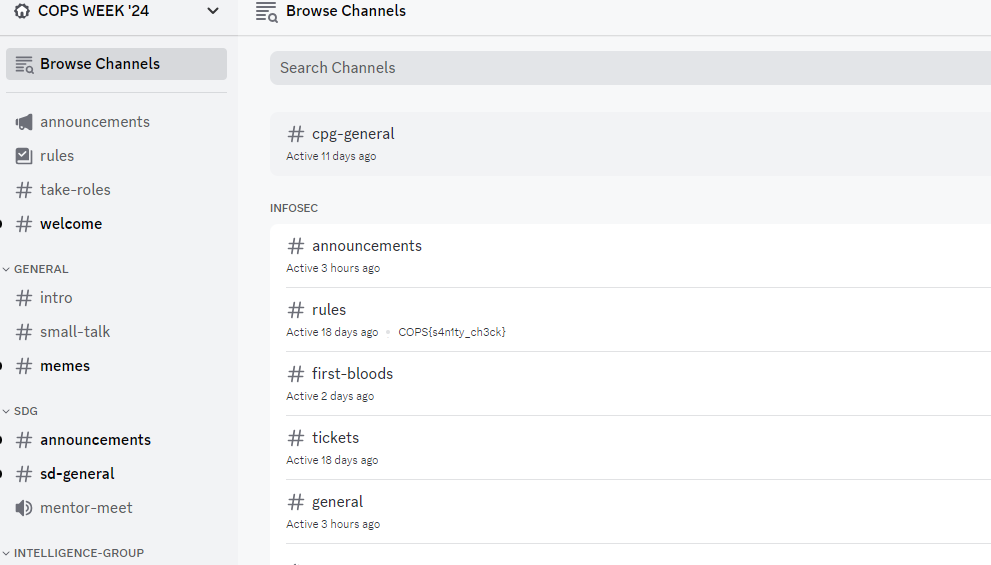
**Wanna Hack CTF Writeup**

MISC  
SANITY:

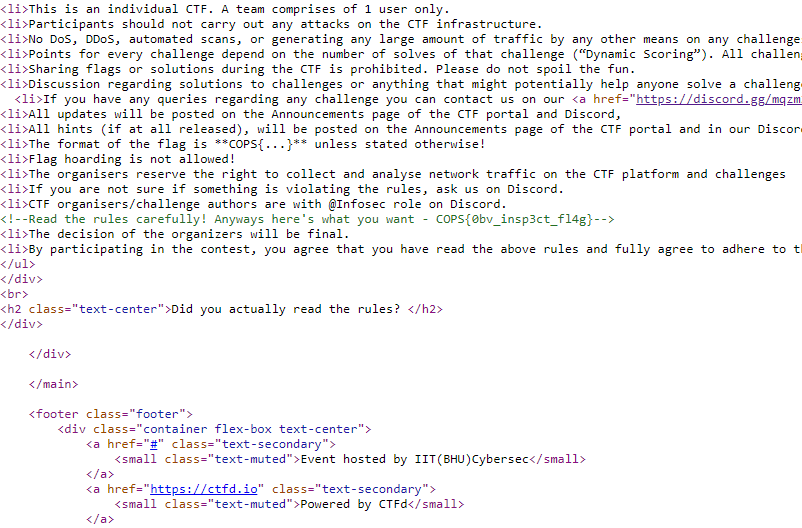
I joined the discord channel using the link. I checked the infosec channel but nothing was there. While exploring the whole channel I discovered something…and yes that was the flag.



WEB

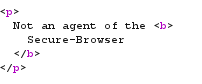
WELCOME:

I opened the link given in the challenge. Read all the rules. But no clue was given. So then I went to view the page source and analyzed the code. Yes I fount the flag being commented.



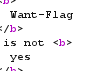
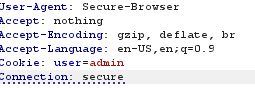
HEADERS!:

Opened the link that was given in the challenge. Not an agent of Secure-Browser. Thought thus to be a little fishy. But anyways ignored it and went directly to the inspect. Saw the whole code but didn’t find anything. Back to the challenge name. Headers.. Headed directly to burpsuite a famouse tool for web exploitation. After heading to the burpsuite I saw how the application works. Ok so did some of the steps told on the internet and opened the website. Now followed the exact same approach as the author wanted to.





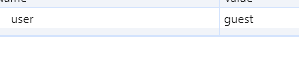






ADMIN:

Cannot think anything than going to Burpsuite after visiting the site. Send it to the repeater and found the in the cookie the user was a guest. And we were supposed to login as admin. Yes, that is how we were supposed to do. Change the user to admin and get the flag.



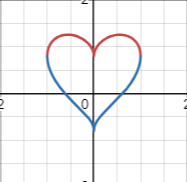
OSINT

Wannabe1:

Got an image. Simply first use exiftool to know details. Something fishy about the author. Decode it from base64 and we get the username as BitForBat.

Wannabe2:

Got to know the shape. There are some mathematical expressions in the umm.md file. Draw the graph on Desmos graphing calculator online and check if there is something useful. Tried the equations the got a heart shape. Yes that’s the answer.



Wannabe3:

The challenge has a key word trapped which has a same file name present in the repository. Observed the message carefully and got something unusual, At the ending of the sentences there are dome dots and dashes. It’s a language of morse code. Decode it and get the flag.



Wannabe4:

Got to know the location of the hacker. There is a file named location in the GitHub repository. Nothing much in there. Checked the commits and saw there were changes made in that. Yes, there is a comment present. What3Words something strange. Google it and checked it is a website. opened it and a specific type of name was asked consisting of 3 words. Read the comment carefully and you’ll get the asked one at the end. Enter it in the website and it will give u the location.

