Background / Scenario

You have been hired to conduct a penetration test for a customer. At the conclusion of the test, the customer has requested a complete report that includes any vulnerabilities discovered, successful exploits, and remediation steps to protect vulnerable systems. You have access to hosts on the 10.6.6.0/24 and 172.17.0.0/24 networks.

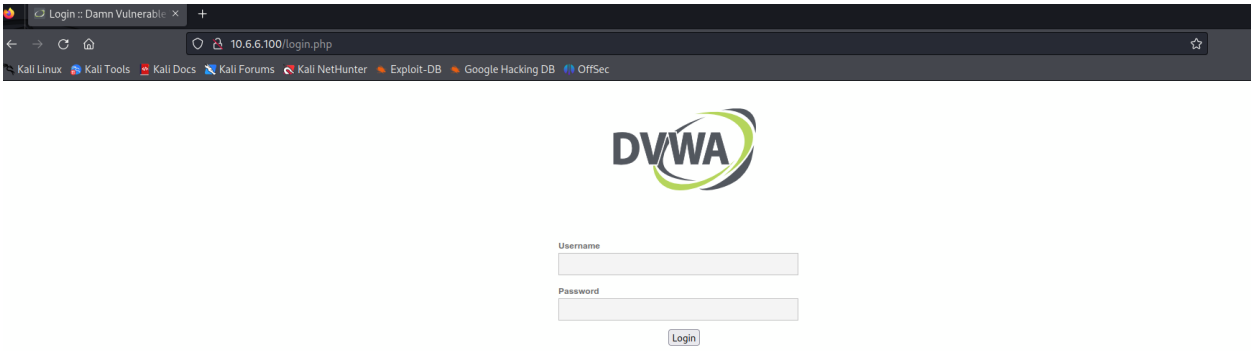
Instructions

Challenge 1: SQL Injection

In this part, you must discover user account information on a server and crack the password of **Gordon Brown's** account. You will then locate the file that contains the Challenge 1 code and use **Gordon Brown's** account credentials to open the file at 172.17.0.2 to view its contents.

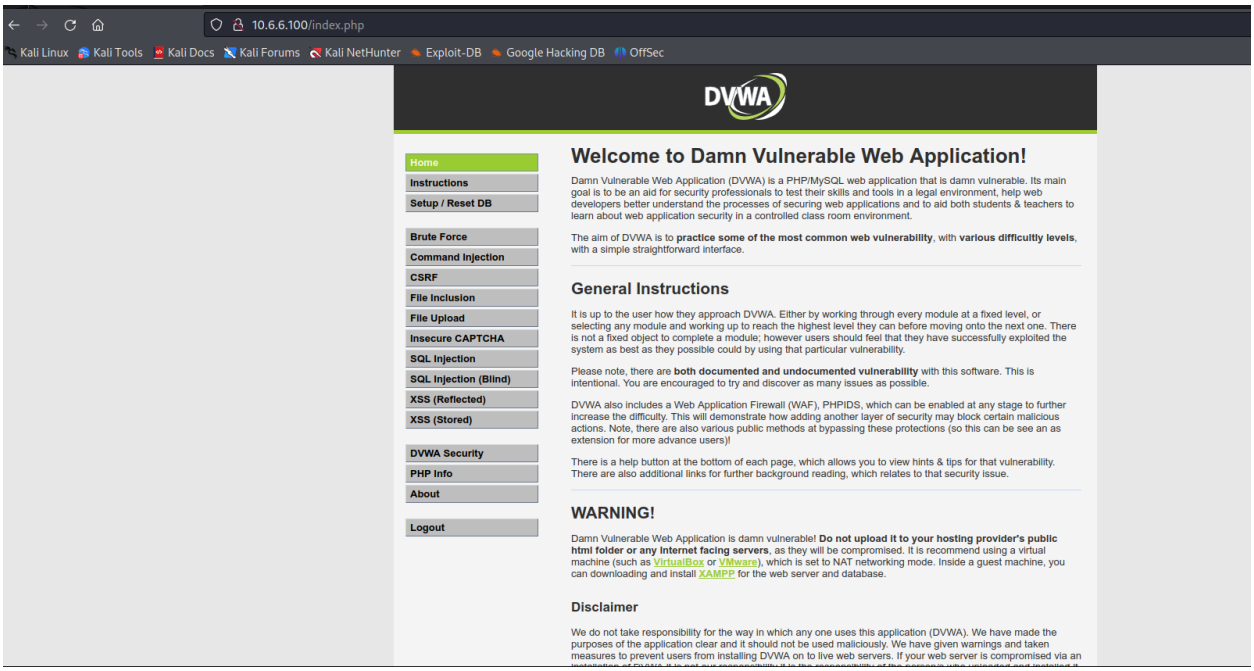
Step 1: Preliminary setup

a. Open a browser and go to the website at 10.6.6.100.

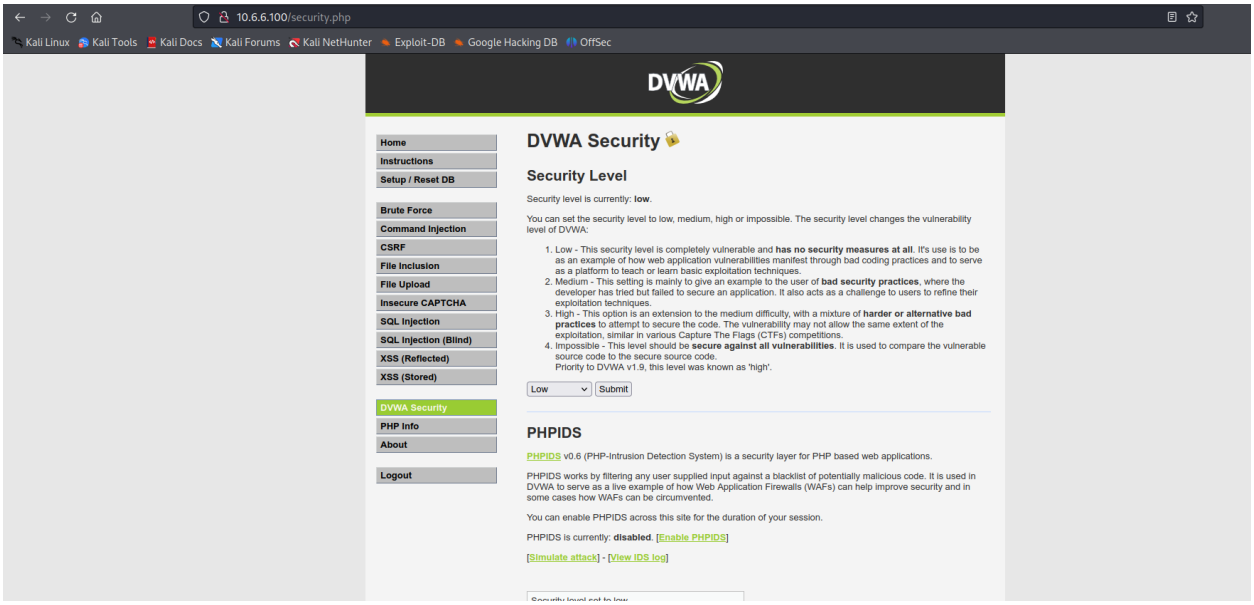


Note: If you have problems reaching the website, remove the https:// prefix from the IP address in the browser address field.

b. Login with the credentials **admin / password**.

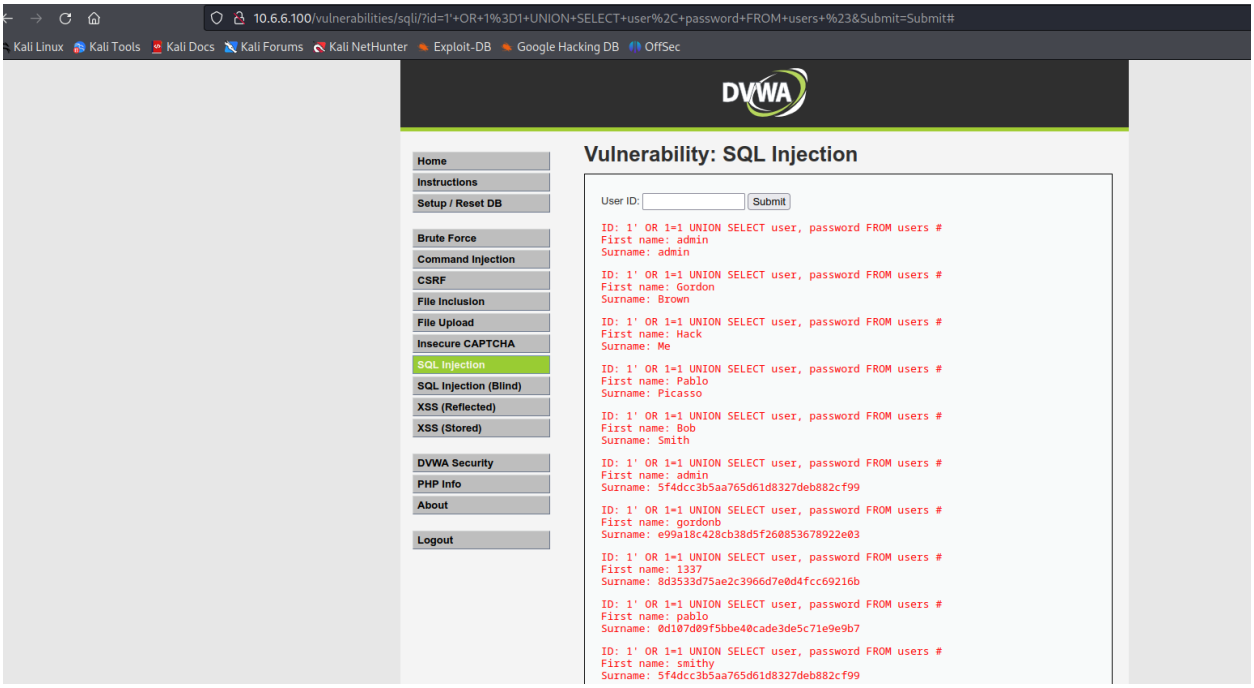


c. Set the DVWA security level to **low** and click **Submit**.



Step 2: Retrieve the user credentials for the Gordon Brown's account.

a. Identify the table that contains usernames and passwords.

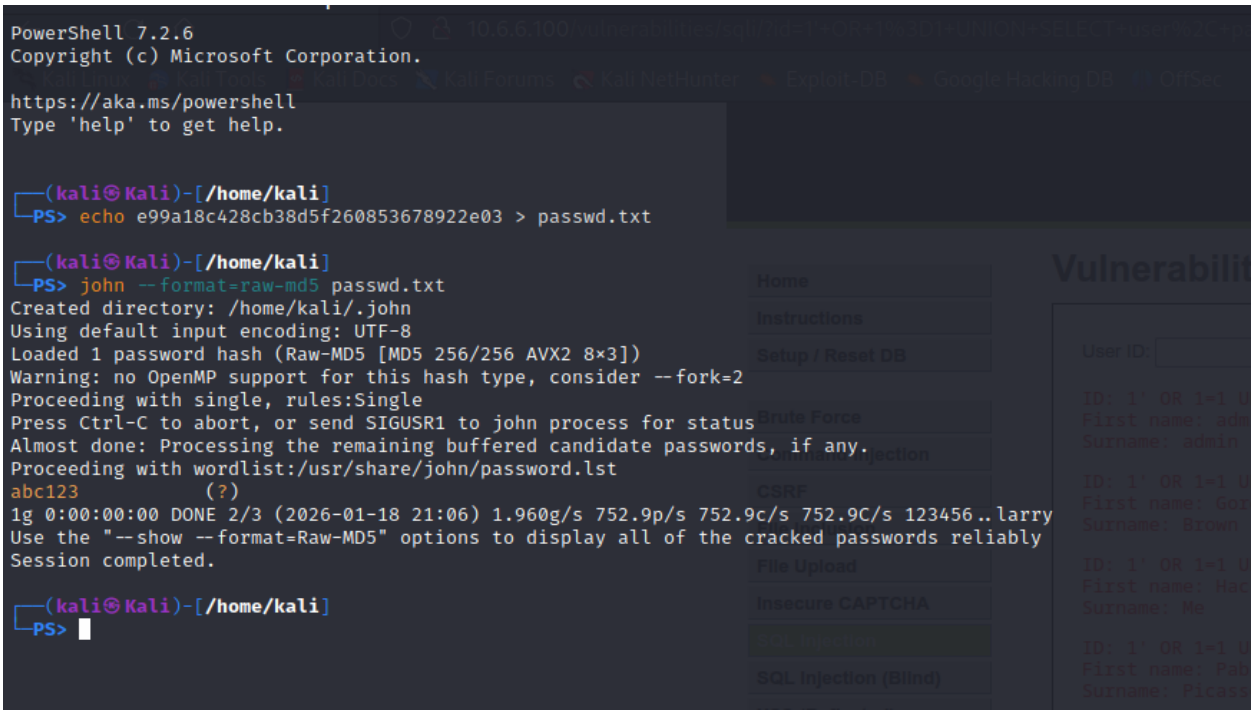


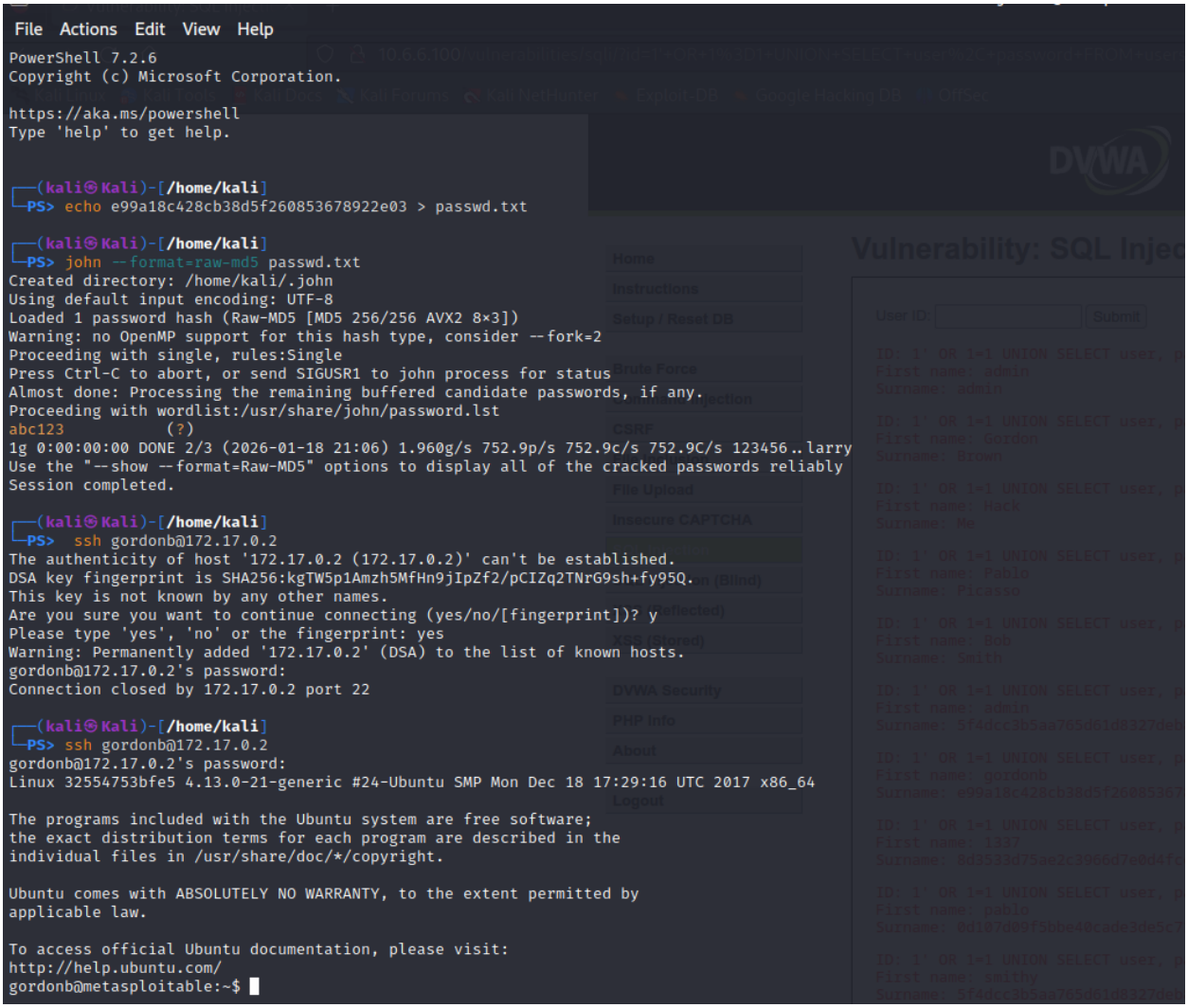
b. Locate a vulnerable input form that will allow you to inject SQL commands.

c. Retrieve the username and the password hash for **Gordon Brown's** account.

Step 3: Crack Gordon Brown's account password.

Use any password hash cracking tool desired to crack Gordon Brown's password.

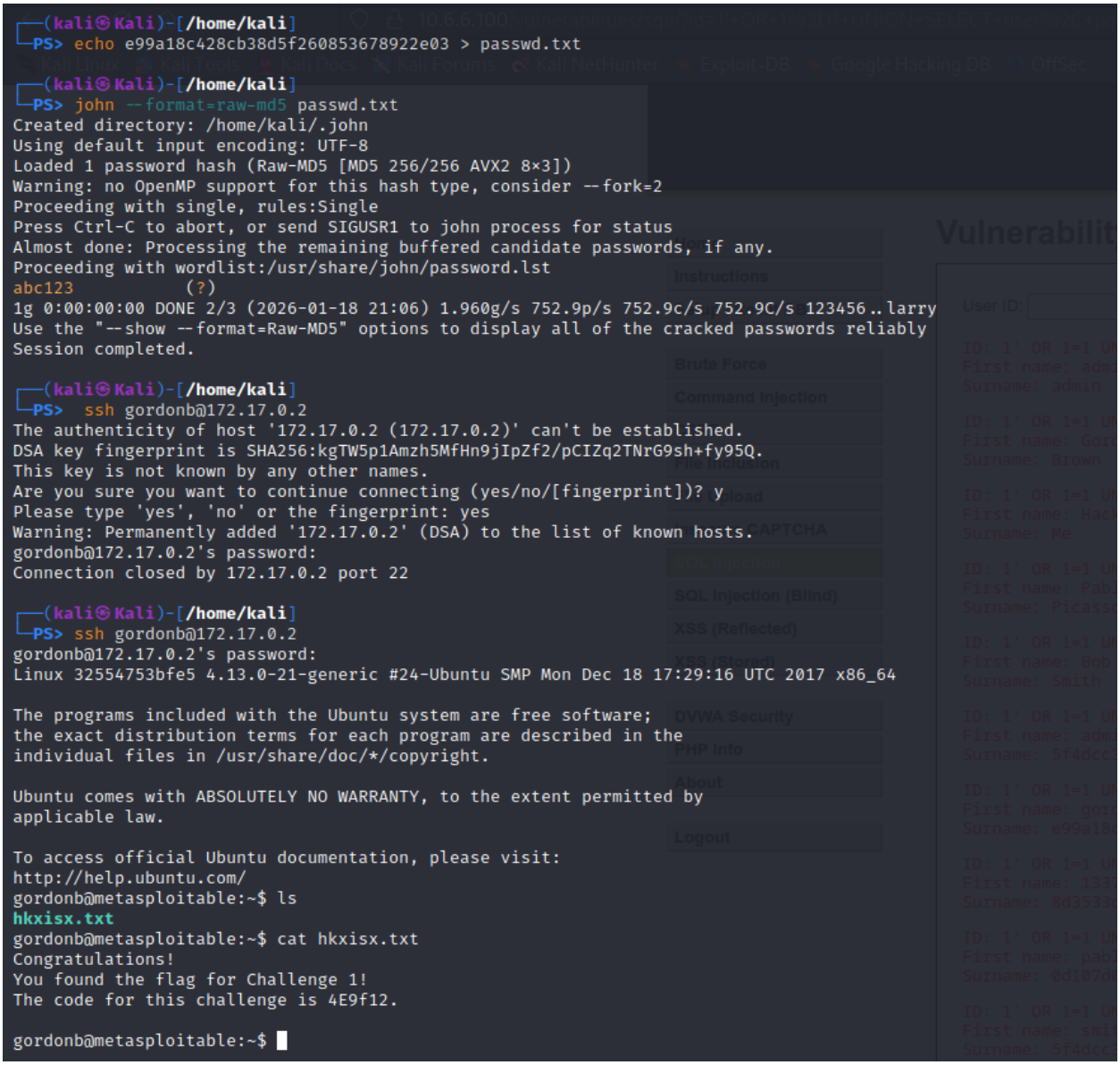




Step 4: Locate and open the file with Challenge 1 code.

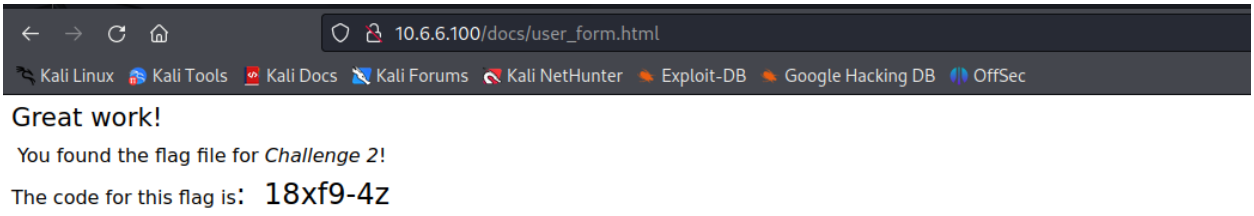
a. Log into **172.17.0.2** as **Gordon Brown**.

b. Locate and open the flag file in the user's home directory.



Challenge 2: Web Server Vulnerabilities

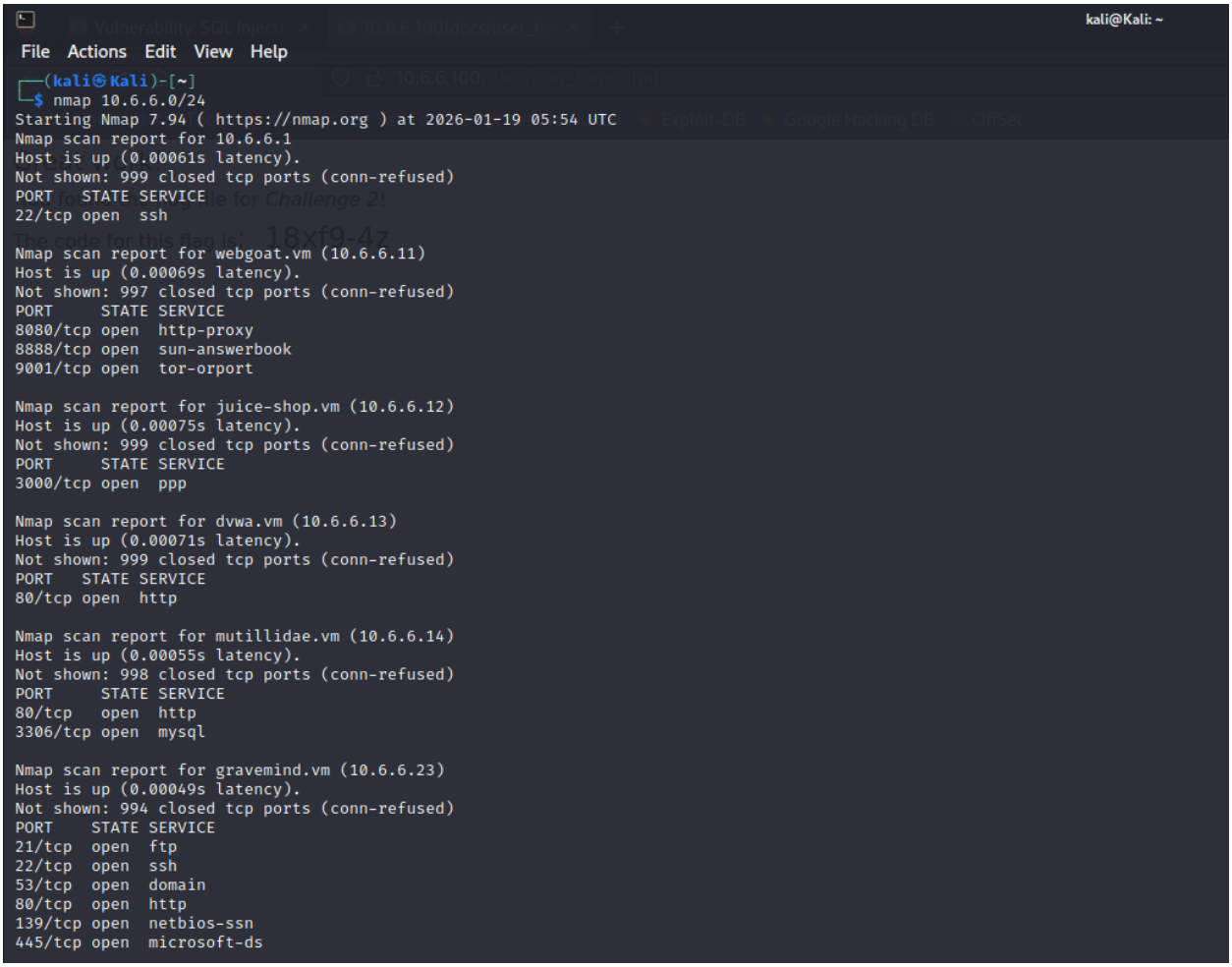
In this part, you must find vulnerabilities on an HTTP server. Misconfiguration of a web server can allow for the listing of files contained in directories on the server. You can use any of the tools you learned in earlier labs to perform reconnaissance to find the vulnerable directories.

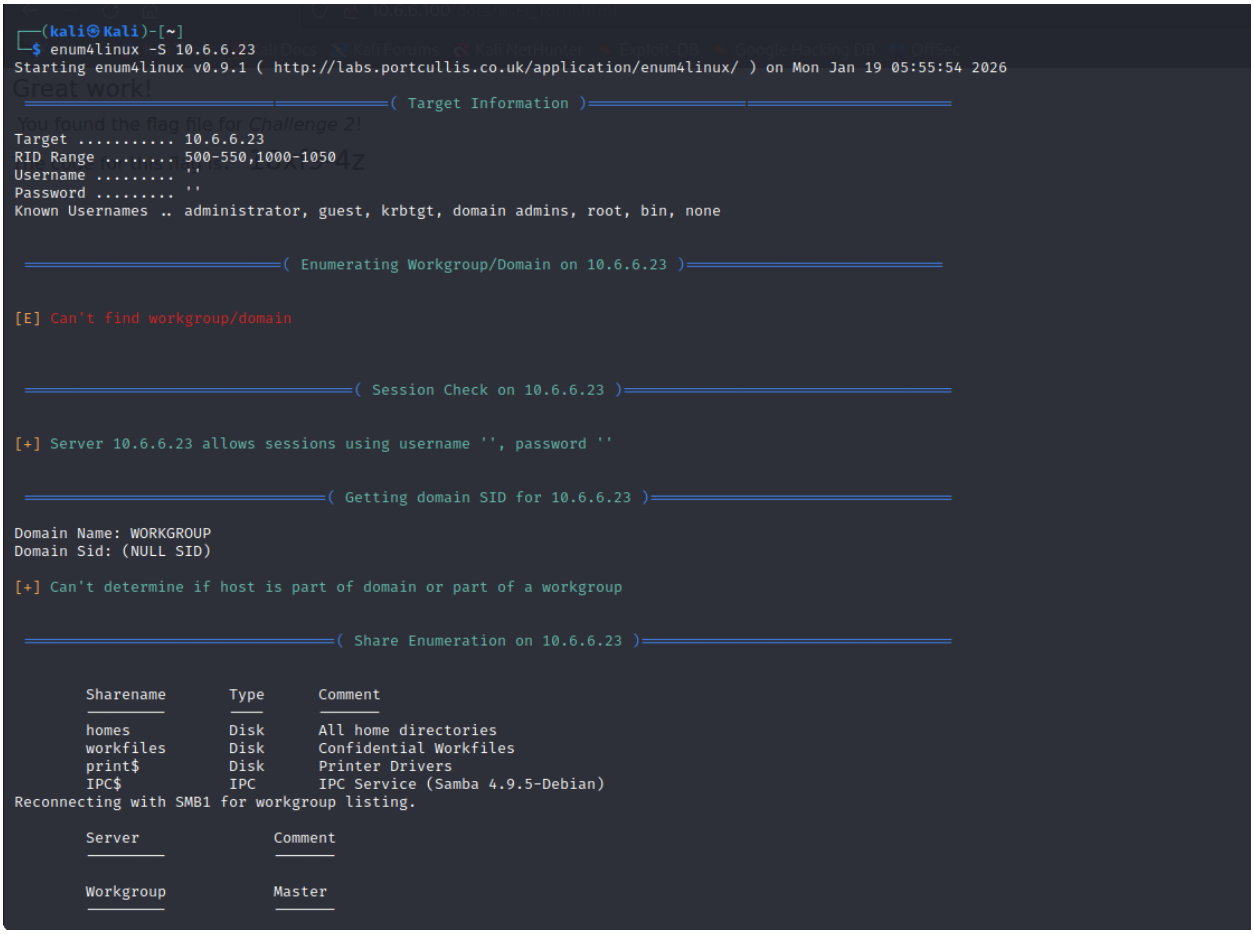


Challenge 3: Exploit open SMB Server Shares

Total points: 25

In this part, you want to discover if there are any unsecured shared directories located on an SMB server in the 10.6.6.0/24 network. You can use any of the tools you learned in earlier labs to find the drive shares available on the servers.





```
kali@Kali: ~
File  Actions  Edit  View  Help
[E] Can't understand response:

tree connect failed: NT_STATUS_BAD_NETWORK_NAME
//10.6.6.23/homes       Mapping: N/A Listing: N/A Writing: N/A
//10.6.6.23/workfiles   Mapping: OK Listing: OK Writing: N/A
//10.6.6.23/print$      Mapping: OK Listing: OK Writing: N/A
[E] Can't understand response:

NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
//10.6.6.23/IPC$        Mapping: N/A Listing: N/A Writing: N/A
enum4linux complete on Mon Jan 19 05:56:07 2026


┌──(kali㉿Kali)-[~]
└─$

┌──(kali㉿Kali)-[~]
└─$ smbclient //10.6.6.23/print$
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Aug 14 09:40:01 2023
  ..                                  D        0  Mon Aug 30 05:00:05 2021
  IA64                                D        0  Mon Sep  2 13:39:42 2019
  x64                                 D        0  Mon Aug 30 05:00:05 2021
  W32X86                              D        0  Mon Aug 30 05:00:05 2021
  W32MIPS                             D        0  Mon Sep  2 13:39:42 2019
  W32ALPHA                            D        0  Mon Sep  2 13:39:42 2019
  COLOR                               D        0  Mon Sep  2 13:39:42 2019
  W32PPC                              D        0  Mon Sep  2 13:39:42 2019
  WIN40                               D        0  Mon Sep  2 13:39:42 2019
  OTHER                               D        0  Tue Aug 10 00:00:00 2021
  color                               D        0  Mon Aug 30 05:00:05 2021

                38497656 blocks of size 1024. 8451648 blocks available
smb: \> cd OTHER
smb: \OTHER\> get taxes.txt
getting file \OTHER\taxes.txt of size 103 as taxes.txt (3.5 KiloBytes/sec) (average 3.5 KiloBytes/sec)
smb: \OTHER\> exit

┌──(kali㉿Kali)-[~]
└─$ cat taxes.txt
Congratulations!
You found the flag for Challenge 3!
The code for this challenge is A9!15wa2.
```

Challenge 4: Analyze a PCAP File to Find Information.