Derrick Mokaya CS-EH03-25219 Final Capstone Project

Objectives

For this Final Capstone Activity, I conducted a complete penetration test starting with reconnaissance and then launching exploits against discovered vulnerabilities. Finally, proposed remediation for the exploits.

This assessment was in the form of a cybersecurity capture the flag exercise. I used my ethical hacking skills to locate files that contained flag values. I then reported the flag values that I found as part of the assessment.

In this simulation of an ethical hacking engagement, I used tools to exploit vulnerabilities that I discovered in order to reach a goal. This entailed a trial-and-error approach that required persistence and included a degree of struggle. For my own skill development, working through this struggle was very productive.

- **Challenge 1** – Used SQL injection to find a flag file.
- **Challenge 2** – Used web server vulnerabilities to investigate directories and found a flag file.
- **Challenge 3** – Exploited open Samba shares to access a flag file.
- **Challenge 4** – Analyzed a Wireshark capture file to find the location of a file containing flag information.

Background / Scenario

I was hired to conduct a penetration test for a customer. At the conclusion of the test, the customer requested a complete report that included any vulnerabilities discovered, successful exploits, and remediation steps to protect vulnerable systems. I had access to hosts on the 10.5.5.0 and 192.168.0.0/24 networks.

Required Resources

- Kali VM customized for the Ethical Hacker course

Instructions

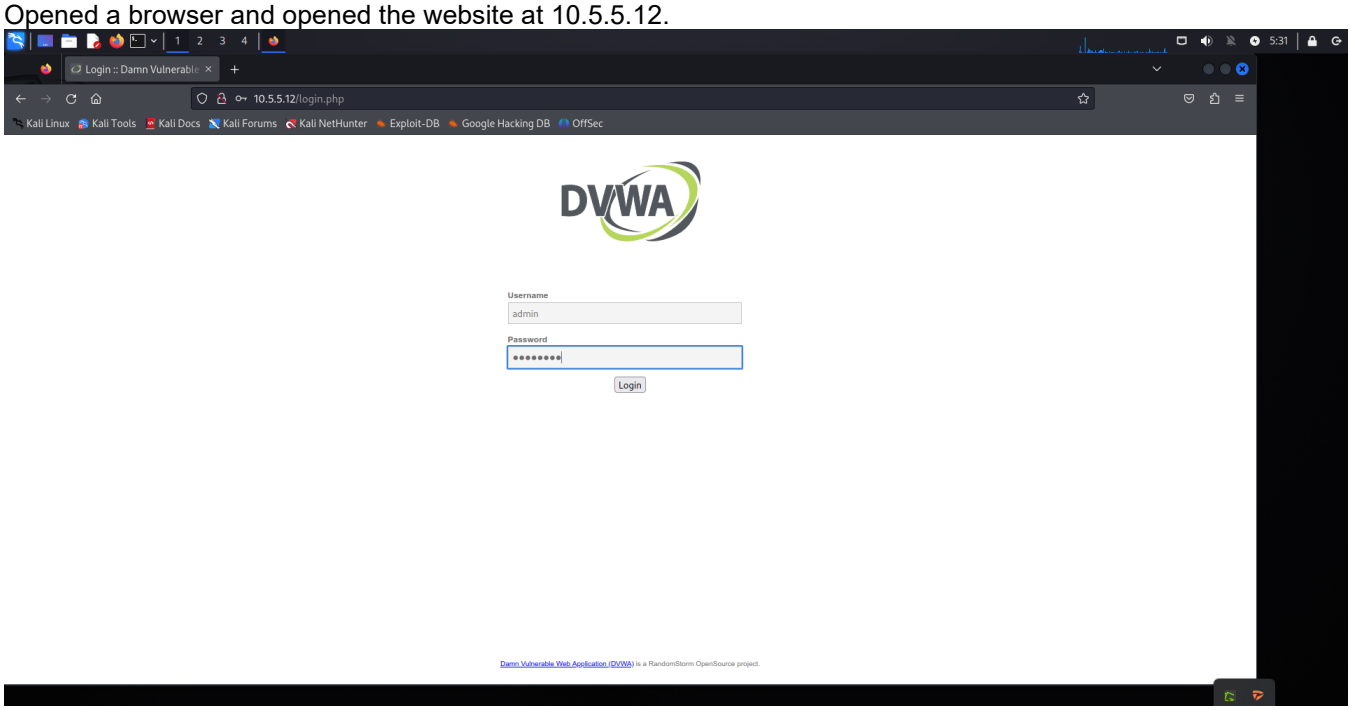
Challenge 1: SQL Injection

Total points: 25

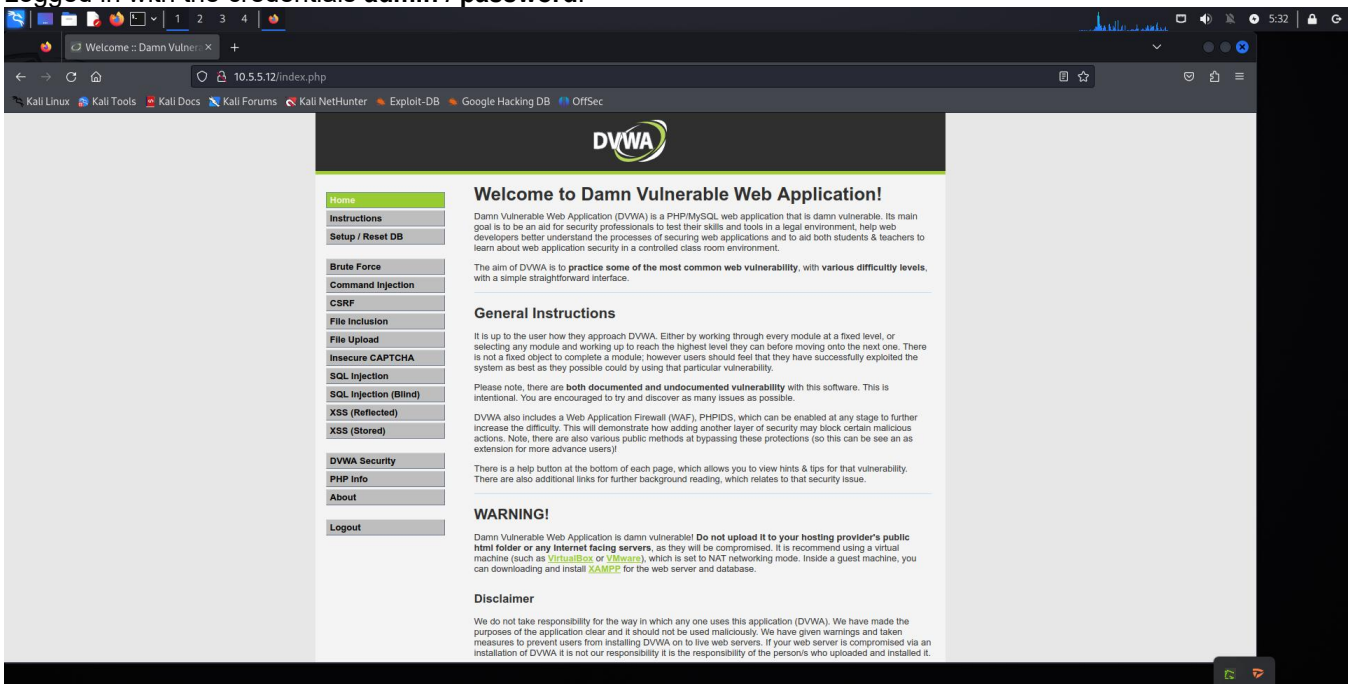
In this part, I had to discover user account information on a server and crack the password of **Bob Smith's** account. I then located the file with Challenge 1 code and used **Bob Smith's** account credentials to open the file at 192.168.0.10 to view its contents.

Step 1: Preliminary setup

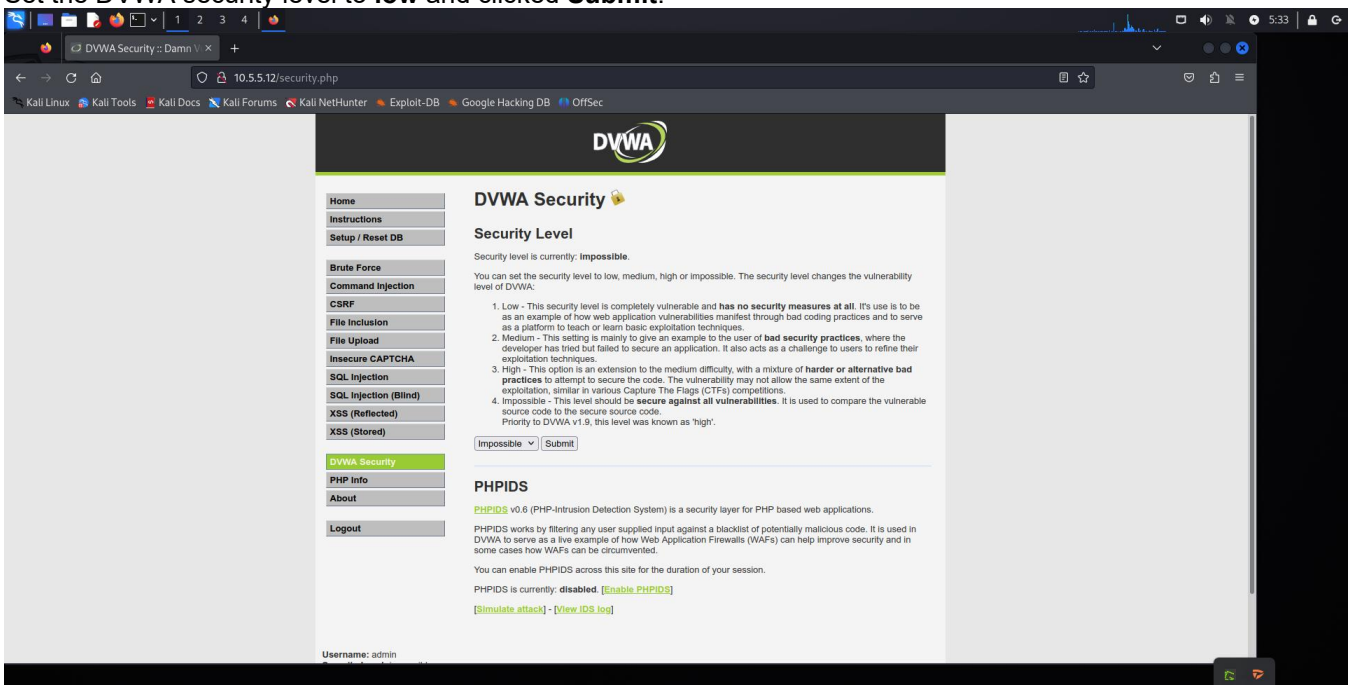
a. Opened a browser and opened the website at 10.5.5.12.

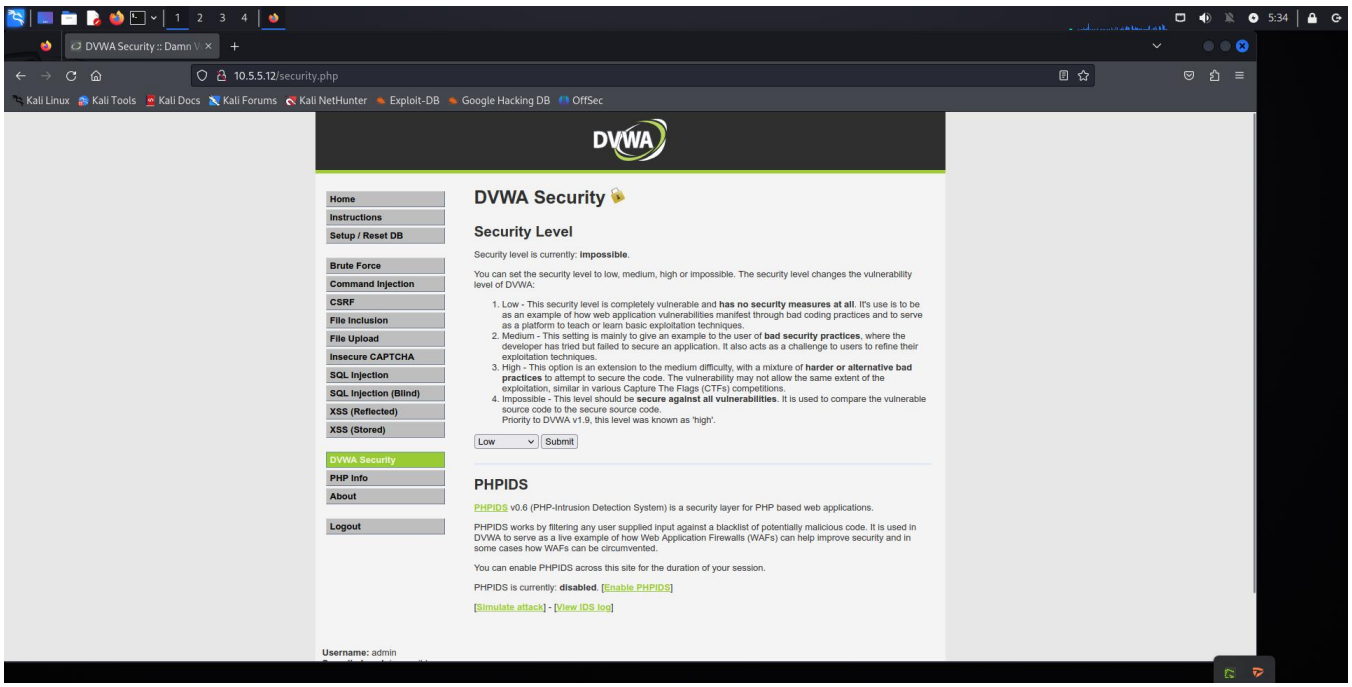


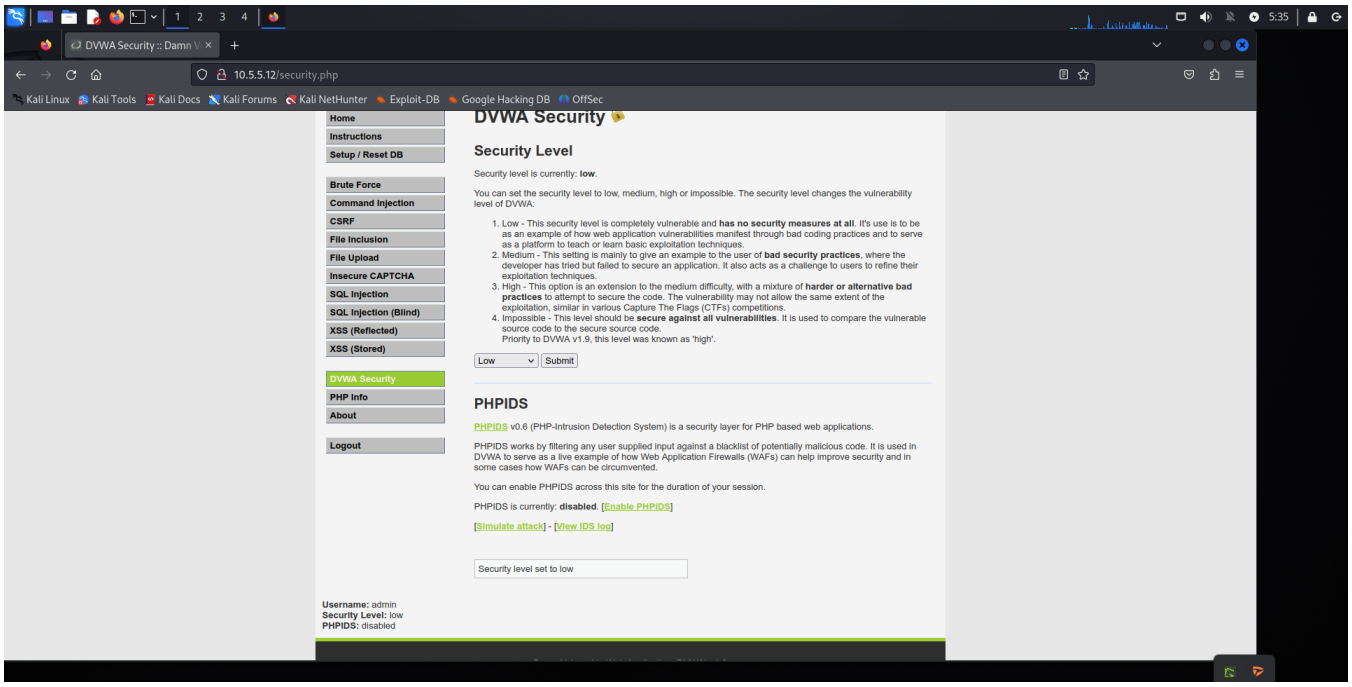
b. Logged in with the credentials **admin / password**.



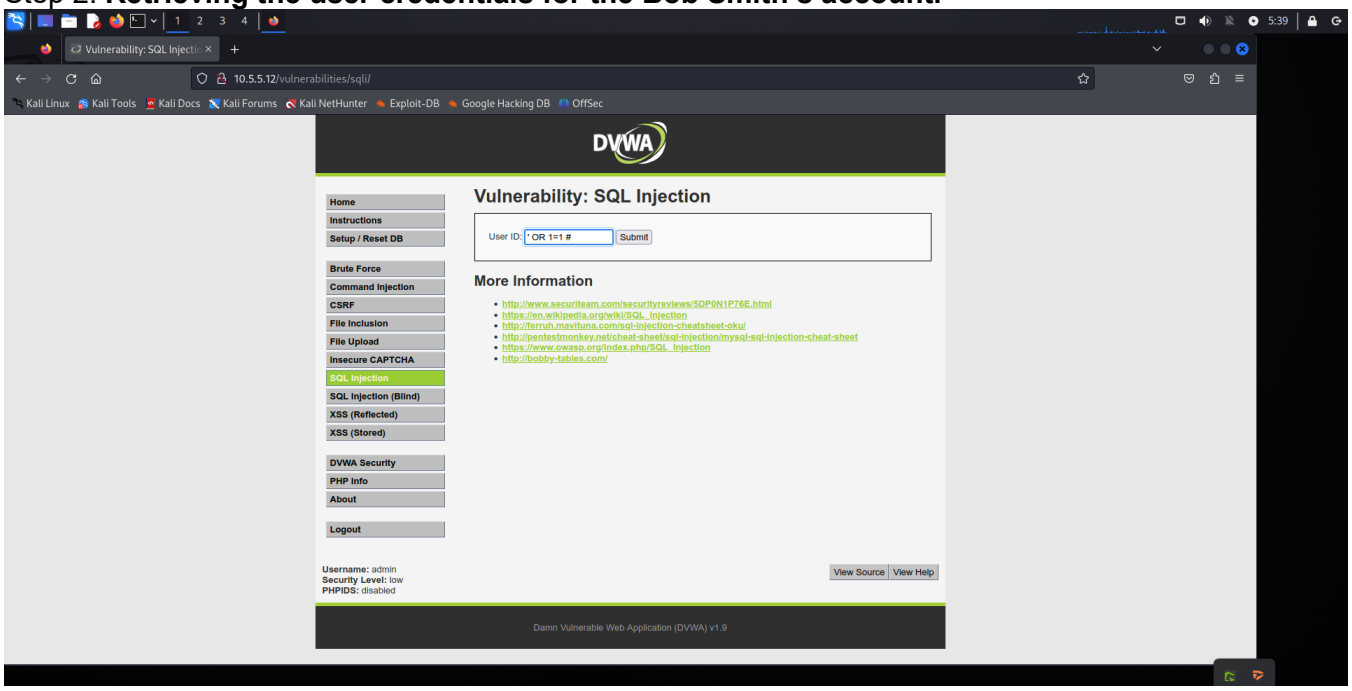
c. Set the DVWA security level to **low** and clicked **Submit**.

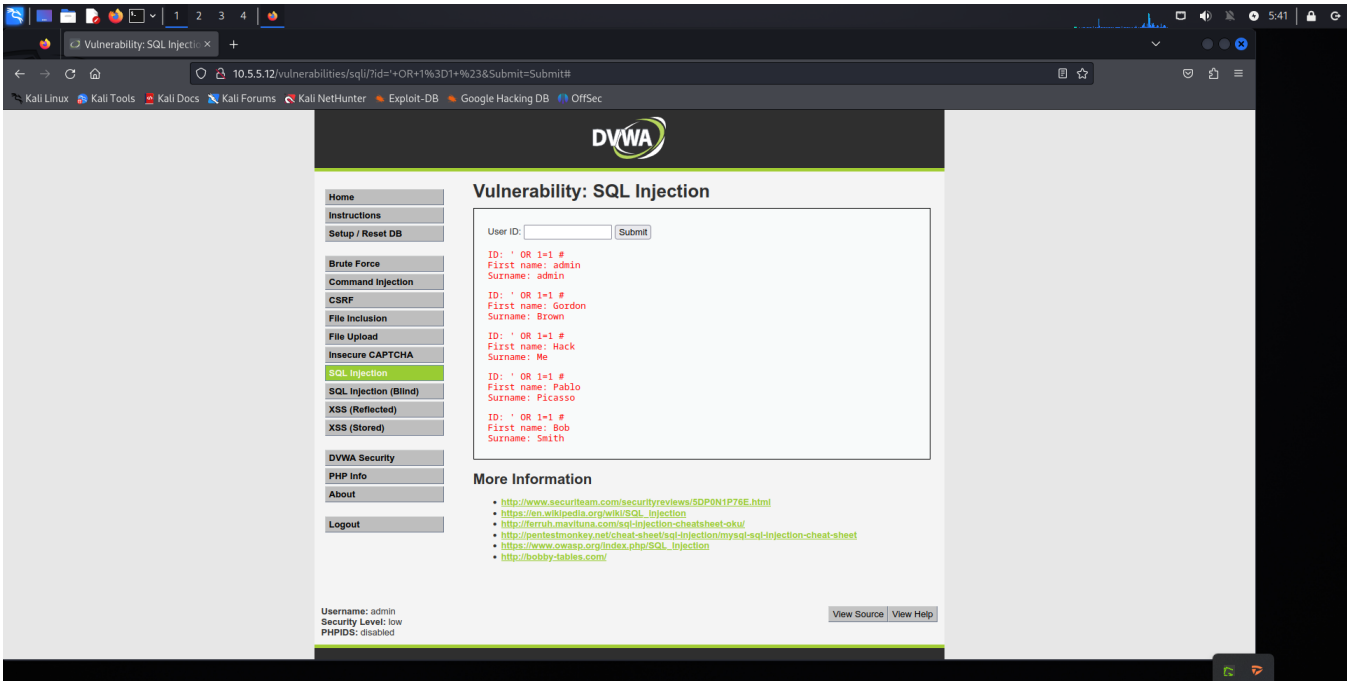


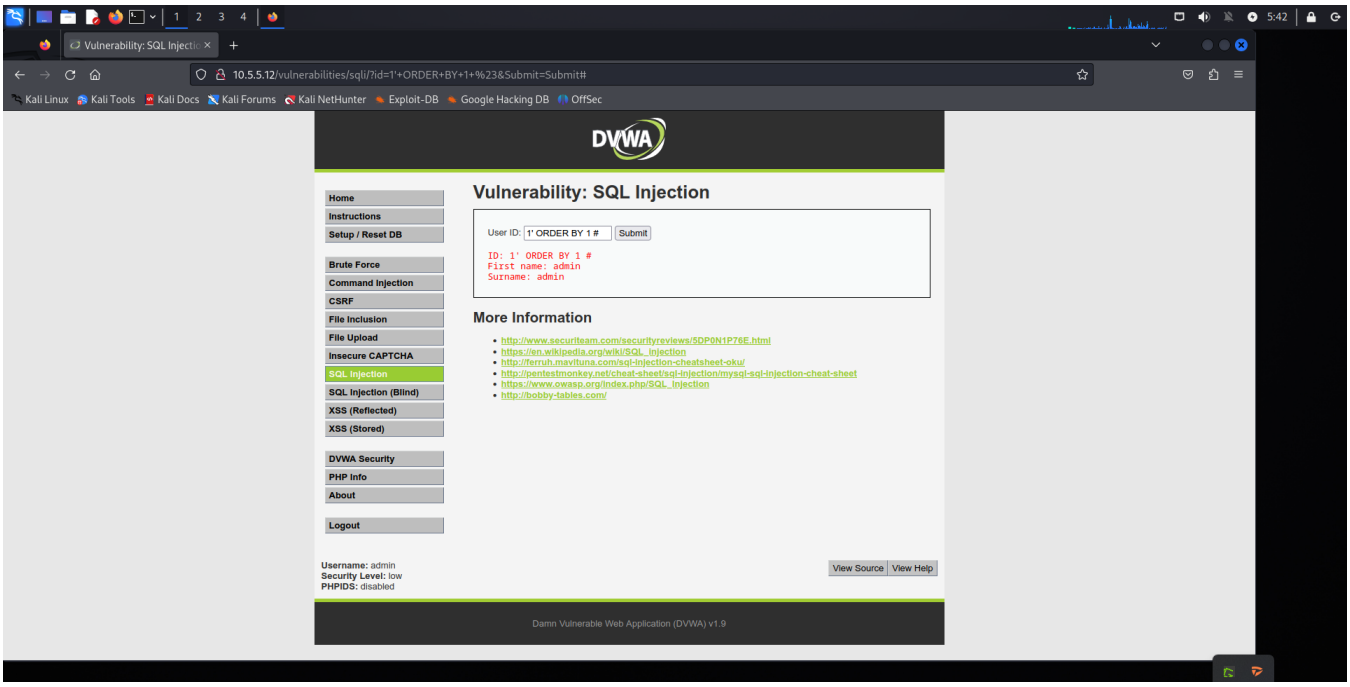


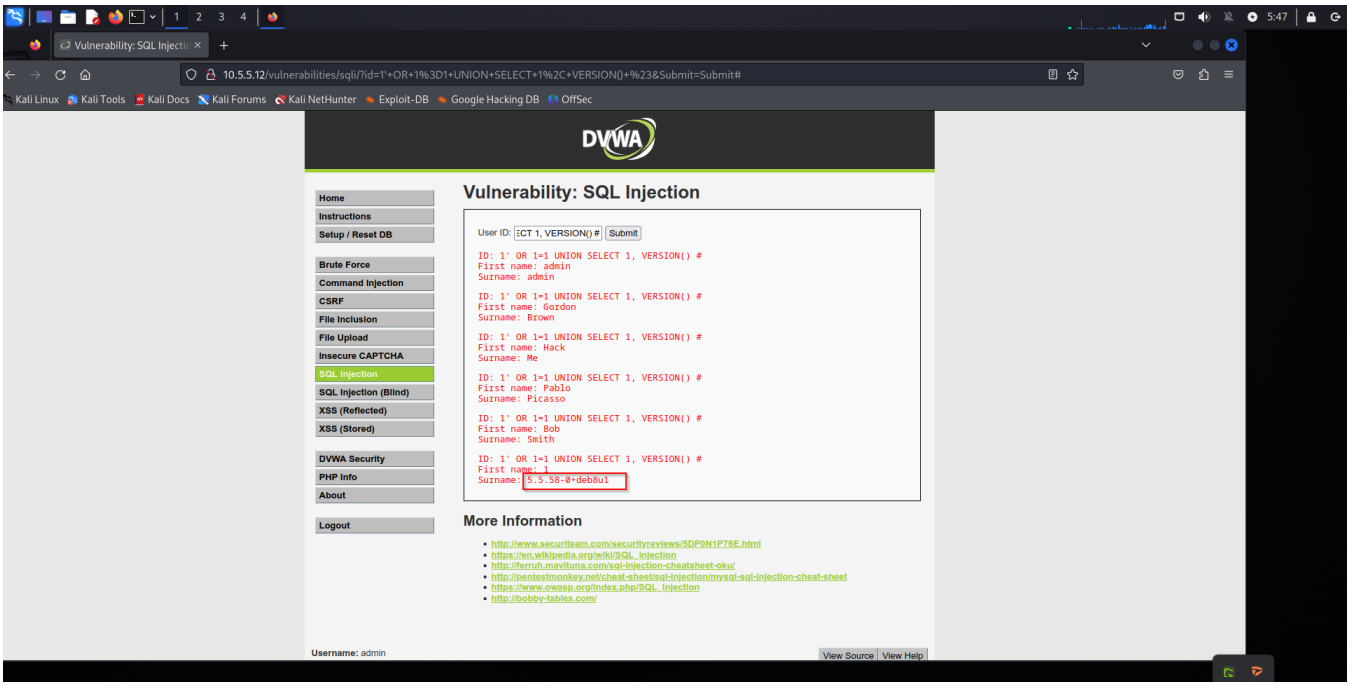


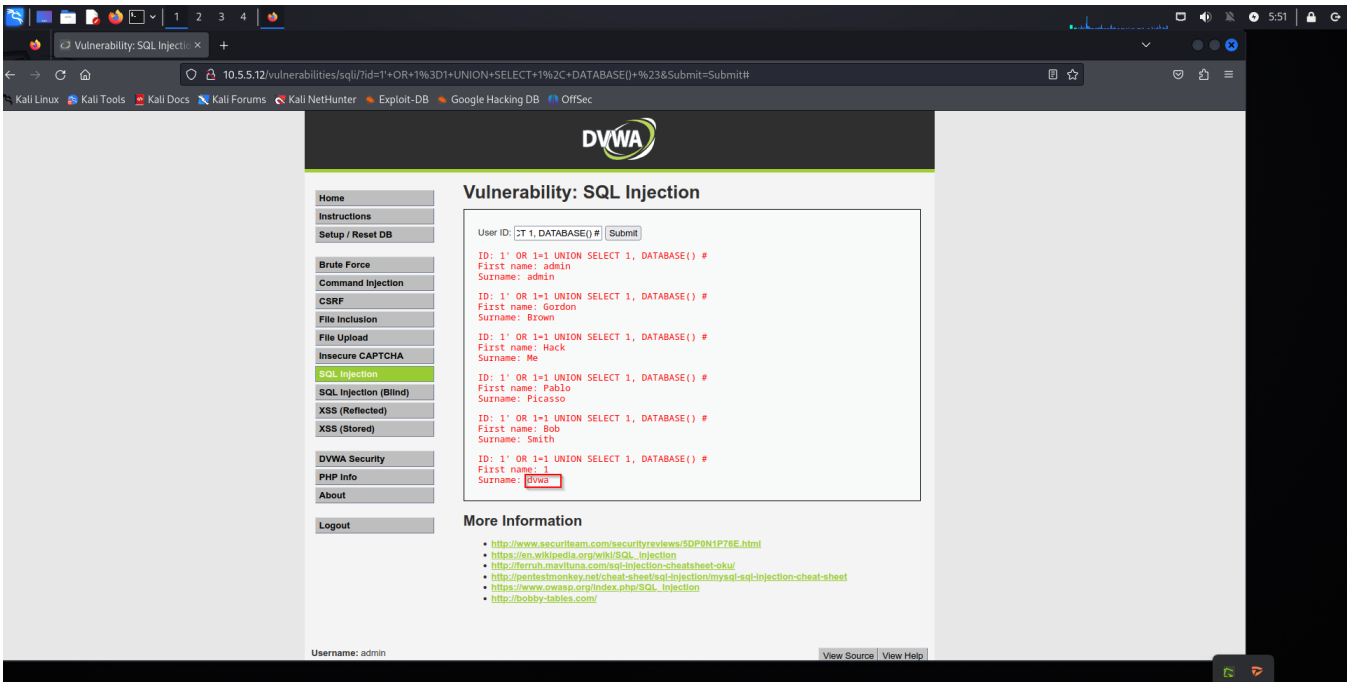
Step 2: **Retrieving the user credentials for the Bob Smith's account.**

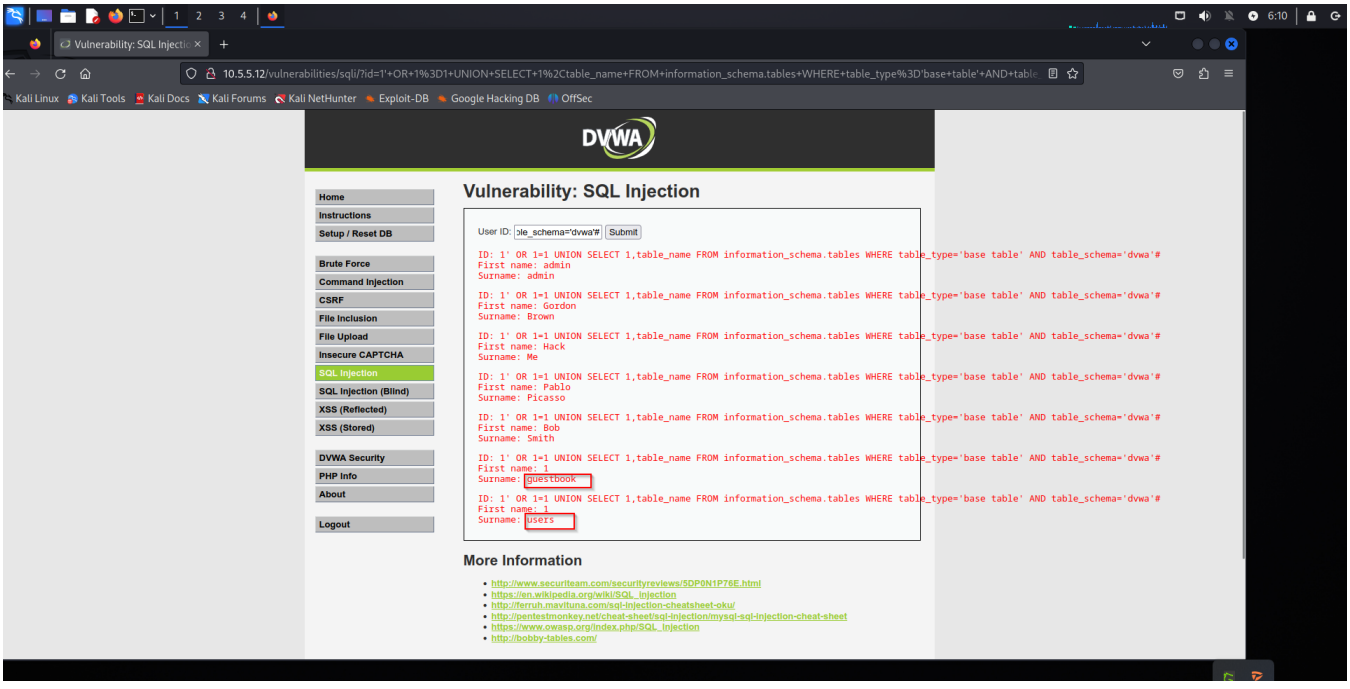


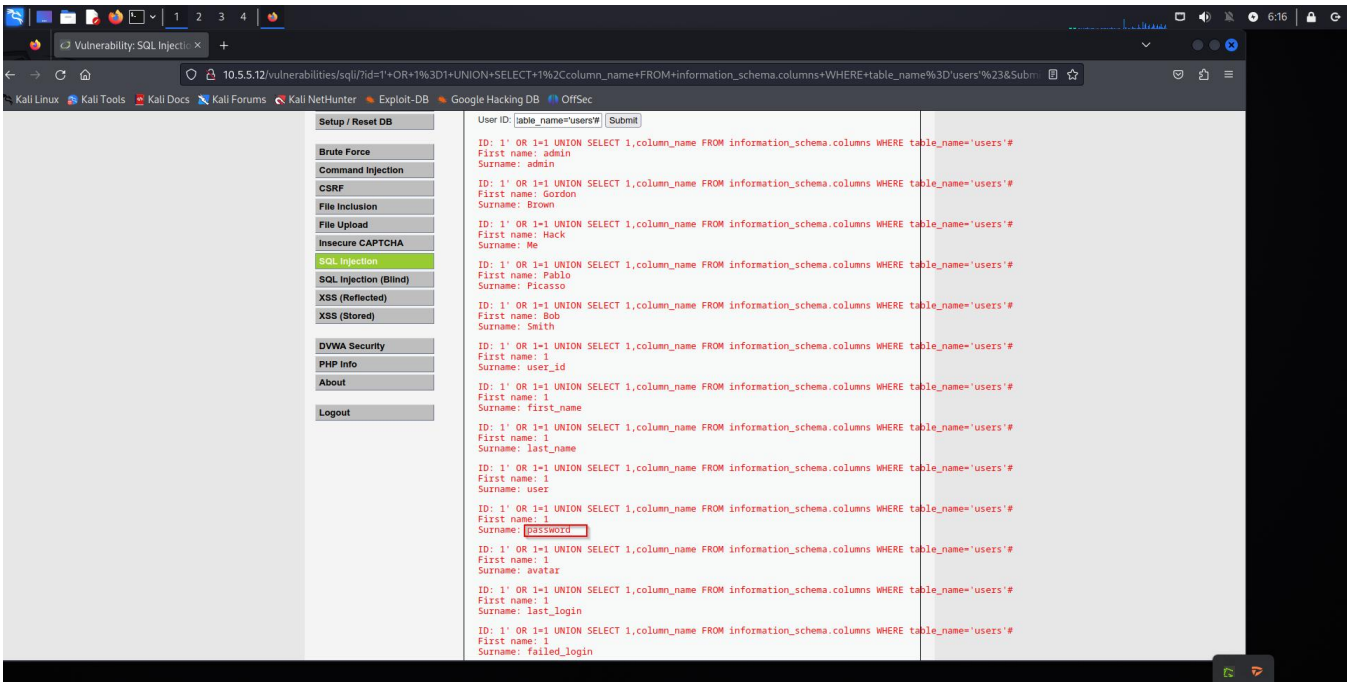


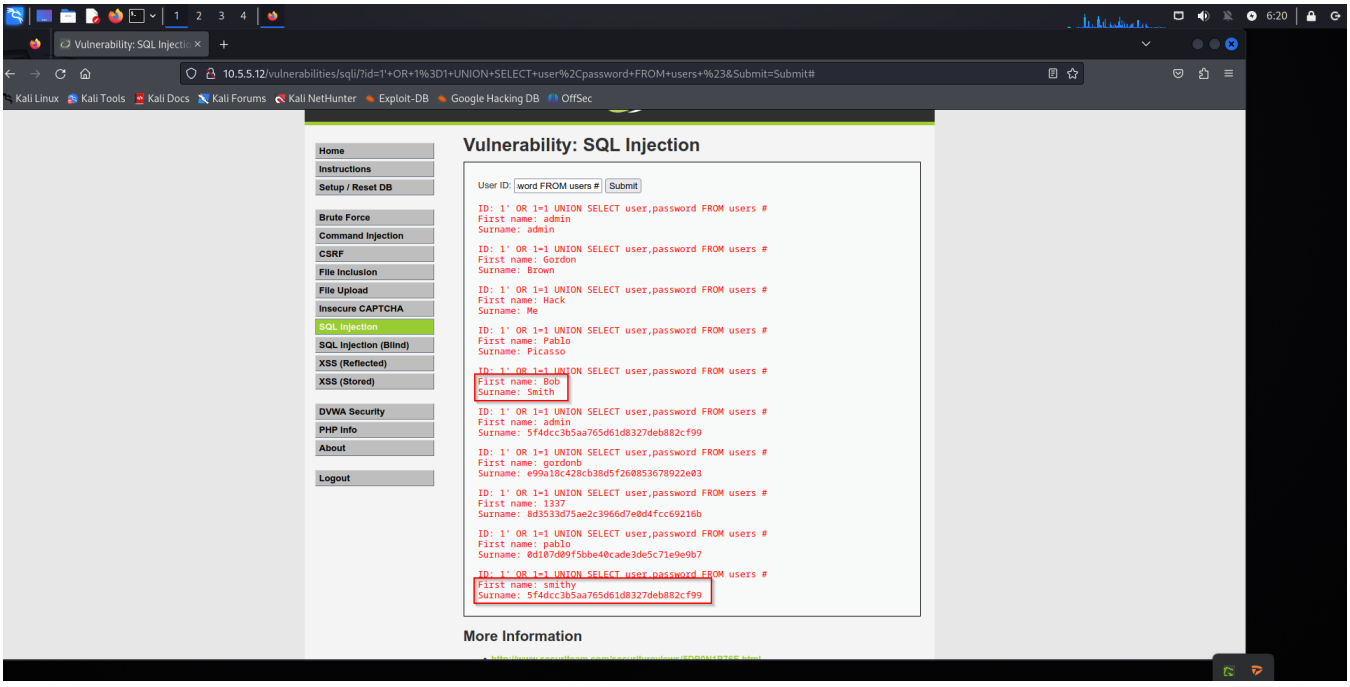












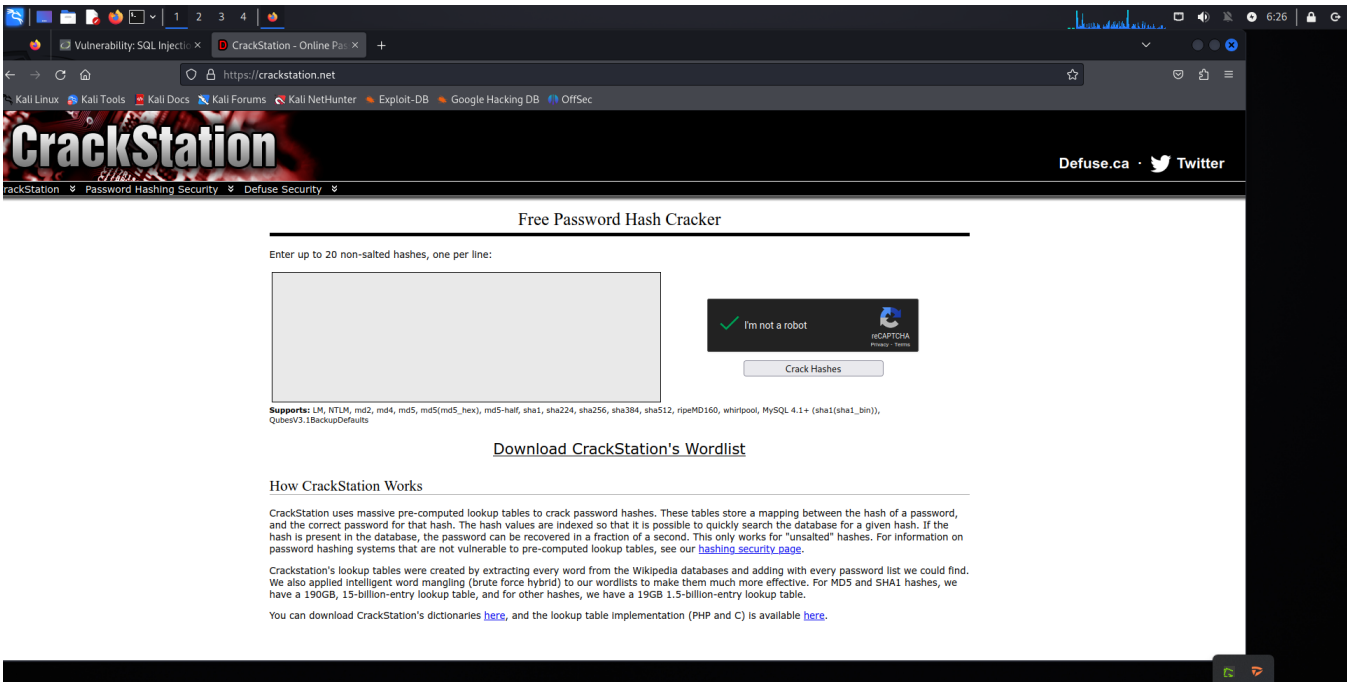
a. Identified the table that contained usernames and passwords.

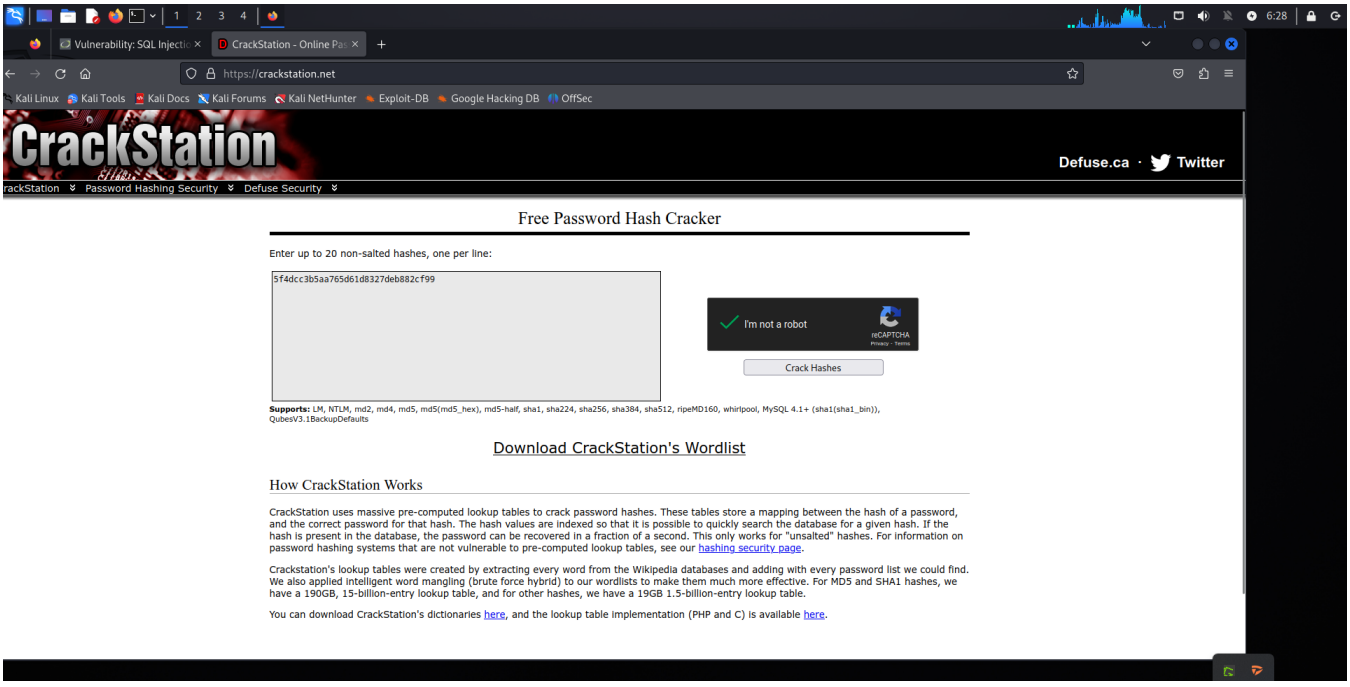
b. Located a vulnerable input form that allowed me to inject SQL commands.

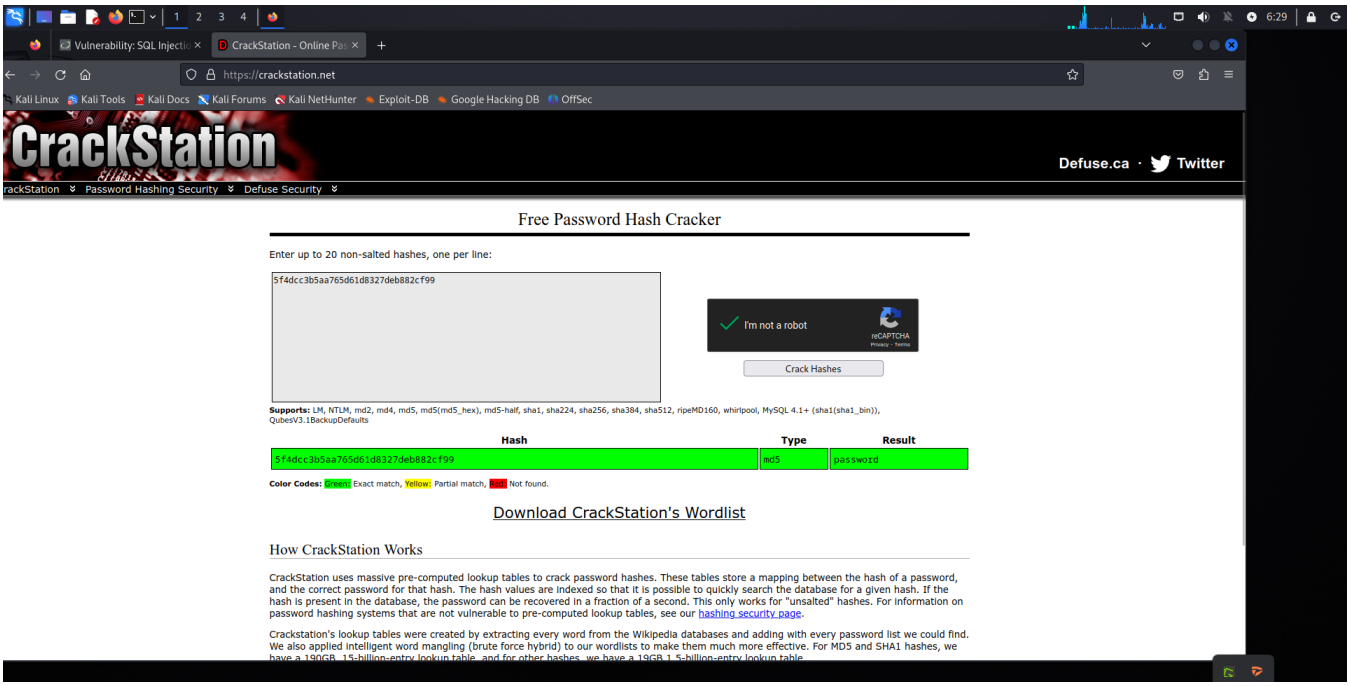
c. Retrieved the username and the password hash for **Bob Smith's** account.

Step 3: Cracking Bob Smith's account password.

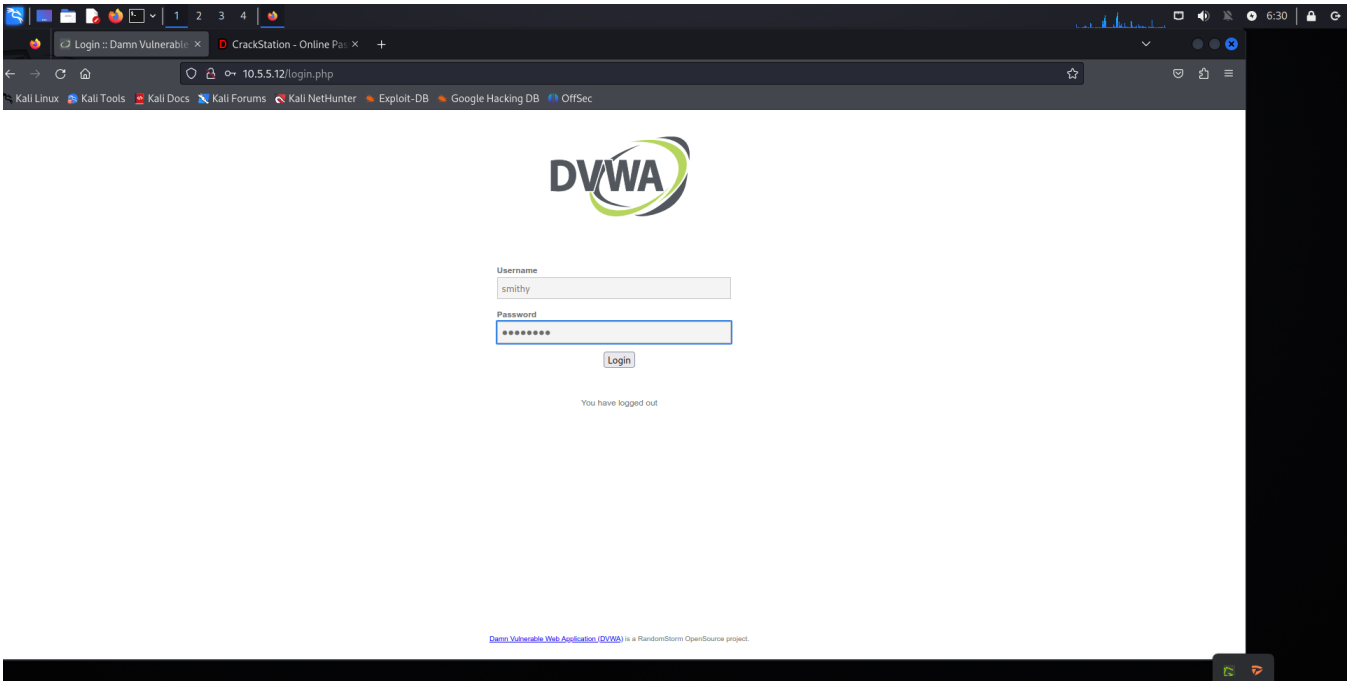
Used password hash cracking tool crackstation.net to crack **Bob Smith**'s password.

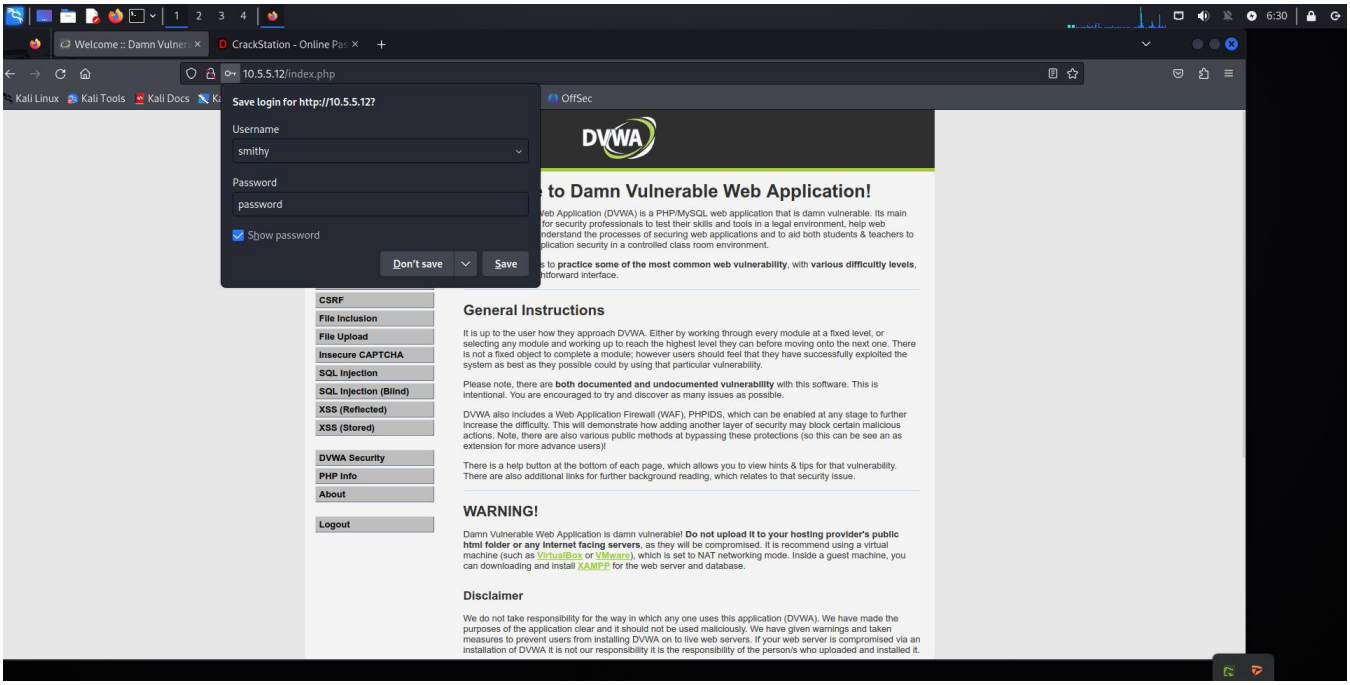






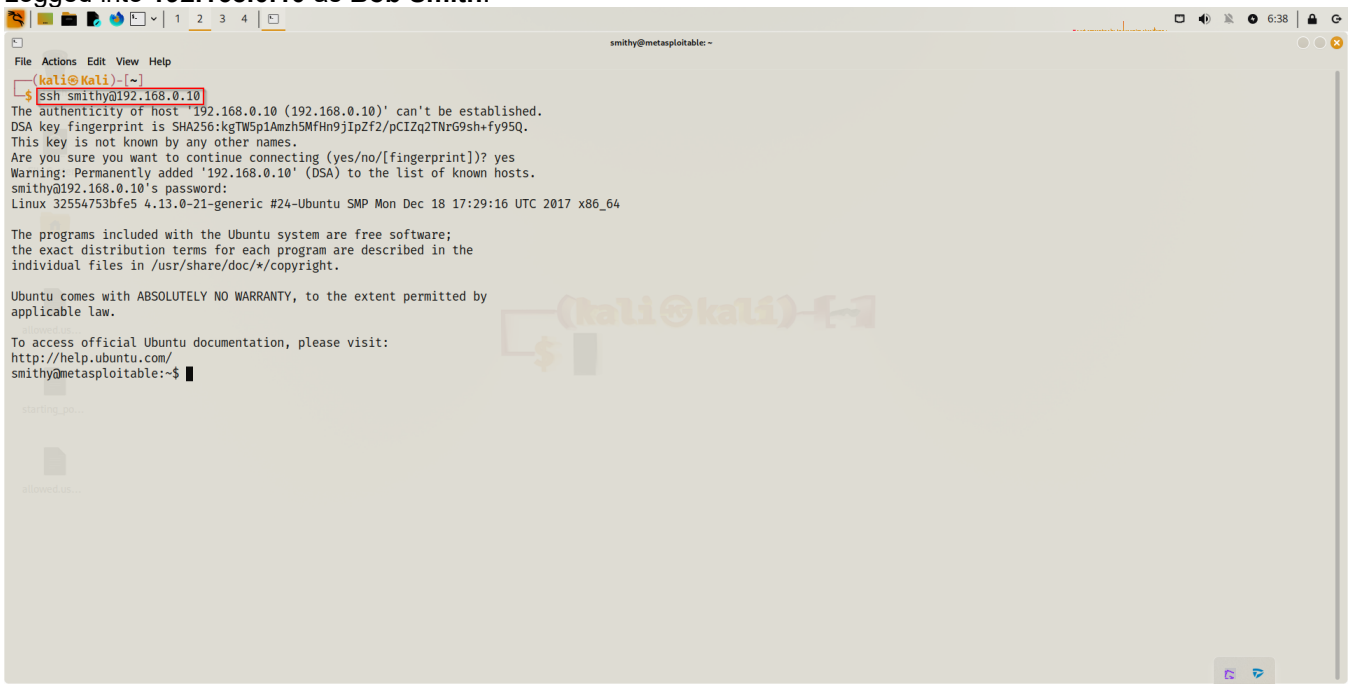
The password of **Bob Smith's** account was found to be…password



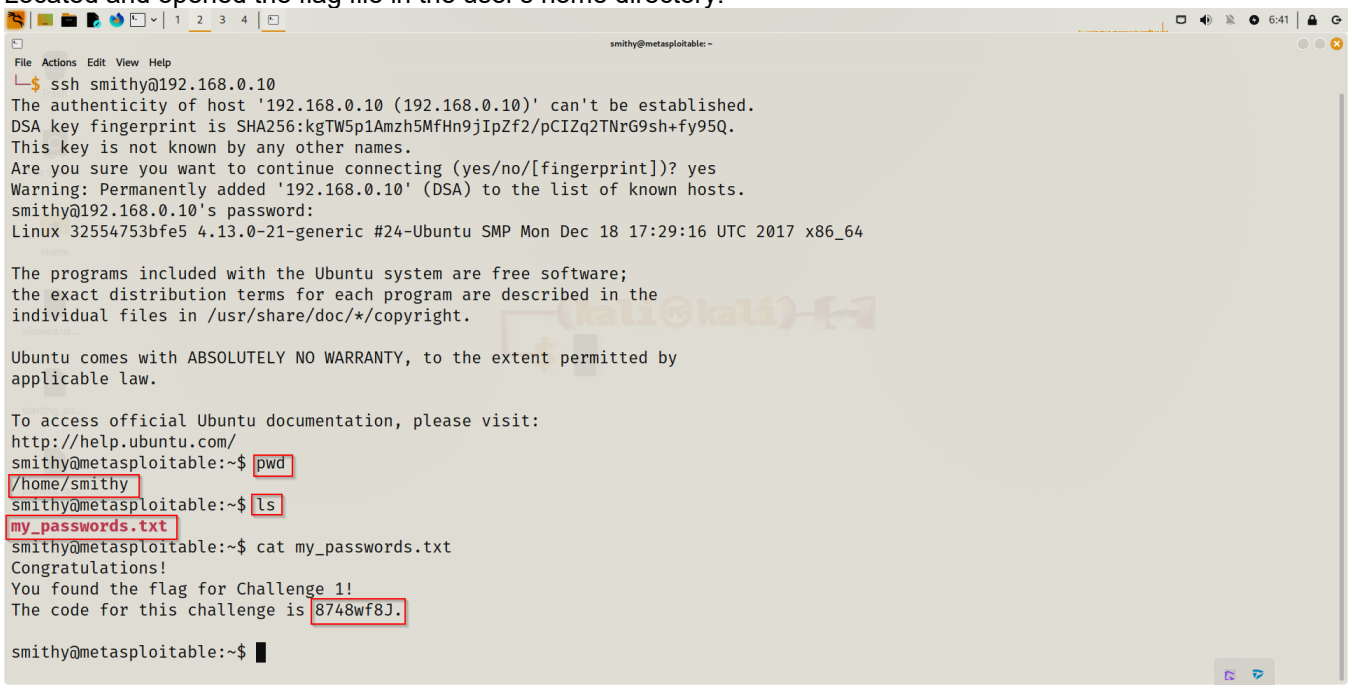


Step 4: Locating and opening the file with Challenge 1 code.

a. Logged into **192.168.0.10** as **Bob Smith**.



b. Located and opened the flag file in the user's home directory.

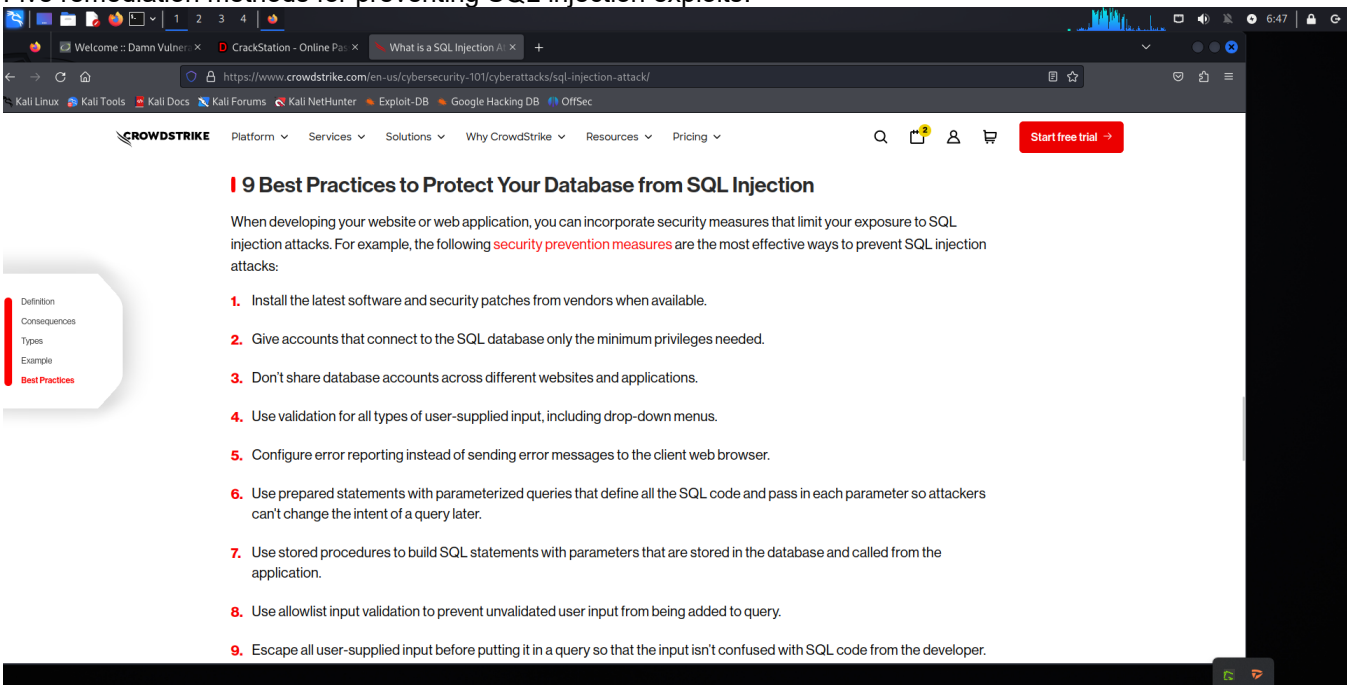


The name of the file with the code was found to be… my_passwords.txt

The message contained in the file was found to be…. 8748wf8j

Step 5: Researching and proposing SQL attack remediation

Five remediation methods for preventing SQL injection exploits.



Challenge 2: Web Server Vulnerabilities

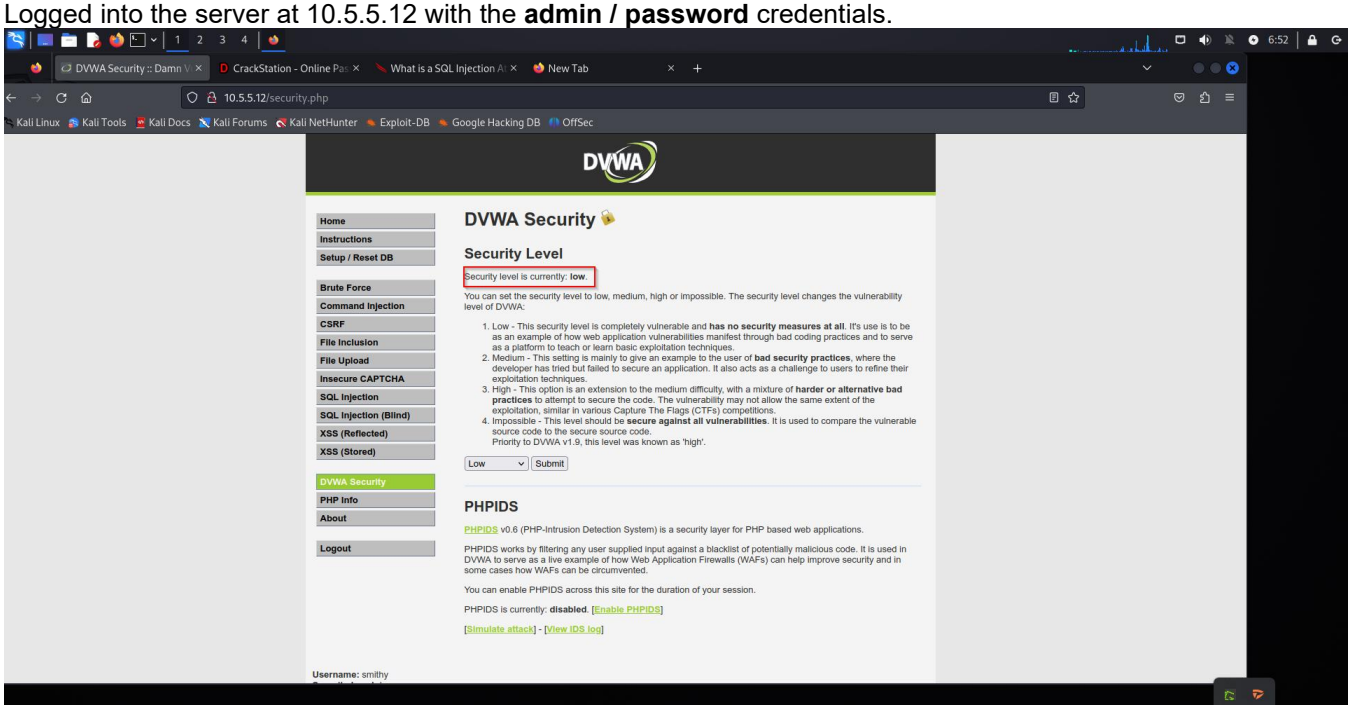
Total points: 25

In this part, I had to find vulnerabilities on an HTTP server. Misconfiguration of a web server can allow for the listing of files contained in directories on the server. I used …. to perform reconnaissance to find the vulnerable directories.

In this challenge, I located the flag file in a vulnerable directory on a web server.

Step 1: Preliminary setup

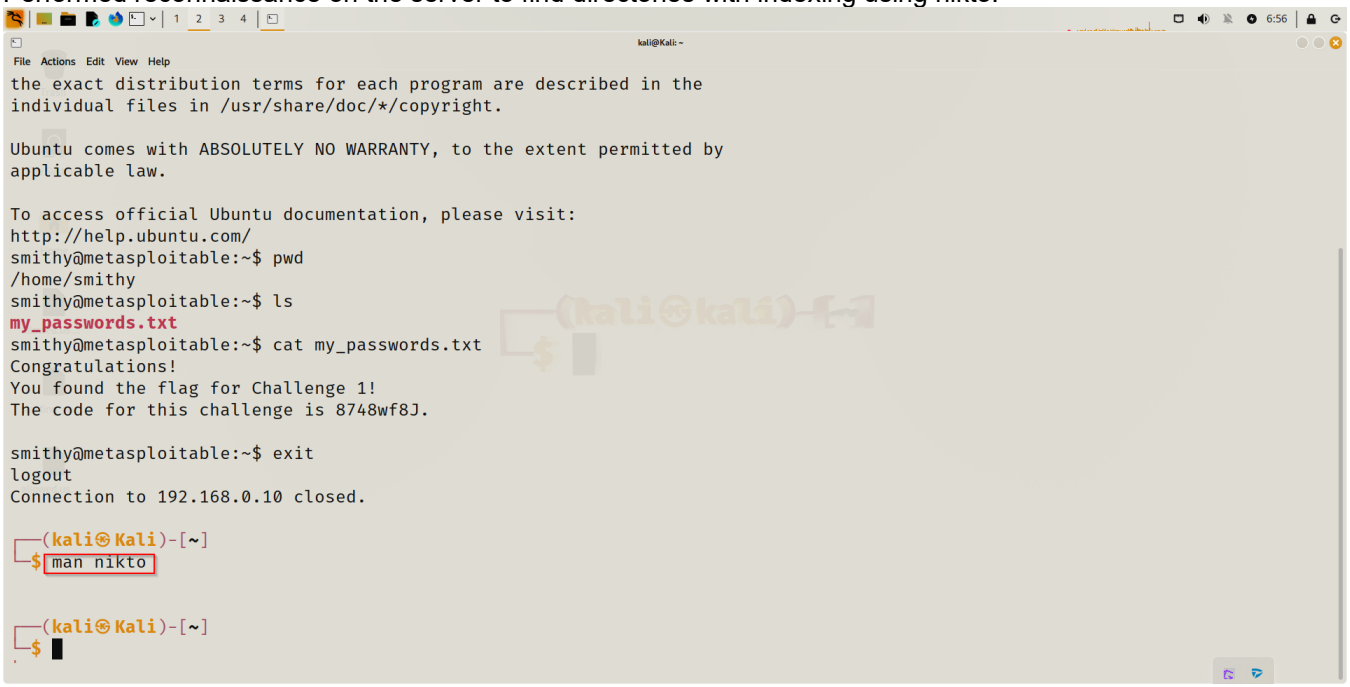
a. Logged into the server at 10.5.5.12 with the **admin / password** credentials.

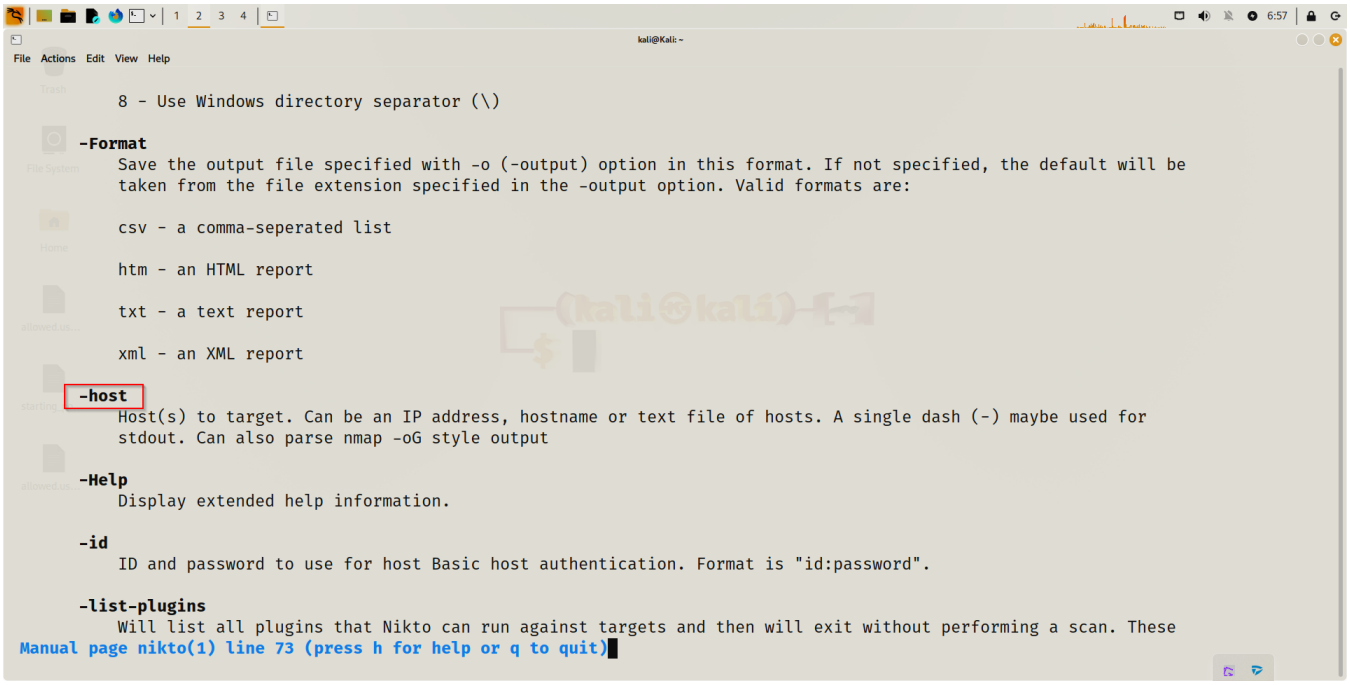


b. Set the application security level to low.

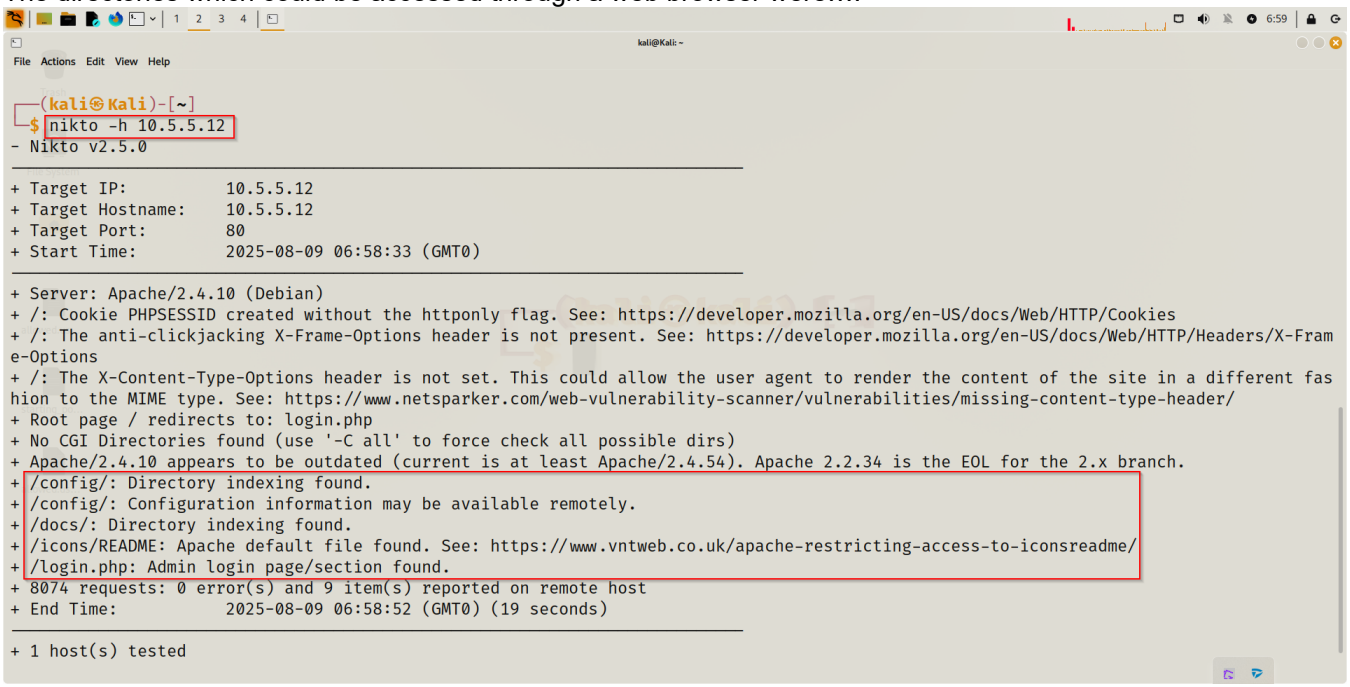
Step 2: From the results of my reconnaissance, I determined which directories were viewable using a web browser and URL manipulation.

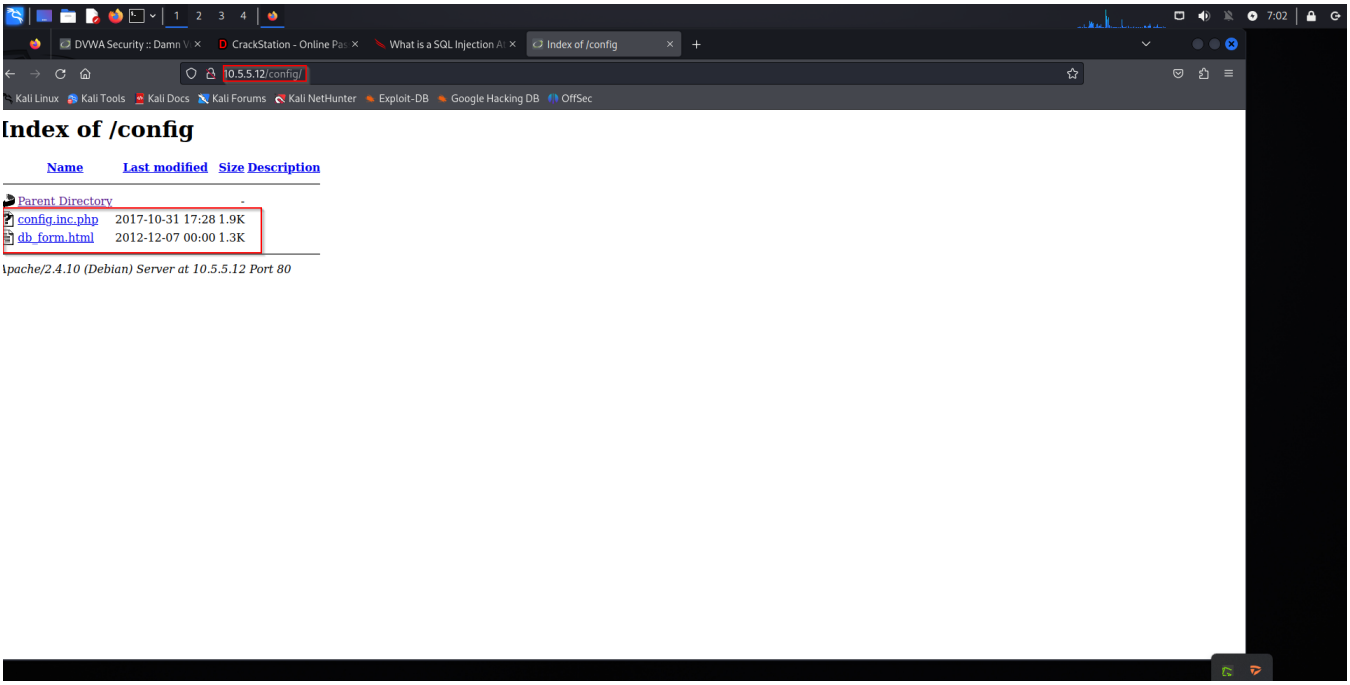
Performed reconnaissance on the server to find directories with indexing using nikto.

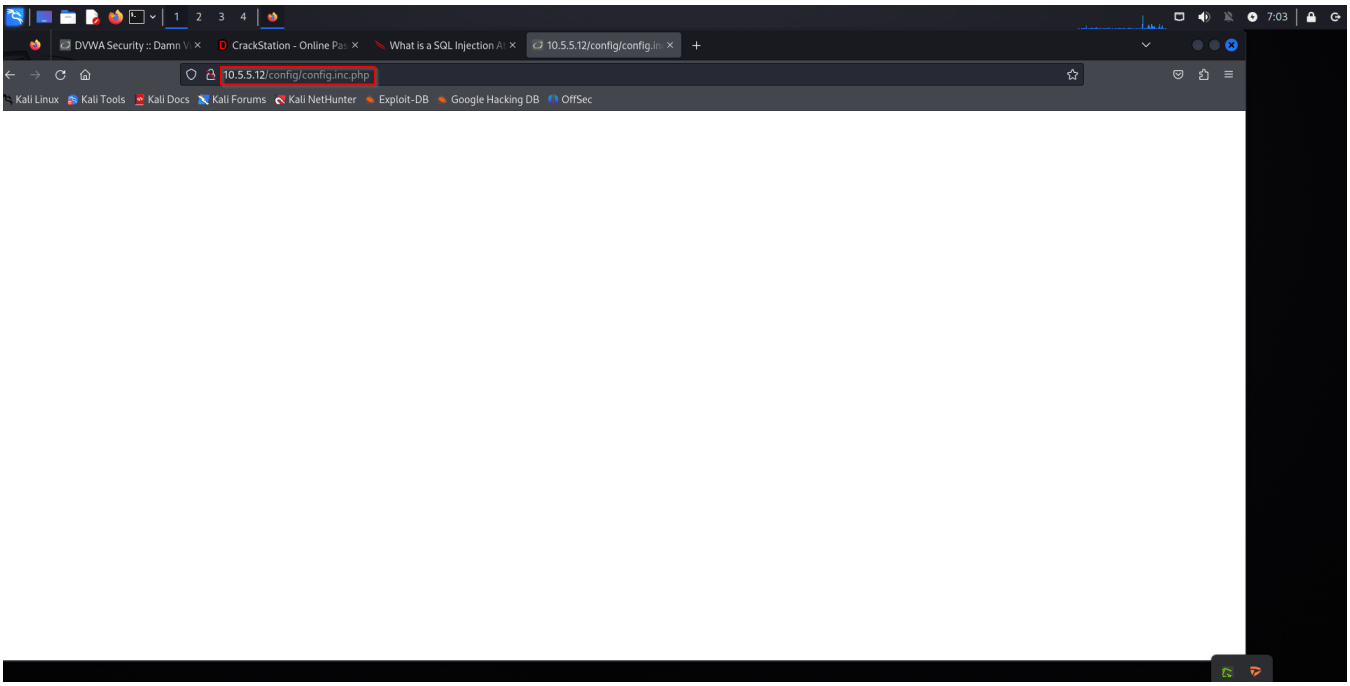


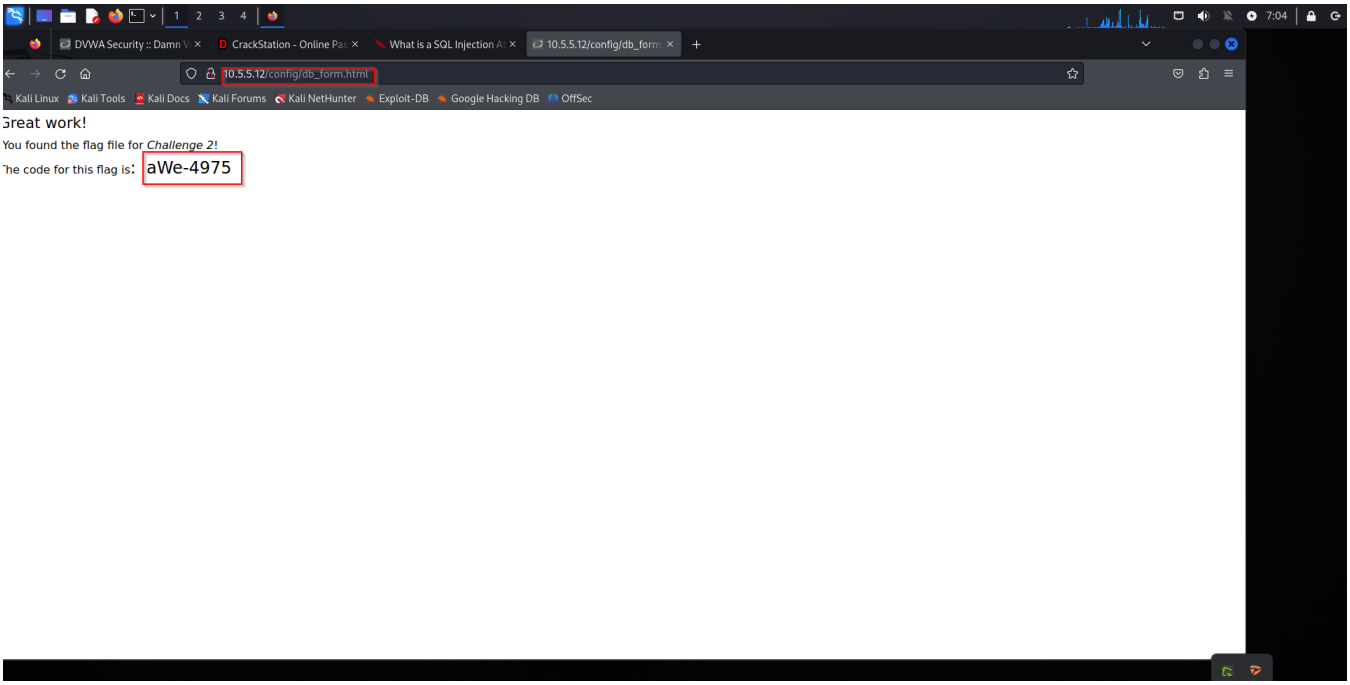


The directories which could be accessed through a web browser were….









Here is a list of the files and subdirectories that they contained…

Step 3: Viewing the files contained in each directory to find the db_form.html file.

Created a URL in the web browser to access the viewable subdirectories. Found the file with the code for Challenge 2 located in one of the subdirectories.

The two subdirectories I could look for the file were… /config and /docs

The filename with the Challenge 2 code was… db_form.html

2012-12-07 00:00 1.3K

The subdirectory which held the file was… http://10.5.5.12/config/db_form.html

The message contained in the flag file was… aWe-4975

Step 4: Researching and proposing directory listing exploit remediation.

Two remediation methods for preventing directory listing exploits

1. **Configuring your web server to prevent directory listings for all paths beneath the web root**
2. **Placing into each directory a default file (such as index.htm) that the web server will display instead of returning a directory listing**

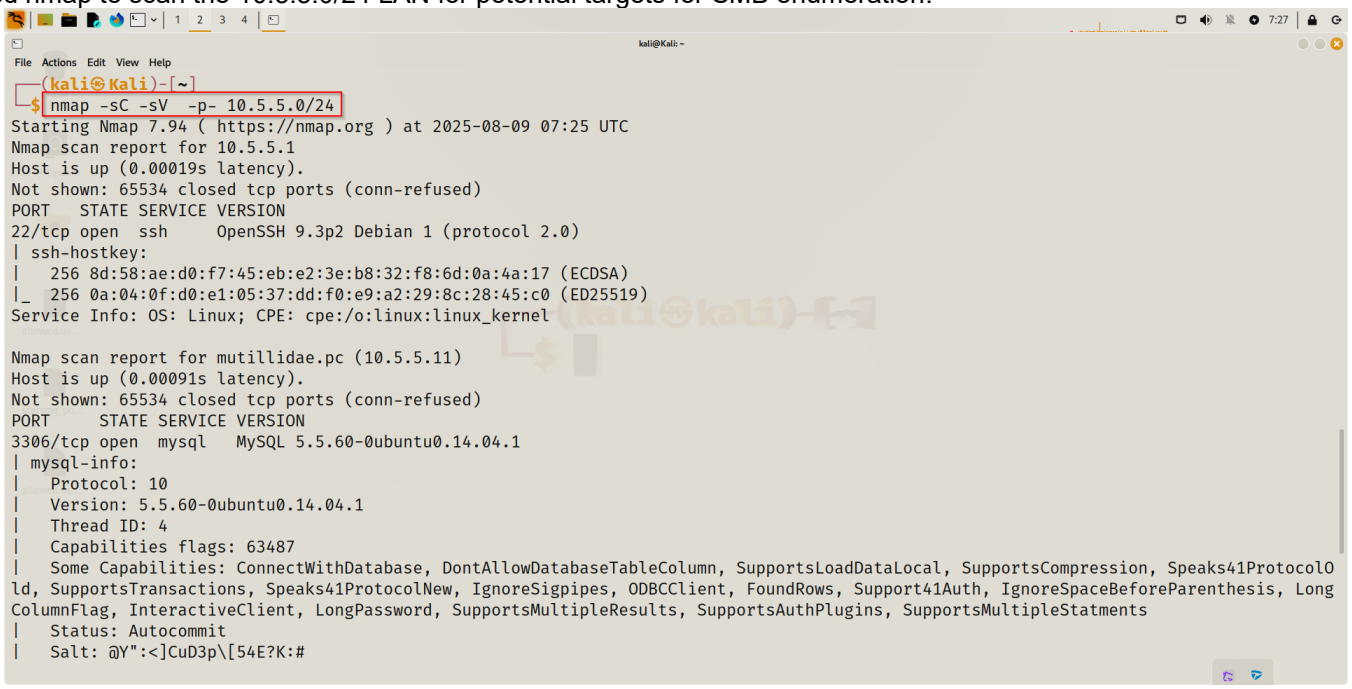
Challenge 3: Exploiting open SMB Server Shares

Total points: 25

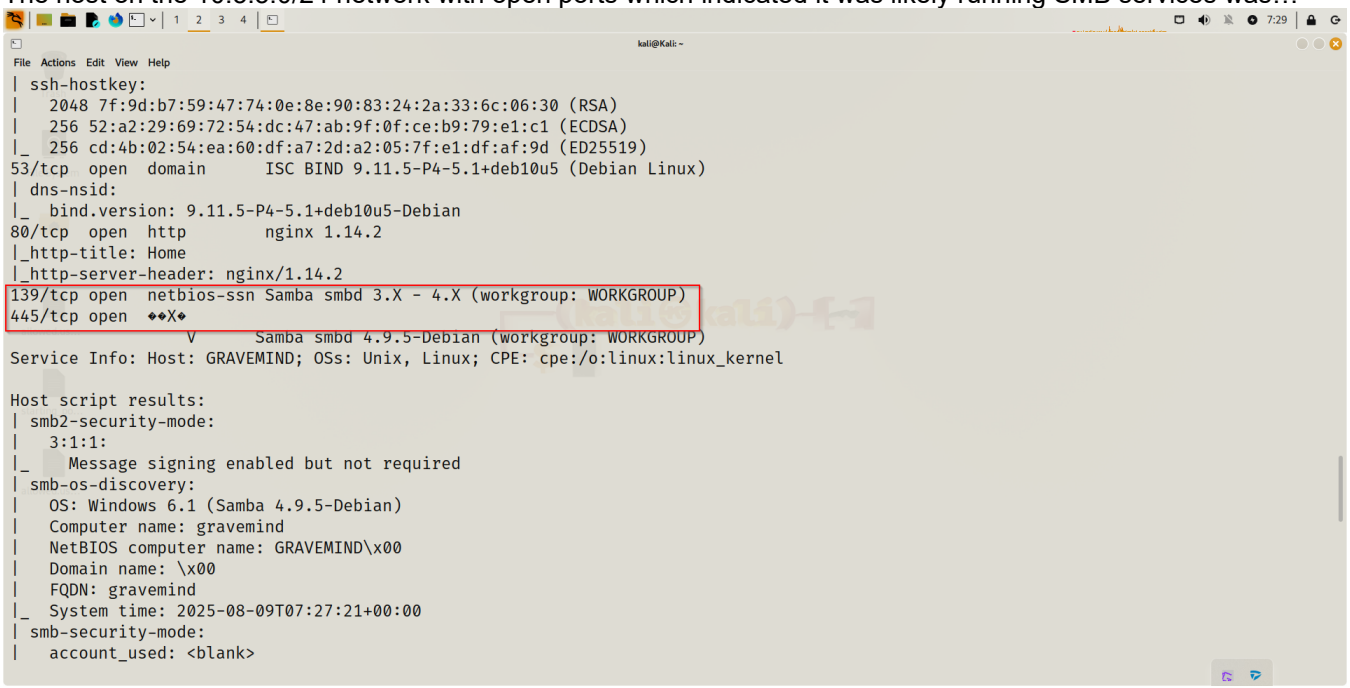
In this part, my objective was to discover if there were any unsecured shared directories located on an SMB server in the 10.5.5.0/24 network. I used … tools to find the drive shares available on the servers.

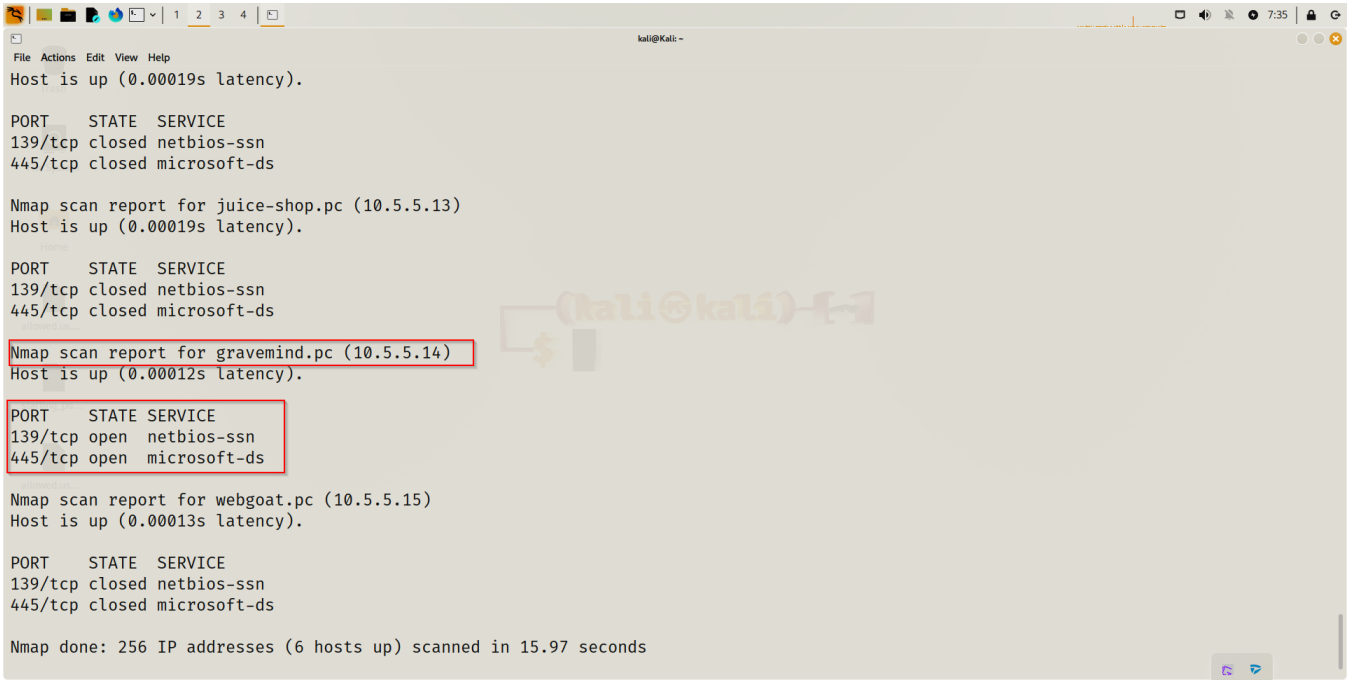
Step 1: Scanning for potential targets running SMB.

Used nmap to scan the 10.5.5.0/24 LAN for potential targets for SMB enumeration.



The host on the 10.5.5.0/24 network with open ports which indicated it was likely running SMB services was…

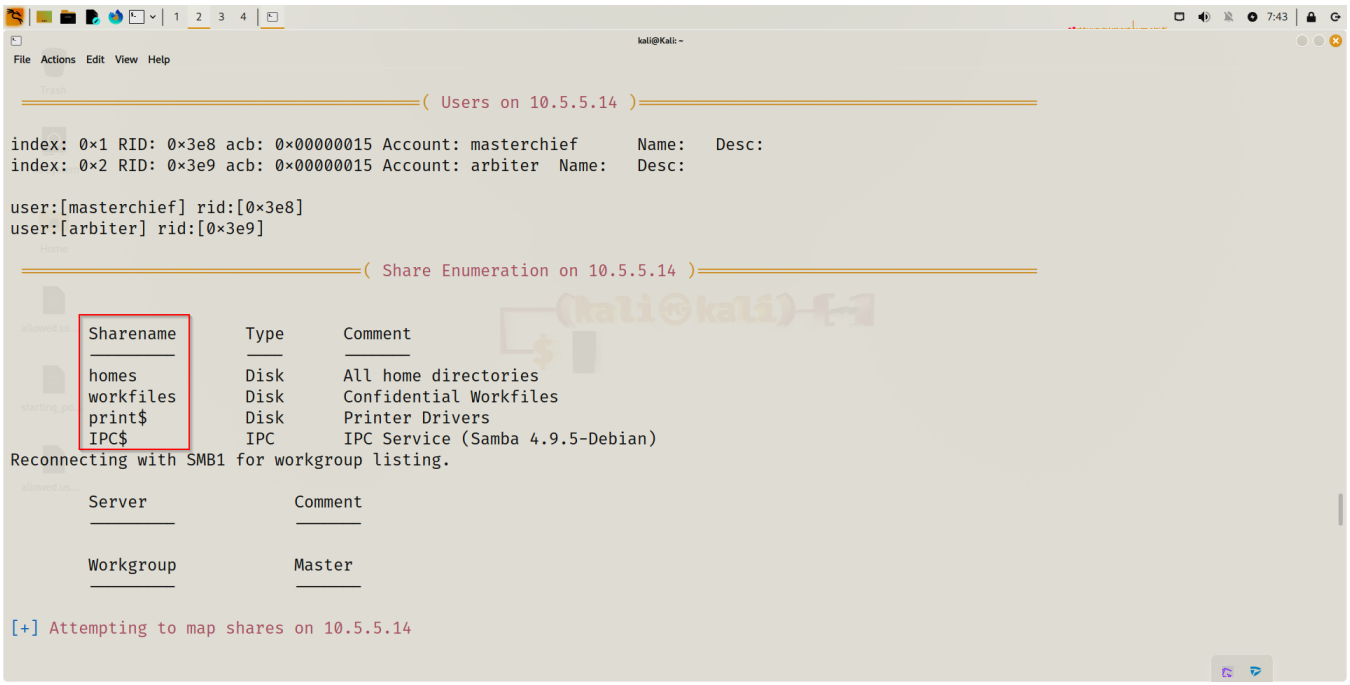




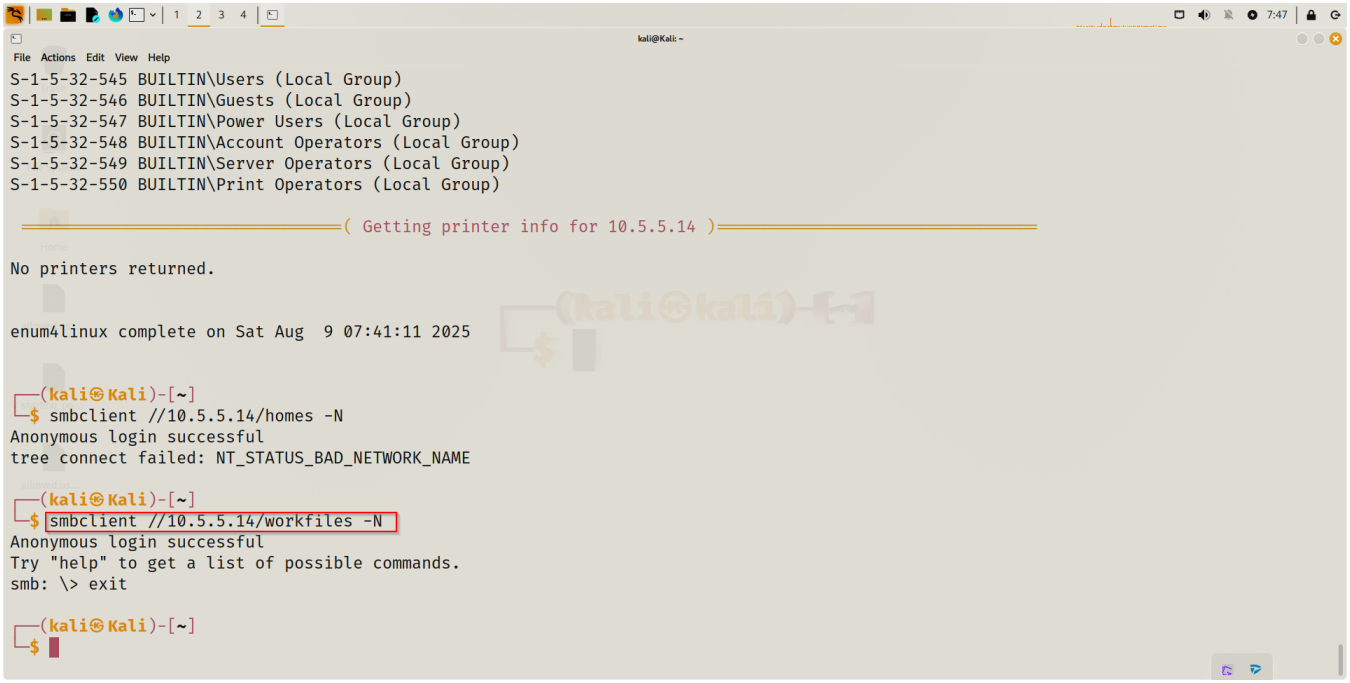
Step 2: Determining which SMB directories are shared and can be accessed by anonymous users.

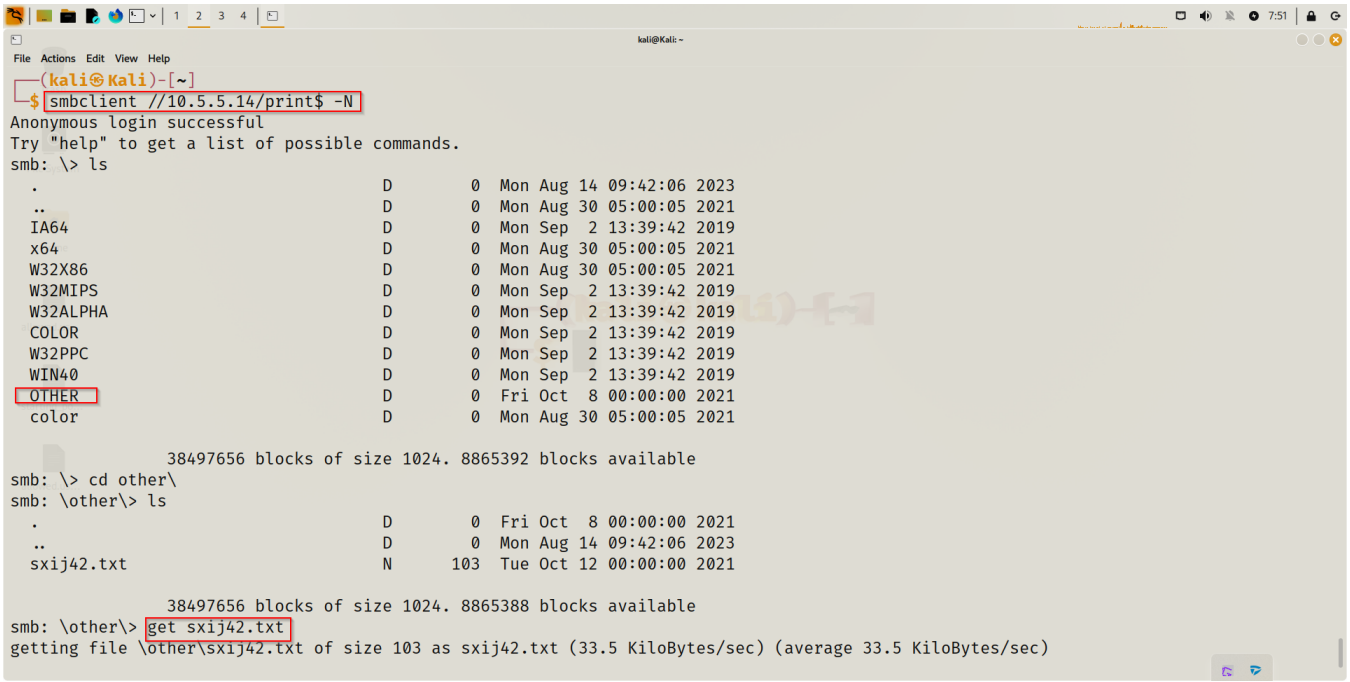
Used enum4linux tool to scan the devices running SMB and located the shares that could be accessed by anonymous users.

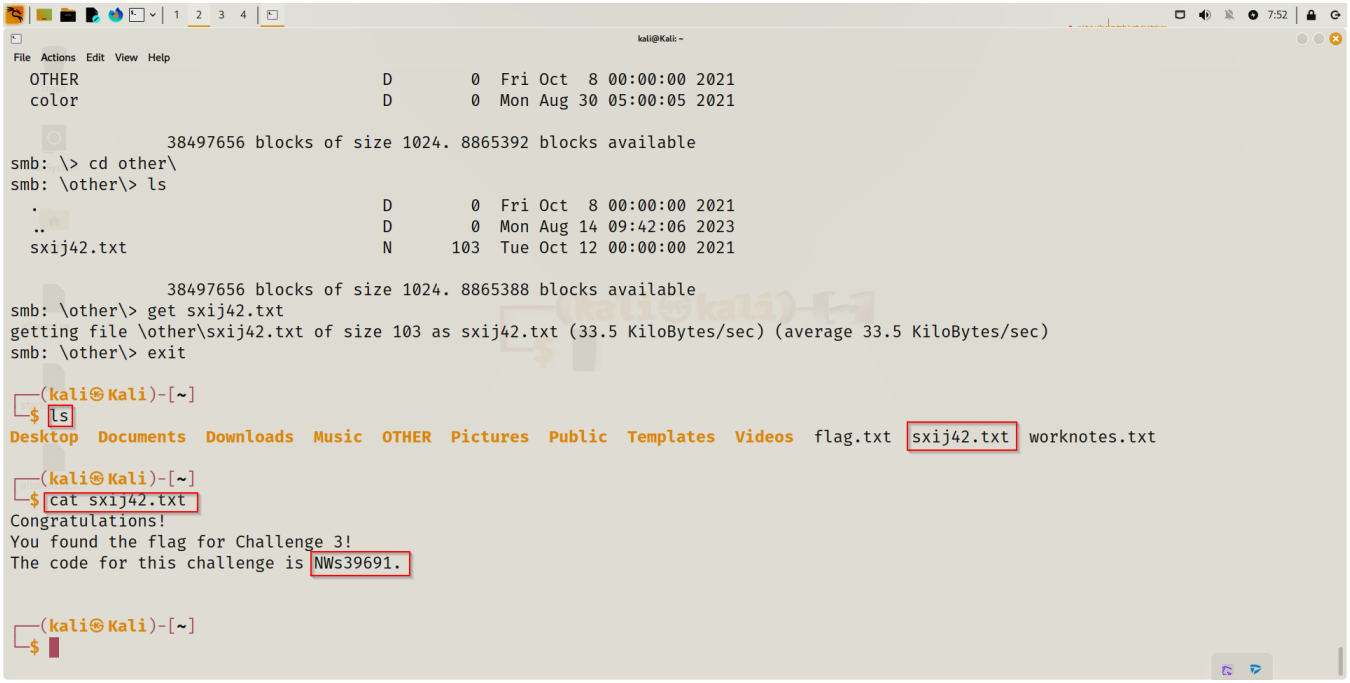
Shares that were listed on the SMB server were…



The ones which were accessible without a valid user login were…







Step 3: Investigating each shared directory to find the file.

Used the SMB-native client to access the drive shares on the SMB server. Used the ls commands to find subdirectories and files.

Located the file with the Challenge 3 code. Downloaded the file and opened it locally.

The file was found in print$ other share subdirectory.

The name of the file with Challenge 3 code was… sxij42.txt

The code for Challenge 3 ... NWs39691

Step 4: Researching and proposing SMB attack remediation.

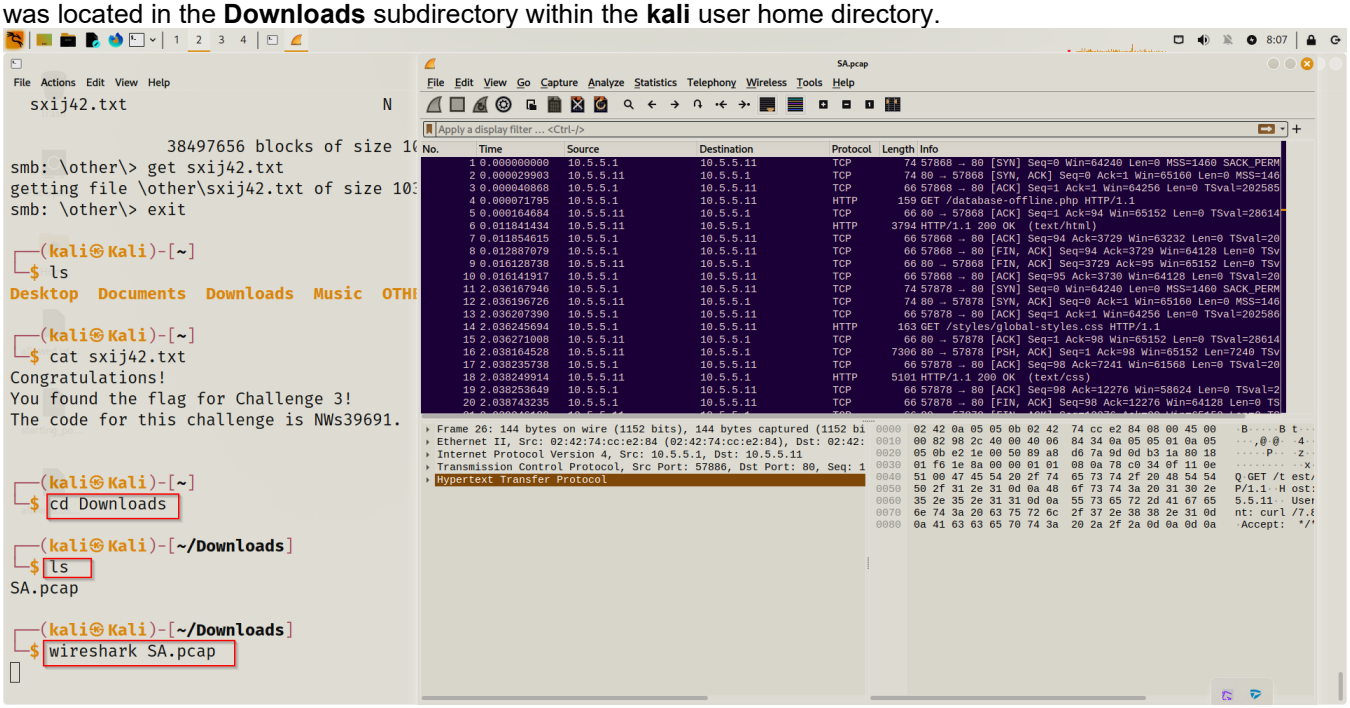
Two remediation methods for preventing SMB servers from being accessed.

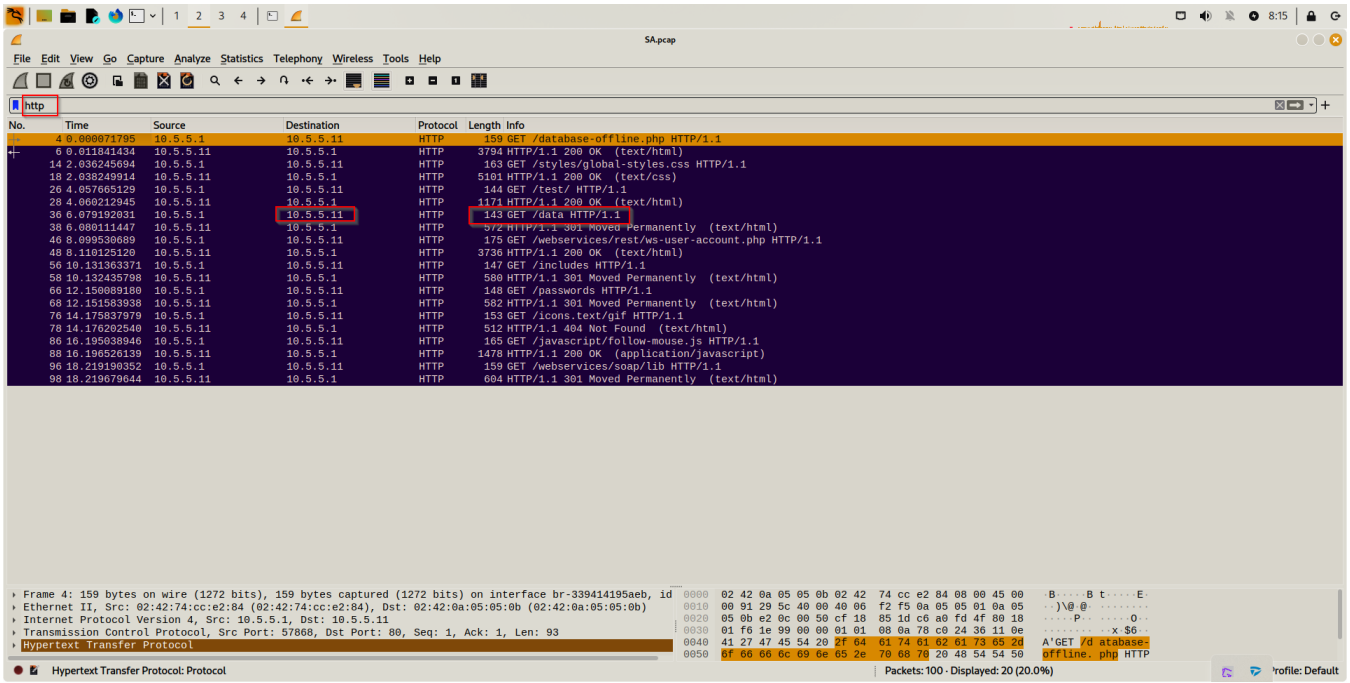
1. Updates and patches.
2. Network segmentation.

Challenge 4: Analyzing a .pcap file to find information.

Total Points: **25**

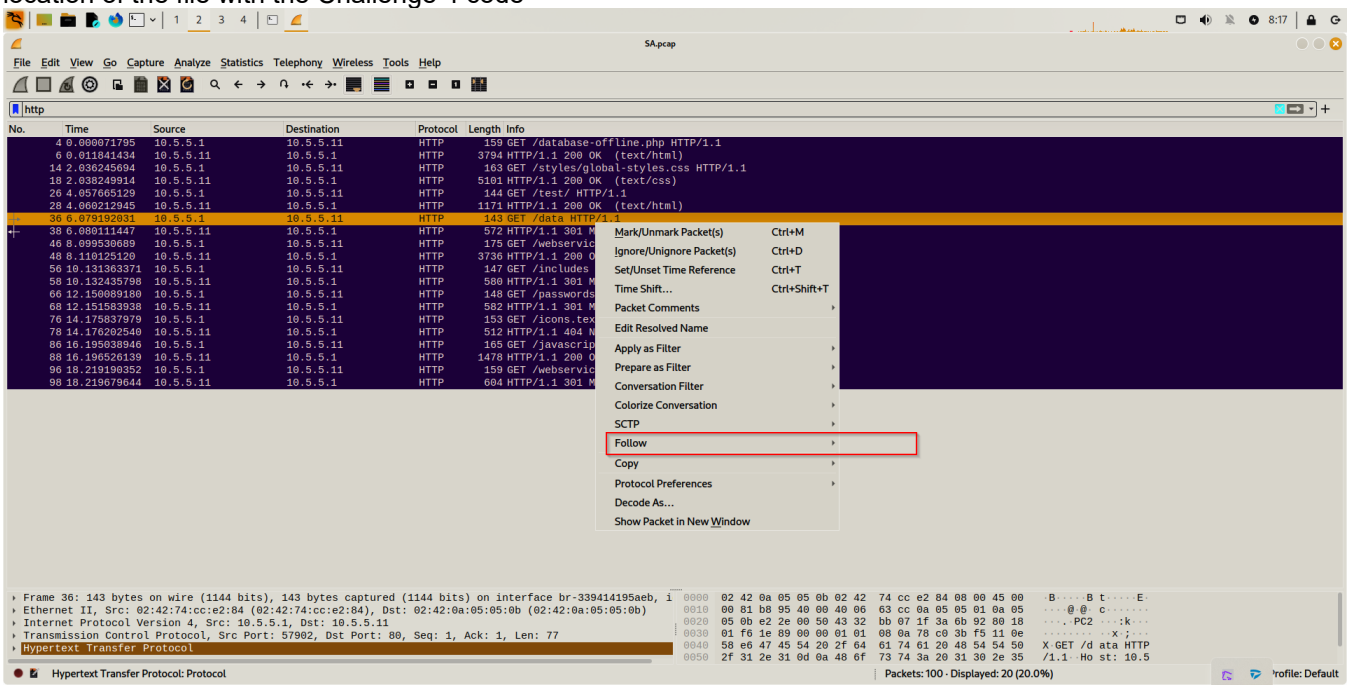
As part of my reconnaissance effort, my team captured traffic using Wireshark. The capture file, **SA.pcap**, was located in the **Downloads** subdirectory within the **kali** user home directory.





Step 1: Finding and analyzing the SA.pcap file.

Analyzed the content of the PCAP file to determine the IP address of the target computer and the URL location of the file with the Challenge 4 code



The IP address of the target computer was…10.5.5.11

The directories on the target that are revealed in the PCAPwere …

Step 2: Using a web browser to display the contents of the directories on the target computer.

Used a web browser to investigate the URLs listed in the Wireshark output. Found the file with the code for Challenge 4.

The URL of the file was …

The content of the file was …

The message contained in the record for Employee ID 0 was …

Step 3: Researching and proposing remediation that would prevent file content from being transmitted in clear text.

Further examining the capture file. The contents of the files should be transmitted in clear text and can be viewed in Wireshark.

Two remediation methods that can prevent unauthorized persons from viewing the content of the files.

1. Use encryption.
2. Implement access control lists (ACL)

The end, Thank you!