**CTF WRITEUPS**

**WELCOME:**

In Discord ,I went to the #announcements. I scrolled to the very first messages and found the flag there: root@localhost{W3lc0m3\_T0\_r00t@l0c4lh3l1!} . I copied the flag and submitted it as the answer.

**The Great Login Heist:**

I reviewed the provided PCAP file to analyze the network traffic. By inspecting the login attempts, I identified the correct username and password. The flag was found in the format root@localhost{username\_password}. I copied the flag and submitted it as the answer.

**Silent Courier:**

In this challenge, I analyzed the challforyou.pcapng file using Wireshark. I inspected the network traffic for any suspicious file transfers or protocols, such as HTTP, FTP, or SMB. After filtering the traffic and examining the payloads, I identified the hidden secret within the transferred data. By extracting the relevant packets and decoding the content, I uncovered the secret .

**play with qr:**

In this challenge, I extracted the contents of the qr\_code.zip file and reviewed the QR code files. I found the timing change in the fake\_669 QR code, which led me to the correct QR code containing the flag. After scanning it, I uncovered the flag .

**Weak:**

I identified that the correct weak and commonly used password is "12345678." This password is frequently used and is considered insecure due to its simplicity.

**Locate the Bridge:**

I used What3Words to locate the bridge at Rajalakshmi Engineering College. By entering the college's approximate location into What3Words, I was able to pinpoint the exact location of the bridge. After locating it, I retrieved the three-word address assigned to that spot

**Find the Lab:**

I used What3Words to locate the Idea Lab at Rajalakshmi Engineering College. I navigated to the specific location using the three-word address and successfully retrieved the corresponding three words.

**The Magnetic Epicenter:**

The exact location in Tamil Nadu that aligns closely with the Earth's magnetic equator is Nataraja Kovil, which is located in Chidambaram. Using What3Words, I pinpointed the specific location and retrieved its three-word address.

**Find the Ranch:**

I used Google Search to find a blog post that provided information about the location of the ranch based on the given file. After reading the post and cross-referencing the details, I pinpointed the exact location and identified the ranch.

**The Cyber Sentinels Hunt:**

I followed the breadcrumbs left by the Cyber Sentinels across platforms like Instagram, LinkedIn, and Discord. I carefully investigated the clues posted on these platforms and gathered the three parts of the flag hidden in the digital footprints. Once I decoded all the clues, I combined the parts to uncover the final flag.

**Echo of Time:**

I analyzed the provided audio file ab to extract a year hidden using steganographic techniques. I used tools like **Audacity** to inspect the spectrogram for embedded patterns or messages. The analysis revealed the year hidden in the audio.

**Hidden Truth:**

Open the challenge.png file using **ExifTool** to inspect its metadata.Locate the **title** field in the metadata and find the Base64-encoded string. Copy the Base64 string.Decode the string using an online Base64 decoder or a command-line tool. Extract the hidden message.

**Easy-Web\_challenge:**

1. Open the URL Right-click on the page and select **View Page Source**.

2. Find the link to the script.js file in the source code and click it to open the script.

3. Inside script.js, I found the Base64 encoded string:

4. const encodedFlag = 'cm9vdEBsb2NhbGhvc3R7VGhlX3dlYl9jaGFsbF9pc19lYXN5fQ==';

5. Copy the encoded string and decode it using an online Base64 decoder or terminal.

**Mini Vulnerable Compiler:**

1.Open the URL

2. Inspect the online Python compiler for potential vulnerabilities like input validation issues.

3. Submit Python command to exploit the vulnerability>

>exec('import os; print(os.popen("cat flag.txt").read())')

4.This command uses os.popen() to run the cat flag.txt command and print the contents of the flag.

**XSS Vulnerability:**

1. Open the URL and Find the input field where you can submit data.

2. Enter this code in the input field

<img src=x onerror=alert('XSS')>

3. If the page is vulnerable, an alert box will appear with the message "XSS" with flag.

4. Submit the flag

**JWT Vulnerability:**

1.Open the URL and Log in using the credentials: demo:demo.

2. Inspect the web app for any JSON Web Token (JWT) used in the headers or cookies

3. Decode the JWT using an online tool like [JWT.io](https://jwt.io/) to view its contents.

4. Modify the JWT payload to escalate your privileges (change the user --🡪 root).

5. Re-encode the modified JWT and replace the old token in your request

6. Reload the page and retrive the flag and Submit it.

**Decode The Hex Value:**

1. Copy the given hex value:

2. Using online hex-to-text converter, s https://www.rapidtables.com/convert/number/hex-to-ascii.html.

3. Paste the hex value into the input box and Click Convert.

4. The output will be the decoded text ,that is flag.

**Route 47:**

1.Copy the given code Go to an online base64 decoder

>https://www.base64decode.org/

2.Paste the code into the input box

3.Click "Decode" to get the result.

4.The output will be the decoded text

5.Submit the flag.

**Byte Buster:** I first copied the given Brainfuck code. Then, I used an online cipher identifier tool to recognize that this is a **Brainfuck** cipher. I used a **Brainfuck interpreter** such as **Dcode**. I pasted the code into the interpreter and ran it to decode the message. The decoded output revealed the flag.