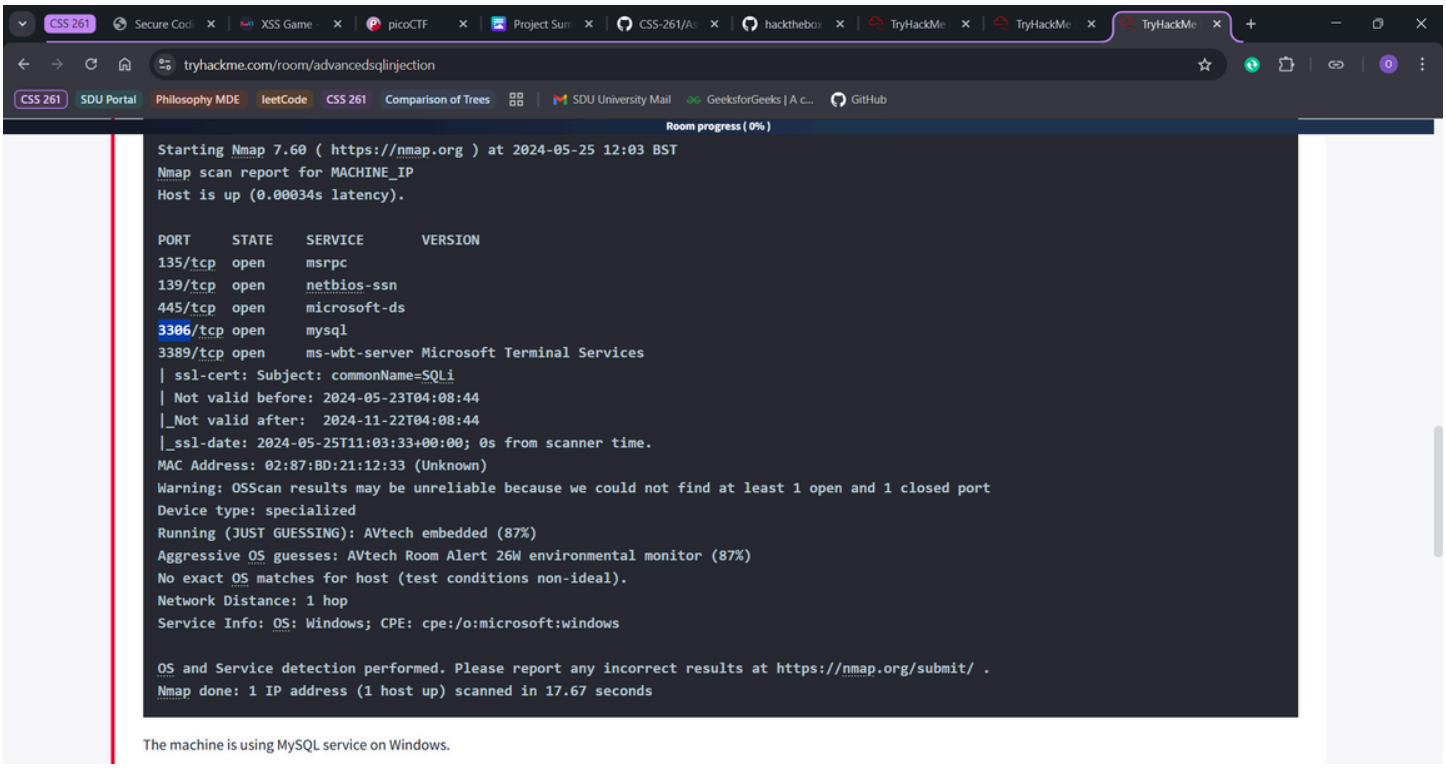
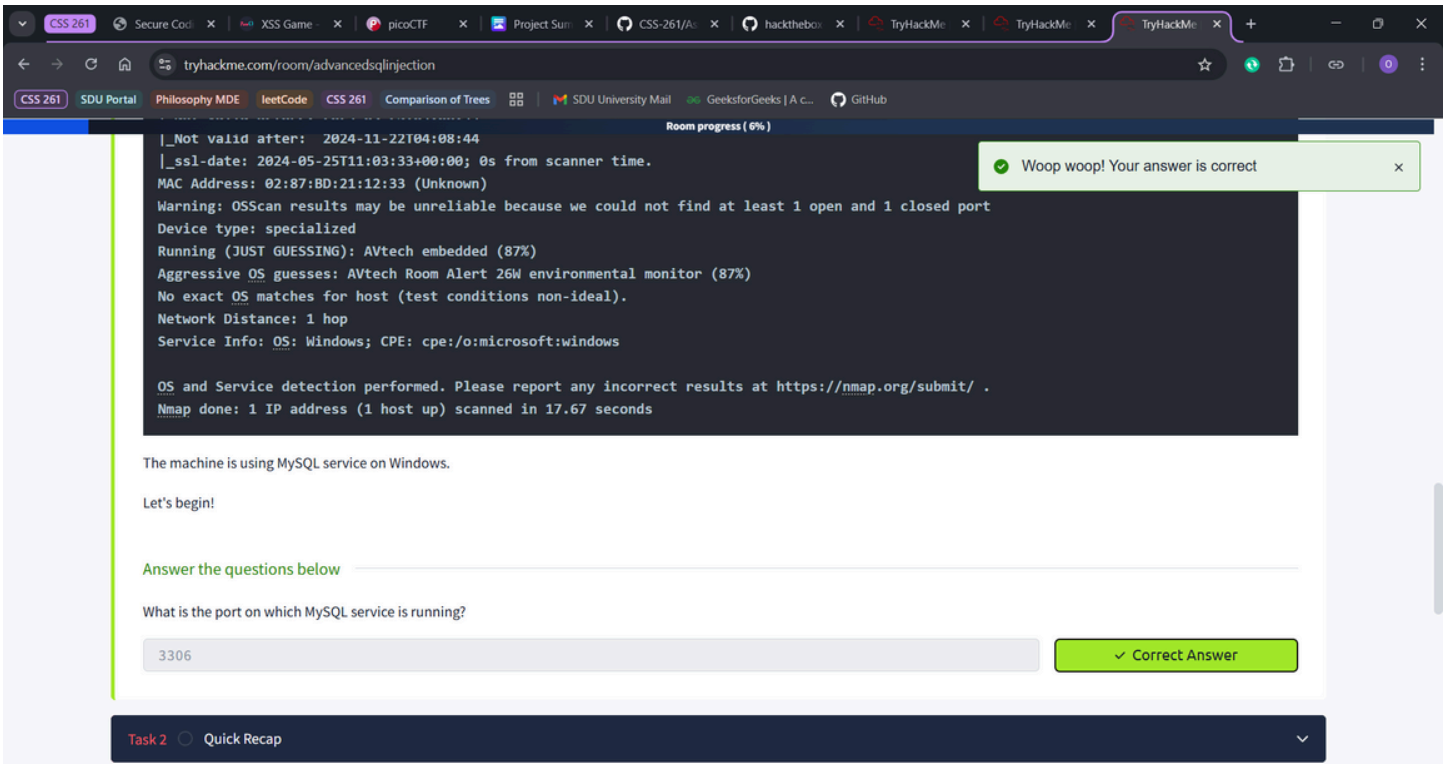
TryHackMe

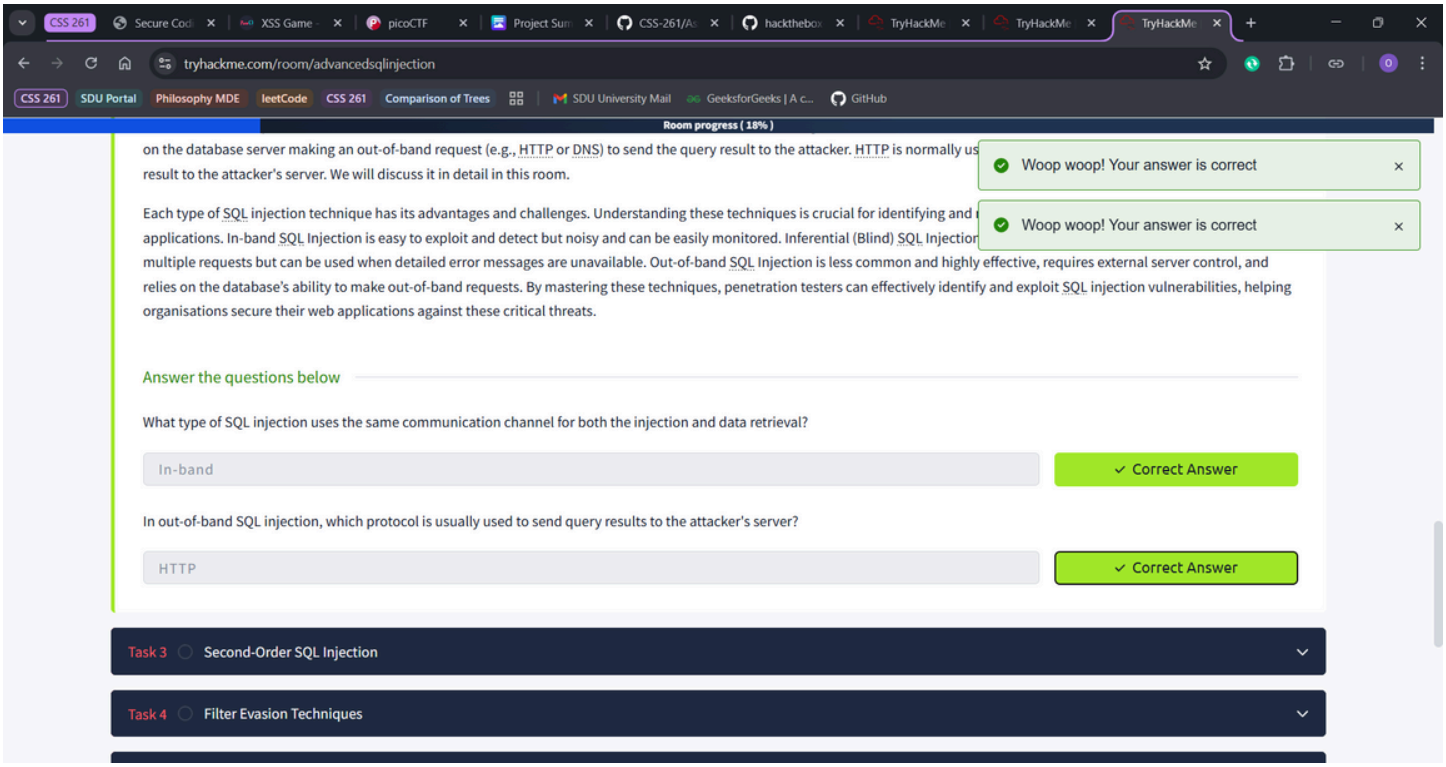
Advanced SQL Injection

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

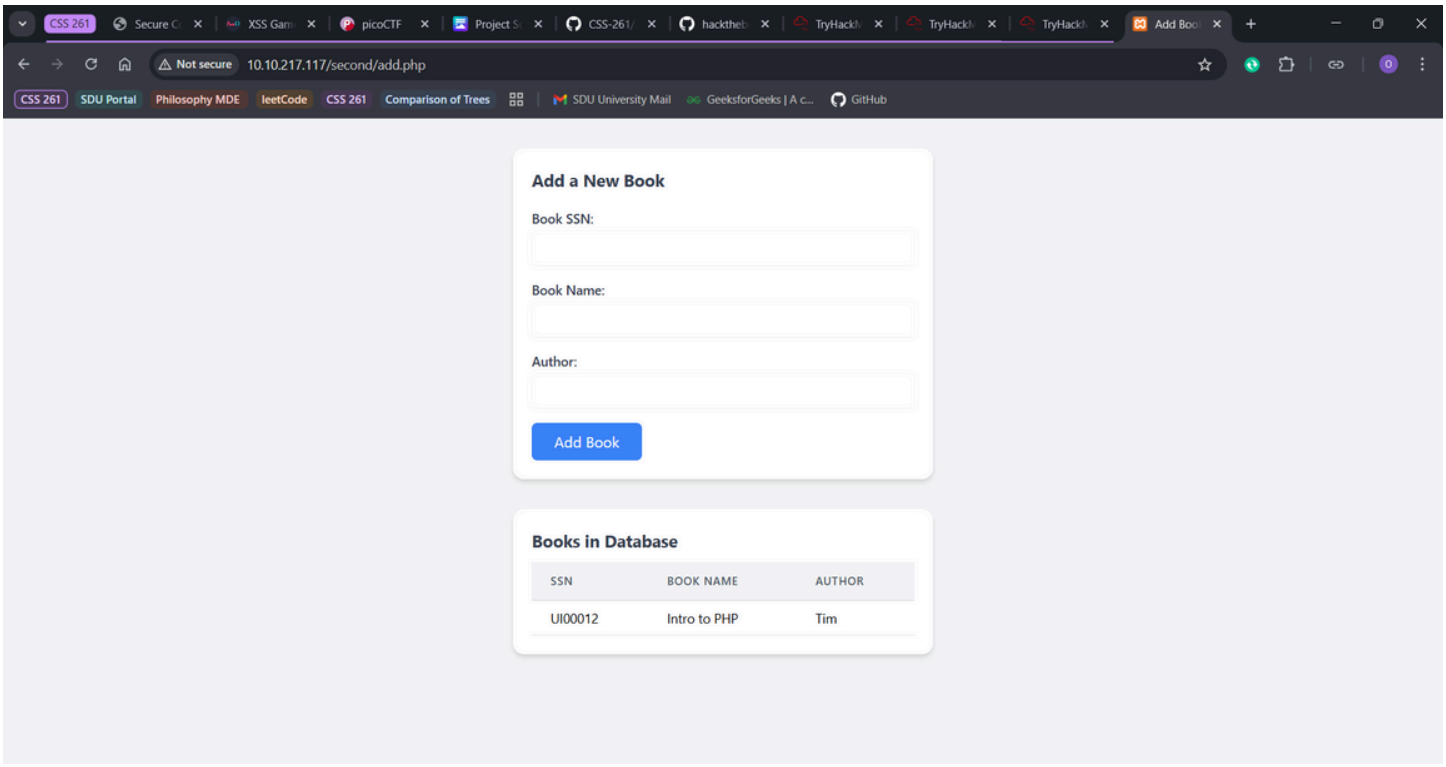
Here we have our room:
I learned a lot from here, and this all the answers to the theoretical part, it wasn't that hard to answer, it literally said in the above, we just need to read it carefully.



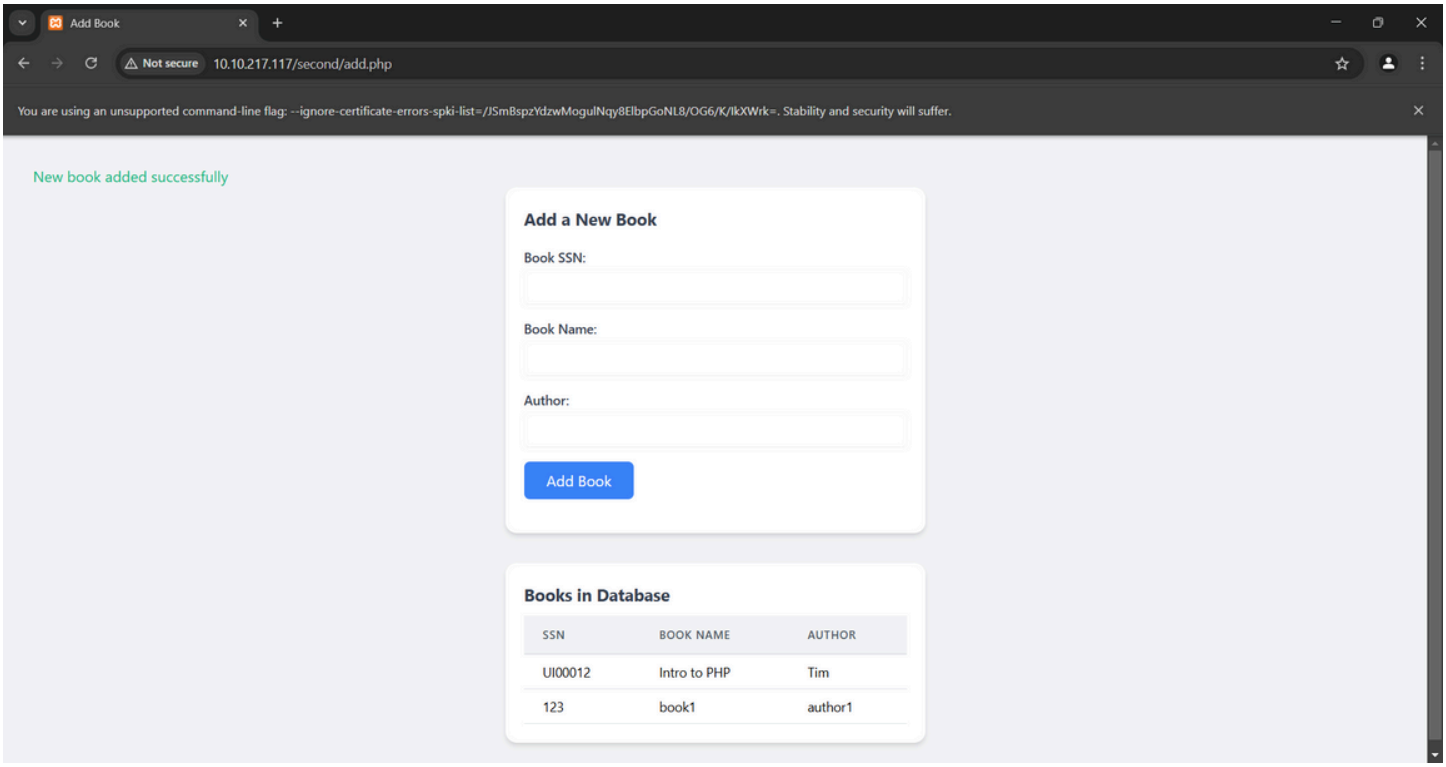




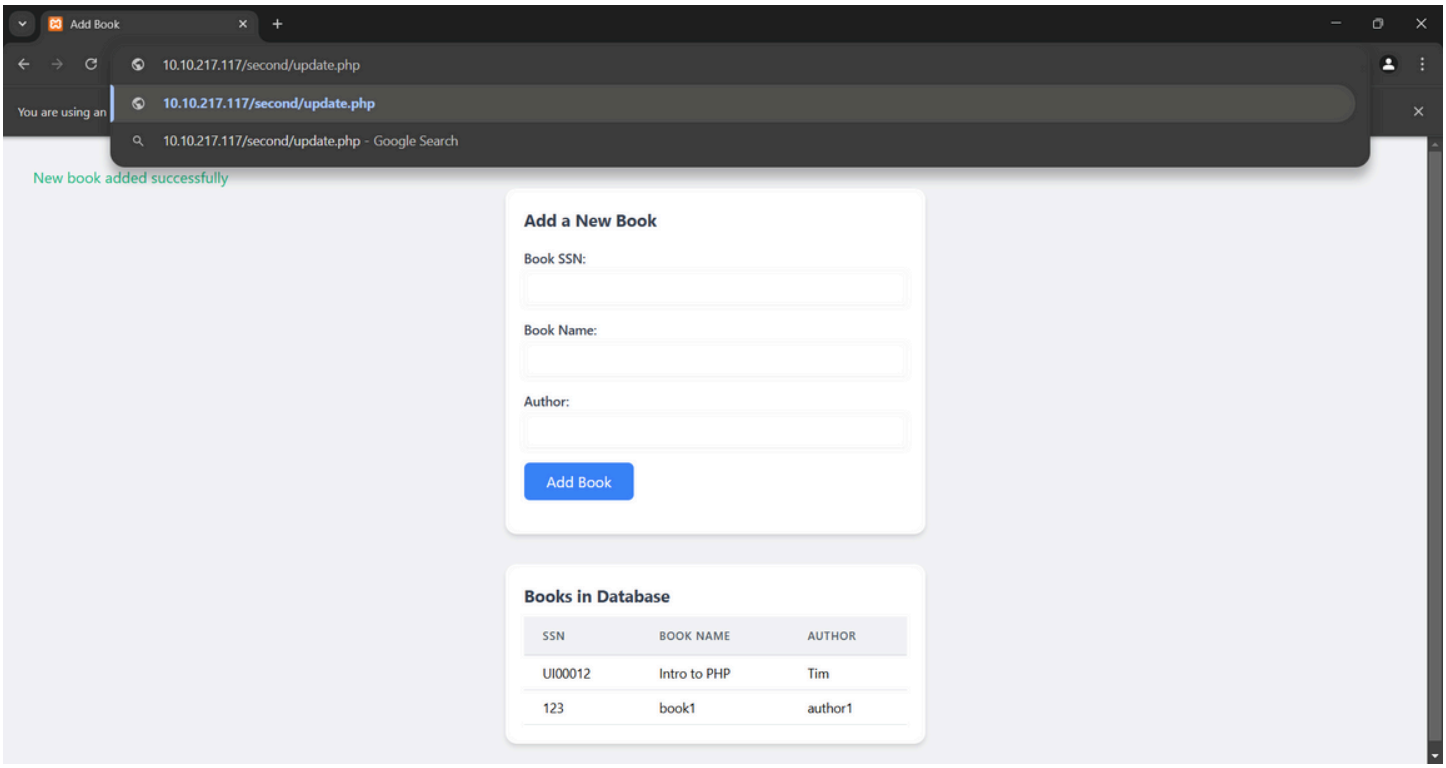
And there is the practical part:



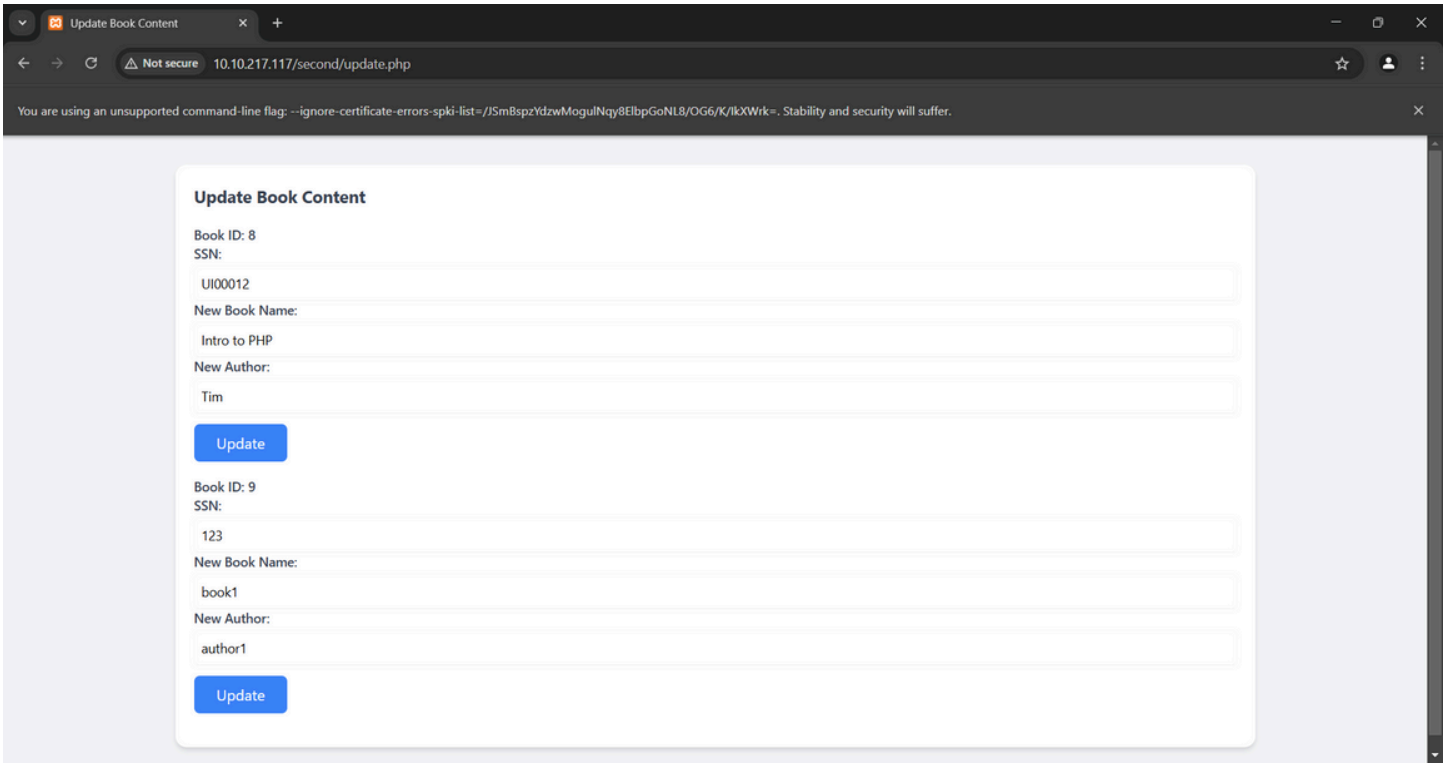
We have this app here with books and stuff



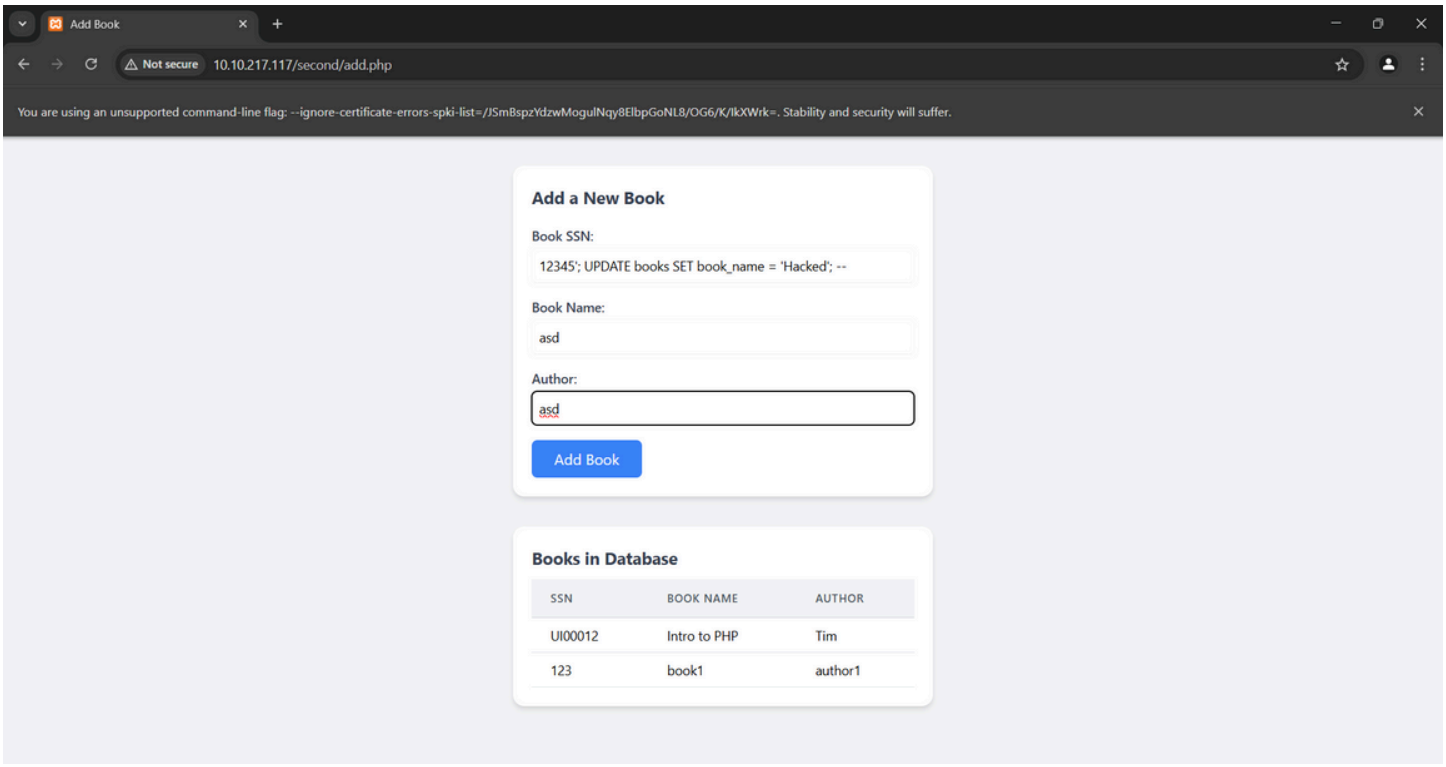
We can add books here, and also we can access to update.php of the app



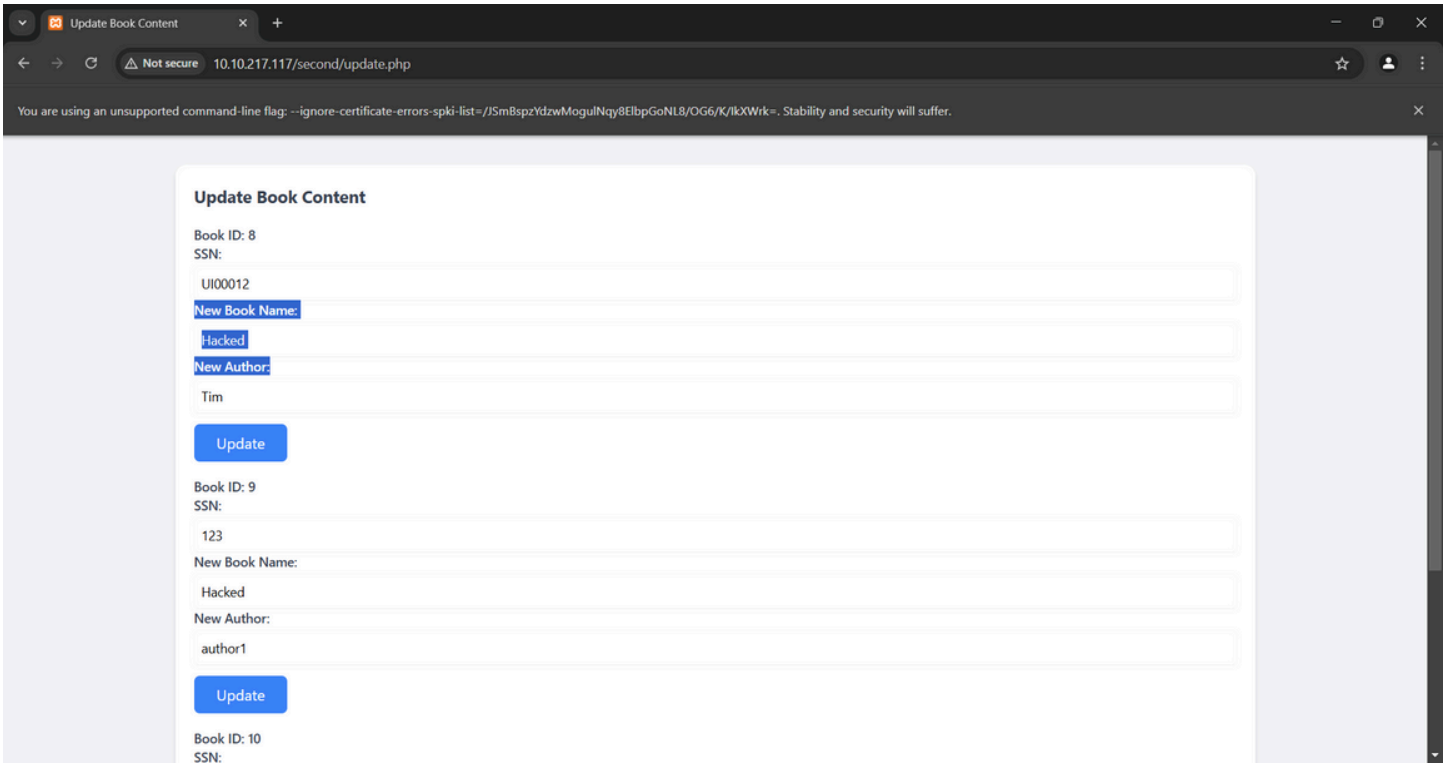
But we can't change anything here



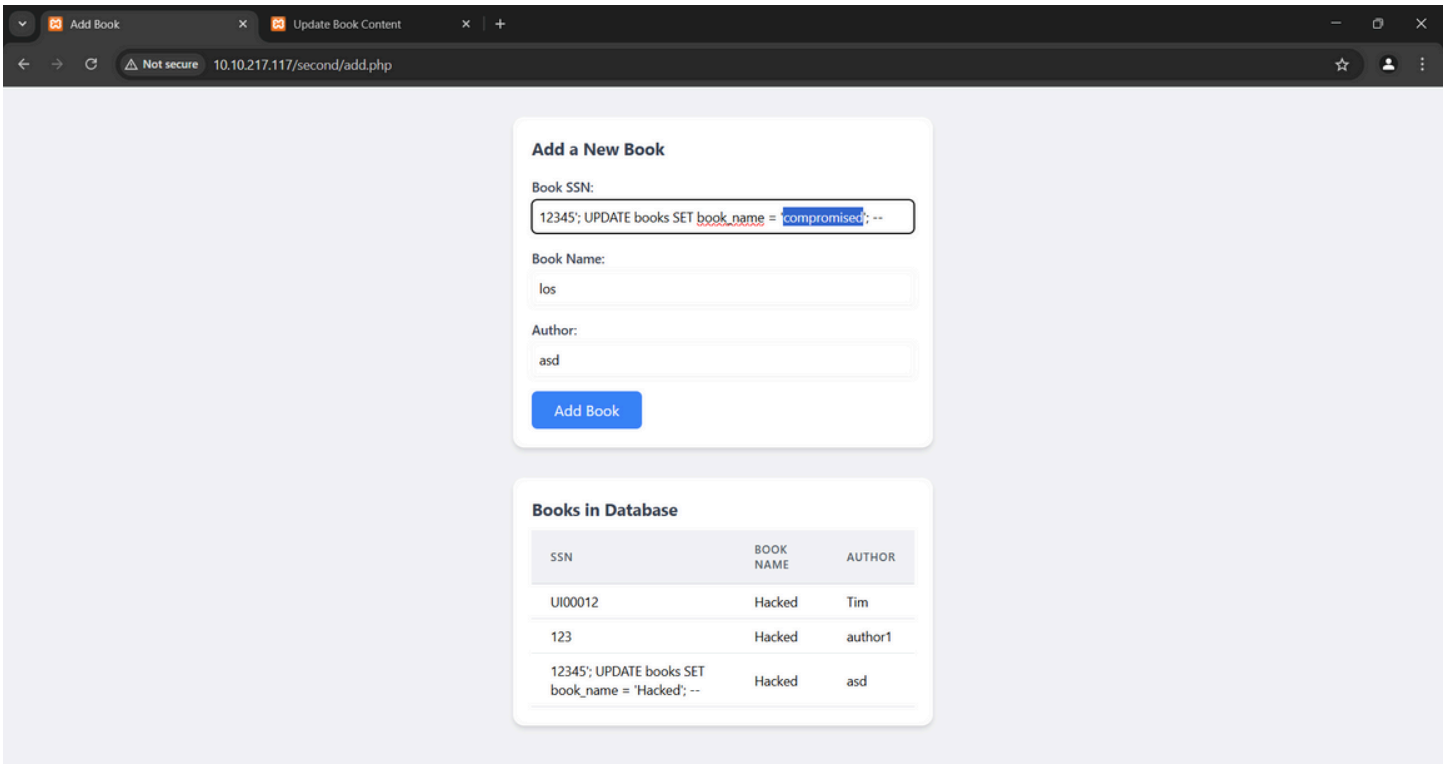
So we'll use the code show in the room



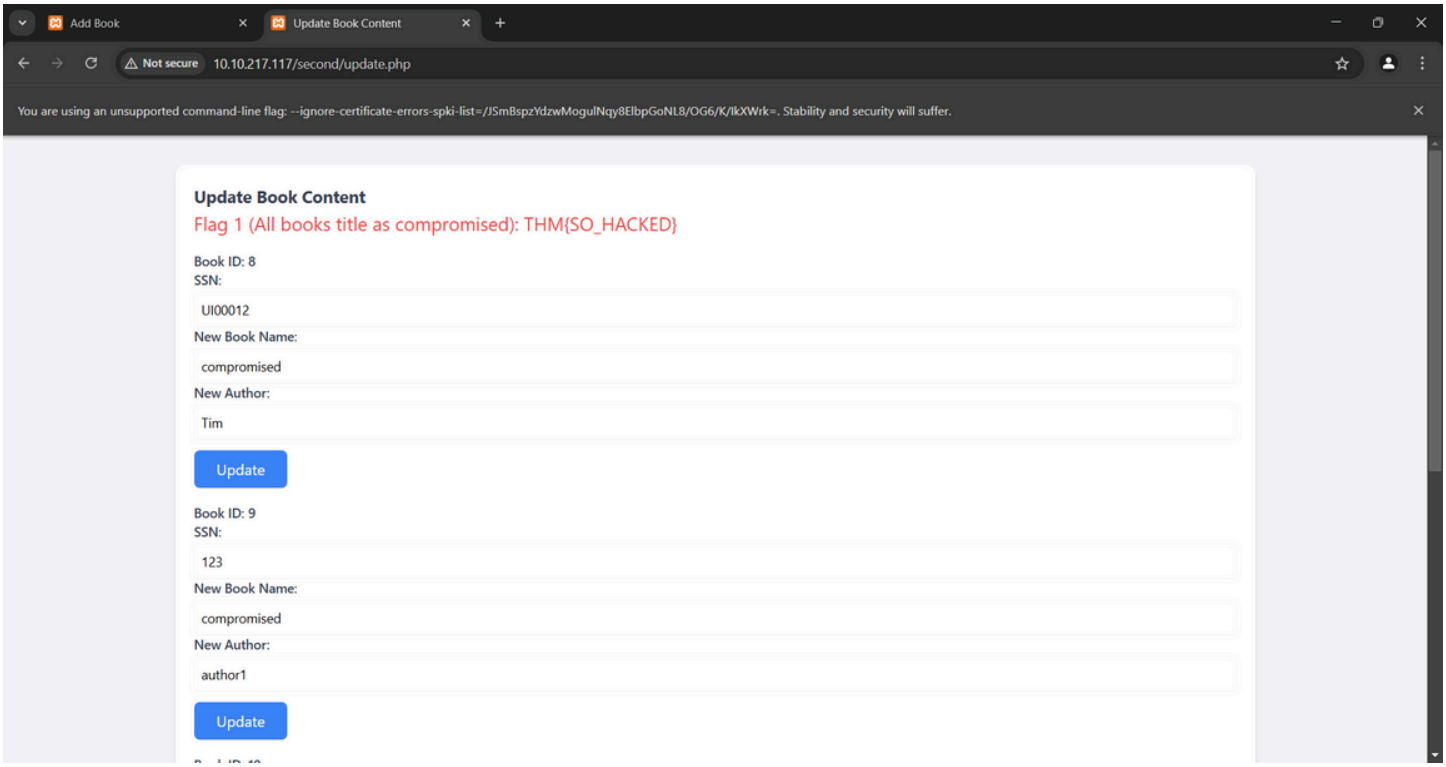
And we see it works perfectly fine, the titles have been updated

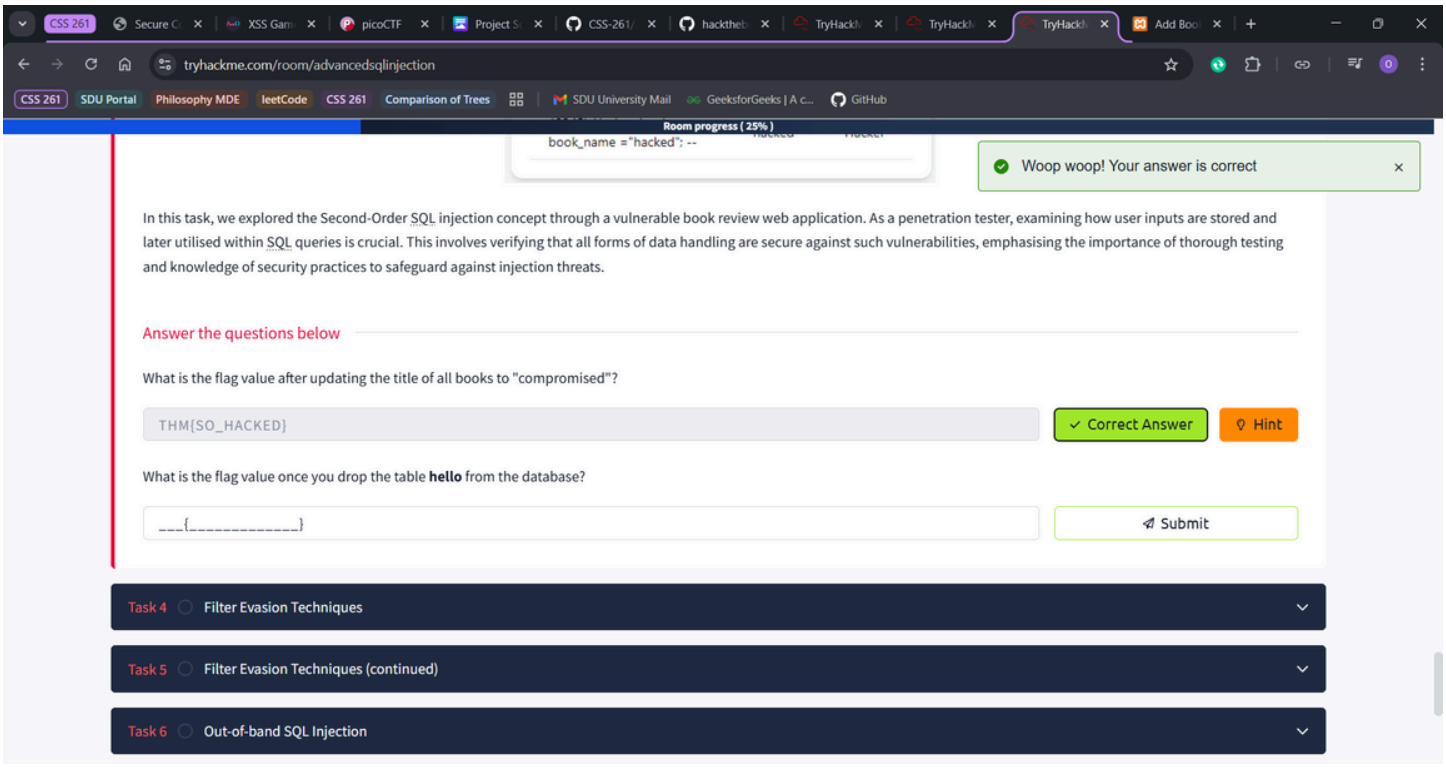


We'll also try these queries

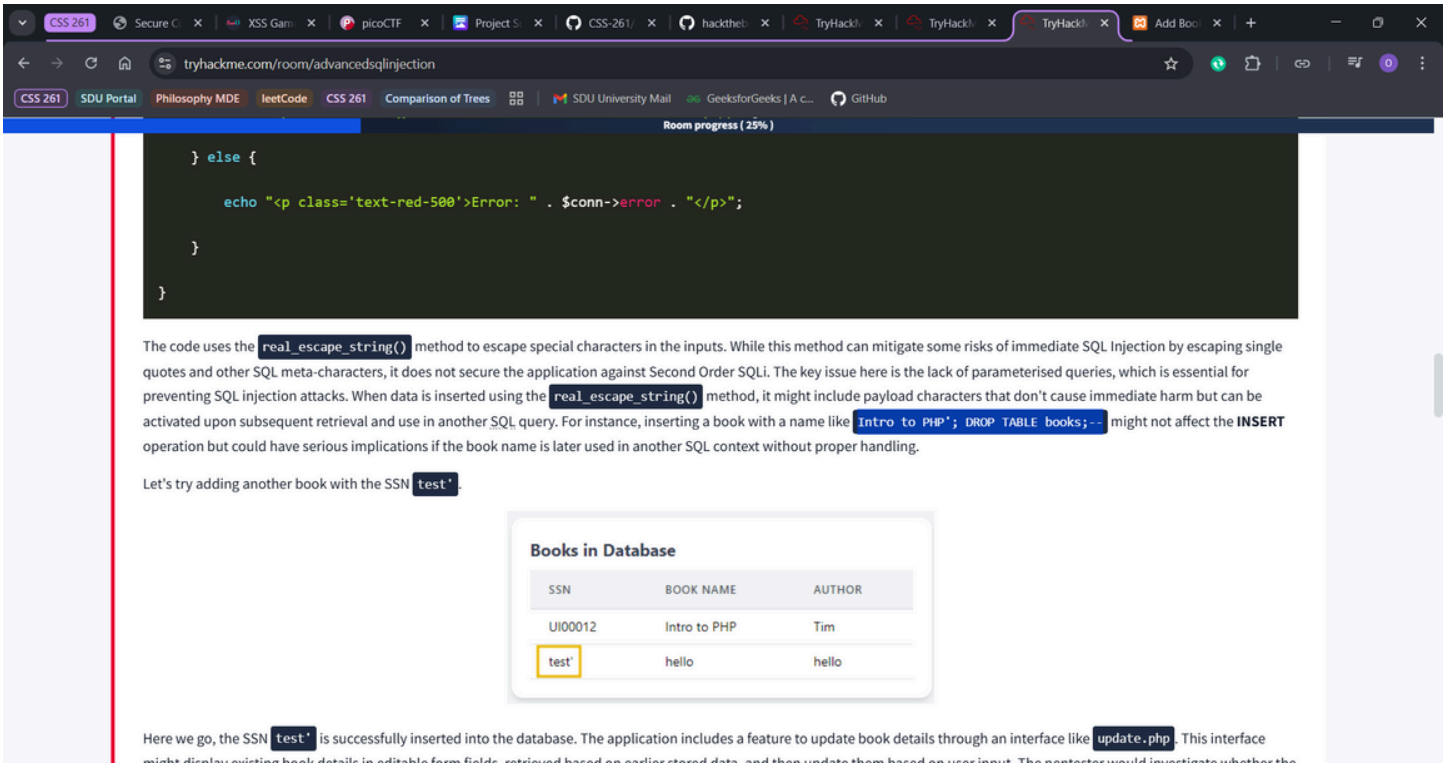


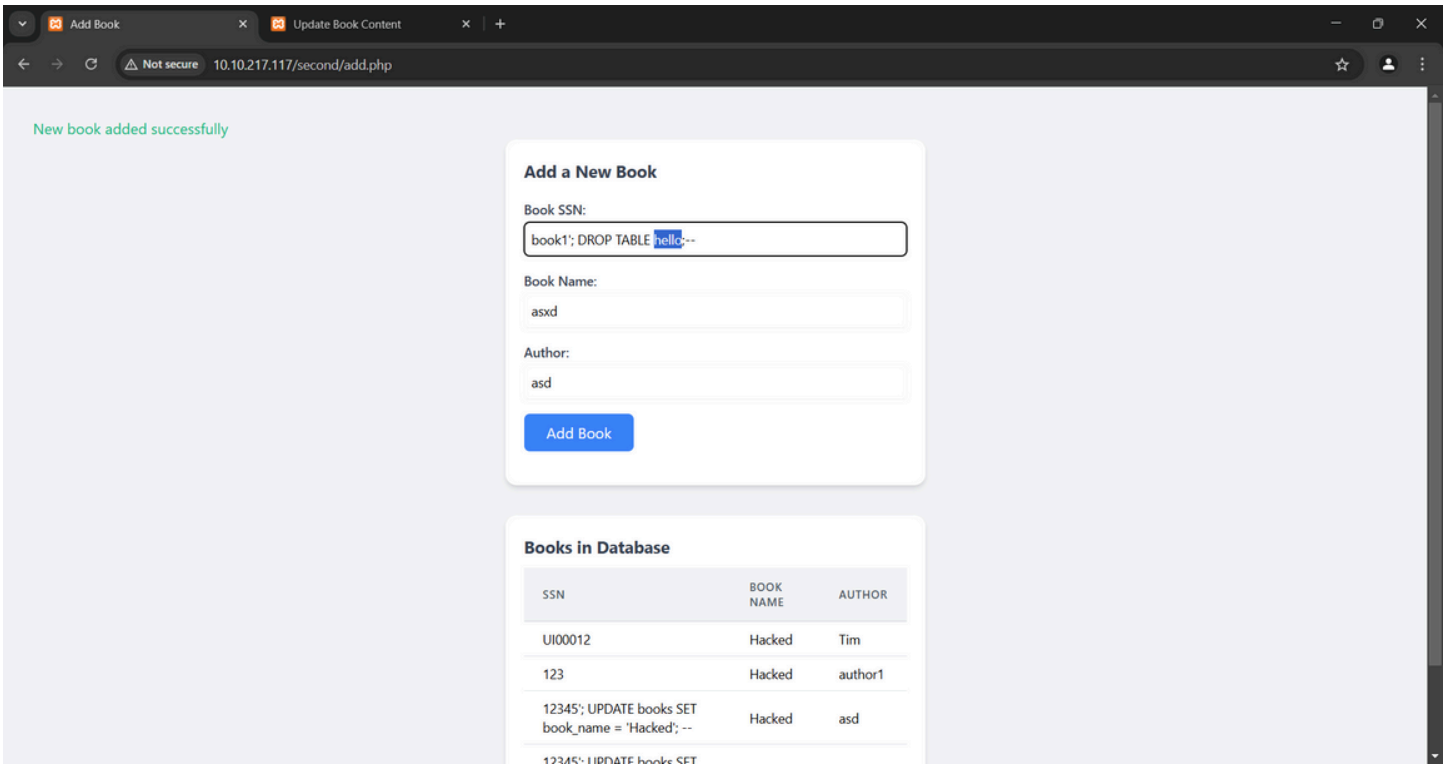
And here is our first flag:



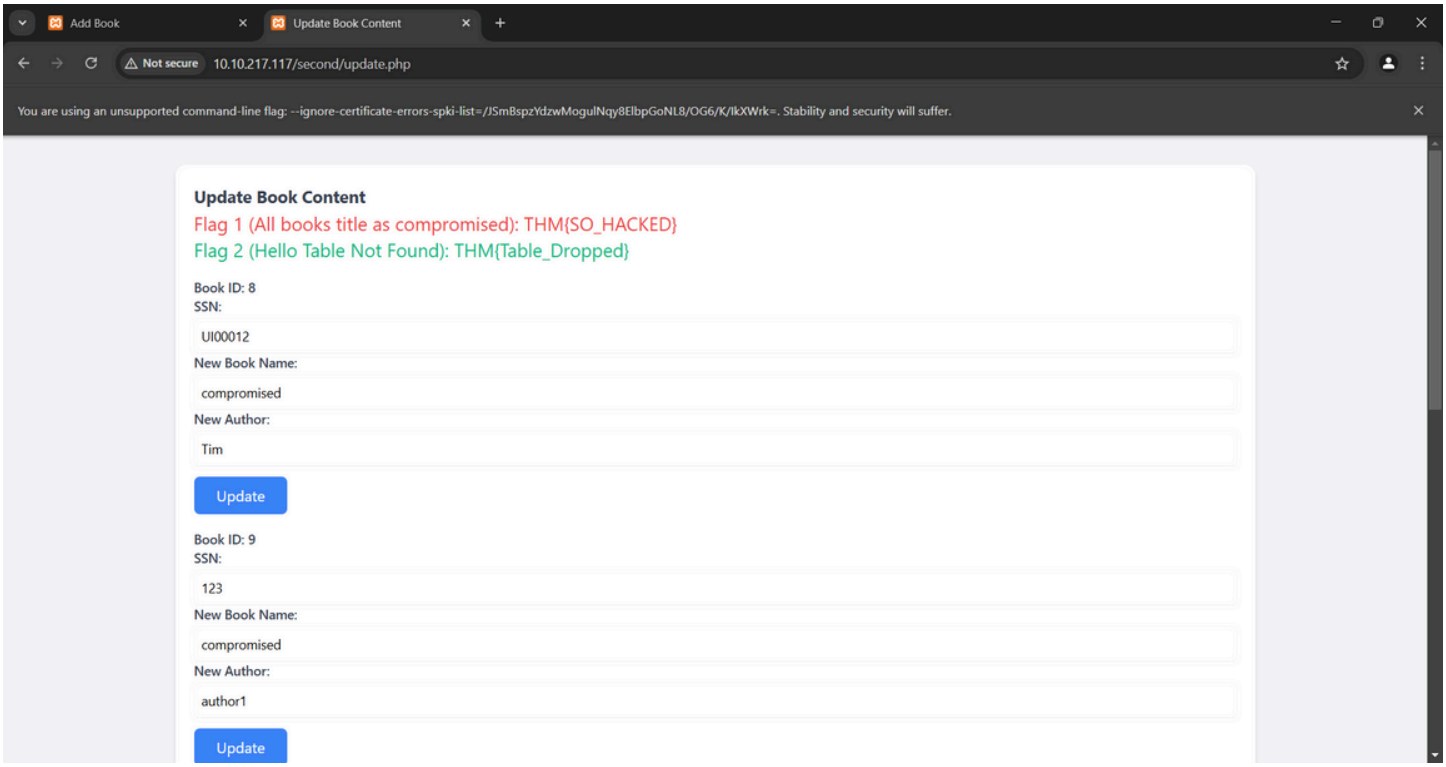


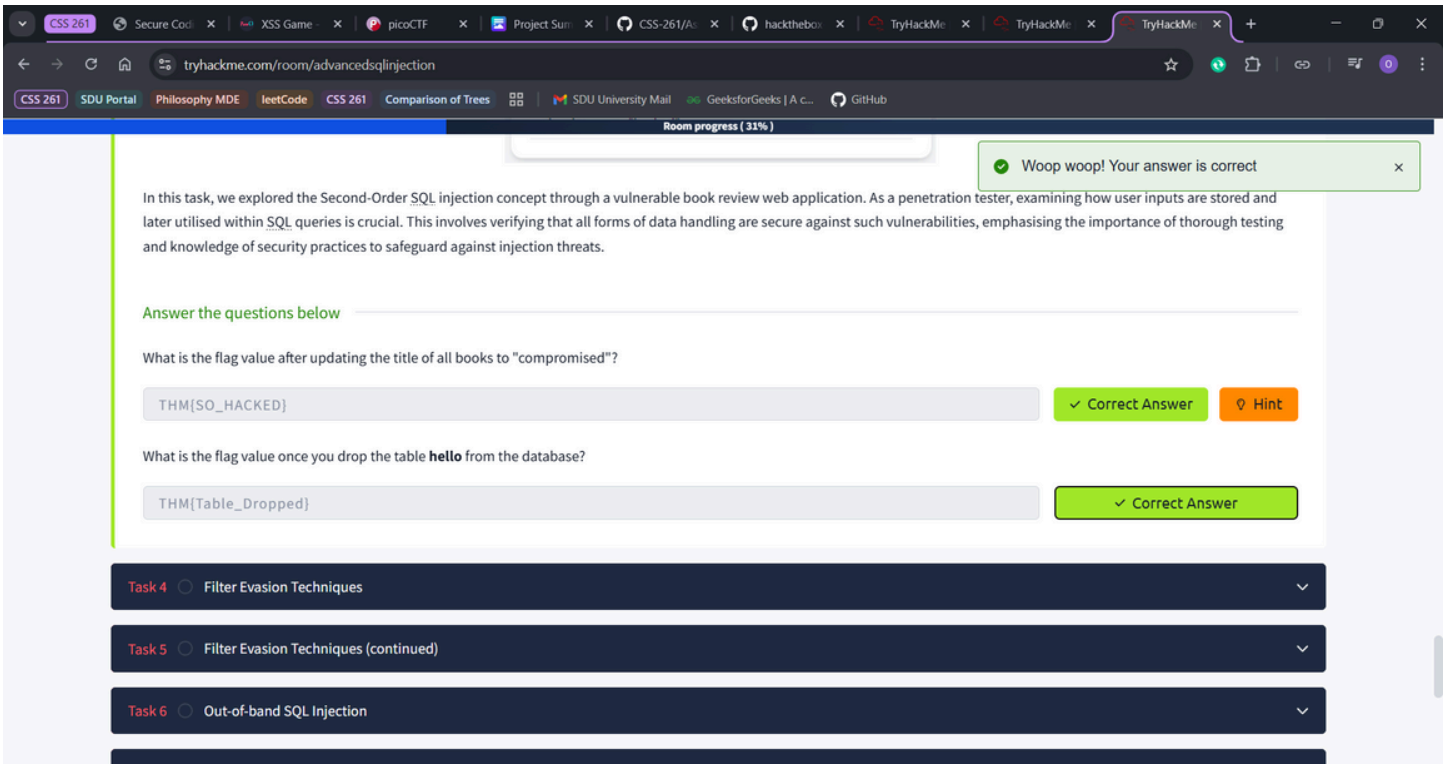
Next, we'll drop book using the query given in the task



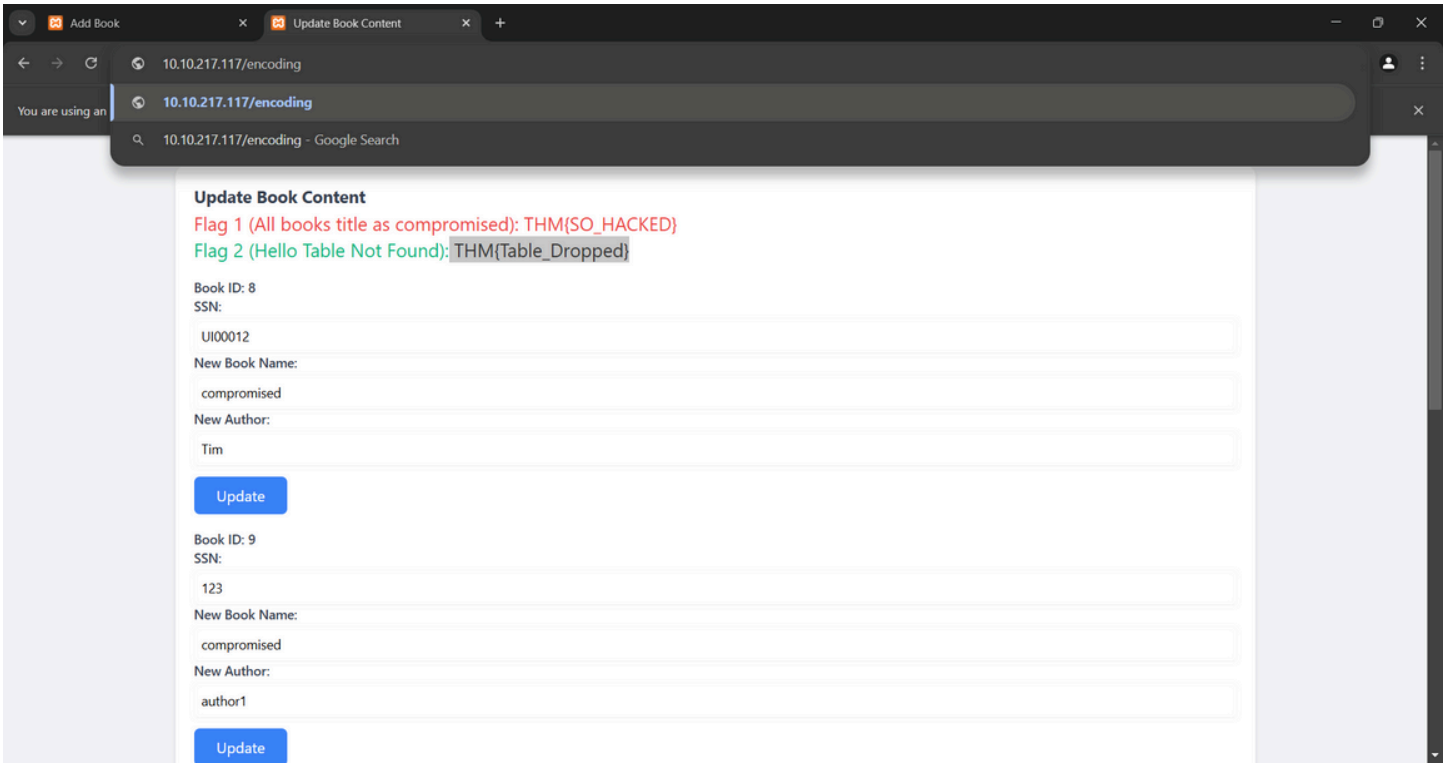


There we have it!

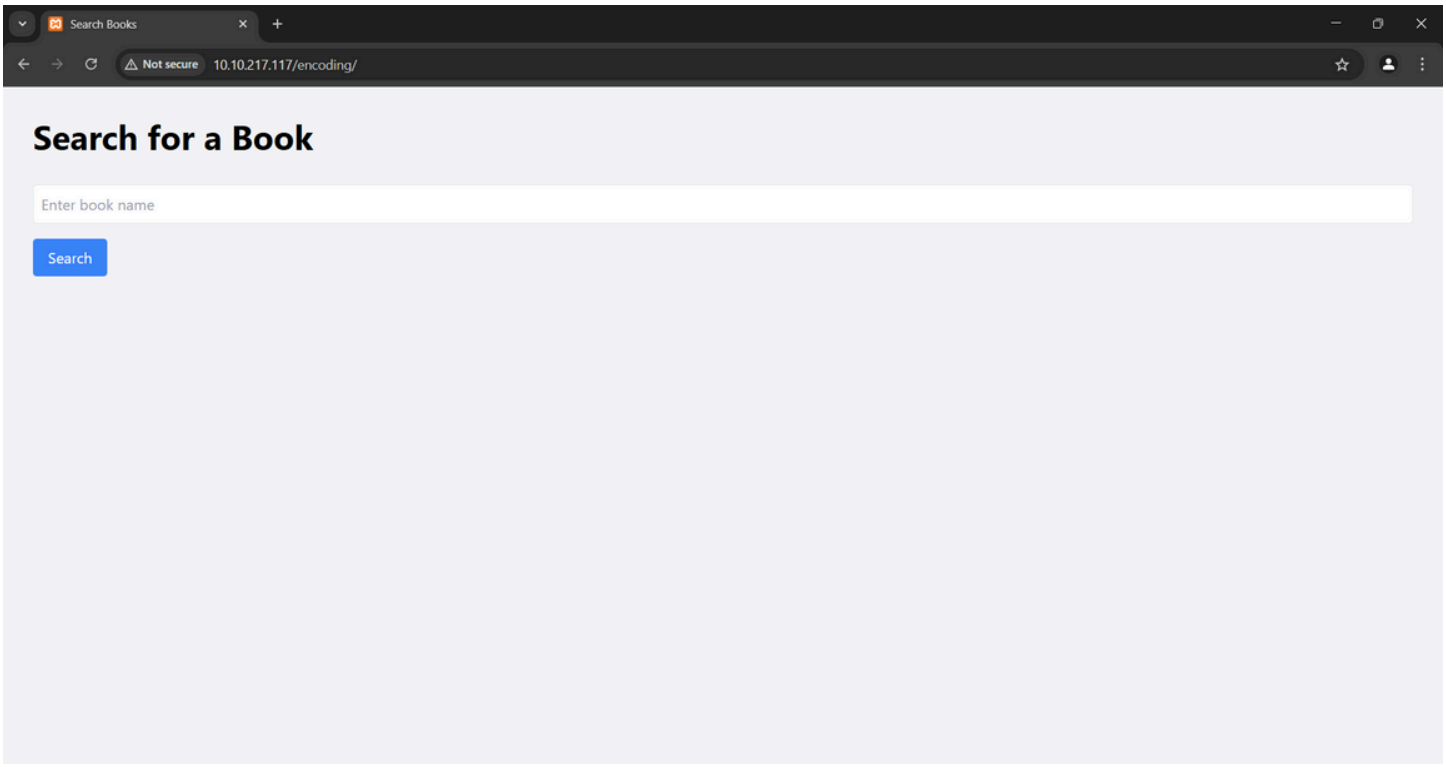




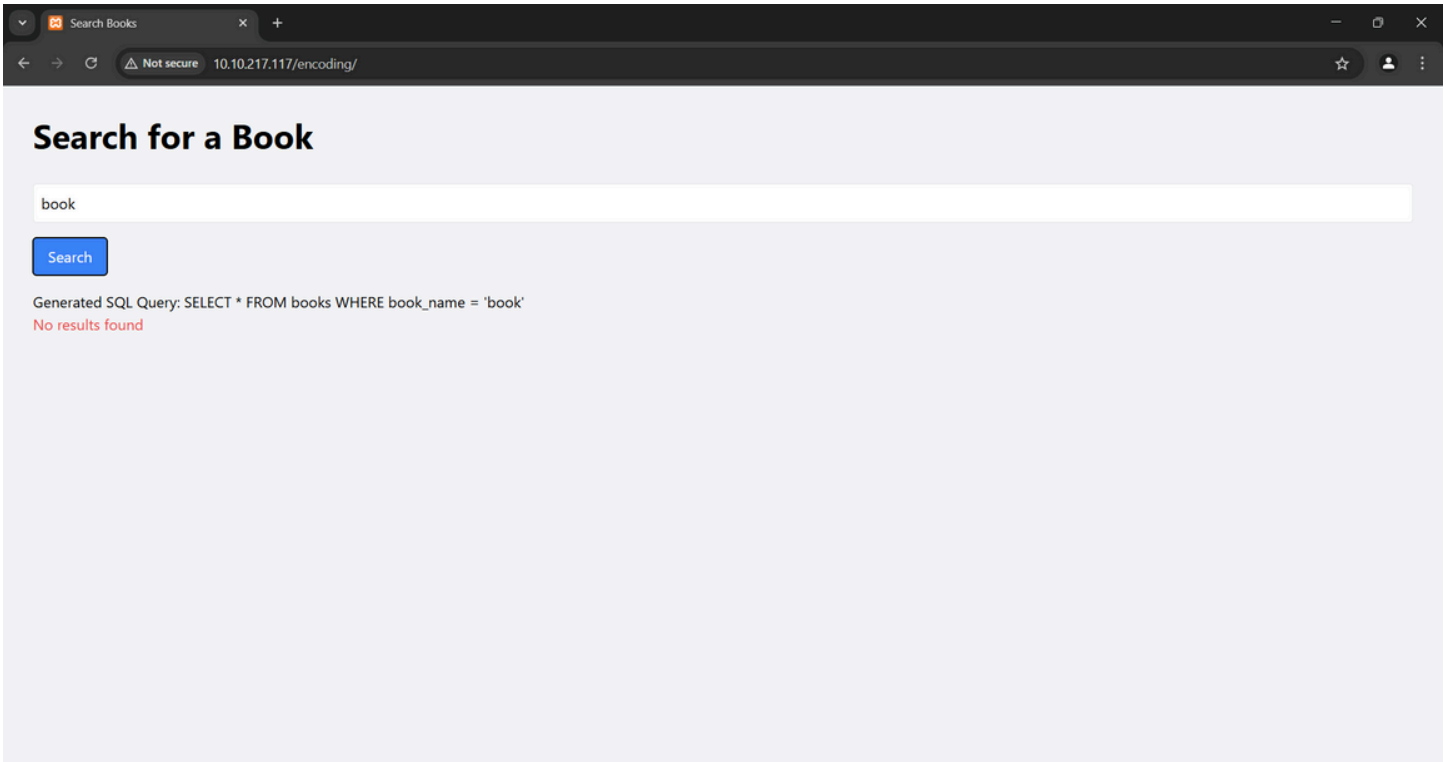
Next, we need to type this

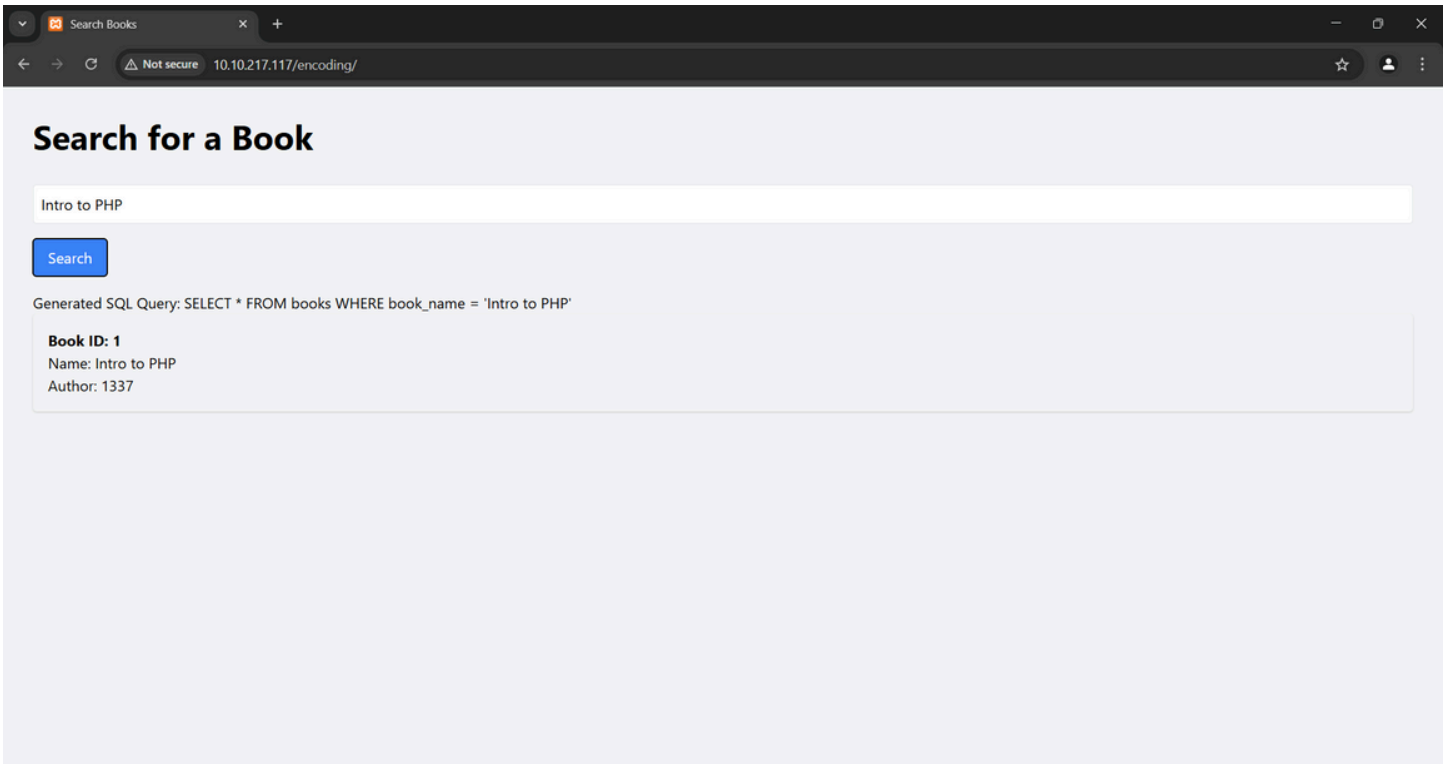


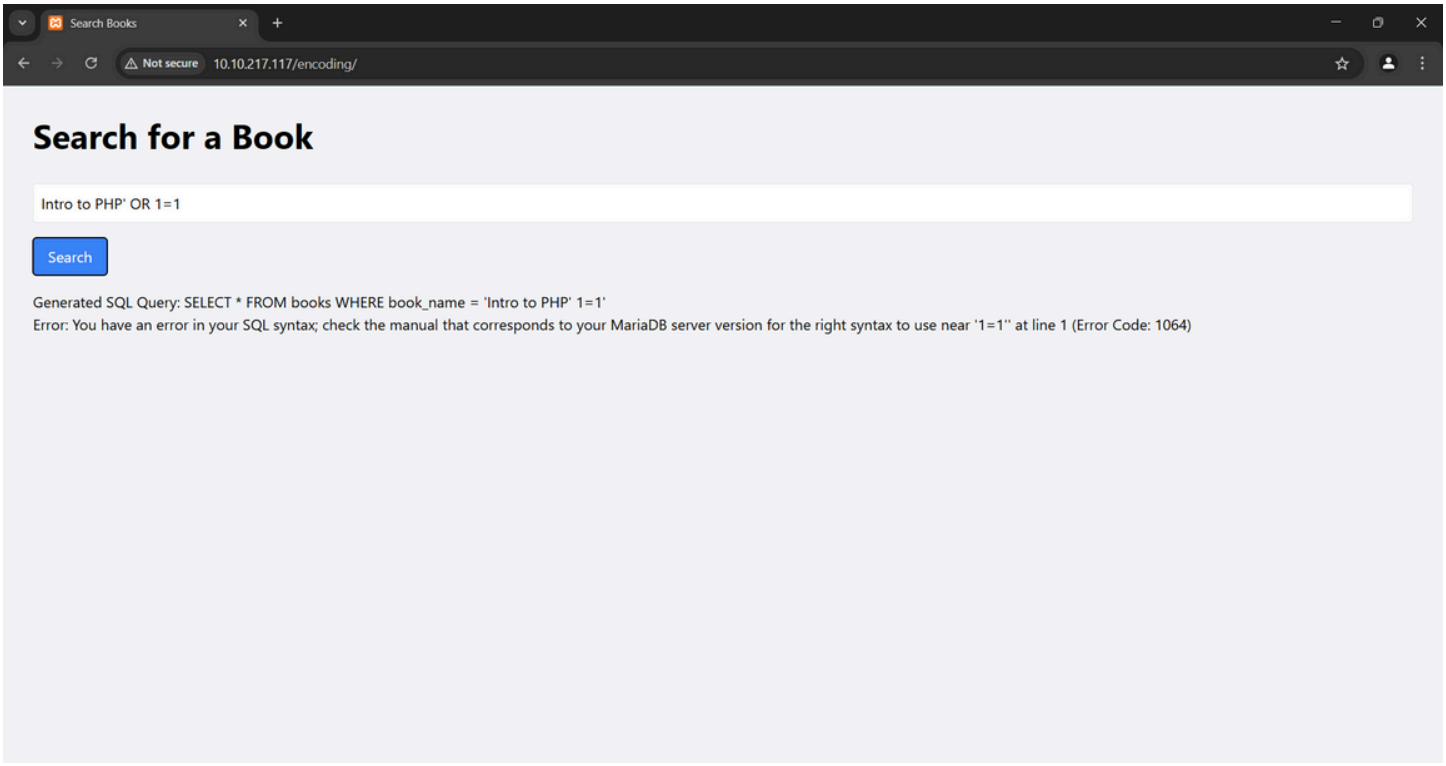
To access to this search bar



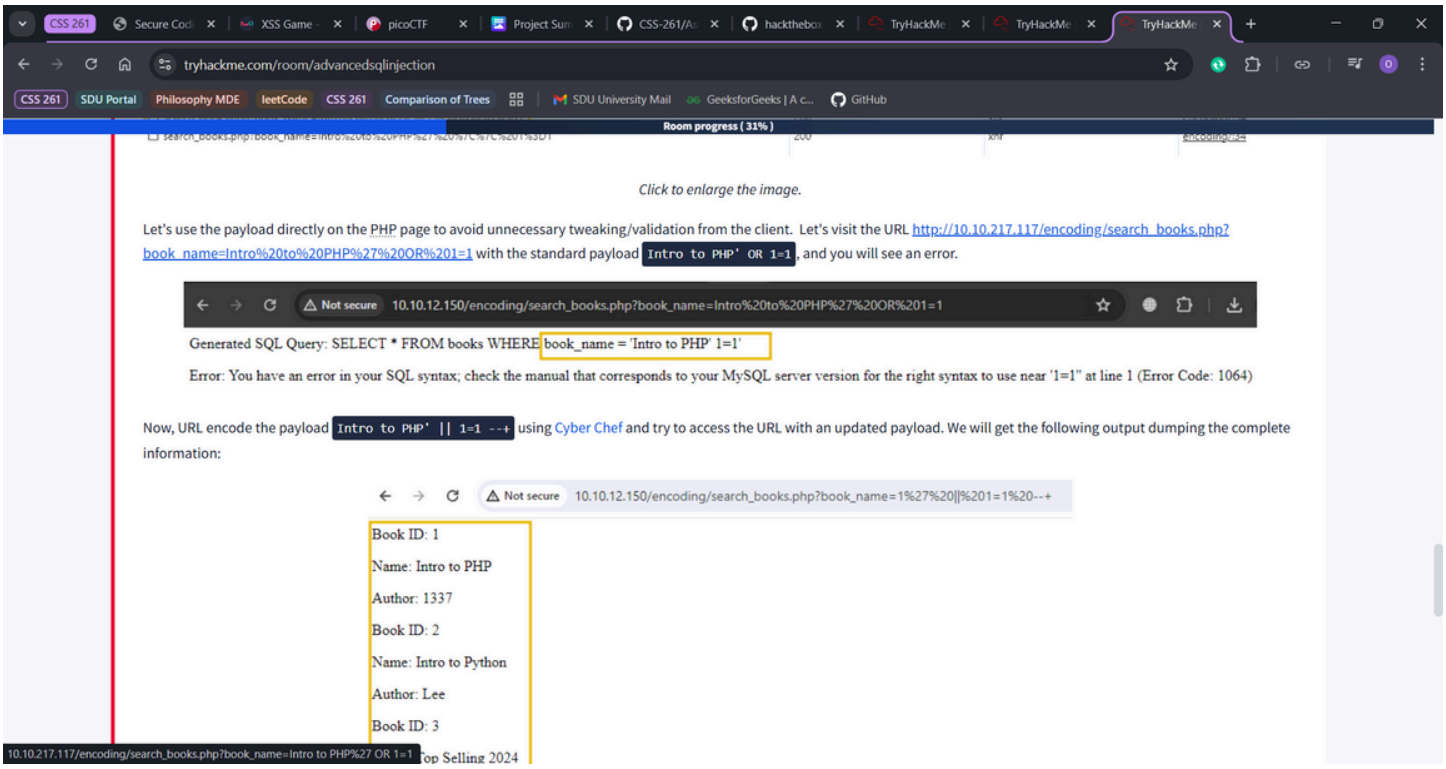
I tested out some things here:



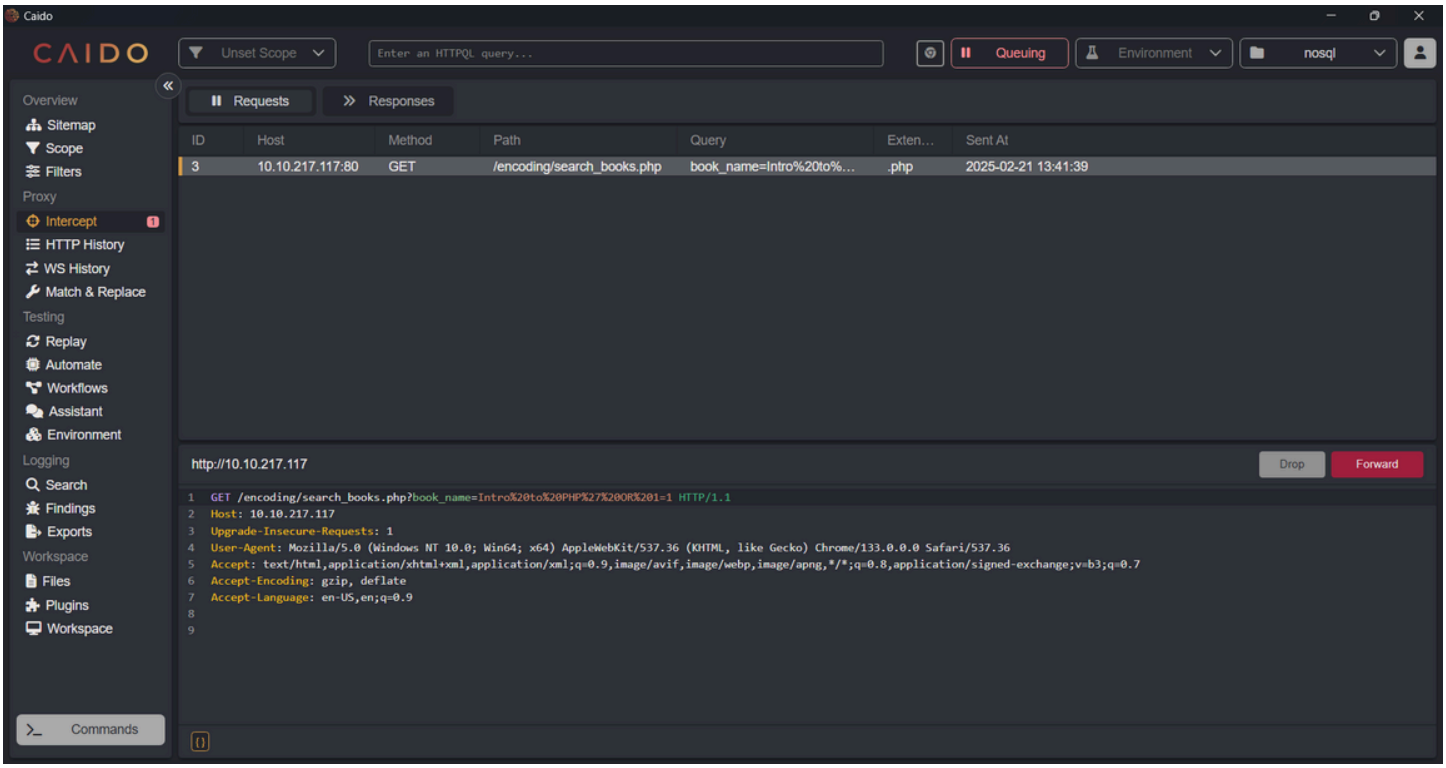




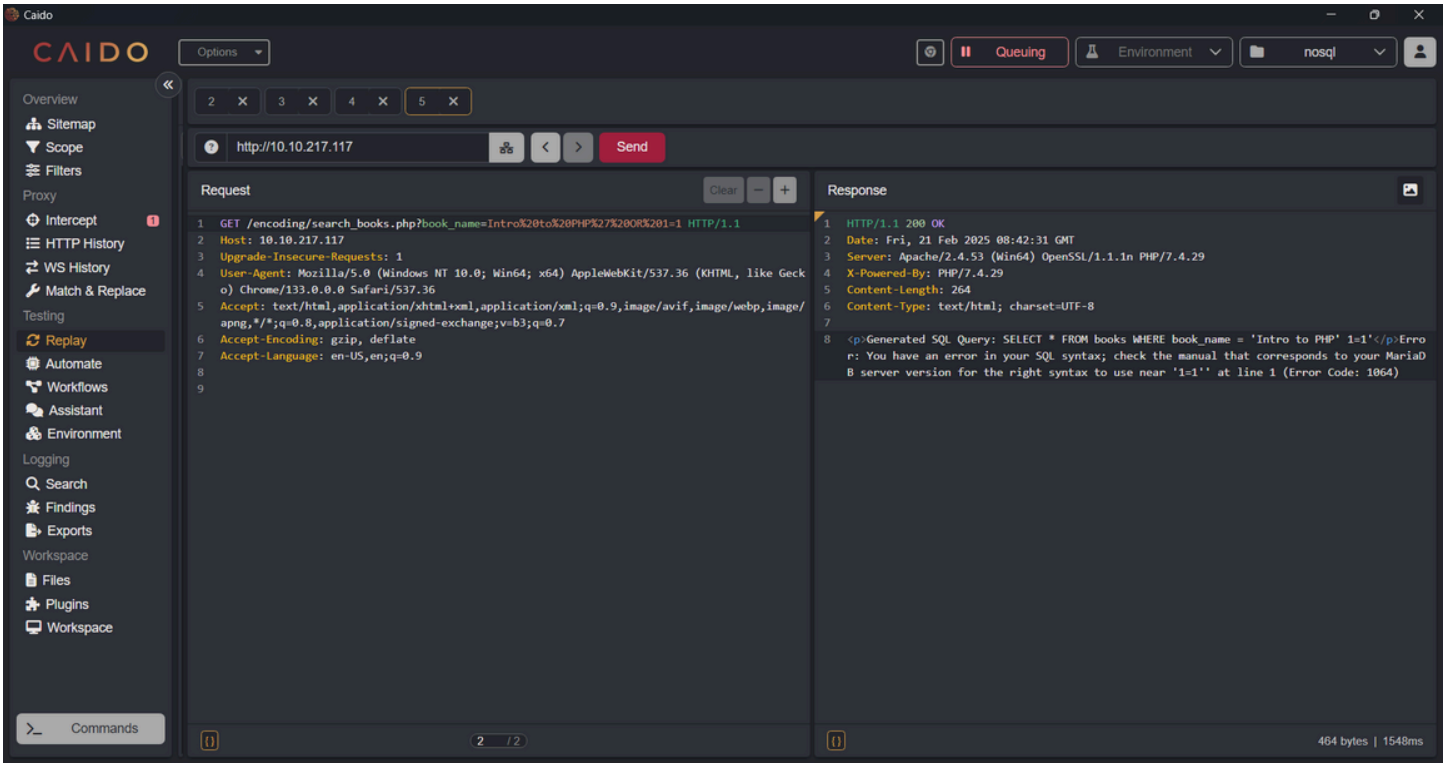
So we will use this query next



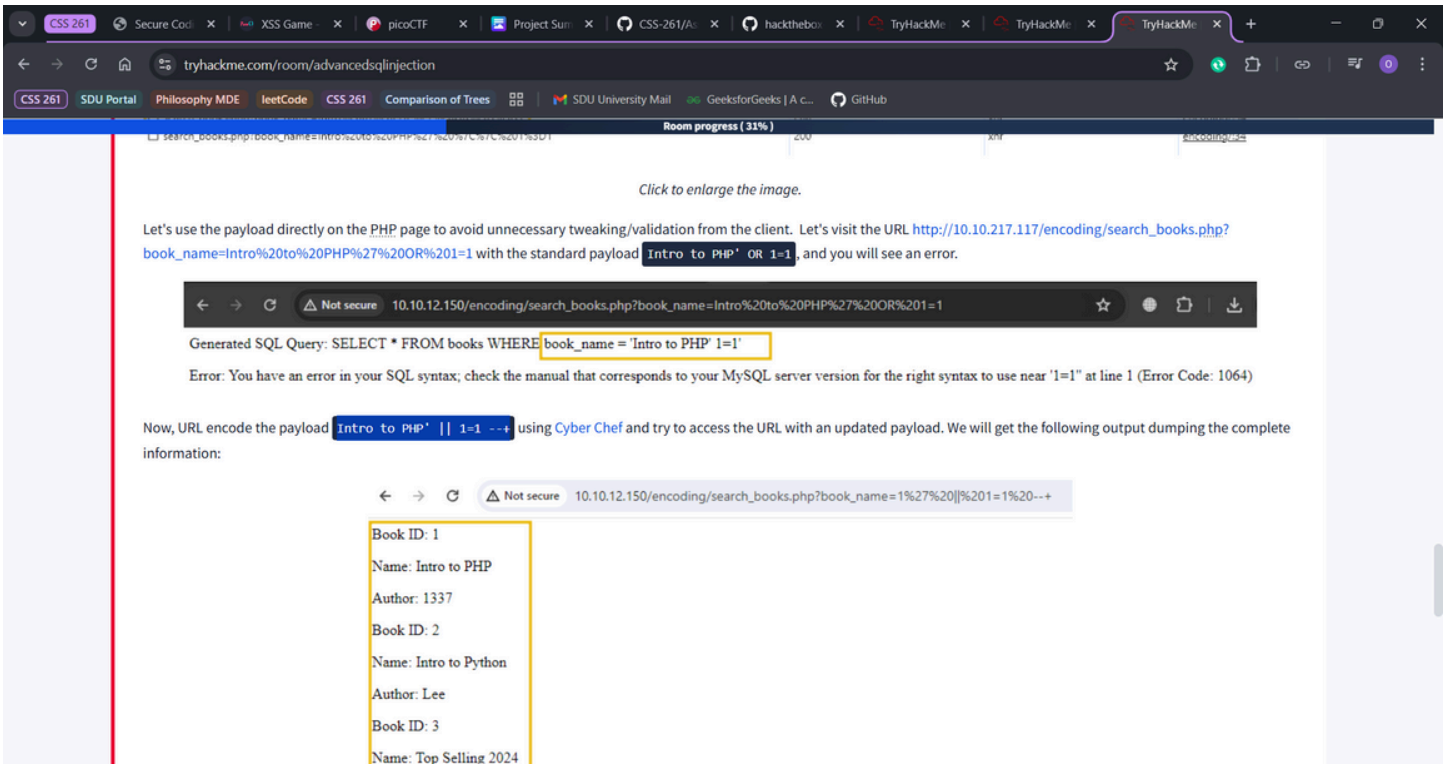
By doing so, we go to the Caido app



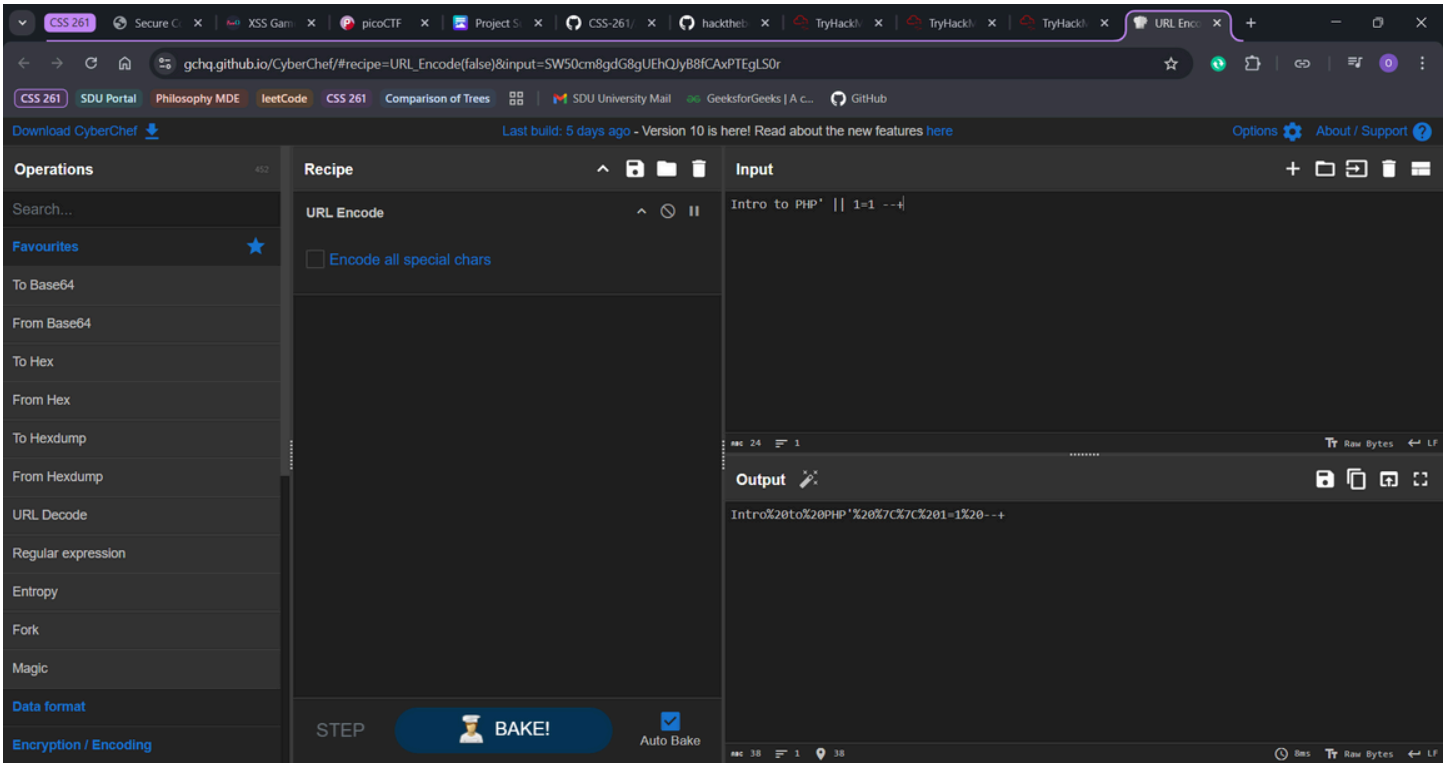
To try out some more requests



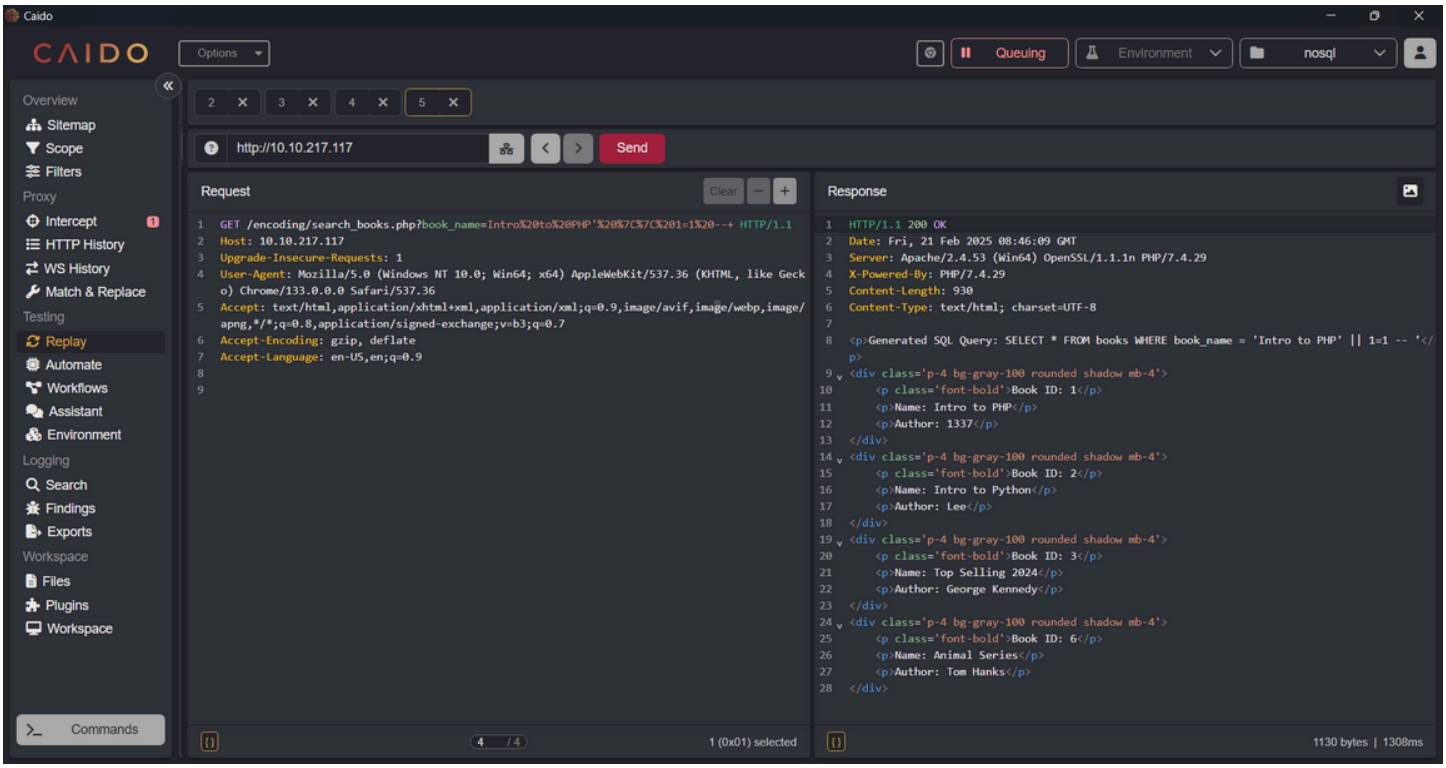
Next, we do as it says in the task



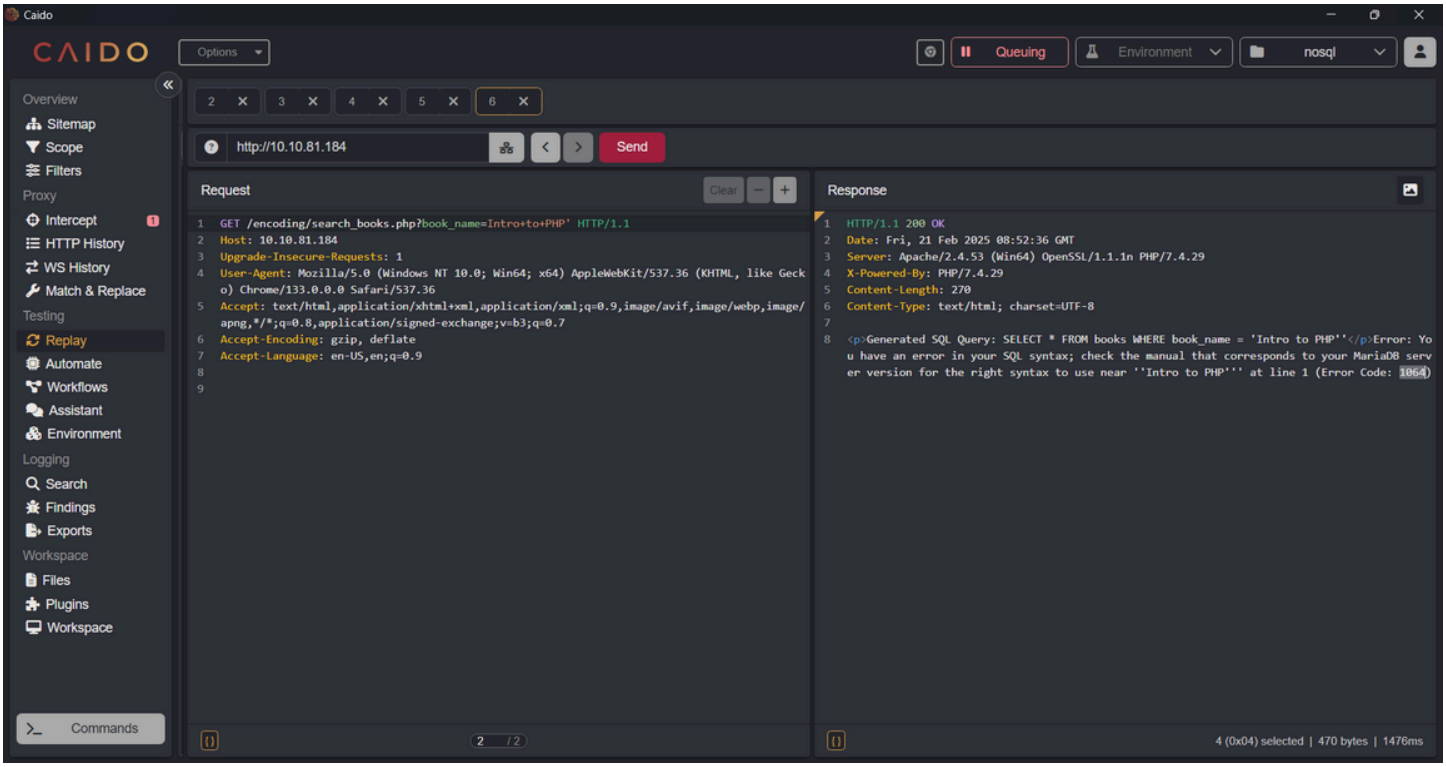
We encode this query to url format in CyberChef

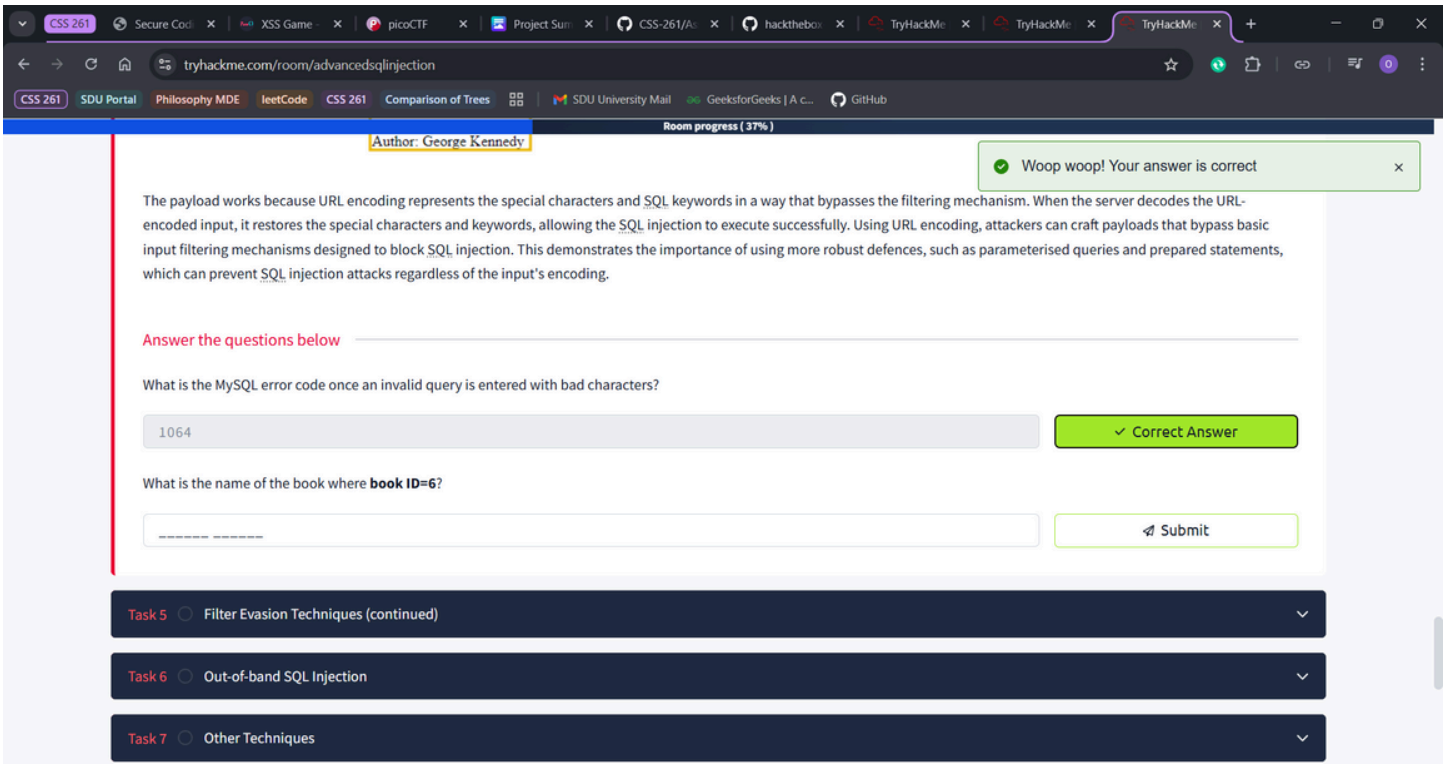


And paste it here:

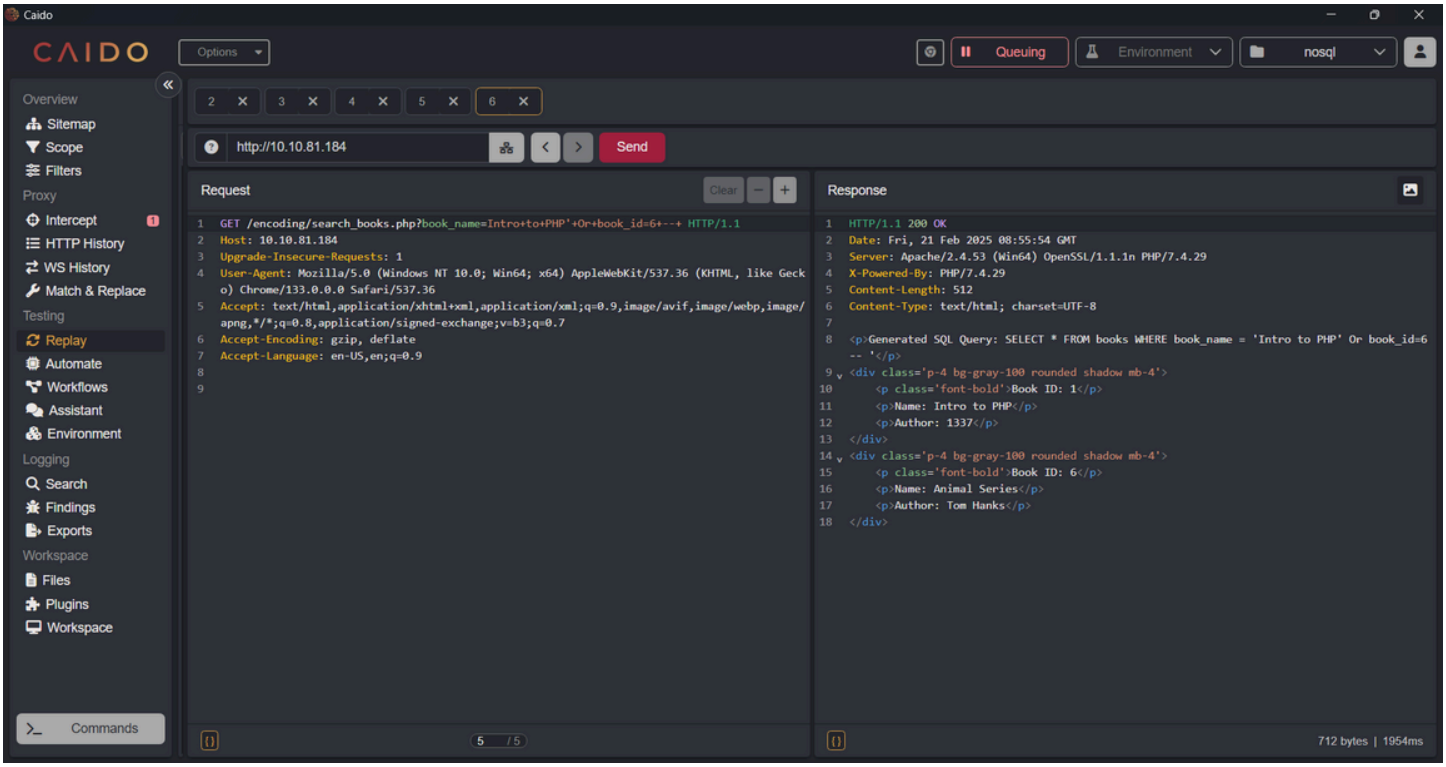


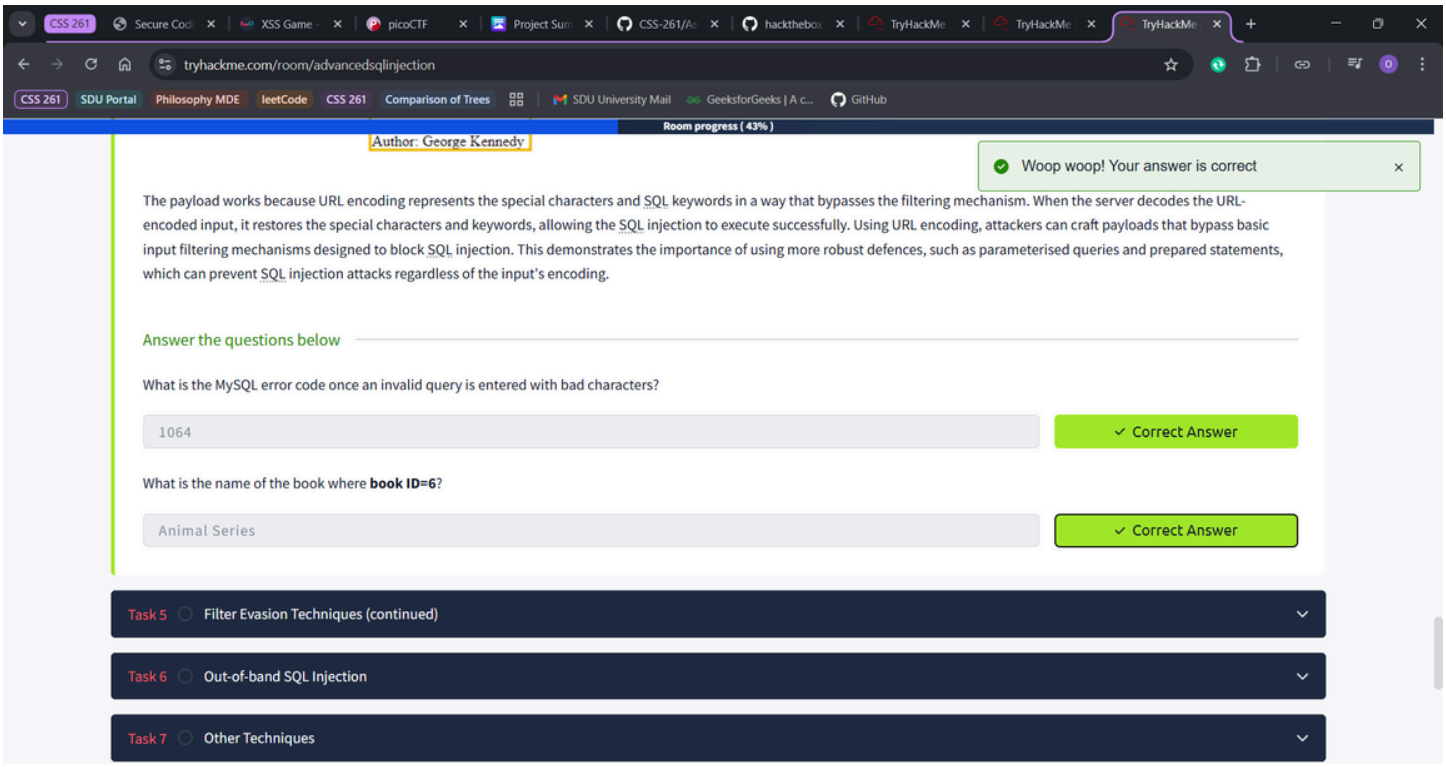
And we see it works perfectly fine. So we find our needed error digits



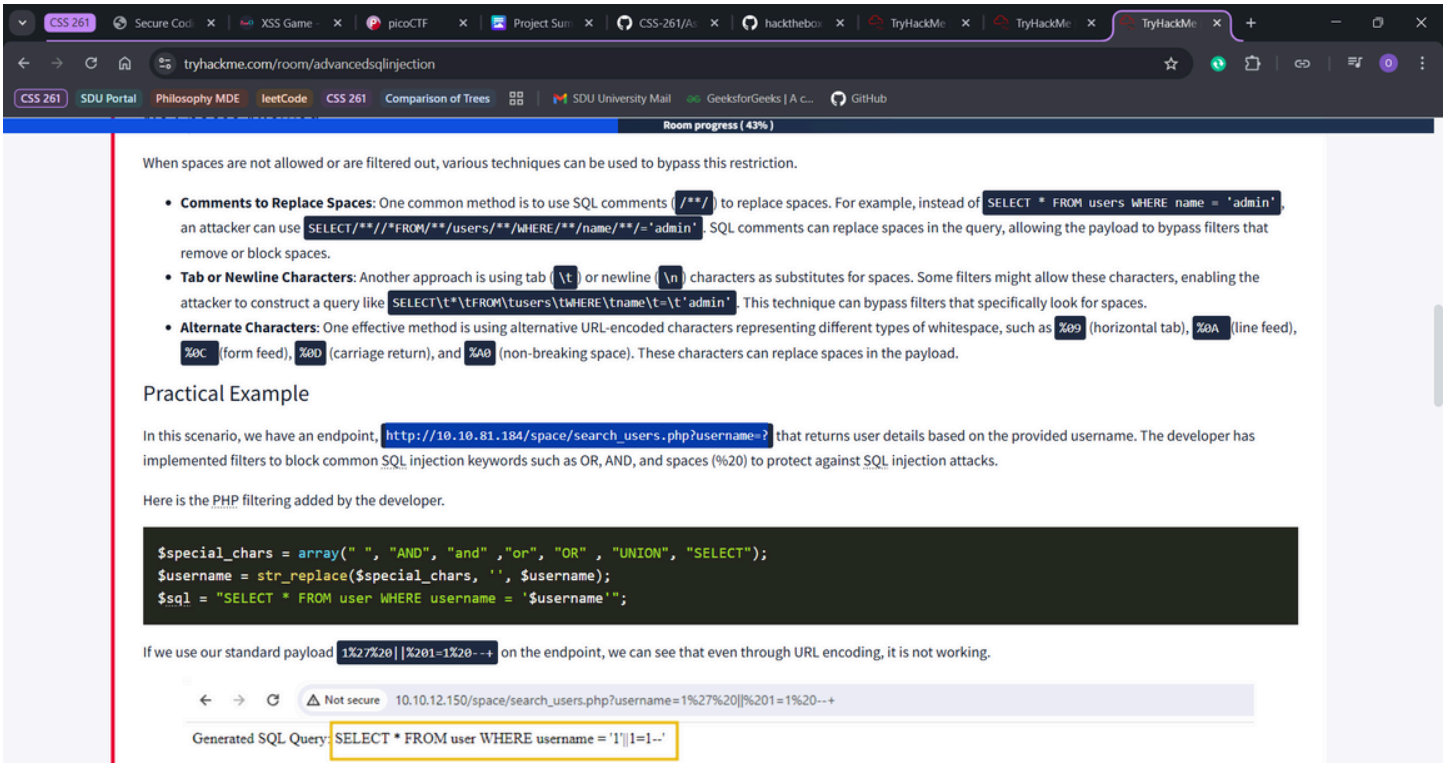


And also book title





Next, we go to here:



We see this site, so we'll try to find our next answers to task

Generated SQL Query: SELECT * FROM user WHERE username = '?'

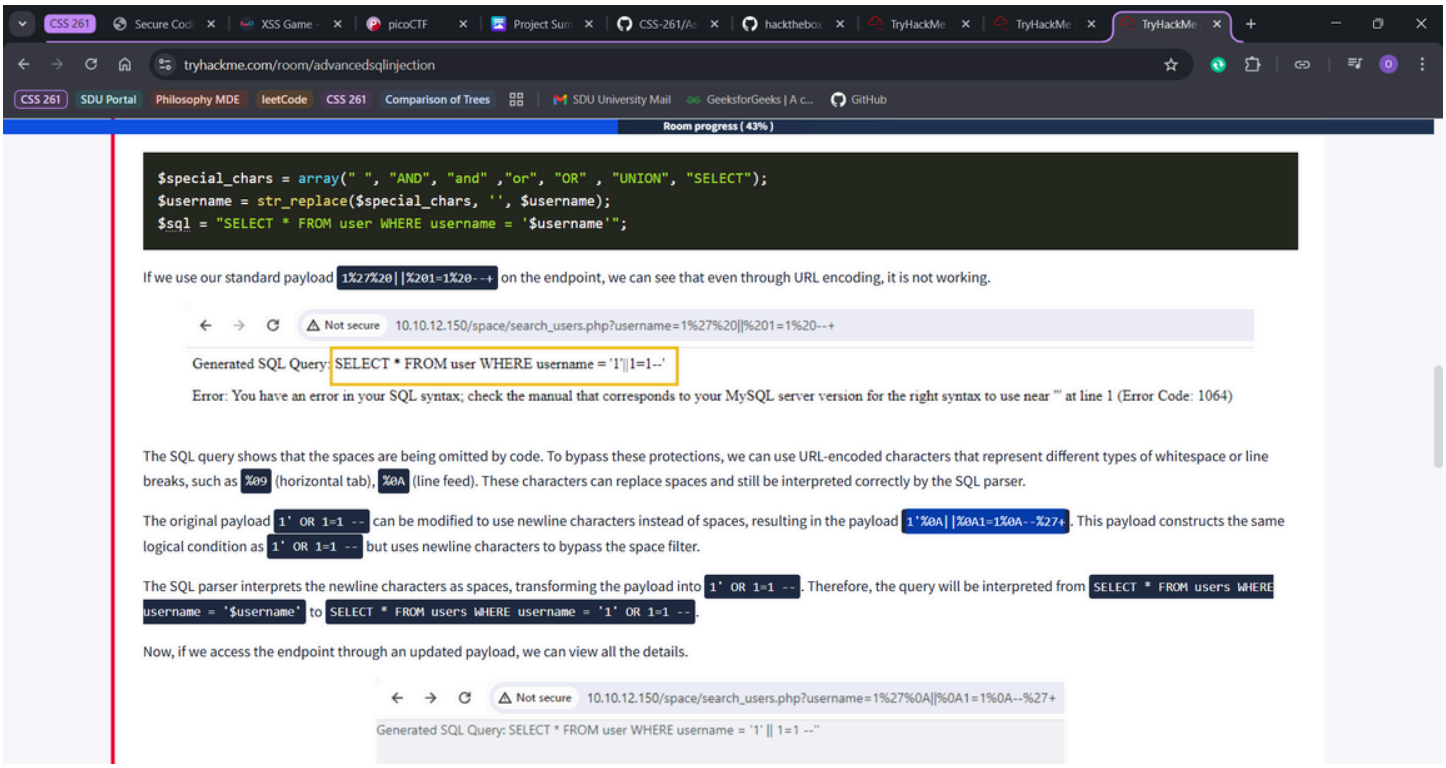
No results found

Try out some more queries here

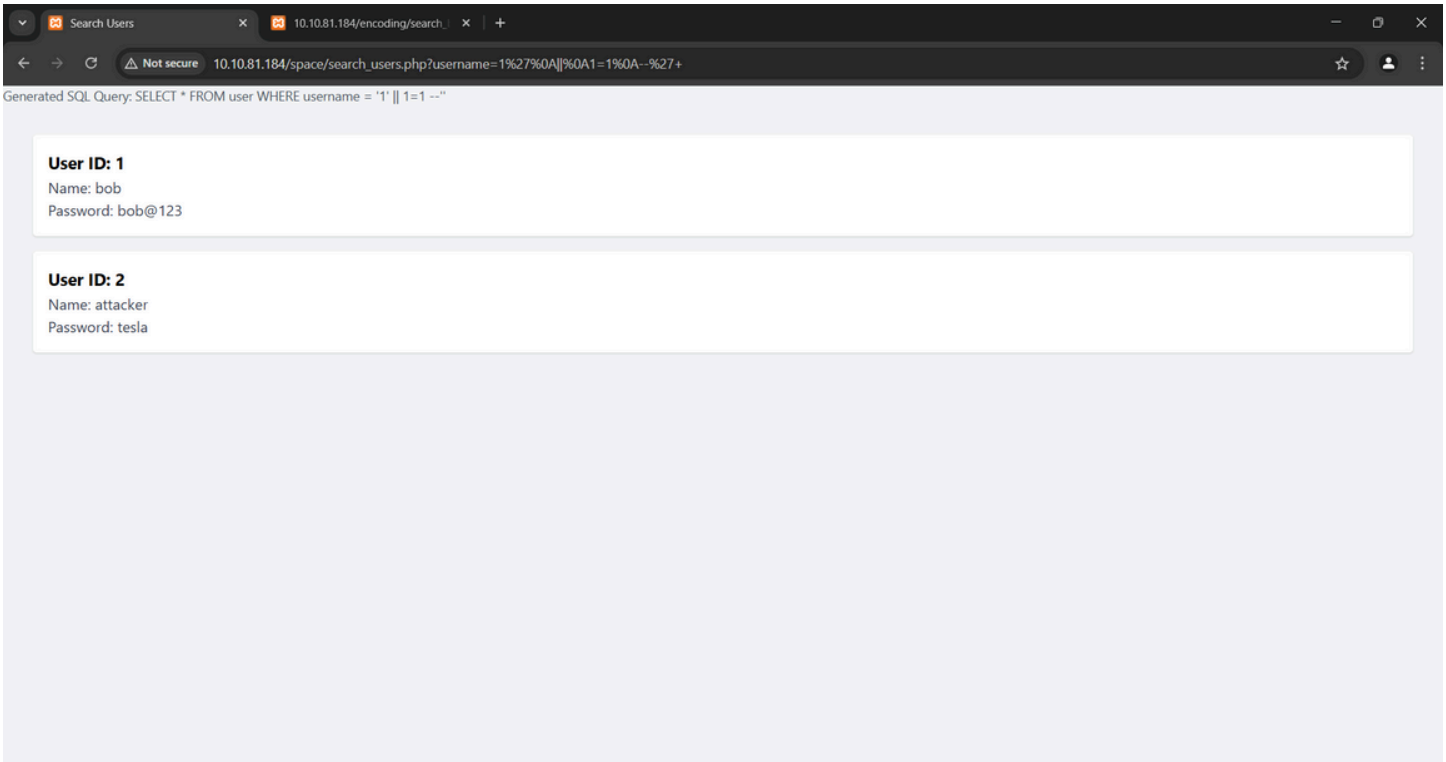
Generated SQL Query: SELECT * FROM user WHERE username = '''

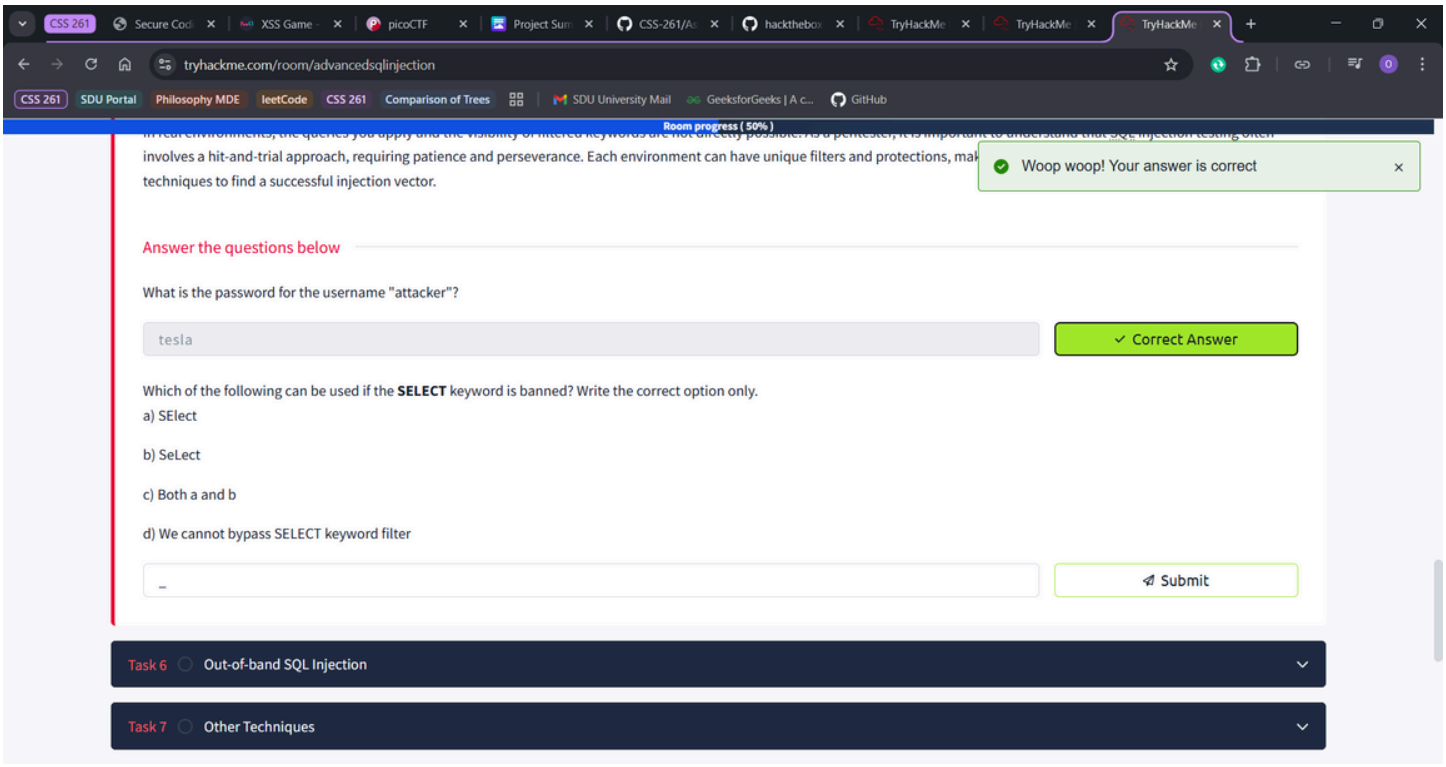
Error: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''''' at line 1 (Error Code: 1064)

And looking at here we see some more information

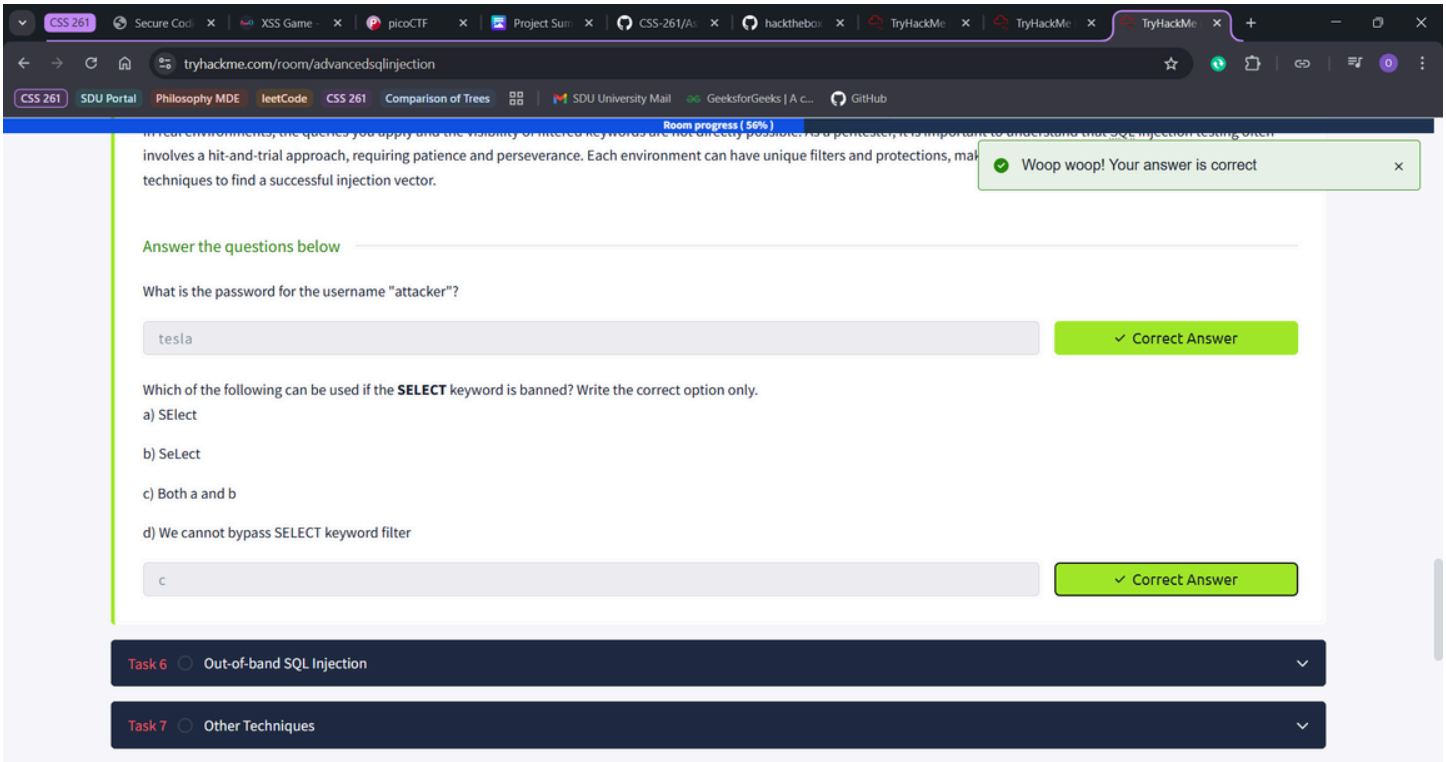


And when we paste it, done! We have the password

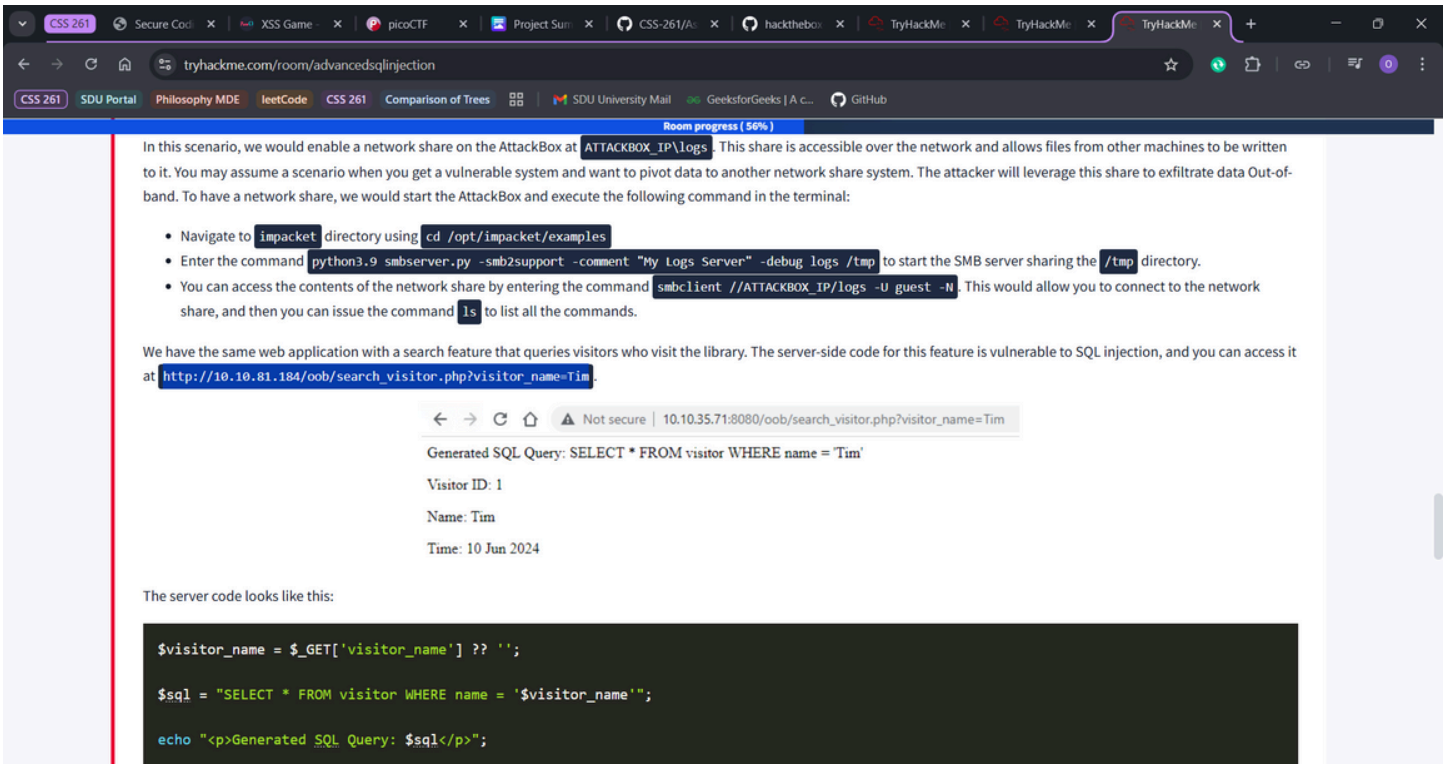




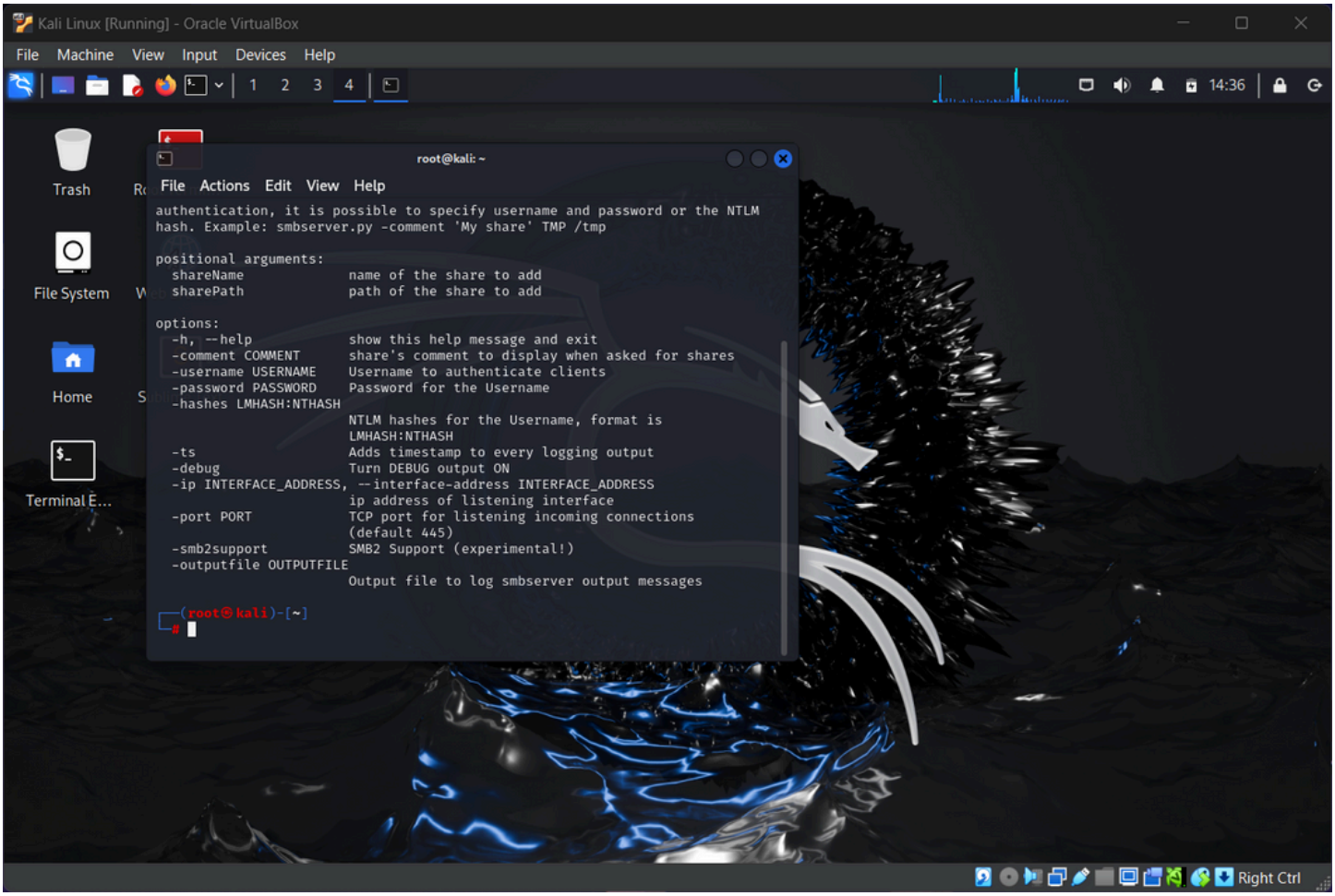
It's answer c, because both will work no matter what



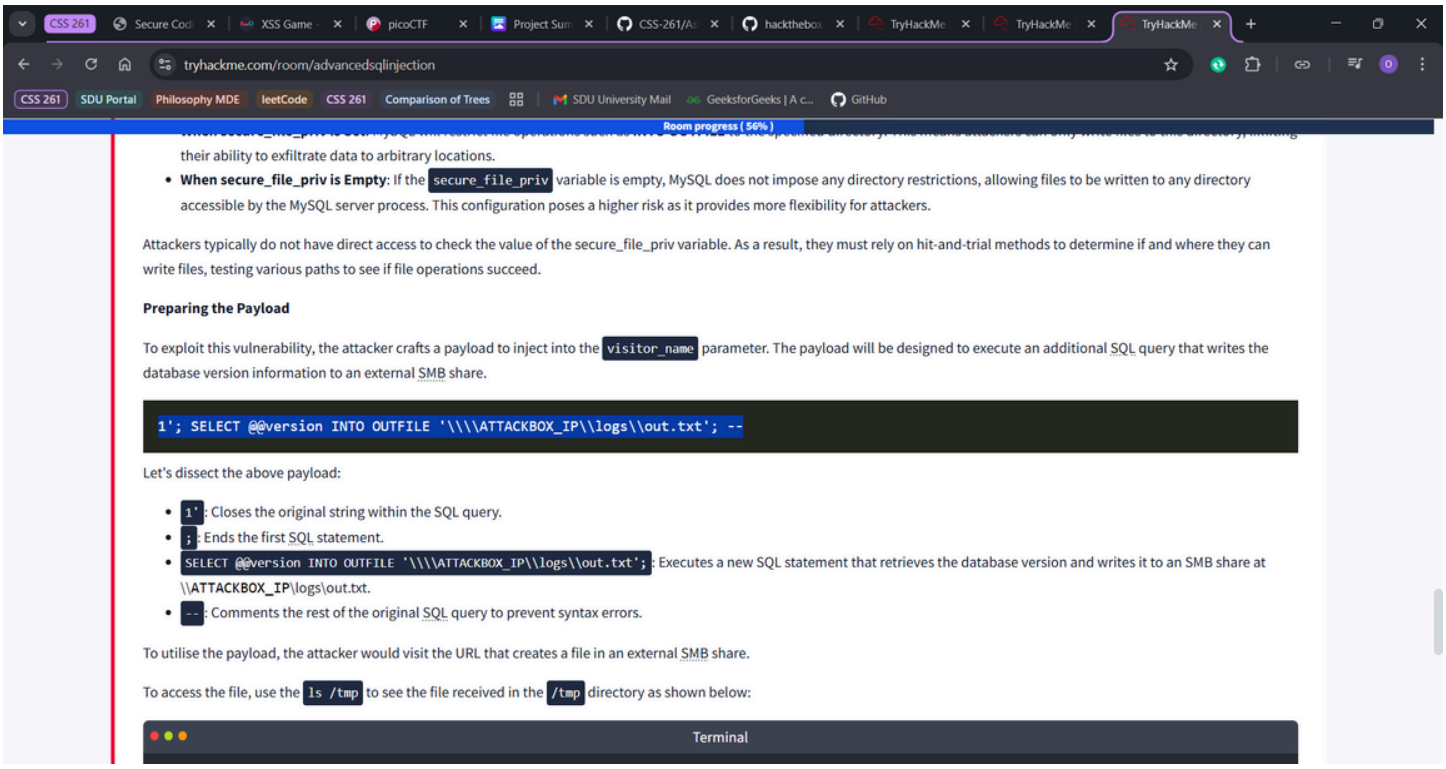
Next, we go here:



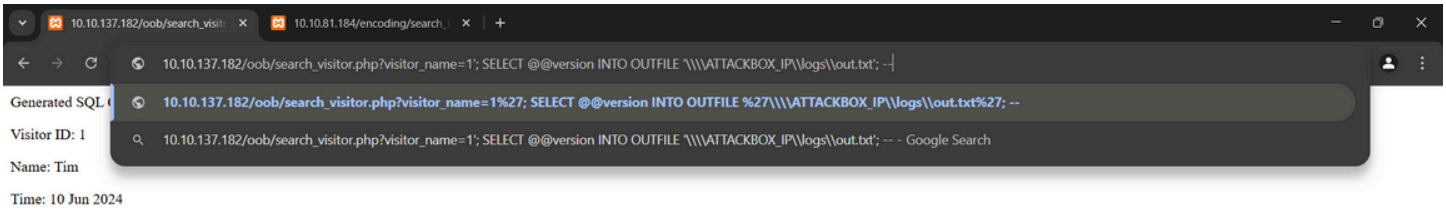
And I'm using the smbserver.py here as you see



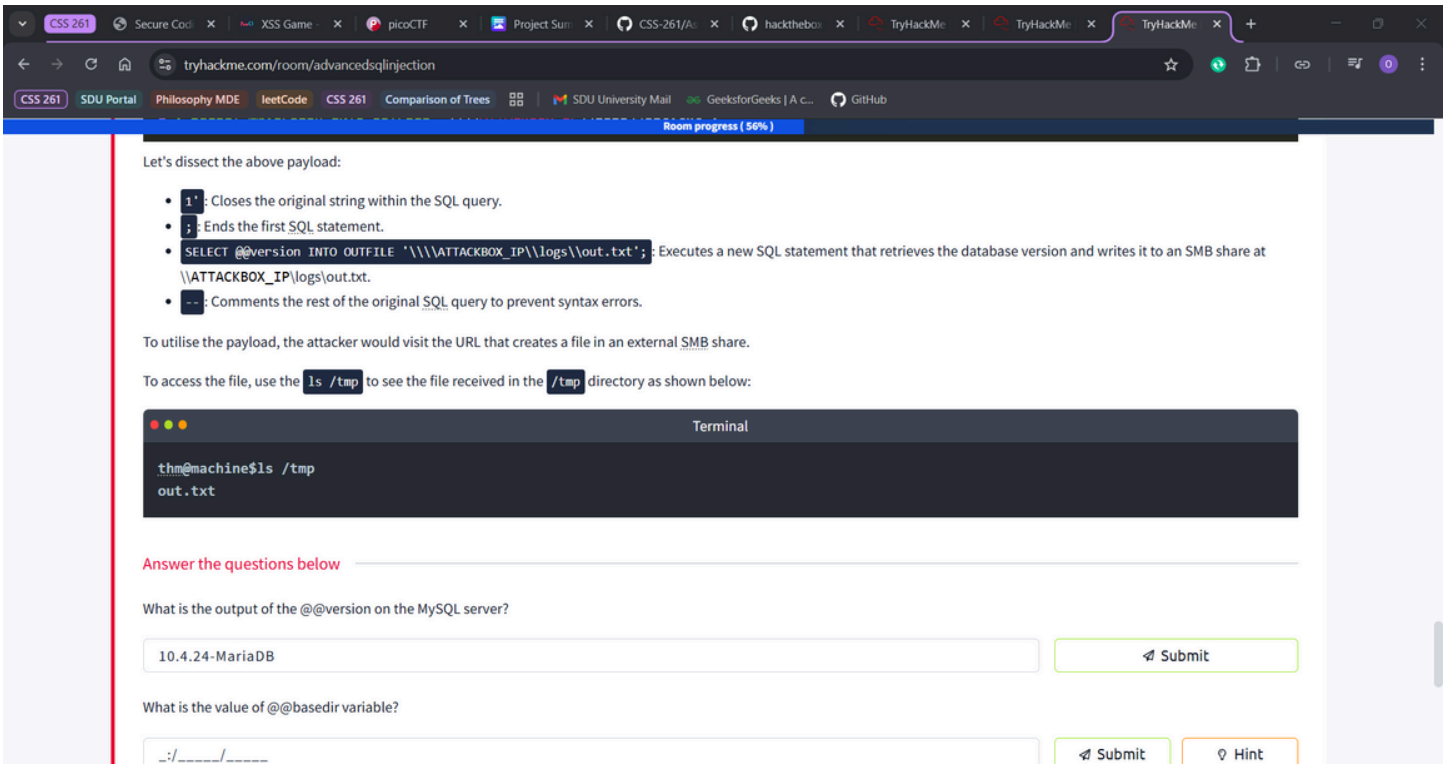
We copy this

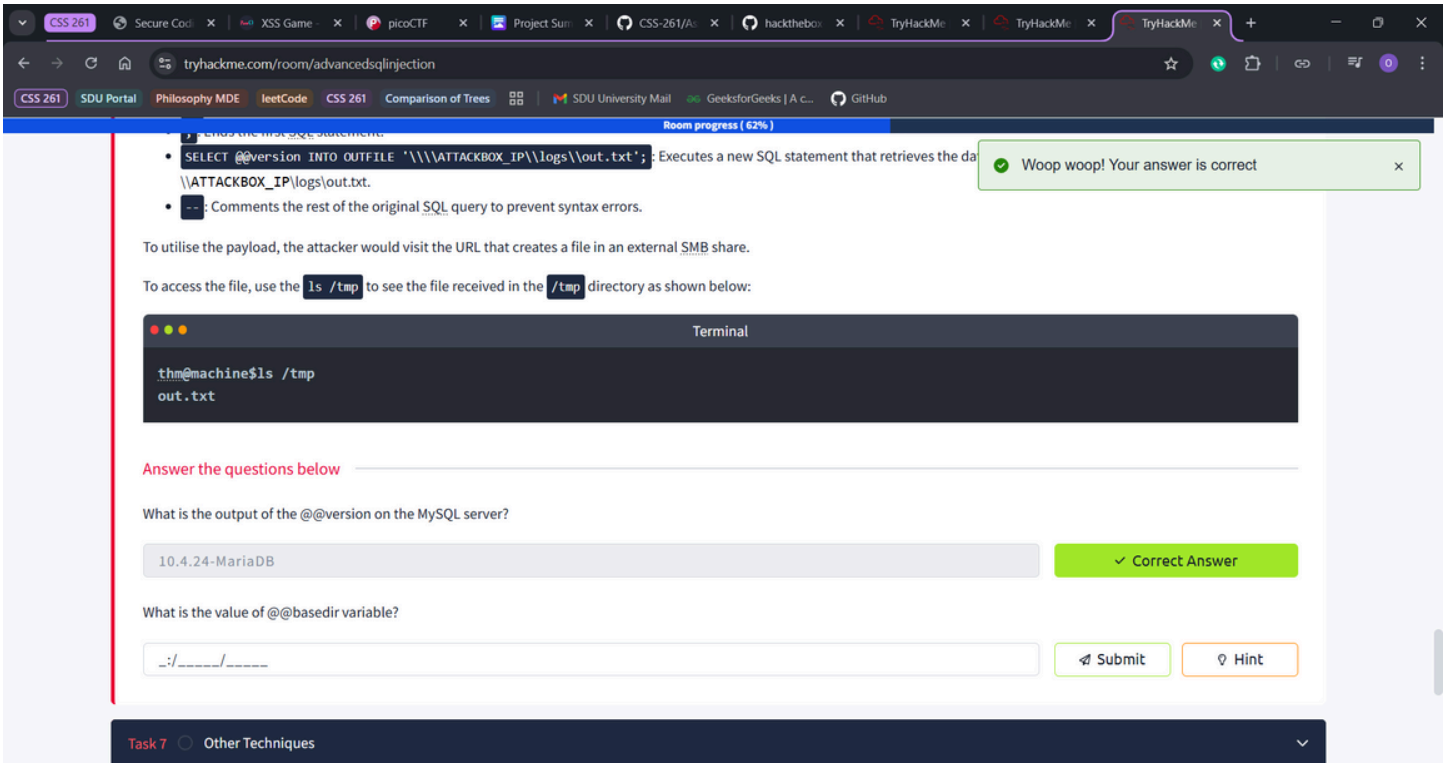


We paste here:

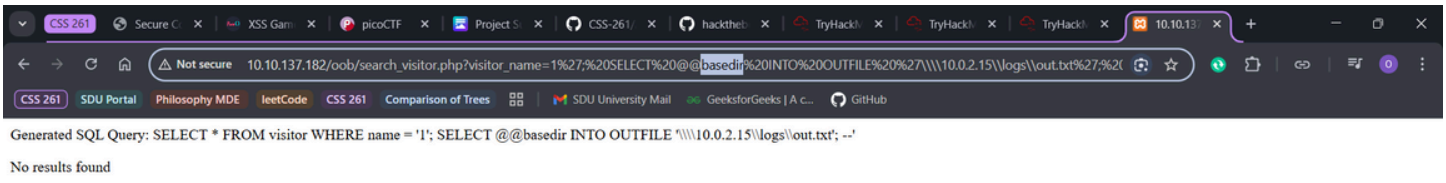


And by doing that we obtain the out.txt file to our virtual machine

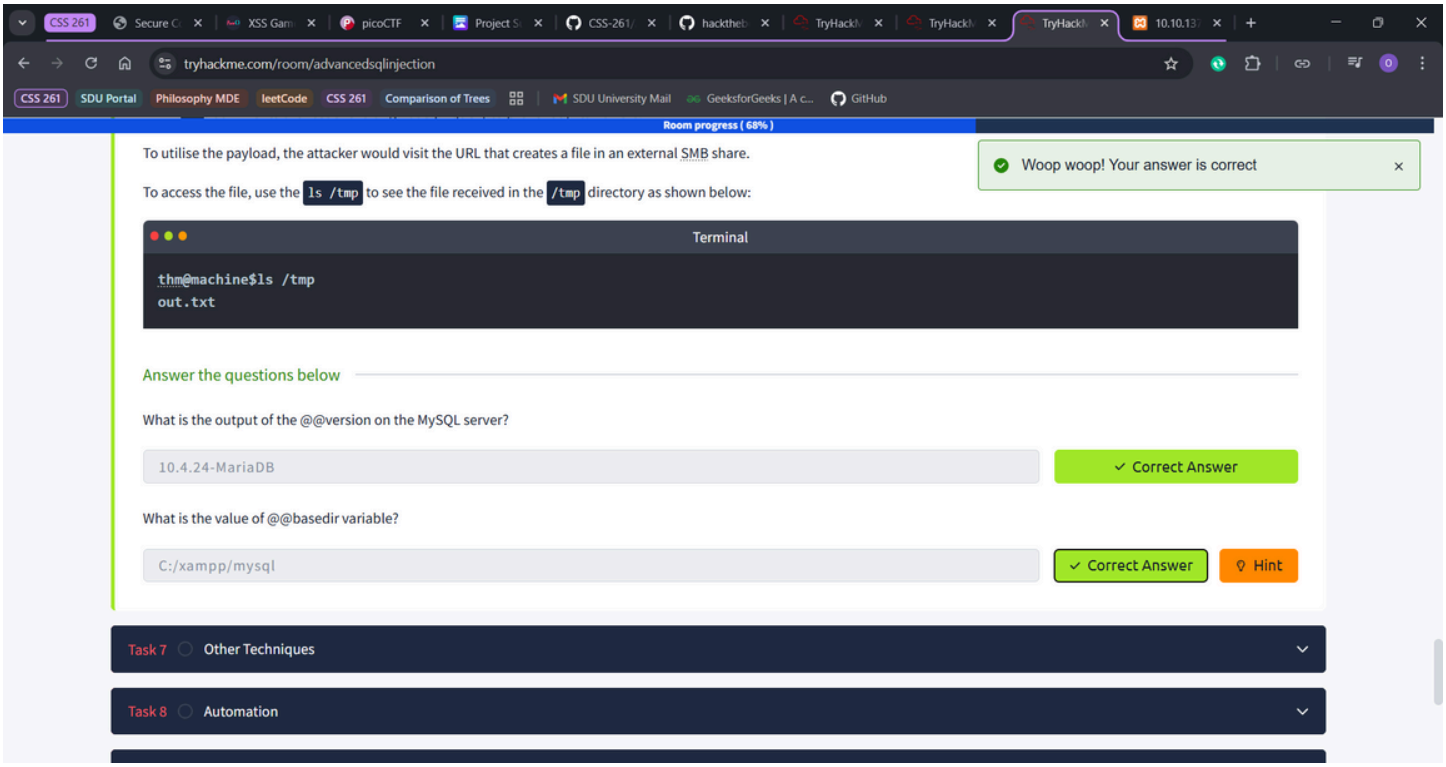




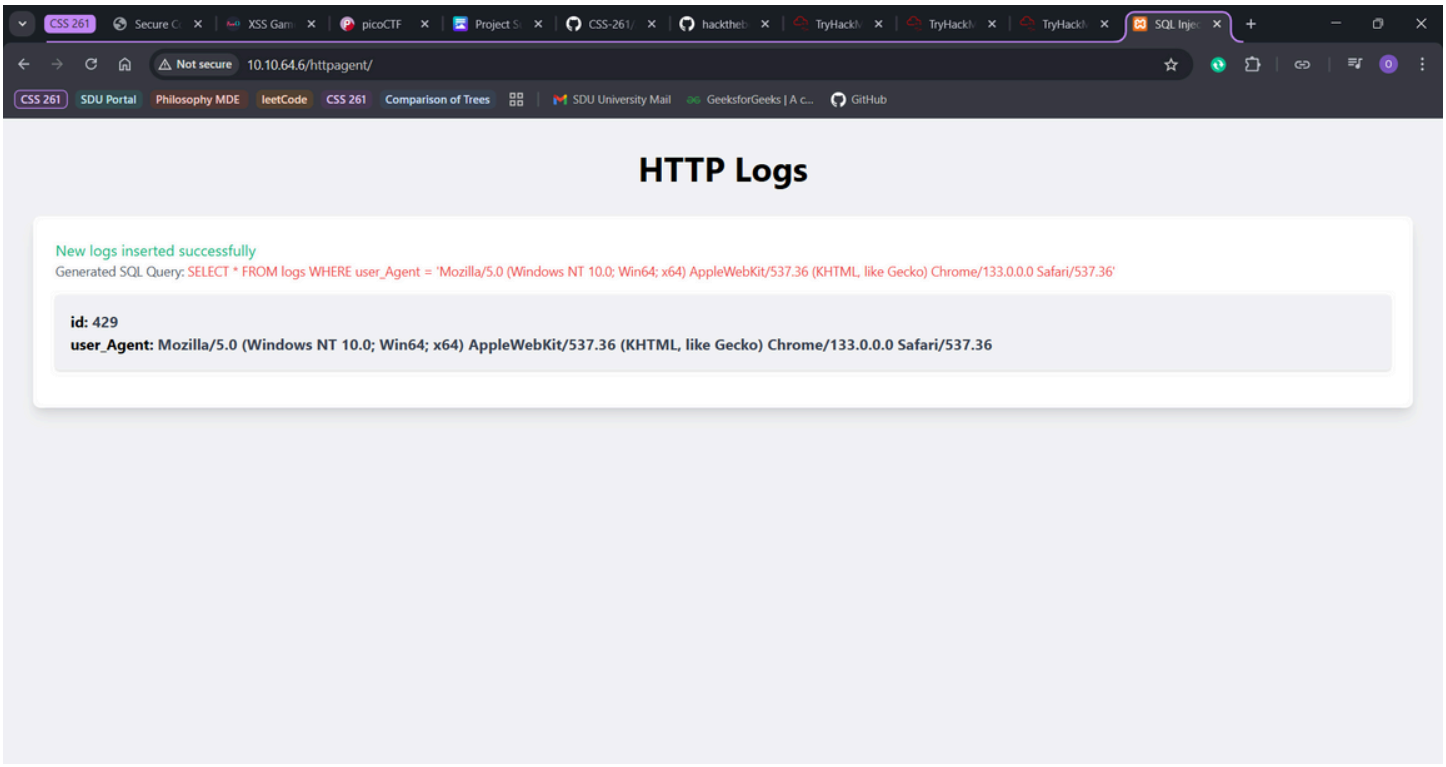
Next, we just change the version to this:



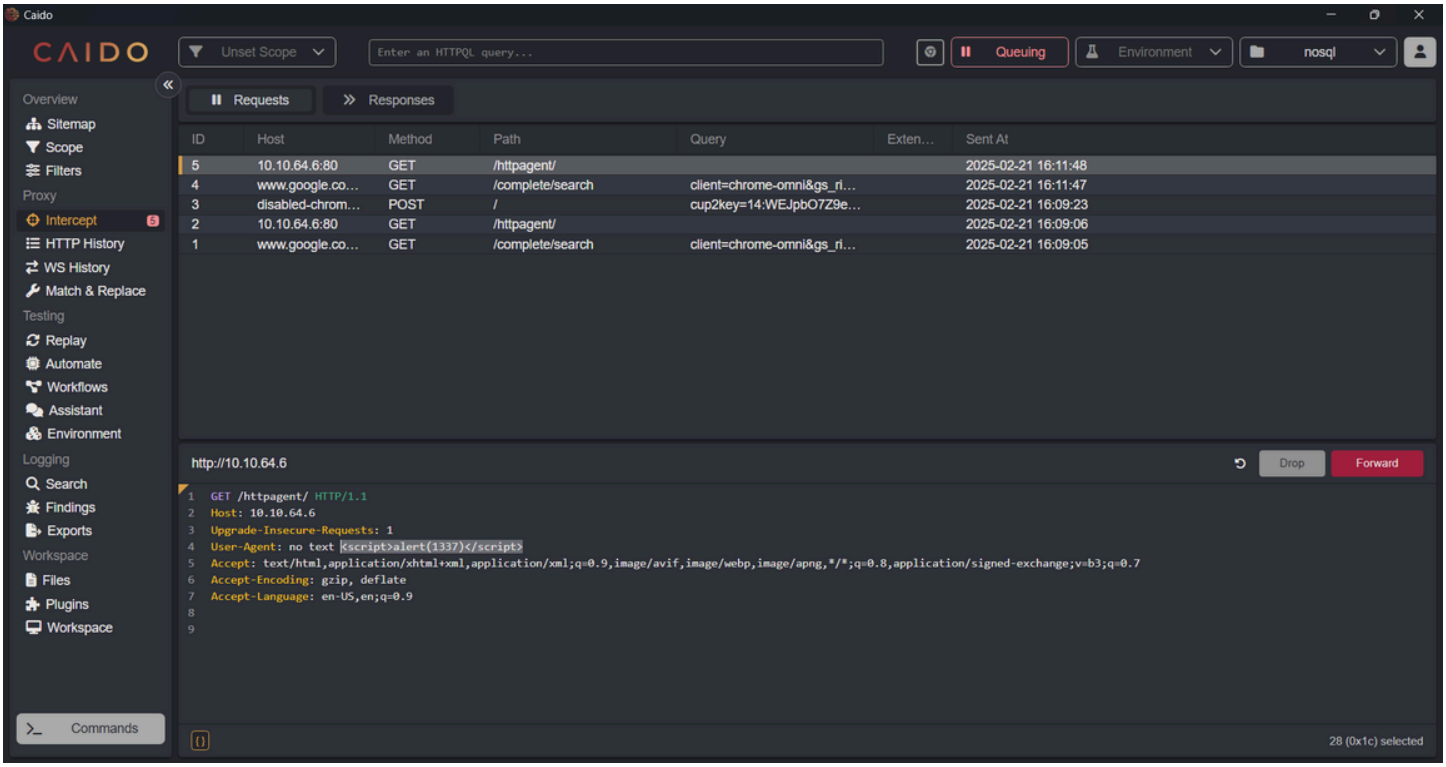
We do the same process here and it's done!



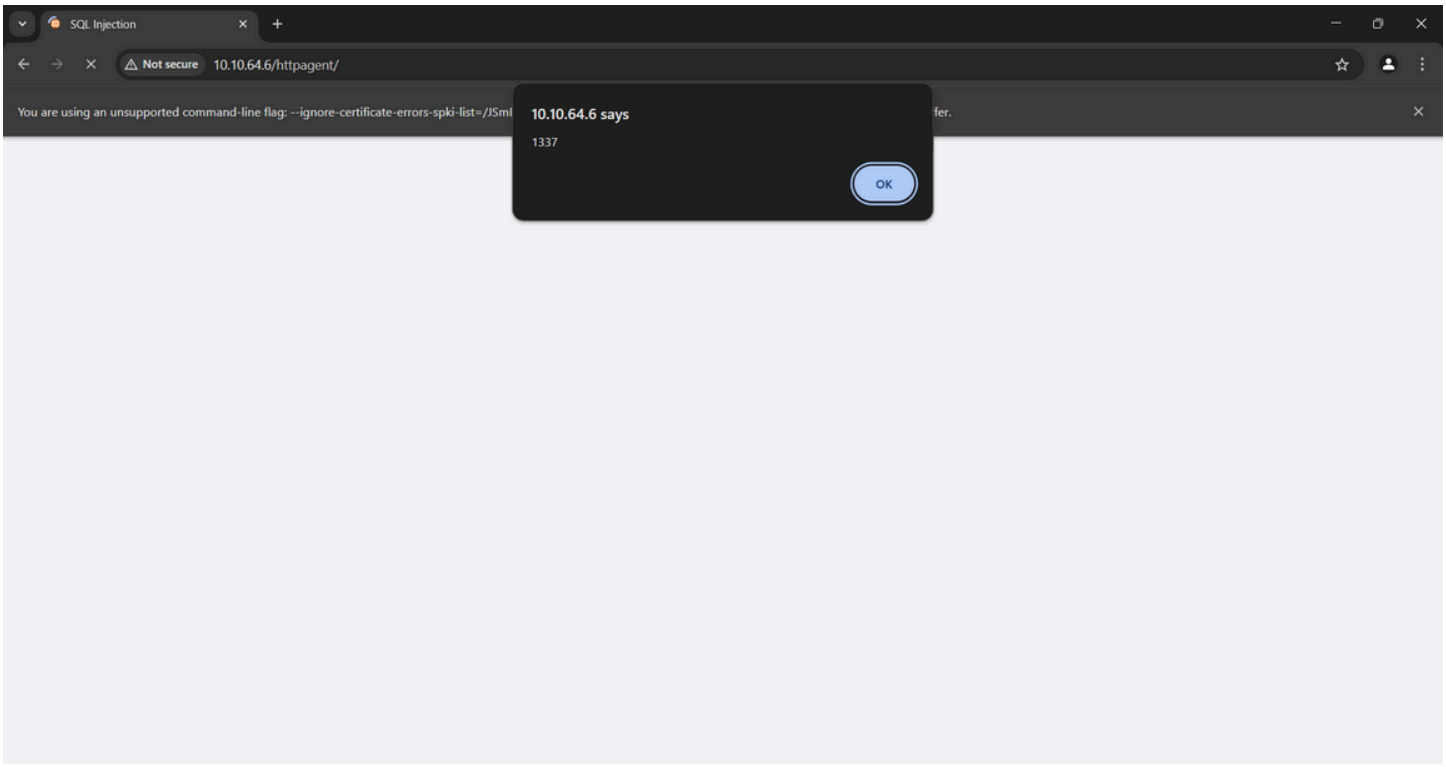
Lastly for practical part, we go this site and see this message



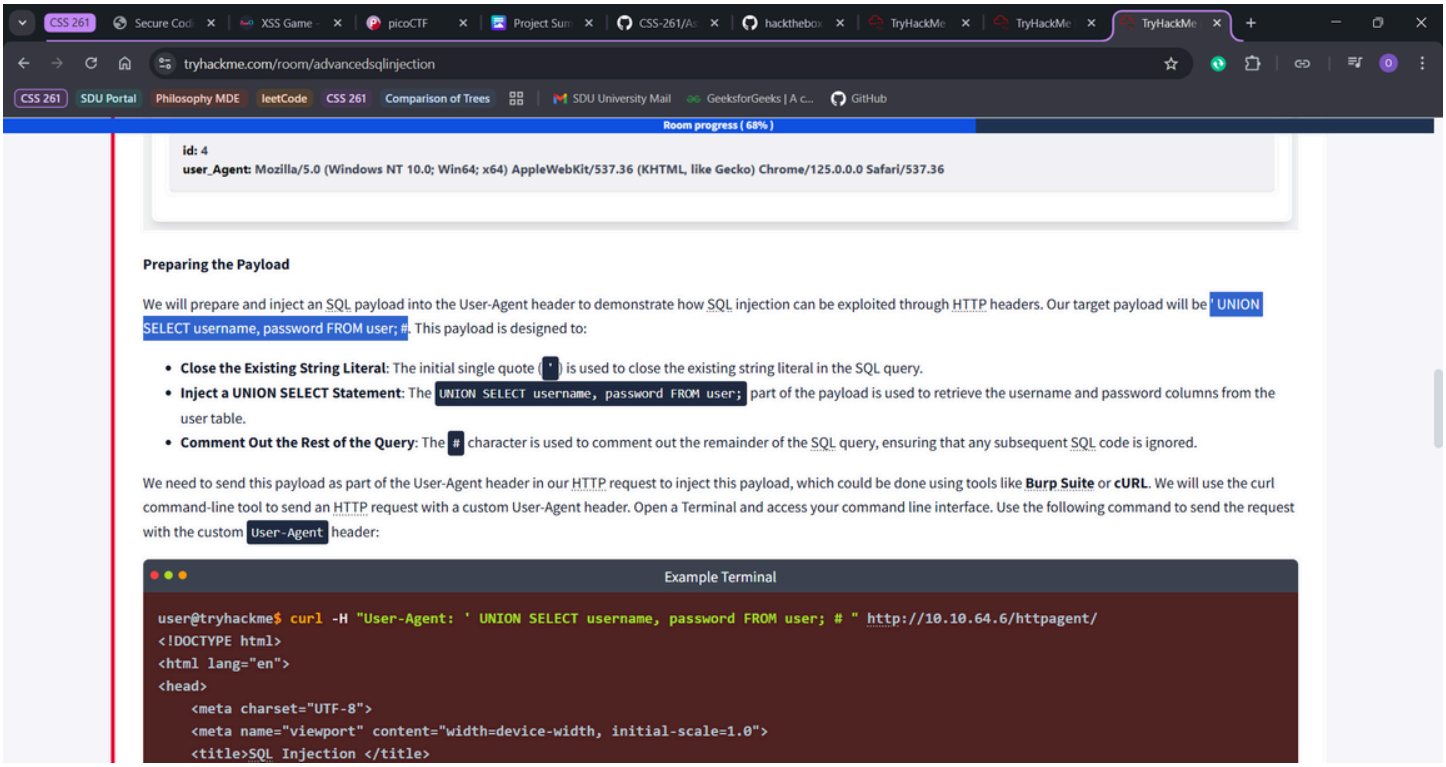
We will also intercept the request

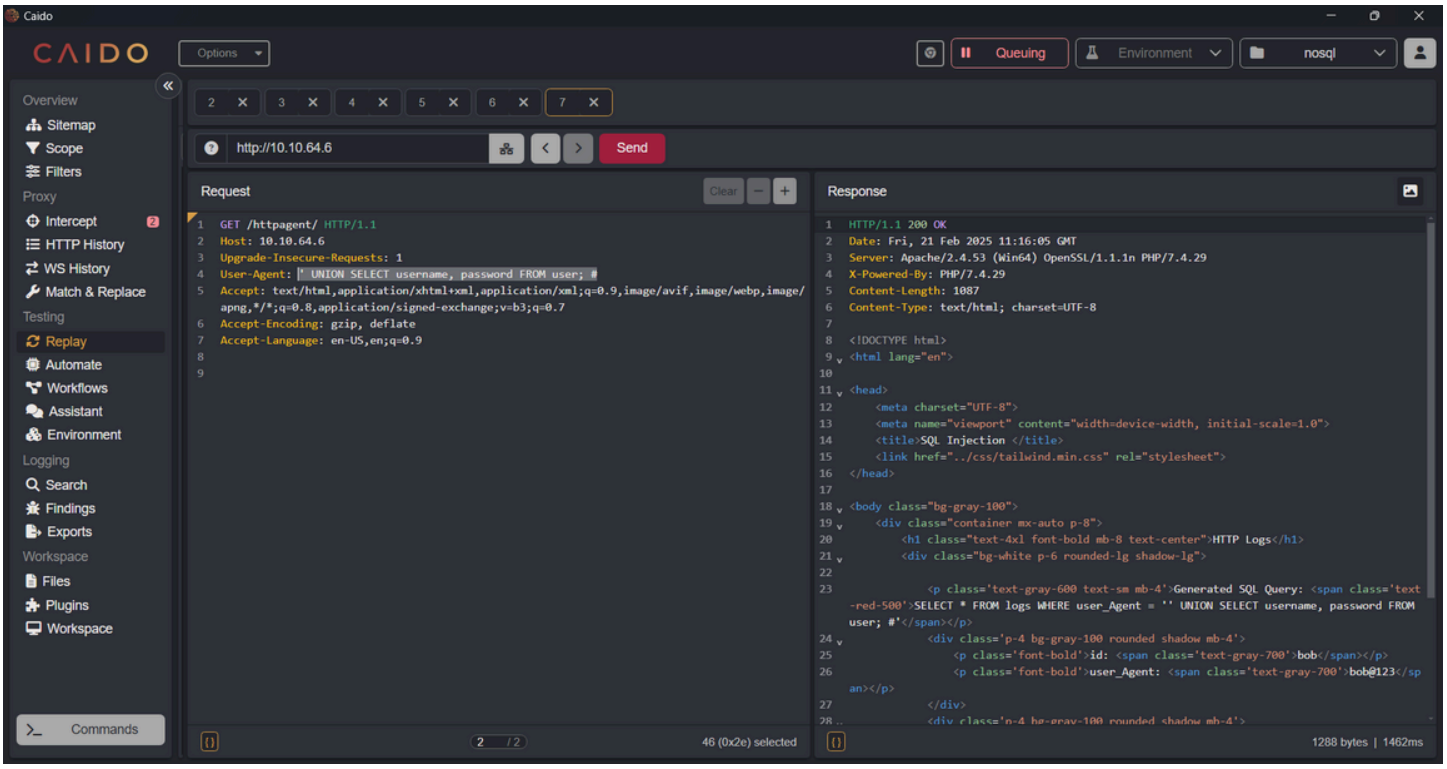


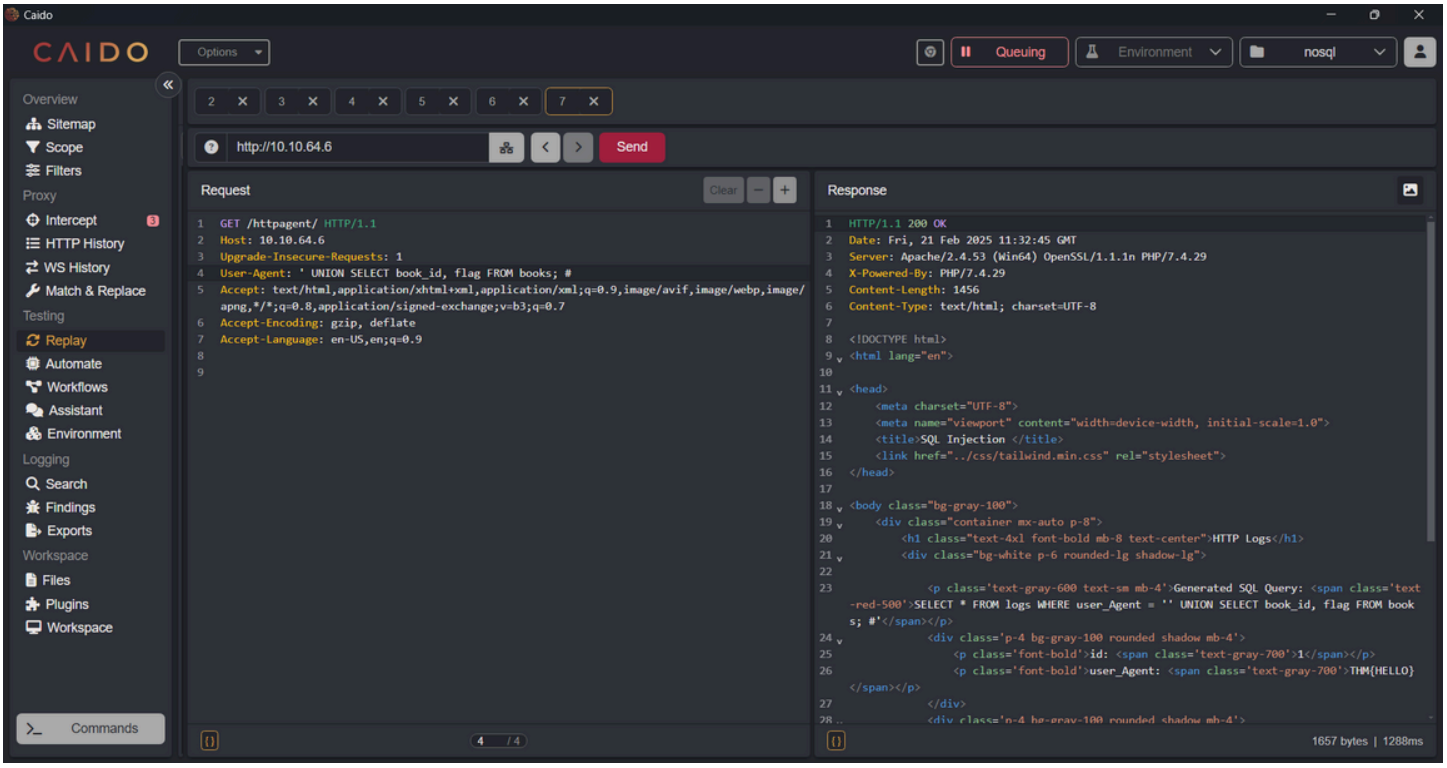
By doing so, now we know the system's vulnerability



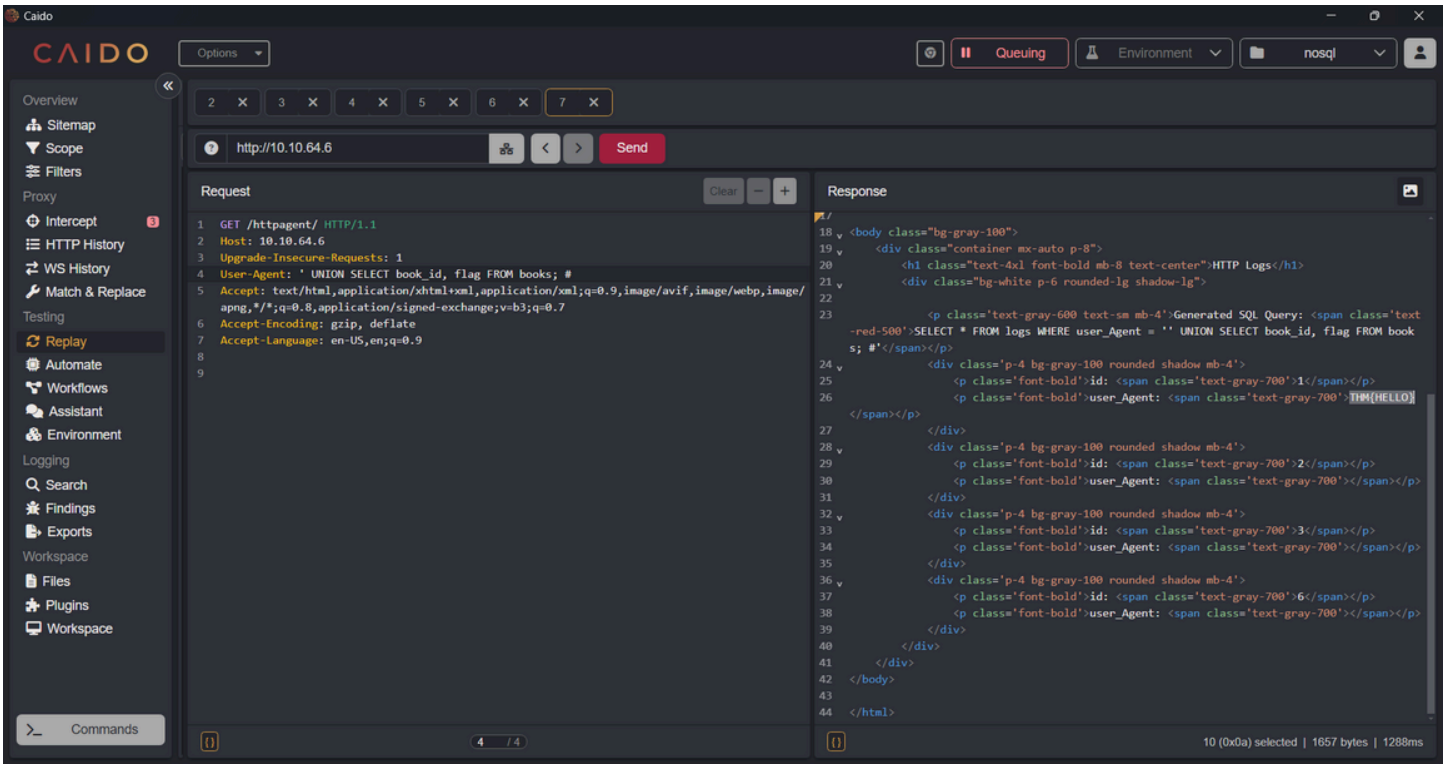
We do as it says in the task:



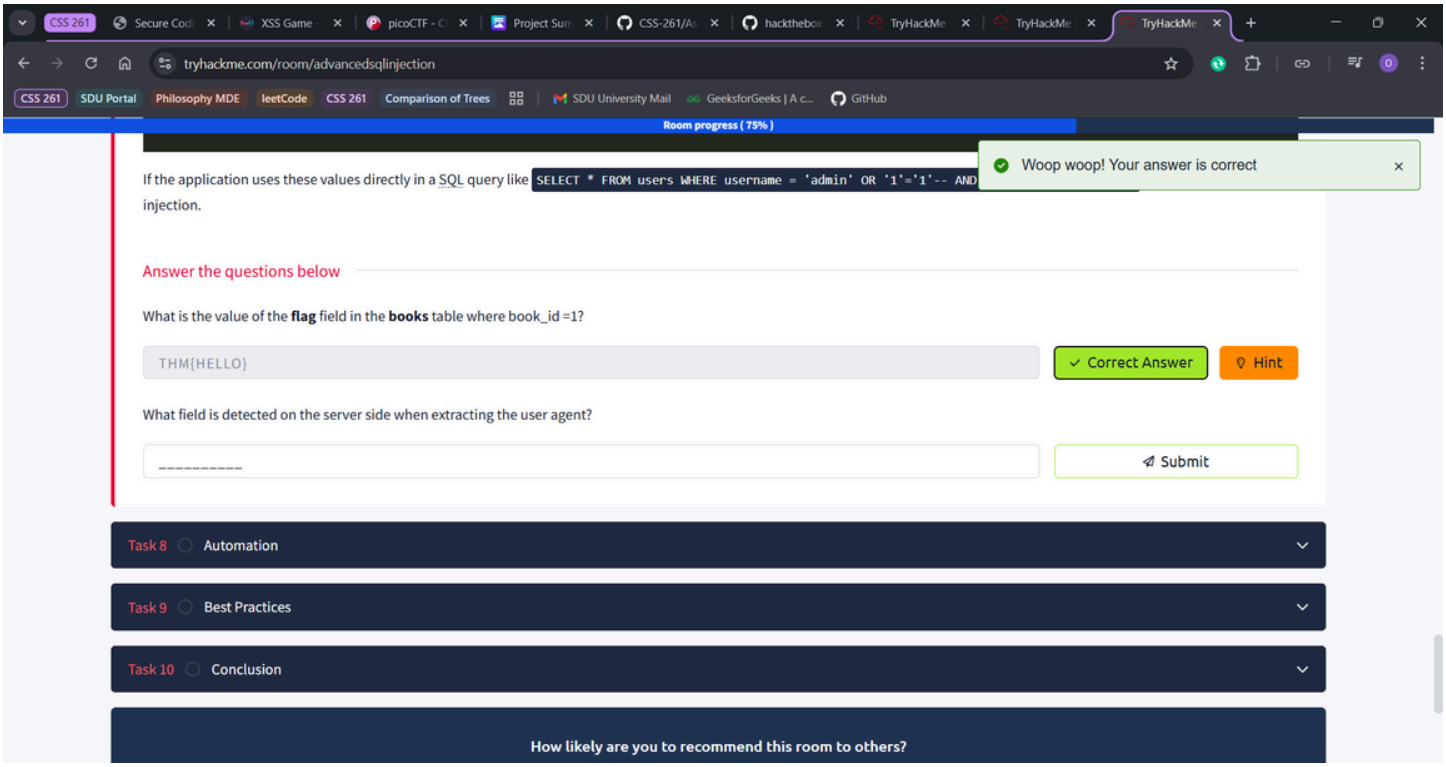




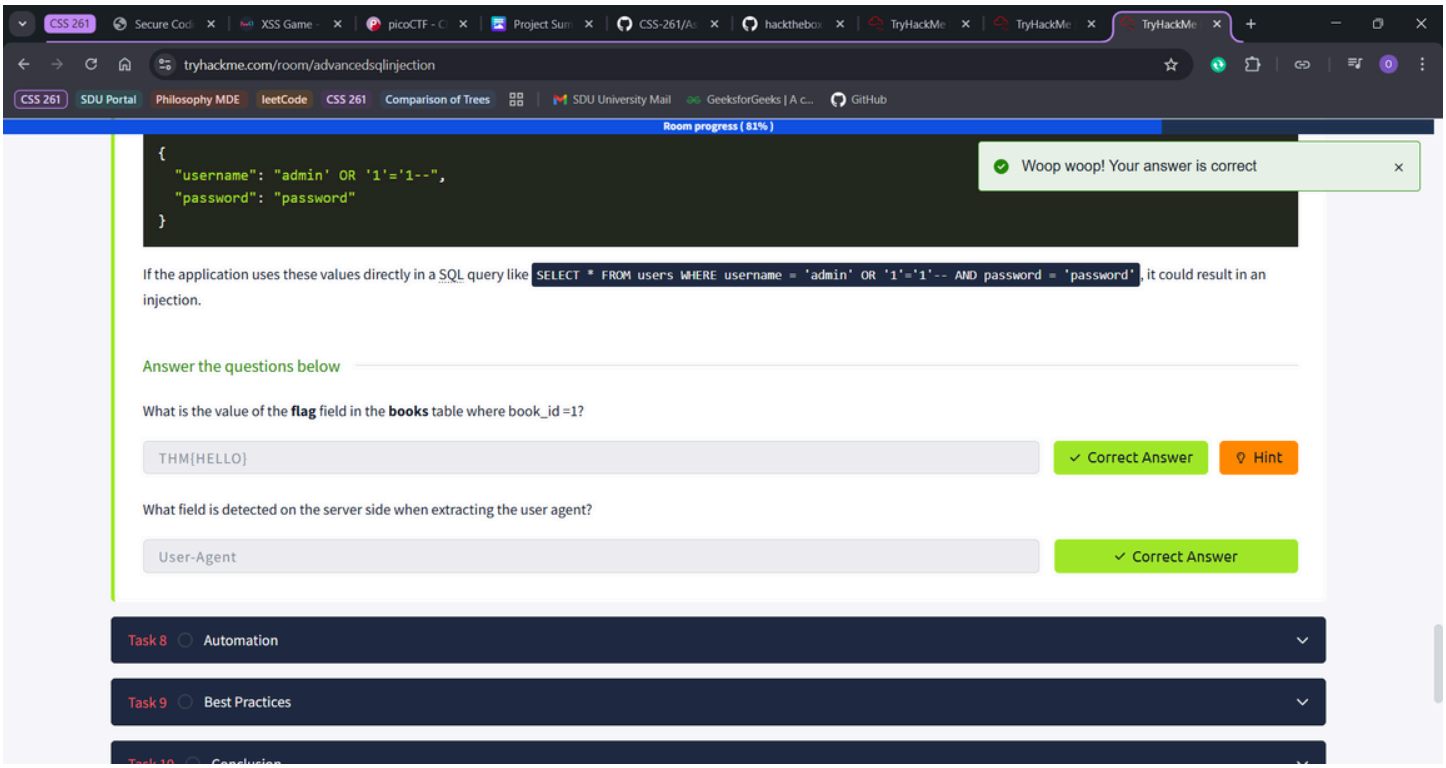
And here we just need to find the flag



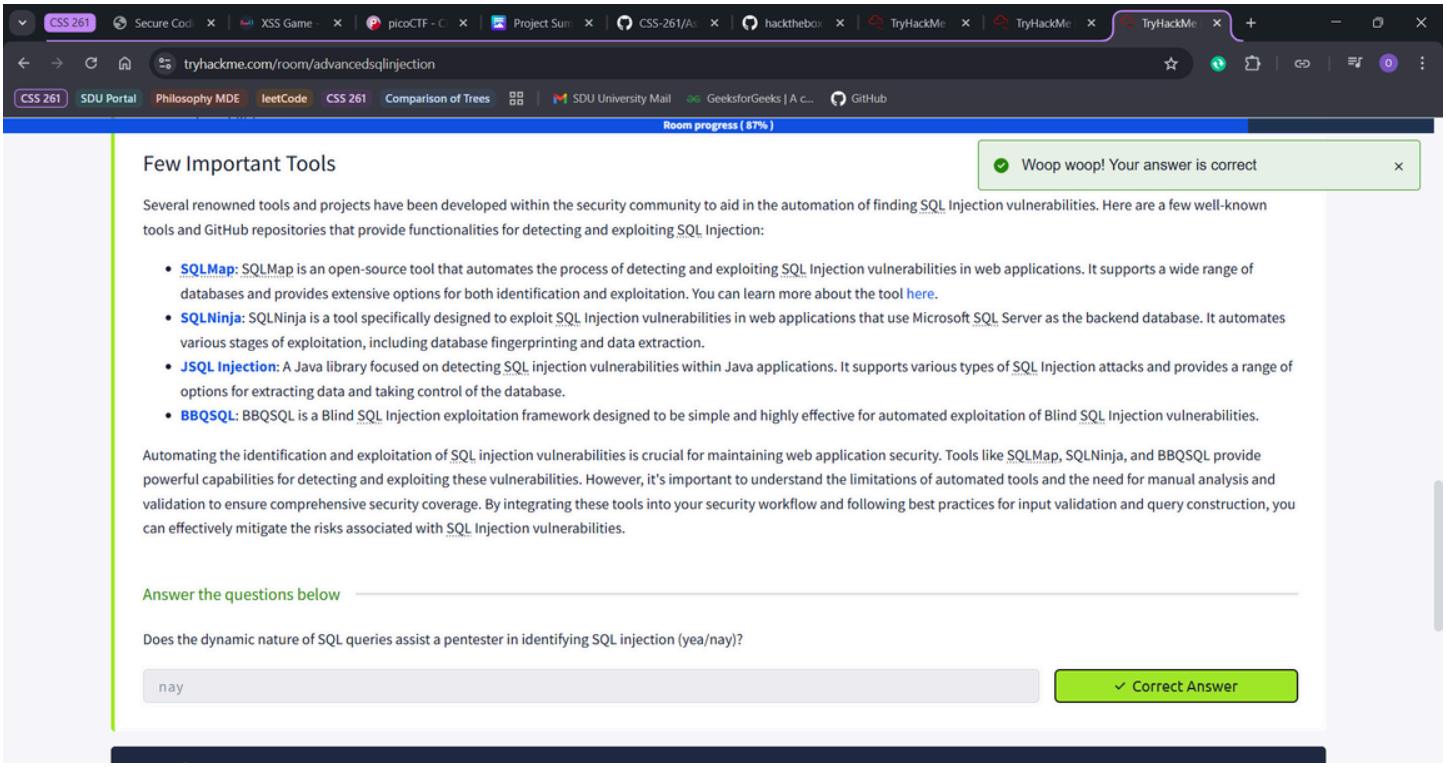
And done.

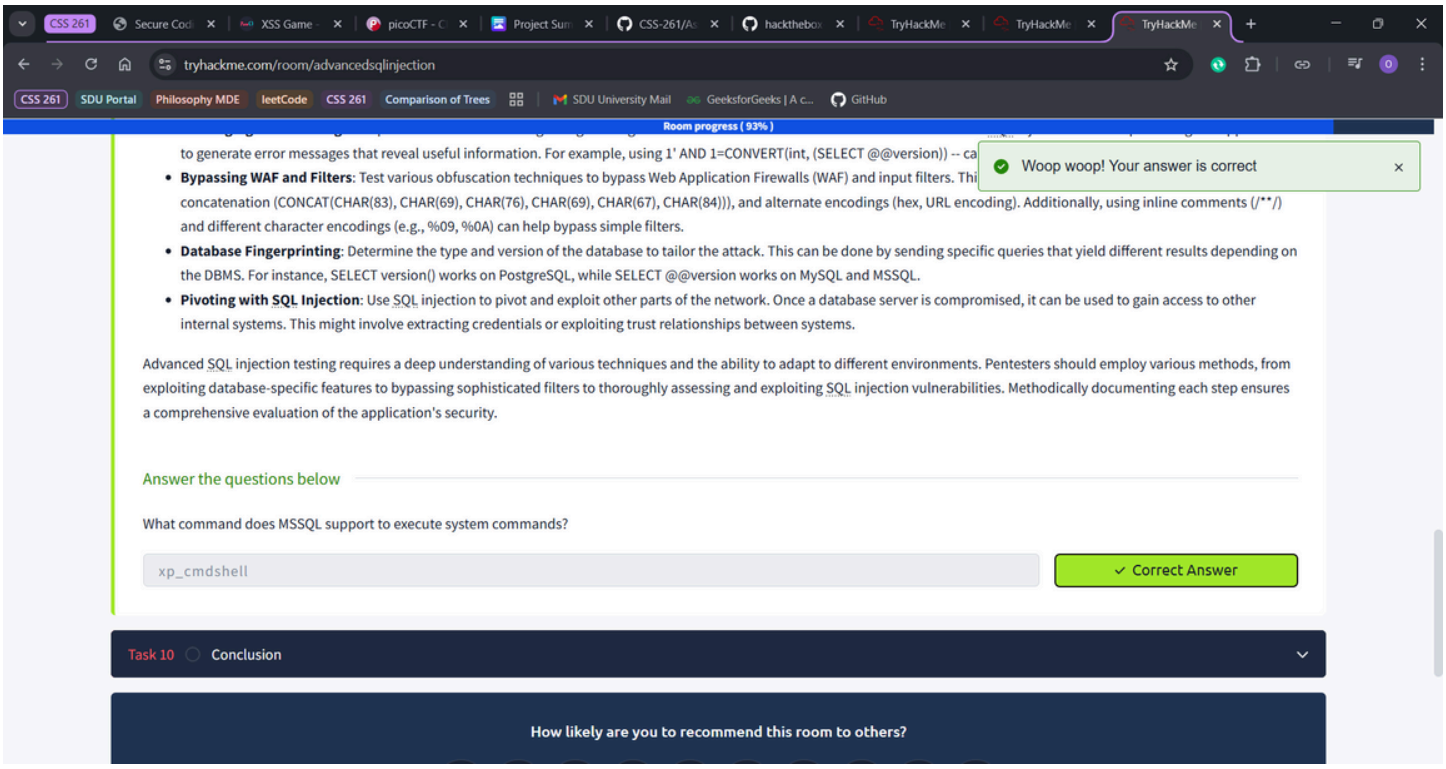


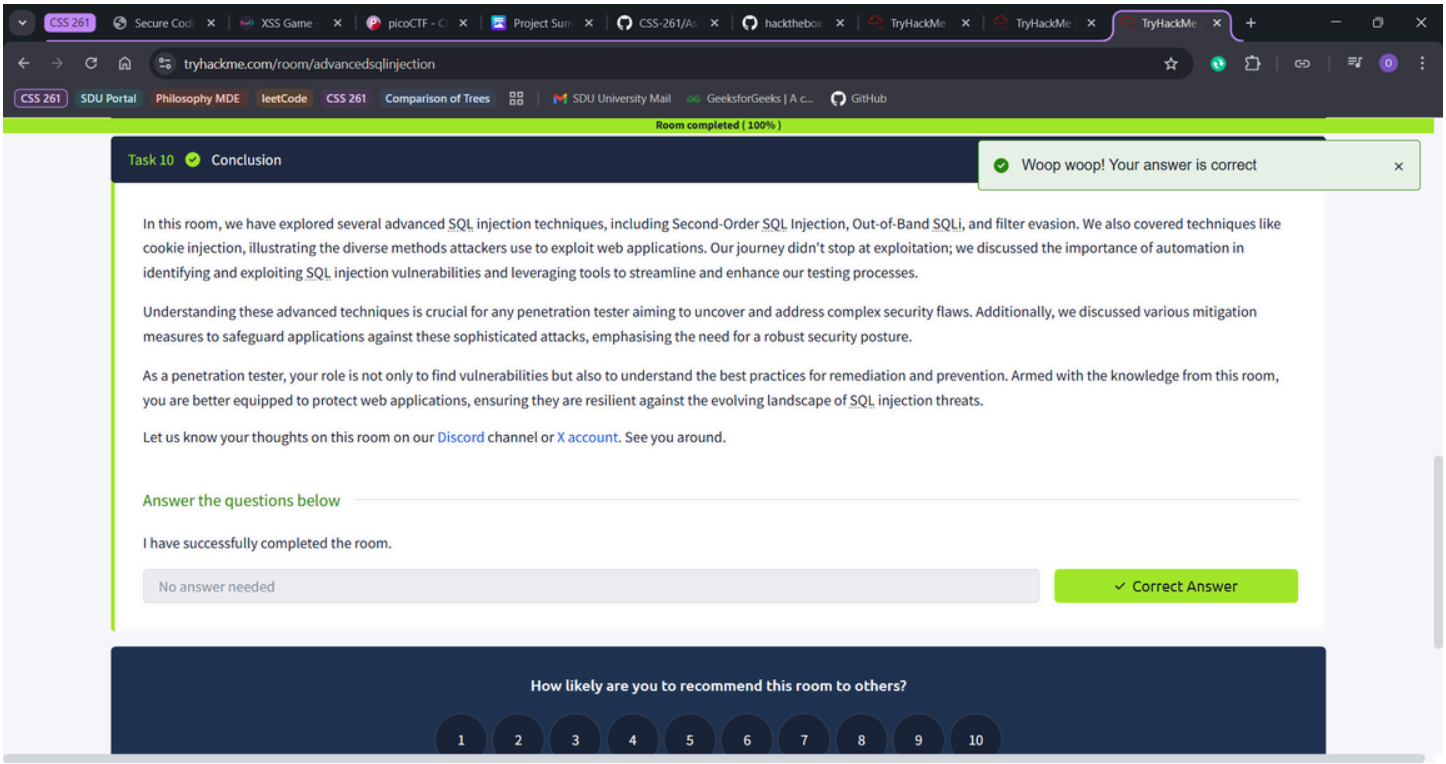
We fill out here:



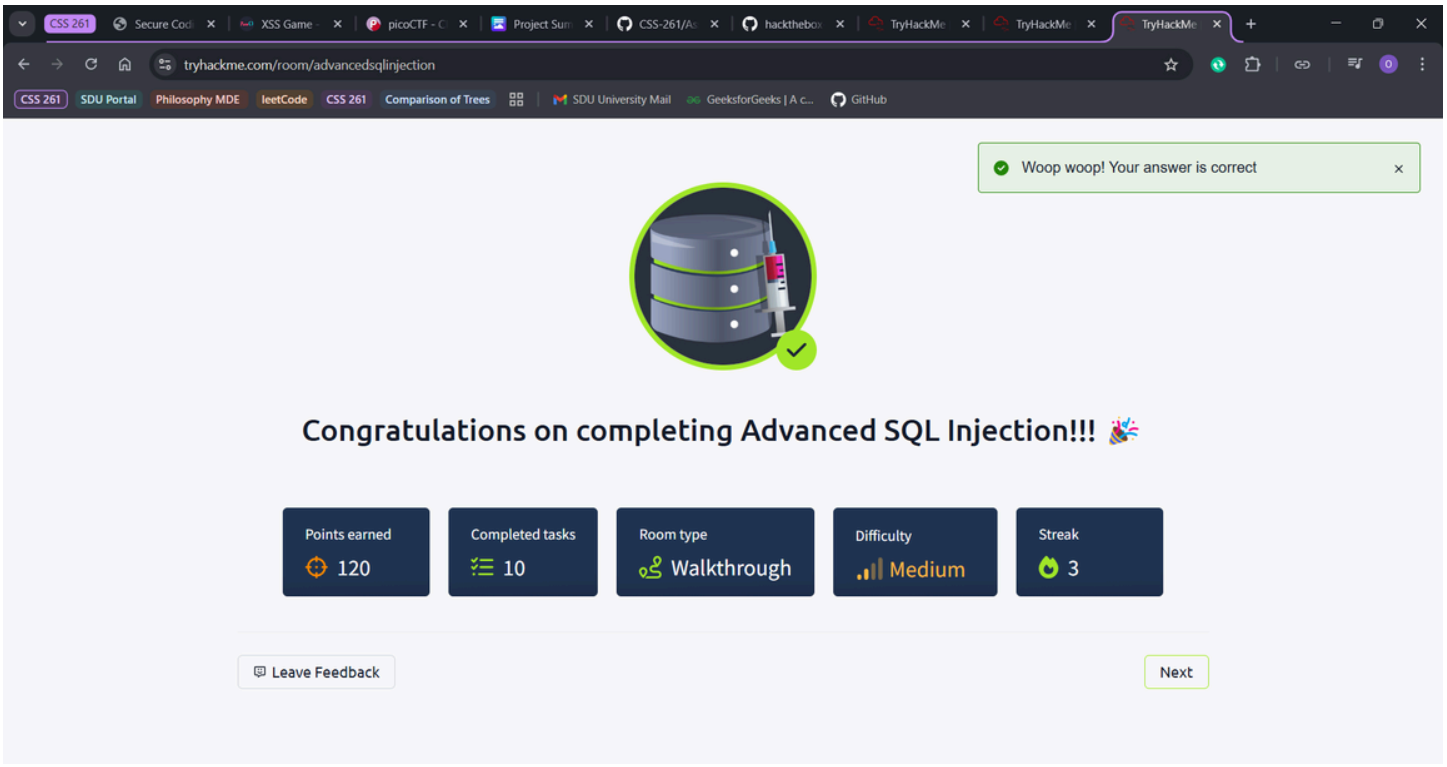
Answer the last questions







And now we've completed the room.


tryhackme.com/room/advancedsqlinjection
Woop woop! Your answer is correct
Congratulations on completing Advanced SQL Injection!!!
Points earned
120
Completed tasks
10
Room type
Walkthrough
Difficulty
Medium
Streak
3
Leave Feedback
Next