**SCHOOL OF COMPUTER SCIENCE**

**UNIVERSITY OF PETROLEUM AND ENERGY STUDIES**

**DEHRADUN, UTTARAKHAND**



**IT DATA SECURITY LAB**

**LABORATORY FILE**

**(2024-2025)**

**For**

**Vth Semester**

**Submitted To: Submitted By:**

Prof. Abhishek Yadav Mr. Akshat Negi

Assistant Professor S.S. 500106533(SAP ID)

[Vth Semester] R2142220414(Roll No.)

School of Computer Sciences B.Tech. CSF (Batch-1)

**LAB EXPERIMENT – 4**

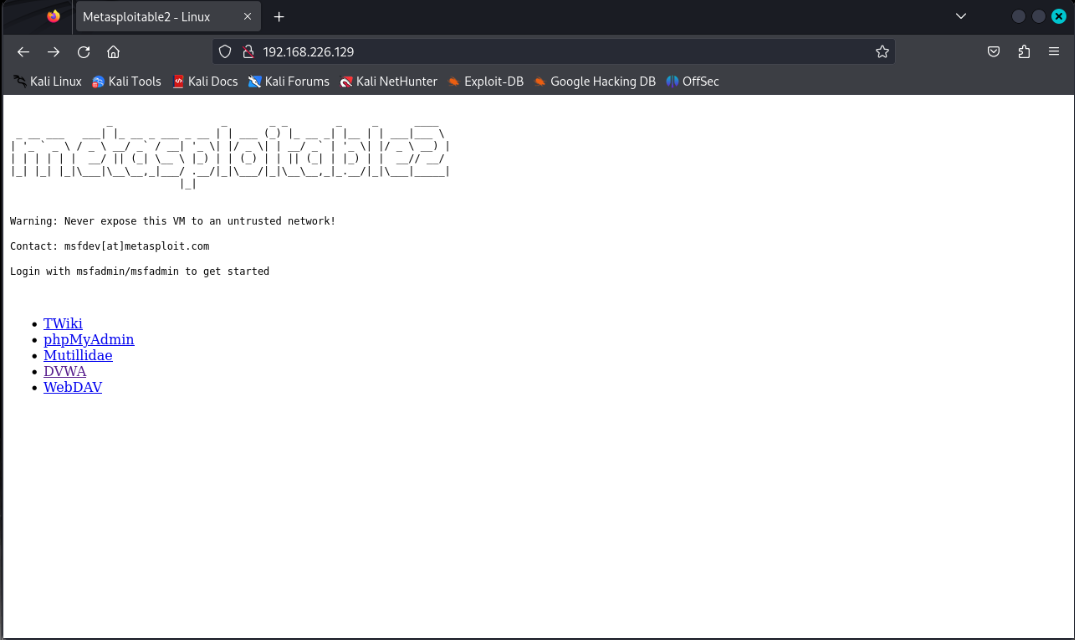
**BSQL – BLIND SQL INJECTION**

1. **INSTALLATION OF DVWA**

Go to browser

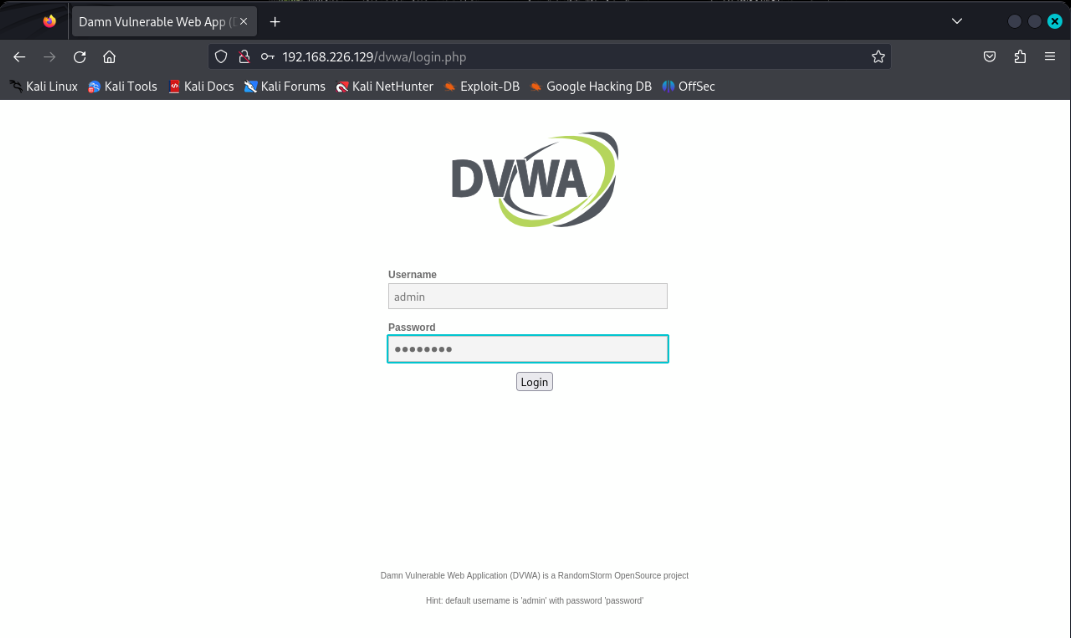
Type 127.0.0.1/dvwa/setup.php

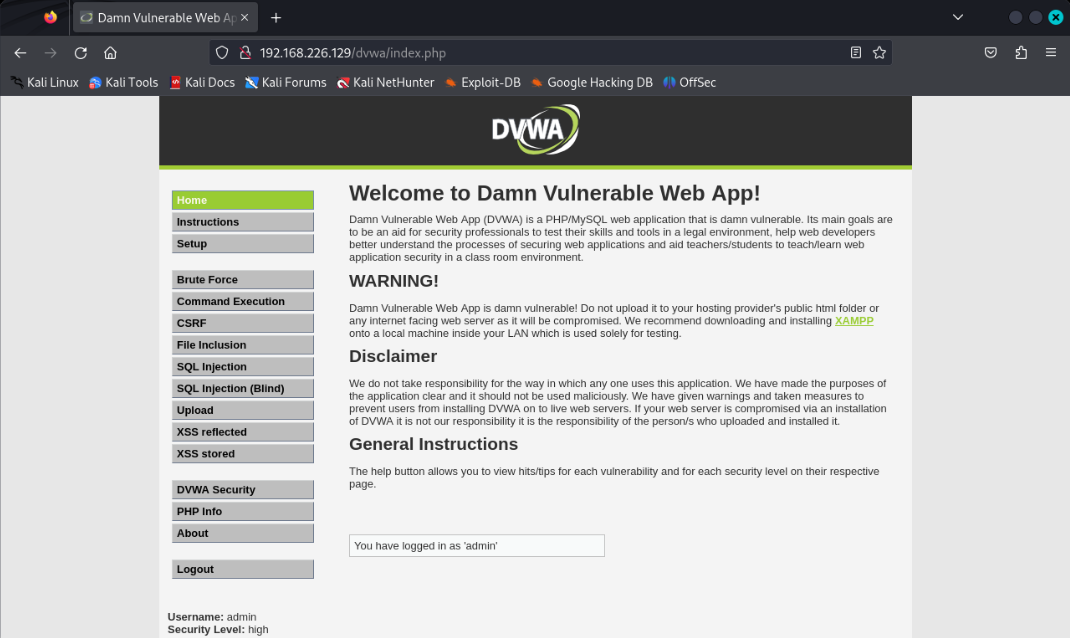
You will be redirected to DVWA



Blind SQL Injection Vulnerability Solution

1.Login to DVWA application and go to Blind SQL Injection challenge





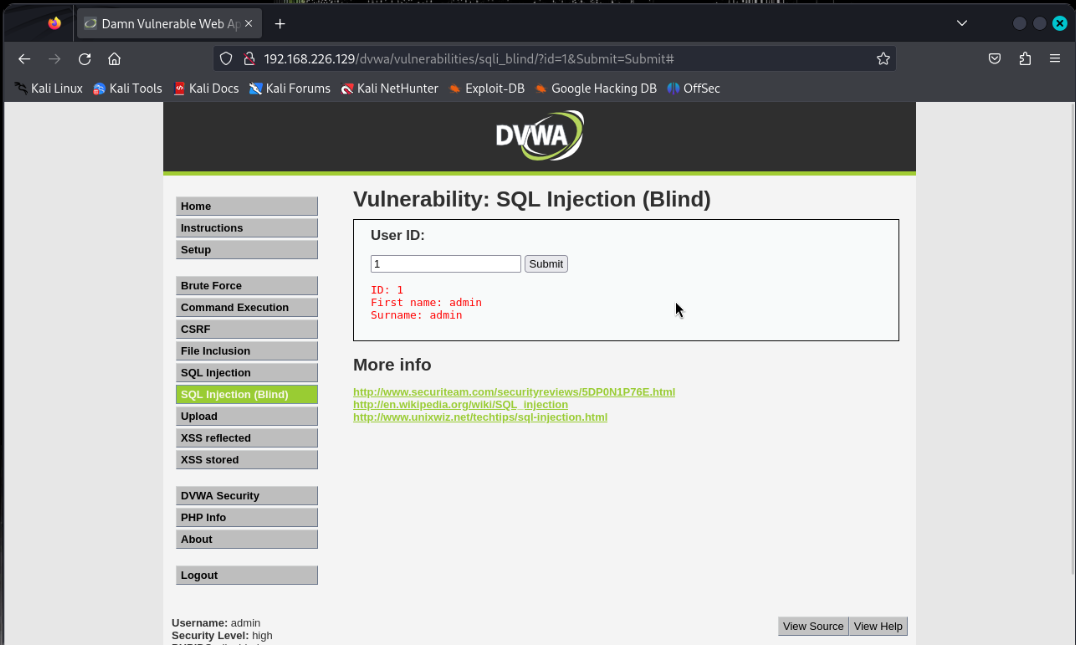
2.Its asking to provide User ID:

3.Let’s provide 1 as User ID

4.We received response as User ID exists in the database. for User ID 1

5.Now provide 9 as User ID

6.For 9, we received response as User ID is MISSING from the database.



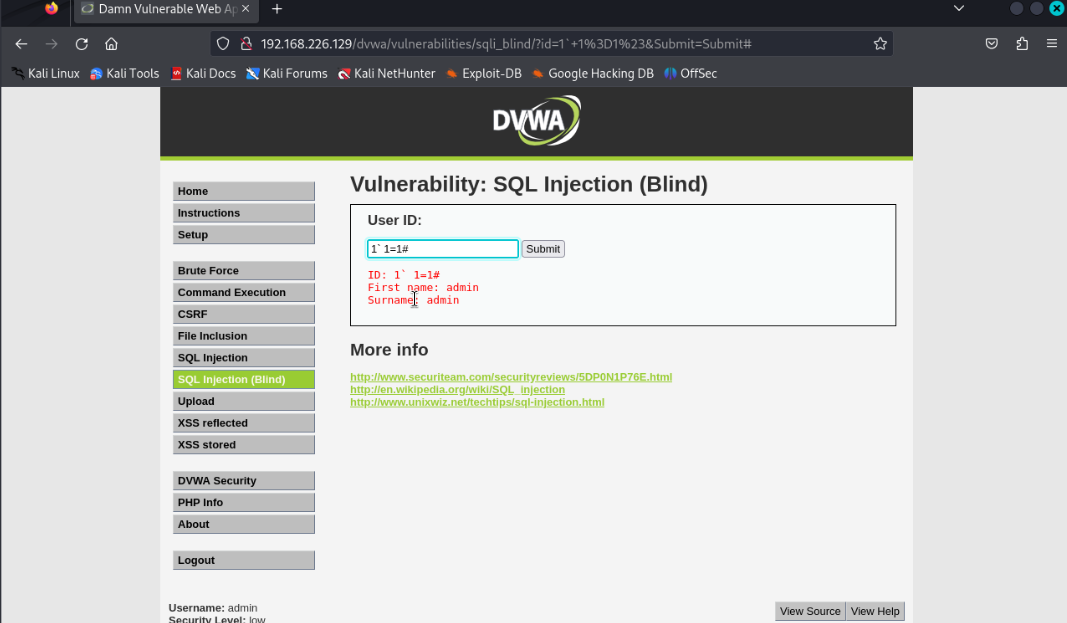
7. Now provide special character '

8.For ', response is - User ID is MISSING from the database.

So, for all invalid data we are getting response as User ID is MISSING from the database

9 Let’s prepare a payload which always return True value l.e. %' or '1'='1

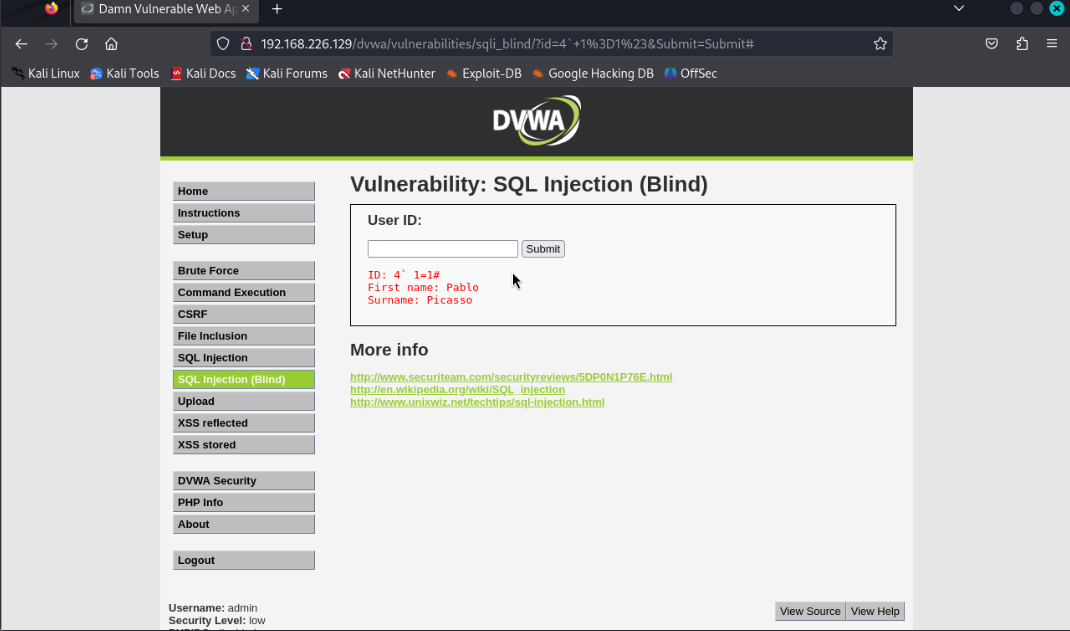
10. We received a response as User ID exists in the database., for %' or '1'='1

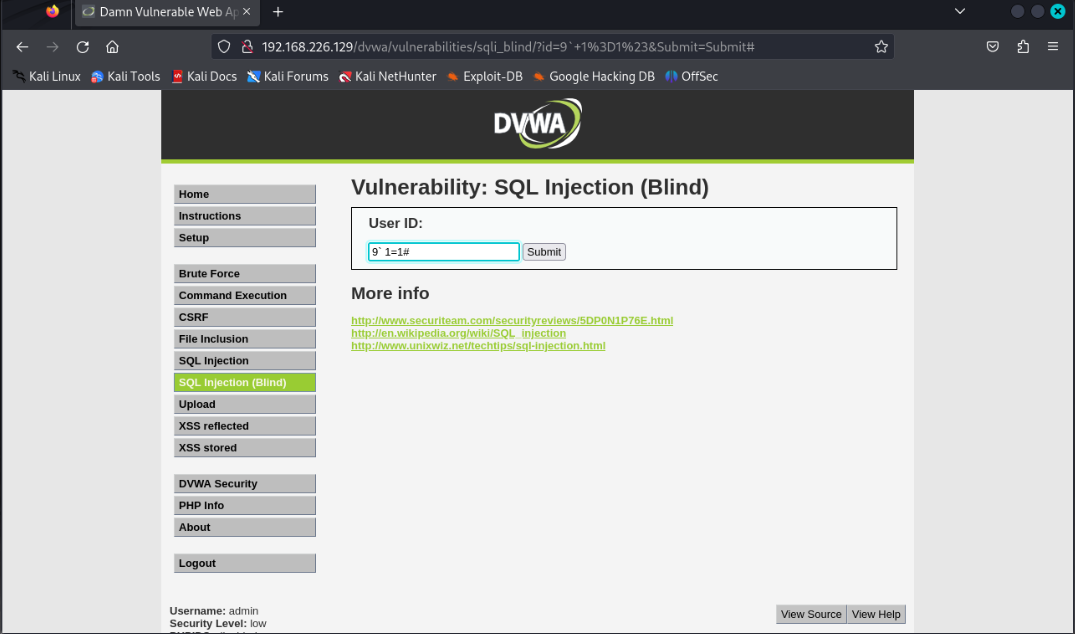


11.now modify the payload, which will return False response %' or '1'='2

12. Now response is - User ID is MISSING from the database.

13. Application considered %' or '1'='1, as a valid User ID.





14. We can conclude an application is vulnerable to SQL Injection, though it's not disclosing any sensitive data such as SQL error, table name or database name.

15. We need to plan our attack further to get sensitive data.