1. Penetration test on DVWA

DVWA REPORT

PRATEEK BANSAL

DATE:17 JULY 2025

EMAIL:bansalp@rknec.edu

1.Penetration testing report

Table of contents

Executive summary 03

Attack narrative 04

Conclusion 13

Recommendation 13

Executive summary:

I have performed a penetration test on Damn Vulnerable Web Application (DVWA) to evaluate its vulnerabilities. The goal was to identify all vulnerabilities of DVWA and try to exploit the system and gain access to the application and report it to its admin for their safety.

My focus is to perform all attacks like bruteforce , sql injection , XSS ,upload etc so that I can identify that web application is vulnerable to which attack to access there sensivitive data by exploiting the system.

3.Penetration testing report

After auditing the security measure of the site DVWA I have find many vulnerabilities in it.It is highly vulnerable and its security measures are low.

Anyone can easily exploit the web application and gain access to their database. It is vulnerable to many attacks like:

1.It has upload feature which also accept risky files like .php or malicious files by that a person can gain access to their whole system.

2.It has weak login system that can be easily brute forced and a person gets login id and password of someone.

3.It is vulnerable to XSS also it accepts javascript code so a person can insert malicious javascript code to gain access or show unnecessary alert to user.

4.The site allows malicious files to be included, which could lead to data leak.

5.The site is also vulnerable to sql injection by that any person can get access to database which he can change or modify or misuse the user informations.

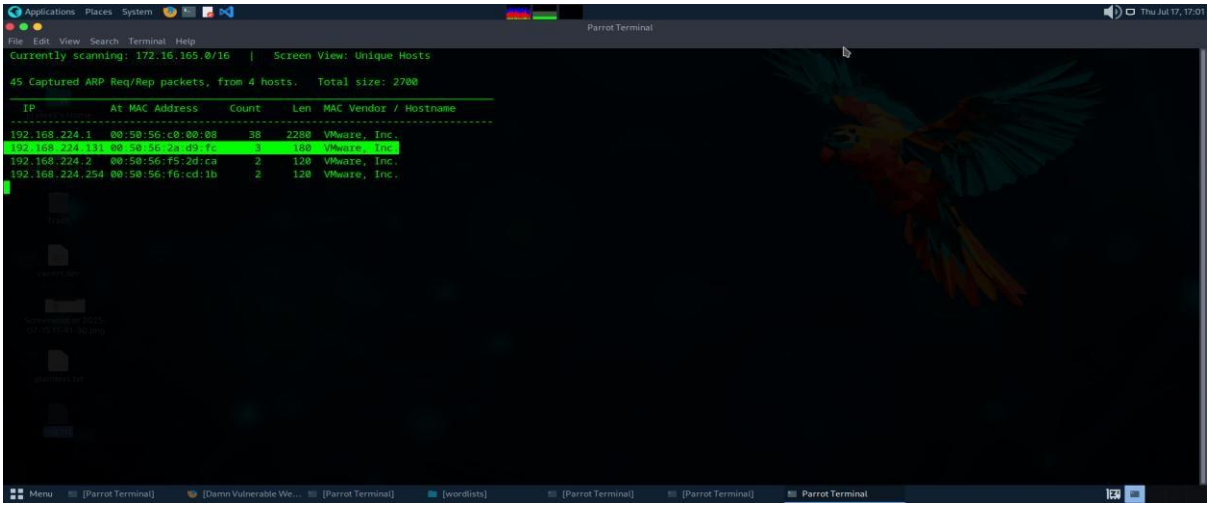
6.The site has also vulnerability of CSRF by that a person can change the password of user and user itself not able to access its information.

It is important to correct all the vulnerability to protect the system and user data .

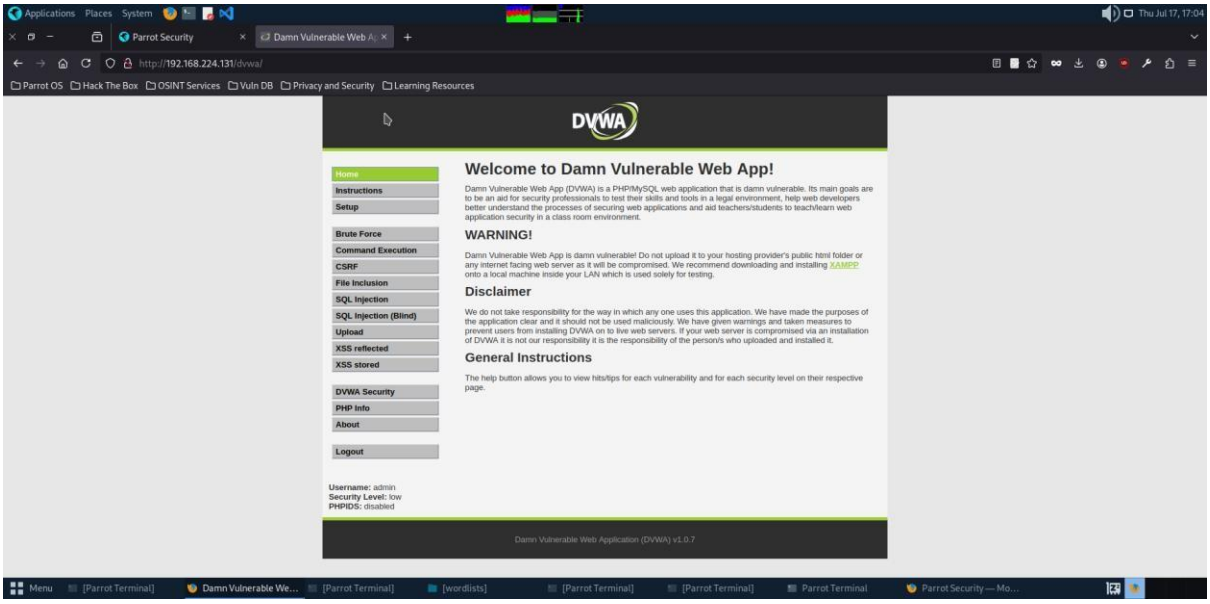
4.Penetration testing report

Attack Narrative:

1. At the beginning of the auditing, we use mac address to identify the IP address of Metasploit using netdiscover command.

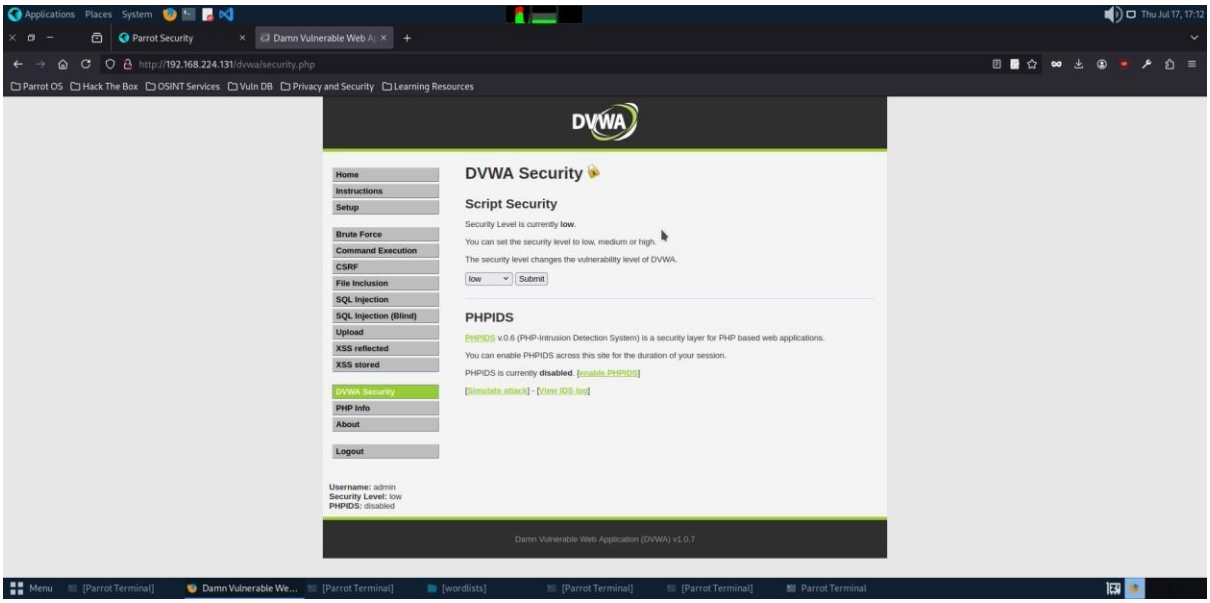


2. After getting the ip address we enter ip address to browser to open Metasploit site after that open dvwa web page .Than On the login page, use the default credentials: Username: admin and Password: password, then click Login to access the application



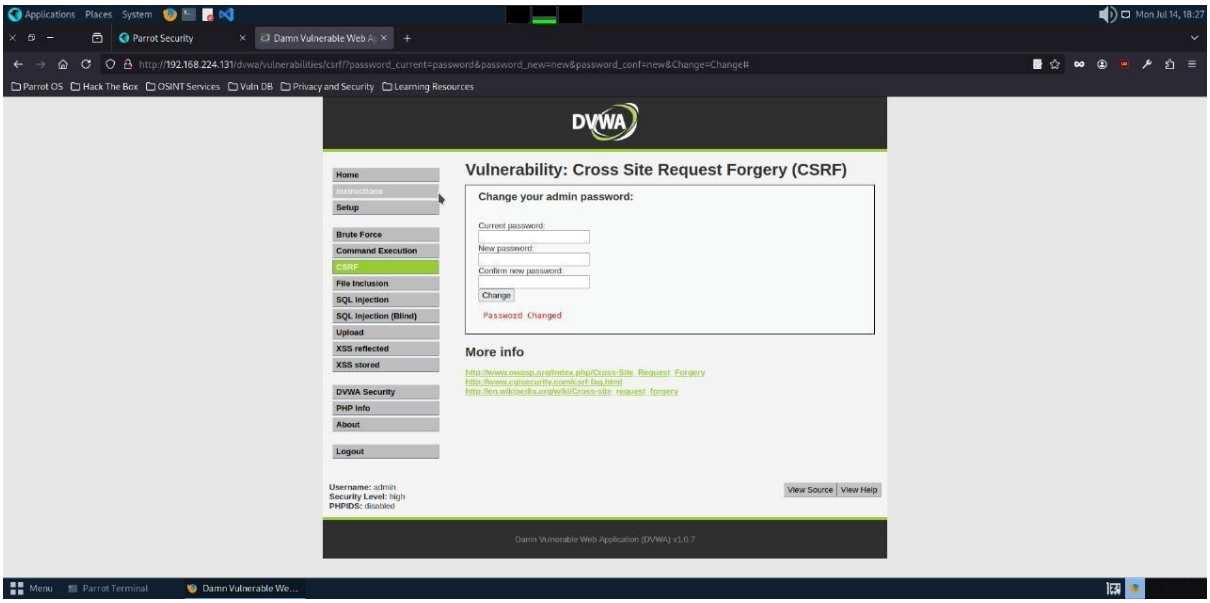
5.Penetration testing report

3. Once logged in, go to the DVWA Security tab in the navigation menu, change the security level to Low.



4. CSRF(CROSS-SITE Request forgery)

Analyze the csrf interface you will see the change password entry fields by that you can easily change the password of user.

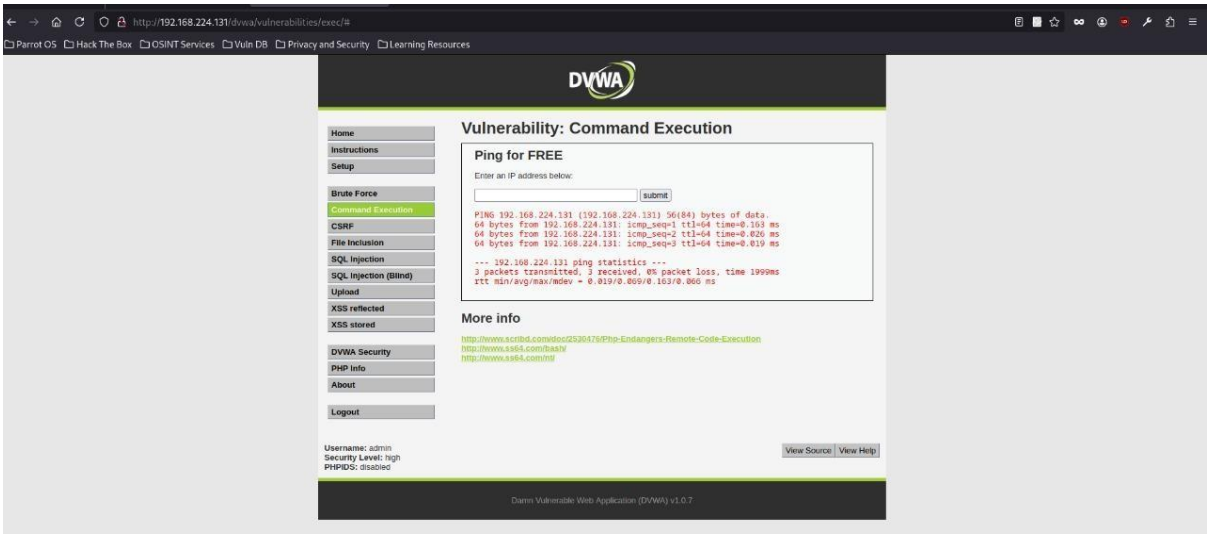


5.Command execution

In these you will see an input field for entering ping command .

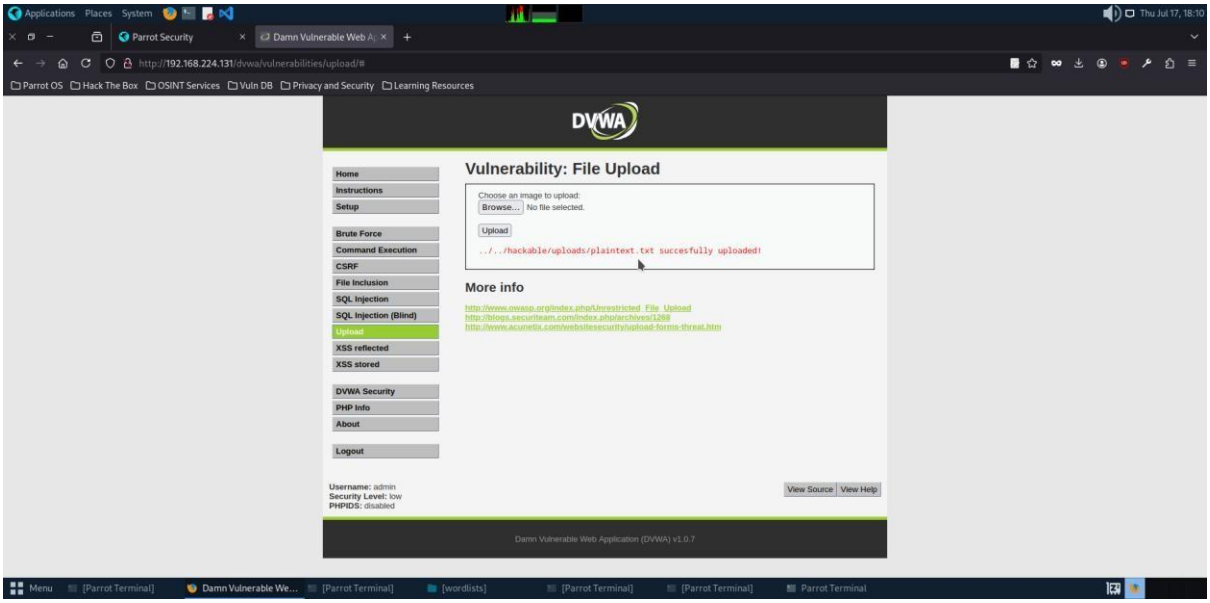
These will give connectivity for the web application hence reveal important information

6.Penetration testing report



6.Upload

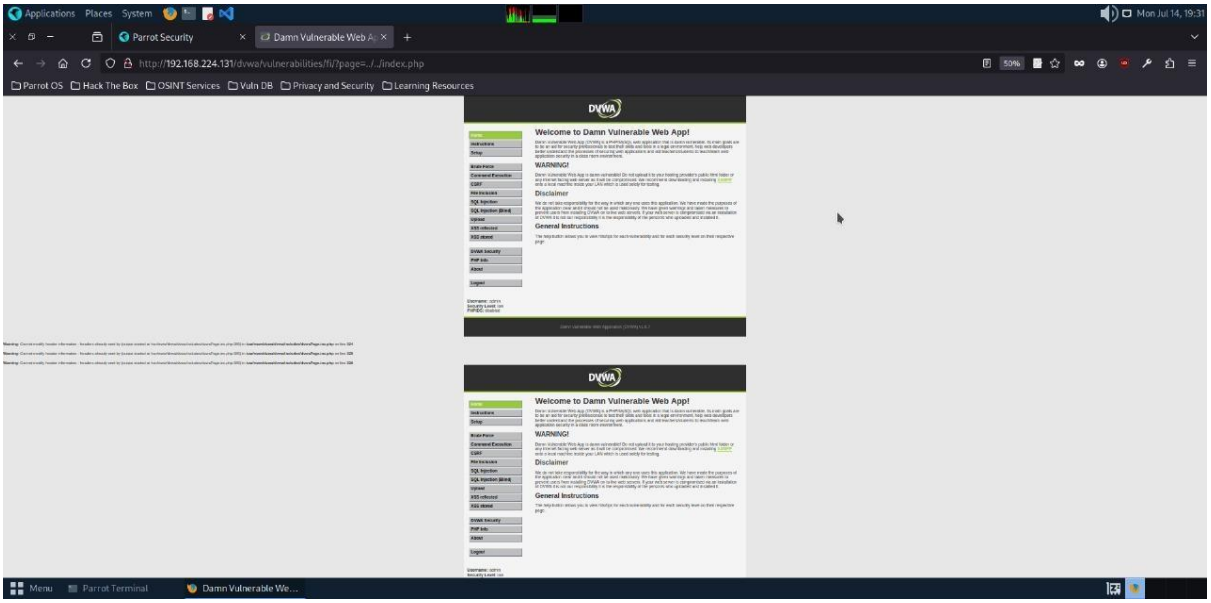
In these you will see an option of uploading image but it is taking file and everything as input so a person can upload reverse shell script or anything malicious and take access to system



7. File inclusion

In these when we upload the file it will give us the full path of file so we can access password file in etc folder by backing in url ../../ or make duplicate page using index.php

7.Penetration testing report

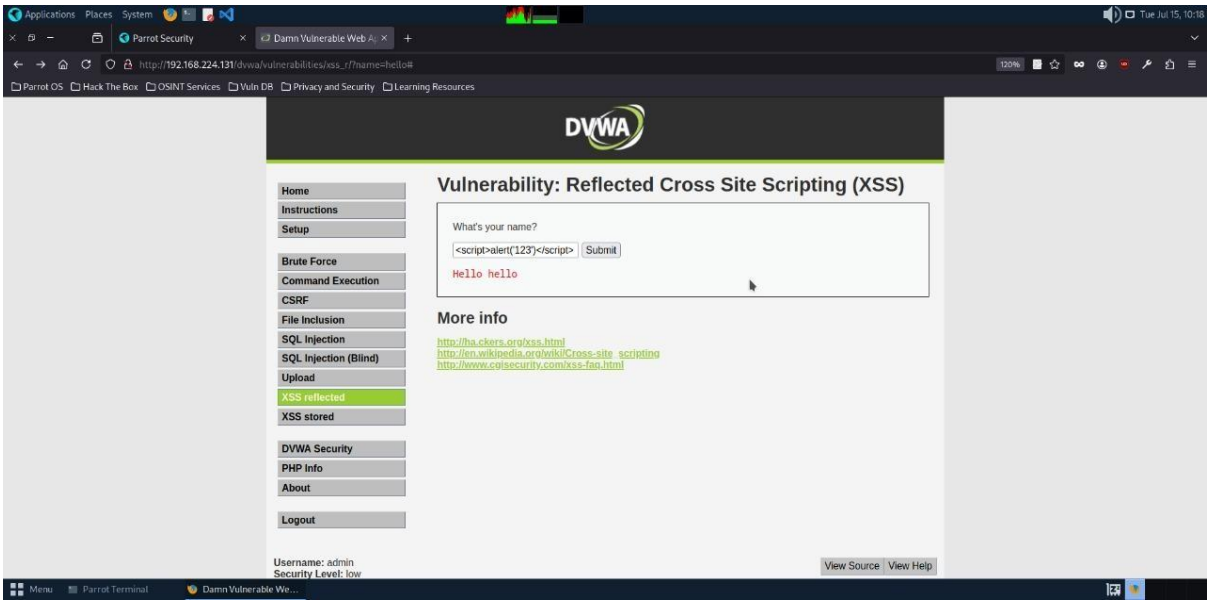


8. XSS(cross site scripting)

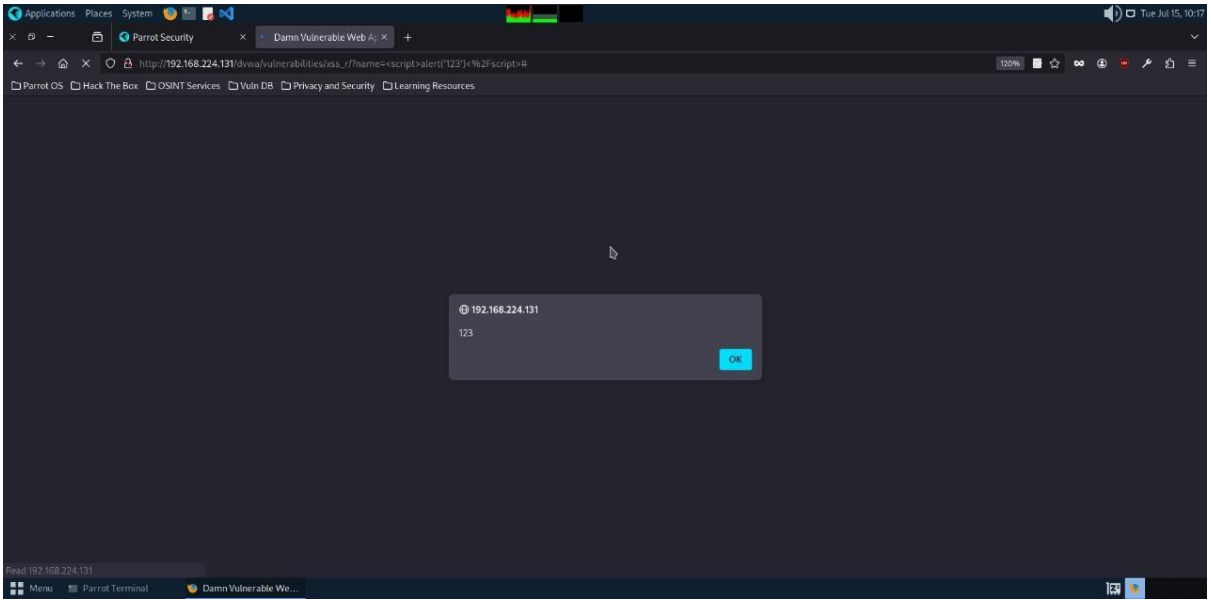
It is a vulnerability that occurs when an attacker injects malicious javascripts into web pages viewed by other users. These scripts steal sensitive information, manipulate content for example give unnecessary alert to users.

1. Reflected XSS

   In these input field we can enter javascript malicious code into the box that will run for example we write hello and javascript code so it gives reflects our message as hello print two times and also run javascript code as alert is also showing.



8.Penetration testing report

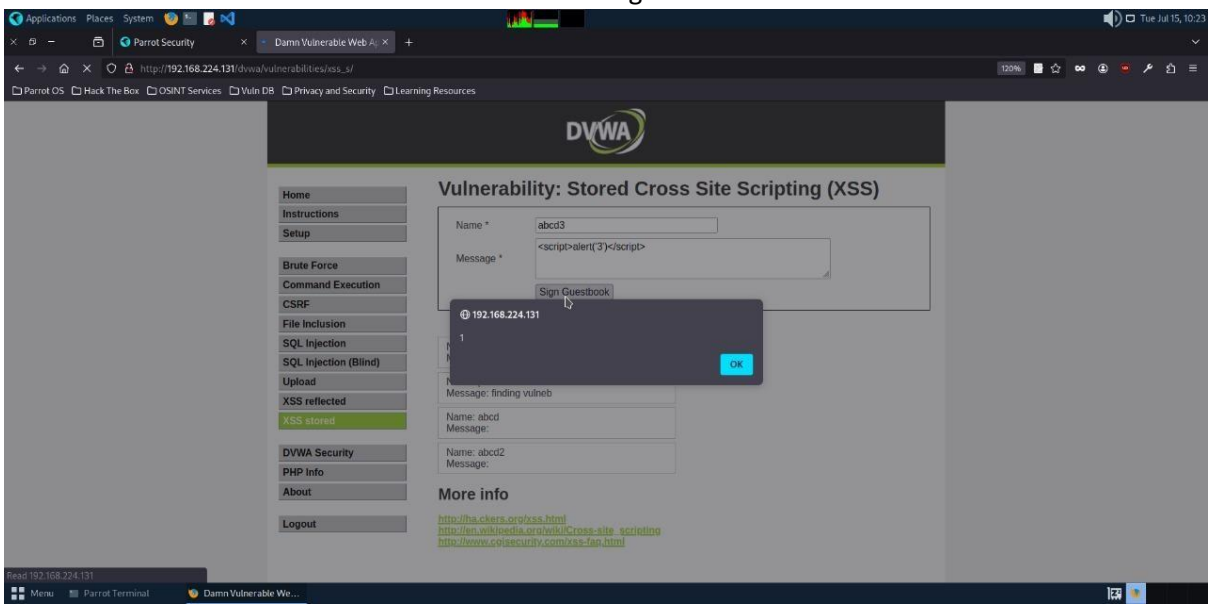


2. Stored xss

   In these attacker injects malicious scripts into a web application, and these scripts are permanently stored on the server and run every time if user run new commanad the previos one is also execute.

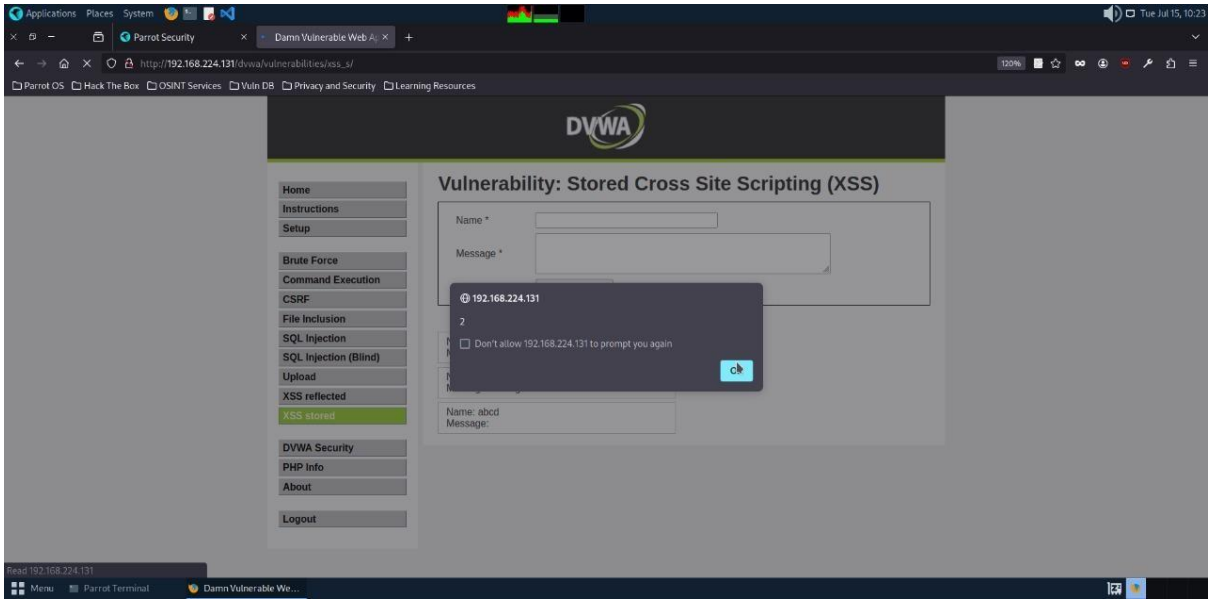
   After executing the third command it will run the first two

   In these first command is run so first alert 1 is showing

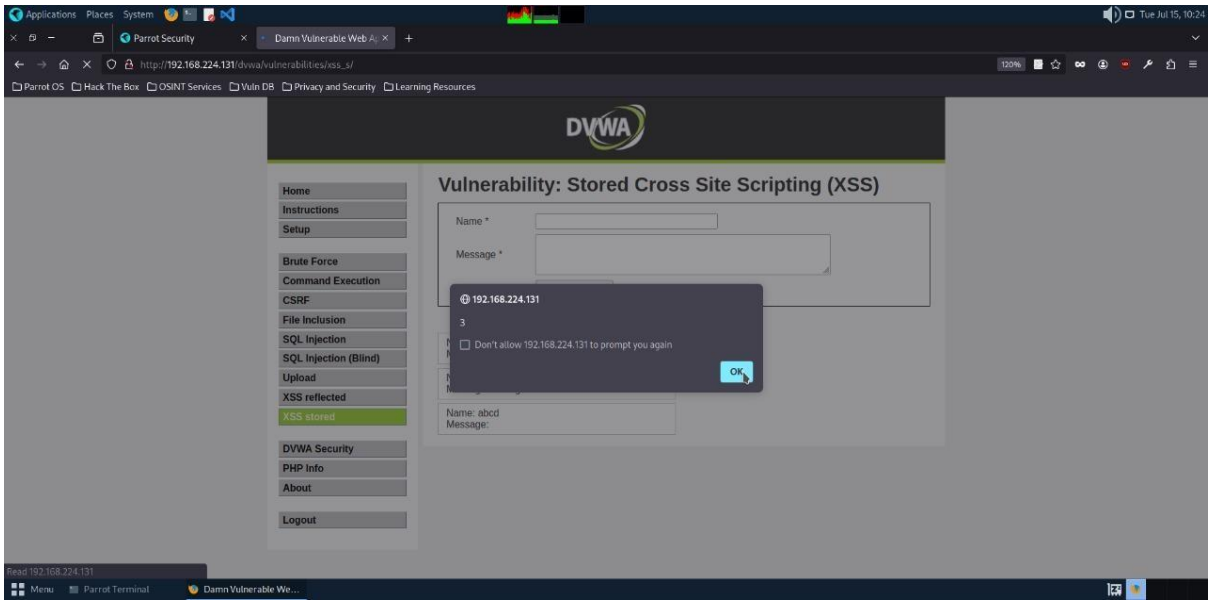


   After first in run second command will run so showing alert 2

9.Penetration testing report



After 2 third command will run so showing alert 3



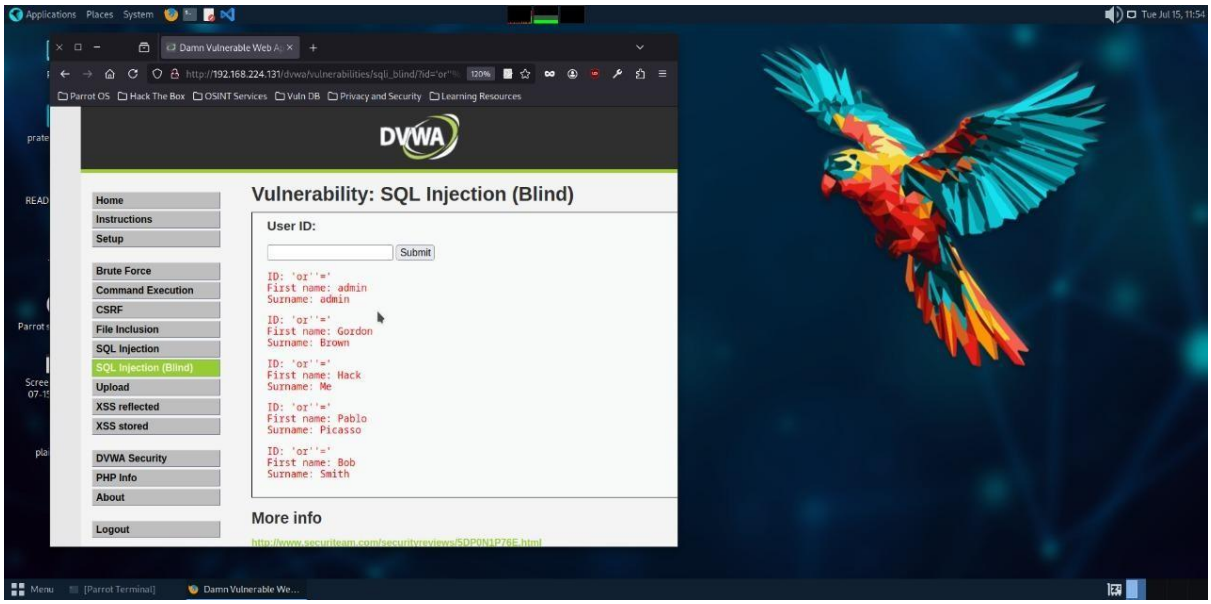
Hence all command will execute from first because it was stored in database

9. Sql injection blind

In these enter parameter like or‘ if it runs but give error that means sql injection vulnerability is present in application. Enter a payload like ' OR '1'='1 in the input field it will return all database records instead of the intended single entry.

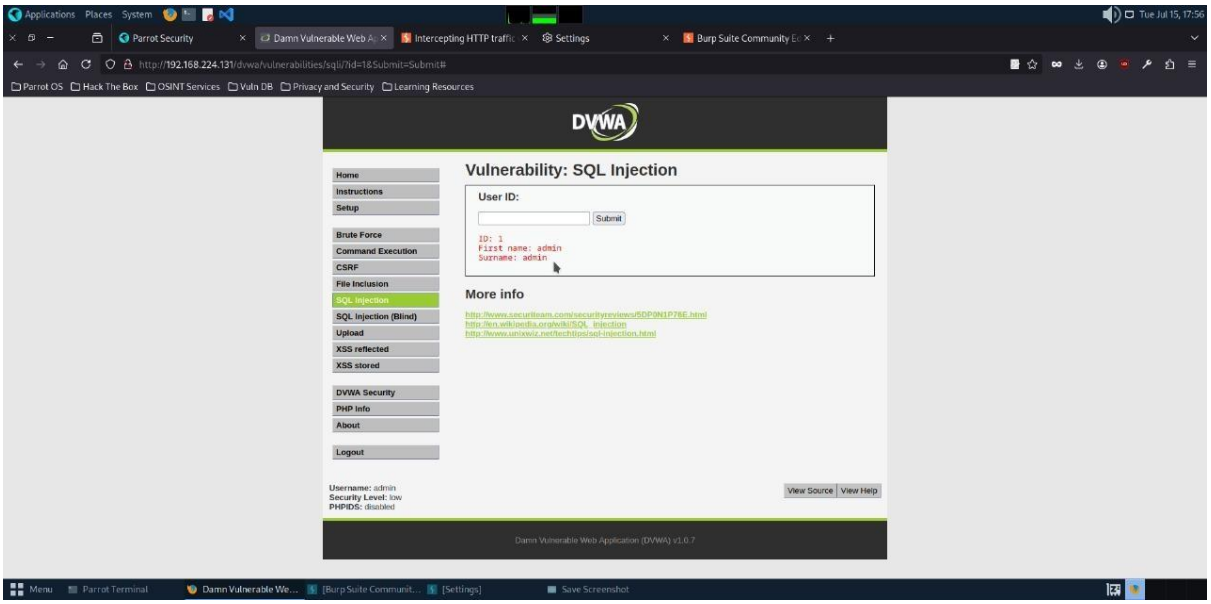
10.P

enetration testing report



10. SQL INJECTION

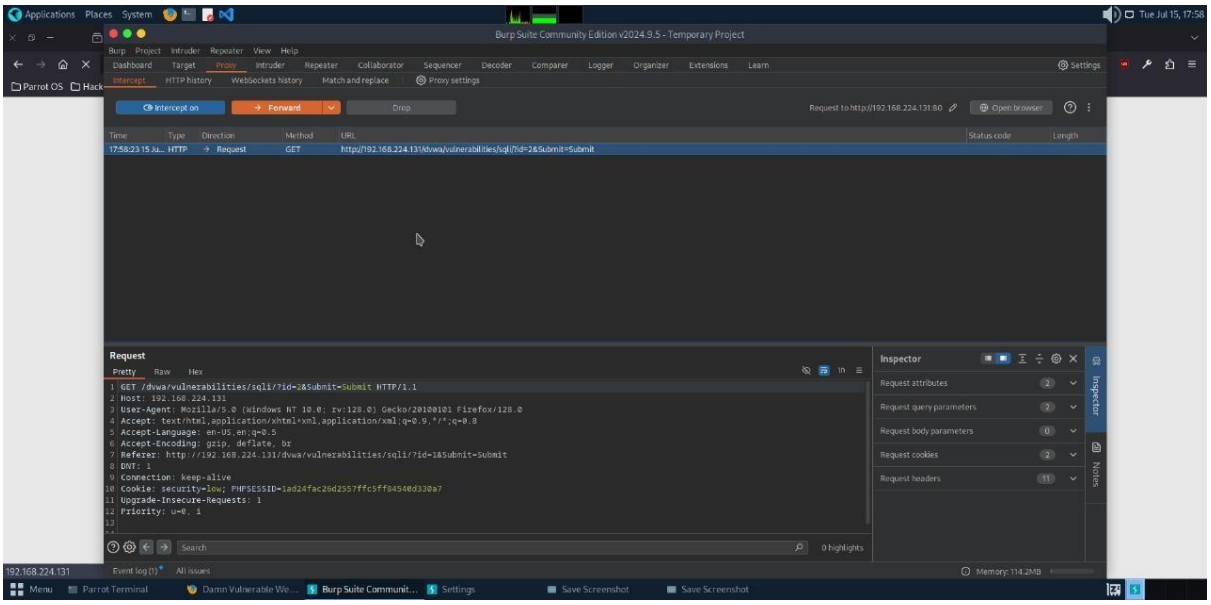
If we enter 1 and he is giving the information about first person



Than we can fetch all the database information . for these we use burp suite application . we turn off the intercept in proxy in burp application . then we saw the ip and port of burp application and enter same port and ip to site settings hence our burp and site is connected with each other than we download ca certificate of site and turn on intercept.after that when we enter

11.Penetration testing report

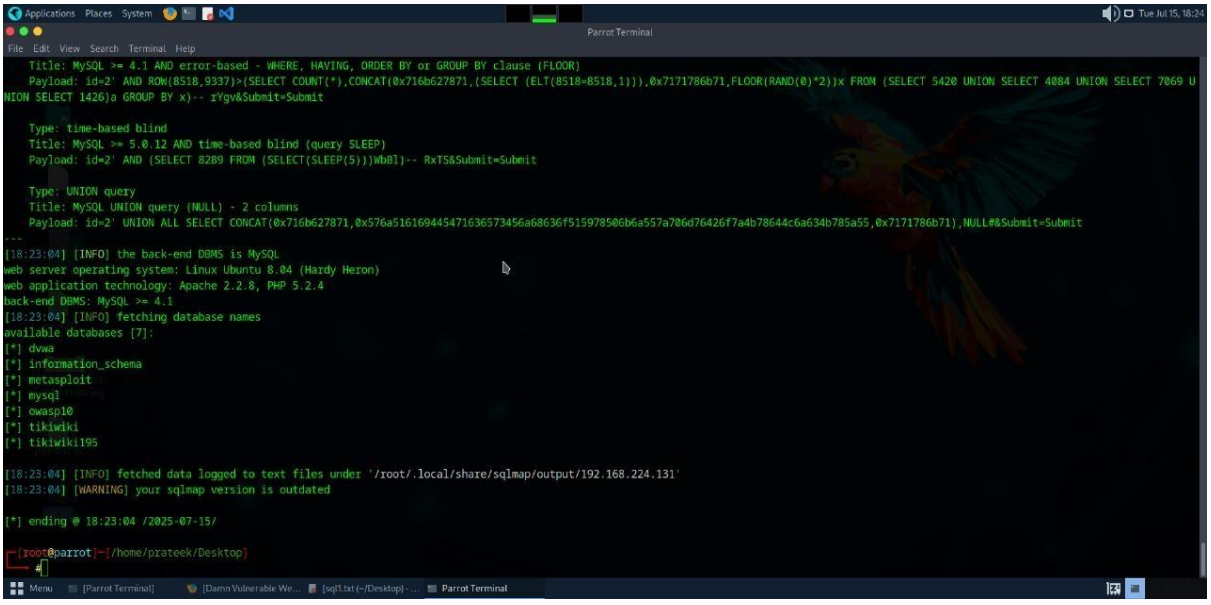
something in dvwa first it will ask permission in burp suite and when we allow or forward than it will run.



Then we run sql map in command prompt and copy the given request information of burp into file and give file to sql map

Run command

Sqlmap -r filename --dbs

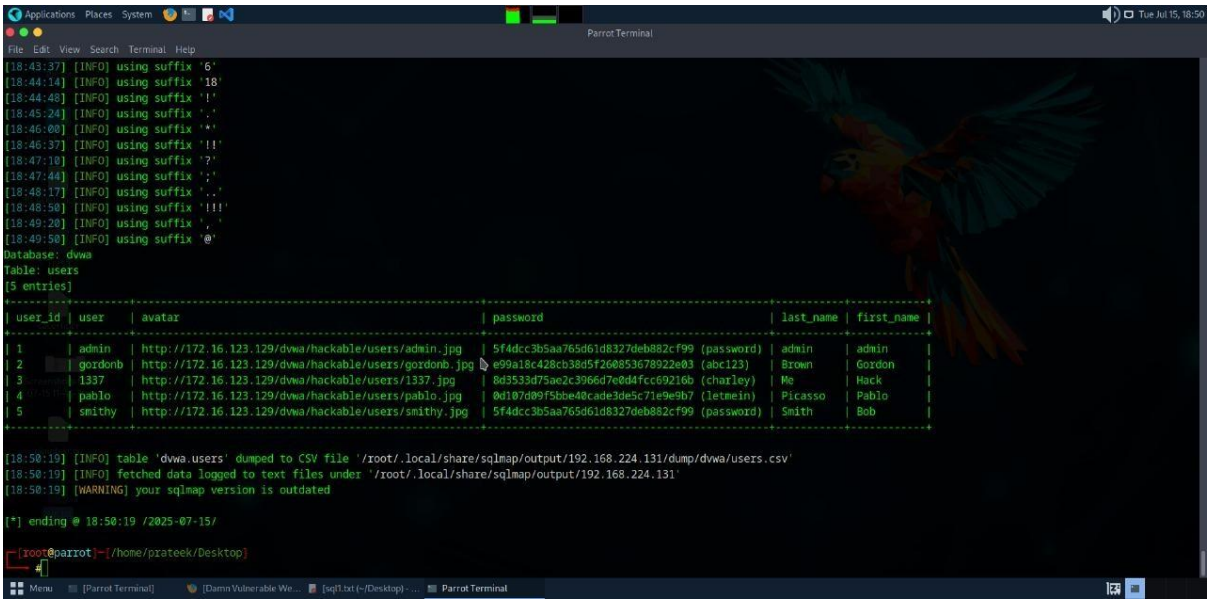


12.Penetration testing report

Sqlmap -r filename -D dvwa --tables –dbs

Sqlmap -r filename -D dvwa -T users --column –-dbs

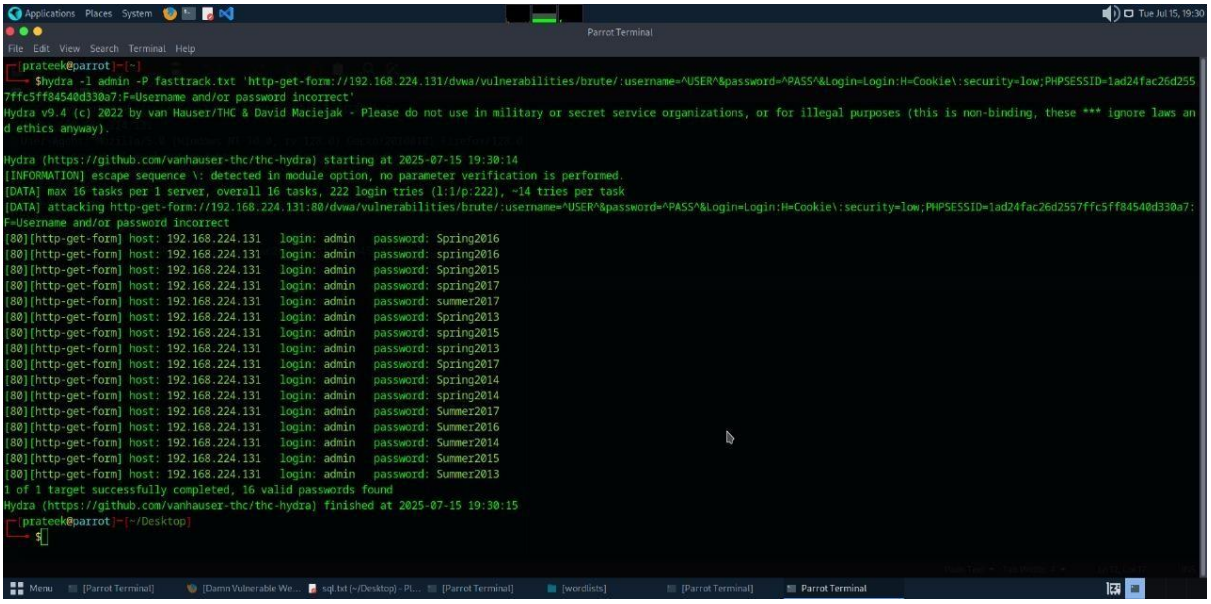
Sqlmap -r filename -D dvwa -T users --dump –-dbs



11. Brute force

In these we try many password to crack it using tool hydra

Hydra tool to automate the attack. Hydra will systematically try different password combinations from the wordlist until it finds the correct password.



13.Penetration testing report

CONCLUSION AND RECOMMENDATION

The penetration test conducted on the DVWA application revealed so many critical vulnerabilities, like SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), File Upload, Brute Force, Command Execution, and File Inclusion. These vulnerabilities, if left unaddressed, could allow an attacker to gain unauthorized access to sensitive data and manipulate that, and compromise the entire system or gain access of system to other person.

SQL Injection: it can be prevented by validating and sanitizing user inputs. They should use parameterized queries, restrict database access, and regularly update applications. Also, web application firewalls (WAFs) can add another layer of protection against these attacks.

Cross-Site Scripting (XSS): To prevent XSS attacks, it is important to encode user inputs before rendering them on the page. This prevents malicious scripts from being executed in the user's browsers.

Cross-Site Request Forgery (CSRF): To protect against CSRF attacks, integrating CSRF tokens into sensitive forms is essential. These tokens should be validated on the server side to ensure that requests are genuine.

File Upload: The file upload functionality should be strictly controlled. Only specific file types, such as images, should be allowed, and each uploaded file should be validated for proper extensions

Brute Force: we should make a strong password that consist of lower and uppercase letters and contain numbers and special symbol like @,#,&etc