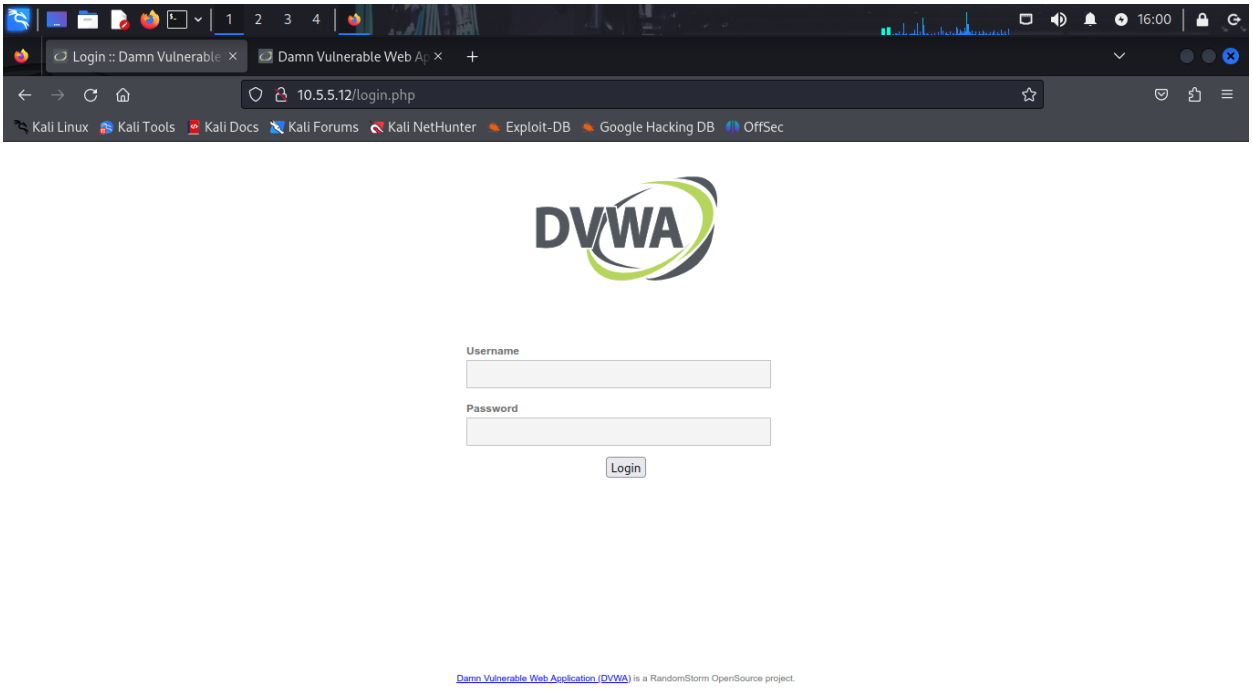
Challenge 1: SQL Injection

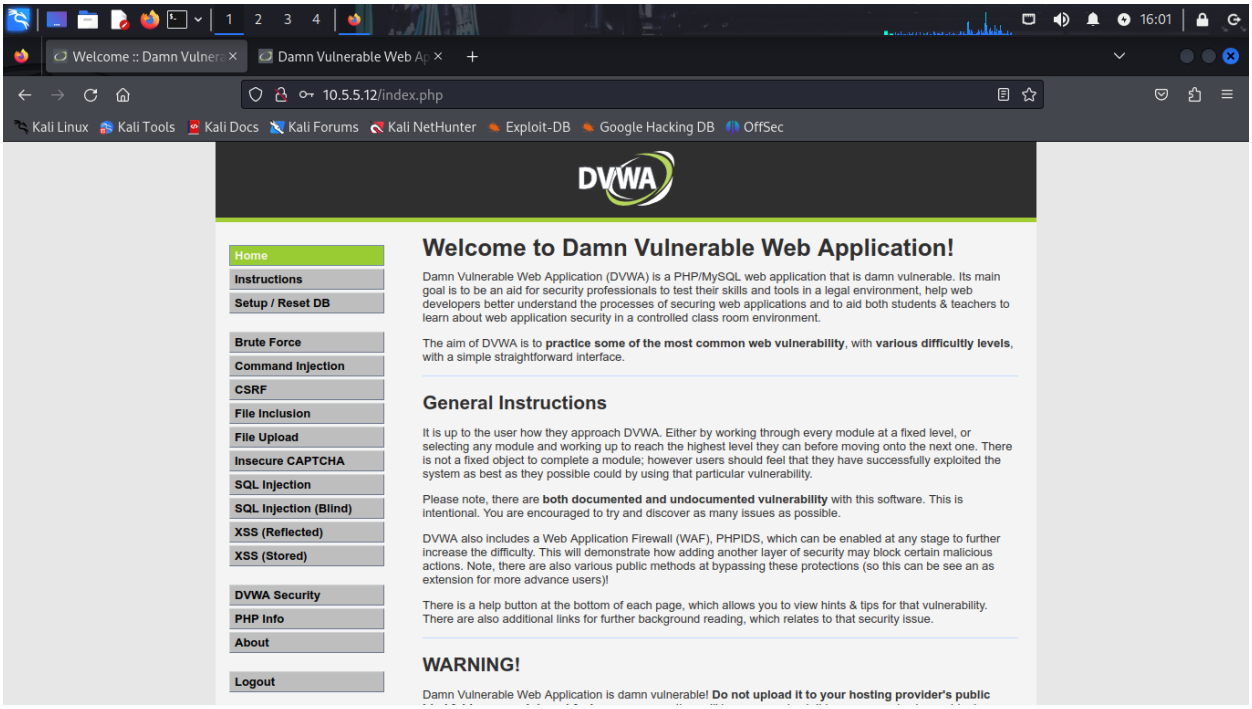
In this challenge, you are required to identify user account details on a server and successfully crack the password for Bob Smith's account. After obtaining his credentials, you will locate the file containing the Challenge 1 code and use Bob Smith's login details to access and open the file located at **192.168.0.10** to view its contents.

Step 1: Setup

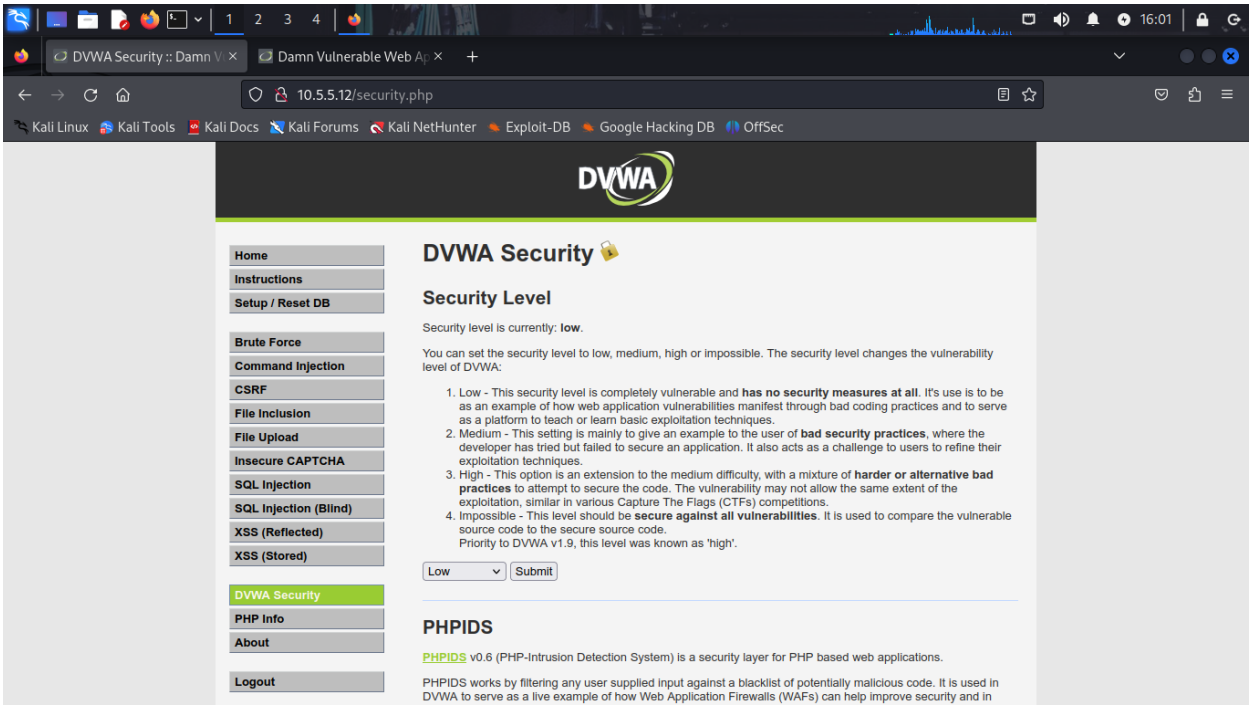
Open a browser and go to the website at 10.5.5.12.



Login with the credentials admin / password



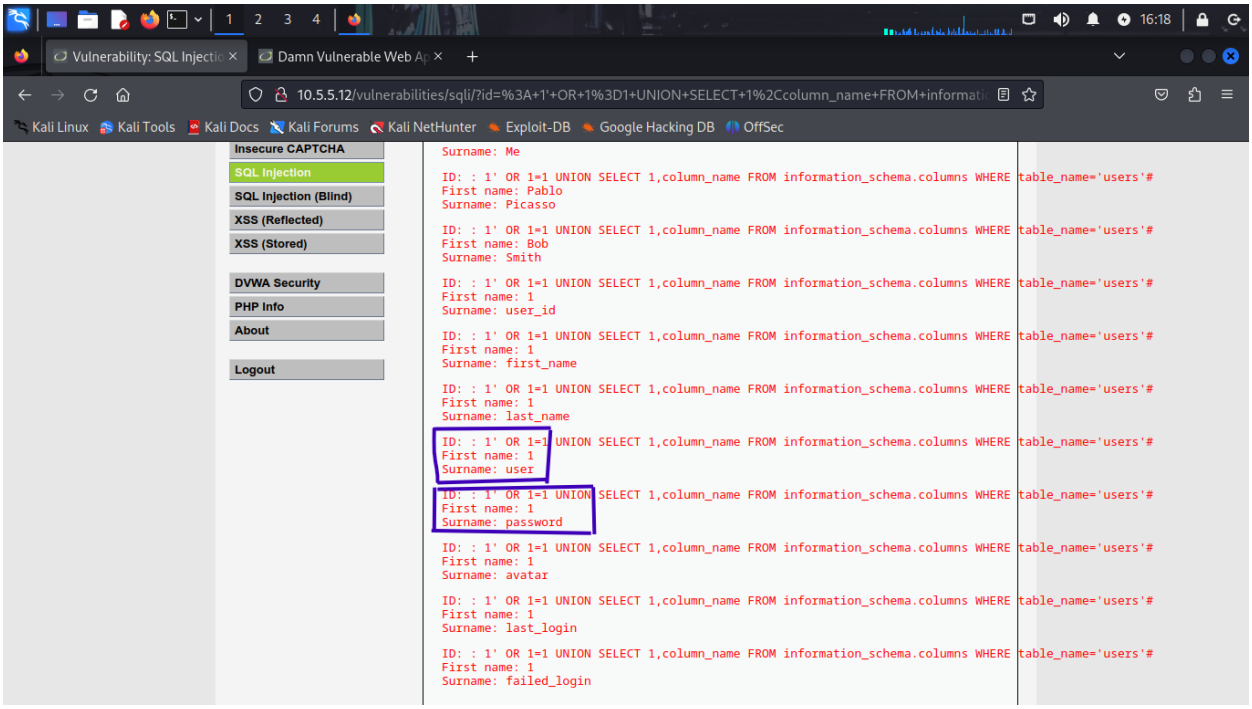
Set the DVWA security level to low and click Submit.



Step 2: Retrieve the user credentials for the Bob Smith's account

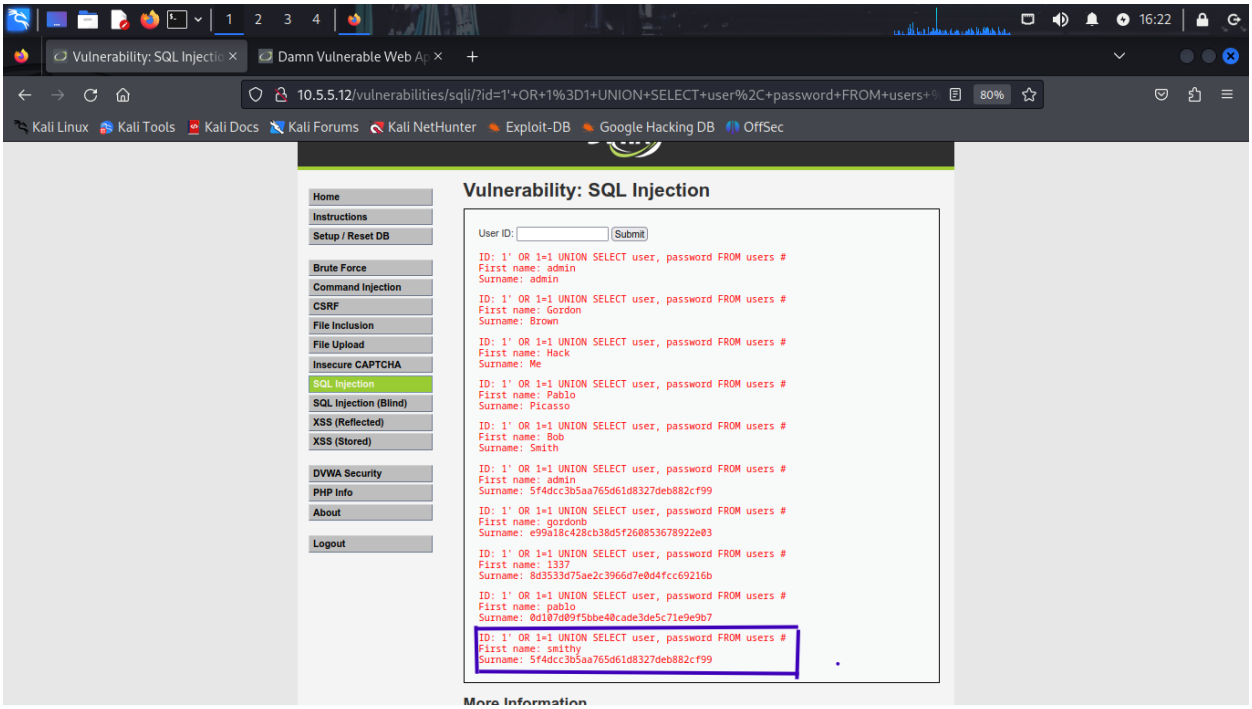
Identify the table that contains usernames and passwords

Use: 1' OR 1=1 UNION SELECT 1,column_name FROM information_schema.columns WHERE table_name='users'#



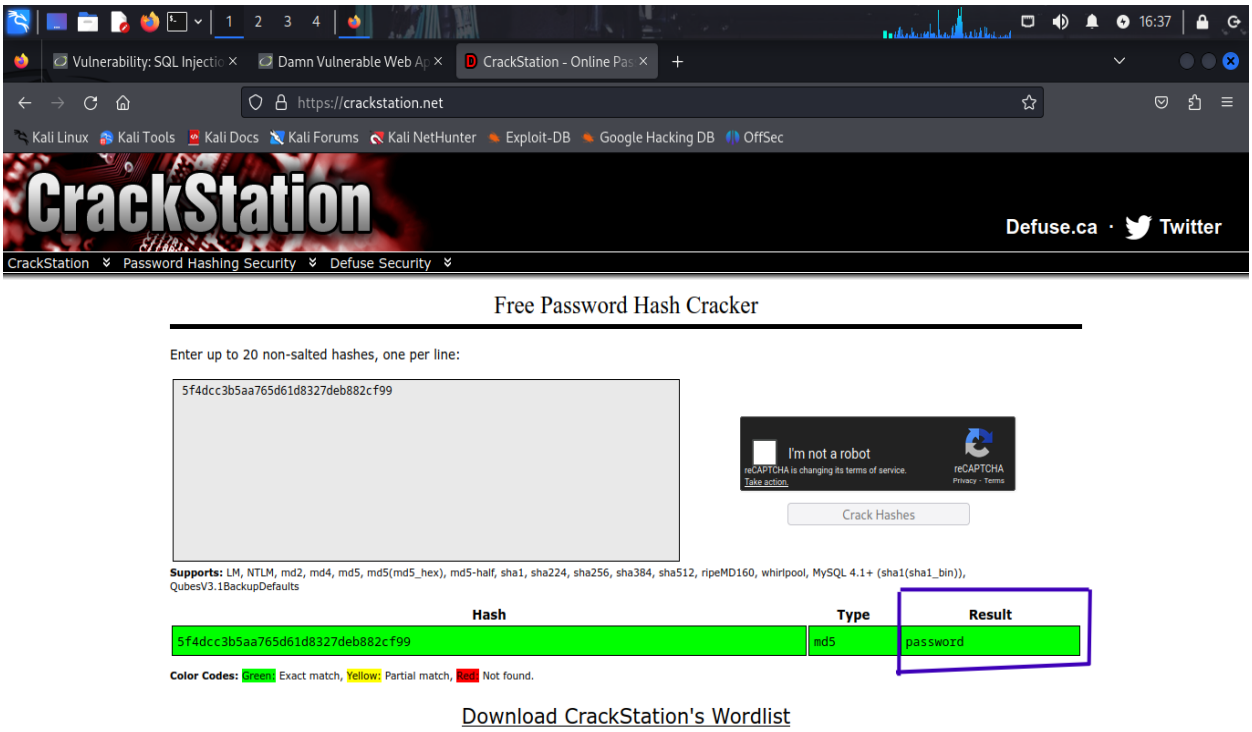
To retrieve the password for the user Bob smith.

Use: 1' OR 1=1 UNION SELECT user, password FROM users #



Step 3: Crack Bob Smith's account password

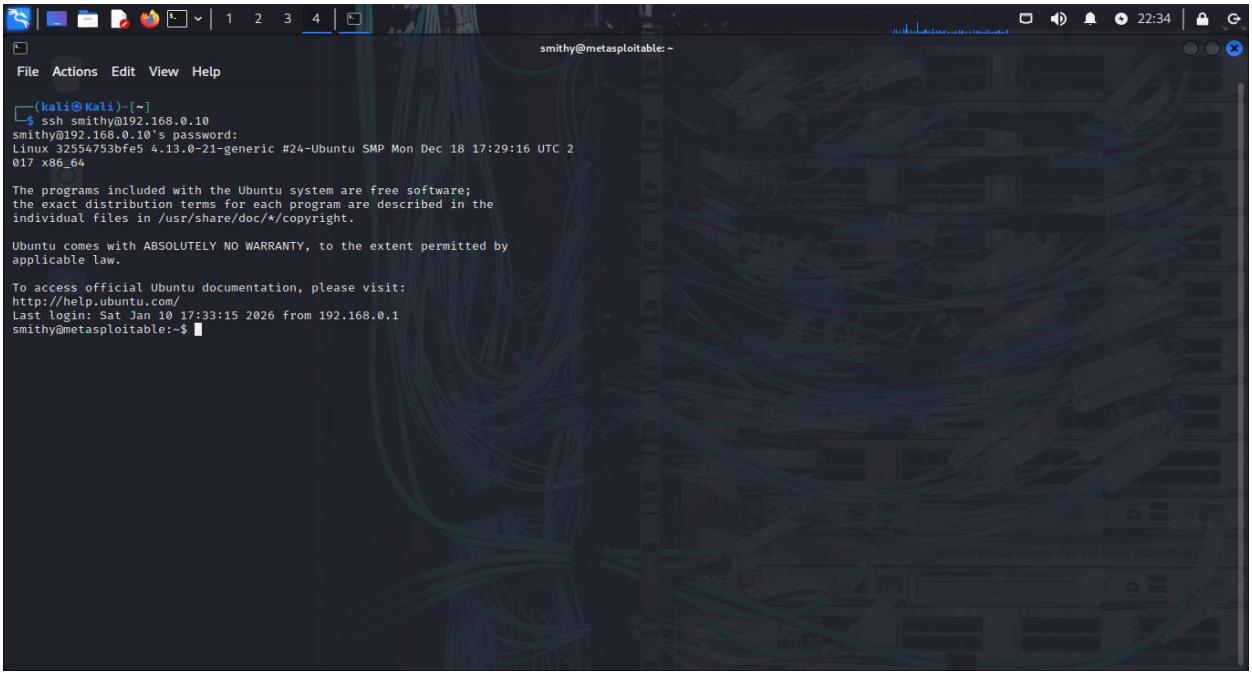
use crackstation to crack the hashed password



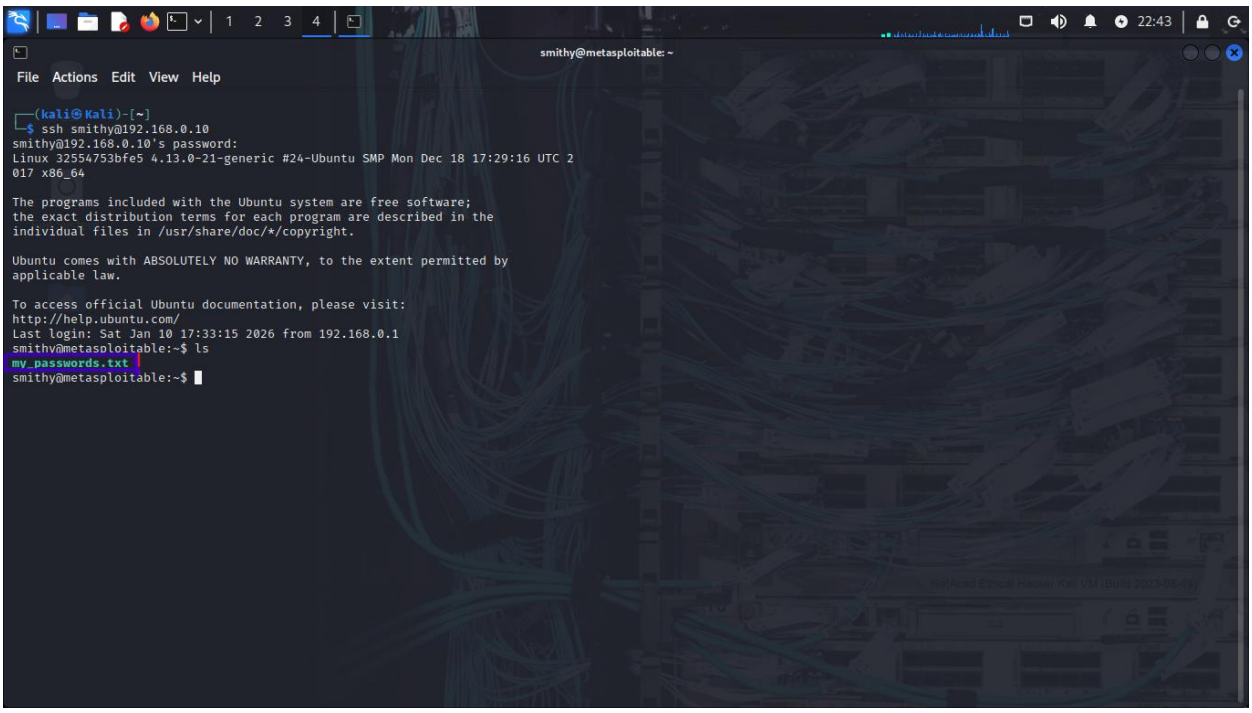
The password of Bob Smith's account: **password**

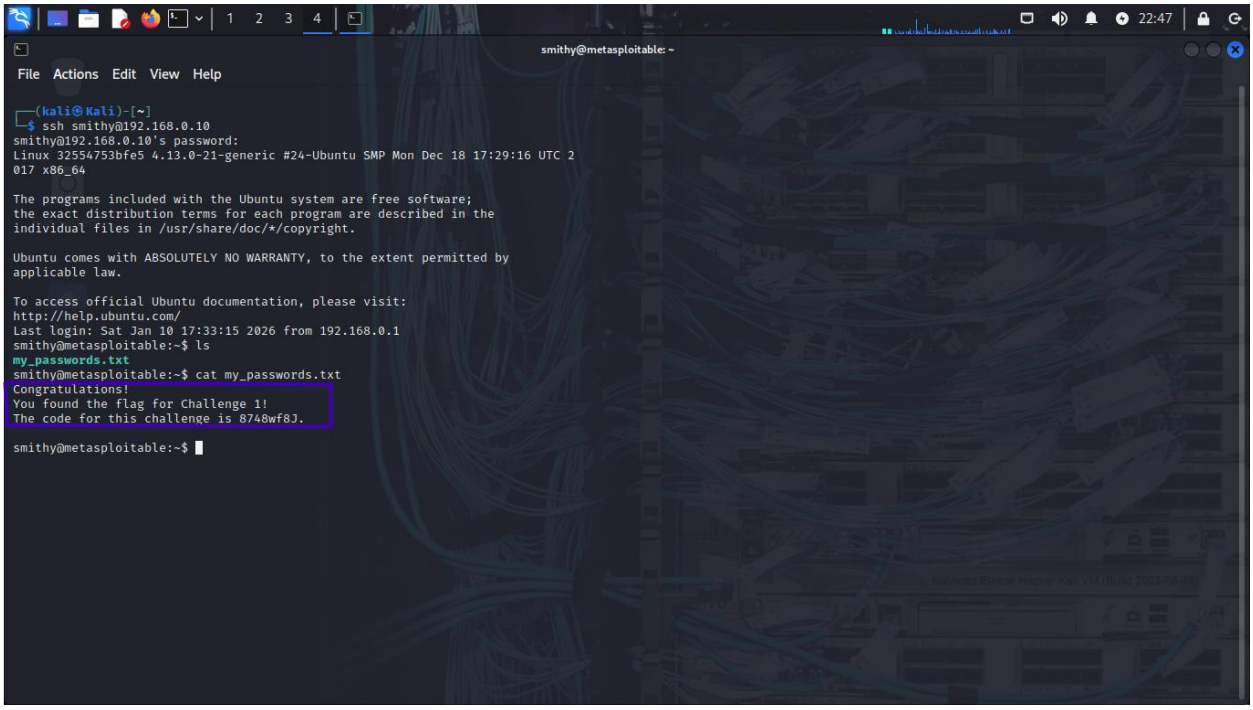
Step 4: Locate and open the file with Challenge 1 code

Log into 192.168.0.10 as Bob Smith using ssh

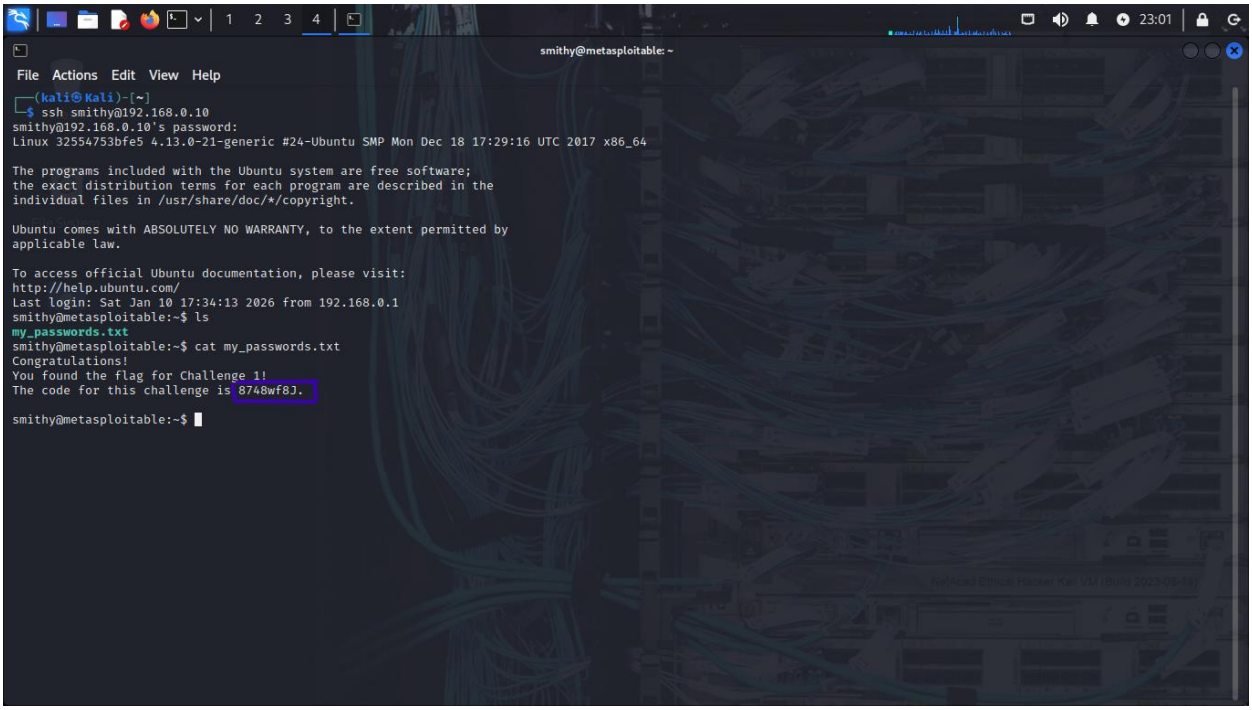


Locate and open the flag file in the user's home directory. What is the name of the file with the code?





What is the message contained in the file?



Step 5: Research and propose SQL attack remediation

What are five remediation methods for preventing SQL injection exploits?

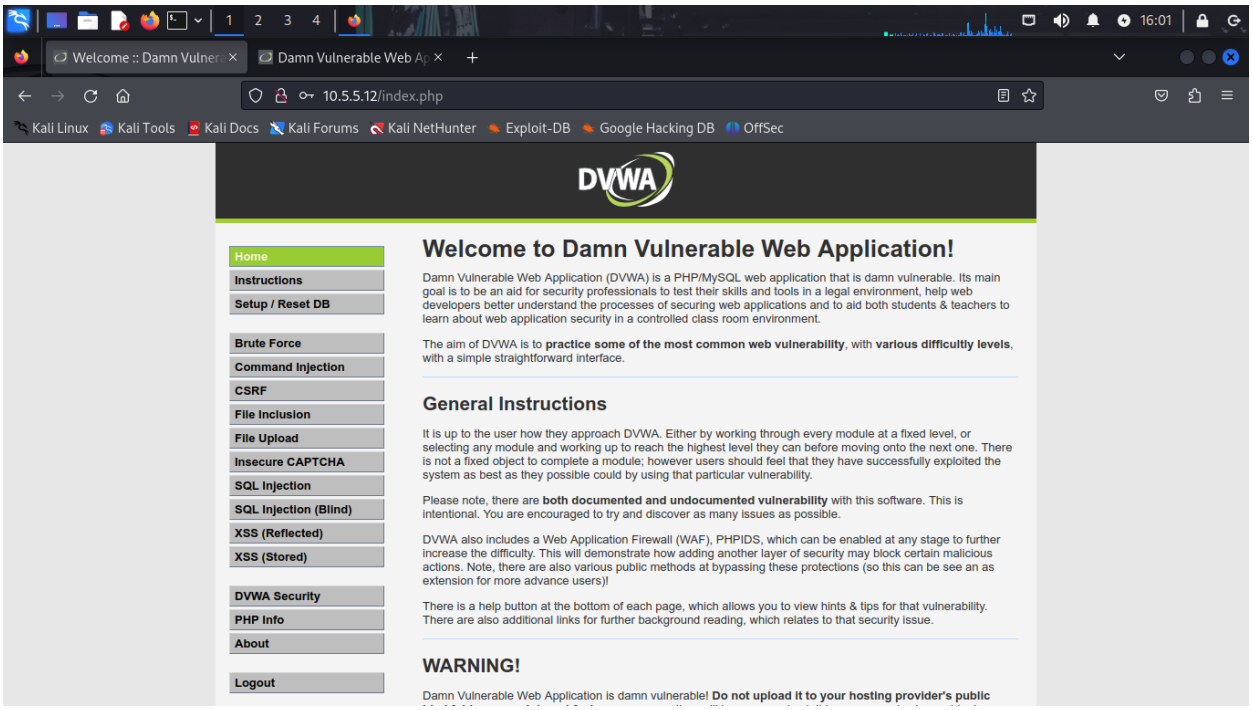
1. Make sure the SQL code structure is fixed and that user input is handled as data only, not executable code, by using parameterized queries.
2. Put input validation and sanitization into practice by rejecting or cleaning user input that contains strange characters or SQL keywords.
3. Use the least privilege principle: Applications should use database accounts with the fewest possible permissions (no admin rights, for example).
4. Use stored procedures: To minimize the creation of dynamic queries, encapsulate SQL logic in pre-established database procedures.
5. Install a Web Application Firewall (WAF) and set up it rules to instantly identify and stop SQL injection attacks.

Challenge 2: Web Server Vulnerabilities

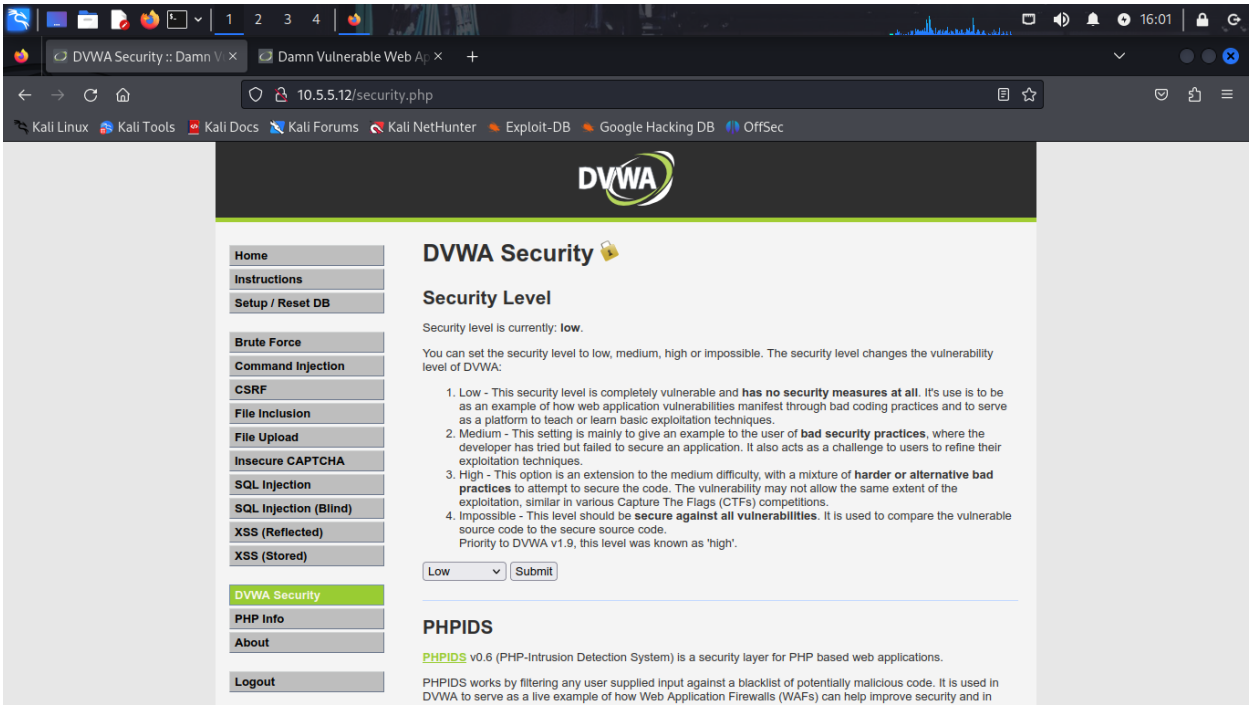
In this part, you must find vulnerabilities on an HTTP server. Misconfiguration of a web server can allow for the listing of files contained in directories on the server. You can use any of the tools you learned in earlier labs to perform reconnaissance to find the vulnerable directories. In this challenge,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

Step 1: Preliminary setup

Log into the server at 10.5.5.12 with the admin / password credentials

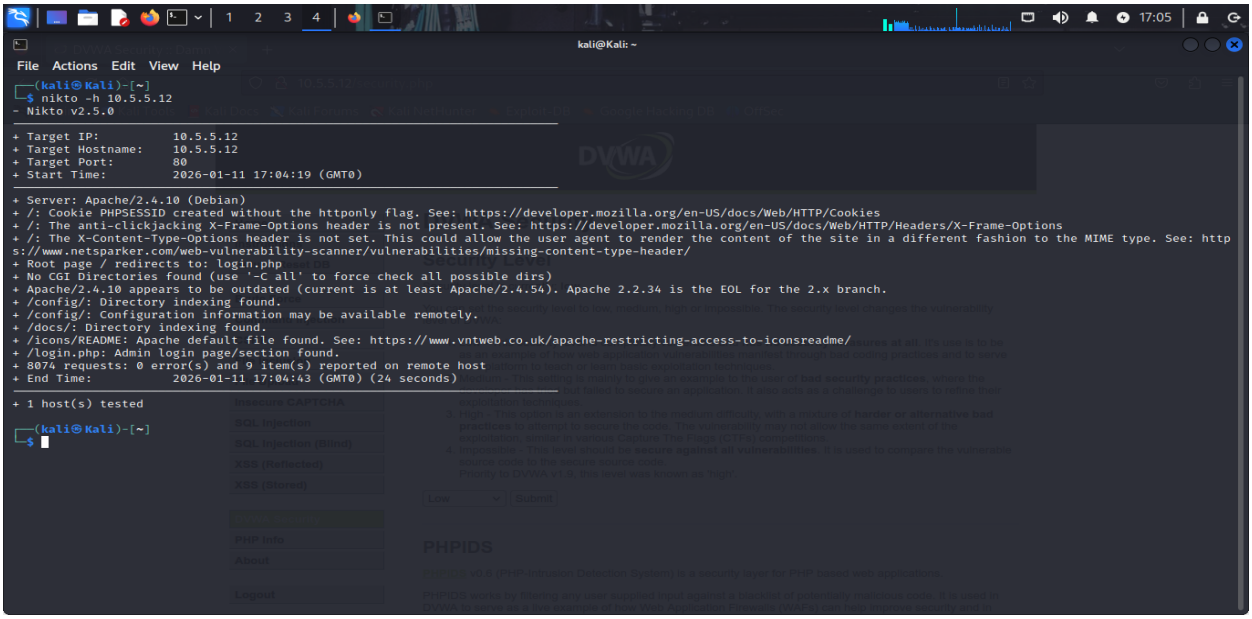


Set the application security level to low.



Step 2: From the results of your reconnaissance, determine which directories are viewable using a web browser and URL manipulation

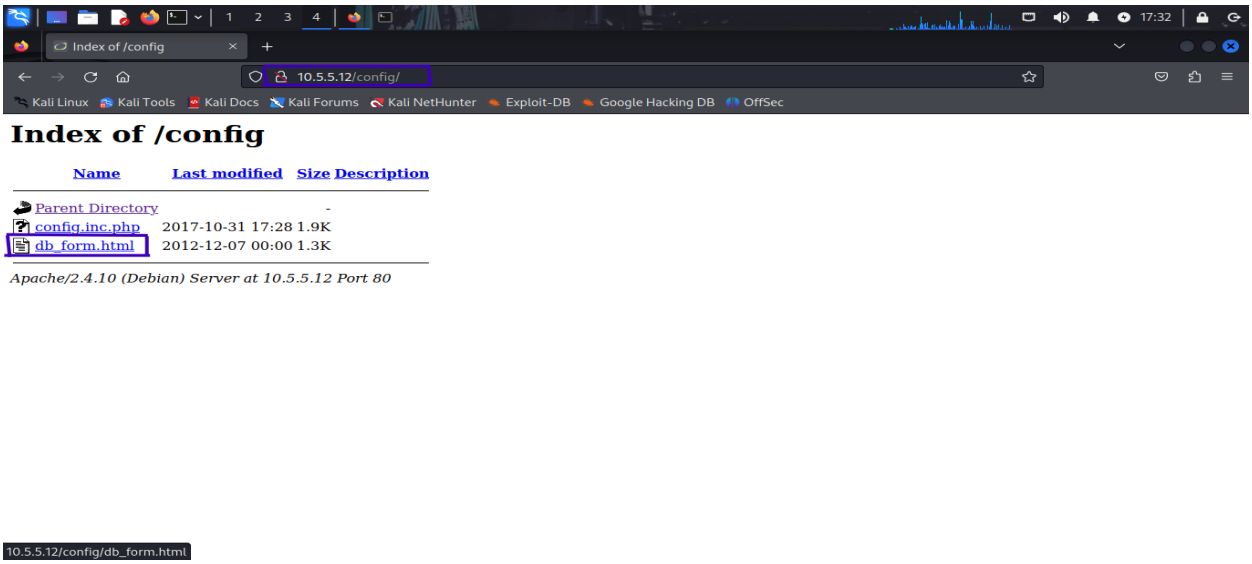
Perform reconnaissance on the server to find directories where indexing was found using Nikto Command: nikto -h 10.5.5.12



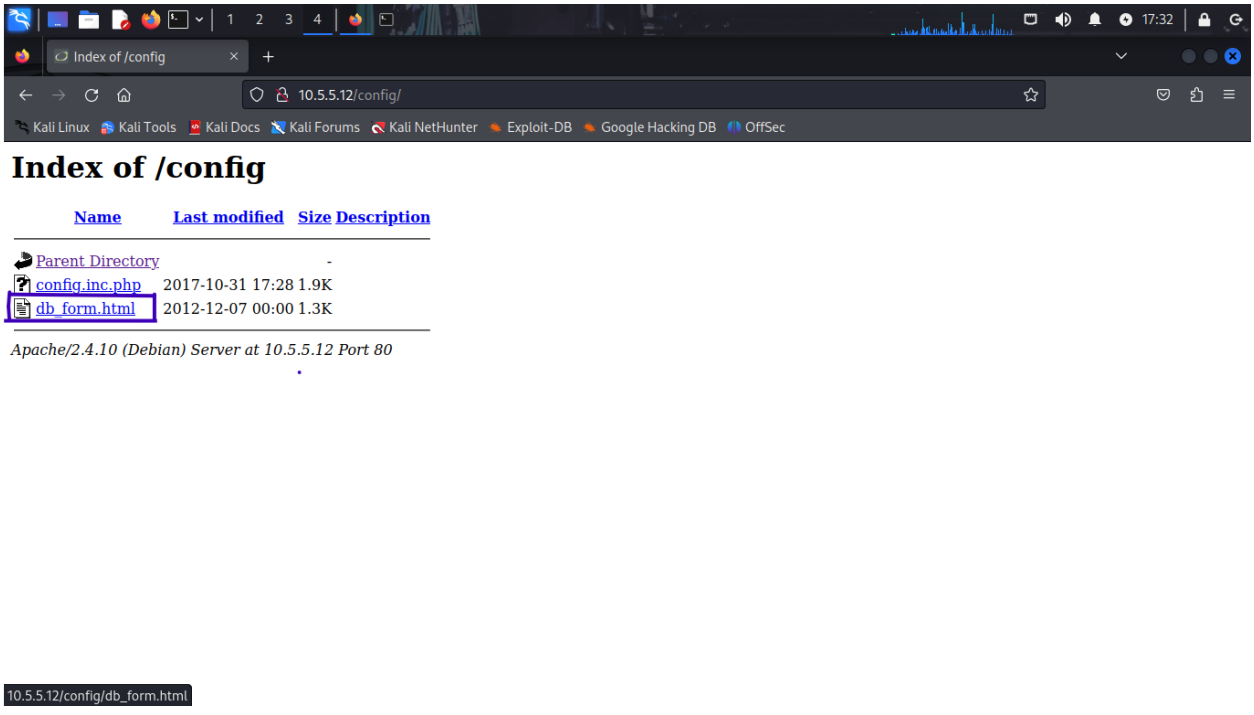
Which directories can be accessed through a web browser to list the files and subdirectories that they contain?

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

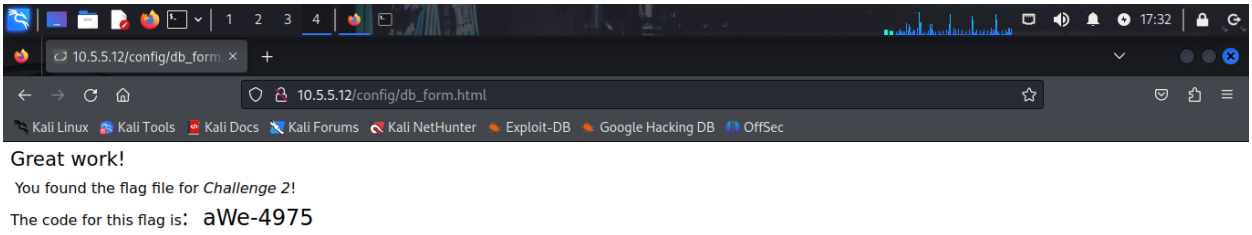
Create a URL in the web browser to access the viewable subdirectories. Find the file with the code for Challenge 2 located in one of the subdirectories



What is the filename with the Challenge 2 code?



What is the message contained in the flag file?



Step 4: Research and propose directory listing exploit remediation

What are two remediation methods for preventing directory listing exploits?

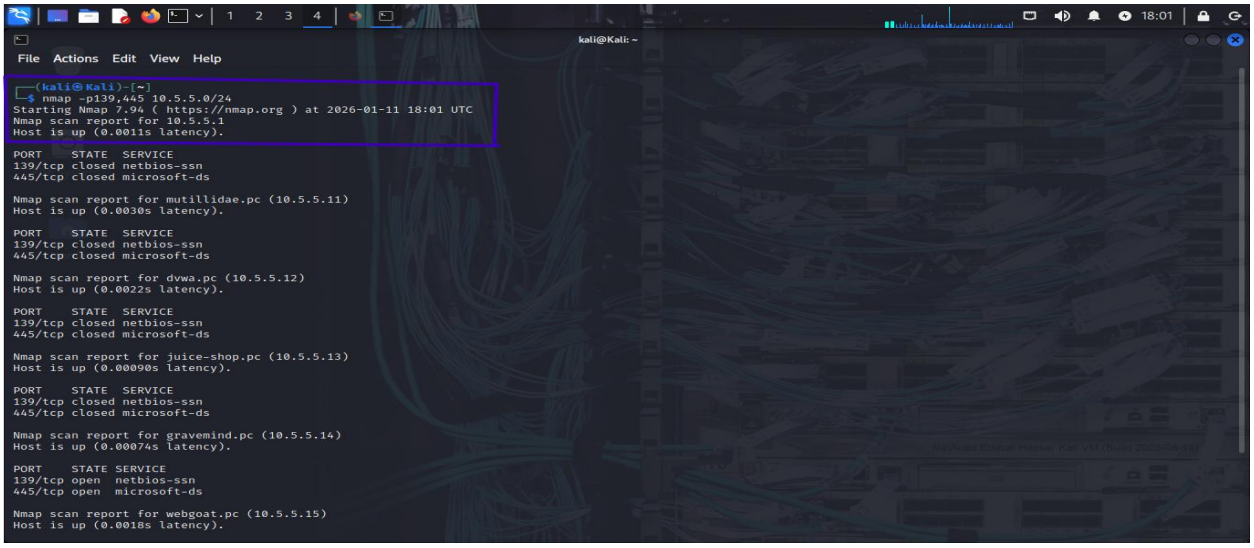
1. Disable directory indexing in the web server configuration – In Apache, set Options -Indexes in the .htaccess or virtual host config. In Nginx, disable autoindex on;.
2. Place a default index file (e.g., index.html, index.php) in every directory – This ensures that if a user accesses a directory, the index file is displayed instead of a file listing.

Challenge 3: Exploit open SMB Server Shares

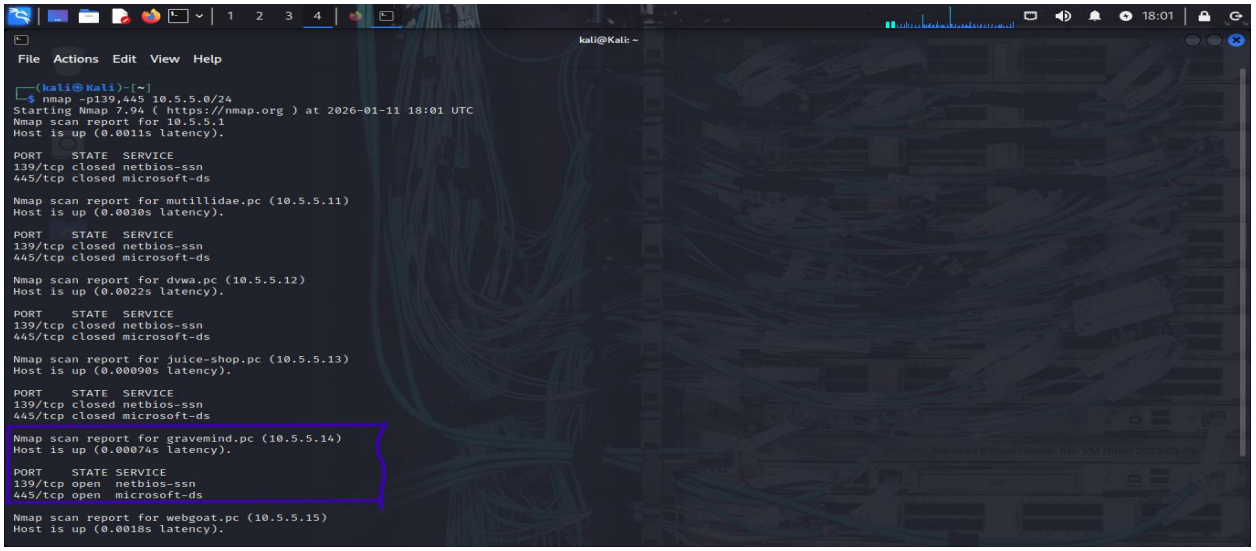
In this part, you want to discover if there are any unsecured shared directories located on an SMB server in the 10.5.5.0/24 network. You can use any of the tools you learned in earlier labs to find the drive shares available on the servers.

Step 1: Scan for potential targets running SMB.

Use scanning tools to scan the 10.5.5.0/24 LAN for potential targets for SMB enumeration.
Command: nmap -p139,445 10.5.5.0/24



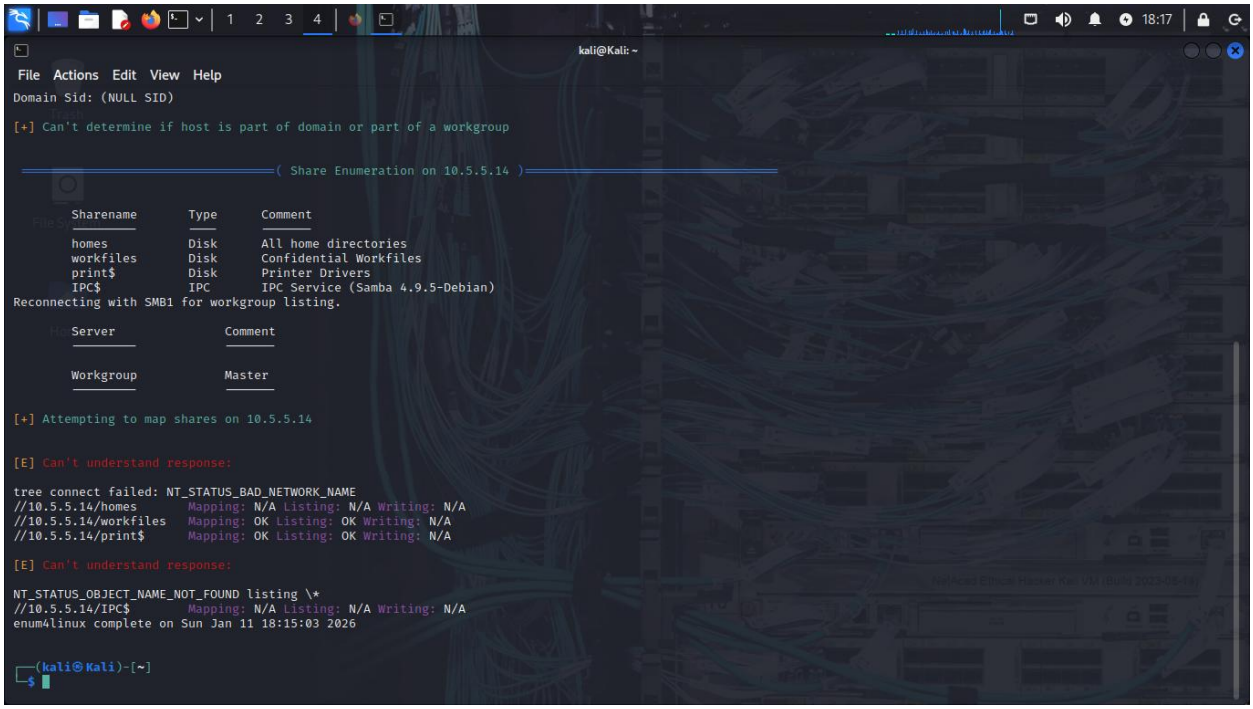
Which host on the 10.5.5.0/24 network has open ports indicating it is likely running SMB services?



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

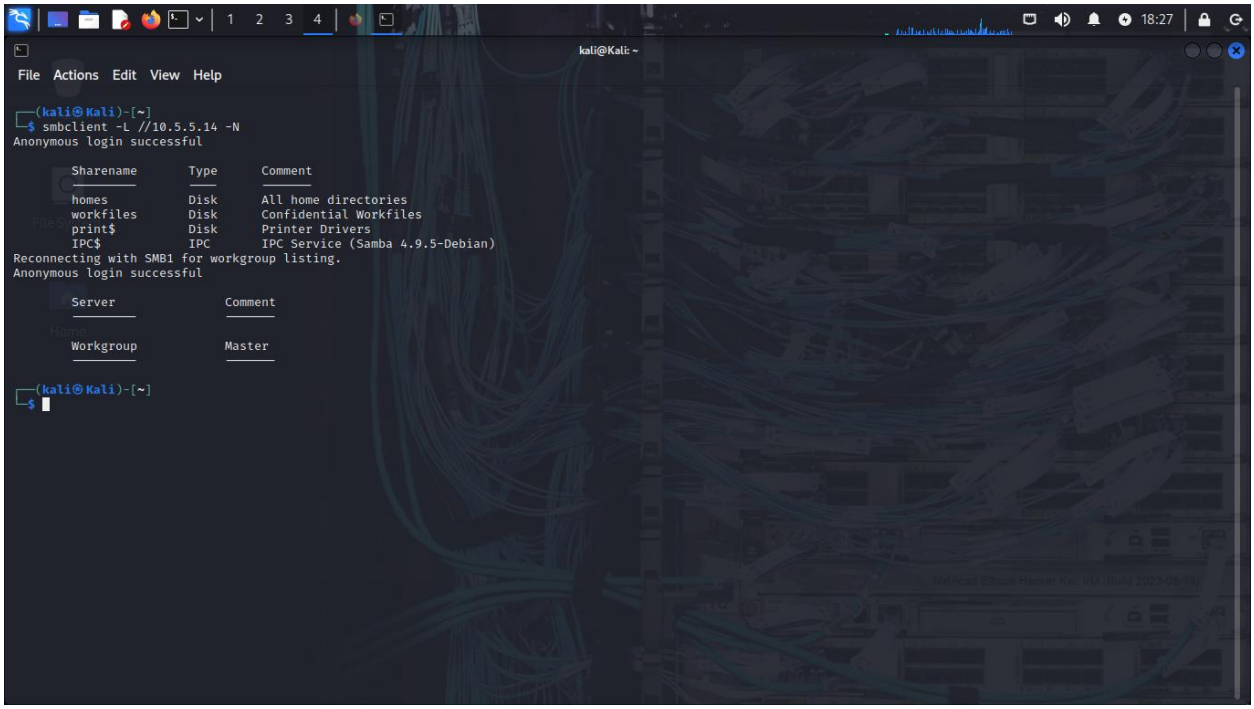
Use a tool to scan the device that is running SMB and locate the shares that can be accessed by anonymous users.

Command: enum4linux -S 10.5.5.14

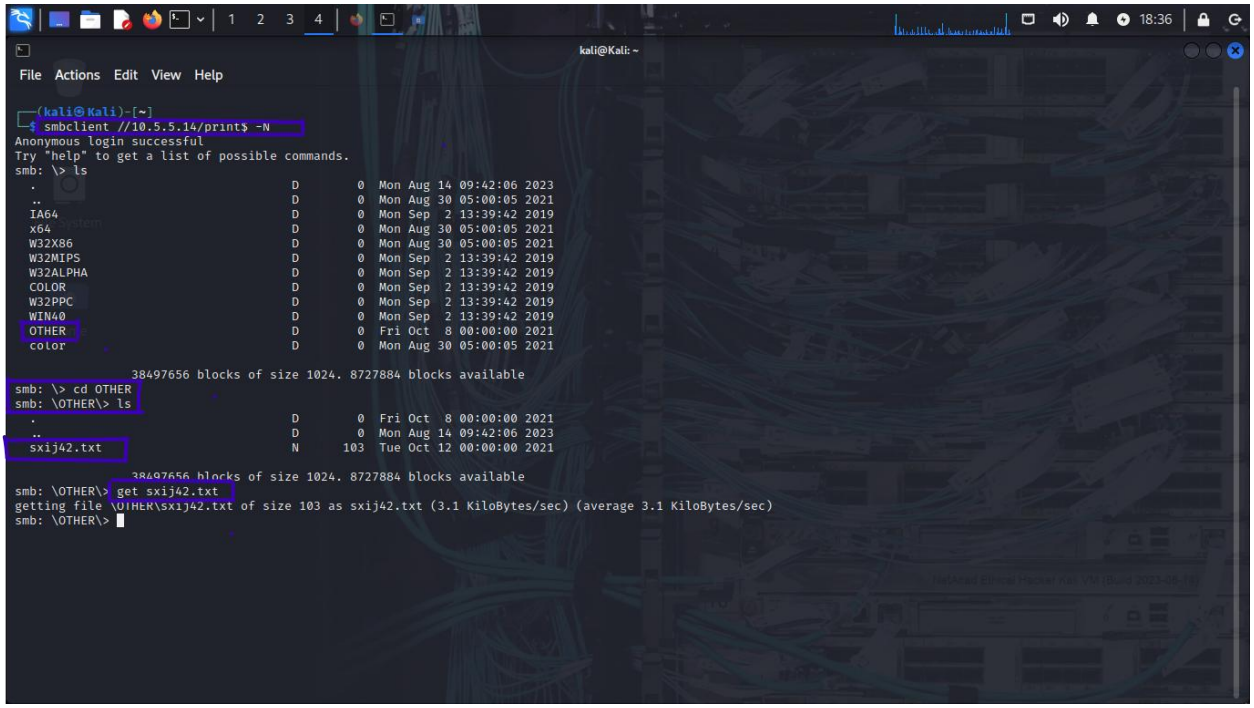


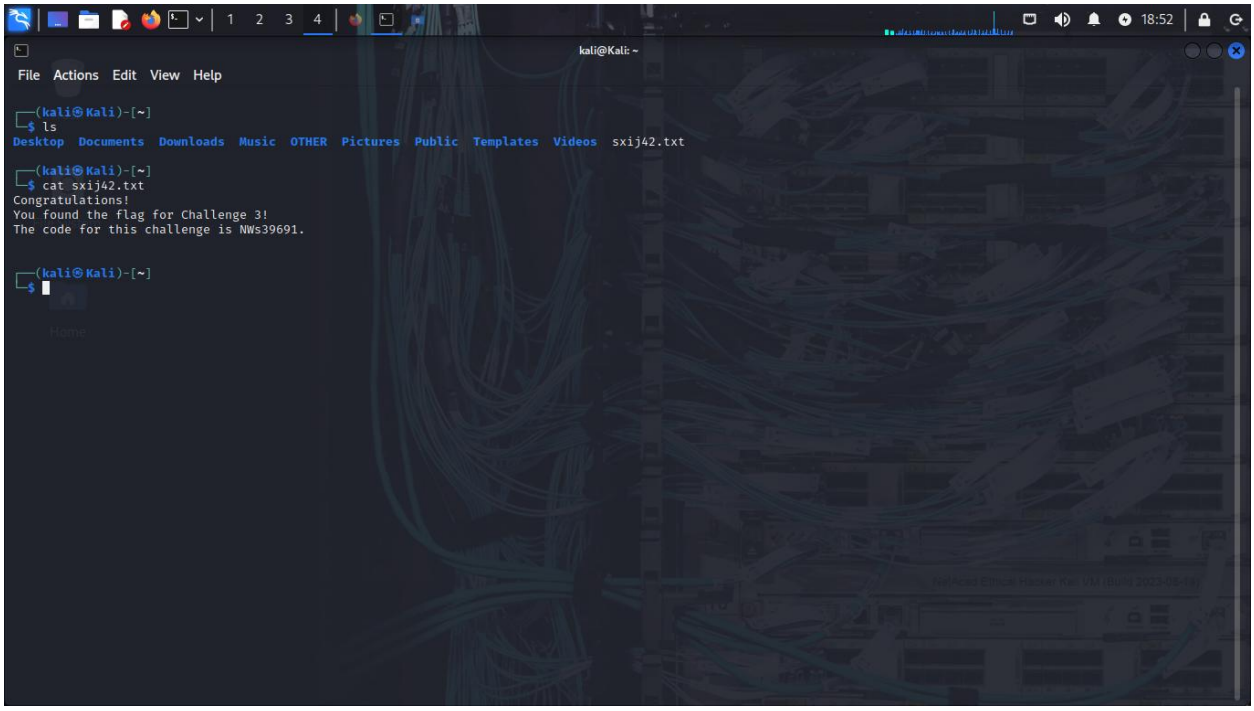
Step 3: Investigate each shared directory to find the file

Use the SMB-native client to access the drive shares on the SMB server. Use the dir, ls, cd, and other commands to find subdirectories and files.
Command: smbclient -L //10.5.5.14 -N



Locate the file with the Challenge 3 code. Download the file and open it locally.





Step 4: Research and propose SMB attack remediation.

1. Regular Patch Management
2. Disable Unnecessary SMB Versions

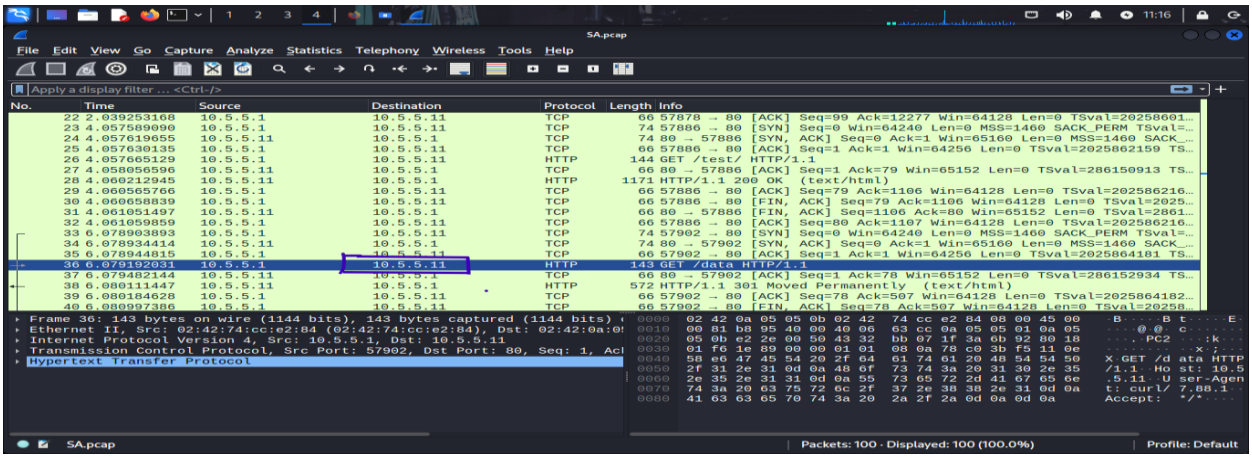
Challenge 4: Analyze a .pcap file to find information.

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

Step 1: Find and analyze the SA.pcap file

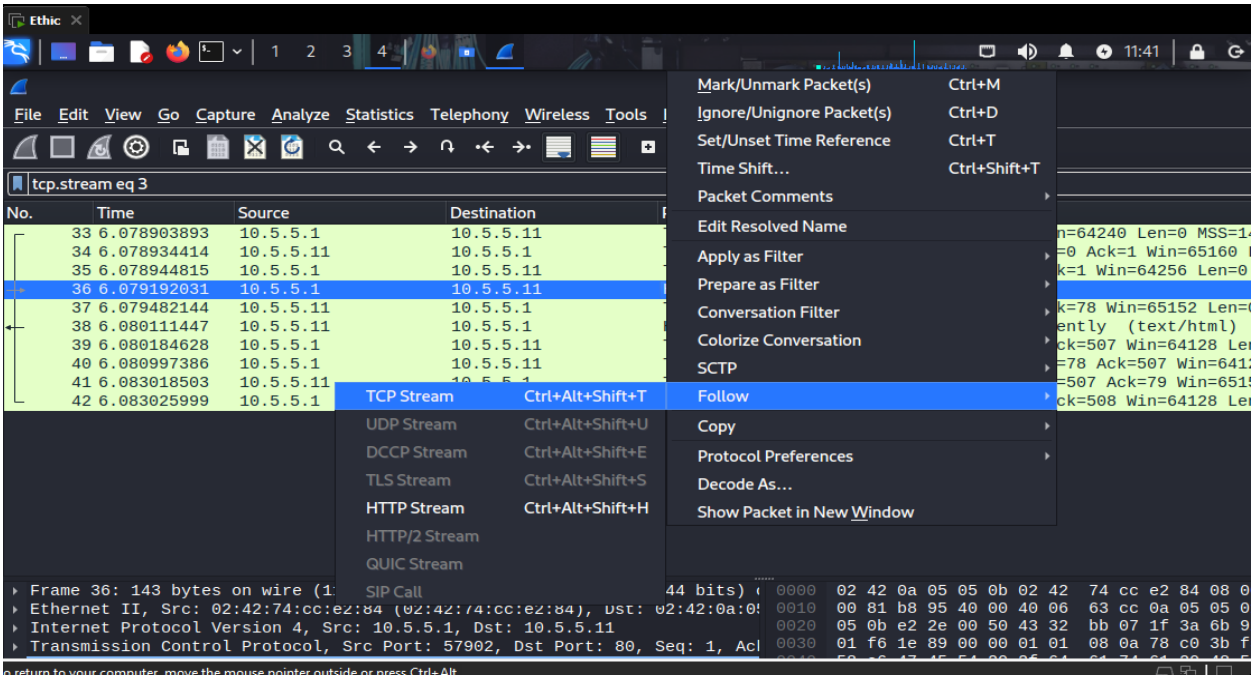
Analyze the content of the PCAP file to determine the IP address of the target computer and the URL location of the file with the Challenge 4 code.

What is the IP address of the target computer?

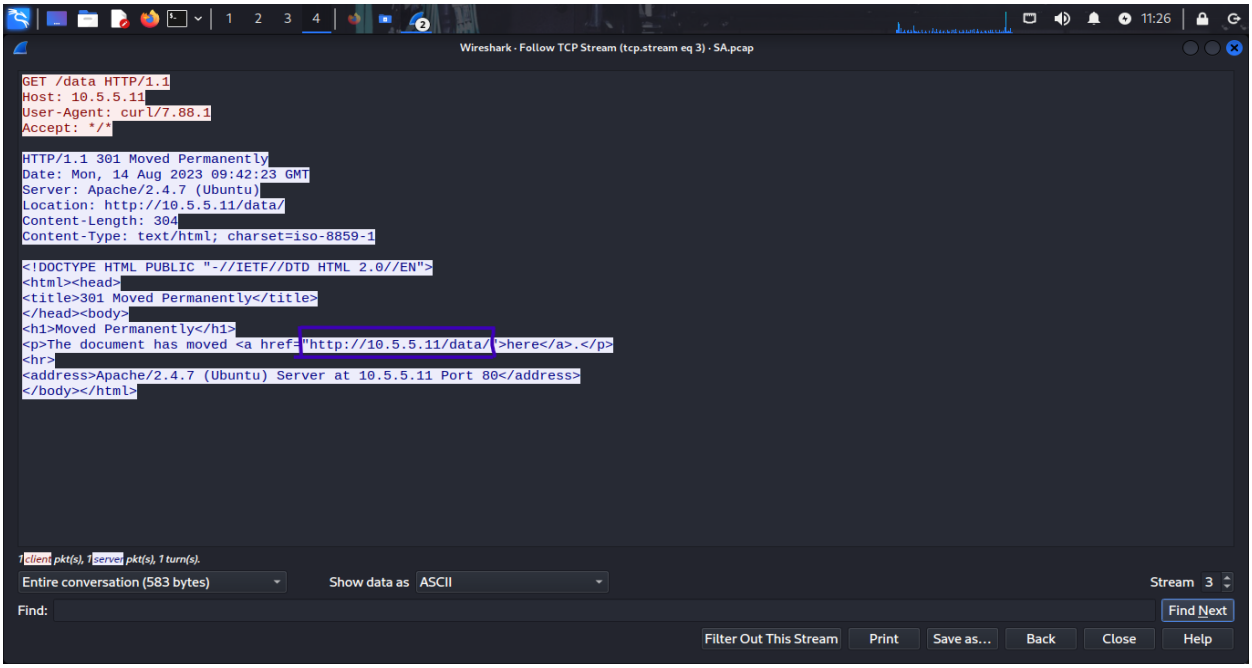


What directories on the target are revealed in the PCAP?

Right click on the target IP and follow the TCP Stream as shown in the picture below

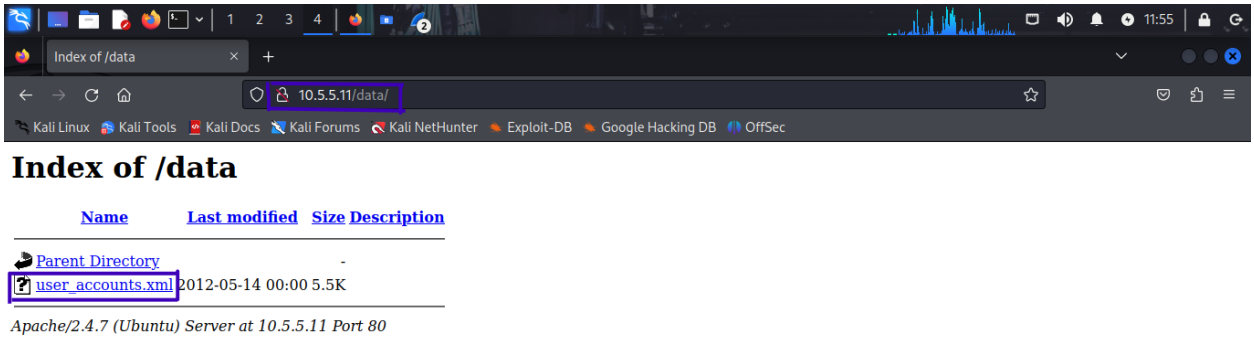


Find the URL location

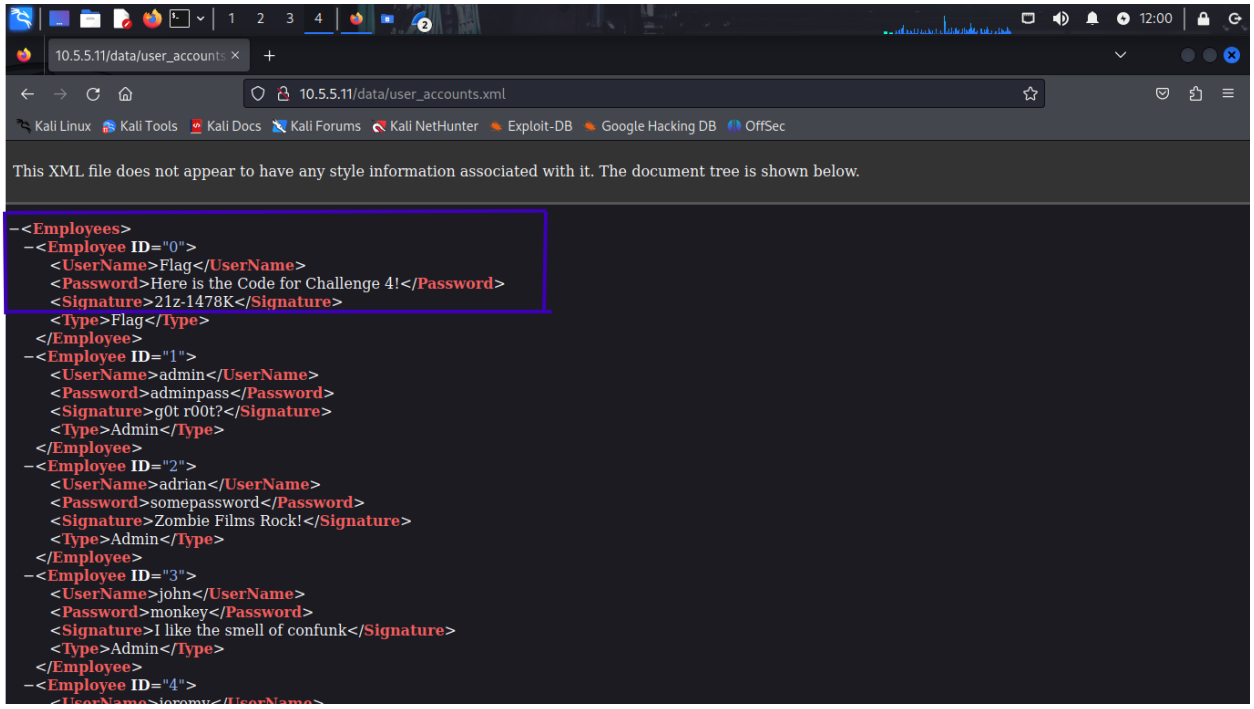


Step 2: Use a web browser to display the contents of the directories on the target computer.

What is the URL of the file?



What is the content of the file?



What message is contained in the record for Employee ID 0? Enter the code associated with the user.

21z-1478K

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

1. Mandate the use of Secure Transfer Protocols
2. Disable Insecure Protocols
3. Implement Strong Encryption for Data in Transit
4. Ensure access Controls and Monitoring systems