

```
POST /o/mcit-forgot-password/v1.0/forgot-password HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/forgot-password/
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: LFR_SESSION_STATE_20099=1715072894528;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0; _ga=GA1.1.128297136.1599395143;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 199
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "email": ">\"'><script>alert(4318)</script>",
 "registerNumber": ">\"'><script>alert(4318)</script>",
```

```
 "userType": ">\"'><script>alert(4318)</script>",
 "recaptcha_token": ">\"'><script>alert(4318)</script>"
}

HTTP/1.1 400
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 551
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=02A9B6B44E7DF49CFE7FD0B233534676; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 09:52:39 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"detail": "Cannot deserialize value of type `java.lang.Integer` from String
\">\"'><script>alert(4318)</script>\": not a valid `java.lang.Integer` value\n at [Source:
(org.apache.cxf.transport.http.AbstractHTTPDestination$1); line: 1, column: 110] (through
reference chain: com.linkdev.mcit.forgot.password.dto.v1_0.ForgotPasswordObject[\"userType\"])",

"status": "BAD_REQUEST",

"title": "Unable to map JSON path \"userType\" with value \">\"'><script>alert(4318)</script>\"
to class \"Integer\"",

"type": "InvalidFormatException"

}
```

Issue 2 of 9

TOC

Unsanitized user input reflected in JSON

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/mcit-registration/v1.0/individualRegistration
Entity:	individualRegistration (Global)
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Reasoning: The test result seems to indicate a vulnerability because the Global Validation feature found an embedded script in the response, which was probably injected by a previous test.

Test Requests and Responses:

```
POST /o/mcit-registration/v1.0/individualRegistration HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/individual-registeration/
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0; _ga=GA1.1.128297136.1599395143;
```

```
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_20099=1715071587281;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0; COOKIE_SUPPORT=true;
GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 938
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "firstName": ">\"'><script>alert(1610)</script>",
 "firstNameAr": ">\"'><script>alert(1610)</script>",
 "lastNameAr": ">\"'><script>alert(1610)</script>",
 "lastName": ">\"'><script>alert(1610)</script>",
 "birthDate": ">\"'><script>alert(1610)</script>",
 "gender": ">\"'><script>alert(1610)</script>",
 "nationalityCode": ">\"'><script>alert(1610)</script>",
 "currentCountryCode": ">\"'><script>alert(1610)</script>",
 "cityCode": ">\"'><script>alert(1610)</script>",
 "identityId": ">\"'><script>alert(1610)</script>",
 "identityType": ">\"'><script>alert(1610)</script>",
 "userType": ">\"'><script>alert(1610)</script>",
 "recaptchaResponse": ">\"'><script>alert(1610)</script>",
 "password": ">\"'><script>alert(1610)</script>",
 "re-password": ">\"'><script>alert(1610)</script>",
 "isNafazAccount": ">\"'><script>alert(1610)</script>",
 "email": ">\"'><script>alert(1610)</script>",
 "mobilePhone": ">\"'><script>alert(1610)</script>",
 "locale": ">\"'><script>alert(1610)</script>"
}

HTTP/1.1 400
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 534
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=0A14535CD1711B6DA2AB3AFBEF493CC8; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 09:34:43 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"detail": "Cannot deserialize value of type `java.lang.Boolean` from String
\">\"'><script>alert(1610)</script>\": only \"true\" or \"false\" recognized\n at [Source:
(org.apache.cxf.transport.http.AbstractHTTPDestination$1); line: 1, column: 253] (through
reference chain: com.linkdev.mcit.registration.dto.v1_0.UserObject[\"gender\"])",

"status": "BAD_REQUEST",

"title": "Unable to map JSON path \"gender\" with value \">\"'><script>alert(1610)</script>\" to
class \"Boolean\"",

"type": "InvalidFormatException"

}
```

Issue 3 of 9

TOC

Unsanitized user input reflected in JSON

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplicationtypes
Entity:	recruitmentapplicationtypes (Global)
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Reasoning: The test result seems to indicate a vulnerability because the Global Validation feature found an embedded script in the response, which was probably injected by a previous test.

Test Requests and Responses:

```
GET
/o/c/recruitmentapplicationtypes?restrictFields=%3E%22%27%3E%3Cscript%3Ealert%285762%29%3C%2Fscri
pt%3E&pageSize=%3E%22%27%3E%3Cscript%3Ealert%285762%29%3C%2Fscript%3E HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
LFR_SESSION_STATE_116486=1715073208993; _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
LFR_SESSION_STATE_20099=1715073020896; _ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0;
_ga=GA1.1.128297136.1599395143; _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEalliOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZ1eHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty


HTTP/1.1 400
Connection: close
Content-Length: 141
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Set-Cookie: JSESSIONID=971D6D39CAC0361C80C9633110A521DE; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 09:58:15 GMT
Content-Type: application/json

{
```

```
"status": "BAD_REQUEST",

"title": "For input string: \">\"'><script>alert(5762)</script>\"",

"type": "NumberFormatException"

}
```

Issue 4 of 9

TOC

Unsanitized user input reflected in JSON

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/js_resolve_modules
Entity:	modules (Global)
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Reasoning: The test result seems to indicate a vulnerability because the Global Validation feature found an embedded script in the response, which was probably injected by a previous test.

Test Requests and Responses:

```
GET /o/js_resolve_modules?modules=frontend-js-alert-support-
web%402.0.13%2Findex%3Cscript%3Ealert%286971%29%3C%2Fscript%3E HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/individual-registeration
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
_ga=GA1.1.128297136.1599395143; LFR_SESSION_STATE_20099=1715071585564;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; COOKIE_SUPPORT=true;
GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Accept: */*
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty


HTTP/1.1 200
Connection: keep-alive
Content-Length: 194
X-Content-Type-Options: nosniff
Keep-Alive: timeout=20
Cache-Control: private
Cache-Control: no-cache
ETag: W/"d18b97c3-14f5-489a-90fa-791afa57880a"
```

```
Set-Cookie: JSESSIONID=DBF6E5E2F43E23BDCC2178B73EB4FA4E; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 10:33:35 GMT
Content-Type: application/json;charset=UTF-8

{
 "pathMap": {

 },
 "configMap": {

 },
 "resolvedModules": [

 ],
 "moduleMap": {

 },
 "errors": [
         "Missing required module 'frontend-js-alert-support-
web@2.0.13\/index<script>alert(6971)<\/script>'"
 ],
 "moduleFlags": {

        }
}
```

Issue 5 of 9

TOC

Unsanitized user input reflected in JSON

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/mcit-registration/v1.0/individualRegistration
Entity:	->"gender" (Global)
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Reasoning: The test result seems to indicate a vulnerability because the Global Validation feature found an embedded script in the response, which was probably injected by a previous test.

Test Requests and Responses:

```
POST /o/mcit-registration/v1.0/individualRegistration HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/individual-registeration/
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0; _ga=GA1.1.128297136.1599395143;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_20099=1715072401645;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0; COOKIE_SUPPORT=true;
GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
```

```
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1266
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "firstName": "appscan",
 "firstNameAr": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "lastNameAr": "\u062a\u0633\u062a",
 "lastName": "test",
 "birthDate": "05-01-2024",
 "gender": "       <script>alert(7101)</script>",
 "nationalityCode": "7",
 "currentCountryCode": "a5850948-fc7e-ee11-a46d-000d3a2df947",
 "cityCode": "",
 "identityId": "11122324",
 "identityType": 753240002,
 "userType": 1,
 "recaptchaResponse":
"03AFcWeA5mBe1lXrnrT8saLAPe3vE167CAe3LvbRrPeWbWd0d8fLJaLv_V4RcbyjlHWuPSMV1Kpu_lgxM9hIXpZlypL55qZR
y-PCv1pd8mOwWAVF0FqepBF2DNPHyaut01vfREz1cZOyblEI2jOVfSLmVku2fNkVzR-
xCUsh8cd7RegyCD1RR2lLcXbyreZDXwt0lUjDn5w2L9BHTclNmCmlv751IBkU04Fu8GRlCtEjQM9VGfgs_VuHUuXnBqB570Gx
nFMB84MYSF8_-ZDDAFQEa5nCrAJ6jm5ny_djdkz47R4PKFqS4SCLp9mZ_-8bllp-
AOX73ZpwEWMug8uhm4bDLlQNJnnpH0KfShzxrLMArkmfbCVndFFTqzBIg2qRj0RKl2sZbVbDx97Rcz44HDn_N84zbUi6U5S2n
Ms1fFwOnONy12Me00AvNNGfApEofZhrjOUwIA02N8a5_32eQebu3LJtyW9ro3qwOVHtLEOjsYZrY3rgLgVdtsgeC6jucda1Nk
jRM6A5DJYrg2HBCLliWqXwddiTewpsbNr9ULk6kdTgms65DUxjERTwz0vIi7zOlup_bAlmJntJvKBuZ-9WV-
PFbdJO9vZqFnOSEtbD_37m2XlvlF-ukTm66FGrKwy3ggdIXwRbpCOK39ek2of7LGZdqh50205PS_E-
tSWz4BPfqEkYsyiuztBeyCJq-6EBJaqbvL3sn_fEkPolRjUFDPWm3Ke7y1Ow",
 "password": "P@ssw0rd",
 "re-password": "P@ssw0rd",
 "isNafazAccount": false,
 "email": "vepapi2863@rehezb.com",
 "mobilePhone": "+966 11 888 6660",
 "locale": "ar_SA"
}

HTTP/1.1 400
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 524
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=DC03BE333FC480C6D92550E989BEC04C; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 10:34:42 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"detail": "Cannot deserialize value of type `java.lang.Boolean` from String \"<script>alert(7101)
</script>\": only \"true\" or \"false\" recognized\n at [Source:
(org.apache.cxf.transport.http.AbstractHTTPDestination$1); line: 1, column: 163] (through
reference chain: com.linkdev.mcit.registration.dto.v1_0.UserObject[\"gender\"])",

"status": "BAD_REQUEST",

"title": "Unable to map JSON path \"gender\" with value \"<script>alert(7101)</script>\" to class
\"Boolean\"",

"type": "InvalidFormatException"

}
```

Issue 6 of 9

TOC

Unsanitized user input reflected in JSON

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/mcit-registration/v1.0/individualRegistration
Entity:	->"isNafazAccount" (Global)
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Reasoning: The test result seems to indicate a vulnerability because the Global Validation feature found an embedded script in the response, which was probably injected by a previous test.

Test Requests and Responses:

```
POST /o/mcit-registration/v1.0/individualRegistration HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/individual-registeration/
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0; _ga=GA1.1.128297136.1599395143;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_20099=1715072401645;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0; COOKIE_SUPPORT=true;
GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1265
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "firstName": "appscan",
 "firstNameAr": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "lastNameAr": "\u062a\u0633\u062a",
 "lastName": "test",
 "birthDate": "05-01-2024",
 "gender": true,
 "nationalityCode": "7",
 "currentCountryCode": "a5850948-fc7e-ee11-a46d-000d3a2df947",
 "cityCode": "",
 "identityId": "11122324",
 "identityType": 753240002,
 "userType": 1,
 "recaptchaResponse":
"03AFcWeA5mBel1XrnrT8saLAPe3vE167CAe3LvbRrPeWbWd0d8fLJaLv_V4RcbyjlHWuPSMV1Kpu_lgxM9hIXpZlypL55qZR
y-PCv1pd8mOwWAVF0FqepBF2DNPHyaut01vfREz1cZOyblEI2jOVfSLmVku2fNkVzR-
xCUsh8cd7RegyCD1RR2lLcXbyreZDXwt0lUjDn5w2L9BHTclNmCmlv751IBkU04Fu8GRlCtEjQM9VGfgs_VuHUuXnBqB570Gx
nFMB84MYSF8_-ZDDAFQEa5nCrAJ6jm5ny_djdkz47R4PKFqS4SCLp9mZ_-8bllp-
AOX73ZpwEWMug8uhm4bDLlQNJnnpH0KfShzxrLMArkmfbCVndFFTqzBIg2qRj0RKl2sZbVbDx97Rcz44HDn_N84zbUi6U5S2n
Ms1fFwOnONy12Me00AvNNGfApEofZhrjOUwIA02N8a5_32eQebu3LJtyW9ro3qwOVHtLEOjsYZrY3rgLgVdtsgeC6jucda1Nk
jRM6A5DJYrg2HBCLliWqXwddiTewpsbNr9ULk6kdTgms65DUxjERTwz0vIi7zOlup_bAlmJntJvKBuZ-9WV-
PFbdJO9vZqFnOSEtbD_37m2XlvlF-ukTm66FGrKwy3ggdIXwRbpCOK39ek2of7LGZdqh50205PS_E-
tSWz4BPfqEkYsyiuztBeyCJq-6EBJaqbvL3sn_fEkPolRjUFDPWm3Ke7ylOw",
 "password": "P@ssw0rd",
```

```
 "re-password": "P@ssw0rd",
 "isNafazAccount": "       <script>alert(7331)</script>",
 "email": "vepapi2863@rehezb.com",
 "mobilePhone": "+966 11 888 6660",
 "locale": "ar_SA"
}

HTTP/1.1 400
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 541
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=BBAA6828D3600806E49D8A237C50E9F2; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 10:36:02 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"detail": "Cannot deserialize value of type `java.lang.Boolean` from String \"<script>alert(7331)
</script>\": only \"true\" or \"false\" recognized\n at [Source:
(org.apache.cxf.transport.http.AbstractHTTPDestination$1); line: 1, column: 1153] (through
reference chain: com.linkdev.mcit.registration.dto.v1_0.UserObject[\"isNafazAccount\"])",

"status": "BAD_REQUEST",

"title": "Unable to map JSON path \"isNafazAccount\" with value \"<script>alert(7331)</script>\"
to class \"Boolean\"",

"type": "InvalidFormatException"

}
```

Issue 7 of 9

TOC

Unsanitized user input reflected in JSON	
Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/mcit-registration/v1.0/individualRegistration
Entity:	->"userType" (Global)
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Reasoning: The test result seems to indicate a vulnerability because the Global Validation feature found an embedded script in the response, which was probably injected by a previous test.

Test Requests and Responses:

```
POST /o/mcit-registration/v1.0/individualRegistration HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
```

```
Referer: https://mcit-liferayqc.linkdev.com/individual-registeration/
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0; _ga=GA1.1.128297136.1599395143;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0; LFR_SESSION_STATE_20099=1715072401645;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0; COOKIE_SUPPORT=true;
GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 1269
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "firstName": "appscan",
 "firstNameAr": "\u0627\u0628\u0633\u0643\u0627\u0646",
 "lastNameAr": "\u062a\u0633\u062a",
 "lastName": "test",
 "birthDate": "05-01-2024",
 "gender": true,
 "nationalityCode": "7",
 "currentCountryCode": "a5850948-fc7e-ee11-a46d-000d3a2df947",
 "cityCode": "",
 "identityId": "11122324",
 "identityType": 753240002,
 "userType": "       <script>alert(7247)</script>",
 "recaptchaResponse":
"03AFcWeA5mBel1XrnrT8saLAPe3vE167CAe3LvbRrPeWbWd0d8fLJaLv_V4RcbyjlHWuPSMV1Kpu_lgxM9hIXpZlypL55qZR
y-PCv1pd8mOwWAVF0FqepBF2DNPHyaut01vfREz1cZOyblEI2jOVfSLmVku2fNkVzR-
xCUsh8cd7RegyCD1RR2lLcXbyreZDXwt0lUjDn5w2L9BHTclNmCmlv751IBkU04Fu8GRlCtEjQM9VGfgs_VuHUuXnBqB570Gx
nFMB84MYSF8_-ZDDAFQEa5nCrAJ6jm5ny_djdkz47R4PKFqS4SCLp9mZ_-8bllp-
AOX73ZpwEWMug8uhm4bDLlQNJnnpH0KfShzxrLMArkmfbCVndFFTqzBIg2qRj0RKl2sZbVbDx97Rcz44HDn_N84zbUi6U5S2n
Ms1fFwOnONy12Me00AvNNGfApEofZhrjOUwIA02N8a5_32eQebu3LJtyW9ro3qwOVHtLEOjsYZrY3rgLgVdtsgeC6jucda1Nk
jRM6A5DJYrg2HBCLliWqXwddiTewpsbNr9ULk6kdTgms65DUxjERTwz0vIi7zOlup_bAlmJntJvKBuZ-9WV-
PFbdJO9vZqFnOSEtbD_37m2XlvlF-ukTm66FGrKwy3ggdIXwRbpCOK39ek2of7LGZdqh50205PS_E-
tSWz4BPfqEkYsyiuztBeyCJq-6EBJaqbvL3sn_fEkPolRjUFDPWm3Ke7ylOw",
 "password": "P@ssw0rd",
 "re-password": "P@ssw0rd",
 "isNafazAccount": false,
 "email": "vepapi2863@rehezb.com",
 "mobilePhone": "+966 11 888 6660",
 "locale": "ar_SA"
}

HTTP/1.1 400
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 528
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=D0DEF4078436170FB88E5CD3F709973F; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 10:35:35 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"detail": "Cannot deserialize value of type `java.lang.Integer` from String \"<script>alert(7247)
</script>\": not a valid `java.lang.Integer` value\n at [Source:
(org.apache.cxf.transport.http.AbstractHTTPDestination$1); line: 1, column: 324] (through
reference chain: com.linkdev.mcit.registration.dto.v1_0.UserObject[\"userType\"])",

"status": "BAD_REQUEST",

"title": "Unable to map JSON path \"userType\" with value \"<script>alert(7247)</script>\" to
class \"Integer\"",

"type": "InvalidFormatException"
```

```
}
```

Issue 8 of 9

TOC

Unsanitized user input reflected in JSON

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/mcit-forgot-password/v1.0/forgot-password
Entity:	->"userType" (Global)
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Reasoning: The test result seems to indicate a vulnerability because the Global Validation feature found an embedded script in the response, which was probably injected by a previous test.

Test Requests and Responses:

```
POST /o/mcit-forgot-password/v1.0/forgot-password HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/forgot-password/
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: LFR_SESSION_STATE_20099=1715072894528;
_ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
_ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0;
_ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
_ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0; _ga=GA1.1.128297136.1599395143;
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
COOKIE_SUPPORT=true; GUEST_LANGUAGE_ID=ar_SA; JSESSIONID=CB89AFEC0BE460CC720DF1E03F3740DF
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 834
Accept: application/json, text/plain, */*
Origin: https://mcit-liferayqc.linkdev.com
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty
Content-Type: application/json

{
 "email": "vepapi2863@rehezb.com",
 "registerNumber": "",
 "userType": "       <script>alert(7397)</script>",
 "recaptcha_token": "03AFcWeA4vldQH_9UnA5U-
qiyvh1wNaAqyp6P2mW7y2zdT4cfnsNCTv3pXUCmN5qszHmI4GFn8hUgxXY6PLXY5eQ2_62qdklxR_CXTjbKZ7xCw2Zmr6pnsE
v5BOUZDY8yqJBtHGyZsjD2pJFnA_ByQyC-
ZqOSkhxpP7Fw1cbF9u14SKAod__c1hngNDIyNagXlAn6CrijXYidLxcQDiRHU_gv639-
0LOnUJjS6rA2IhZaWGabxQdwnZQxnB_UwAHT3GEEUxbb-CfHj9nh4oSUTMCRzN34jM-n1j8-80KV-j6GKBdvsiT49A3BJH2-
Rh0R3sRBa53IGv1EbBVN22rldXfvR9Cj82qj_oYOelBsritzaZ9aOuwZHV9BL5y8YrZqOZrUijNwAqnOTbLDNcqE0TZrNg0R3
oBgkJ5VNkBom9GGIm1t5w_WhoSIxUX2khce8kggXZDgSaqCCO74F5bL3wO1dzgeRt90aIHczAfE8Udx49rDacXQI1ckMPGGed
pwrhKAPC94QBcI2OBLA4SlGoCNqaj47r3bjr0NJx5IShJ7epOFUlsCHhMRH_Pun-
9BaaYLcU7SAJ9yXza6qpgHhvTTbOygMZiR8a1XRFq16b3lMK8g2xAcGMBWkn4HfYuD-
```

```
LLEBsoBj6VW5_LBTdtcKm5GDr7G5SOIG8kmD6WWqCQ2WO8y84pEz2fju0xrZlpV4SJQKNfzb1XGc"
}

HTTP/1.1 400
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://mcit-liferayqc.linkdev.com
Content-Length: 540
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Access-Control-Allow-Headers: *
Set-Cookie: JSESSIONID=16366D4E740967CD54F4ACC632A83D98; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 10:36:31 GMT
Access-Control-Allow-Methods: *
Content-Type: application/json

{

"detail": "Cannot deserialize value of type `java.lang.Integer` from String \"<script>alert(7397)
</script>\": not a valid `java.lang.Integer` value\n at [Source:
(org.apache.cxf.transport.http.AbstractHTTPDestination$1); line: 1, column: 65] (through
reference chain: com.linkdev.mcit.forgot.password.dto.v1_0.ForgotPasswordObject[\"userType\"])",

"status": "BAD_REQUEST",

"title": "Unable to map JSON path \"userType\" with value \"<script>alert(7397)</script>\" to
class \"Integer\"",

"type": "InvalidFormatException"

}
```

Issue 9 of 9

TOC

Unsanitized user input reflected in JSON

Severity:	Informational
CVSS Score:	0.0
URL:	https://mcit-liferayqc.linkdev.com/o/c/recruitmentapplicationtypes
Entity:	pageSize (Global)
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Reasoning: The test result seems to indicate a vulnerability because the Global Validation feature found an embedded script in the response, which was probably injected by a previous test.

Test Requests and Responses:

```
GET /o/c/recruitmentapplicationtypes?
restrictFields=creator,actions&pageSize=100000%3Cscript%3Ealert%287713%29%3C%2Fscript%3E HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0.0 Safari/537.36
Referer: https://mcit-liferayqc.linkdev.com/recruitment?isFresh=true
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Cookie: _ga_QYNNTJQ6GM=GS1.1.1713806037.3.0.1713806037.0.0.0;
```

```
__gsas=ID=1755b564f4af5420:T=1701520365:RT=1701520365:S=ALNI_MaTXOVHpKBwLrX-ZDNGS8OTIECFDg;
LFR_SESSION_STATE_116486=1715073208993; _ga_KLXX5BX6KP=GS1.2.1705399938.13.1.1705400542.0.0.0;
LFR_SESSION_STATE_20099=1715073020896; _ga_07TBBJNX97=GS1.1.1705405770.19.0.1705405770.0.0.0;
_ga=GA1.1.128297136.1599395143; _ga_N1TBFH7DS6=GS1.1.1702916994.4.1.1702918479.0.0.0;
COOKIE_SUPPORT=true; ID=78692f674d56476771344b754c46314878394f5043513d3d;
GUEST_LANGUAGE_ID=ar_SA;
LiferayJWTToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMTY0ODYiLCJyb2xlcyI6W3t9LHt9XSwi
bmFtZSI6ImFwcHNjYW4iLCJwdWJsaWNLZXkiOiJNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQ
WdKUWl3RVV3Z1kwWFNNeDgwU0pYMzMyckluUXcxYVZOQ3laV1d3S21NTEVtWFo5NHl2Q1Rmb21KNkRjYktSeldMaDdwWU5YVj
NxZU9sYVNqOGl4SjhyRkh2bU45SXhGK0ptR2NENkdjZys0M2lqc3JjSVBWd25EcjlzbmxlZnJnYXozR3JtTCtVenNYdStTOWd
OVWZzcG1sbzVhRXJVTkJEa1liOWVlN0FqZDhUeVV4WnlkaFZDWUZGNmJZXC8xenFrOHFGcXZLekNcL2RaOVp1ZDNBc3dPZ2tO
MkdidTI5c2xWUnJVSHNcLzJxOUFDU3ZLcXF1NVwveTBuU2JiRmRnc1BiY2xrbll0b0M0SzJFejNCUVNDYkdRRVppZ2NEdHRrO
WRWU1pQTUdLdFduczZleHZpMkpGeCszR2JMK1VZM1RiWWl1KzBSZVQ4SGlDaThBQ0NWR3piR3dJREFRQUIiLCJleHAiOjE3MT
UwNzMzNzAsImVtYWlsIjoidmVwYXBpMjg2M0ByZWhlemIuY29tIn0.Su2RAp0fTmyt3hVNREylsLS1DF7VKVOq_acAVYWR--
I-
GZFw7giz17d2vmGXnmc_trPTi01r0pDujkPfvgwBiinYcUmM41MEaBgFK1x9BrdBA4UrNAhZtmUelDlR559E2YNOpOqFH0f7Z
8WbFWoFCLJAFUOgKAOnJU_aUH7ooVh95L0T3EgaiK4otF1YVv64h528vIE7n_jIil_DK9RfXBNf1PO33w0PT5B4uDVPAAJNpL
8Wq_bivgBYpzfq5FbxlYU0Oq6FF5V-mz5G-
TbFuiOYaMEDZXPO4tuw6bVbbaSxuyuIYLfaAThEPZdfDt0uqWn092HTHgVX1OIrUy-j4A;
JSESSIONID=7BD2E866456FB3087B3CA0539AD839EF; COMPANY_ID=20096
Connection: keep-alive
Host: mcit-liferayqc.linkdev.com
Sec-Fetch-Mode: cors
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Dest: empty


HTTP/1.1 400
Connection: close
Content-Length: 142
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Set-Cookie: JSESSIONID=0241CB020D8D547A7621DB260BADA2D3; Path=/; Secure; HttpOnly
Date: Tue, 07 May 2024 10:50:44 GMT
Content-Type: application/json

{

"status": "BAD_REQUEST",

"title": "For input string: \"100000<script>alert(7713)</script>\"",

"type": "NumberFormatException"

}
```