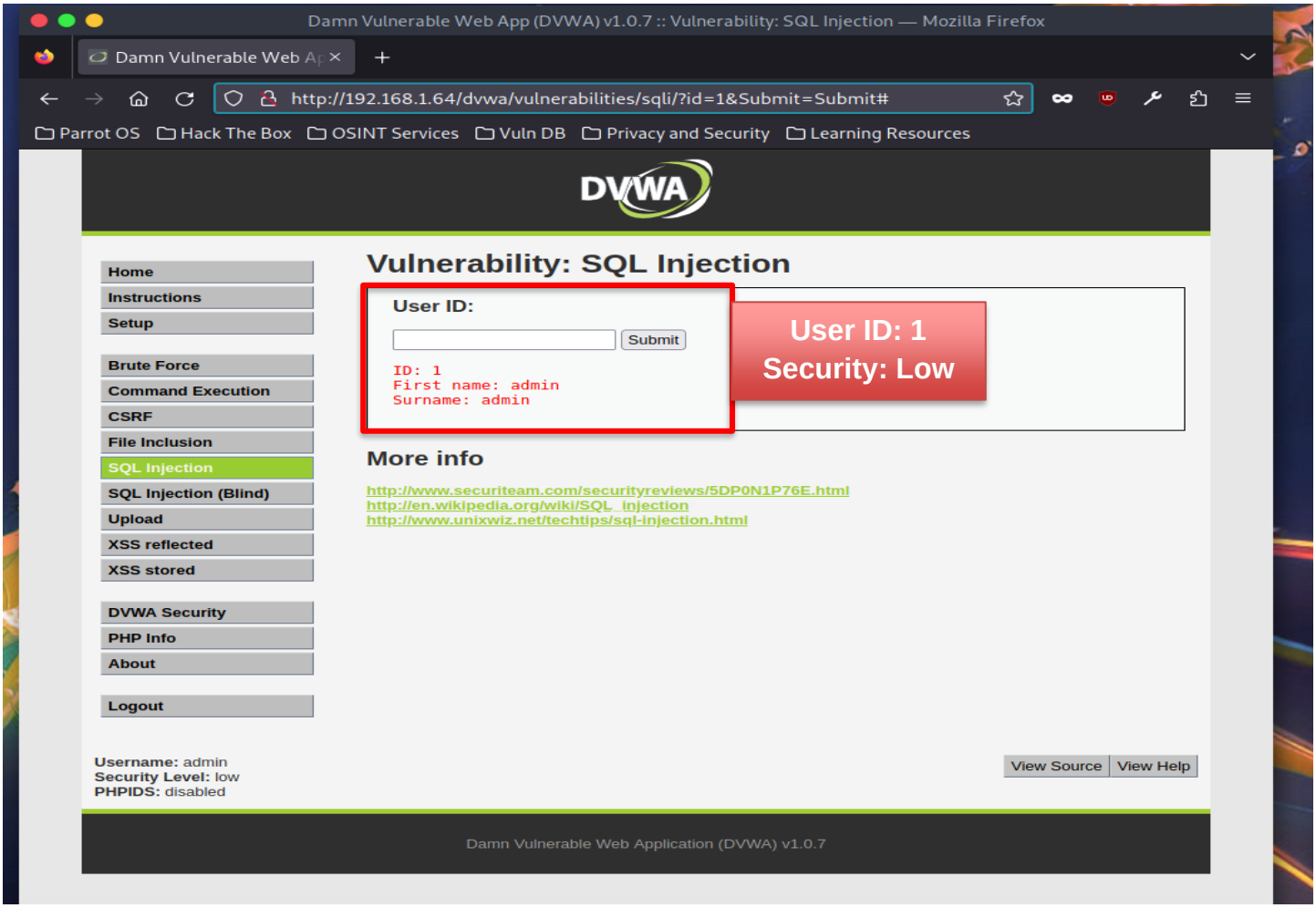
LUKE DUNK
11/30/2023
PROF. VATSA

CYSE 450 - Ethical Hacking & Penetration Testing Assignment – 12

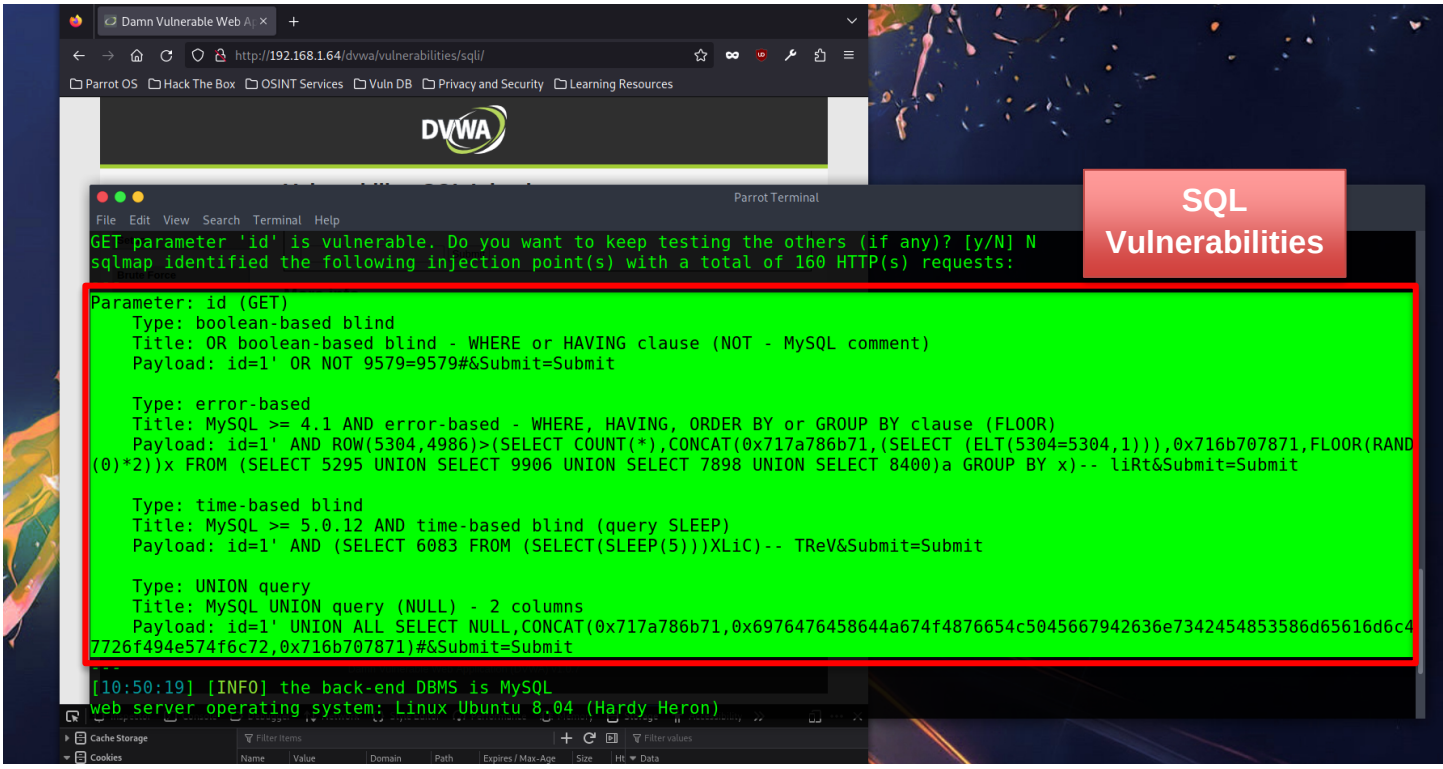
Task A: Using SQLMap to automate SQL injection to Obtain data from DVWA Application

1. Open terminal in Kali Linux
2. Login to Metasploitable2 VM and find the IP address.
3. In the browser, in Kali VM, type the Ip address of metasploitable2 and login to DVWA application.
4. Set the" DVWA Security" to "low", Select "SQL Injection" tab and type"1" in the User Id box. Hit the Submit button. Don't forget to copy the URL after submitting action. Please submit the screenshot for this step.



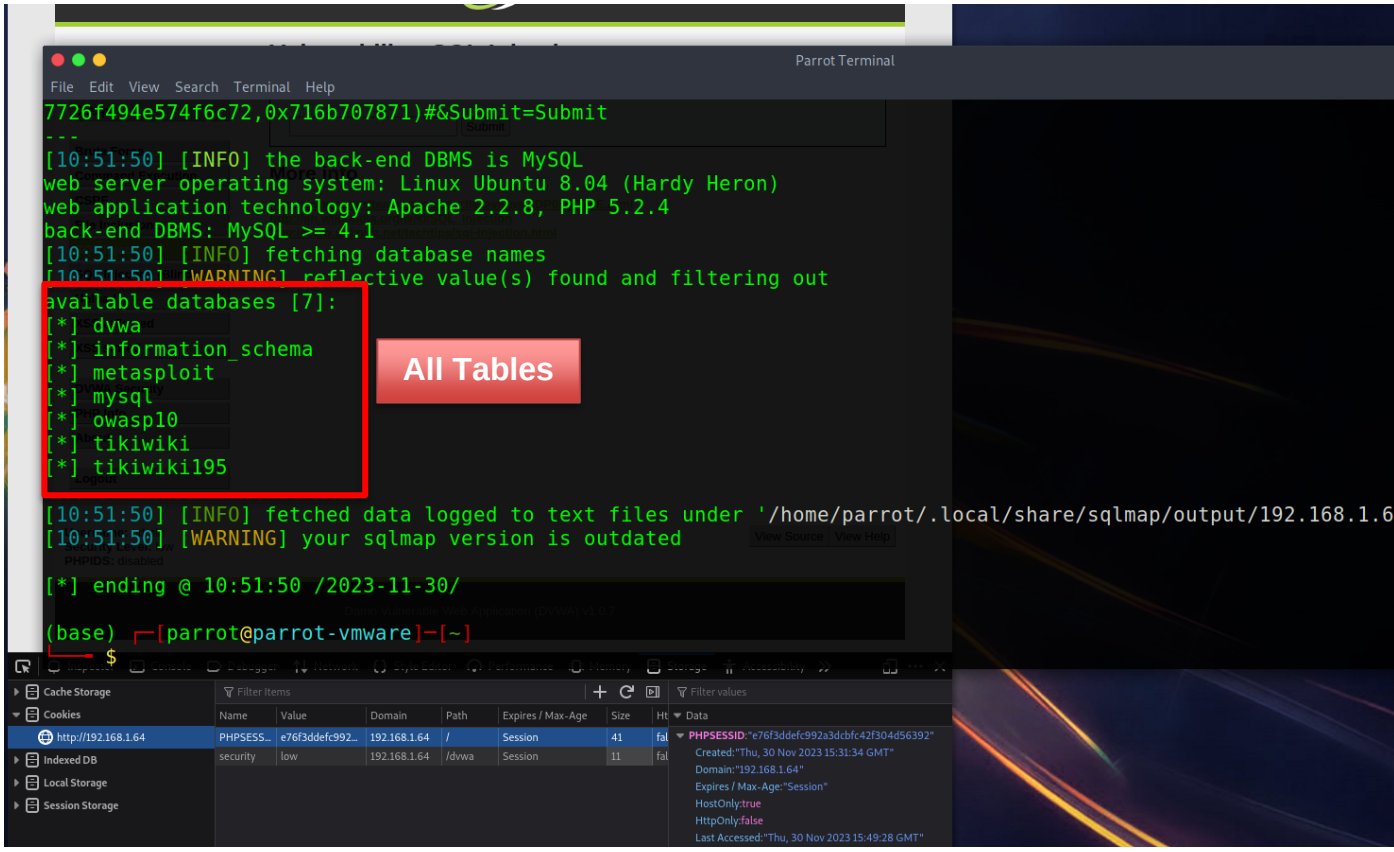
LUKE DUNK
11/30/2023
PROF. VATSA

5. Use sqlmap tool/command to find the vulnerabilities for SQL injection in the URL copied in the above step. Highlight the Vulnerabilities detected for SQL injection. Please submit the screenshot for this step.



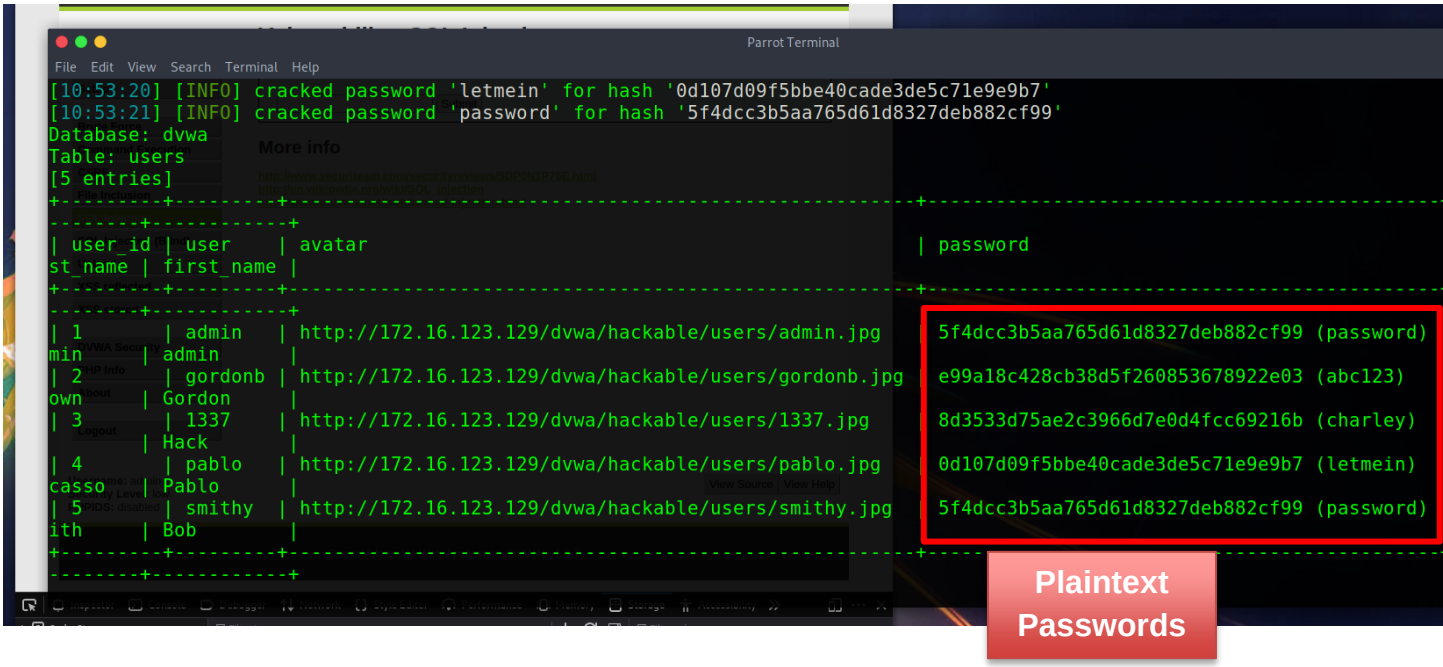
LUKE DUNK
11/30/2023
PROF. VATSA

6. In Kali terminal, use SQLmap command to display all the tables used by DVWA database. Please submit the screenshot for this step.



LUKE DUNK
11/30/2023
PROF. VATSA

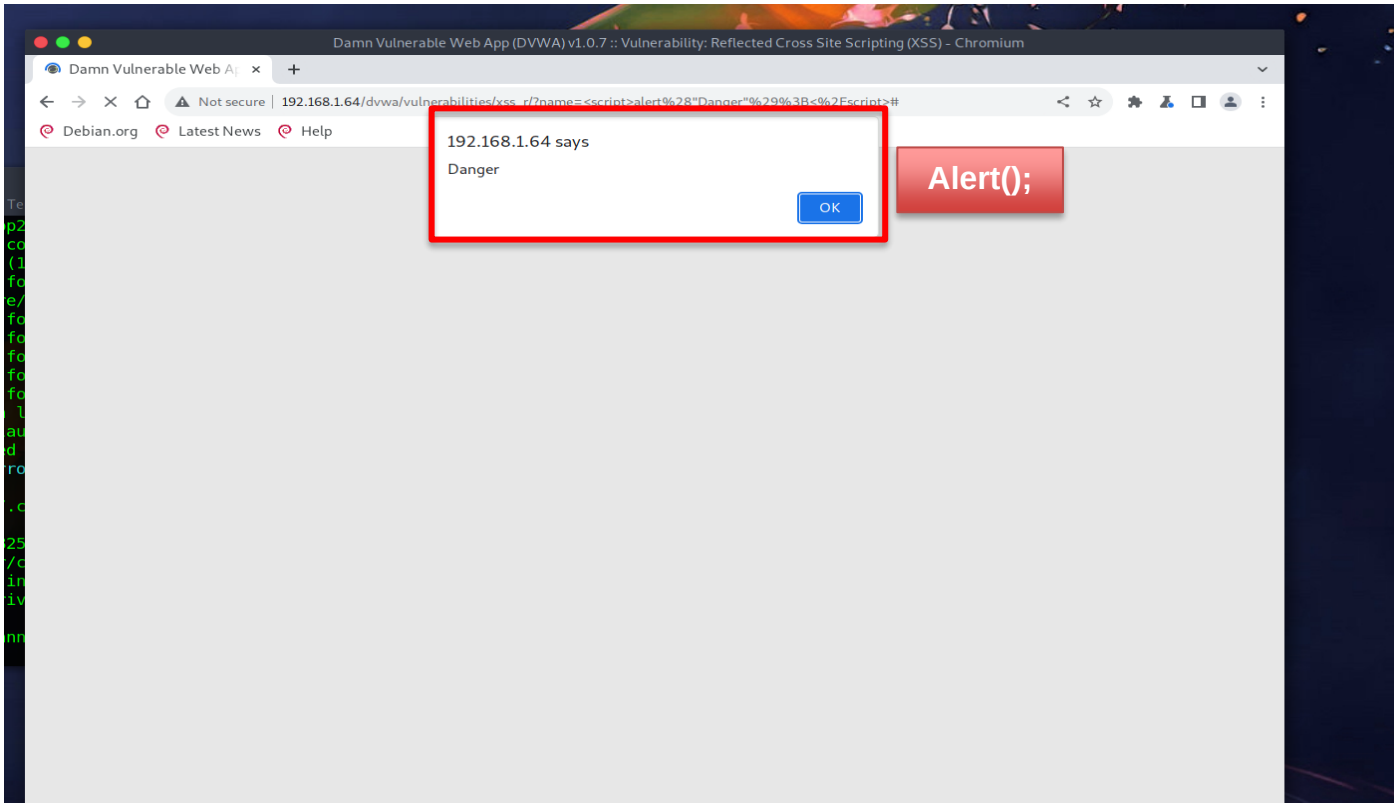
7. Use SQLmap command to display all the users along with passwords in plaintext format in "users" table. Please submit the screenshot for this step.



LUKE DUNK
11/30/2023
PROF. VATSA

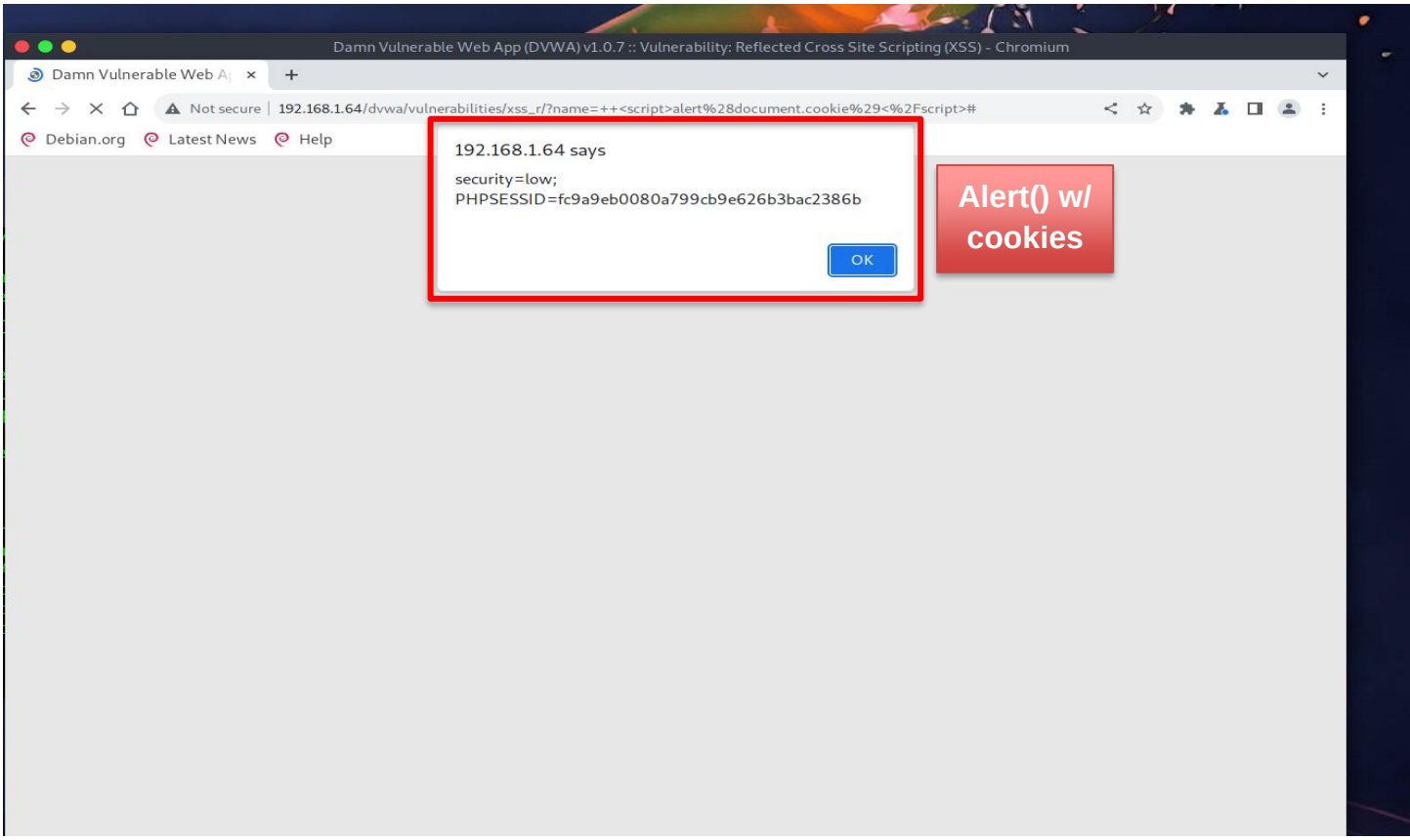
Task B: Using Cross Site Scripting to Obtain data from DVWA Database

1. Login to DVWA application and set the “DVWA Security” to “low”.
2. Select “XSS reflected” and post a Malicious Message to Display an Alert Window in DVWA application Window by embedding a JavaScript program in the “What is Your name?” field.



LUKE DUNK
11/30/2023
PROF. VATSA

3. Post a malicious code to display cookies using alert(),as demonstrated in the class.



LUKE DUNK
11/30/2023
PROF. VATSA

4. Select “XSS Stored” and in the message box, use “<script>document.location=Ip-address of DVWA website</script> to perform DOM based Cross site scripting.

ss_s/