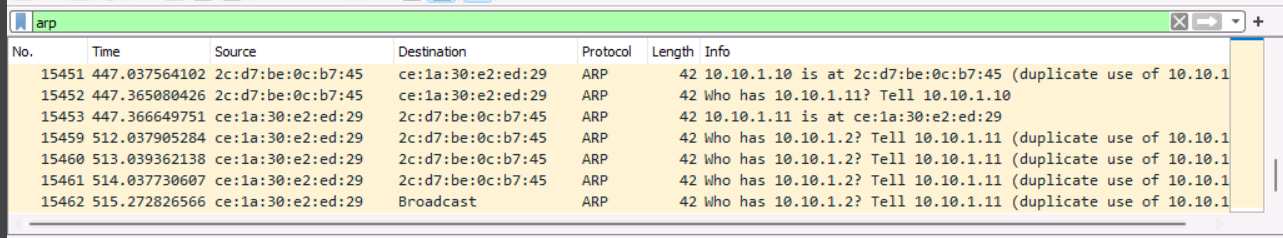
**CEH Engage part 3**

1. CEHORG suspects of a possible session hijacking attack on a machine in its network. The organisation has retained the network traffic data for the session at C:\Users\Admin\Documents in the EH Workstation – 2 as sniffsession.pcap. You have been assigned a task to perform an analysis and find out the protocol that has been used for sniffing on its network. (Format: AAA)

Answer: ARP

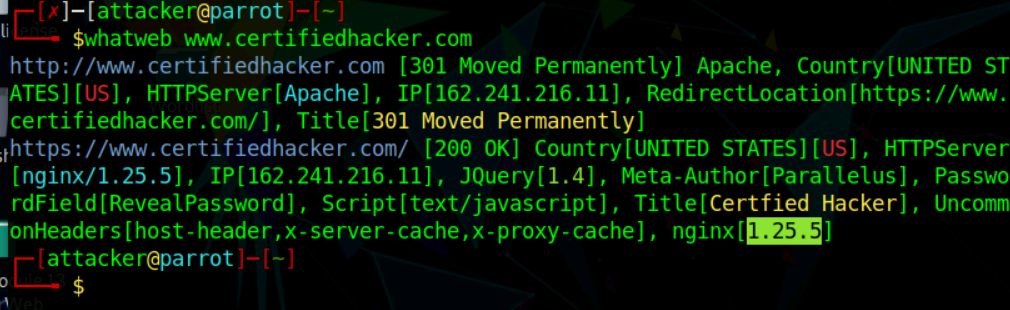
Because It is used to convert addresses between different networks. To discover the MAC addresses of other computers on the network, **any networked devices that need communication will broadcast ARP queries.**



1. Perform an HTTP-recon on www.certifiedhacker.com and find out the version of Nginx used by the web server. (Format: N.NN.N)

Answer: 1.25.5

Whatweb is use for http-recon



1. An FTP site is hosted on a machine in the CEHORG network. Crack the FTP credentials, obtain the “flag.txt” file and determine the content in the file. (Format: Aaaaaaa\*AAA)

Answer: Secrets@FTP

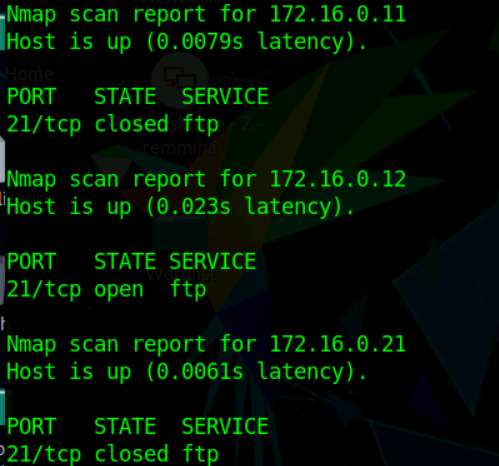
Perform nmap first on these network.

nmap -p 21 172.16.0.0/24

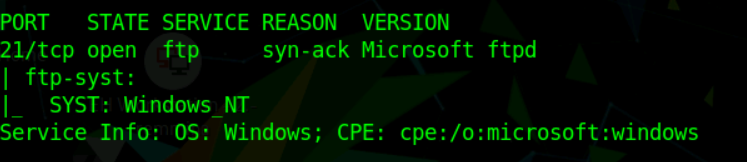
nmap -p 21 10.10.10.0/24

nmap -p 21 192.168.0.0/24

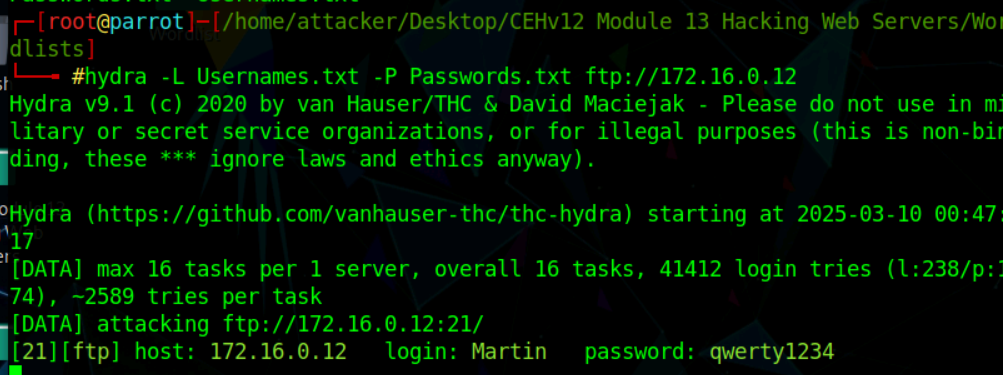
We found that we have only port open in 172.16.0.12 other all network and subnet(192, 10) both have unfiltered and close port.

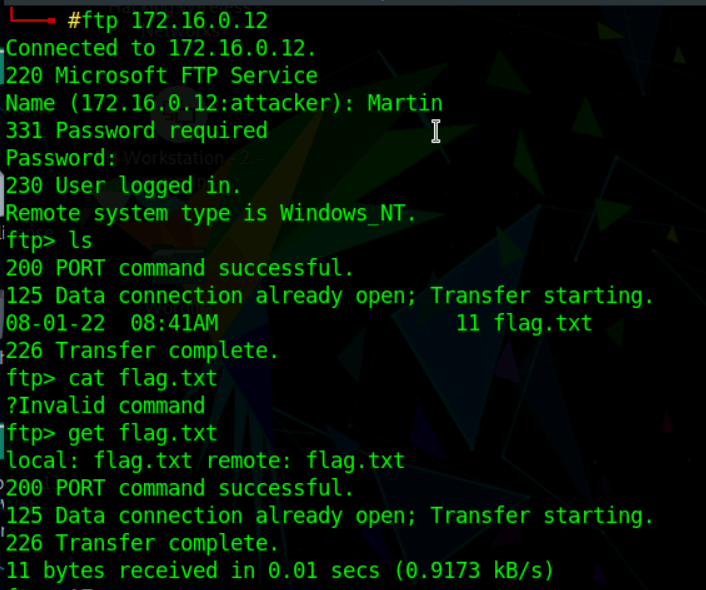


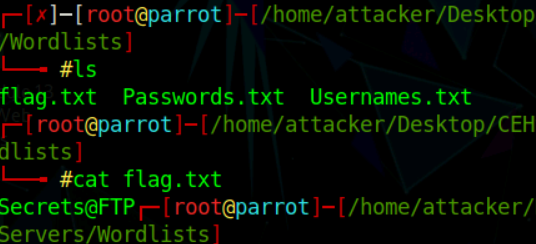
If use -vv then we get in details



Perform hydra to bruteforce the ftp password. Make sure that use Module 13 wordlist.



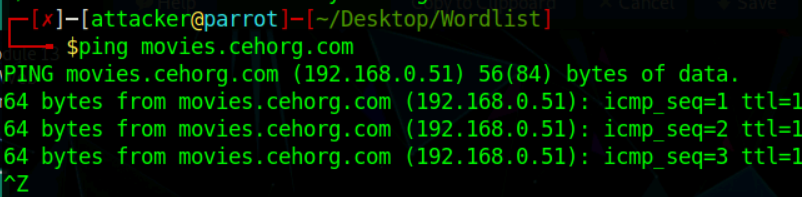




1. Perform Banner grabbing on the web application movies.cehorg.com and find out the ETag of the respective target machine. (Format: "NaNNNNNaaaNaaNN\*N")

Answer: “8d13646dbb9bd61:0”

Find IP of movies.cehorg.com

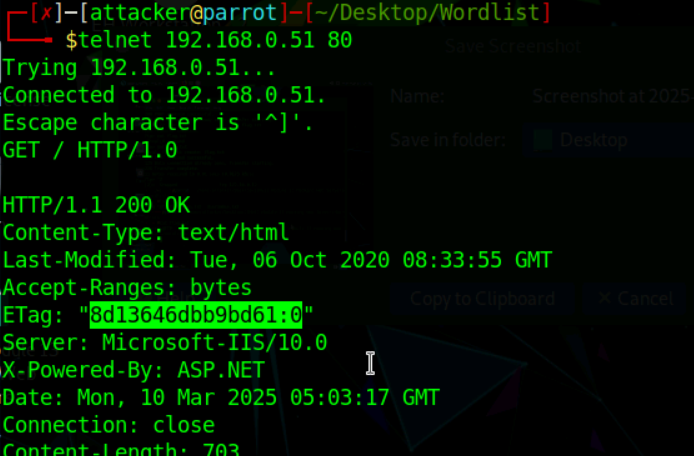


Use telnet for banner grabbing with port 80.

After ‘^]’.

Press enter and write **GET / HTTP/1.0** and hit enter.

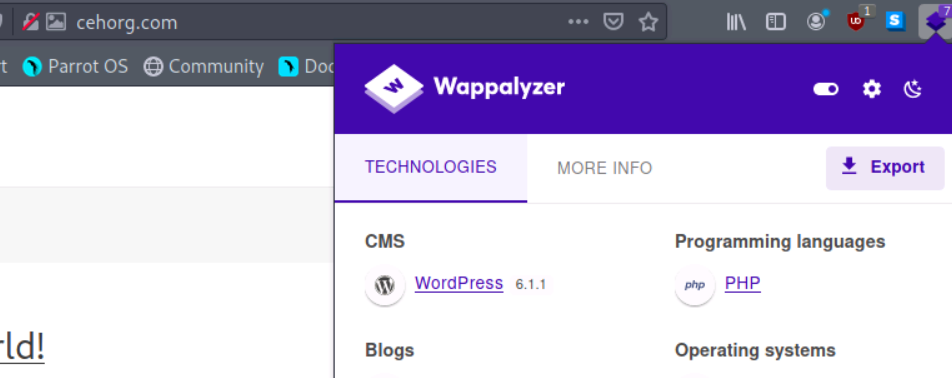
And we got the ETag

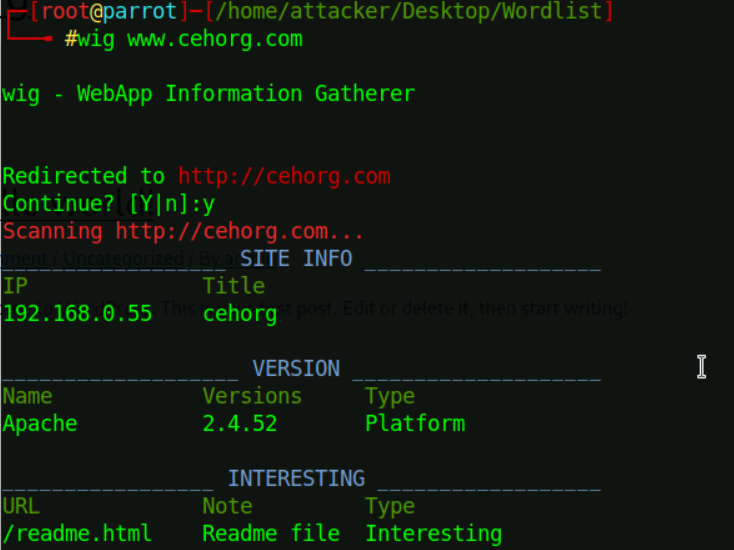


1. Identify the Content Management System used by www.cehorg.com. (Format: AaaaAaaaa)

Answer: WordPress

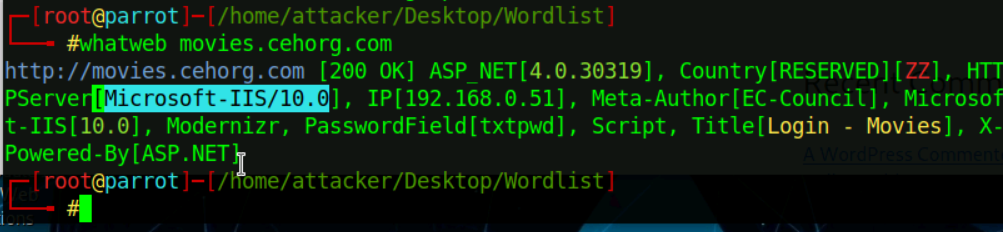
Install Wappalyzer in browser OR use wig command but it will work some time only.





1. Perform web application reconnaissance on movies.cehorg.com and find out the HTTP server used by the web application. (Format: Aaaaaaaaa-AAA/NN.N)

Answer: Microsoft-IIS/10.0



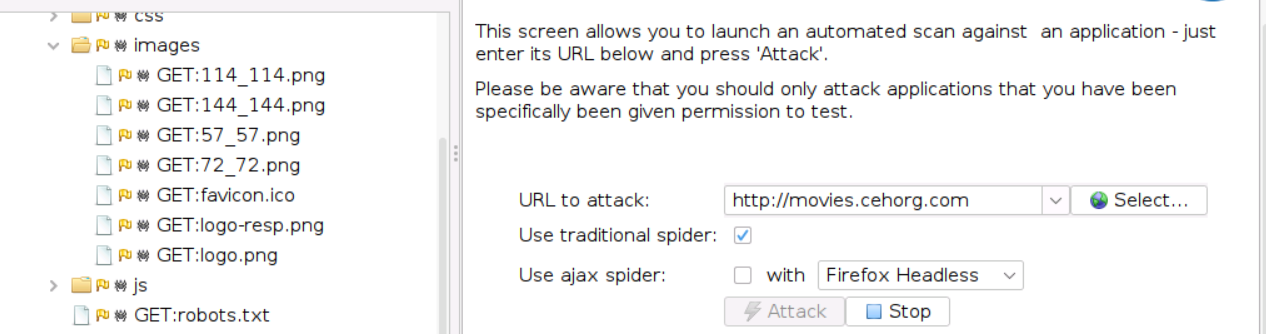
1. Perform Web Crawling on the web application movies.cehorg.com and identify the number of live png files in images folder. (Format: N)

Answer: 6

Just write **owasp-zap** in terminal and it will open.

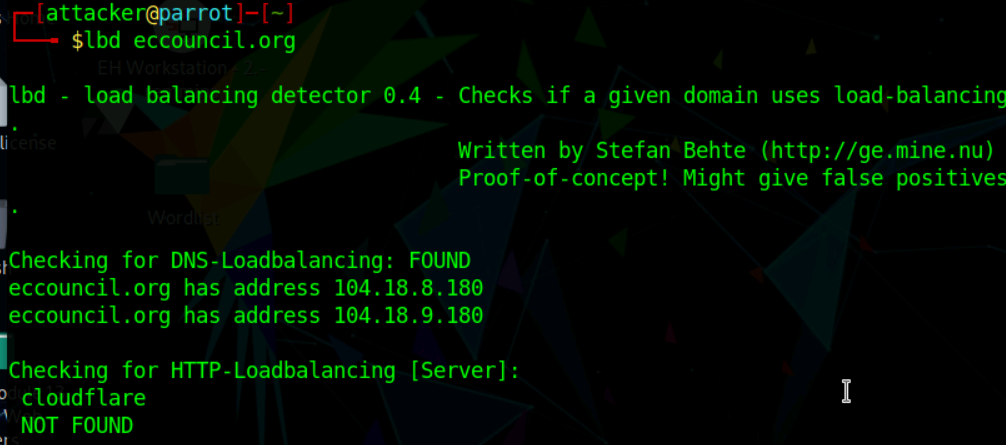
Click on automated scan and give site url and click on attack.

In left side under site we have list of folder and in that images we can find 6 .png images



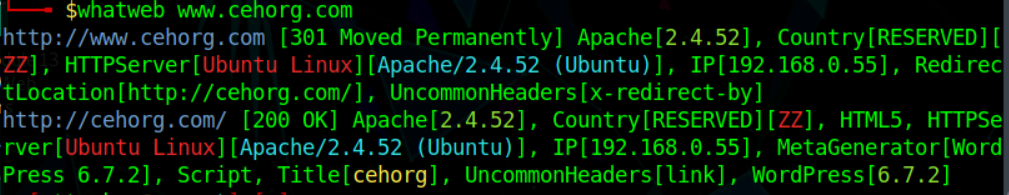
1. Identify the load balancing service used by eccouncil.org. (Format: aaaaaaaaaa)

Answer: cloudflare



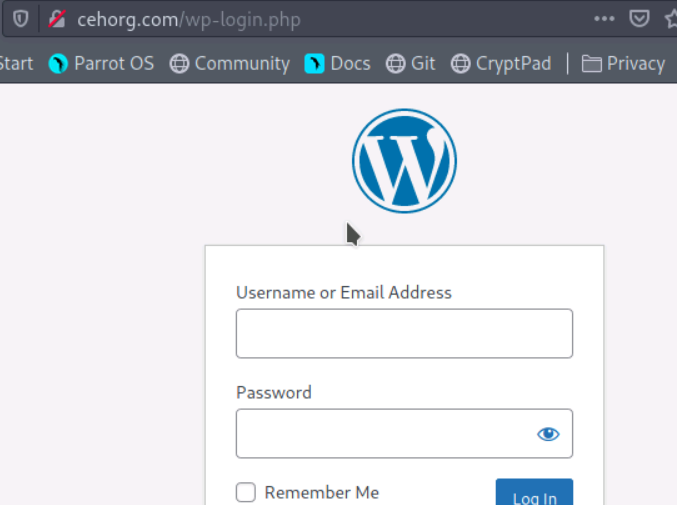
1. Perform a bruteforce attack on www.cehorg.com and find the password of user adam. (Format: aaaaaaNNNN)

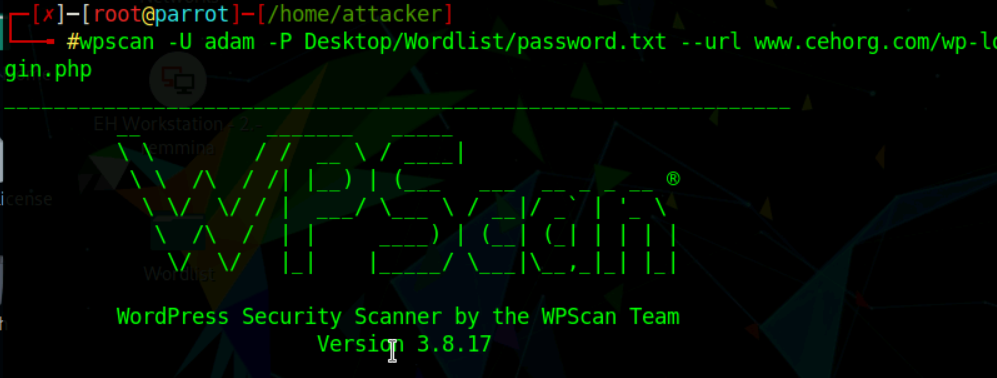
Answer: orange1234

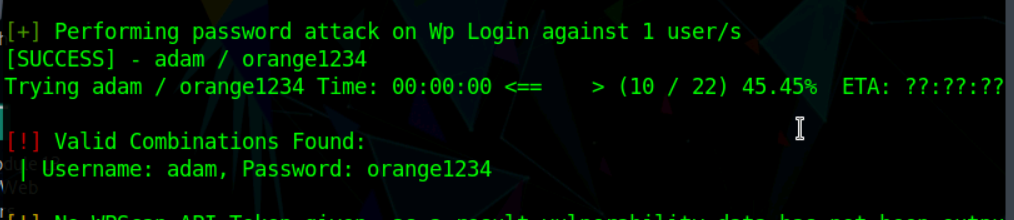


We found wordpress is there so we try with wpscan and before that check that is login page is there.

And we found by manual writing wp-login.php



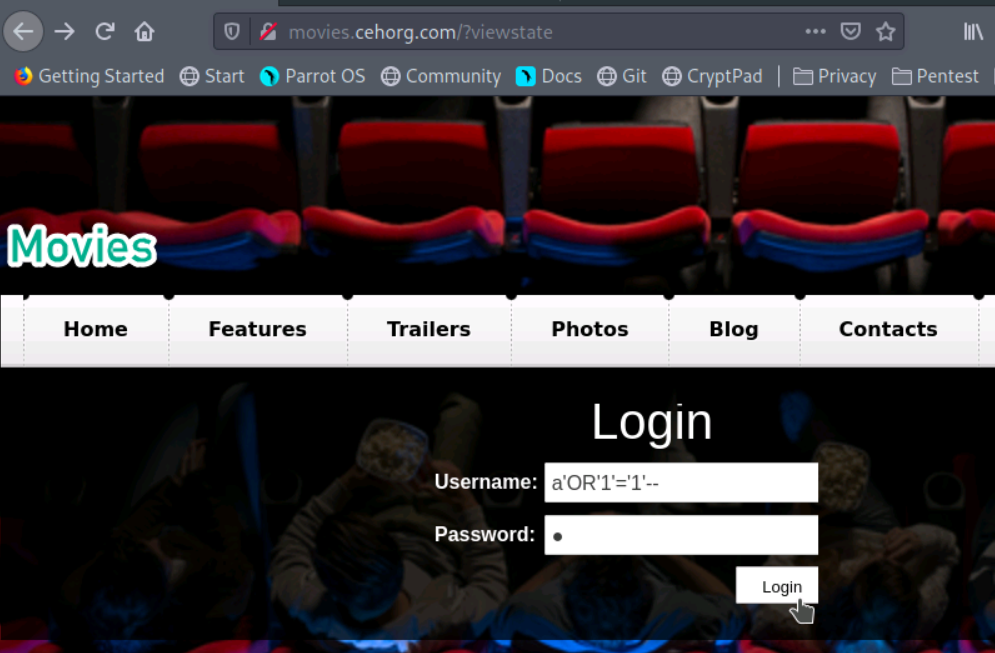


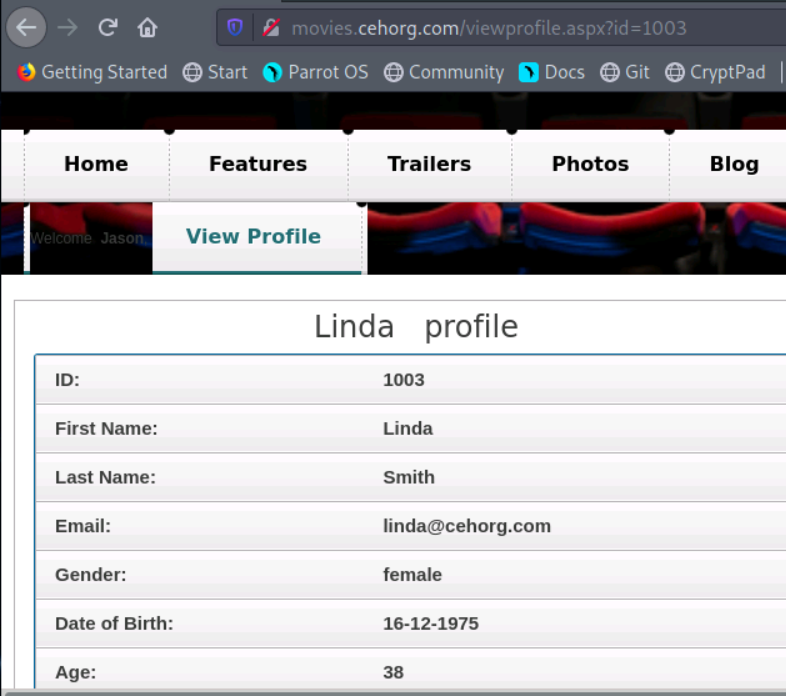


1. Perform parameter tampering on movies.cehorg.com and find out the user for id 1003. (Format: Aaaaa)

Answer: Linda

Simple SQL Injection and get view profile page.

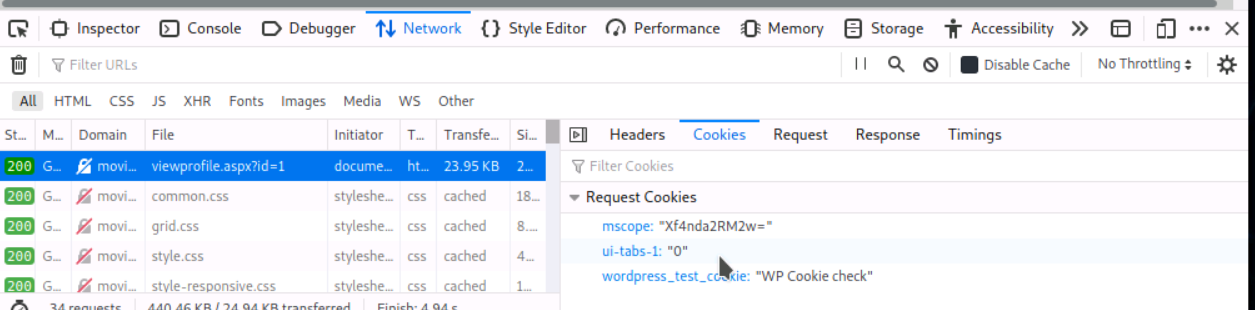




1. Perform a SQL Injection attack on movies.cehorg.com and find out the number of users available in the database. Use Jason/welcome as login credentials. (Format: N)

Answer: 9

Copy the cookie,

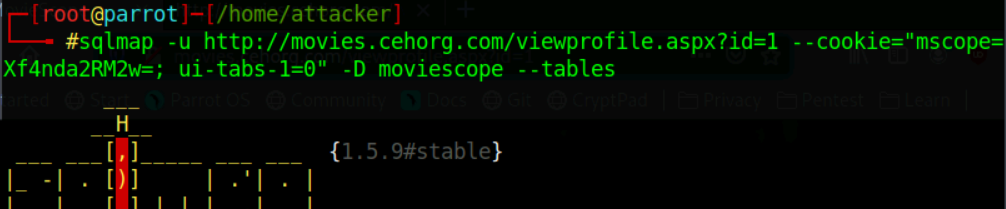


First check the database by this command





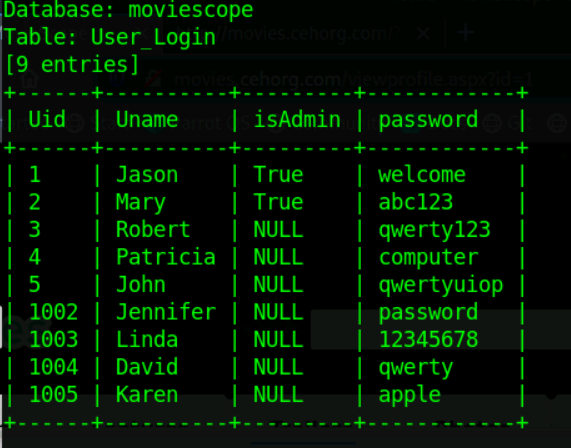
Now check in moviescope DB and enum. The table





Select any user table and use –dump to view the data





1. Perform XSS vulnerability test on www.cehorg.com and identify whether the application is vulnerable to attack or not. (Yes/No). (Format: Aa)

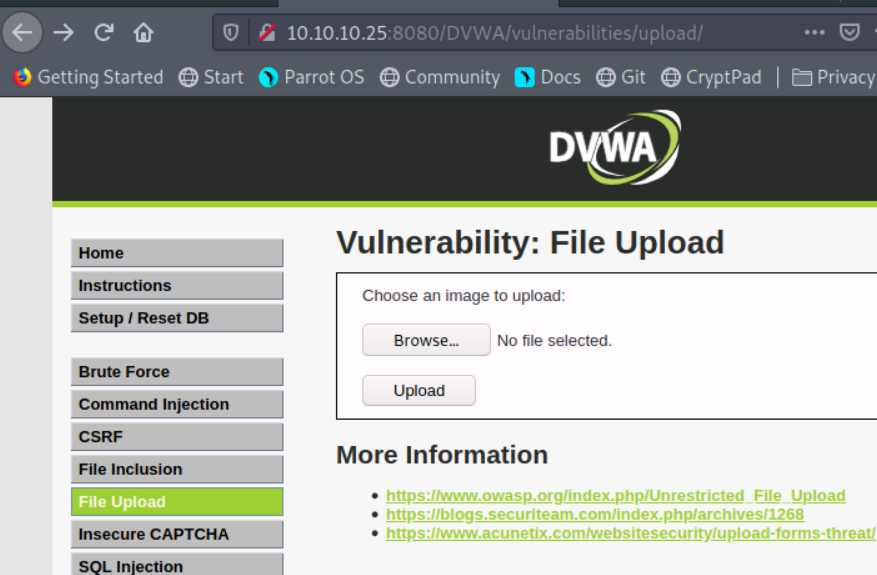
Answer: No

Write normal alert statement and check in search box.

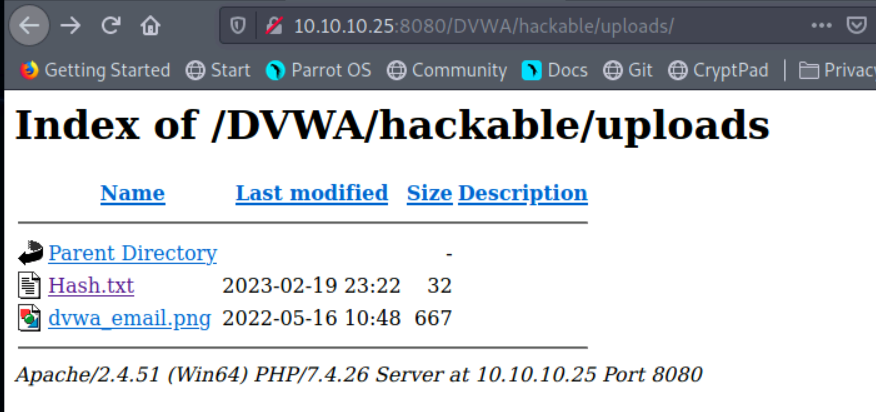
1. A file named Hash.txt has been uploaded through DVWA (http://10.10.10.25:8080/DVWA). The file is located in the directory mentioned below. Access the file and crack the MD5 hash to reveal the original message; enter the content after cracking the hash. You can log into the DVWA using the following credentials. Note: Username- admin; Password- password Path: C:\wamp64\www\DVWA\hackable\uploads\Hash.txt Hint: Use “type” command to view the file. Use the following link to decrypt the hash- https://hashes.com/en/decrypt/hash (Format: Aa\*aaNa)

Answer: Cr@ck3d

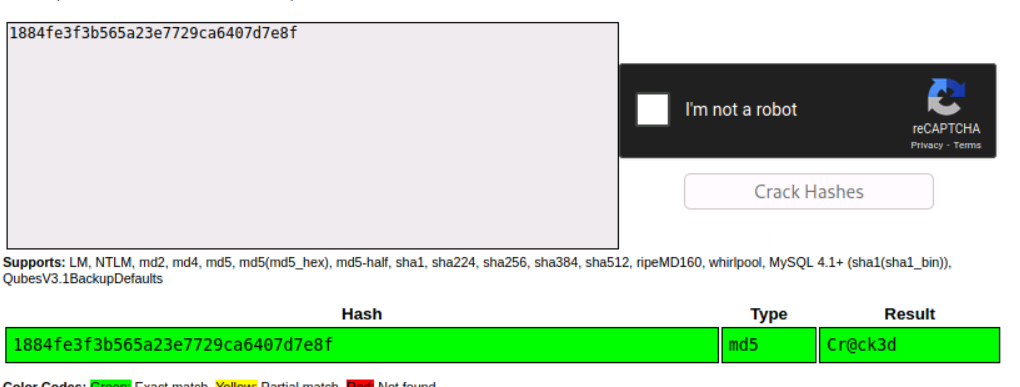
Go to file upload option



As per given in question change the URL till DVWA and we got hash



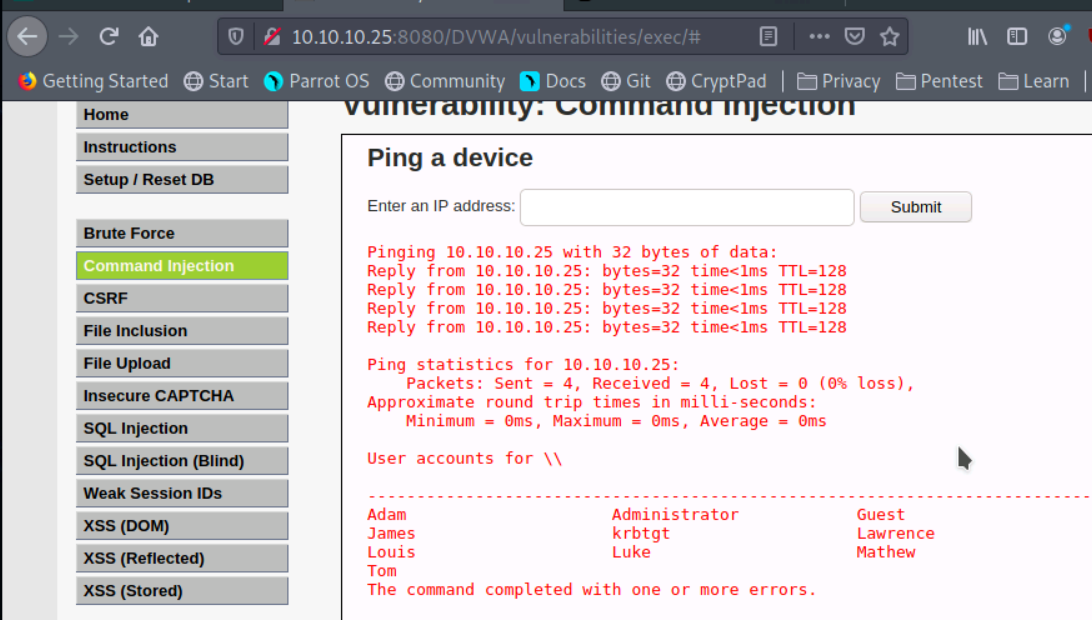
Crack the hash



1. Perform command injection attack on 10.10.10.25 and find out how many user accounts are registered with the machine. Note: Exclude admin/Guest user (Format: N)

Ans: 8

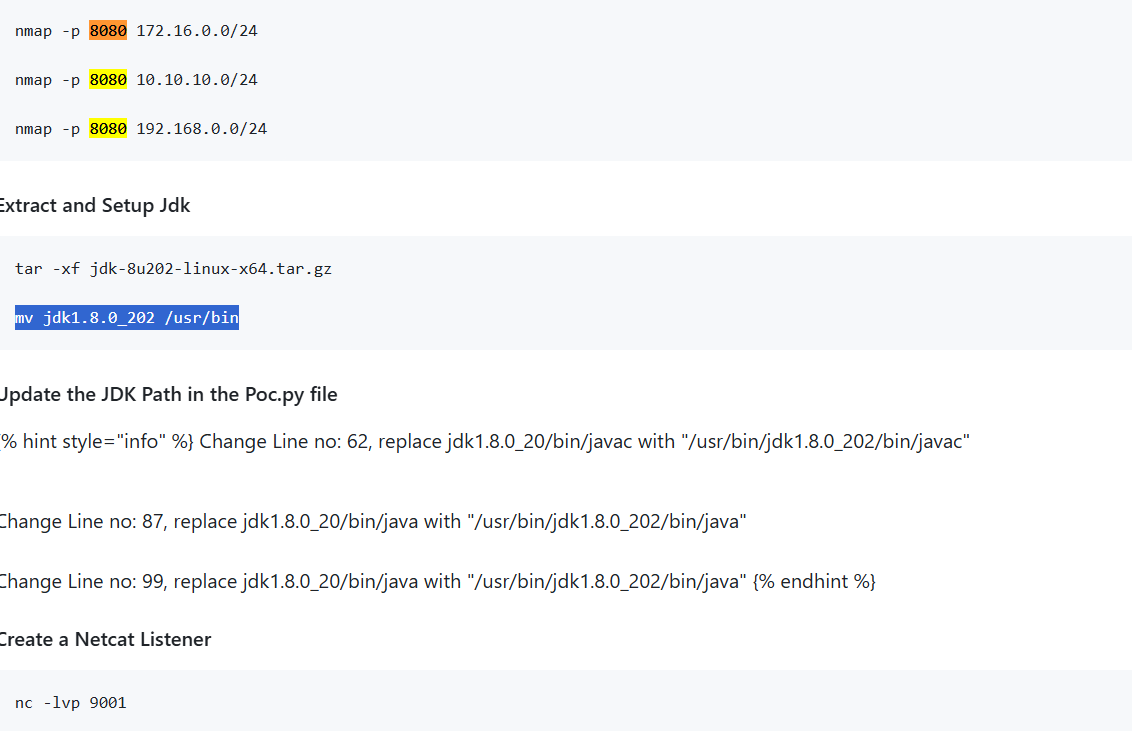
If not able to get then change security to low and then try



1. You have identified a vulnerable web application on a Linux server at port 8080. Exploit the web application vulnerability, gain access to the server and enter the content of RootFlag.txt as the answer. (Format: Aa\*aaNNNN)

Answer: Ch@mp2022

The log4j- poc shell file in Downloads





Paste send (payload) in login page

