**25Q2 CSOC Helpdesk-dev.zalaris.com Manual**

**Penetration Test June 11**

PREPARED BY:

Mohammed Sharoz

REVIEWED BY:

Diwakar Thanikachalam

SIGNED-OFF BY:

Name Middle Lastname

### Introduction:

The applications that are owned or used within Zalaris are actively tested for vulnerability using automated scan followed by manual Pen-test of the report. The scan is done twice within a week for a duration of four weeks.

# 

Table of Contents

[Introduction: 2](#_Toc13115)

[2025 Q2 CSOC Manual Penetration test of Alumni Portal 3](#_Toc19788)

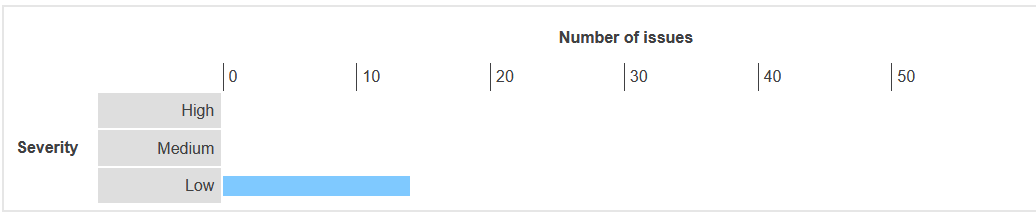
[Executive Summary 3](#_Toc15116)

[Cross Site Request Forgery: 4](#_Toc17574)

### 2025 Q2 CSOC Manual Penetration test of Alumni Portal

### Executive Summary

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level, and the bars fade as the confidence level falls.



### Client SIde JSON Injection (DOM Based):

**Category:** Low

|  |  |
| --- | --- |
| Type |  |
| Status |  |

**Description**

Reflection of input arises when data is copied from a request and echoed into the application's immediate response.

**Links Tested**

|  |
| --- |
| * Sample Links goes here |

Steps:

* Eigeben Schritte heir

[Konvertieren Screenshot geht hier]

Content

|  |
| --- |
|  |

**WORKLOG**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| When | What | Who | Recommended Action | Action plan |
|  |  |  |  |  |

### Cookie Manipulation (DOM Based):

**Category:** Low

|  |  |
| --- | --- |
| Type |  |
| Status |  |

**Description**

Reflection of input arises when data is copied from a request and echoed into the application's immediate response.

**Links Tested**

|  |
| --- |
| * Sample Links goes here |

Steps:

* Eigeben Schritte heir

[Konvertieren Screenshot geht hier]

Content

|  |
| --- |
|  |

**WORKLOG**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| When | What | Who | Recommended Action | Action plan |
|  |  |  |  |  |

### Cross site scripting (Stored):

**Category:** Low

|  |  |
| --- | --- |
| Type |  |
| Status |  |

**Description**

Reflection of input arises when data is copied from a request and echoed into the application's immediate response.

**Links Tested**

|  |
| --- |
| * Sample Links goes here |

Steps:

* Eigeben Schritte heir

[Konvertieren Screenshot geht hier]

Content

|  |
| --- |
|  |

**WORKLOG**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| When | What | Who | Recommended Action | Action plan |
|  |  |  |  |  |

### Cross site scripting (Reflected):

**Category:** Low

|  |  |
| --- | --- |
| Type |  |
| Status |  |

**Description**

Reflection of input arises when data is copied from a request and echoed into the application's immediate response.

**Links Tested**

|  |
| --- |
| * Sample Links goes here |

Steps:

* Eigeben Schritte heir

[Konvertieren Screenshot geht hier]

Content

|  |
| --- |
|  |

**WORKLOG**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| When | What | Who | Recommended Action | Action plan |
|  |  |  |  |  |

### External Service Interaction(DNS):

**Category:** Low

|  |  |
| --- | --- |
| Type |  |
| Status |  |

**Description**

Reflection of input arises when data is copied from a request and echoed into the application's immediate response.

**Links Tested**

|  |
| --- |
| * Sample Links goes here |

Steps:

* Eigeben Schritte heir

[Konvertieren Screenshot geht hier]

Content

|  |
| --- |
|  |

**WORKLOG**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| When | What | Who | Recommended Action | Action plan |
|  |  |  |  |  |

### User Agent Dependent Response:

**Category:** Low

|  |  |
| --- | --- |
| Type |  |
| Status |  |

**Description**

Reflection of input arises when data is copied from a request and echoed into the application's immediate response.

**Links Tested**

|  |
| --- |
| * Sample Links goes here |

Steps:

* Eigeben Schritte heir

[Konvertieren Screenshot geht hier]

Content

|  |
| --- |
|  |

**WORKLOG**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| When | What | Who | Recommended Action | Action plan |
|  |  |  |  |  |

### Input Returned in Response(Stored)

**Category:** Low

|  |  |
| --- | --- |
| Type |  |
| Status |  |

**Description**

Reflection of input arises when data is copied from a request and echoed into the application's immediate response.

**Links Tested**

|  |
| --- |
| * Sample Links goes here |

Steps:

* Eigeben Schritte heir

[Konvertieren Screenshot geht hier]

Content

|  |
| --- |
|  |

**WORKLOG**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| When | What | Who | Recommended Action | Action plan |
|  |  |  |  |  |

### Input Returned in Response (Reflected):

**Category:** Low

|  |  |
| --- | --- |
| Type |  |
| Status |  |

**Description**

Reflection of input arises when data is copied from a request and echoed into the application's immediate response.

**Links Tested**

|  |
| --- |
| * Sample Links goes here |

Steps:

* Eigeben Schritte heir

[Konvertieren Screenshot geht hier]

Content

|  |
| --- |
|  |

**WORKLOG**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| When | What | Who | Recommended Action | Action plan |
|  |  |  |  |  |

### Frame-able Response (Potential Click jacking):

**Category:** Low

|  |  |
| --- | --- |
| Type | False Positive |
| Status | Tested and confirmed as False positive no action needed |

**Description**

If a page fails to set an appropriate X-Frame-Options or Content-Security-Policy HTTP header, it might be possible for a page controlled by an attacker to load it within an iframe. This may enable a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. By inducing victim users to perform actions such as mouse clicks and keystrokes, the attacker can cause them to unwittingly carry out actions within the application that is being targeted. This technique allows the attacker to circumvent defenses against cross-site request forgery, and may result in unauthorized actions.

Note that some applications attempt to prevent these attacks from within the HTML page itself, using "framebusting" code. However, this type of defense is normally ineffective and can usually be circumvented by a skilled attacker.

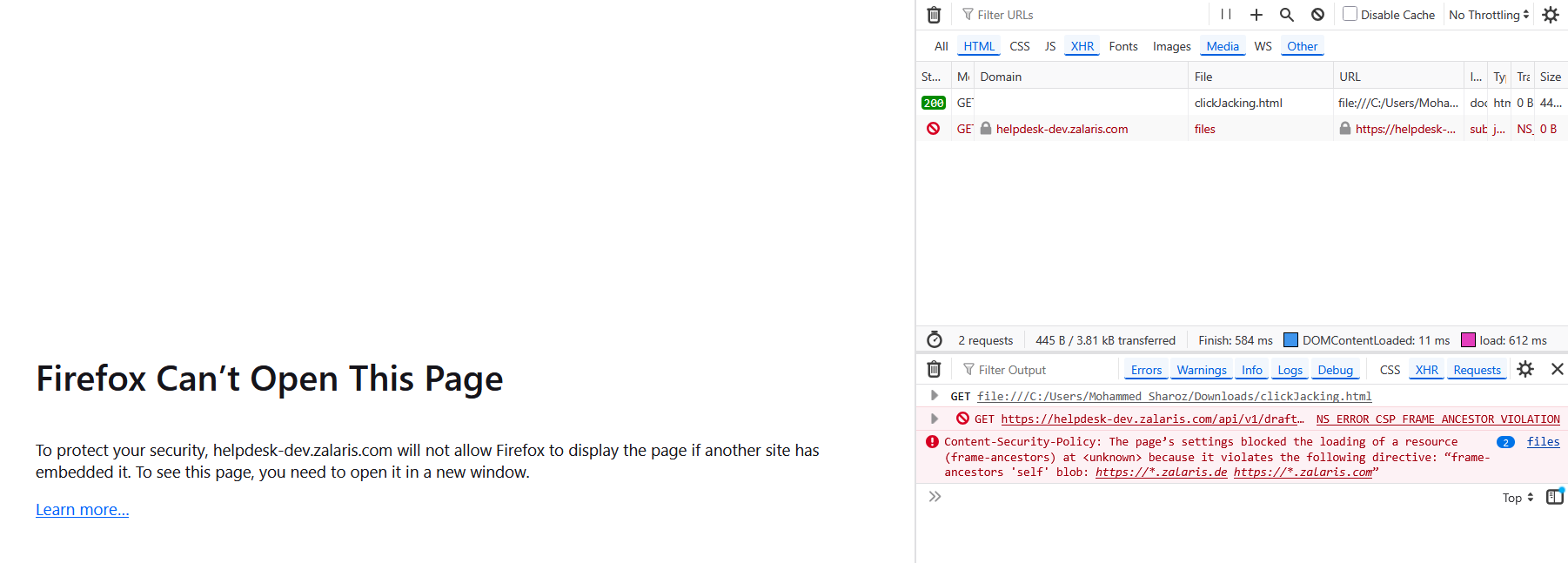
You should determine whether any functions accessible within frameable pages can be used by application users to perform any sensitive actions within the application.

**Links Tested**

|  |
| --- |
| * / |

Steps:

* Access the path helpdesk-dev.zalaris.com/510
* Capture the request using burp proxy and analyze the response headers
* The application has X-Frame-Options header set with the value “DENY”
* Also the CSP has security policy set so that application does not load in a any frame whether the ancestors [current frame] that requests for he resource to be loaded in the iframe is not ‘zalaris.com’
* The screenshot for the same is attached below



* A
* The content Security Policy for Helpdesk is given below and the frame-ancestor value for the same is highlighted

|  |
| --- |
| Content-Security-Policy: default-src 'unsafe-inline' 'self' blob: \*.zalaris.de \*.zalaris.com https://s3.scriptcdn.net/cdn/c7fa7451-6f95-4815-ac32-b8cc2537837a https://login.microsoftonline.com/ https://dzudiostorage.blob.core.windows.net/ \*.b2clogin.com https://pzudiostorage.blob.core.windows.net/ https://northeurope-2.in.applicationinsights.azure.com/v2/track https://\*.in.applicationinsights.azure.com https://helpdesk-dev.zalaris.com https://alhvbcpn2.accounts.cloud.sap https://ar2hdcts7.accounts.cloud.sap/ mypayslip-dev.zalaris.com mypayslip.zalaris.com; script-src 'self' \*.zalaris.de \*.zalaris.com https://s3.scriptcdn.net/cdn/c7fa7451-6f95-4815-ac32-b8cc2537837a https://login.microsoftonline.com/ https://dzudiostorage.blob.core.windows.net/ \*.b2clogin.com https://cdn.form.io/ace/1.4.12/mode-html.js https://cdn.form.io/ace/1.4.12/mode-json.js https://cdn.form.io/flatpickr/flatpickr.min.js https://cdn.form.io/ace/1.4.10/ace.js https://cdn.form.io/ace/1.4.10/theme-xcode.js https://cdn.form.io/ace/1.4.10/mode-html.js https://cdn.form.io/ace/1.4.10/mode-json.js https://cdn.form.io/ace/1.4.10/worker-html.js https://cdn.form.io/ace/1.4.10/worker-json.js https://pzudiostorage.blob.core.windows.net/ https://northeurope-2.in.applicationinsights.azure.com/v2/track https://cdn.form.io/flatpickr-formio/4.6.13-formio.3/l10n/; img-src 'self' \*.zalaris.de \*.zalaris.com data: dzudiostorage.blob.core.windows.net https://pzudiostorage.blob.core.windows.net/; style-src 'unsafe-inline' 'self' \*.zalaris.de \*.zalaris.com https://s3.scriptcdn.net/cdn/c7fa7451-6f95-4815-ac32-b8cc2537837a https://dzudiostorage.blob.core.windows.net/ \*.b2clogin.com https://cdn.form.io/flatpickr/flatpickr.min.css https://pzudiostorage.blob.core.windows.net/ https://helpdesk-dev.zalaris.com/; media-src 'self' \*.zalaris.de \*.zalaris.com https://s3.scriptcdn.net/cdn/c7fa7451-6f95-4815-ac32-b8cc2537837a https://dzudiostorage.blob.core.windows.net/ \*.b2clogin.com https://pzudiostorage.blob.core.windows.net/ https://northeurope-2.in.applicationinsights.azure.com/v2/track; font-src 'self' \*.zalaris.de \*.zalaris.com https://s3.scriptcdn.net/cdn/c7fa7451-6f95-4815-ac32-b8cc2537837a https://alumnidev.b2clogin.com/alumnidev.onmicrosoft.com/ https://login.microsoftonline.com/ https://dzudiostorage.blob.core.windows.net/ data: https://pzudiostorage.blob.core.windows.net/ https://northeurope-2.in.applicationinsights.azure.com/v2/track; frame-src 'self' blob: \*.zalaris.de \*.zalaris.com https://s3.scriptcdn.net/cdn/c7fa7451-6f95-4815-ac32-b8cc2537837a https://login.microsoftonline.com/ https://dzudiostorage.blob.core.windows.net/ \*.b2clogin.com https://pzudiostorage.blob.core.windows.net/ https://view.officeapps.live.com/op/embed.aspx https://northeurope-2.in.applicationinsights.azure.com/v2/track mypayslip.zalaris.com mypayslip-dev.zalaris.com https://dzudiostorage.blob.core.windows.net https://zudioinnomotics.blob.core.windows.net/ https://view.officeapps.live.com blob:https://mypayslip.zalaris.com; frame-ancestors 'self' blob: \*.zalaris.de \*.zalaris.com; form-action 'self' \*.zalaris.de \*.zalaris.com https://s3.scriptcdn.net/cdn/c7fa7451-6f95-4815-ac32-b8cc2537837a https://login.microsoftonline.com/ https://dzudiostorage.blob.core.windows.net/ \*.b2clogin.com https://northeurope-2.in.applicationinsights.azure.com/v2/track; |

**WORKLOG**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| When | What | Who | Recommended Action | Action plan |
| 11 June 2025 | Frame-able Response (Potential Click-jacking) is manually tested | CSOC | No action needed. The following security Measures are set :  Frame ancestors set to load helpdesk only if the ancestor / current page where the frame is loaded is belongs to zalaris  The X-Frame-Options header are set to the value “DENY” in most pages  The configuration Frame ancestors together with the X-Frame-Options header prevents the site from loading inside an iframe | No Action Needed |

### HTML 5 Storage Manipulation(DOM Based):

**Category:** Low

|  |  |
| --- | --- |
| Type |  |
| Status |  |

**Description**

Reflection of input arises when data is copied from a request and echoed into the application's immediate response.

**Links Tested**

|  |
| --- |
| * Sample Links goes here |

Steps:

* Eigeben Schritte heir

[Konvertieren Screenshot geht hier]

Content

|  |
| --- |
|  |

**WORKLOG**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| When | What | Who | Recommended Action | Action plan |
|  |  |  |  |  |

### TLS Certificate:

**Category:** Low

|  |  |
| --- | --- |
| Type | Informational alert |
| Status | TLS Information are manually verified. No issues are found |

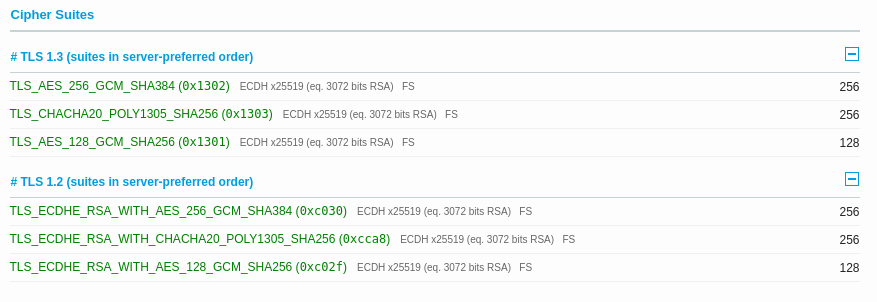
**Description**

The server presented a valid, trusted TLS certificate. This issue is purely informational.

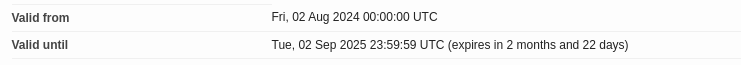
**Steps:**

* Access Qualys ssl labs : <https://www.ssllabs.com/ssltest/analyze.html?d=helpdesk-dev.zalaris.com>
* The following must be checked from the result obtained
  1. Cipher Suite Strength
  2. Certificate Validity
  3. Chain Issues

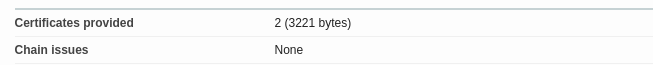
The cipher suite strength has no issues screenshot for the same is attached below



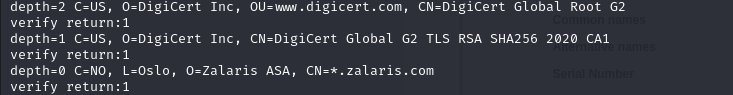
The Certificate has validity set till September 2nd 2025



No Chain issues are found .



Certificate chain verified via open\_ssl command no issue found. Screenshot for the same is attached below



**WORKLOG**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| When | What | Who | Recommended Action | Action plan |
|  |  |  |  |  |