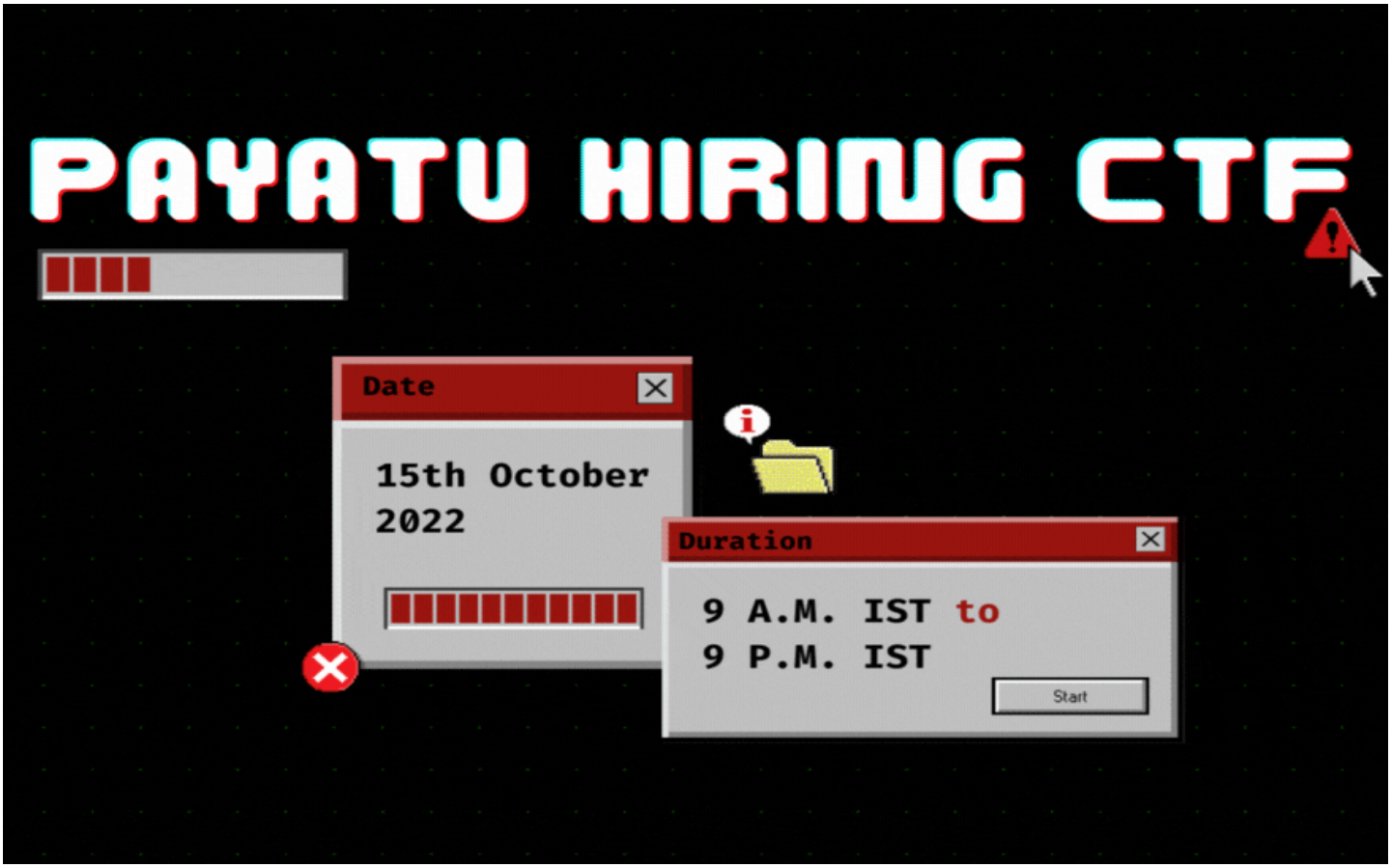
Ctf Writeup

Payatu Hiring CTF

Md Tajdar Alam Ansari (MacTavish)



Introduction

Payatu hosted a hiring CTF on the 15th of October 2022, which was a 12 hour CTF from 9 a.m. to 9 p.m. I participated in the CTF using the alias **MacTavish** and solved 9 challenges.

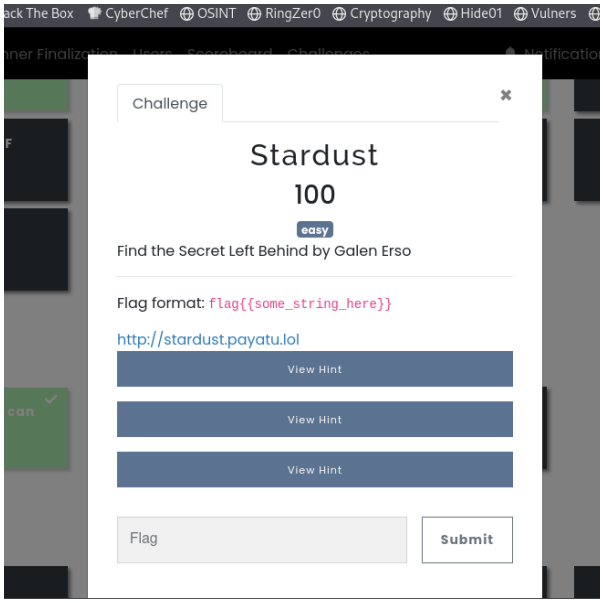
The Challenges I solved were

1. Creds - IoT
2. U:P - IoT
3. Stardust - Web
4. Baby SQLi - Web
5. EasyCalc - Web
6. Catch me if you can - OSINT
7. Mistake -1 - Network
8. Mistake -2 - Network
9. Woopress-1 - Network

The pages below show a summary of how I found the flags by solving the challenges.

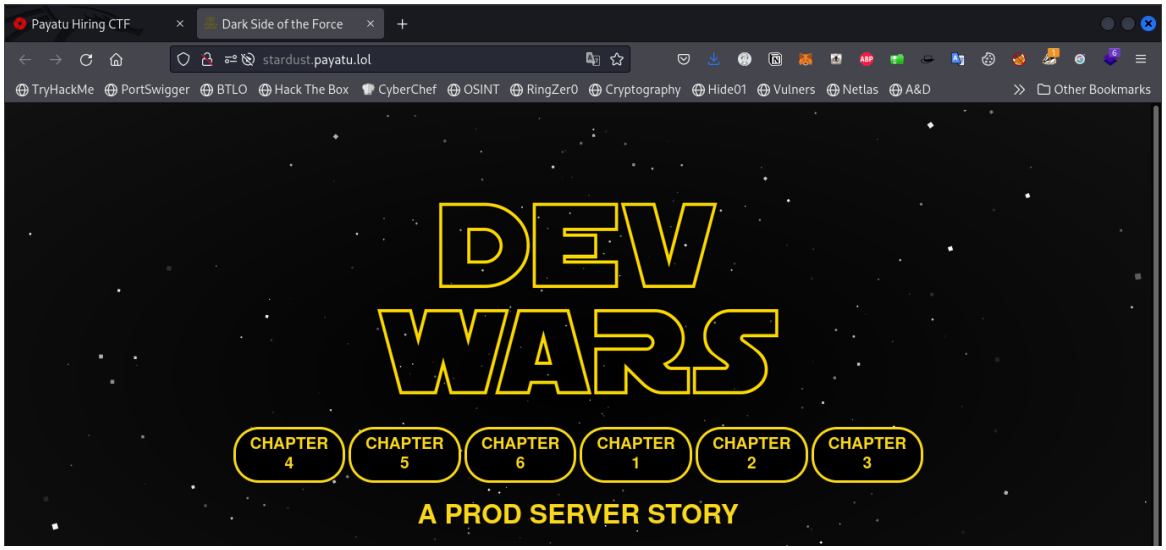
WEB challenges

1. Stardust



This was a SSTI (server side template injection) attack based challenge where we had to render some malicious output into the template via concatenation and then execute it on the server side.

On opening the link we found a Star Wars parody page



On opening any chapter I noticed the URL of the page which was something like this:

http://stardust.payatu.lol/chapter?episode=a+new+hope

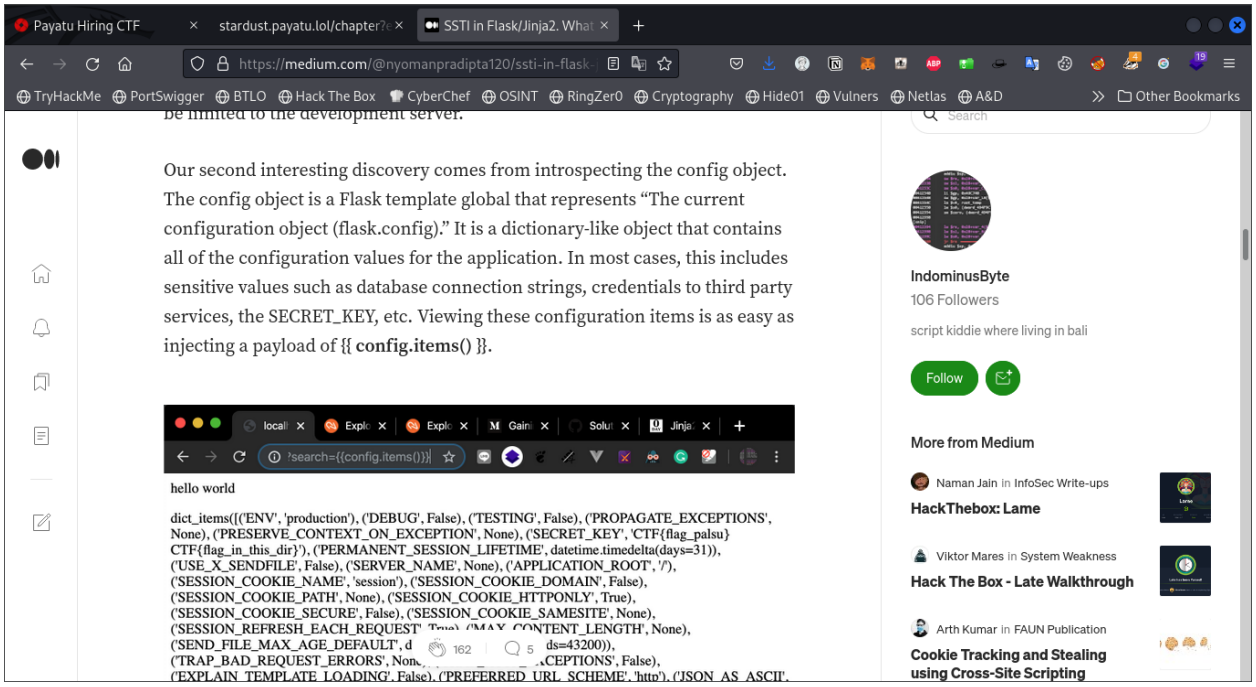
http://stardust.payatu.lol/chapter?episode=the+firewall+strikes+back

It occurred to me to check the rendering of {(7*7)} after the episode to render the result.

Upon receiving 49 as a result my hunch was correct and I went for the attack.

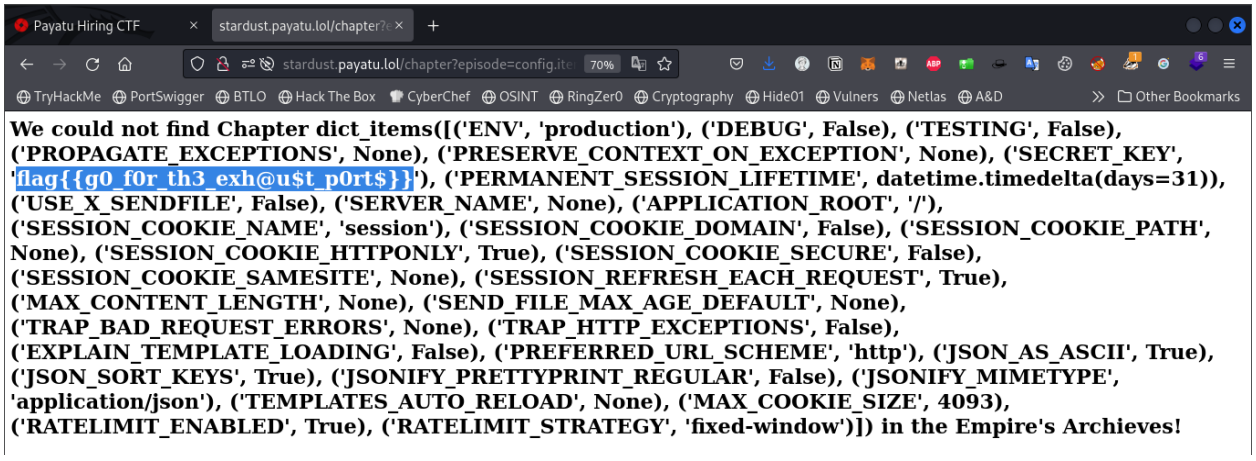
I used the payload available on medium

(https://medium.com/@nyomanpradipta120/ssti-in-flask-jinja2-20b068fdaeee):

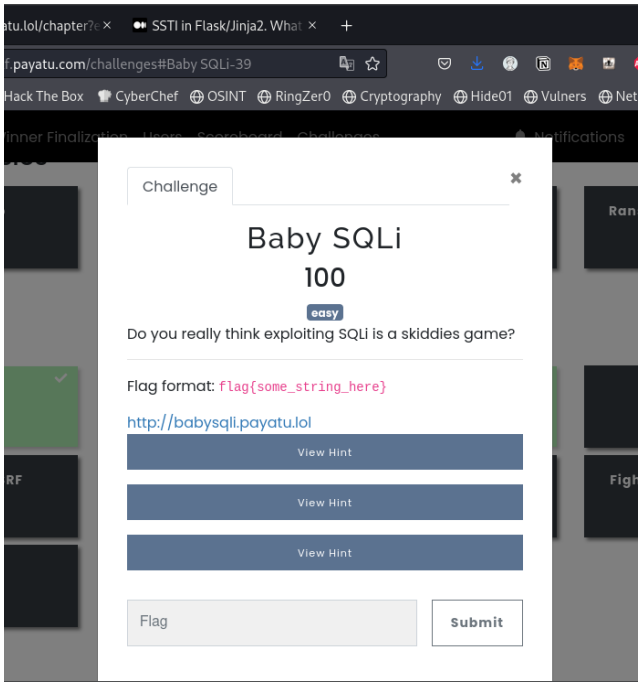


Since during the flask rendering was clearly looking for a chapter named 7*7 which equals 49. We can then search for configuration of items too.

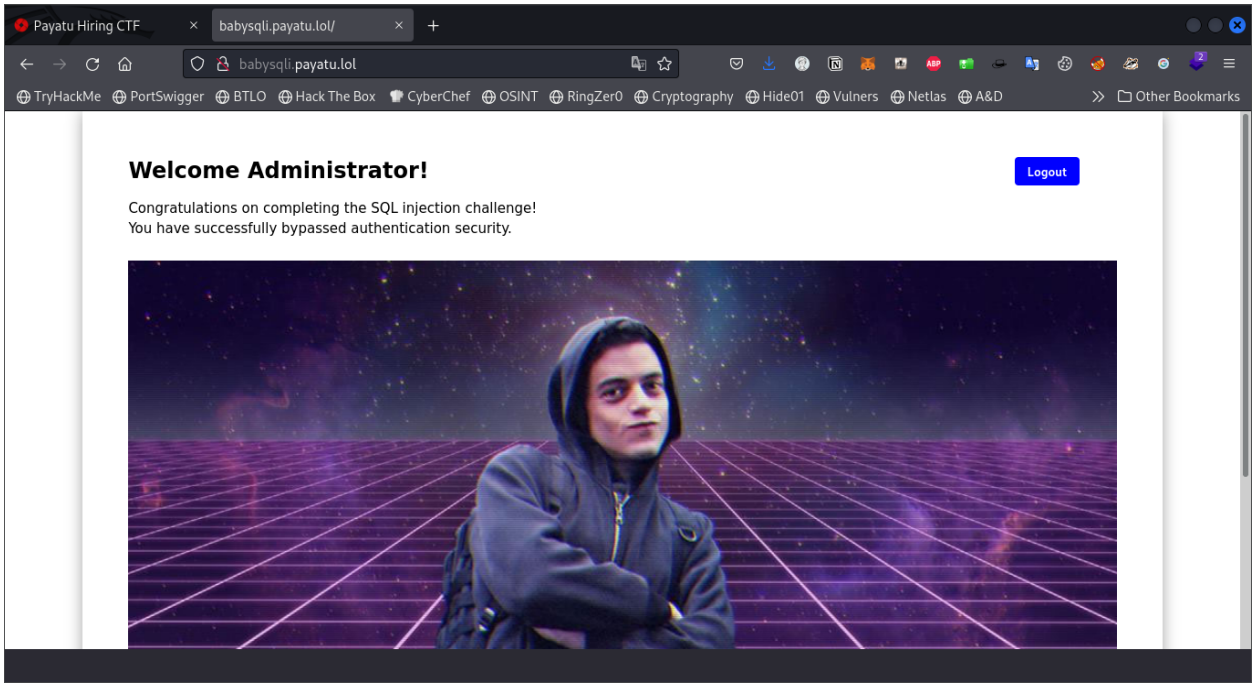
http://stardust.payatu.lol/chapter?episode=config.items()



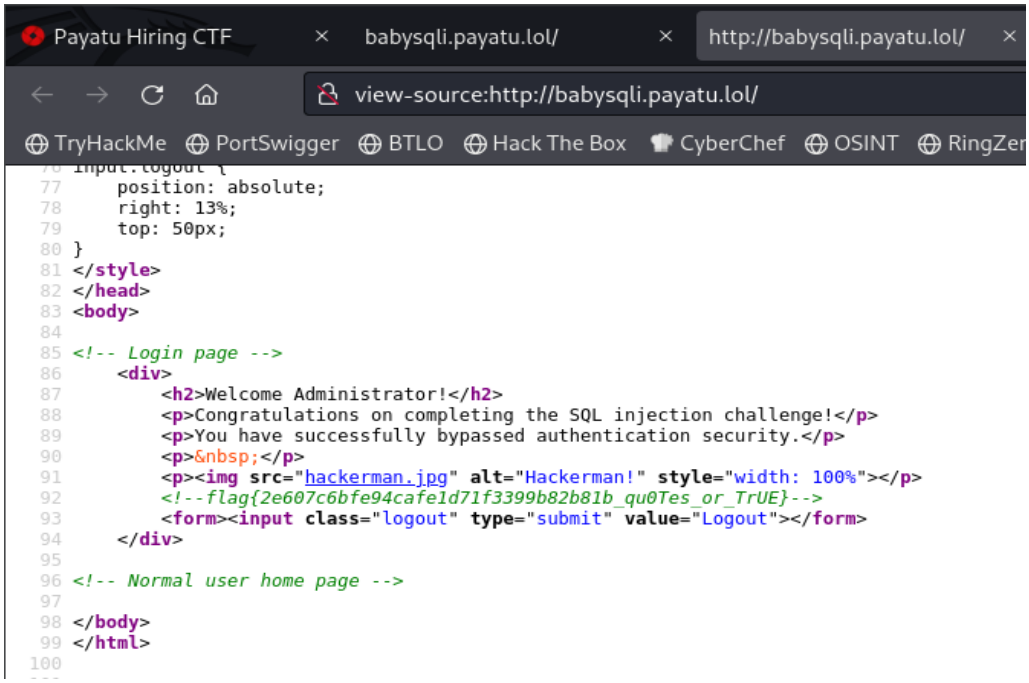
2. Baby SQLi



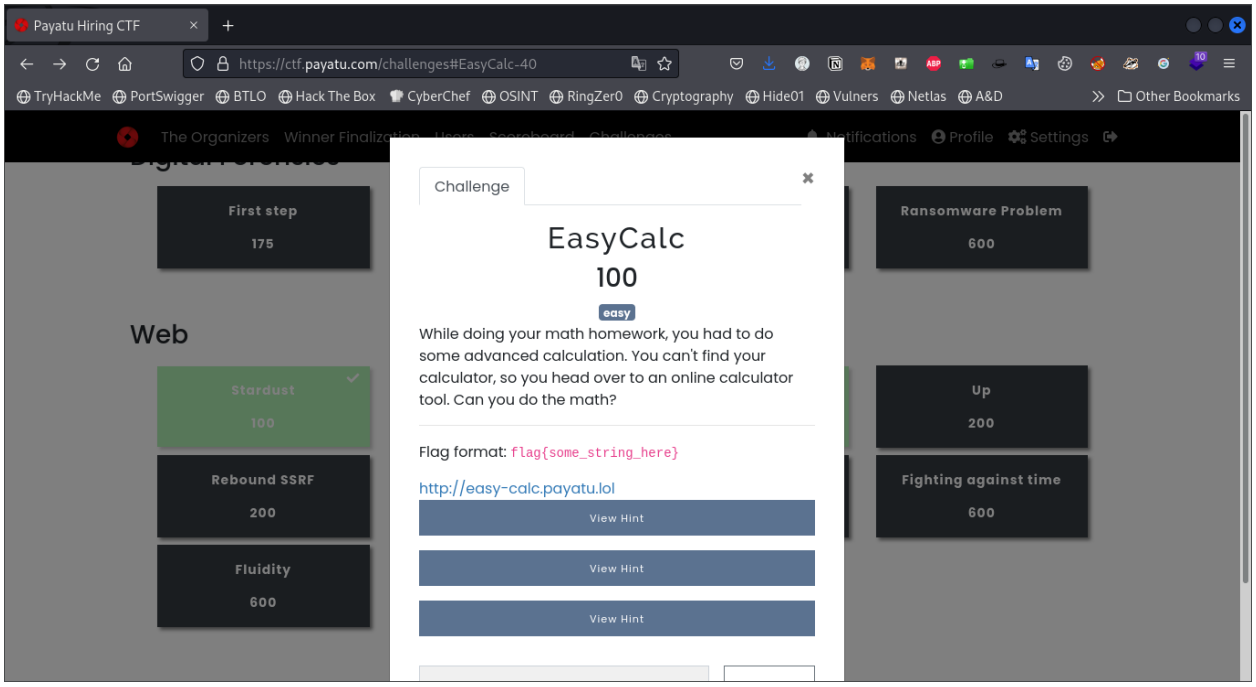
This was a simple SQLi challenge. Upon opening we find a login page. So I tried the infamous **x'or'x'='x** query which did not work, and everytime it would return saying incorrect username, when I decided to leave the username blank and go for the password only. I used **"or""="** as the payload and there was a successful login.



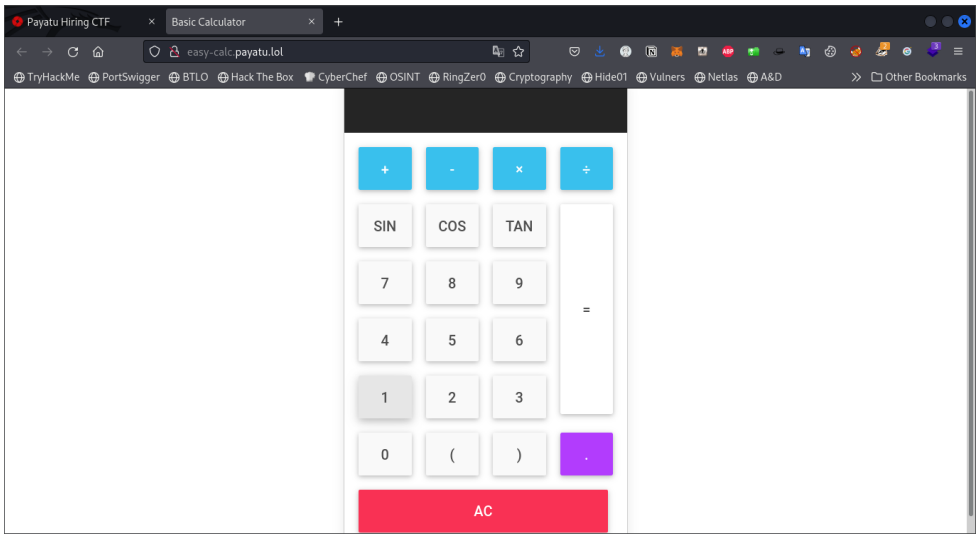
Upon Inspecting html code I got the flag for this challenge.



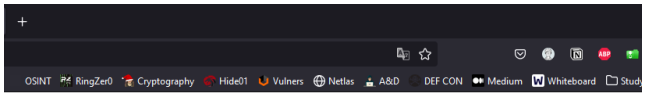
3. EasyCalc

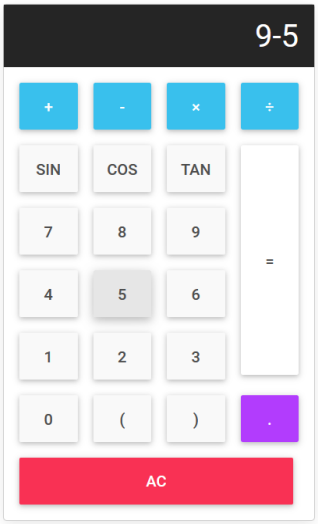


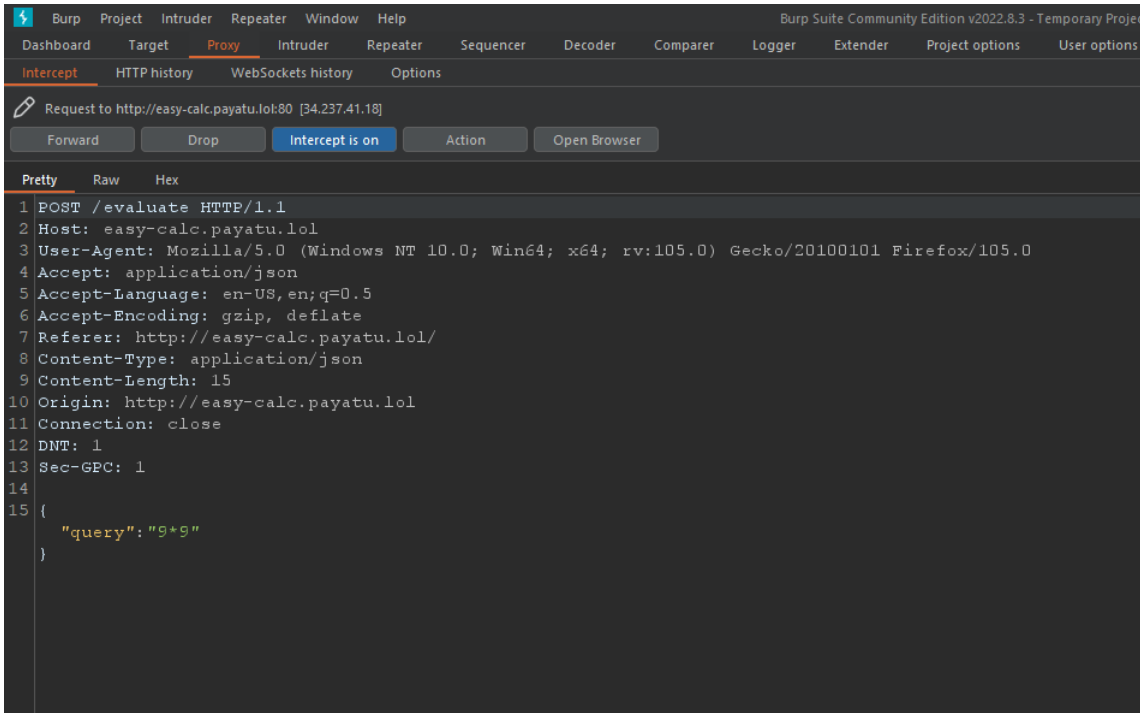
This was a calculator challenge where we had to modify the POST request to a payload which would then return us the flag. There was also a video of John Hammond on a similar CTF walkthrough that I remembered, where he used Burpsuite to modify the request.



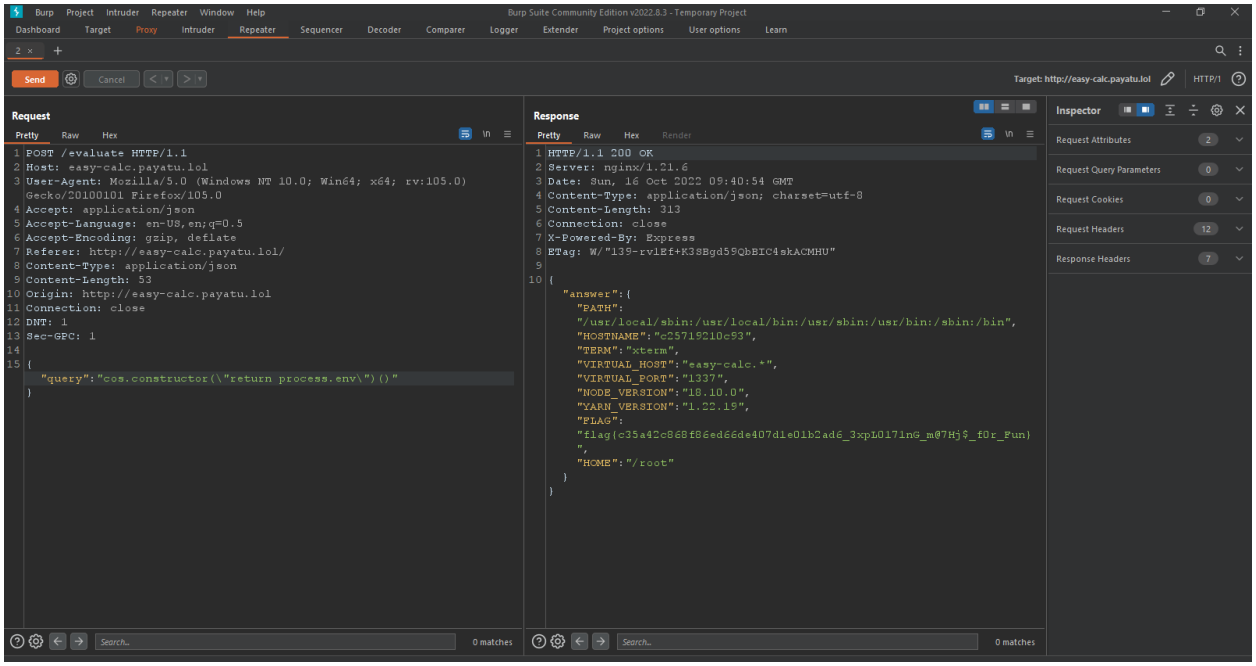
So I fired up Burpsuite and intercepted the traffic.







Sent the request to the repeater and found a payload on the internet **cos.constructor(\"return process.env\")()** to send as a POST request.

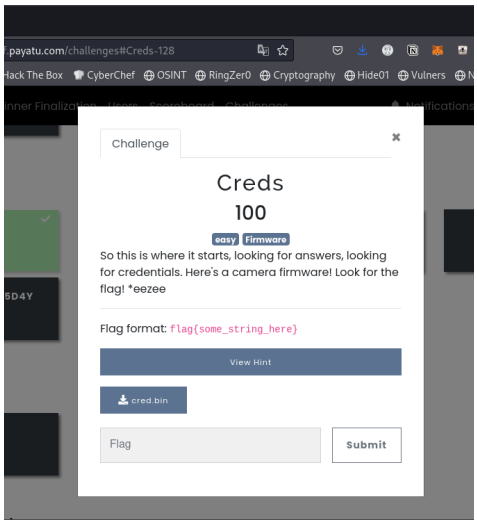


Where I found the flag

flag{c35a42c868f86ed66de407d1e01b2ad6_3xpL0171nG_m@7Hj$_f0r_Fun}

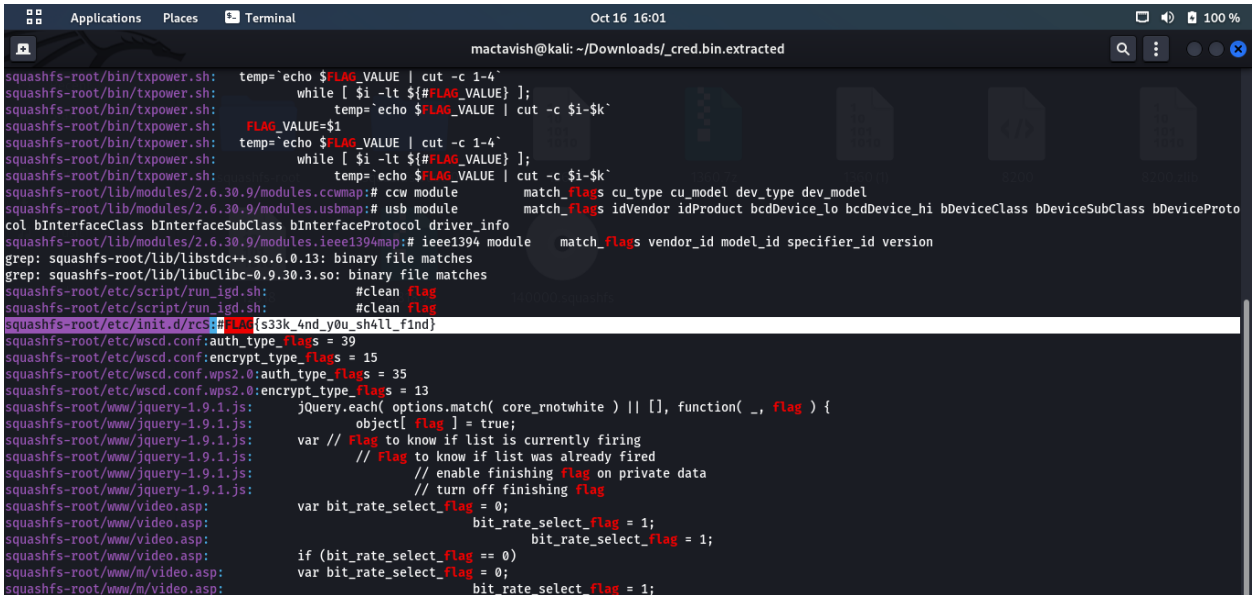
IoT challenges

1. Creds

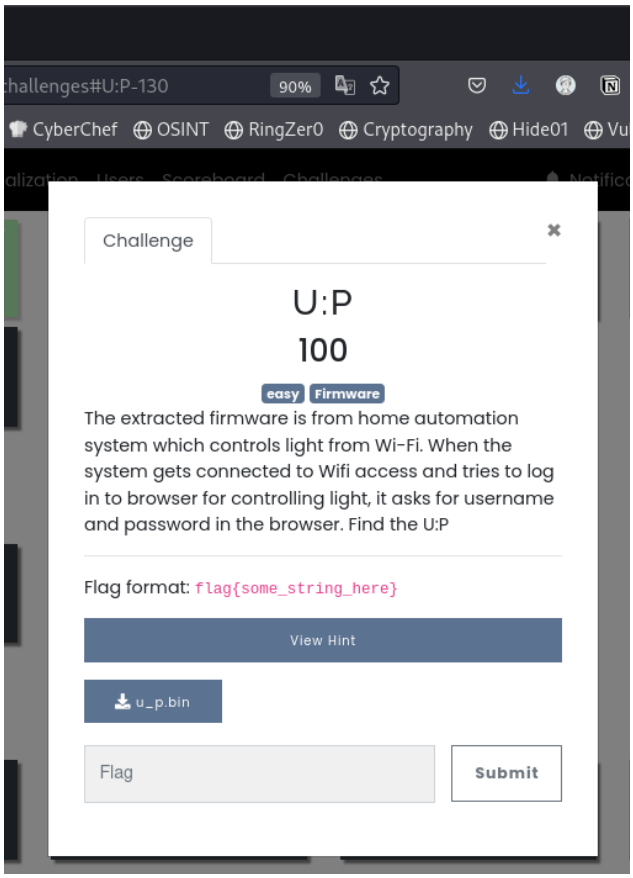


Here in this challenge we are given a firmware and we need to look for the flag which is deemed to be *eezee and it was

Just download the bin file and binwalk extract it for the firmware using **binwalk -e cred.bin**. Next just get inside the folder and **grep -ir flag**

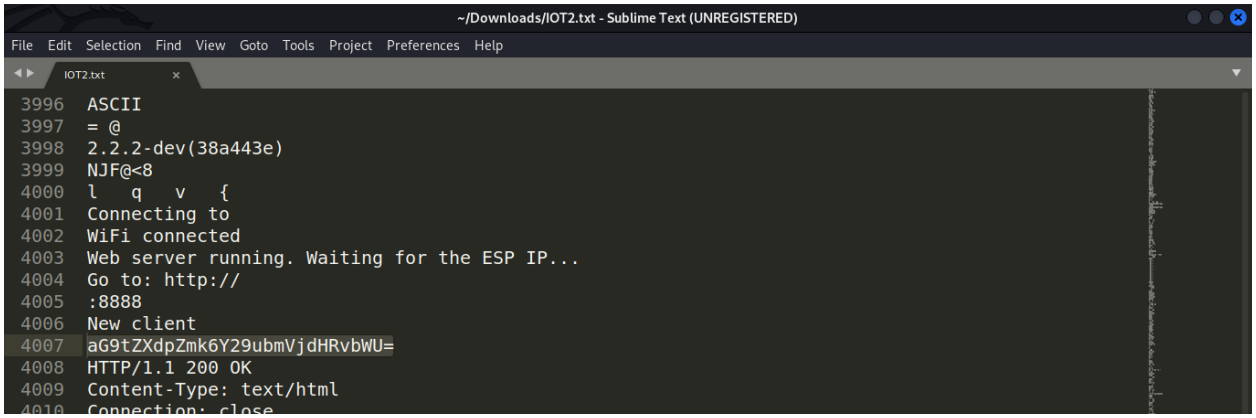


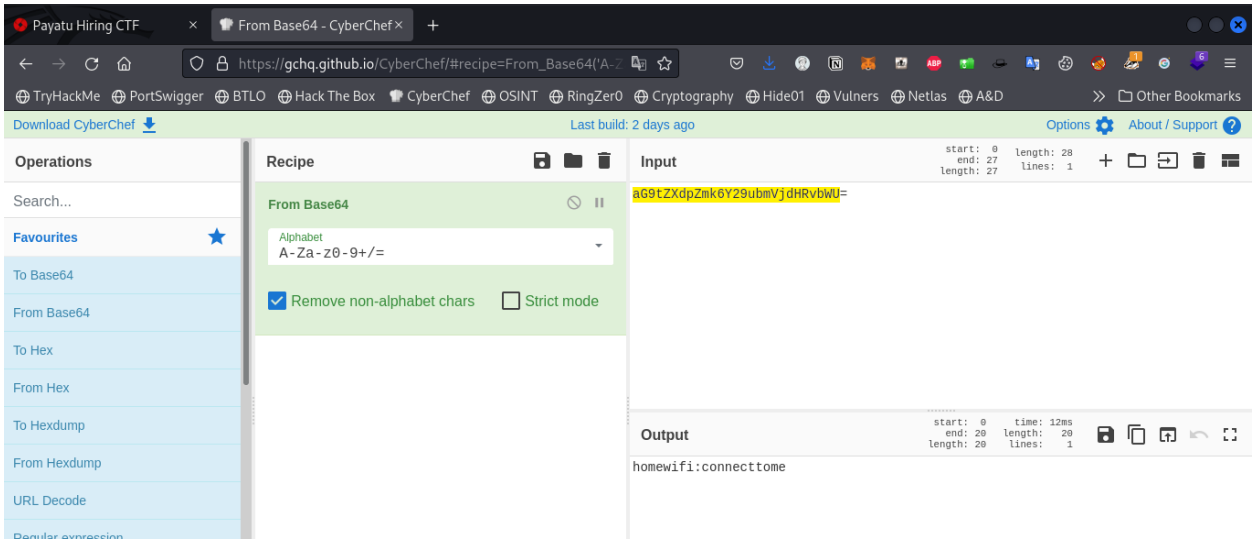
2. U:P



For this challenge we are given a binary file from where we are asked to extract userID and

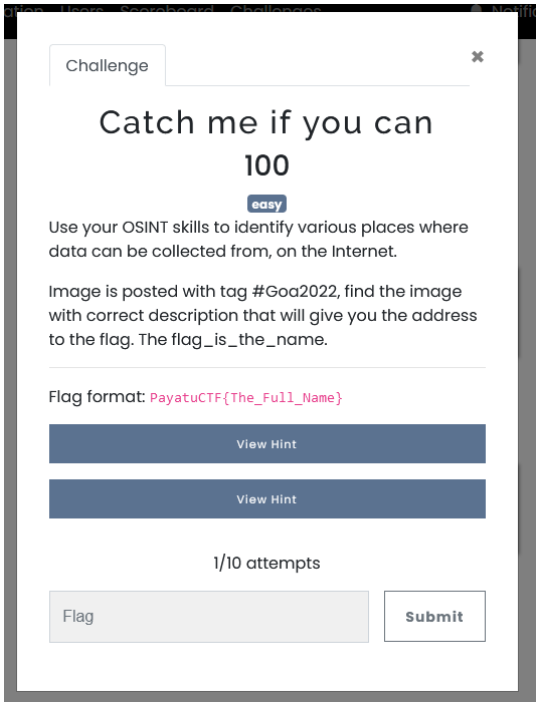
Password of a router. So after downloading the bin file I applied strings on the bin file and searching through the text at line 4007 I got a base 64 text which was the flag.



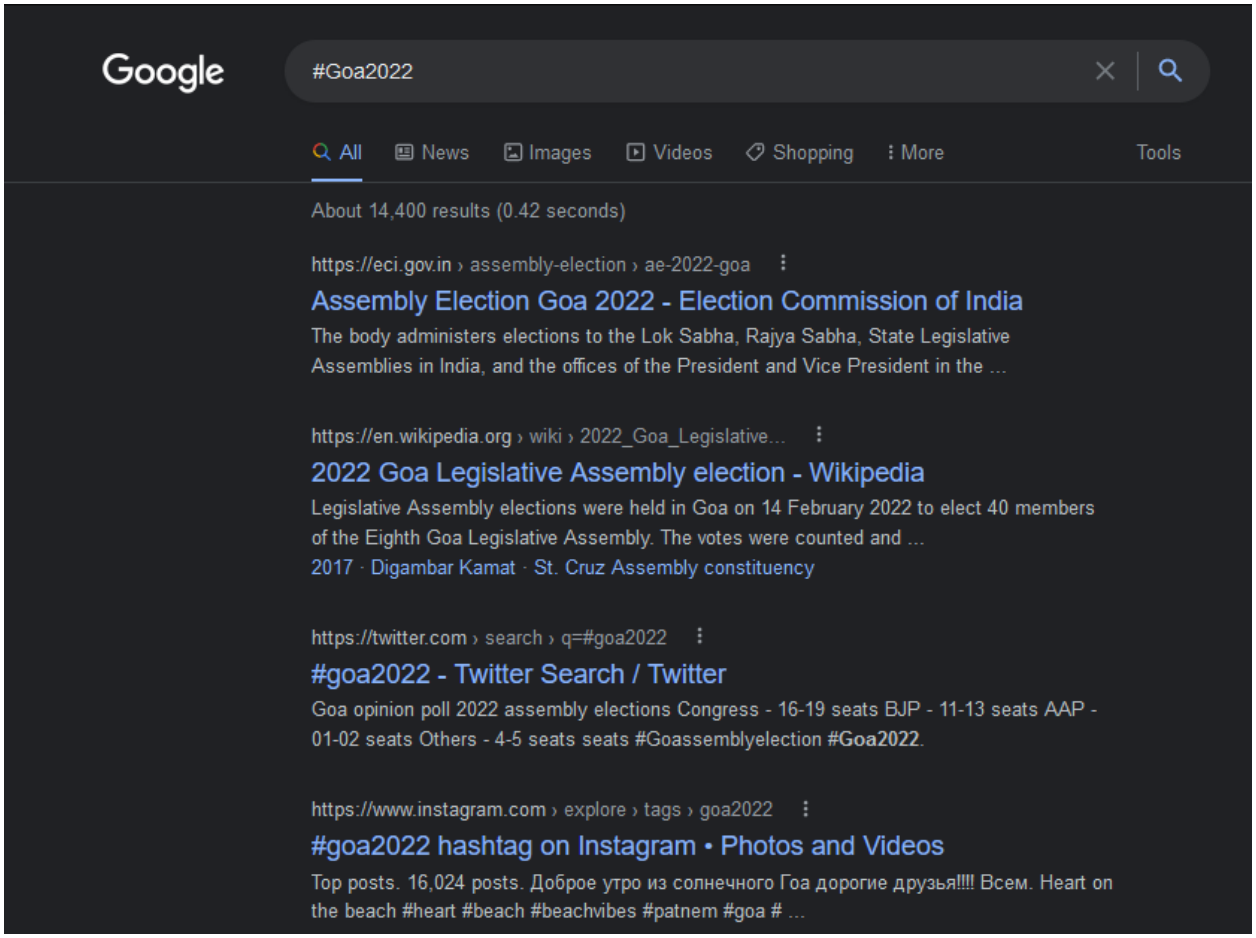


OSINT challenges

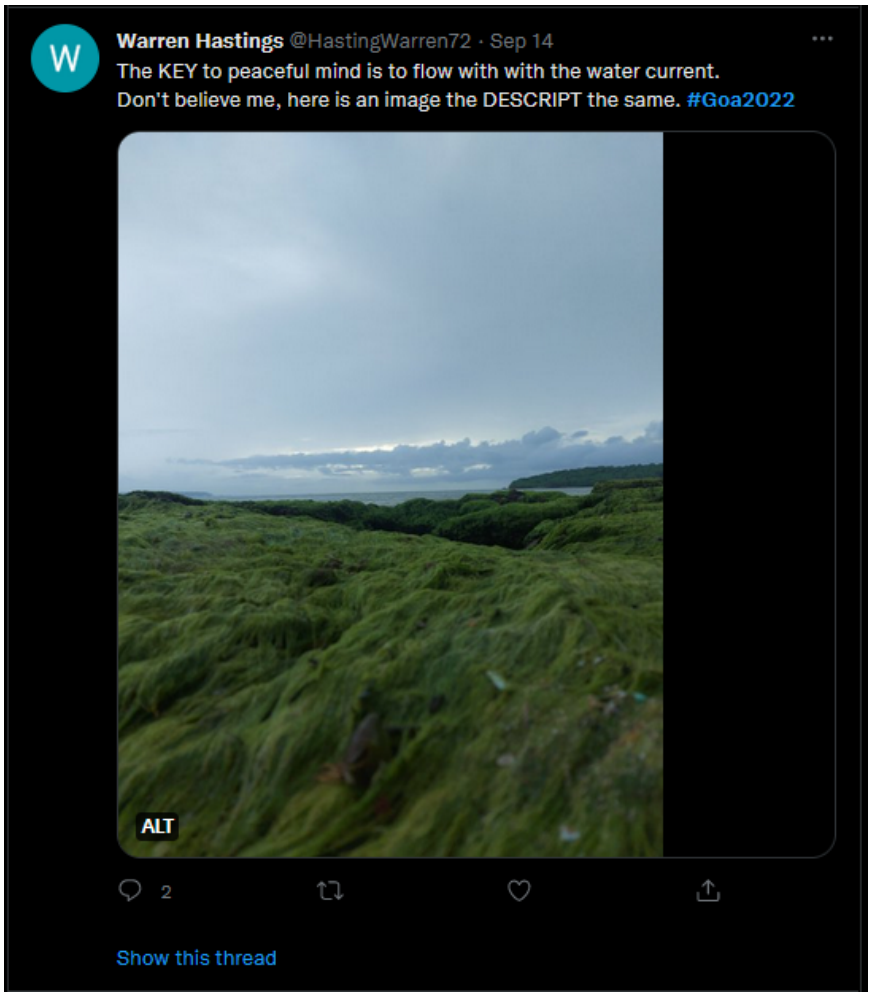
1. Catch me if you can



In this challenge I was given a hashtag #Goa2022 and was to find an image with the correct description. Since I was given a hashtag I immediately opened up instagram hoping to find something but Nullcon 2022 was held in Goa with a ton of potential images and none matched the description. I then tried to Google it instead and found that there were twitter results too.



And then surfing through posts a suspicious post hit me. It was also pointing to the description. So I tried to exif the image and binwalk it but no results until I clicked the **alt** button and got a coordinate.


Warren Hastings @HastingWarren72 · Sep 14
The KEY to peaceful mind is to flow with with the water current.
Don't believe me, here is an image the DESCRIPT the same. #Goa2022
ALT
2
Show this thread

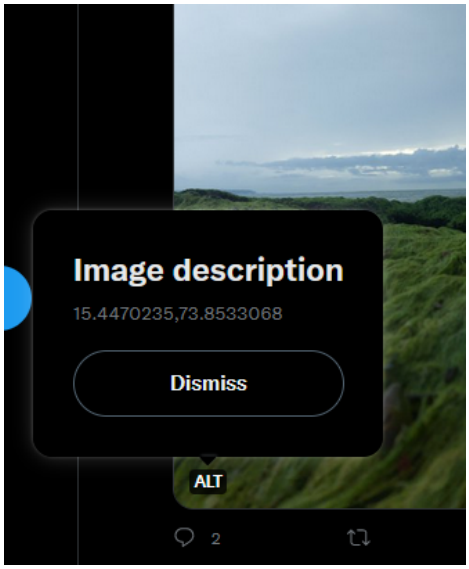
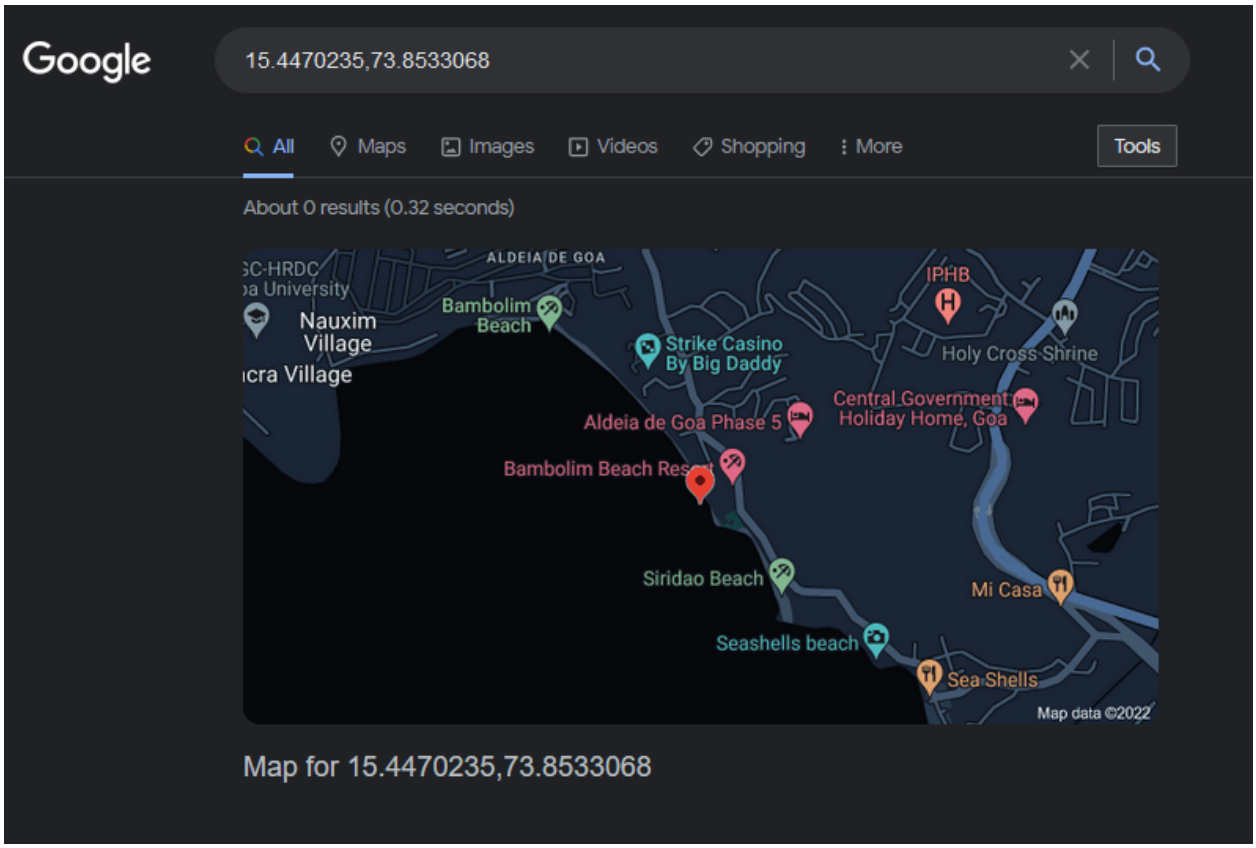


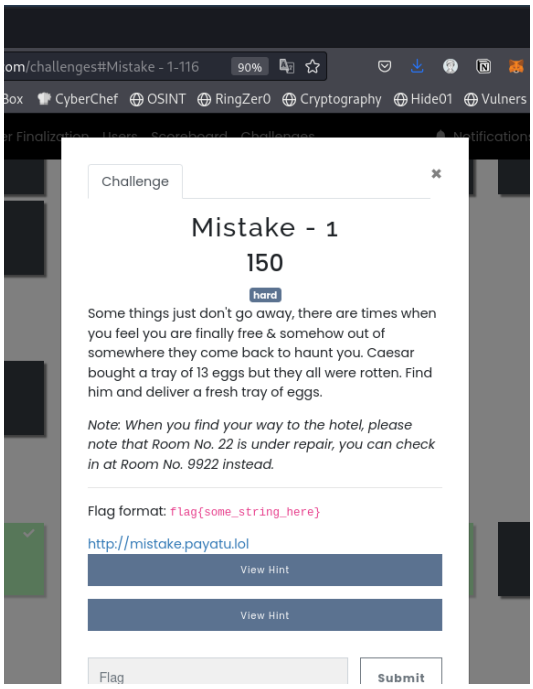
Image description
15.4470235,73.8533068
Dismiss
ALT
2

A general search on Google gave me the name of a resort in Goa and that was the flag value.



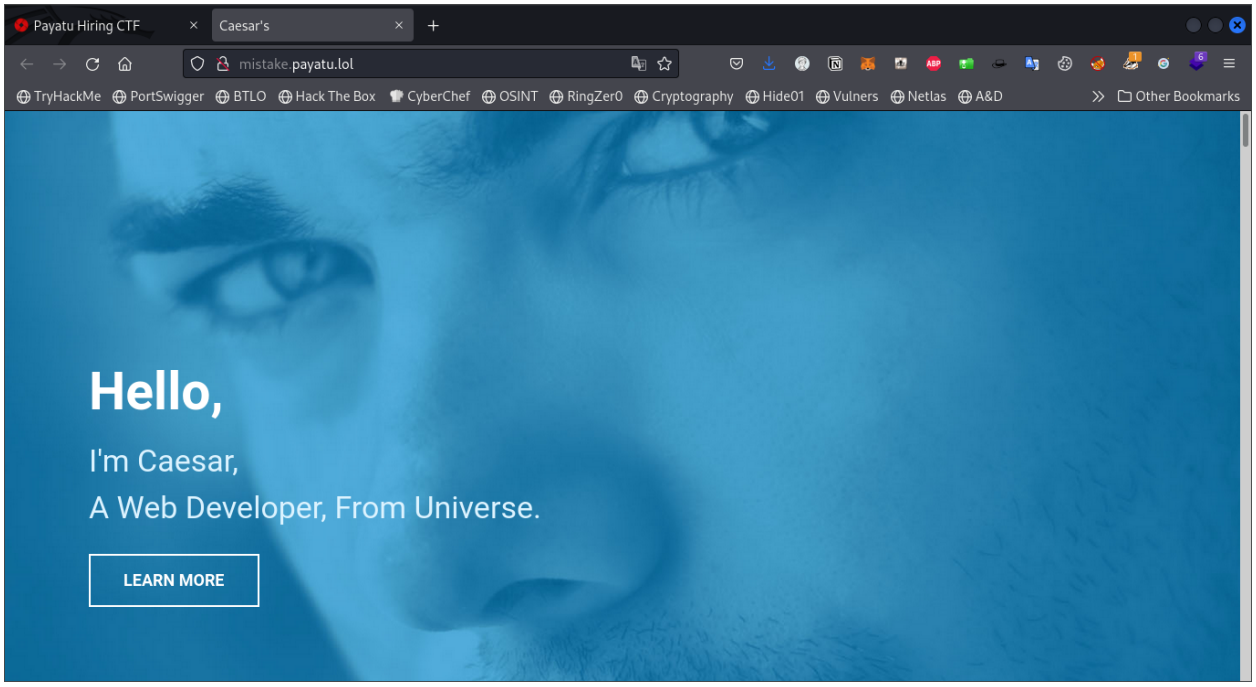
Network challenges

1. Mistake - 1

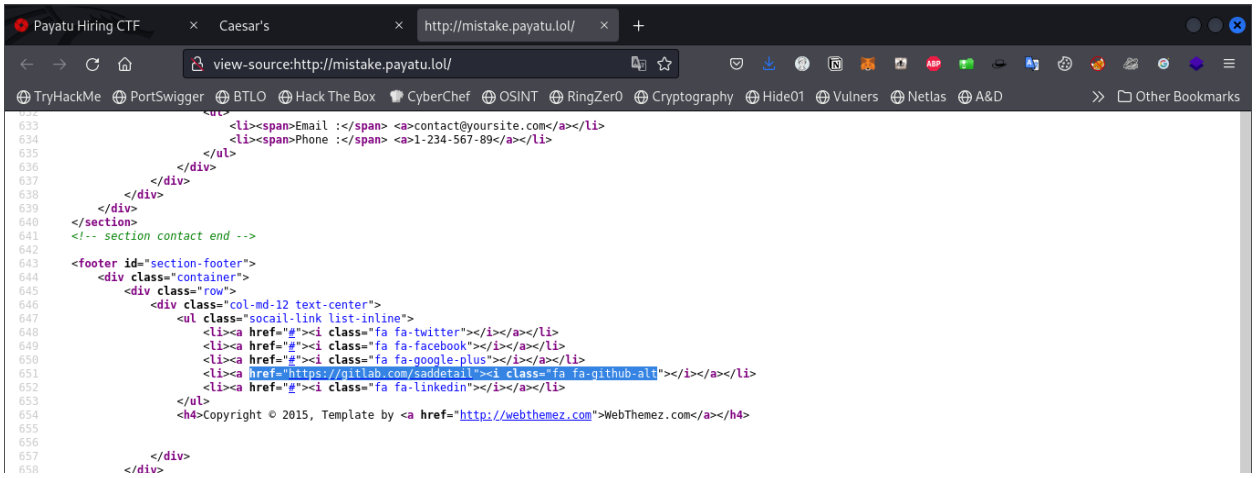


This challenge got me hinted to a ROT13 text where as per description I was searching for ROT13 text.

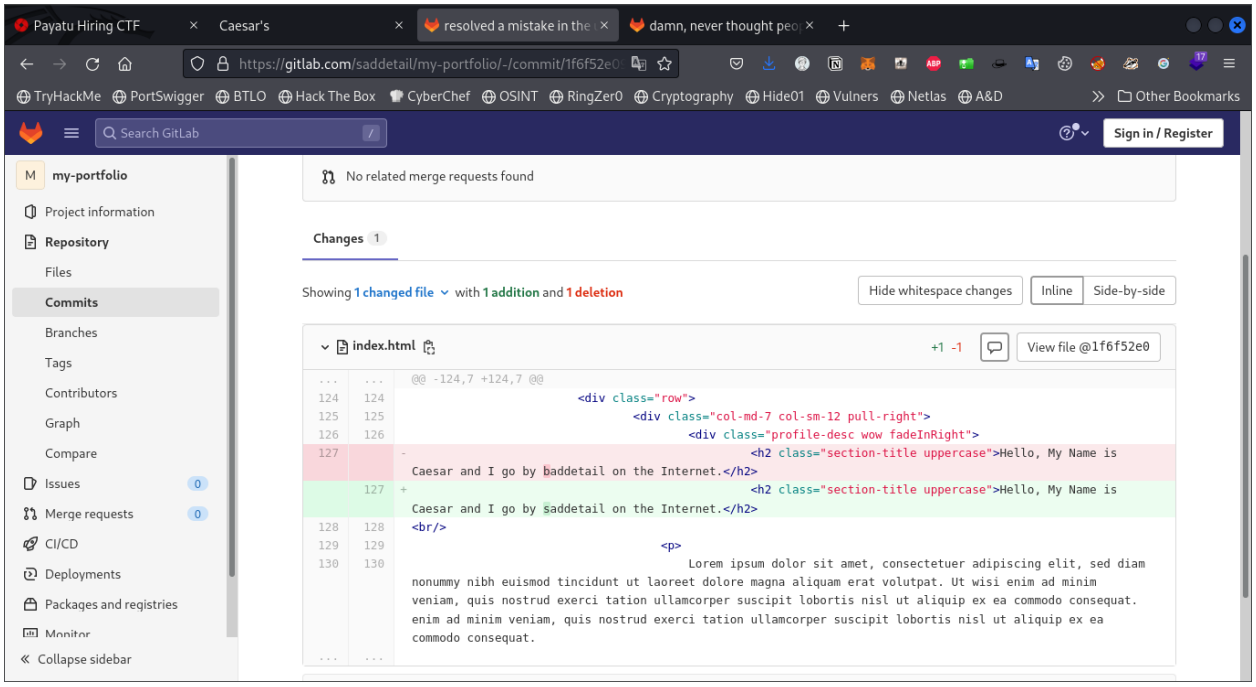
The objective was this challenge was to get into a machine using port 9922 which was running **ssh** as per **nmap** scan. We had to find the username and password.

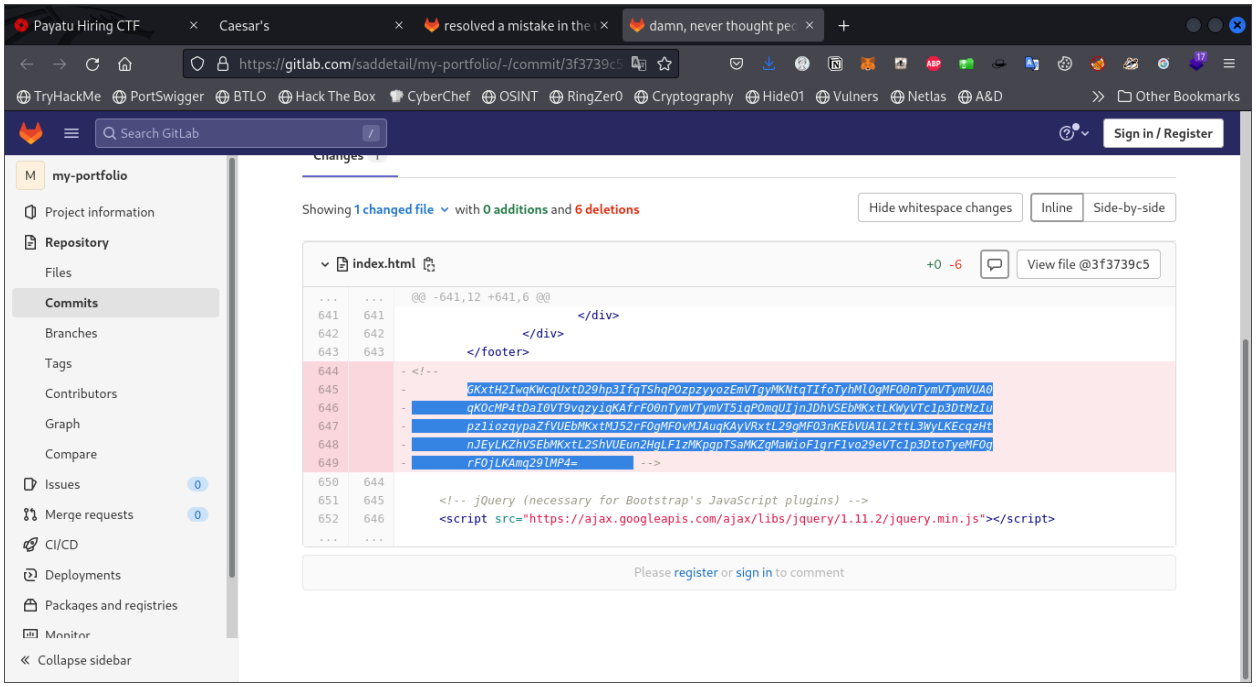


The website had a gitlab repo which was worth digging into.

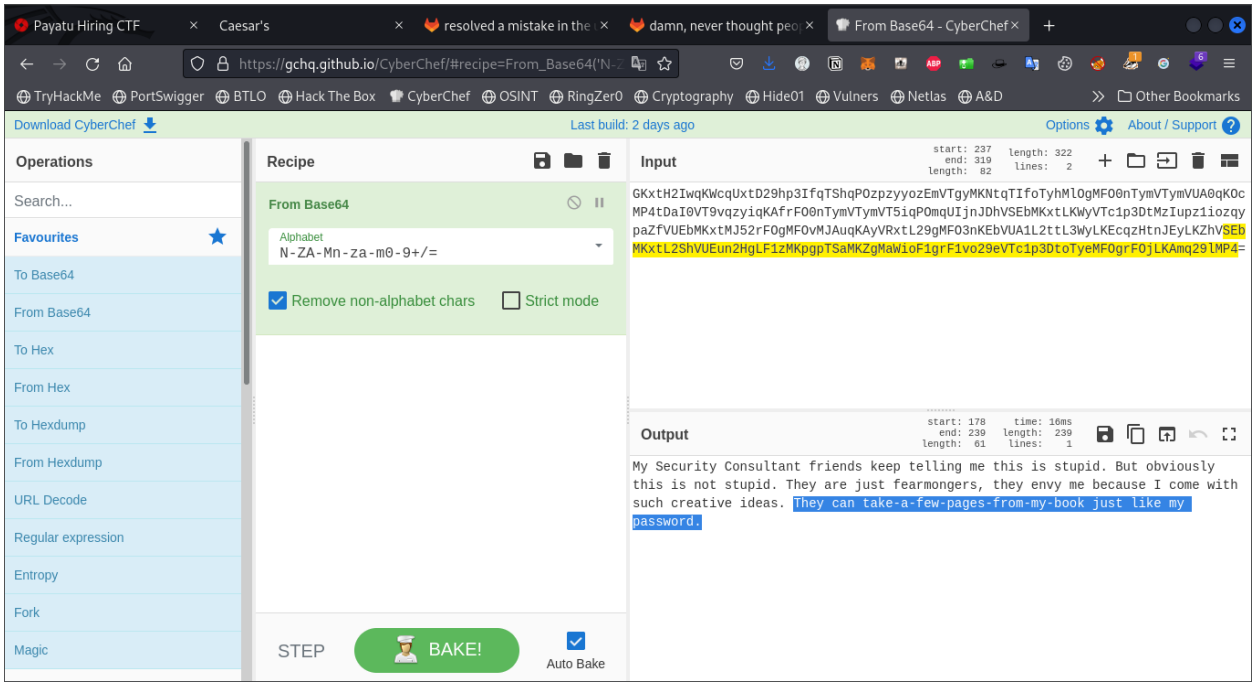


Upon opening the repo I saw some commits and got to know that the username was **saddetail** but the password was unknown until I found the ROT13 cipher text.



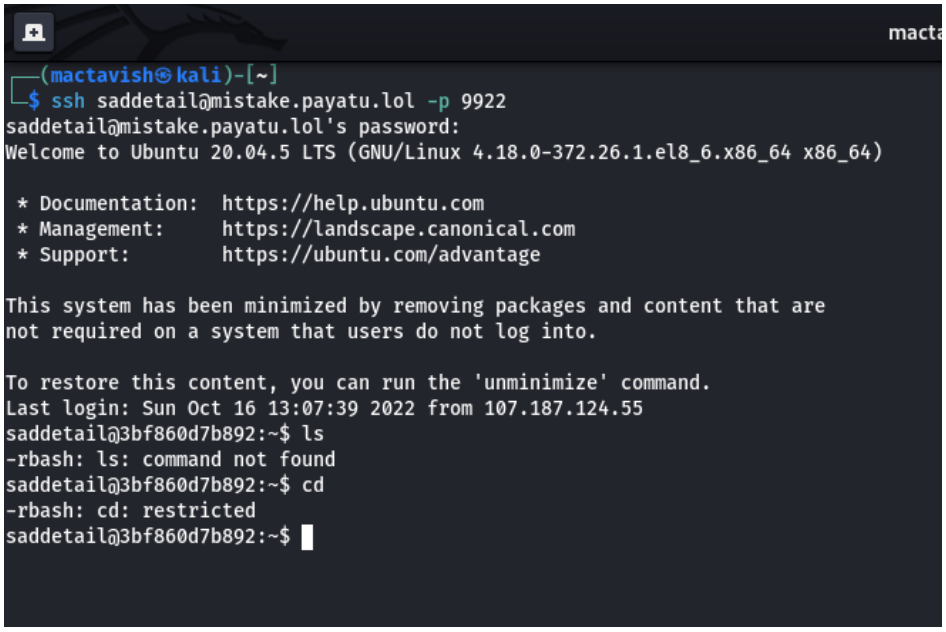


Upon translating it we found the password



We got the password to be **take-a-few-pages-from-my-book**.

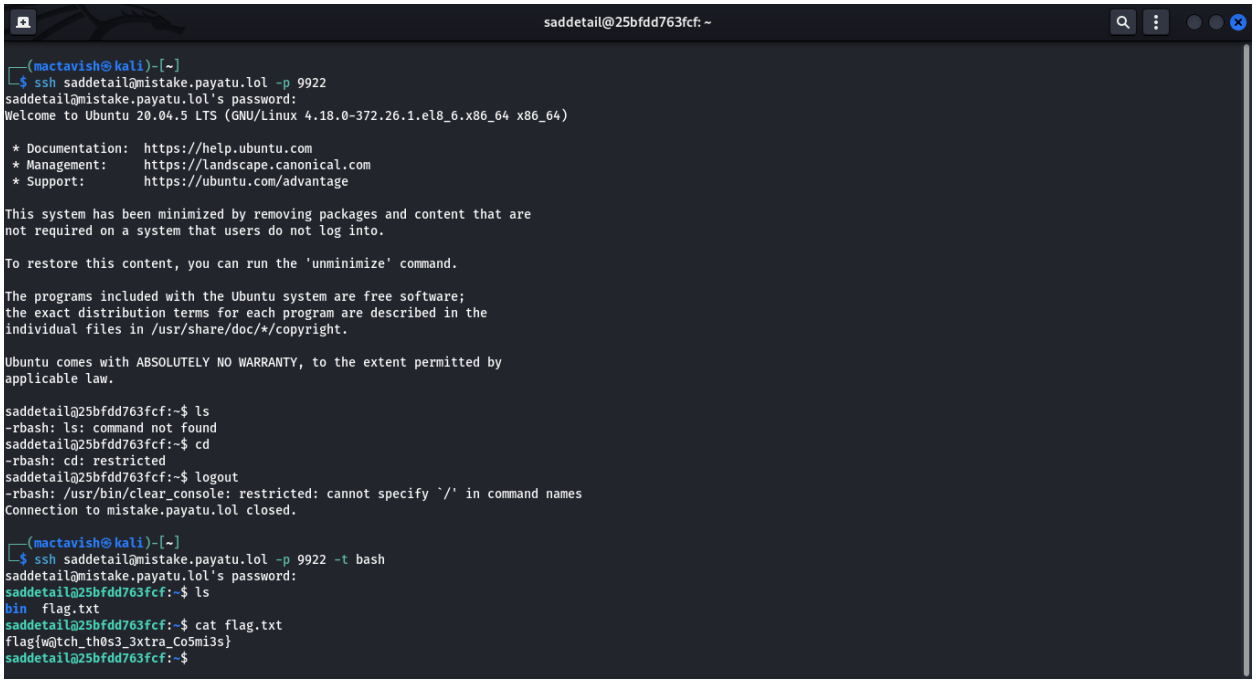
So that now we have Username and Password let's go for the ssh.



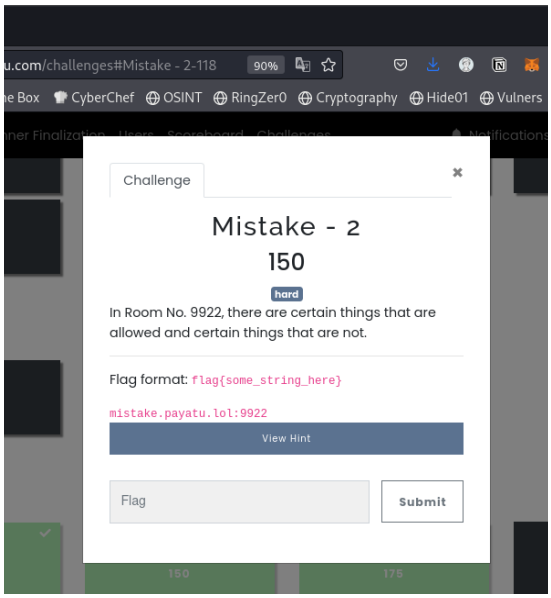
This machine was using rbash. Restricted bash or rbash doesn't allow all commands to run.

So I used the oldest hack in the manual to escape the restriction using **-t bash**

And now I have an interactive shell and the flag.



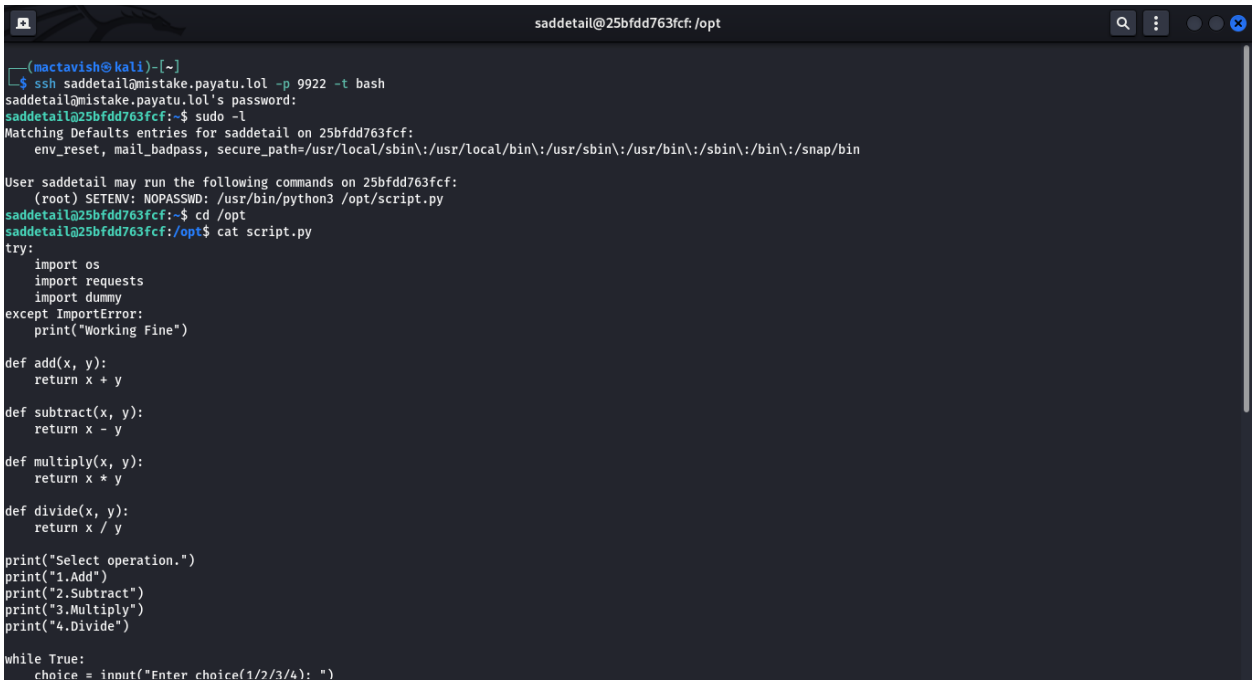
2. Mistake - 2



This is the second part of the previous challenge where we need to become root.

I used sudo -l to check what can we run as root using sudo

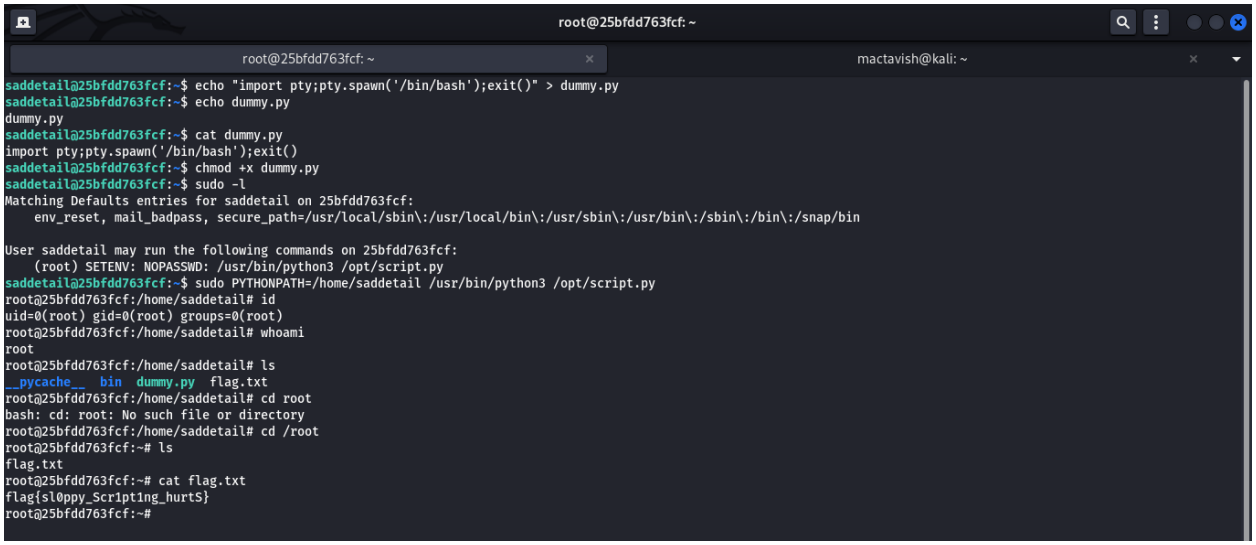
And we got this output. Traversing to this path and cat the contents we see that it is a simple calculator app using python.



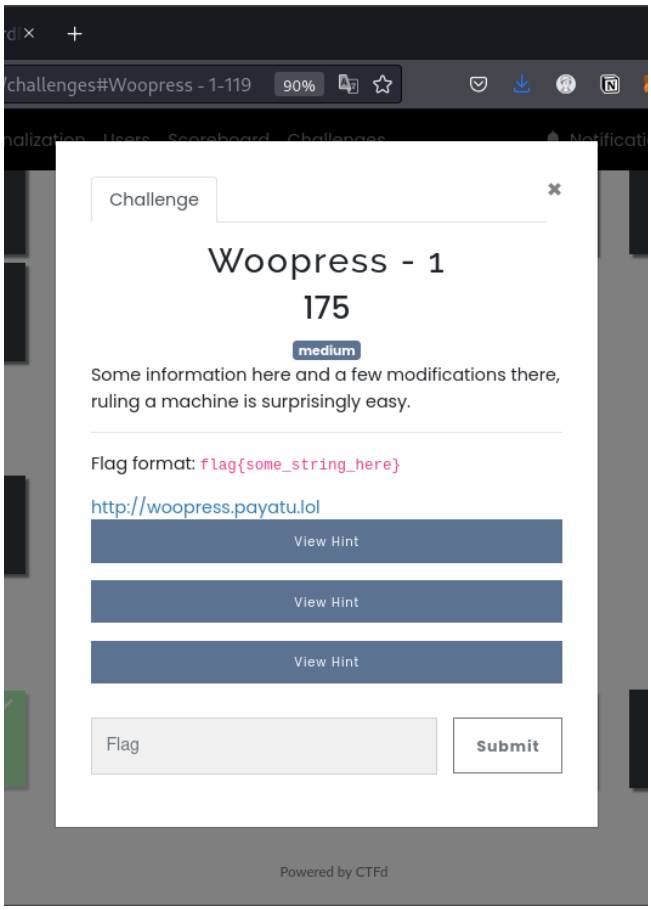
After this I saw a module as dummy which was being imported. So it was time for me to perform Python lib hijacking. Using **gtfo bins** i used the pty spawn shell command.

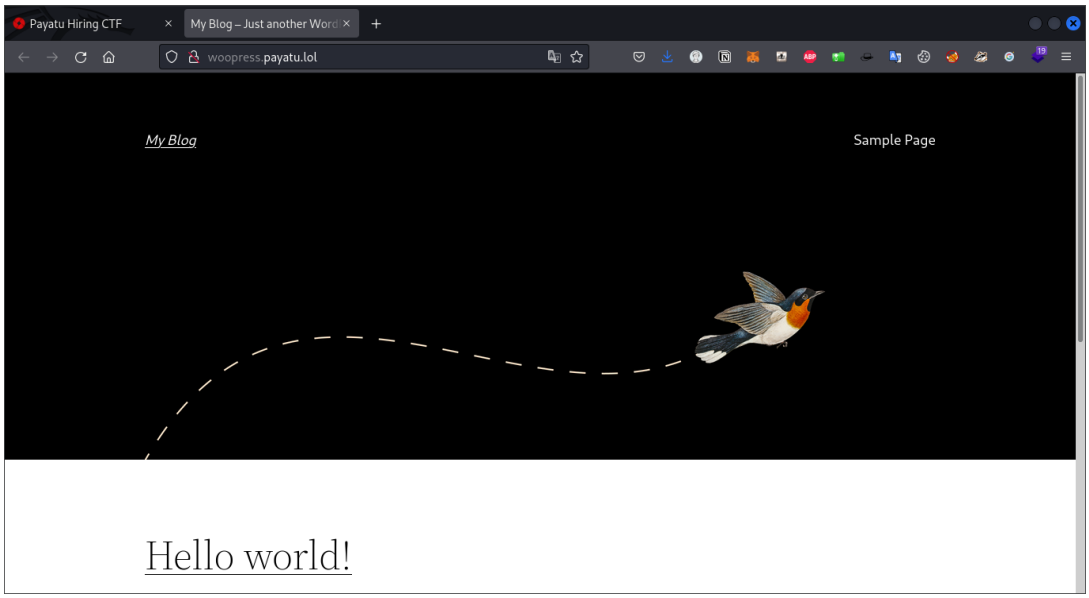
import pty;pty.spawn('/bin/bash');exit()

And then ran the calculator app which in turn imported the module that I crafted as dummy. And now I am root and have the flag as well.

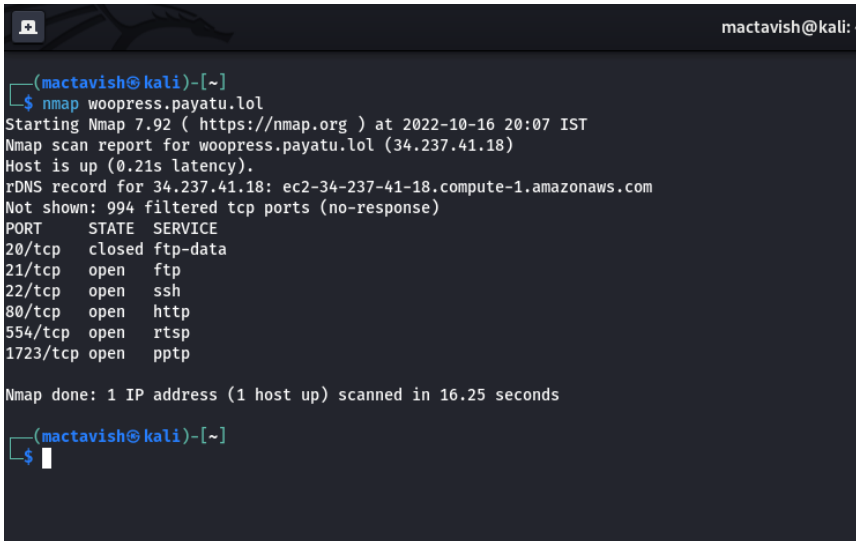


3. Woopress - 1

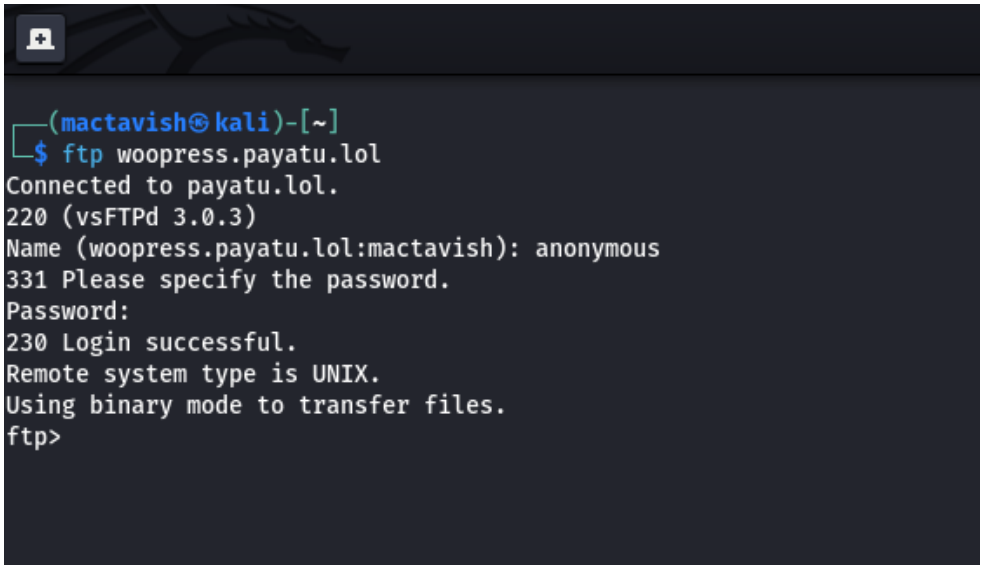

challenges#Woopress - 1-119
90%
Challenge
Woopress - 1
175
medium
Some information here and a few modifications there, ruling a machine is surprisingly easy.
Flag format: flag{some_string_here}
http://woopress.payatu.lol
View Hint
View Hint
View Hint
Flag
Submit
Powered by CTFd


Payatu Hiring CTF
My Blog – Just another Word
woopress.payatu.lol
My Blog
Sample Page
Hello world!

This machine surprisingly had a lot of ports open

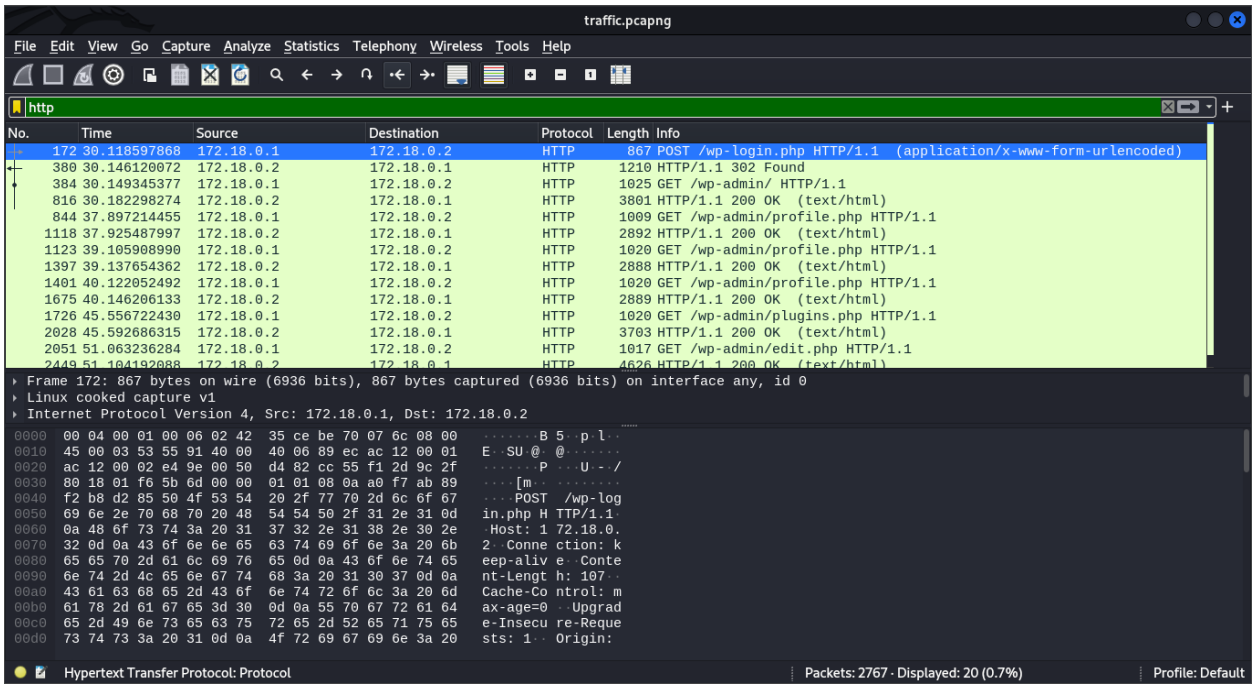


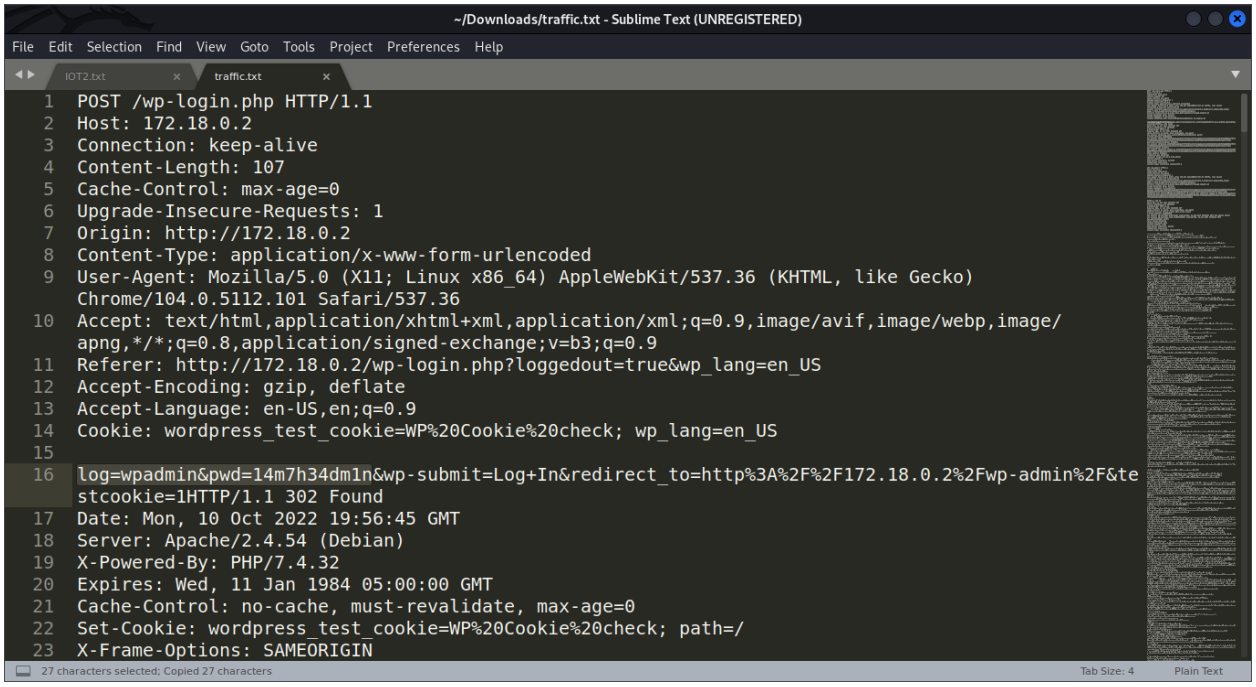
I first tried anonymous login on the ftp server



But it was in passive mode which can be turned off using binary mode and then passive off where we can find a pcap file and download that.

Analyzing the pcap file I had a lot of options to play with finally when I started analyzing the HTTP filter and then saving the traffic to a text file we get something.





I found some login credentials. Keeping in mind that this is a wordpress site I started directory listing for a login page. Here we find a /wp-login subdomain.

(The instance was taken down by the time I was scanning. So I couldn't provide screenshots. But I'll be writing down the steps below.)

Using the username and password **wp-admin** and **14m7h34dm1n** we login to a wordpress dashboard. From here we can do 2 things. We can either upload a modified webshell as a template and activate it.

Or we can use https://github.com/rastating/wordpress-exploit-framework by https://github.com/bigb0sss and get our flag using traditional methods.