Decode the hex value

Took the value and put it in dcode website from hex to text to get the flag

Flag:root@localhost

The rail conductor’s Secret

Copied the value to dcode’s cipher finder and found that it was rail fence cipher And decided that it required the field values to be 24 through the clue given

play with qr

Extracted the file scrolled through the entire extracted file and noticed the the fake_qr669 was different from other by noticing the diff in the file size and scanned it to try it out and I had the flag in it

flag:root@localhost{7h3_q6_!s_fun}

Route 47

Copied the code and pasted in dcode’s cipher finder found it was rot 47 put it in its decoder and got the flag (yes ik you were supposed to use the clue guess I was both a idiot and genius at the same time)

Byte buster

Copied the symbols and pasted in dcode’s cipher and found it was brainfuck put it into its decoder and submitted the flag

Welcome

After clicking the link got redirected to discord took the flag from the announcements and submitted it

The Great login heist

Fired up wireshark went to file clicked on export objects was able to find the POST and the username and password was inside the xml header copied those and made it as an flag as per the format and submitted it

flag:root@localhost{Liam_24_P%40ssw0rd!2024}

Weak

Searched for “the most commonly used passwords in the world” in google tried everyone in the list till I got it right (source:https://en.wikipedia.org/wiki/List_of_the_most_common_passwords)

Locate the bridge

Googled what3words found the site and went to it searched for “REC college” For from there just searched till found the connection bridge and then copied the three words in The correct format from above the search bar and submitted it

Find The lab

The same the challenge “Locate the bridge” but you search for idea factory and copy the three words in the correct format and submit it

The magnetic epicentre

Using the clues given in the challenge searched google for “the point in Tamil Nadu which aligns closely to the magnetic epicentre of the Earth” And managed to get the location same which is **Chidambaram temple** and as before pasted the the location to “What3words” got the flag and submitted it

Find The Ranch

Did an reverse google image search got an hit clicked onto the website after after scrolling through some anime stuff found an write up for an CTF clicked onto it and the second challenge in it was this pic and the exif data was also given but at the end of this challenge I found the location directly without geolocating the place and submitted the flag in the correct format

The Cyber Sentinels

By the clue given in the challenge we get to know that the flag is split into three parts and each one is hidden in LinkedIn,Instagram and Discord respectively so started the search of the handles in these platforms

Linkedin Searched the fields of 1.About (couldn’t find the part of the flag) 2.Home (couldn’t find the part of the flag) 3.Post It was only then that I found that one of the post had more comments than others so check it’s comments and came to find the first part of the flag but it still isn’t over since it was in a cipher ran an quick cipher finder and found that is was base64 so used an base64 decoder and found the part of the flag and stored it in the text editor

Instagram

Followed the same steps used in LinkedIn and first tried to look for the flag in the posts since the last time I found it there and it wouldn’t hurt to give it a try and my logic wasn’t wrong In one of the posts I was able to see the flag disguised as an reply for one of the comments and copied it and since the last cipher of the flag was base64 I put in the base64

decoder and fair enough it was and and joined the two parts of the flag in the text editor

Discord

Opened up discord and checked the announcements and found that 3rd part of the flag

And decoded it from base64

flag:r00t@localhost

EDIT

from the clues given I had an Idea that it had something to do with hex and to just make sure I tried opening the png file but showed an error message so now I was sure that it had something wrong with the headers and trailers of the png so I went to https://www.garykessler.net/library/file_sigs.html (https://www.garykessler.net/library/file_sigs.html) To see if those was correct and when I put the header of the png in the search bar it didn't show up on anything so I checked it with .png header in the site and found that the value of the first hex of the header was changed from 89 to 90 and I reverted it back and saved the file and now when I opened it these was an flag in the .png image as usual typed the flag in the challenge and submitted it

Easy-Web_challenge

Clicked on the link and got directed to an webpage and since it had only 50 points and the word "EASY" I went ahead and opened up the developer tools in my browser and poked around and soon enough I found the username and password in plain text logged in to the website using those credentials and got my flag

flag:root@localhost

iDoor: The Secret Portal

Clicked the url and went to the website and started pressing buttons and other stuff in an attempt to find anything out of the ordinary and finally my dumb brain found that url had an encoded soon found that it was sha-256 so I put the hash in an hash decoder and which gave me 20 came to know the hash was for 20 and the cust Id helped to find it and I found out the hash for 0 and pasted it in the url and when the site loaded it showed me the flag and I submitted it

flag:root@localhost{770a058a80a9bca0a87c3e2ebe1ee9b2}

Echo of Time

Downloaded the audio file opened up audacity and imported the audio into it then clicked the option to change the waveform to spectogram After that I was able to see the flag And I further checked it by playing the audio which was only distorted till the flag and was fine after it and submitted the flag

flag:r00t@localhost{2025}

Hidden Truth

Downloaded the challenge.png file and used exiftool to find the meta data and found that there was an Title field with an string knowing that it was an cipher found the type of cipher used and decoded it the cipher used was base64 and found the flag after decoding it

flag:root@localhost{C0ngr@t$_Y0u_F0und_Th3_Myst3ry_N0w}

Pixel Secrets

Got a file and a list of passwords started going through the passwords where I found a suspicious one H@rdP@ssw0rd!2024 Using openstego I tried this one along with the upcoming ones that's when I found the flag using this password ej,;m=;$IL}@

flag:root@localhost

**Silent Courier **

Fired up wireshark looked at the option of export object from the file button in the tool bar got an protected.zip file got John the ripper up and running and cracked its password

flag:r00t@localhost

Secret Stash

Used steghide with -sf to extract the files from the steg2 Which gave steg2.jpg and steg2_pass.txt And used an combination of John the ripper and hashcat since both has advantages and disadvantages in cracking passwords Using these tool was able to get the flag

**DOCM analysis **

Downloaded the .docm file and analysed it using VBA and found it had an base64 string in the file and decoded it using dcode's base64 decoder to find the flag

flag:root@localhost

REV

Used ghidra to analyse the functions in the code found that there was an secret function in the code Decompiled it to find the flag

flag:root@localhost

**Enigma Unveiled & Avengers

Used google docking to find the GitHub repository for these challenges

P.s:you guys were the one who told that it’s similar to an open book test

JWT

Since the name is JWT it’s about tokens Decoded the token using fusionauth.io Cracked the token using JWT cracker And used this to get an new token And used this token which has root access to get to the flag

Since they announced that there was an cloud section in the CTF I knew that it would be in AWS(Amazon Web Services) but just wasn’t sure what it’s about

And I had an guess it would be in S3 buckets and as you guys guessed it was about it

Unlike other challenges you need some stuff first to get started as they mentioned in the challenge :

1.S3 browser-

2.AWS CLI - basically an terminal but just for AWS services and you just install it in the terminal And to the windows guys you can do the same in the cmd

3.An AWS account which just make this all work easier but I don’t think most people have it But it’s an option

And any one of these is enough not sure about the S3 browser tho since I didn’t use it I personally used AWS cli for this if you have a bit of experience in the terminal then it’ll be easy But for people with windows it might look hard at first but since the commands are less you can learn it just fine

Misconfigured Bucket

By the title I came to know that the bucket is configured wrong basically it is made public and can be accessed without even an account And another reason is that they didn’t give any other info on the bucket so that must be only possibility AWS is for activating the AWS cli and s3 is for the type of service you’re accessing from the AWS CLI

So started this challenge by copying the bucket name which is and fired up the terminal And entered this command which basically finds the bucket and lists its contents on the screen

and the **—no-sign-request** this is used cause normally this command usually gives the credentials on its own and when you haven't entered any credentials it throws an error message And for an public bucket you don't need an credentials so we use this to not send any credentials on our own

Now you can see that there is indeed an file in the bucket Now let's copy it to an file in our system the same code but you just change the ls to cp

Here ls is for listing the contents of an file

cp is for copying an given file to another file

And another change which you would have to do is that add an whack **"/"** And copy paste the file name to the command after the whack and have to name a file where you want to save this file we took from the bucket Then you can use the cat <> or just use the file manager to access the file and you get the flag and submit it

S3crets

As for this I'm not sure if this is the expected way to do the challenge but I got the flag so not really my problem I think the link it was there just to throw people off since the url wasn't really necessary

I just followed the same process which I used for the Misconfigured bucket and got the secrets.txt file did cat on it And got the flag and just like any flag submitted it on the website