CYSE 450: Ethical Hacking and Penetration Testing

Lab 6: DVWA vs Multillidae

Total Points: 30

Tasks:

---

1) Login to Kali Linux and Metasploitable 2. Use ***msfadmin*** as both username and password to login to the Metasploitable 2 VM.

2) Get the IP address of Metasploitable 2 using the ***ifconfig*** command and ping it from the Kali VM. If Kali VM cannot ping the Metasploitable 2 VM, check the network adapter setting for both machines and set "**Bridged Adapter"** as the adapter option.

3) In your Kali VM, make sure that there is no proxy set up for the Firefox.

4) Enter the following URL in your Firefox browser (in your Kali VM):

https://<Metasploitable 2 IP>/dvwa/login.php

Note that 10.254.218.172 is the IP address of my Metasploitable 2 VM.

5) Login to DVWA using the following credentials:

Username: admin

Password: password

6) Select **SQL Injection** from the menu and enter **any value other than 2** as the User ID. Submit the user id and take a screenshot like the attached one showing the result. Briefly explain how SQL Injection can be implemented to get the same result. Give the relevant SQL query you need to use.

10 points

SQL query that can be used to get the same result:

3' OR '1'='1

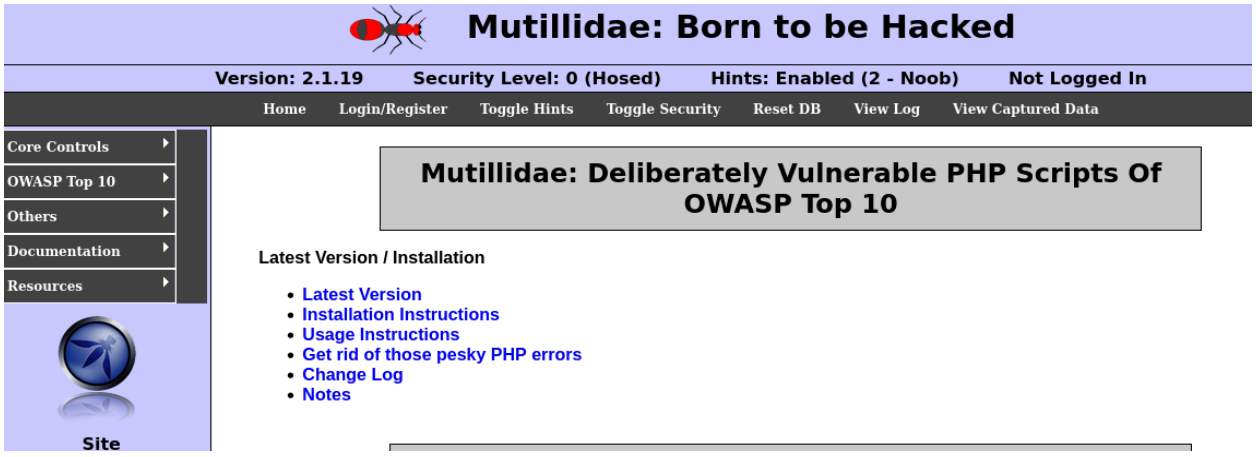
This query will always give true value because OR condition is used, which means that if either one condition is met, it will give true value. In this query, the statement "1=1" is always true. So, it will always give true value.

7) In Firefox, go the following URL:

http://<Metasploitable 2 IP>/multillidae/

You will get a page like this. Click multiple times on the buttons "**Toggle Security"** and "**Toggle Hints**". Briefly explain what happens when you change these settings. Take relevant screenshots to attach to your submission.

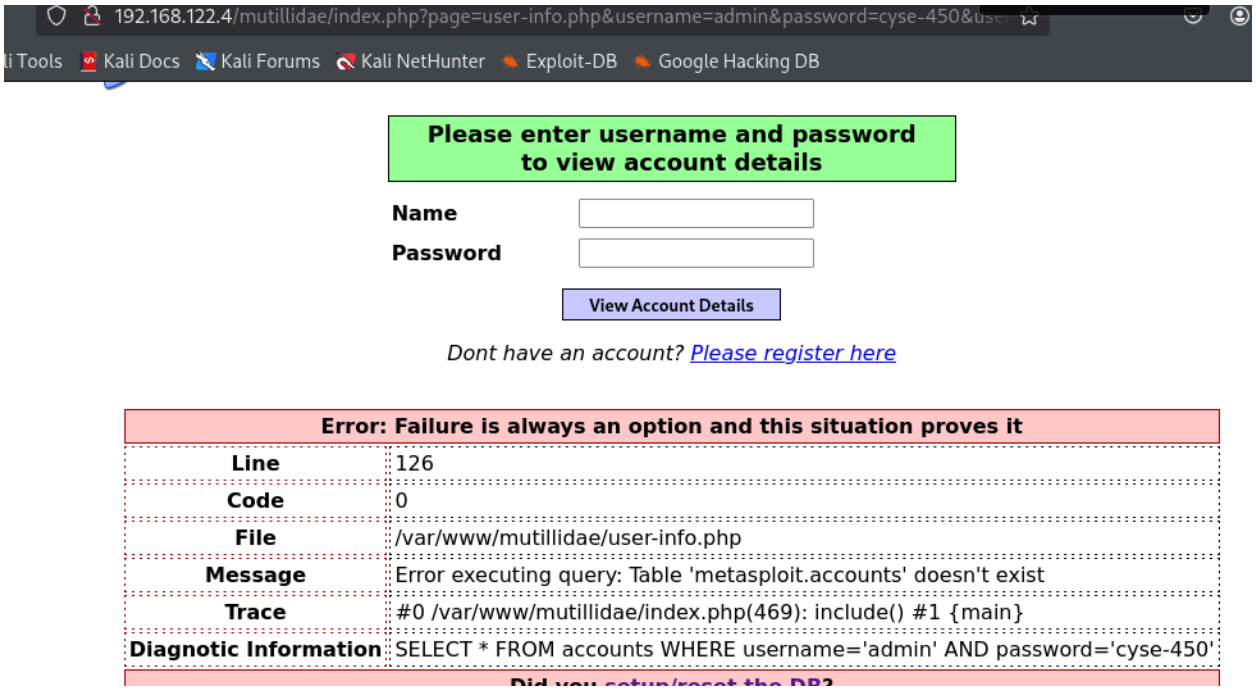
4 points



When I clicked on the buttons "**Toggle Security"** and "**Toggle Hints**" multiple times, I noticed that the security level and Hints options kept changing. Other than that, I didn't see any changes.

8) Navigate: **OWASP Top 10 → A1 - Injection → SQLi - Extract Data → User Info.**

Enter "***admin***" as Name and "***cyse-450"*** as Password. Click on the button "***View Account Details"***.



9) Similar to the following screenshot, show the SQL query that has been executed. ***Note***

that you used the password "cyse-450", not "password". If you get an error message like the message shown in the screenshot, explain the reason behind this error. If there is no error message, take screenshots of the resultant output.

6 points

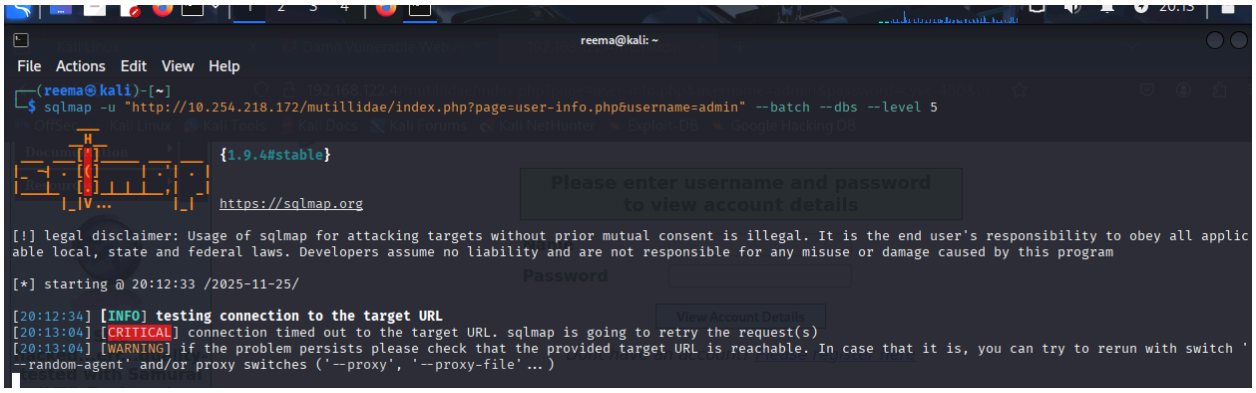
SQL query that was executed:

SELECT *FROM accounts WHERE username='admin' AND password='cyse-450'

We get this error because the condition is not met. In this query AND operator is used, which means that the statement will give true value only when both conditions are met. In this case, either username or the password is incorrect. Therefore, the condition is not met and it gives an error.

10) Run the sqlmap command shown in the following screenshot in your Kali Terminal. Take necessary screenshots showing your results.

4 points



11) Explore different features of the ***Mutillidae*** application and provide a brief comparison with the DVWA application. Make sure you discuss the features of both applications in your comparative discussion.

6 points

Both Mutillidae and DVWA are free, open source, vulnerable web applications intentionally designed with a wide range of security flaws. They serve as practical training grounds for learning, testing, and improving web security skills. Mutillidae offers a broader range of scenarios including, OWASP Top 10, web services, and authentication. It has over 40 vulnerabilities and challenges. DVWA, on the other hand, is a lightweight training platform, mainly focused on SQL and PHP vulnerabilities. It offers hands-on-experience with SQL injection, XSS (Cross-site Scripting), Command Injection etc.