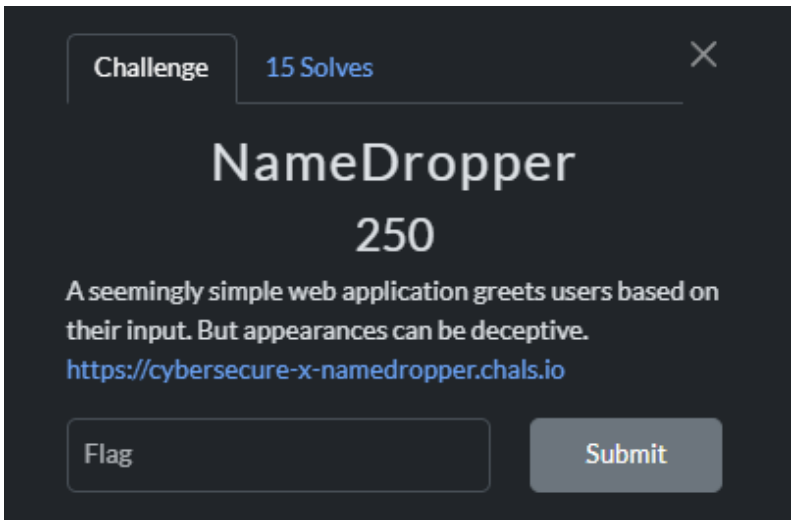
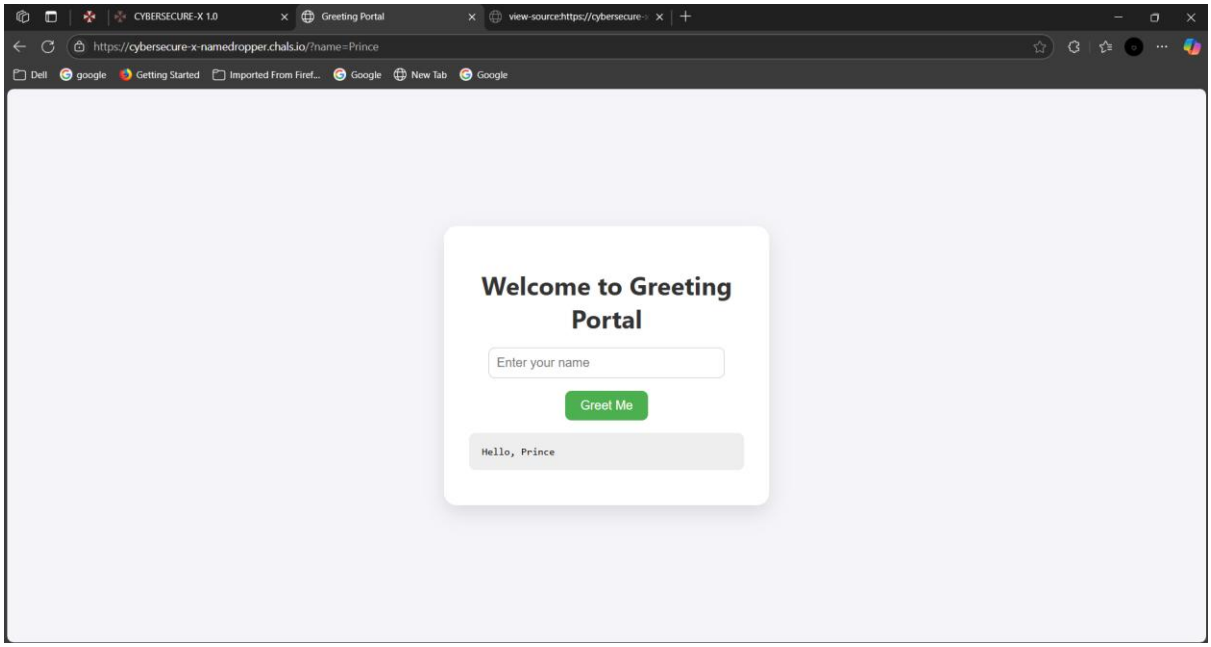
🕵️‍♂️ Challenge Name: NameDropper (250 Points) (Web)



🧠 Initial Observation:

Visiting the link shows a minimal webpage titled **Greeting Portal**. There's a simple input box asking for your name. When you enter something like "Prince" and hit "Greet Me", the page displays a greeting like:

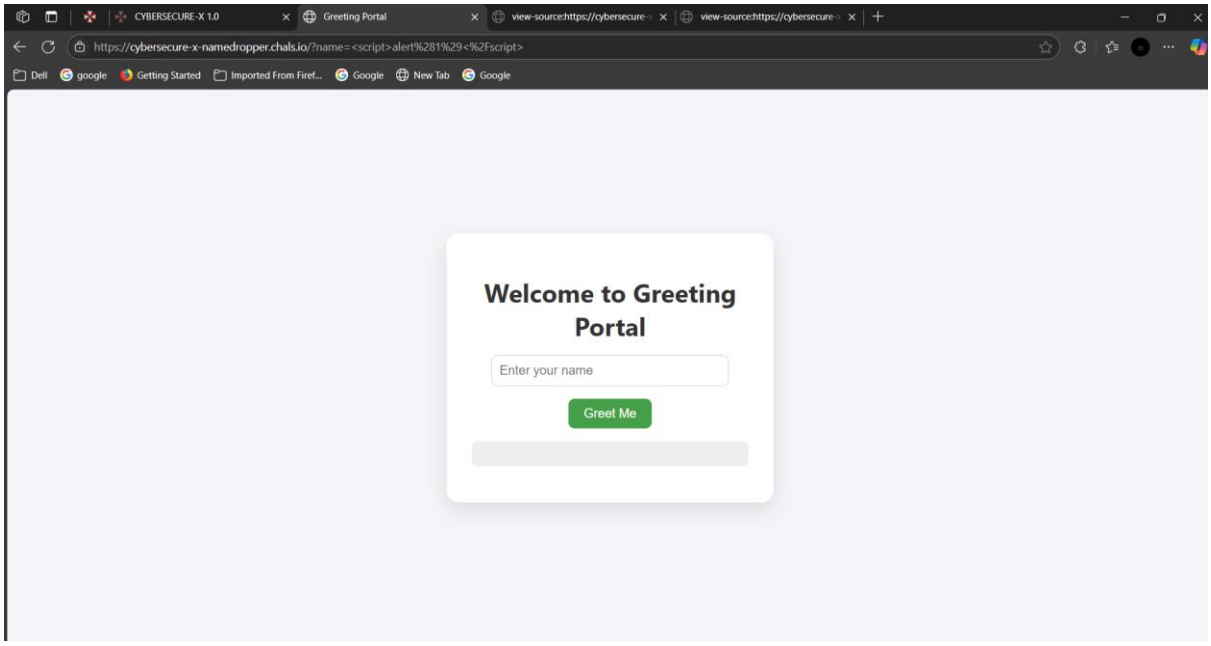


Looks harmless, right? But since it's a CTF challenge, we know there's something fishy 👀

🔥 Time to Test for Vulnerabilities

Since the input is reflected directly in the output, this smells like a potential **XSS (Cross-Site Scripting)** vulnerability.

Let's test it out with a harmless XSS payload:

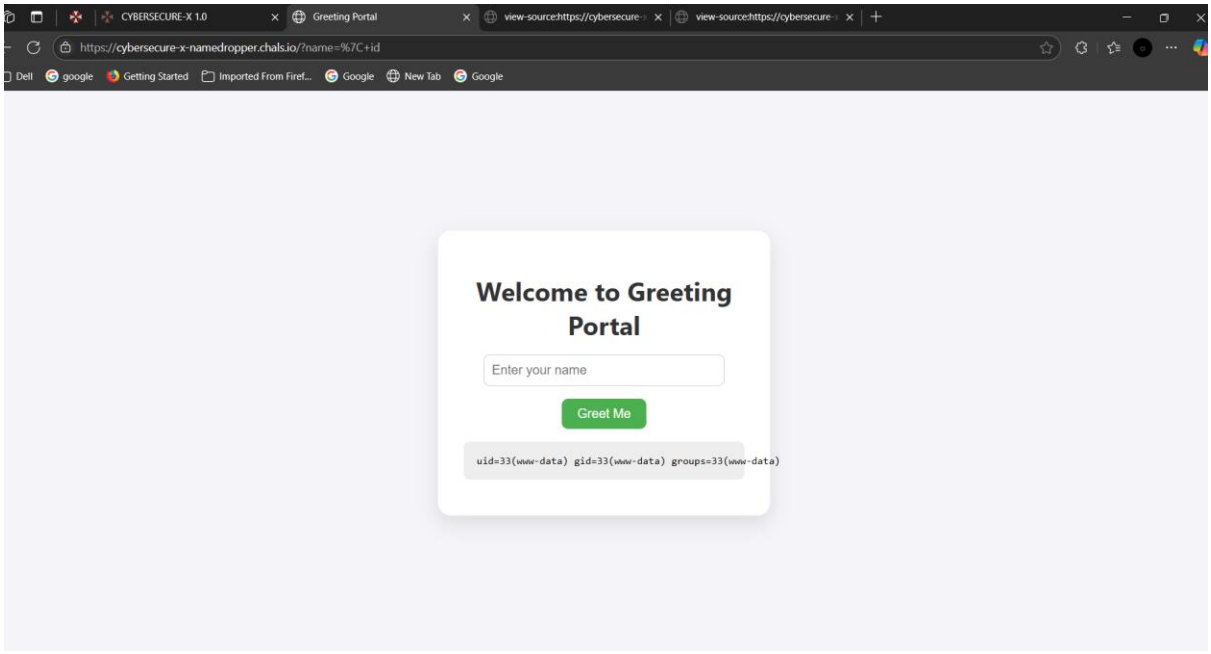


Got nothing. 😑
I tried several variations, but still no luck.

At this point, I figured... maybe it's not XSS - or at least not a simple one.

Switched and started testing for **Command Injection**.

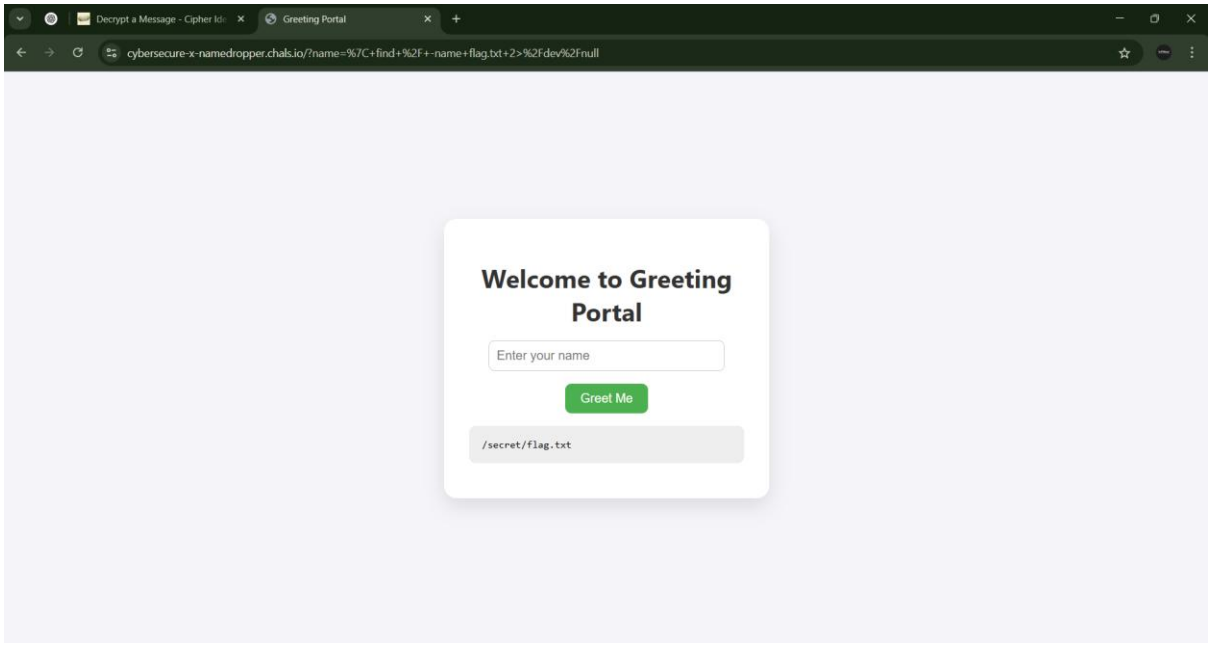
I began trying various payloads but didn't work then I used this one "**| id**" and boom it injected and the output was like:



So, the input was being passed to a shell command without sanitization. Classic command injection.

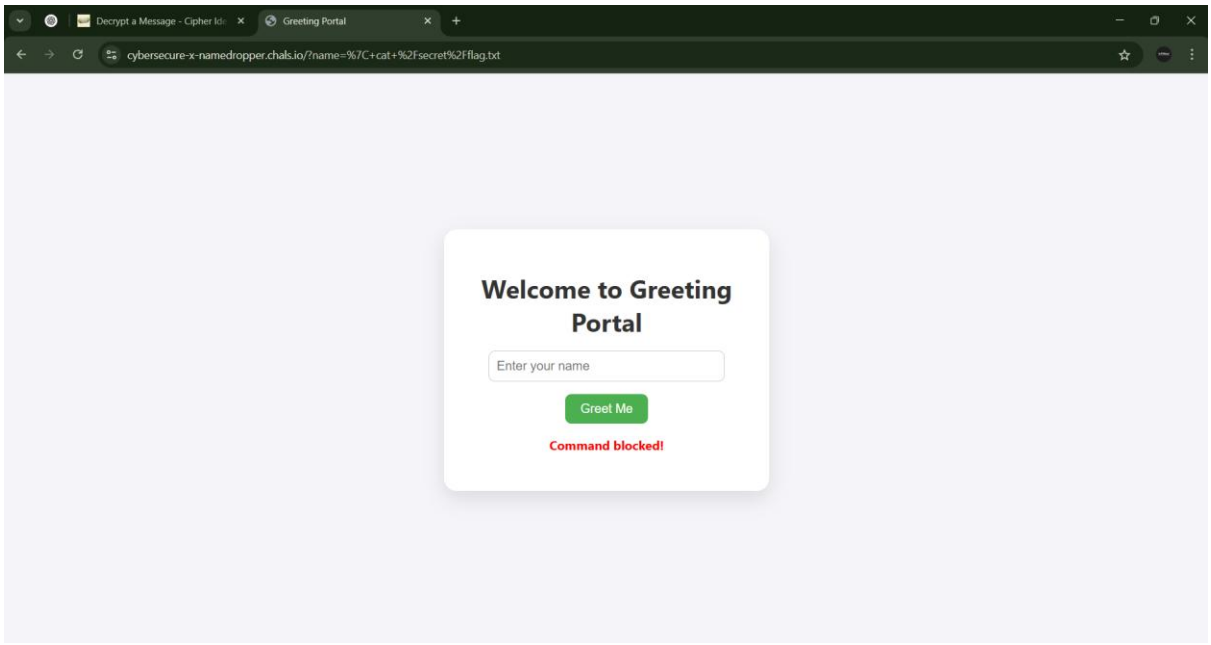
Next step is to grab the flag from it, so I ran this command:

“ **| find / -name flag.txt 2>/dev/null** ” and go this output.



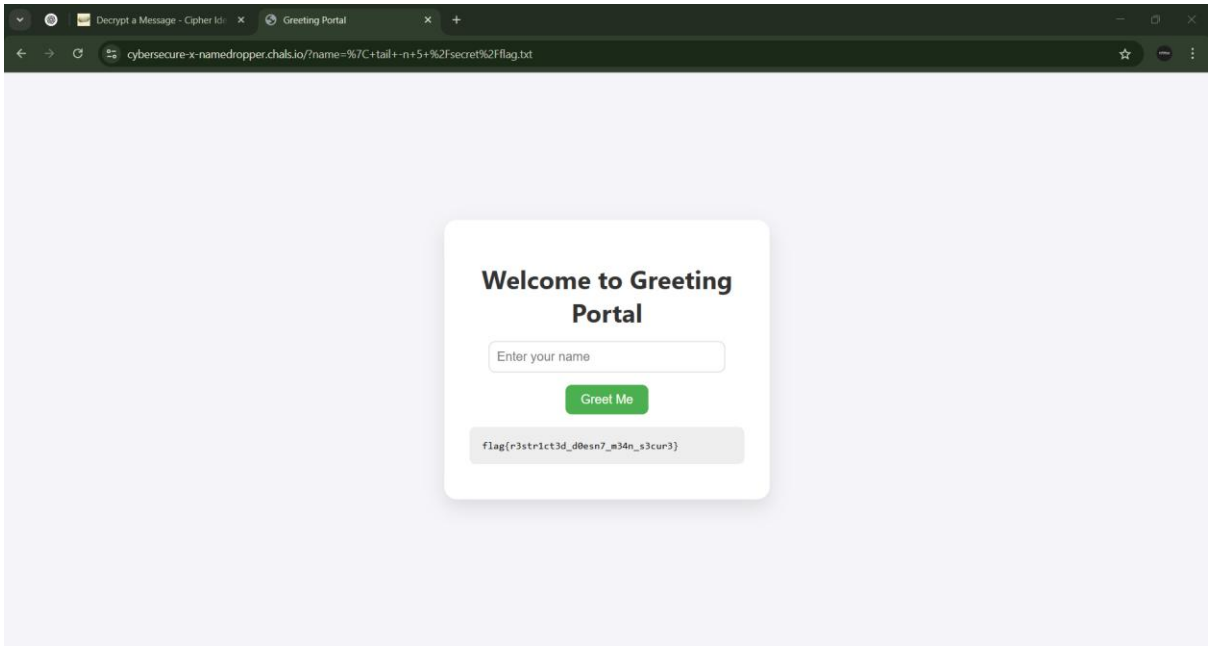
That gave me the exact path to the flag file.

Then I simply ran: "**| cat /secret/flag.txt**"



But it didn't work the server had **cat blocked** 😐

So I used: "**| tail -n 5 /secret/flag.txt**"



✅ And that worked! Got the flag.

FLAG: flag{r3str1ct3d_d0esn7_m34n_s3cur3}

~By Team justahacker.