6CYSE 450: Ethical Hacking and Penetration Testing

Lab 6: DVWA vs Multillidae

Total Points: 30

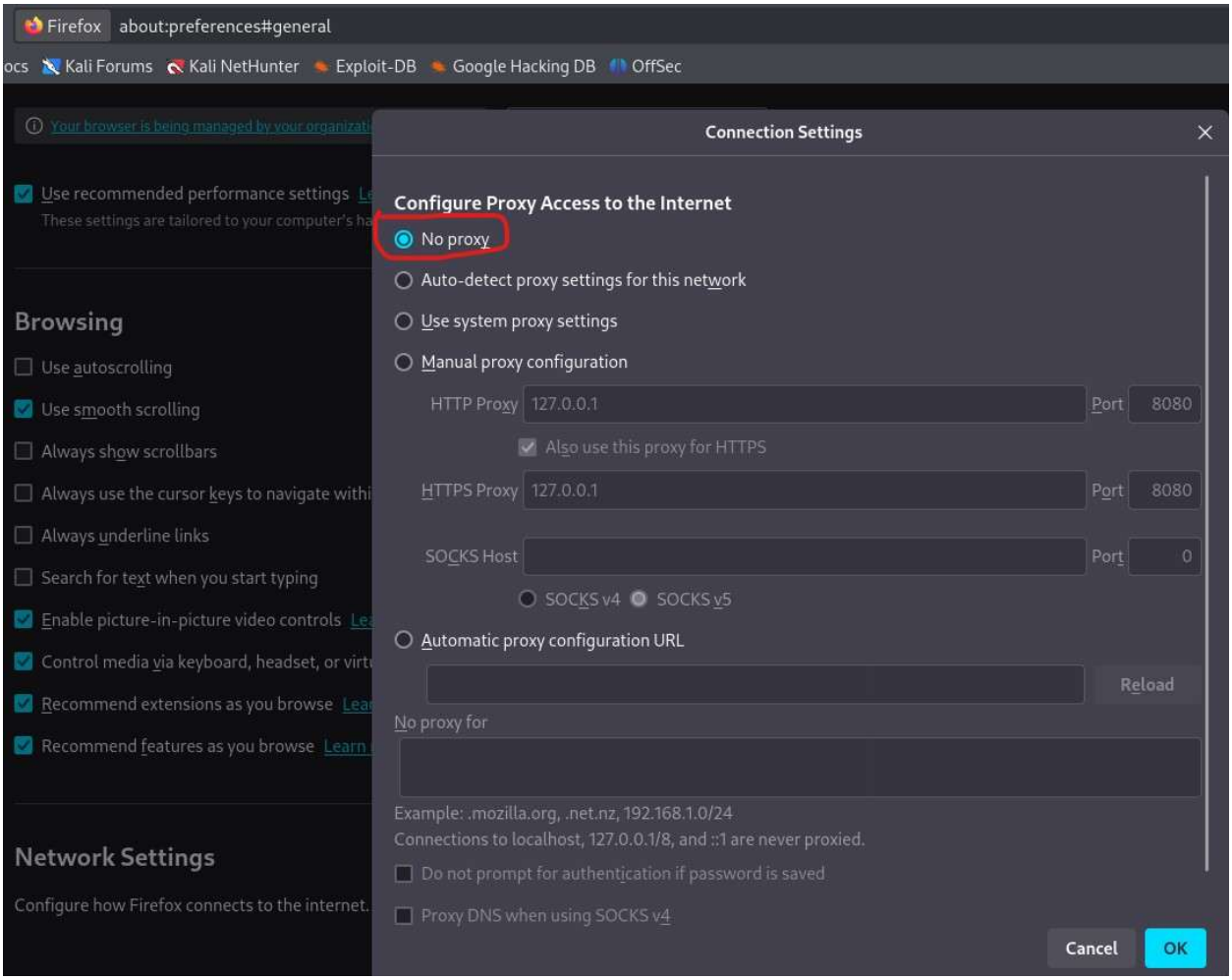
Tasks:

---

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.

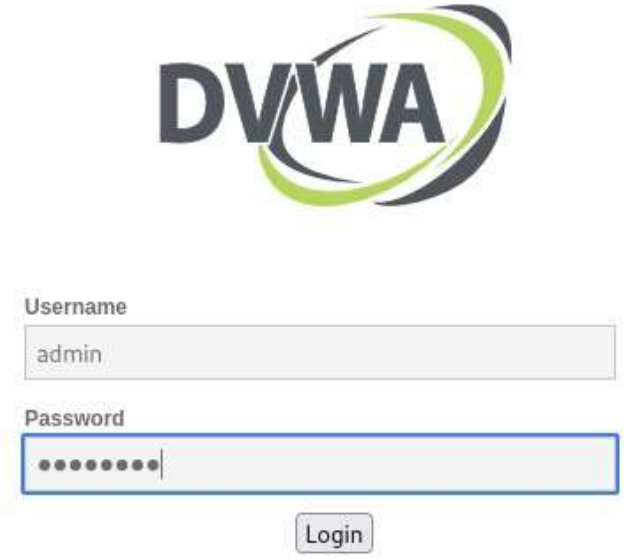


4) Enter the following URL in your Firefox browser (in your Kali VM):

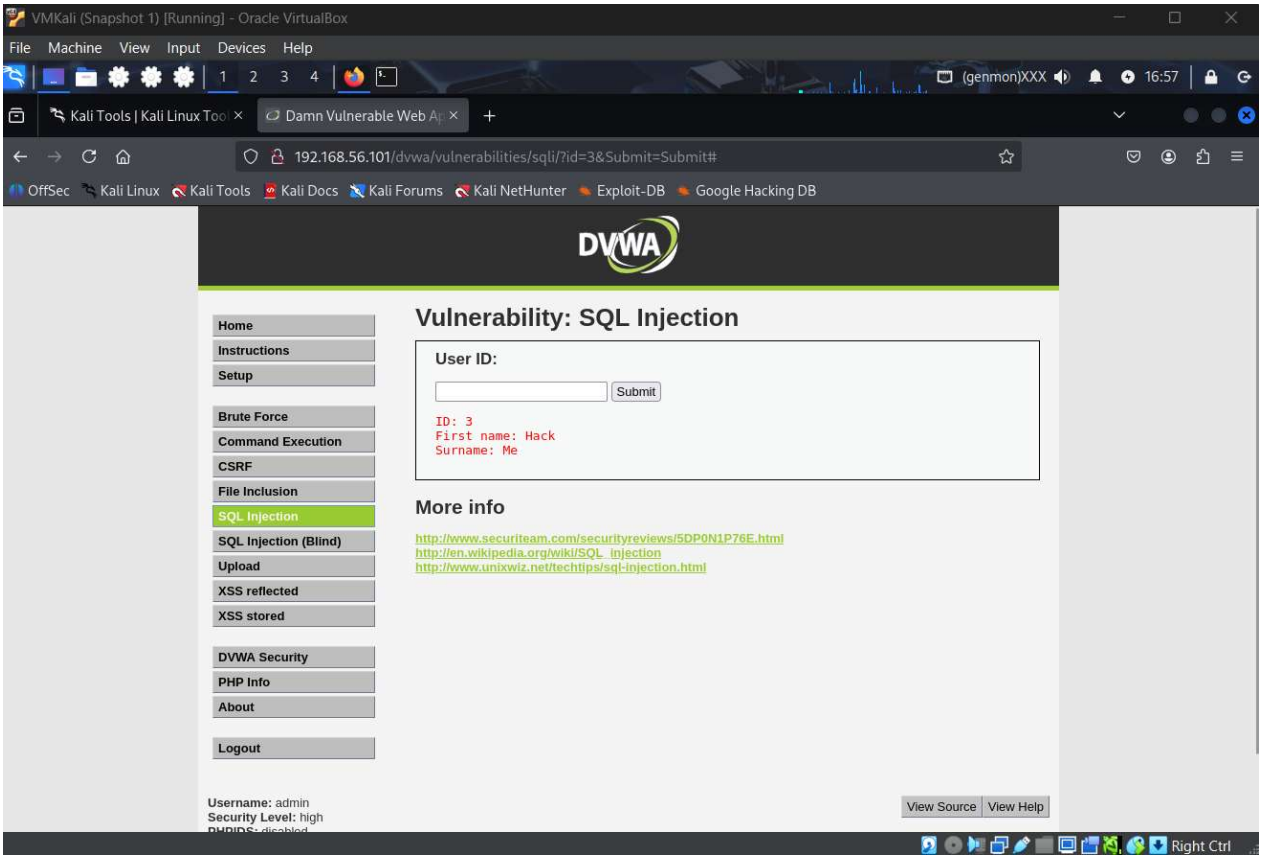
https://<Metasploitable 2 IP>/dvwa/login.php

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**



An SQL query could be used to give the same result by essentially making the server execute the code that the user puts into a text box because the code is not properly sanitized. An SQL query to find this would be 3' OR '3'='3'#

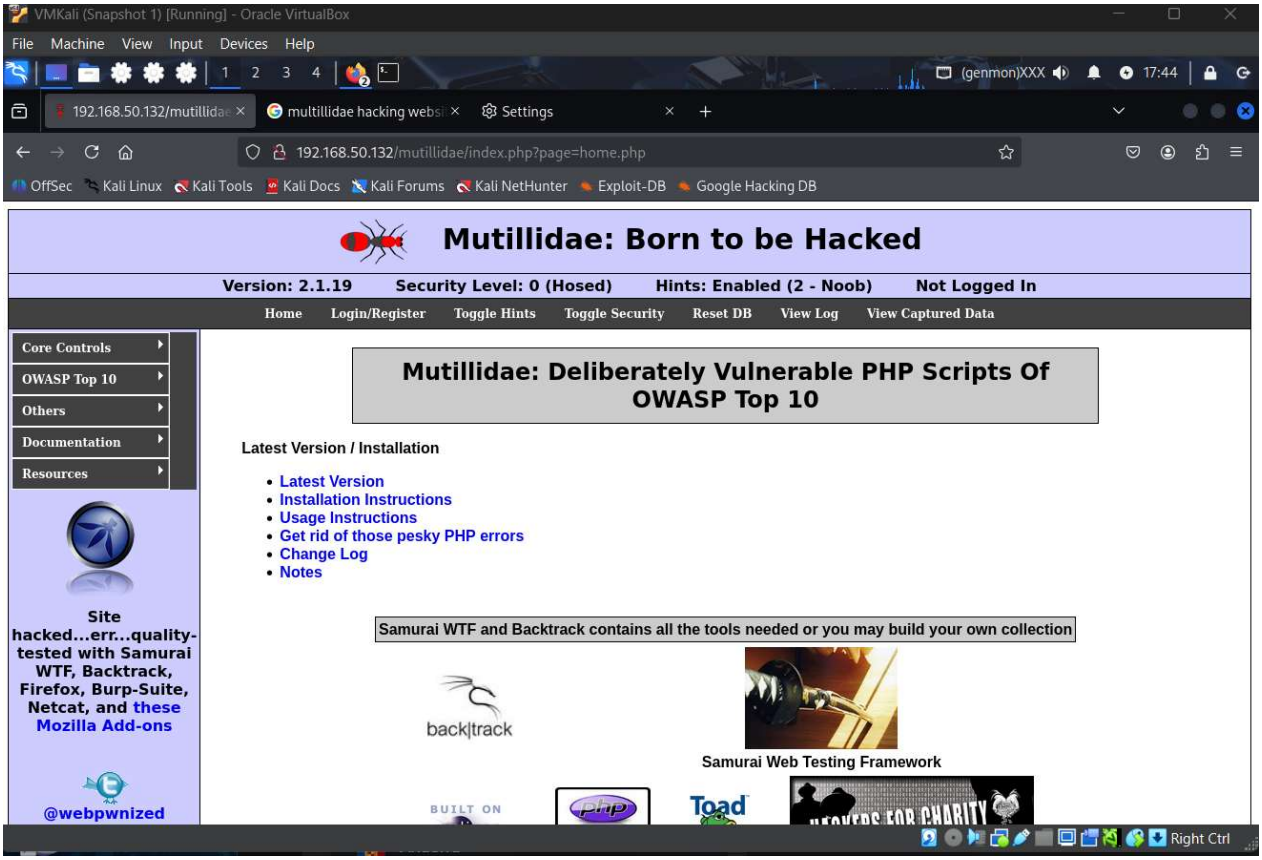
7) In Firefox, go the following URL:

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

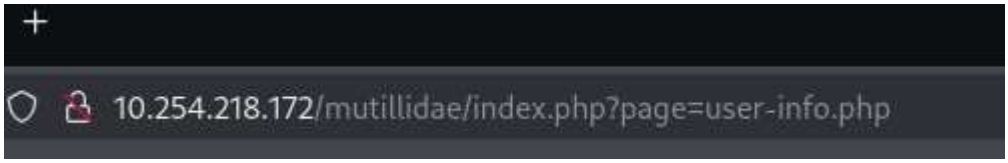
You will get a page like this. Click multiple times on the buttons "**Toggle Security**" and "**Toggle Hints**". Briefly explain what happens when you change these settings. Take relevant screenshots to attach to your submission. **4 points**

When you click the Toggle security button, the hints disappear and the level of security at the top changes. When you click the hints button when you are on security level 0, the level of hints

change from level 0-2



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



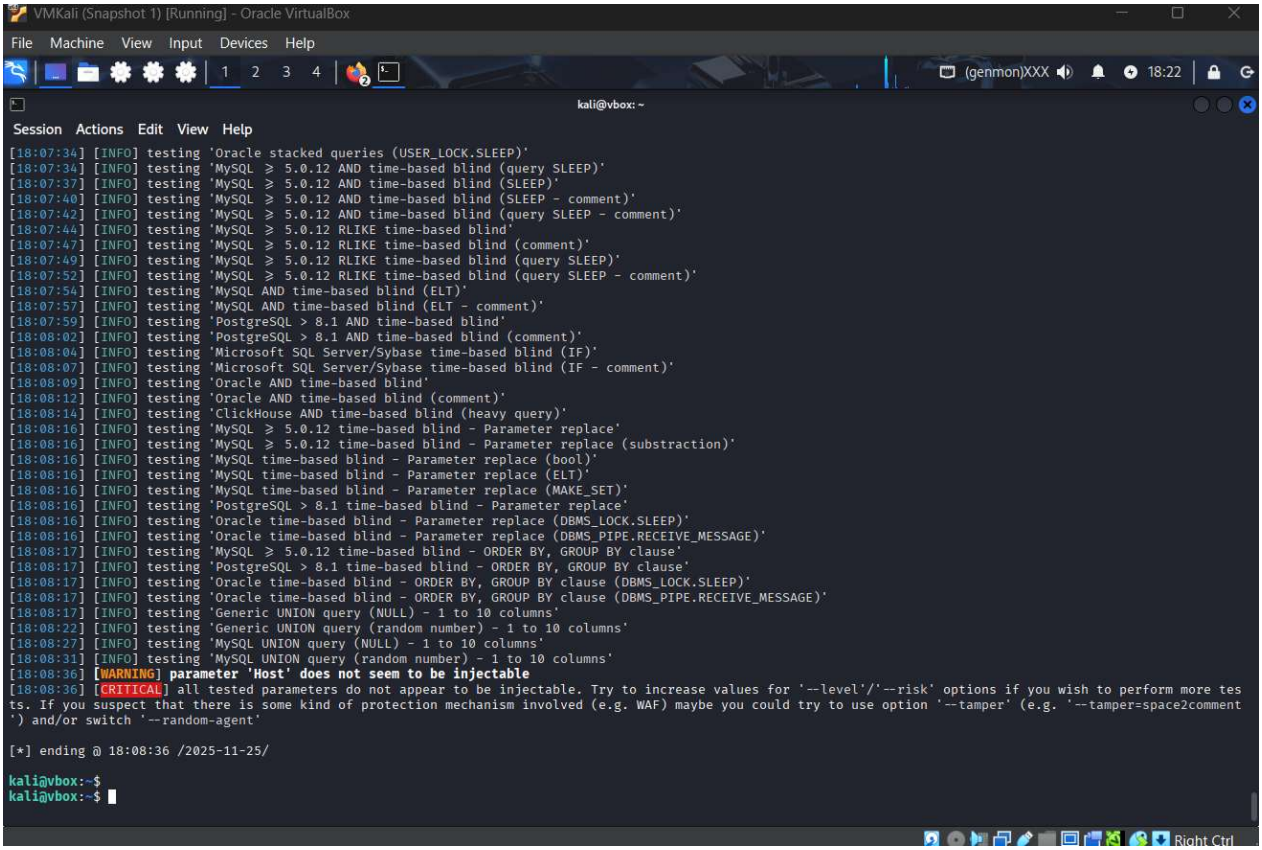
Enter ***"admin"*** as Name and ***"cyse-450"*** as Password. Click on the button "**View Account Details**".

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**

   I got an error message like the screenshot. This is because the account I am inputting does not exist

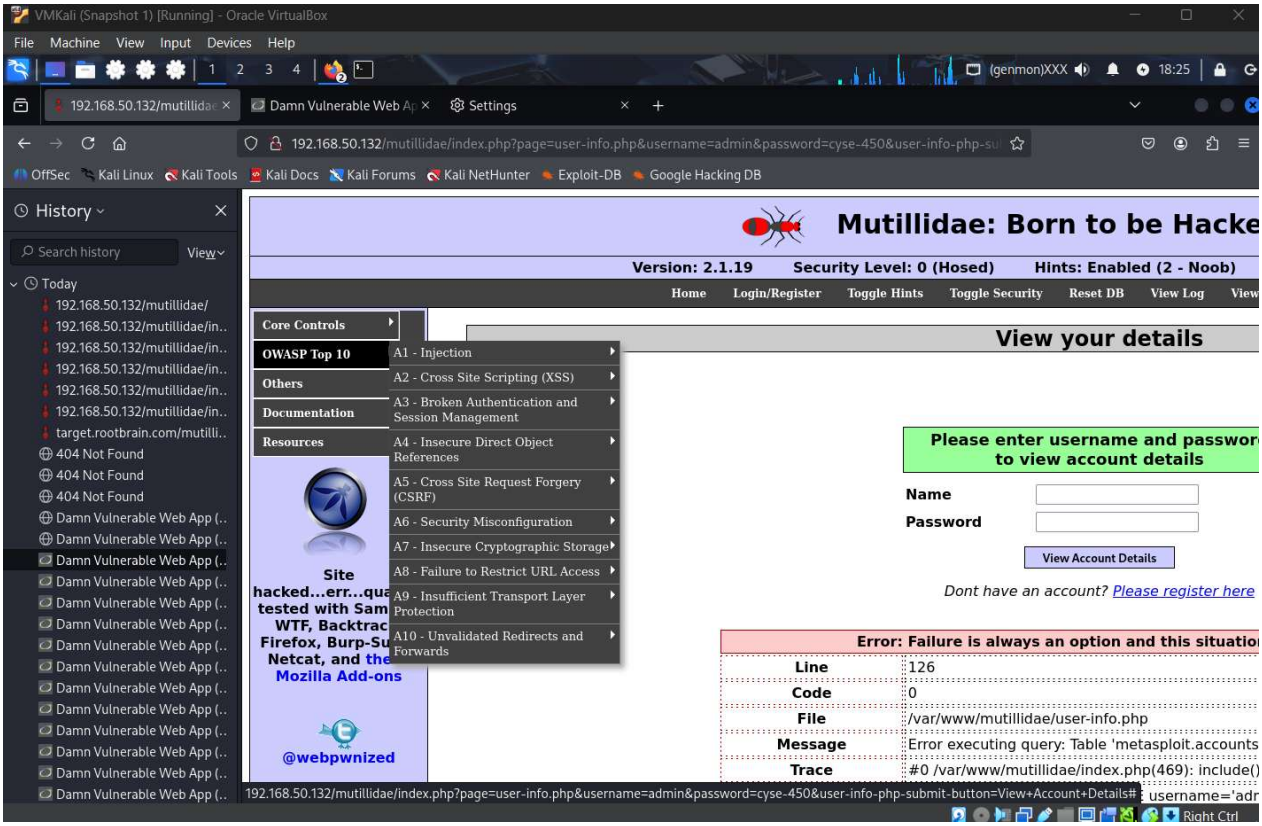
10) Run the sqlmap command shown in the following screenshot in your Kali Terminal. Take necessary screenshots showing your results.

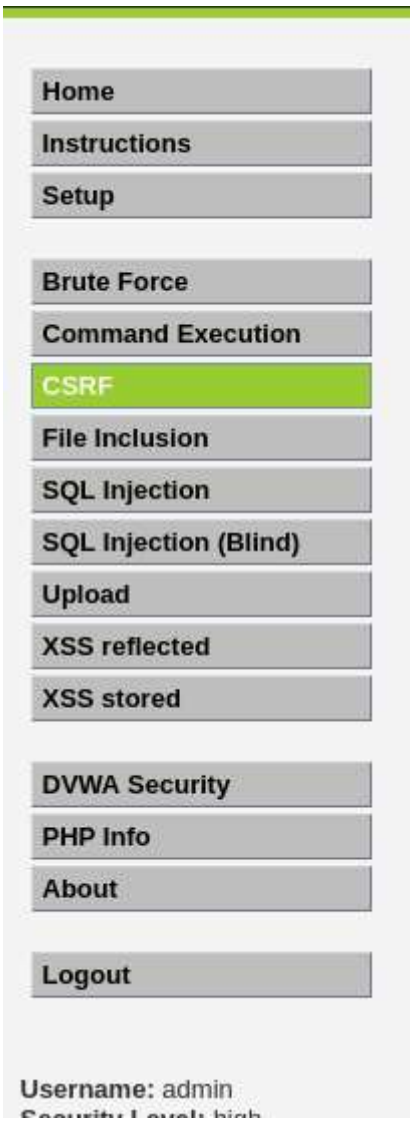
4 points



11) Explore different features of the ***Multillidae*** 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**





DVWA and mutillitude both have plenty of tools for testing different kinds of attacks as shown by the highlighted tools above, but they both have mostly different tools. For example, DVWA and Mutillitude both have XSS and SQL Injection, but DVWA does not have things like CSRF, or insecure cryptographic storage.