**25Q2 CSOC Alumni-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)

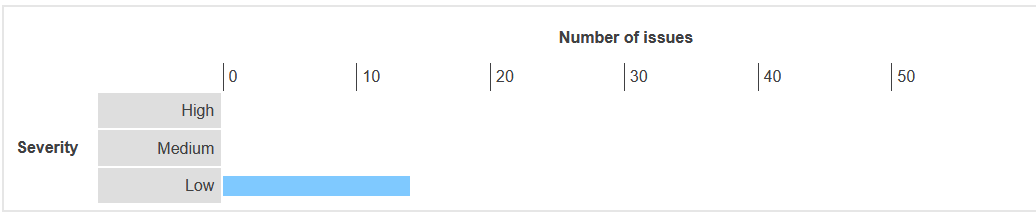
[Executive Summary 3](#_Toc15116)

[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.



### Content Security Policy: allowlisted script resources:

**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:

Enter Steps here

[Screenshot goes here r]

Content

|  |
| --- |
|  |

**WORKLOG**

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

### Content Security Policy:allow untrusted style execution

**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:

Enter Steps here

[Screenshot goes here r]

Content

|  |
| --- |
|  |

**WORKLOG**

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

### Content Security Policy allows clickjacking

**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:

Enter Steps here

[Screenshot goes here r]

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:

Enter Steps here

[Screenshot goes here r]

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:

Enter Steps here

[Screenshot goes here r]

Content

|  |
| --- |
|  |

**WORKLOG**

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

### Frame-able response (Potential Click-jacking)

**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:

Enter Steps here

[Screenshot goes here r]

Content

|  |
| --- |
|  |

**WORKLOG**

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

### HTML5 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:

Enter Steps here

[Screenshot goes here r]

Content

|  |
| --- |
|  |

**WORKLOG**

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

### Robots File

**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:

Enter Steps here

[Screenshot goes here r]

Content

|  |
| --- |
|  |

**WORKLOG**

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

### Cacheable HTTPS 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:

Enter Steps here

[Screenshot goes here r]

Content

|  |
| --- |
|  |

**WORKLOG**

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

### TLS Certificate

**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:

Enter Steps here

[Screenshot goes here r]

Content

|  |
| --- |
|  |

**WORKLOG**

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