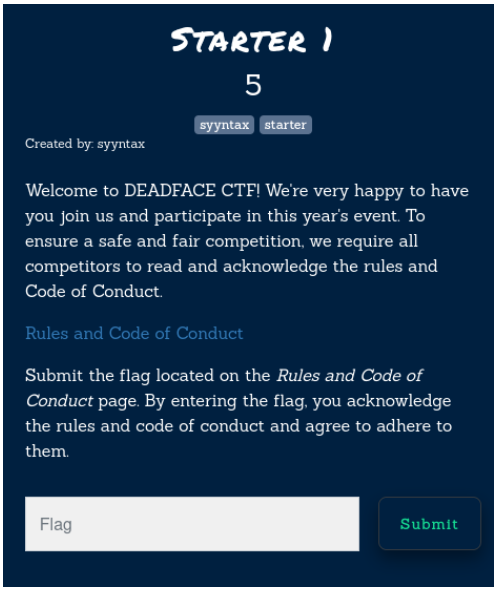
Deadface CTF 2023 writeup

Chall Url -> https://deadface.ctfd.io
Ctftime-url -> https://ctftime.org/event/2031

I will provide solutions with two categories (solved by me AND unsolved but should be solved)

First we have to solve Starter 1 then Starter 2 to access other challenges , if not challenges can't be seen!!!

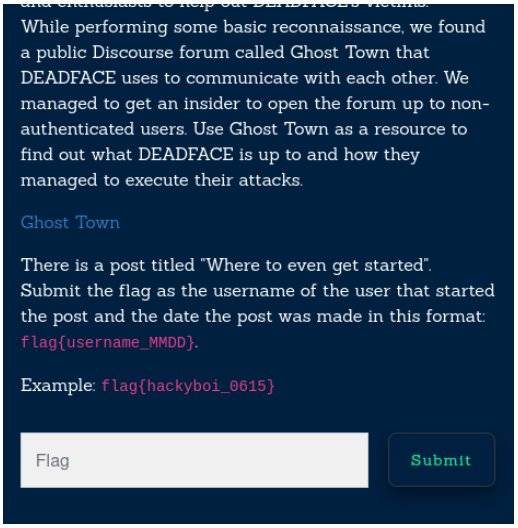
Starter 1 (5 pts)



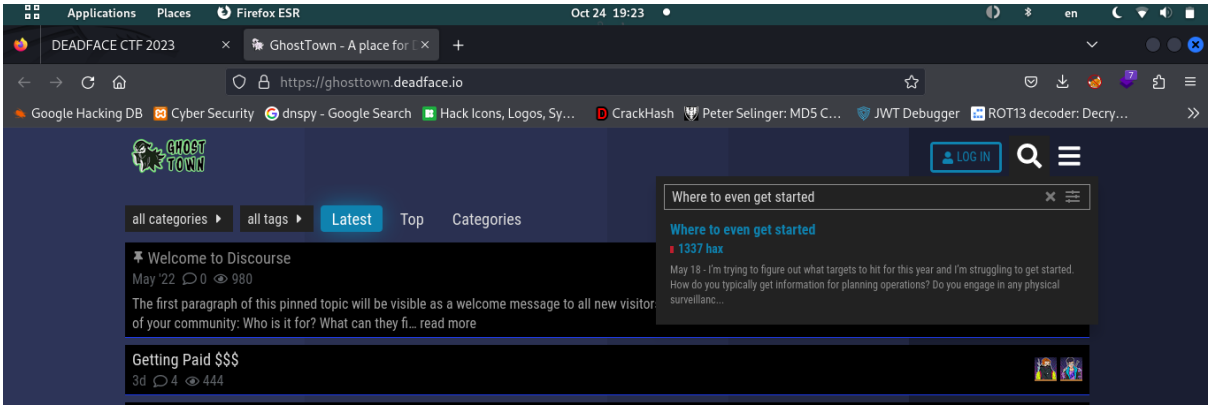
This challenge is ez af , we only need to read the rules via link "Rules and Code of Conduct" and the flag is at the end.

```
flag{I_acknowledge_the_rules}
```

Starter 2 (5 pts)



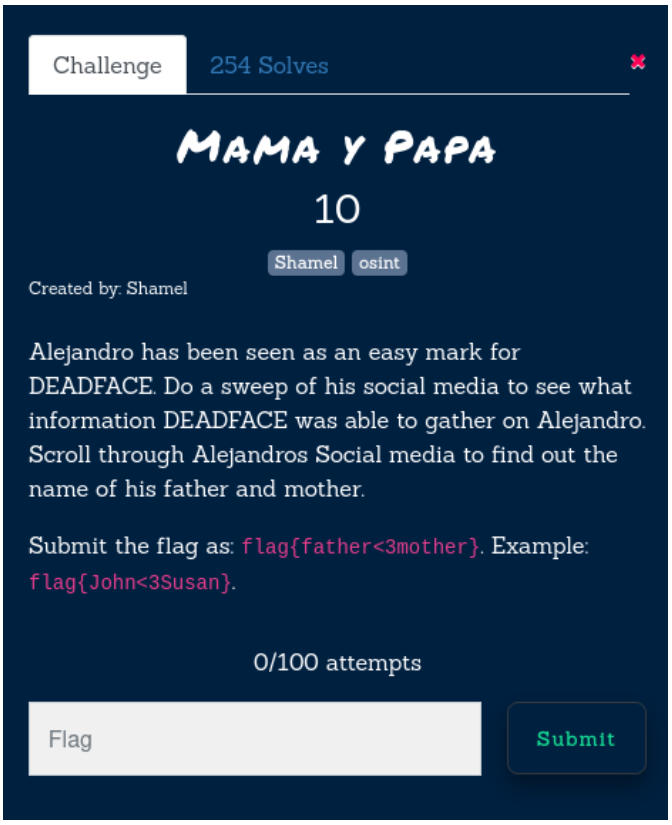
It's like OSINT category coz we have to find username and date from a website!
They provide us a website that u can go via Ghost Town (https://ghosttown.deadface.io) .
And I try to search with post title "Where to even get started" in searchbar.



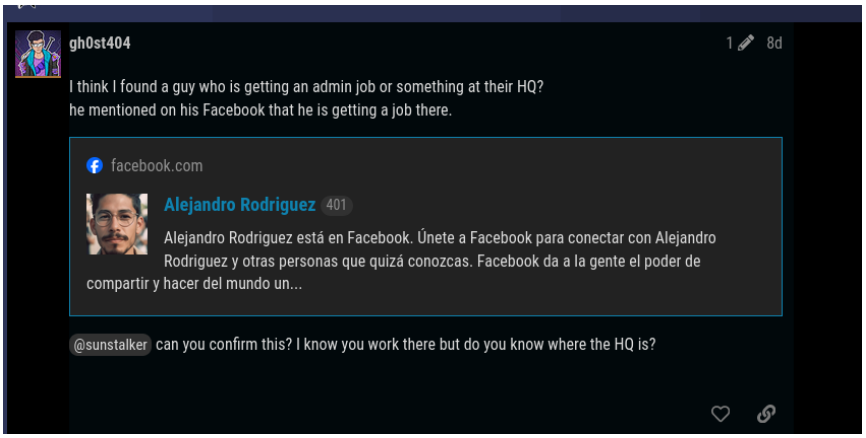
Username is daem0n AND posted date is May 18. So I put it in flag format .
flag{daem0n-0518}

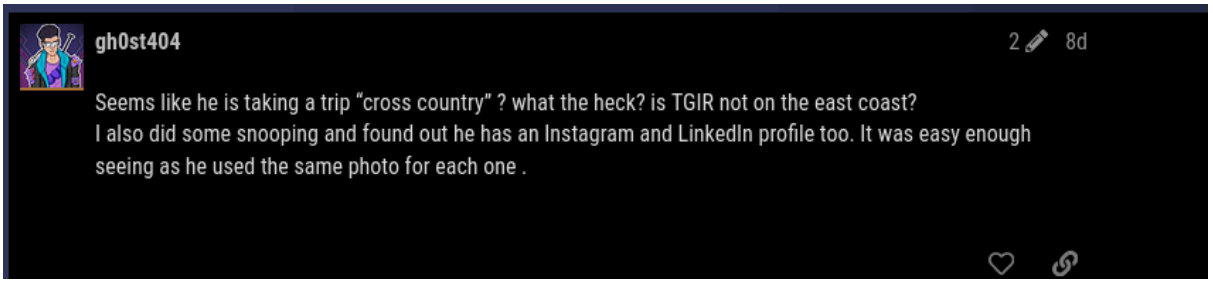
OSINT (Open-source intelligence)

Mama y Papa (10 pts) (unsolved)



This challenge is not ez for me, it took me like a day to solve although it's only 10pts.. First I tried to search "Alejandro" on their ghost town site https://ghosttown.deadface.io. I found a useful info!



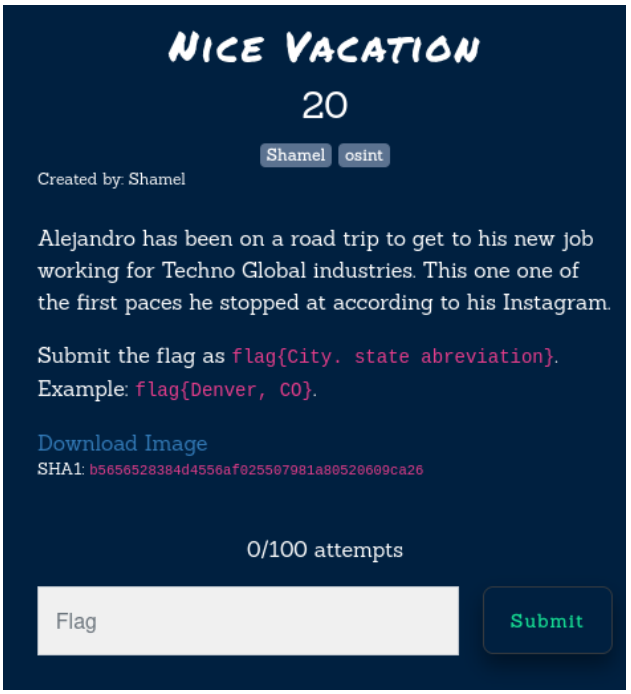


Ghost town post -> https://ghosttown.deadface.io/t/tgri-and-lytton-labs/96/9

We got facebook account name and we know he has Instagram and LinkedIn accs with same pfp. So I searched for his ig acc and on his account , I found his Mama and Papa names.
IG post -> https://www.instagram.com/p/CszzgV9u25Y

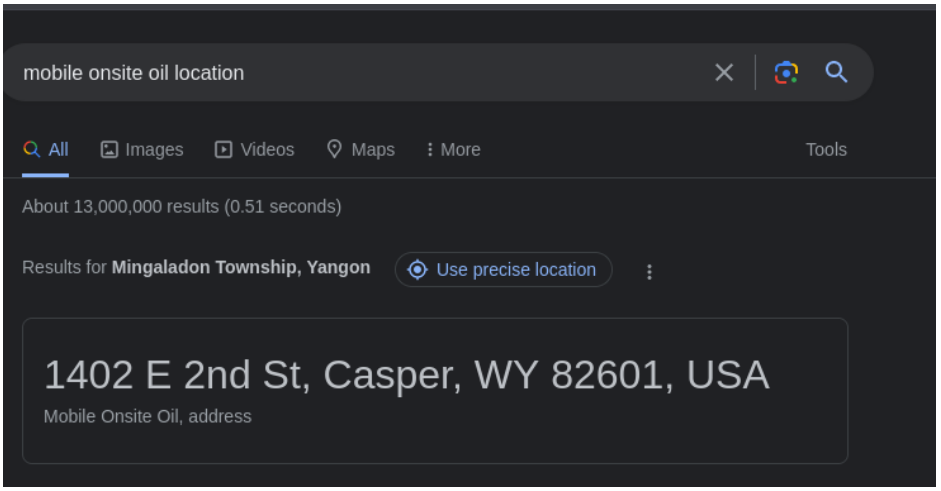
flag{Carmelo<3Delfina}

Nice Vacation (20 pts) (solved)



This chall gave us the following image to download.

If u zoom in the pic ,there are words on the board “Mobile Onsite Oil” , So I dont think too much. Just Google it “Mobile Onsite Oil location” .. Boom! Got the location and put it in flag format.



flag{Casper, WY}

Steganography

You’ve Been Ransomwared (10 pts) (solved)

This chall was solved by my teammate but I’ll write it up!!!!

So downloaded the given image!! I tried useful tools like exiftool,steghide,zsteg but didn't okay.So I have stegsolve tool to try.

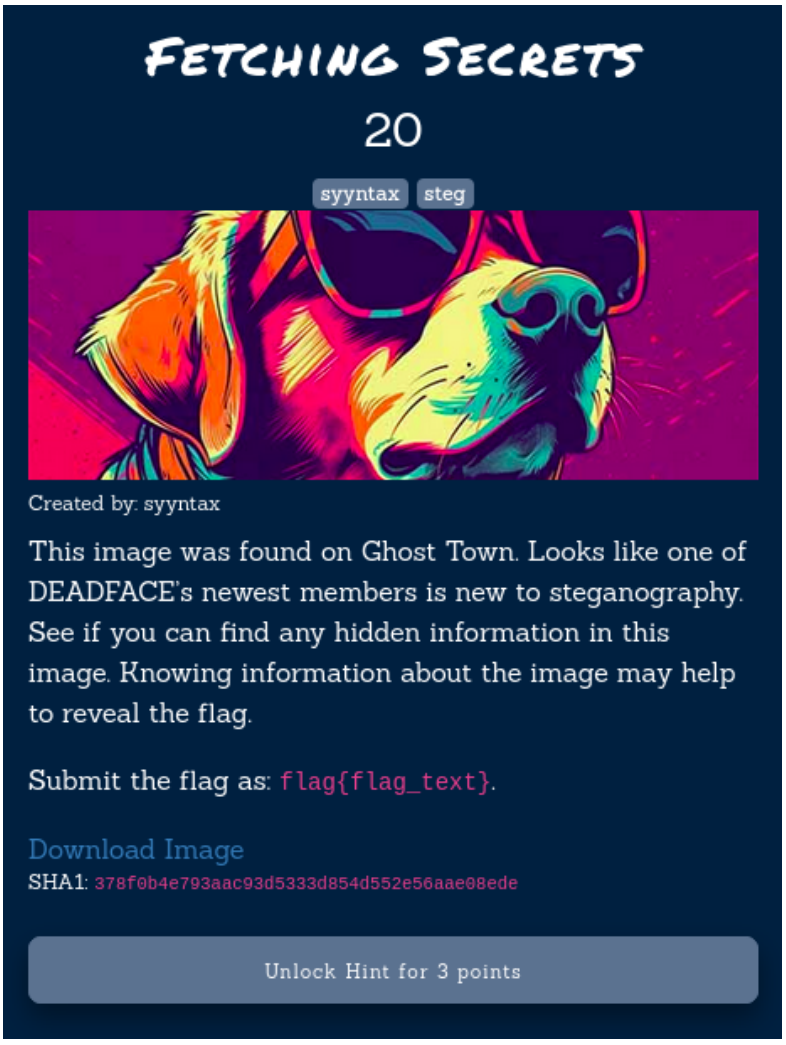
[Here u can install Stegsolve]

So I opened the image with this tool and I saw some binary words at the end of image.So I changed Blue Plane 5 to see more clearly

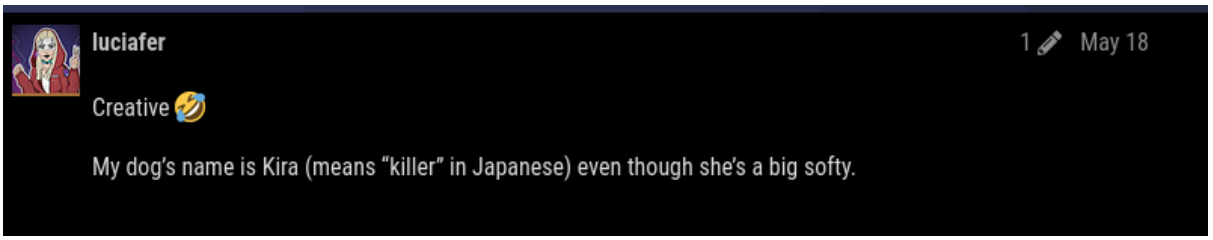
01010100 01101000 01101001 01110011 00100000 01110010 01100001 01101110 01110011 01101111 0110001 01110010 01100101 00100000 01100010 01110010 01101111 01110101 01100111 01101000 01110100 00100000 01110100 01101111 00100000 01111001 01101111 01110101 00100000 01100010 01111001 00100000 01101101 01101001 01110010 01110110 01100101 01100001 01101100 00101110

Got them so translate it into plain text here . “This ranso1re brought to you by mirveal “ flag{mirveal}

Fetching Secrets (20 pts) (Solved)



Hint -> image was found on Ghost Town



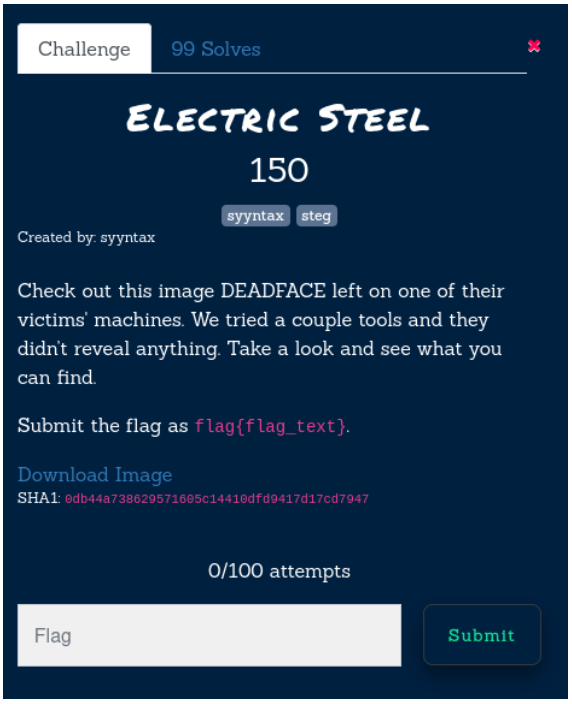
I checked if there was embedded data or not with steghide tool.

steghide --info cyberdog.jpg
Yes there was ! But we need passphrase to extract! But we knew dog's name is Kira. So the most possible password is kira . So I extracted data with

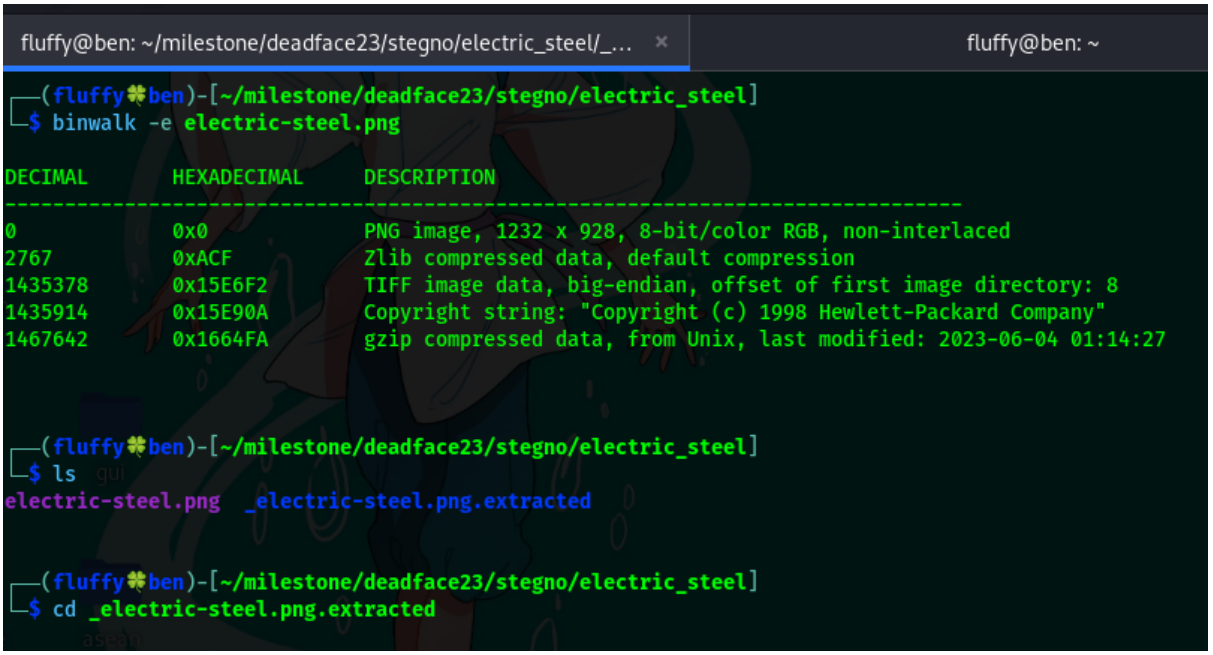
steghide extract --sf cyberdog.jpg -xf flagisout.jpg

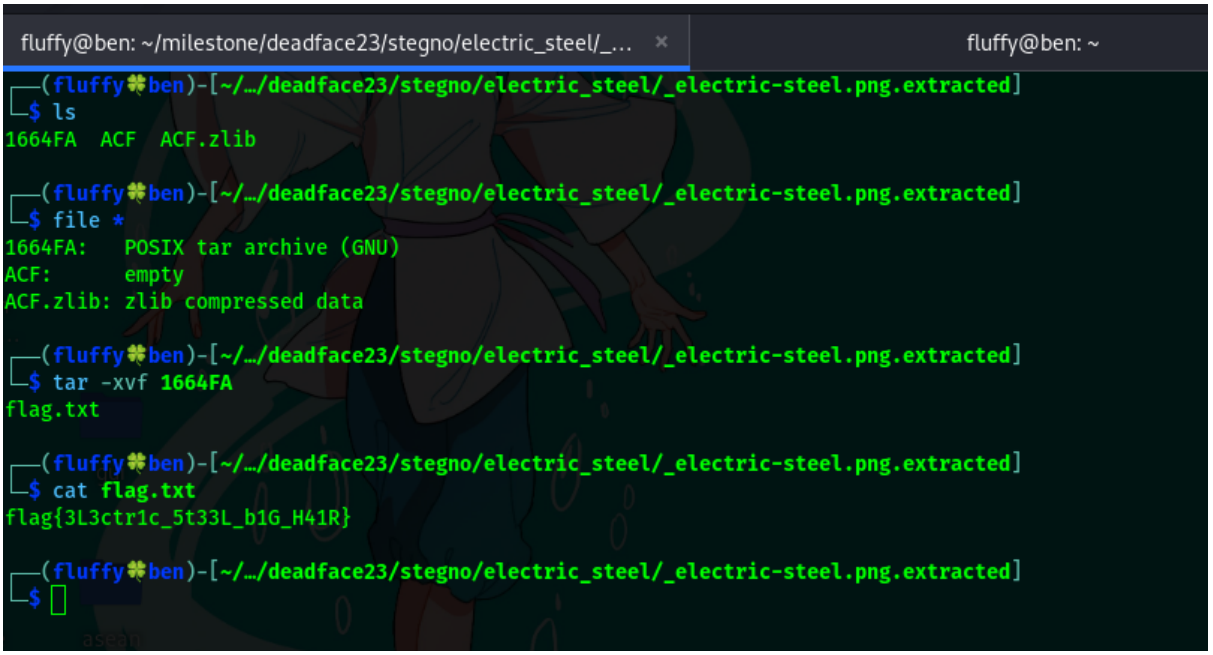
flag{g00d_dawg_woofw00f}

Electric Steel (150 pts) (unsolved)



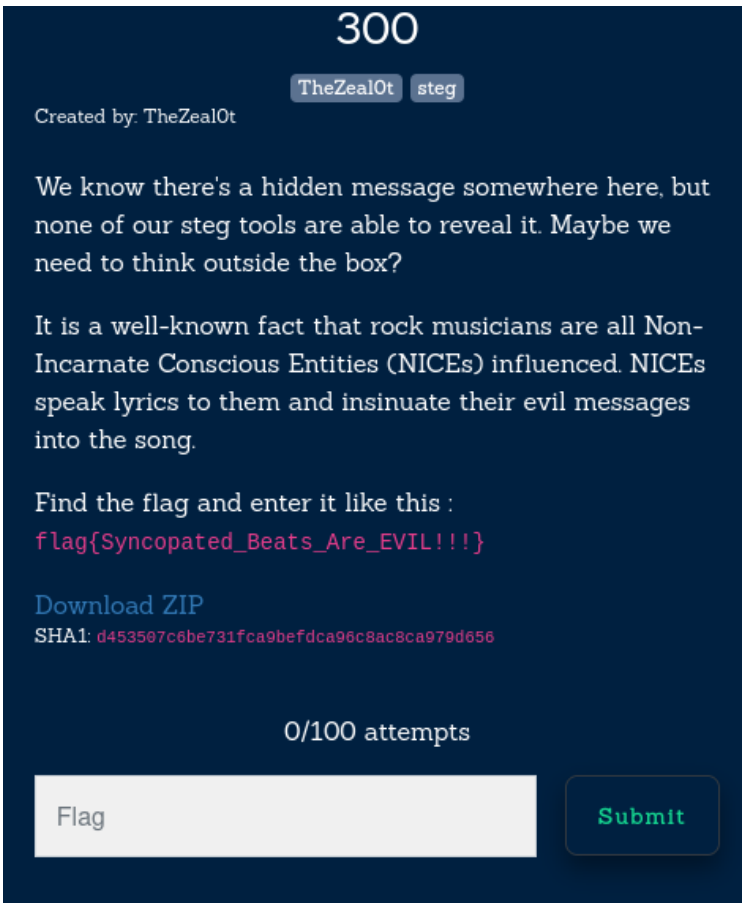
This chall should be solved :(
I tested the given image with steghide,exiftool.stegsolve,zsteg.strings but didn't work
So I extracted data with binwalk tool. In the extracted folder, there are 3 file (one with tar file , one empty and another zlib file) I didn't checked these files :3 so I didn't solved.
We can check what file type is with "file" command. Then I extracted again tar file and fking flag is out .





flag{3L3ctr1c_5t33L_b1G_H41R}

Syncopated Beat (300 pts) (unsolved)



I think I could solve it buttttttttttt .. I wont add screenshots coz if I start up my window on virtualbox , it will crash lmao!!
A zip file is given in description. Unzip it and two wav files are out.

Syncopated-Beat-2023.wav
Mysterious_music.wav

If u listen “Syncopated-Beat-2023.wav” carefully, u’ll notice like evil sound but I know it’s reversed. So we need to reverse it again using Audacity tool.

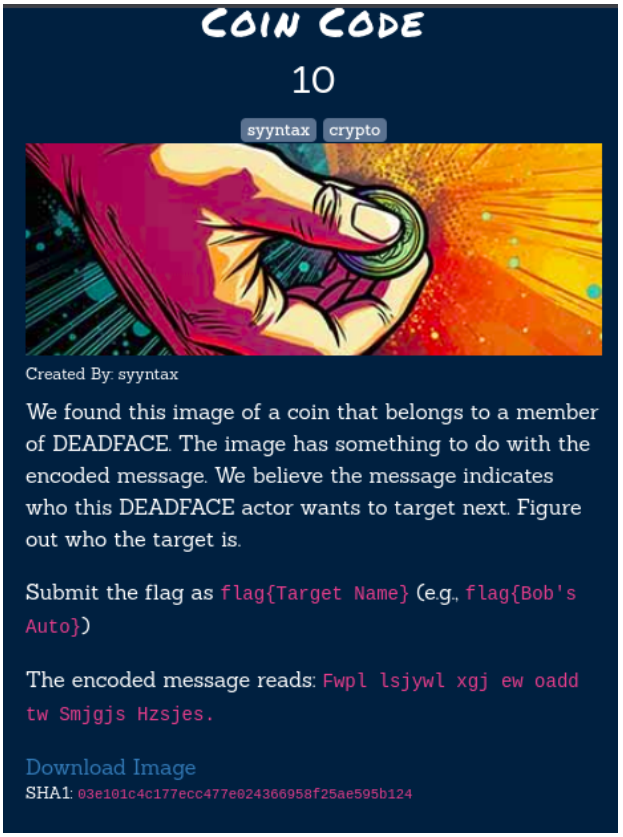
Import Syncopated-Beat-2023.wav file and select evil sound waves part
Then in tab menu, click effect > special > reverse

So we can hear human listenable voice. This is a hint and in this, they want me to use Deepsound tool that works on Windows.And the password is new cto of Evil Corp(e corp) and all caps ,no spaces.

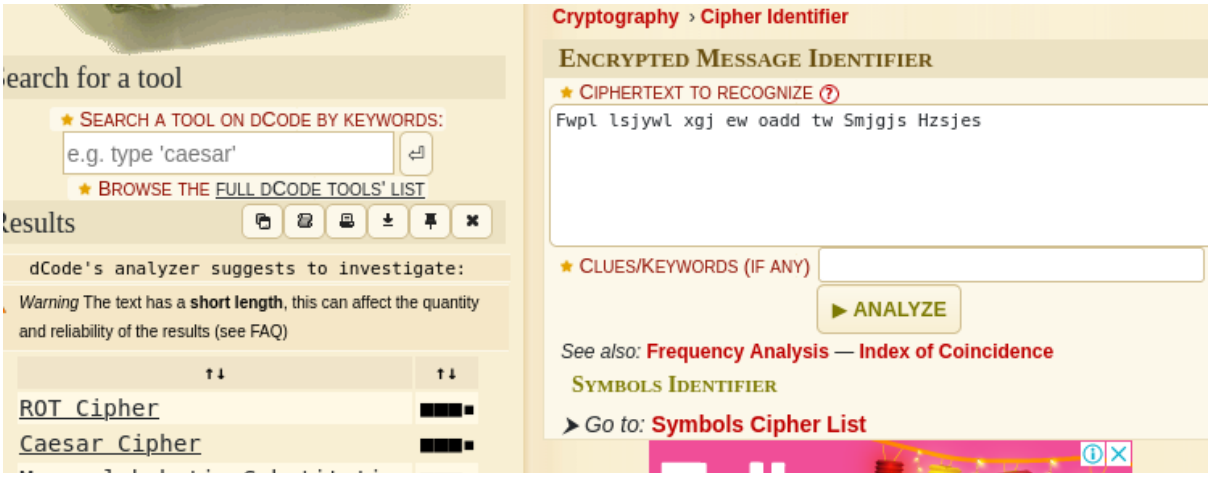
So the password be TYRELLWELLICK . Open deepsound tool and import “Mysterious_music.wav” , type password and click on extract files. Then a jpg is out. The flag is in there!!!!!

Cryptography

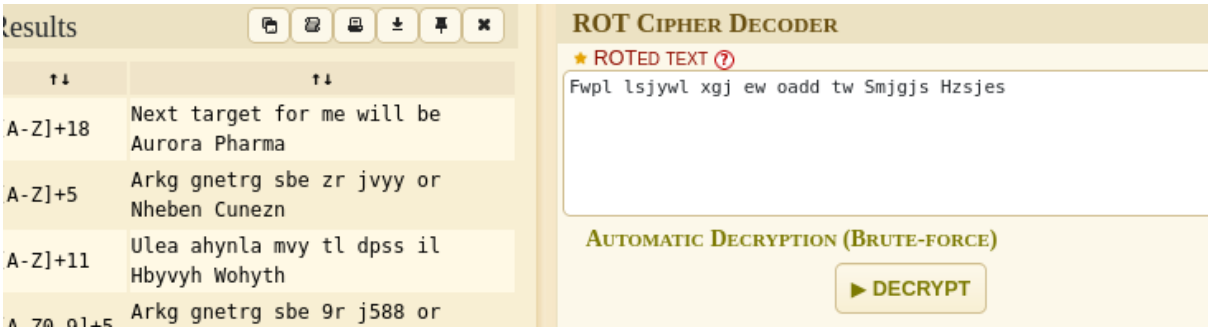
Coin Code (10 pts) (solved)



So I copied the given cipher text and analysed it to know what cipher is.

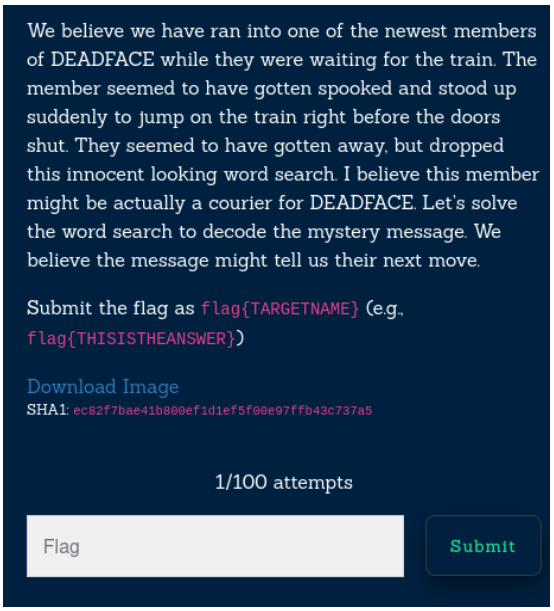


So ROT and Caesar are possible ,I decipher with Rot13 and flag is out



flag{Aurora Pharma}

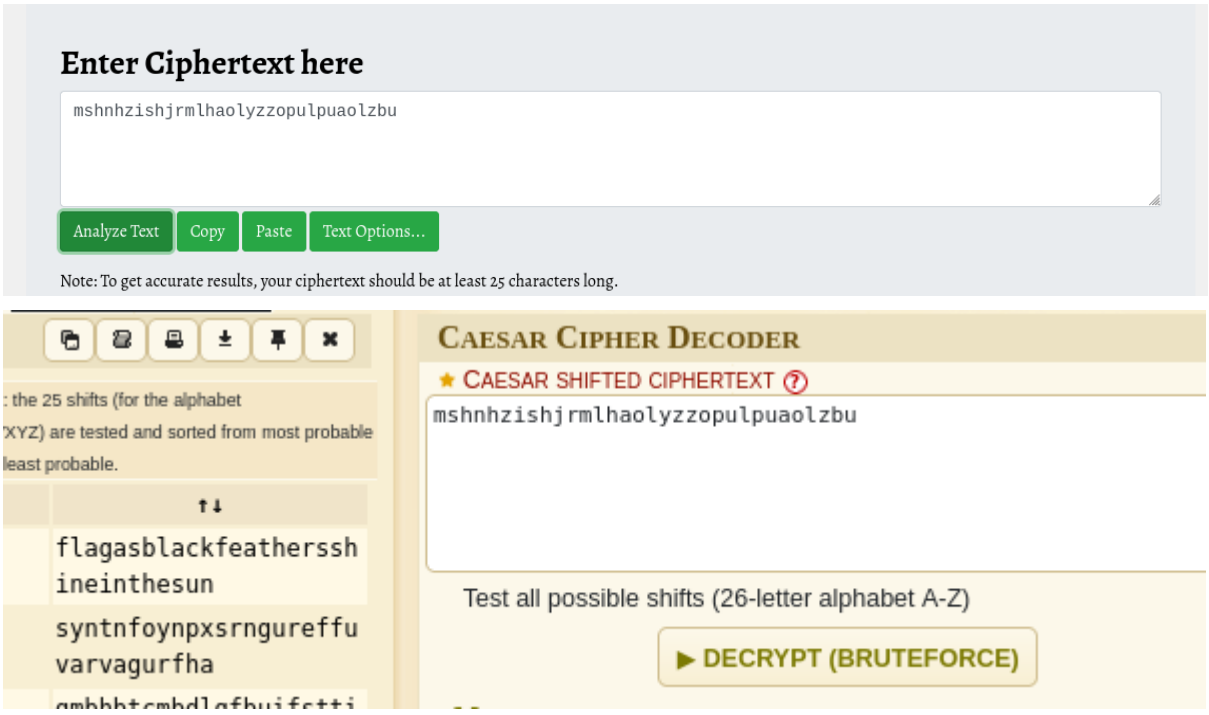
Letter Soup (10 pts) (unsolved)



This is only 10 pts but didn't solve lmao!!
A halloween word search image is given and we have to find and circle the words

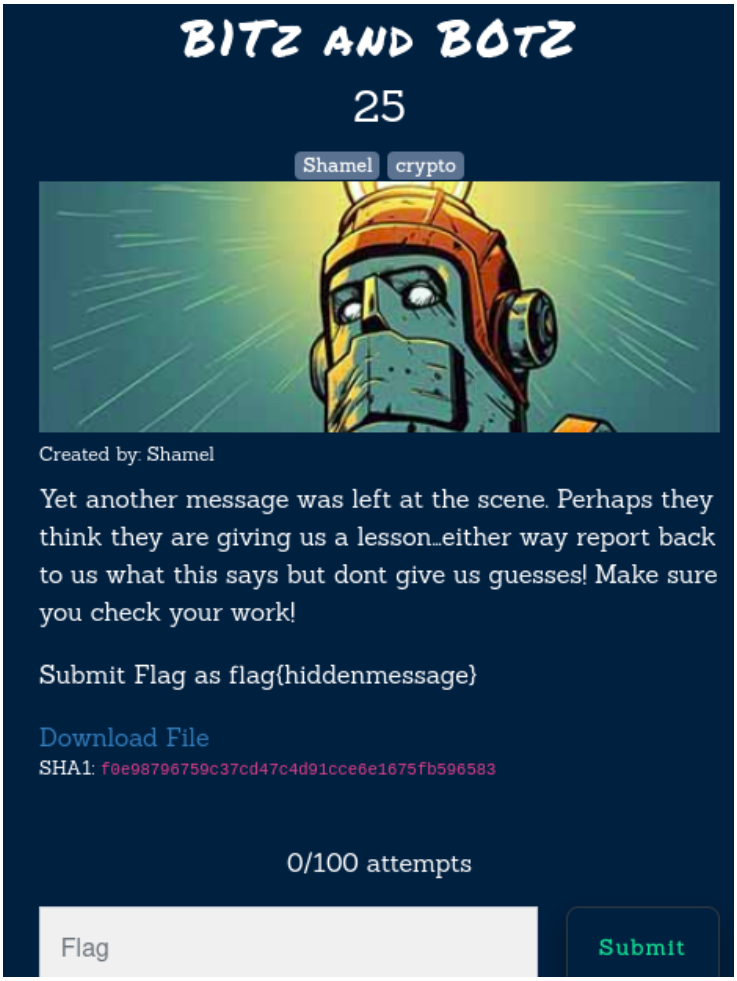
Then write down the remaining words and they became a cipher

mshnhzishjrmlhaolyzzopulpuaolzbu
Analyze with Cipher Identifier and it shows Caesar cipher , So decode with Caear decoder

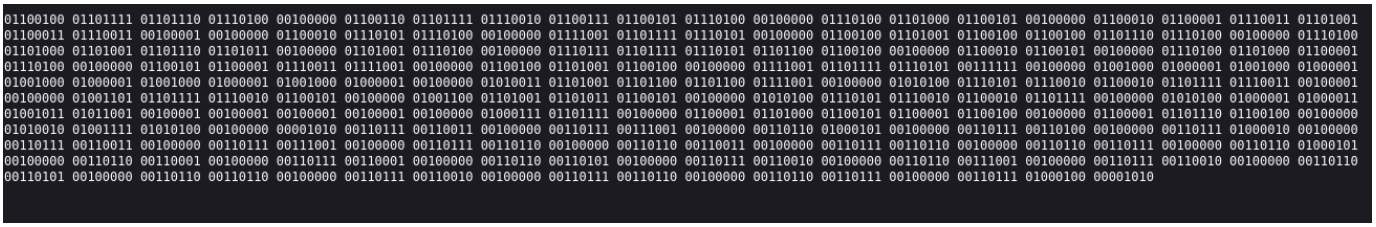


flag{asblackfeathersshineinthesun}

B1Tz and B0tZ (25 pts) (solved by teammate)



In the given file, binary texts are included.

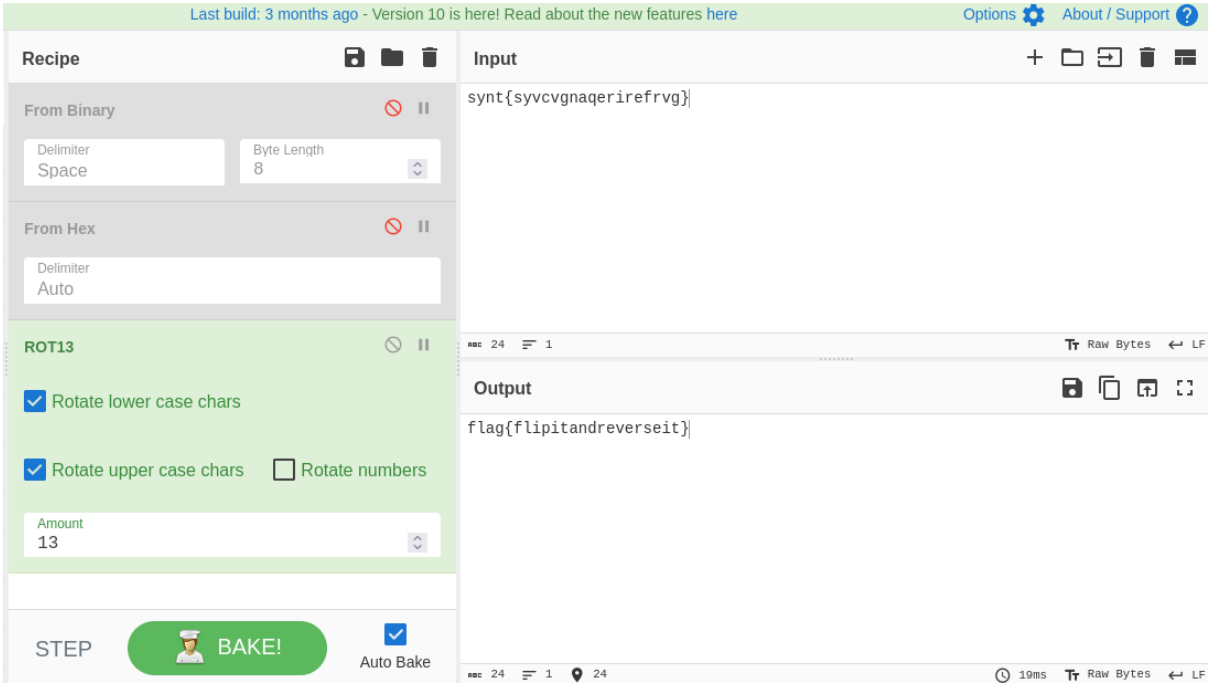


I solved the whole chall using cyberchef .
I copied and translated binary text.
And I got the following

dont forget the basics! but you diddnt think it would be that easy did you? HAHAHAHAHA
Silly Turbos! More Like Turbo TACKY!!!! Go ahead and ROT
73 79 6E 74 7B 73 79 76 63 76 67 6E 61 71 65 72 69 72 65 66 72 76 67 7D

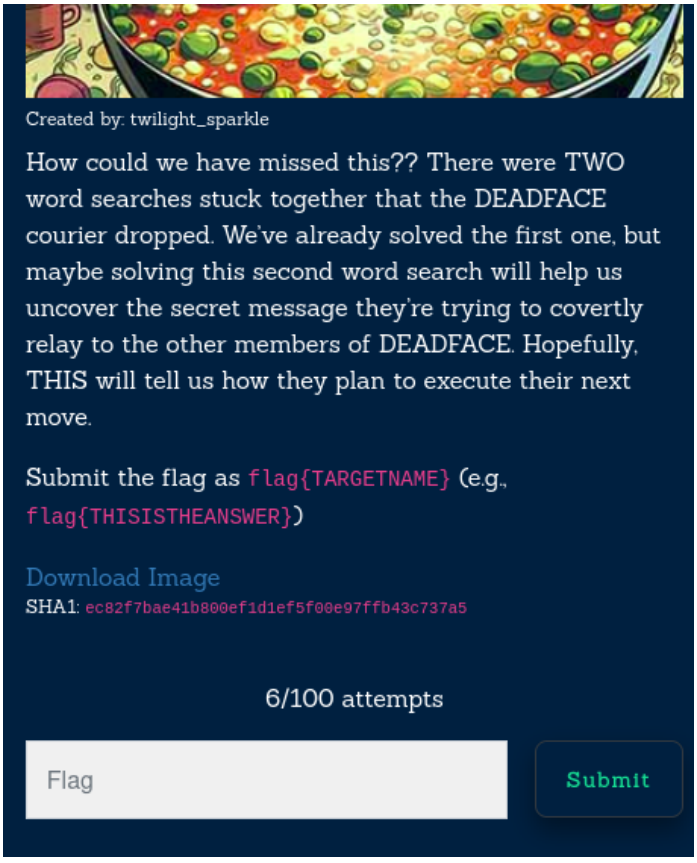
I know hex are given and must convert it .After , I got a cipher ,ROT is got above and decoded with ROT13 and flag is out.

(binary => hex => Rot13 => plain text)

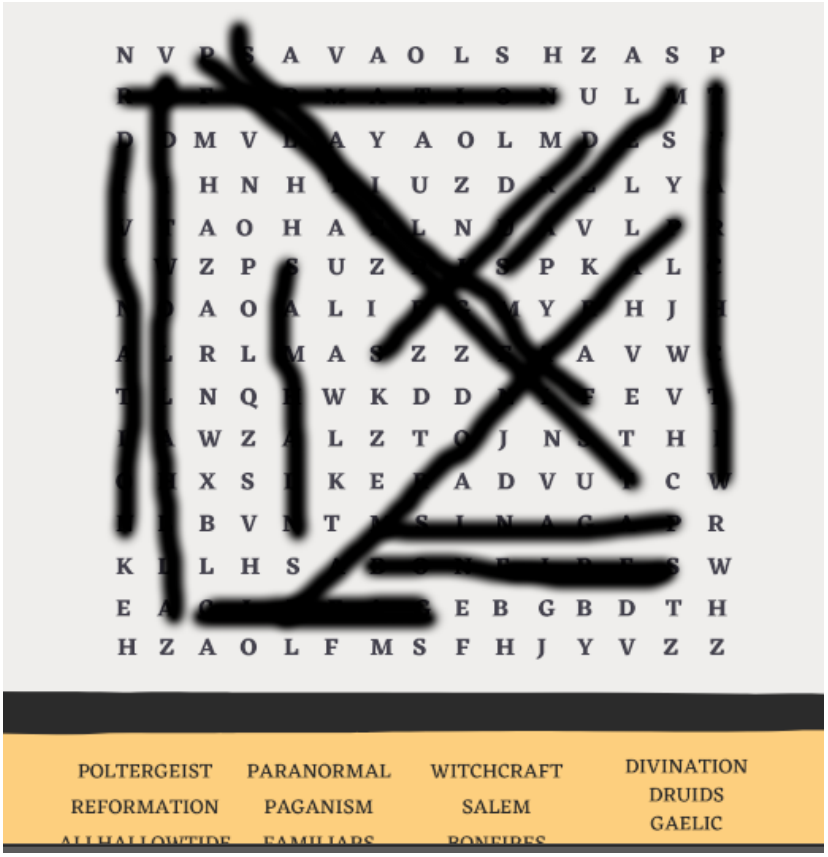


flag{flipitandreverseit}

Refill On Soup (75 pts) (unsolved)

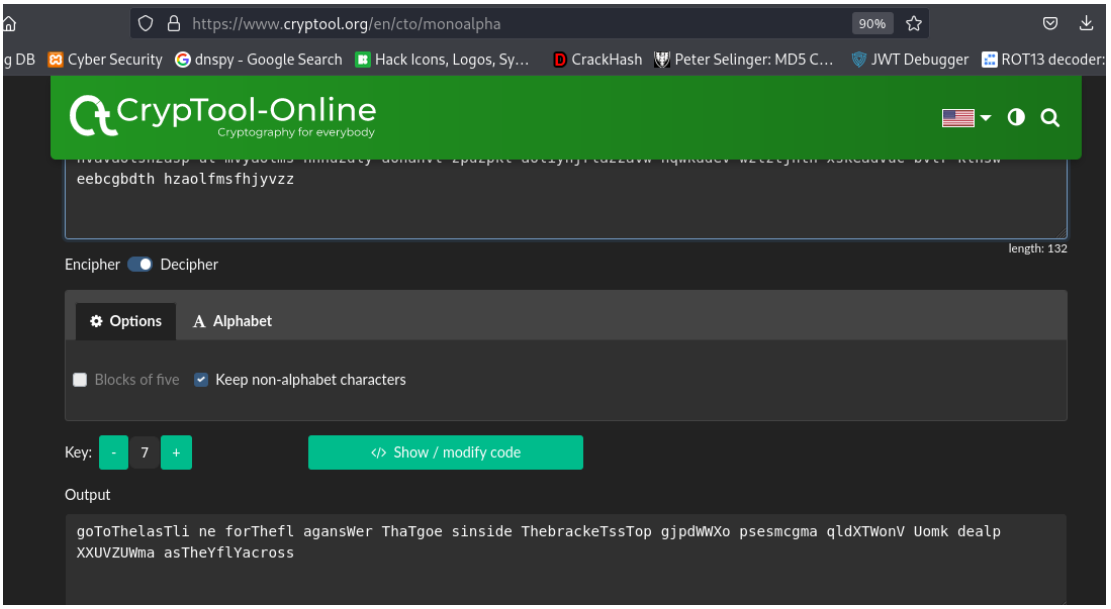


I do the same way like Letter Soup and write down the remained alphabets. But I space if one row is completed.



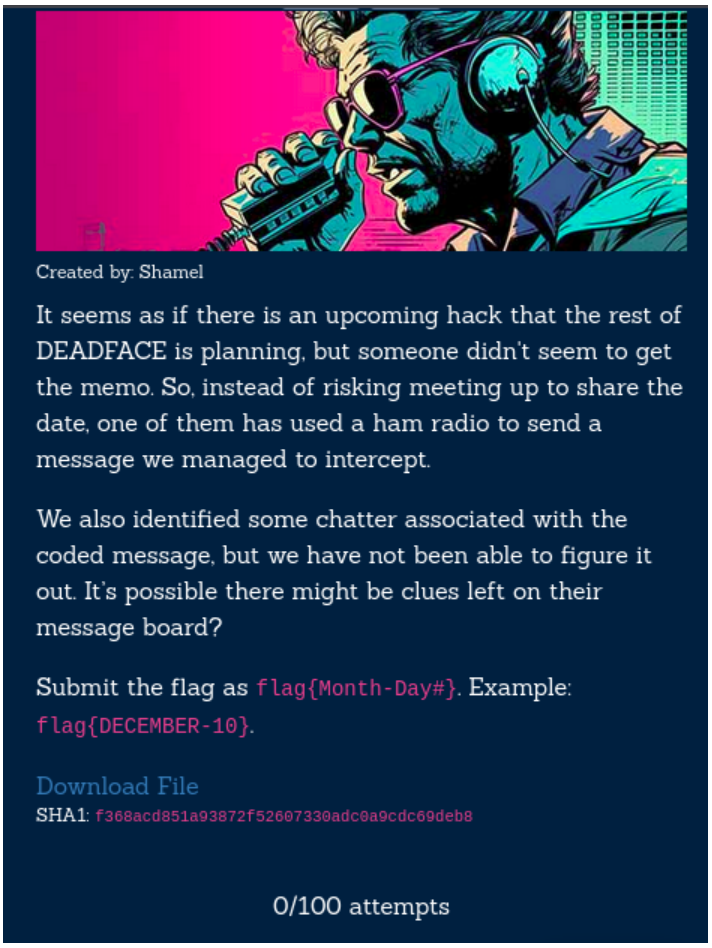
nvavaolshzasp ul mvyaolms hnhuzdly aohanvl zpuzpkl aoliyhjrlazzavw nqwkddev wzlztjnth xskeadvuc bvtr klhsw eebcgbdth hzaolfmsfhjyvzz

Analyze cipher and decode with [MonoAlphabetic Substitution]



Flag is the last line So,
flag{astheyflyacross}

HAM JAM (75 pts) (unsolved)

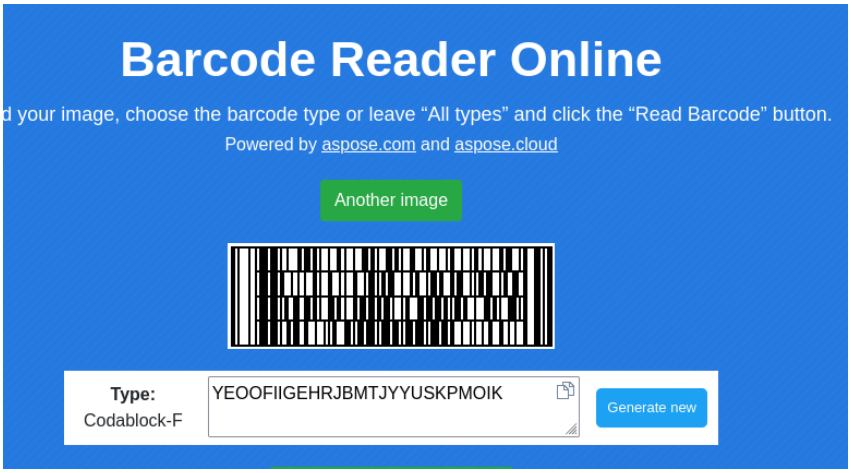


Morse Wav file is given, I decoded with [Morse Audio Decoder]

Decoded message => THE KEY IS HACKTHEPLANET

So we got a key but dont know what to do with it. Trick is that we have to research on ghost town associated with ham radio . I found a post and got barcode image

So scanned it using [Barcode Reader]



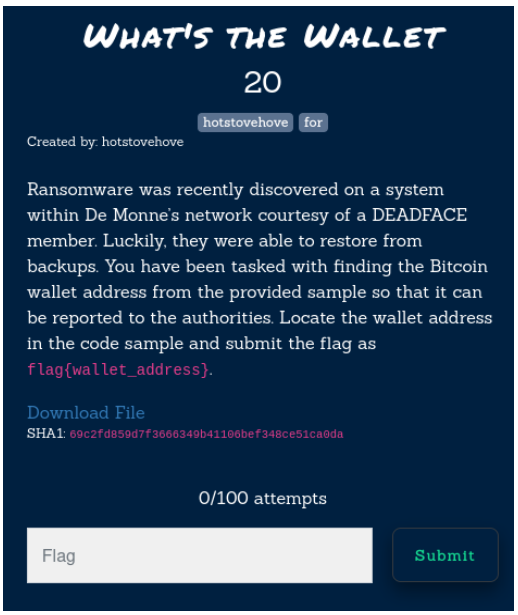
A cipher text is appeared. I know we got a key so, that must be Vigenere cipher. I decoded using [Vigenere Decoder] with key ‘ HACKTHEPLANET ‘ and got the paint text.

But we have to fix in flag format.

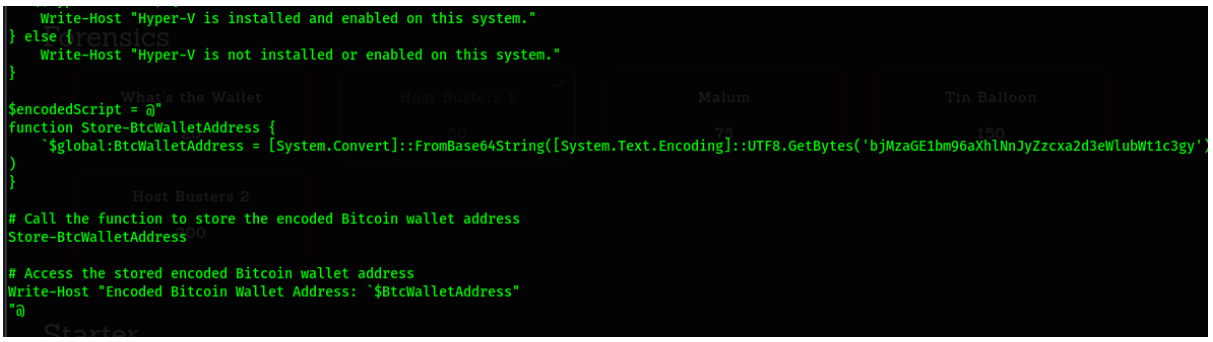
flag{NOVEMBER-5}

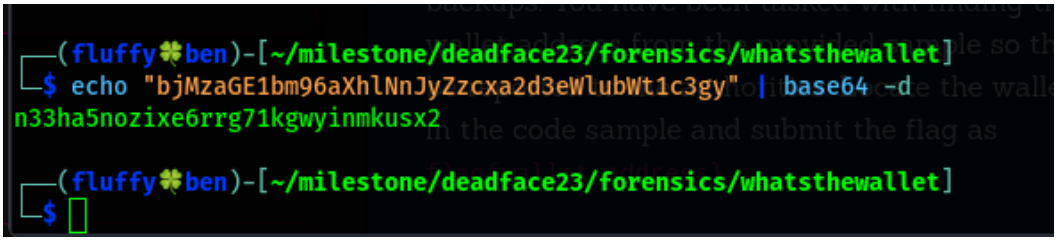
Forensics

What’s the Wallet (20 pts) (solved by teammate)



It's really ez . Bitcoin.txt file is given. Download and read with 'cat' command
A useful function that store BTC address but encoded with base64 so. Decode it and flag is out.

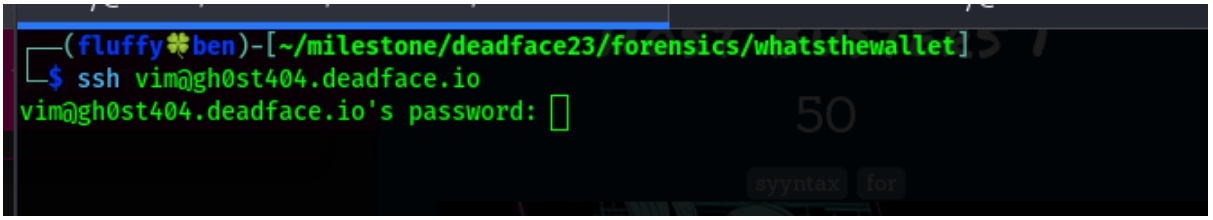




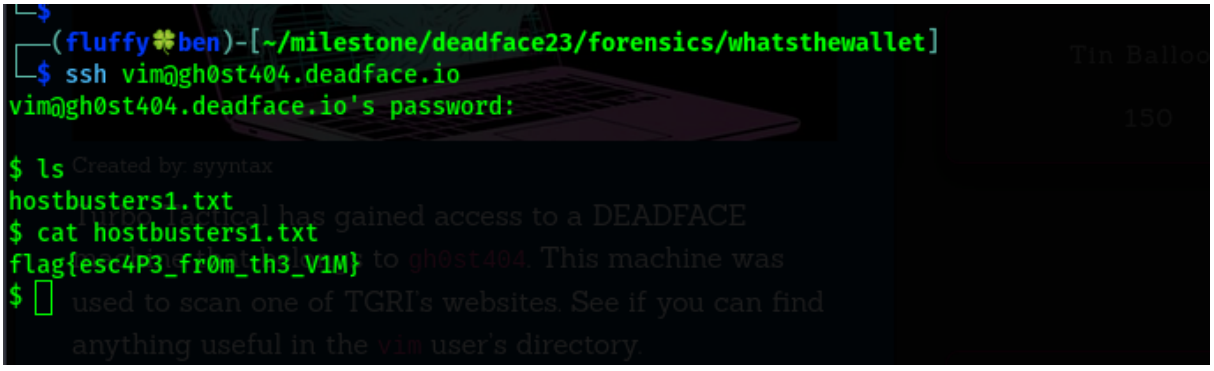
flag{n33ha5nozixe6rrg71kgwyinmkusx2}

Host Busters 1 (50 pts) (solved)

ssh credentials are given !
So connect ssh with password letmevim

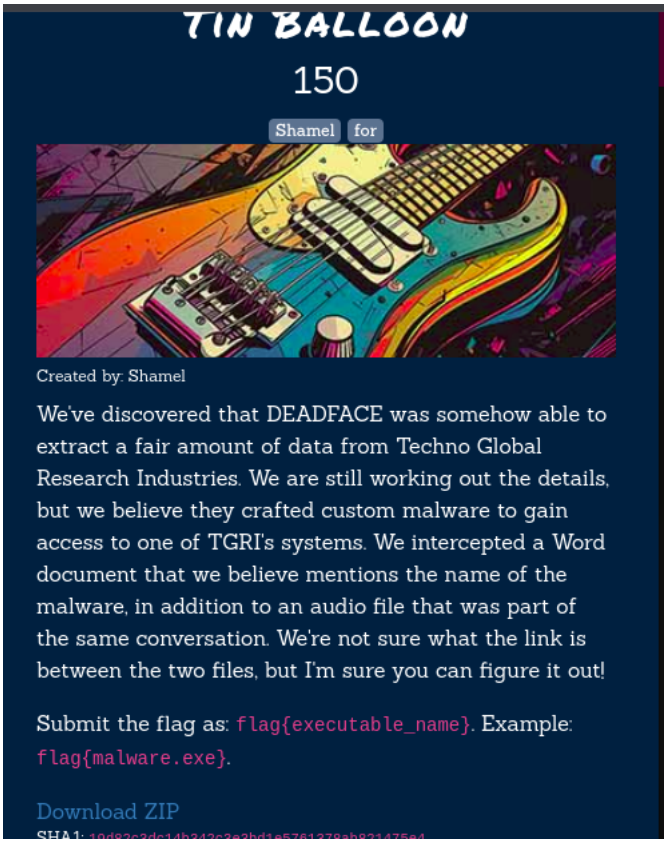


Then vim editor is automatically opened ! I know I should try to get shell access via vim.
Here u can explore VimToShell . I used " :shell " to gain shell .
Then used ' ls ' command to list dirs and found a txt file that can has flag text.
So opened this txt file using ' cat ' command and flag is outtt.

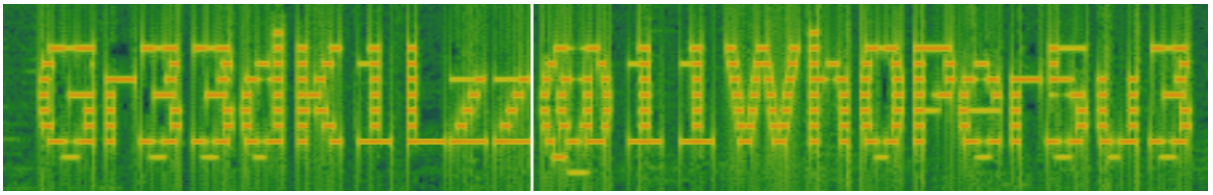


flag{Hunt_4_UDP_s3rv3r}

Tin Ballon (150 pts) (solved)



Unzipped the given file and the followings are out.
Sequence 01.mp3
Untitlednosubject.docx
When I open the docx file , it requires password to be opened. So I know the password is in mp3 file. I used Sonic Visuliser and add spectrogram to this mp3 file and got the password



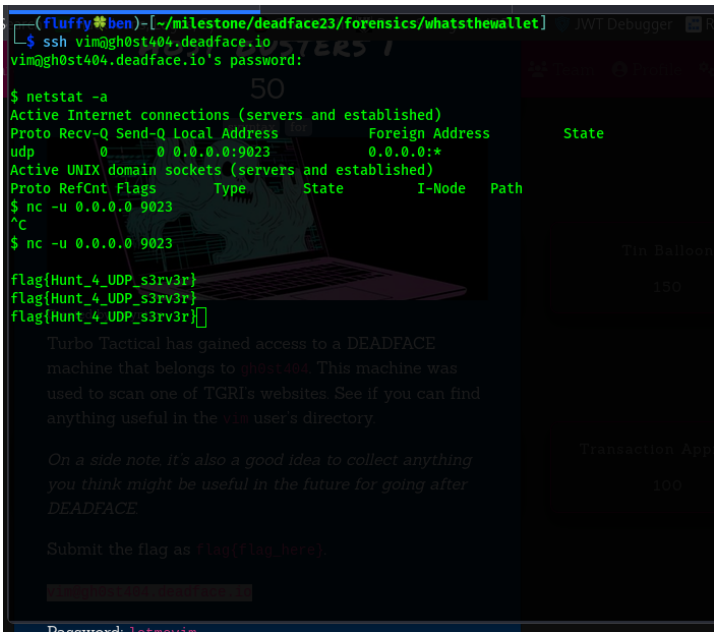
Gr33dK1Lzz@11Wh0Per5u3
I used it to open docx file and boom , i got name of malware.exe

flag{Wh1t3_N01Z3.exe}

Host Busters 2 (200 pts) (unsolved)

This series of host busters 1 and we have to find the flag not switching other users .
So we checked the network status with ‘ netstat ‘ command.

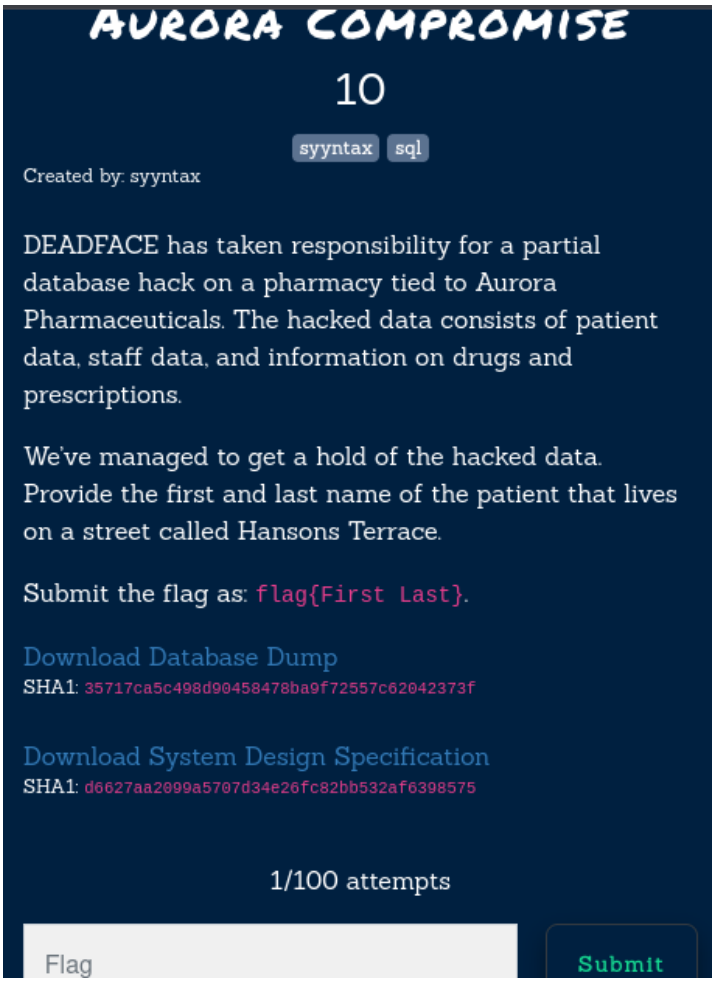
After that we can see a connection is alive and connect it with netcat ‘ nc ‘ .



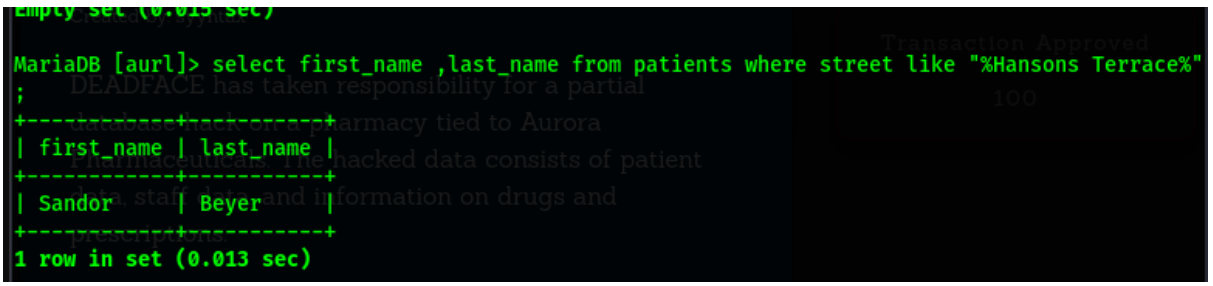
Enter twice and flag is out
flag{Hunt_4_UDP_s3rv3r}

SQL

Aurora Compromise (10 pts) (solved)

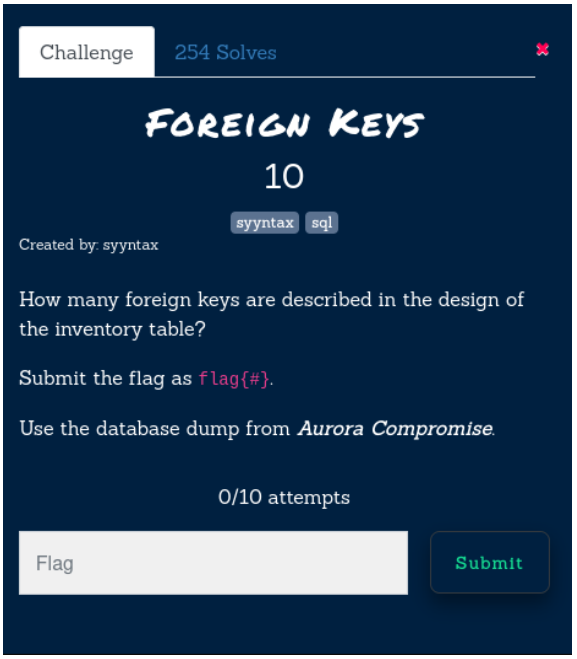


Query -> select first_name ,last_name from patients where street like "%Hansons Terrace%";



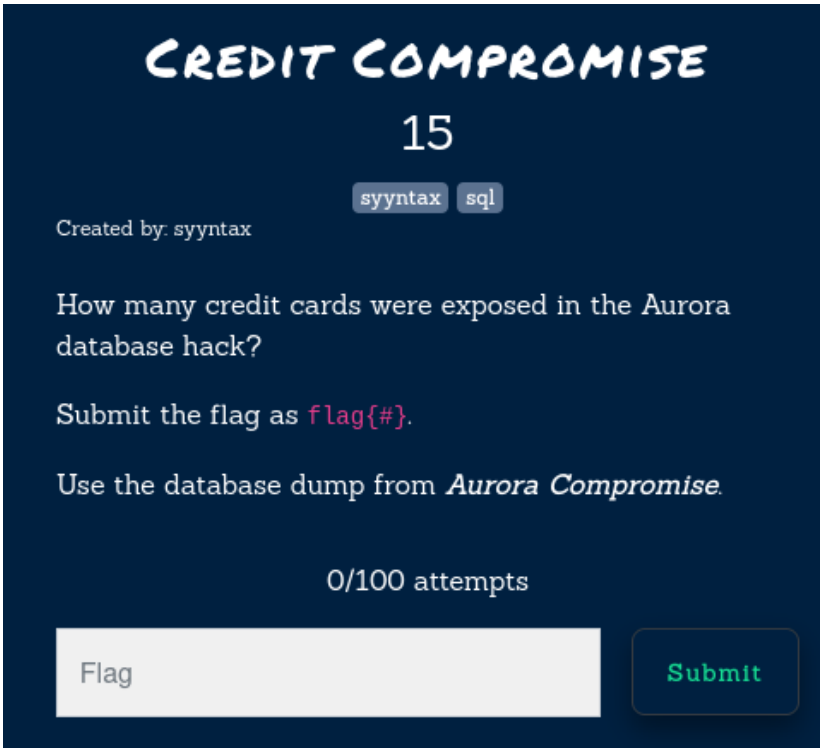
flag{Sandor Beyer}

Foreign keys (10 pts) (solved)



Open the pdf file given in Aurora Compromise and search for foreign
There are 2 foreign keys in Inventory table
flag{2}

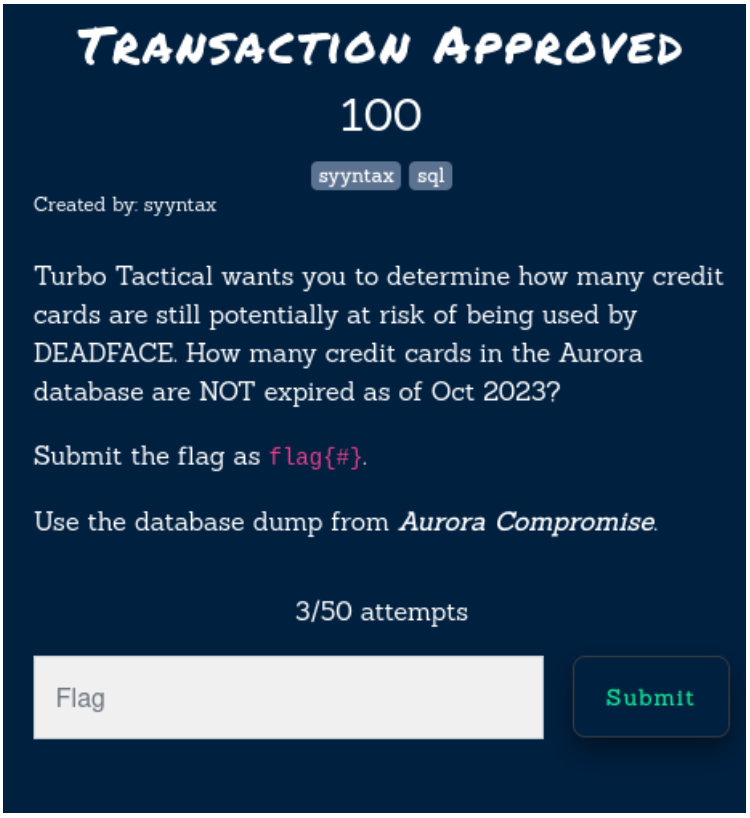
Credit Compromise (15 marks) (solved by teammate)



Query -> select count(card_num) from billing;

flag{10391}

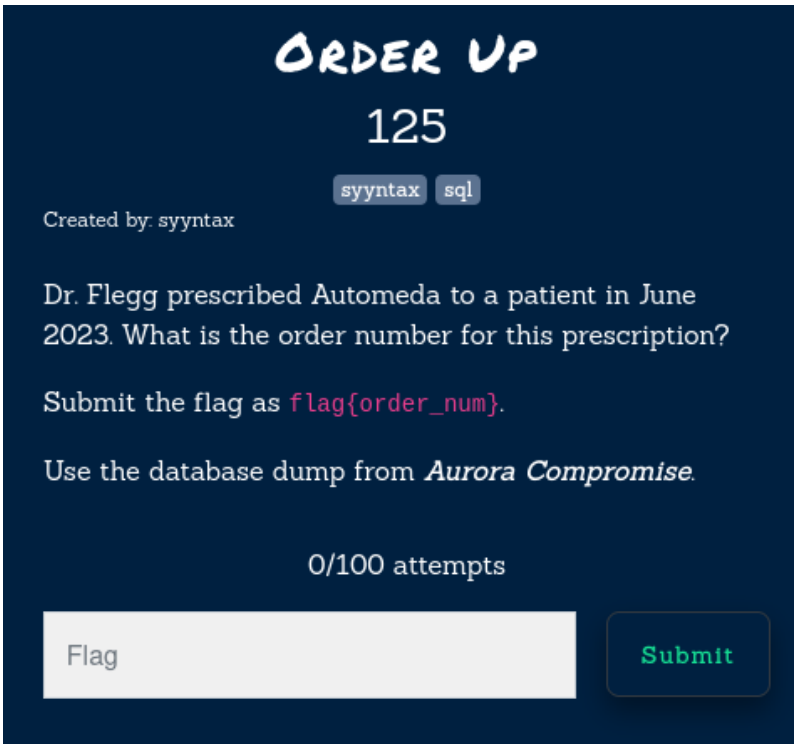
Transaction Approved (100 pts) (solved)



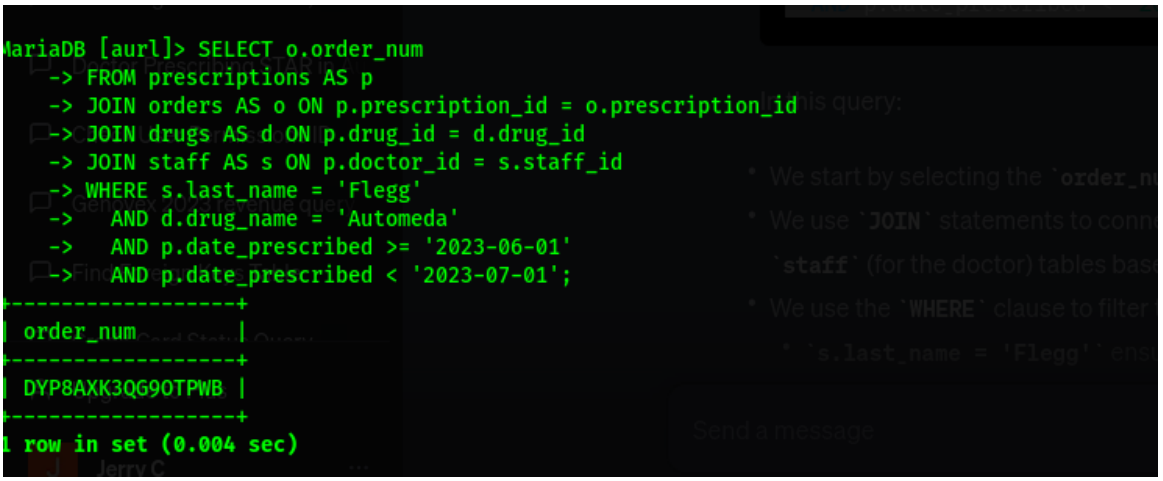
Query -> select count(card_num) from billing where exp > '2023-10';

flag{8785}

Order Up (125 pts) (unsolved)
I got the flag and the challenge is over ! So sad :(



Query -> SELECT o.order_num
FROM prescriptions AS p
JOIN orders AS o ON p.prescription_id = o.prescription_id
JOIN drugs AS d ON p.drug_id = d.drug_id
JOIN staff AS s ON p.doctor_id = s.staff_id
WHERE s.last_name = 'Flegg'
  AND d.drug_name = 'Autometa'
  AND p.date_prescribed >= '2023-06-01'
  AND p.date_prescribed < '2023-07-01';



flag{DYP8AXK3QG9OTPWB}

Author : M1n Y3ll S1 T8u
0ct 25 , 23
Hope we can explore new new things together
Have fun guyss