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

**Penetration Test June 11**

kl

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 once a month

# 

Table of Contents

[Introduction: 2](#_Toc22723)

[2025 Q2 CSOC Manual Penetration test of Alumni Portal 4](#_Toc398)

[Executive Summary 4](#_Toc6086)

[Client SIde JSON Injection (DOM Based): 4](#_Toc18888)

[Cookie Manipulation (DOM Based): 5](#_Toc8816)

[Cross site scripting (Stored): 6](#_Toc9823)

[Cross site scripting (Reflected): 6](#_Toc8973)

[External Service Interaction(DNS): 7](#_Toc15617)

[User Agent Dependent Response: 8](#_Toc733)

[Input Returned in Response(Stored) 9](#_Toc27408)

[Input Returned in Response (Reflected): 10](#_Toc26195)

[Frame-able Response (Potential Click jacking): 10](#_Toc30053)

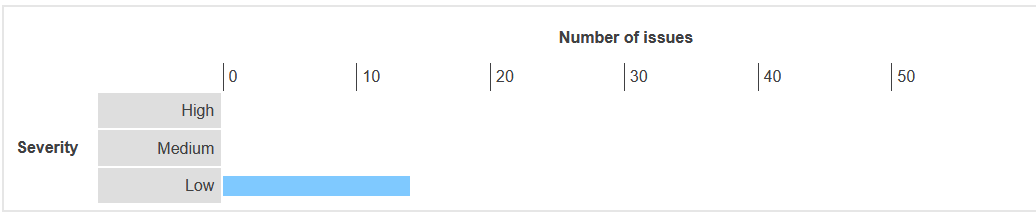
[HTML 5 Storage Manipulation(DOM Based): 13](#_Toc12365)

[TLS Certificate: 14](#_Toc18217)

### 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]

**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):

|  |  |
| --- | --- |
| Type | False Positive |
| Status | No action Needed the alert is false positive |

**Description**

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

**Links Tested**

|  |
| --- |
| * /api/v1/drafts?reporterId=1421414 |

Steps:

* Login into helpdesk-dev.zalaris.com/510
* Access the page reported with the Stored Cross Site Scripting and look for response. The Response contains

[Konvertieren Screenshot geht hier]

Content

|  |
| --- |
|  |

**WORKLOG**

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

### Cross site scripting (Reflected):

**Category:** Low

|  |  |
| --- | --- |
| Type | False Positive |
| Status | Have been added to back log for further testing |

**Description**

The value of the **size** request parameter is copied into the HTML document as plain text between tags. The payload **xz5ds<script>alert(1)</script>a9mey** was submitted in the size parameter. This input was echoed unmodified in the application's response.  
  
This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.  
  
The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

**Links Tested**

|  |
| --- |
| * /api/v1/tickets |

Steps:

* Login into Helpdesk-dev.zalaris.com/510
* Access the following page reported in the alert /api/v1/tickets?contactId=1421414&size=3xz5ds%3cscript%3ealert(1)%3c%2fscript%3ea9mey&sort=waitingForCustomer%2Cdesc&sort=lastChangedAt%2Cdesc
* Inject a script into the applications size parameter and forward the request look for the response. The response shows that the script is sanitized.
* The screenshot for the same is attached below



* The payload is reflected as a normal text and not executed as a Java Script

**WORKLOG**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| When | What | Who | Recommended Action | Action plan |
| 11 June 2025 | Manually Tested the reported Reflected XSS issue | CSOC | The Injected scripts are reflected in the response but, not executed as Java Scripts. Considering this alert as informational | Need further testing to break out of the sanitized area |

### External Service Interaction(DNS):

**Category:** Low

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

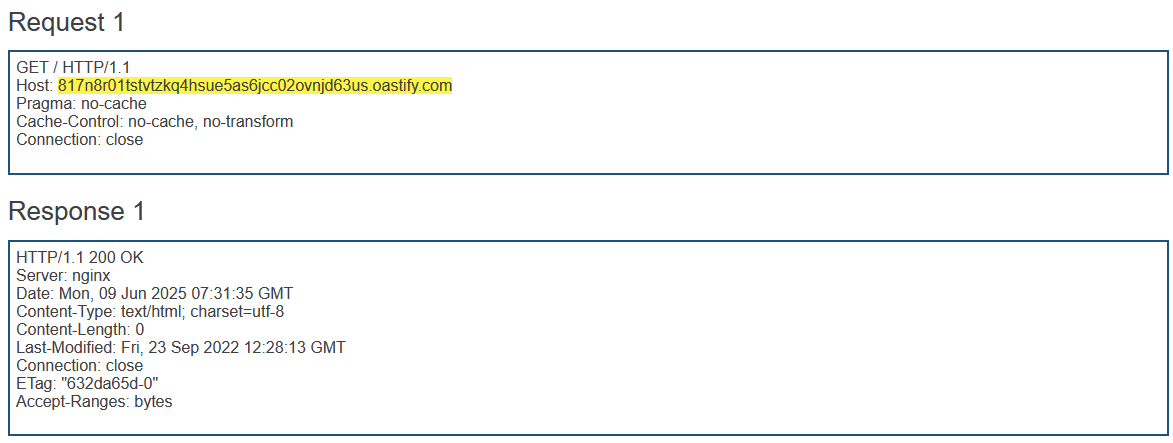
**Description**

It is possible to induce the application to perform server-side DNS lookups of arbitrary domain names.  
  
The payload **817n8r01tstvtzkq4hsue5as6jcc02ovnjd63us.oastify.com** was submitted in the SSL SNI value and the HTTP Host header.  
  
The application performed a DNS lookup of the specified domain.

**Links Tested**

|  |
| --- |
| * /country-flags/de.svg |

**Note:** The alert provided is false positive since the request was directly made to the burp collaborator. Screenshot for the same is attached below



But the path that is mentioned in the alert is /country-flags/de.svg which is not releveant to external DNS Interaction

**WORKLOG**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| When | What | Who | Recommended Action | Action plan |
| 12 June 2025 | External DNS Interaction Manually Tested | CSOC | No Action Needed. The Alert is False Positive | No Action Needed |

### User Agent Dependent Response:

**Category:** Low

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

**Description**

Application responses may depend systematically on the value of the User-Agent header in requests. This behavior does not itself constitute a security vulnerability, but may point towards additional attack surface within the application, which may contain vulnerabilities.

This behavior often arises because applications provide different user interfaces for desktop and mobile users. Mobile interfaces have often been less thoroughly tested for vulnerabilities such as cross-site scripting, and often have simpler authentication and session handling mechanisms that may contain problems that are not present in the full interface.

To review the interface provided by the alternate User-Agent header, you can configure a match/replace rule in Burp Proxy to modify the User-Agent header in all requests, and then browse the application in the normal way using your normal browser.

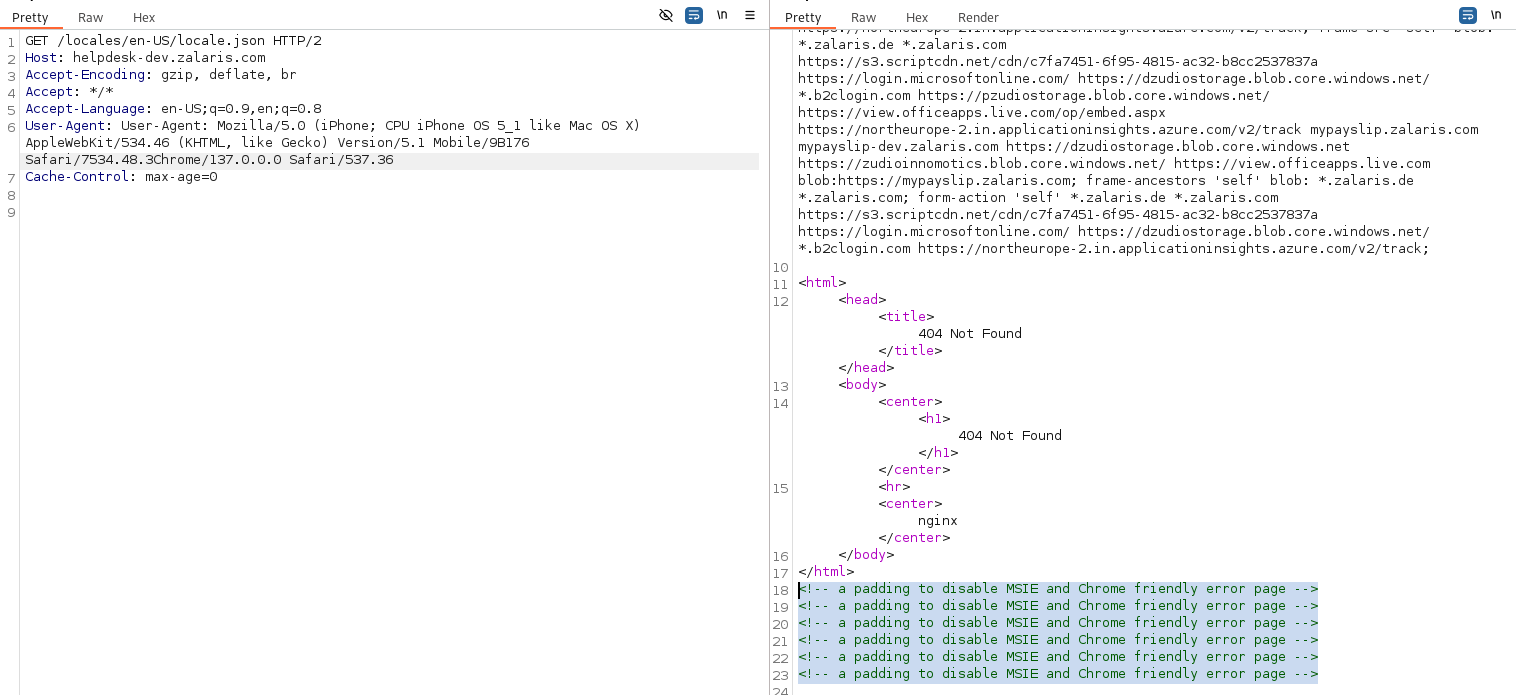
**Links Tested**

|  |
| --- |
| * **/locales/en-US/locale.json** |

Steps:

* Access the path reported with User Agent Dependent response
* The Response Varies according to the User Agent. The screenshot for the same is attached below





* This behavior is itself is not an issue since the User Agent Header is used to display or render the content to the user based on the device used . Still there needs to be User-Agent Based test that is needed to execute scripts such as Shell-Shock

**WORKLOG**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| When | What | Who | Recommended Action | Action plan |
| 11 June 2025 | Manually Tested the User Agent based attack reported in the mandatory Automated Audit | CSOC | The alert is just informational | Perform Injection attacks against the User agent header targeting the server or the application |

### 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.

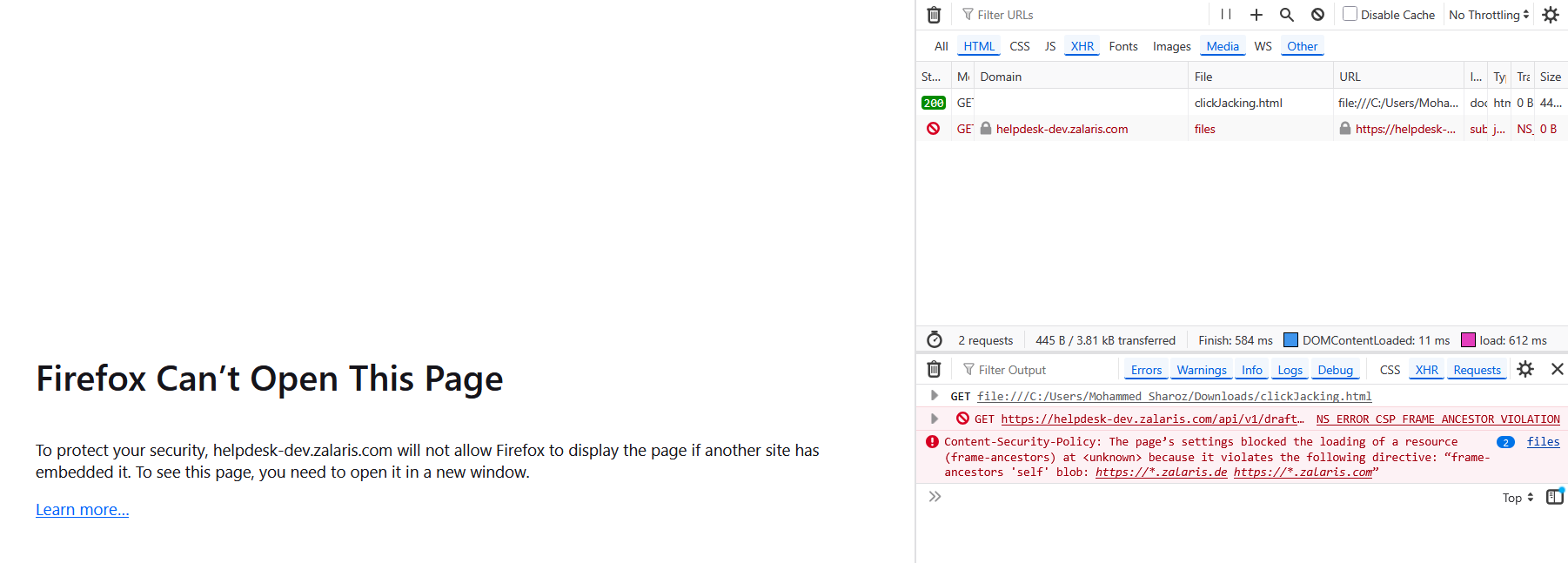
You should determine whether any functions accessible within frameable pages can be used by application users to perform any sensitive actions within the application.

**Links Tested**

|  |
| --- |
| * /510/tickets/new/sick-leave-certifikcate1 |

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



* 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**

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

HTML5 storage manipulation arises when a script stores controllable data in the HTML5 storage of the web browser (either localStorage or sessionStorage). An attacker may be able to use this behavior to construct a URL that, if visited by another application user, will cause the user's browser to store attacker-controllable data.

This behavior does not in itself constitute a security vulnerability. However, if the application later reads the data back from storage and processes it in an unsafe way, then an attacker may be able to leverage the storage mechanism to deliver other DOM-based attacks, such as cross-site scripting and JavaScript injection.

Burp Suite automatically identifies this issue using dynamic and static code analysis. Static analysis can lead to false positives that are not actually exploitable. If Burp Scanner has not provided any evidence resulting from dynamic analysis, you should review the relevant code and execution paths to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

**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 |

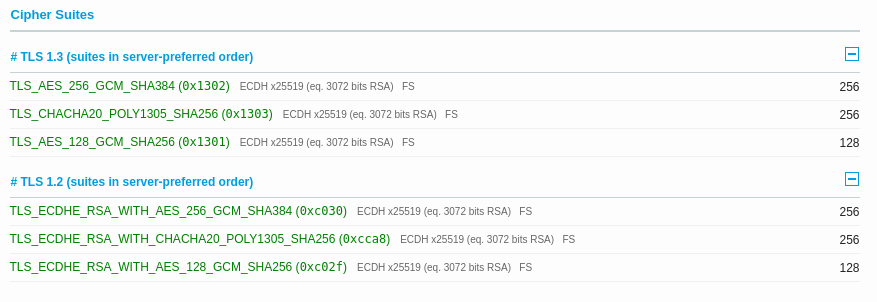
**Description**

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

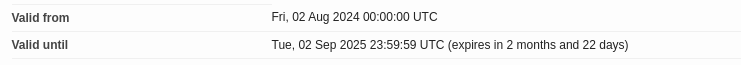
**Steps:**

* 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

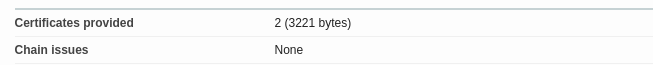
The cipher suite strength has no issues screenshot for the same is attached below



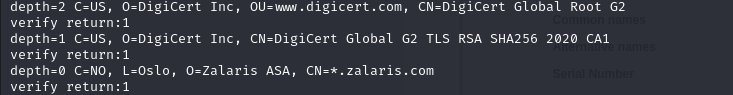
The Certificate has validity set till September 2nd 2025



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 |
| 10 June 2025 | Manually analyzed the TLS configuration for issues | CSOC | No Issues Found | No action needed |