CTF CYBER-SENTINELS

WRITE UPS

MISC:

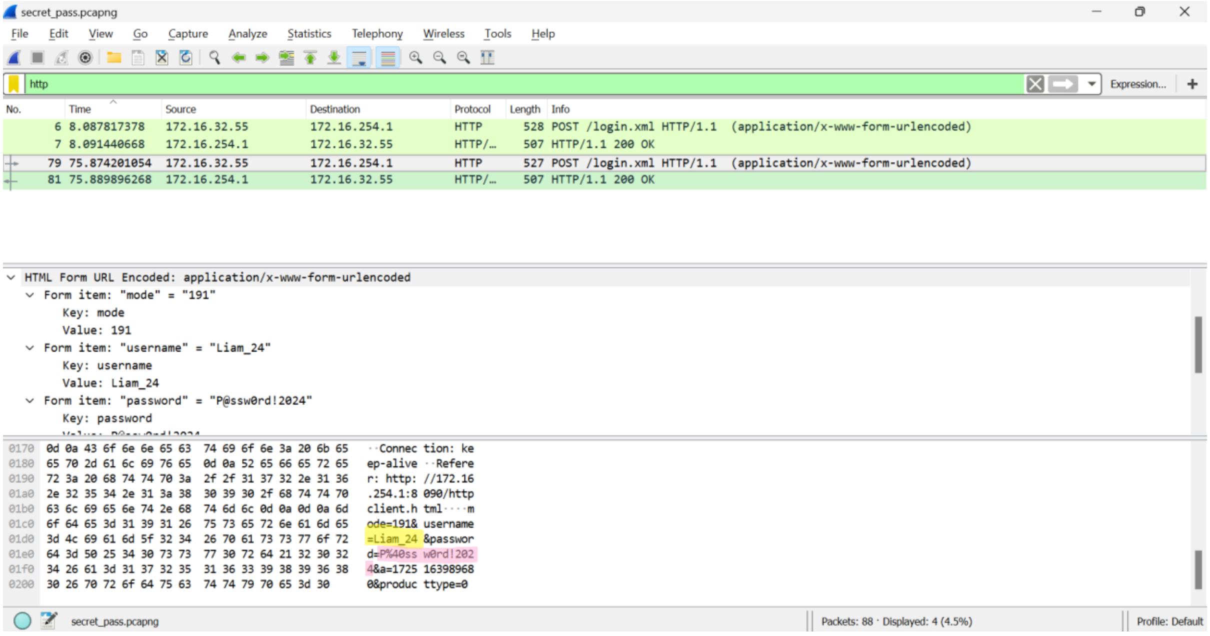
1. The Great Login Heist

Problem statement:

In a daring attempt at digital mischief, a crafty threat actor tried to break into Cybertown Tech Solutions' secure web interface. Their sneaky login attempts were caught red-handed in a PCAP file, thanks to our vigilant network monitoring.

Steps:

1. Open the given pcap file in wireshark
2. Check for the parameters like username and password


secret_pass.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

```
http
```

```
No.   Time          Source         Destination    Protocol  Length  Info
    6 8.087817378   172.16.32.55   172.16.254.1   HTTP        528  POST /login.xml HTTP/1.1  (application/x-www-form-urlencoded)
    7 8.091440668   172.16.254.1   172.16.32.55   HTTP/…      507  HTTP/1.1 200 OK
   79 75.874201054  172.16.32.55   172.16.254.1   HTTP        527  POST /login.xml HTTP/1.1  (application/x-www-form-urlencoded)
   81 75.889896268  172.16.254.1   172.16.32.55   HTTP/…      507  HTTP/1.1 200 OK
```

```
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "mode" = "191"
      Key: mode
      Value: 191
  Form item: "username" = "Liam_24"
      Key: username
      Value: Liam_24
  Form item: "password" = "P@ssw0rd!2024"
      Key: password
      Value: P@ssw0rd!2024
```

```
0170  0d 0a 43 6f 6e 6e 65 63  74 69 6f 6e 3a 20 6b 65   ··Connec tion: ke
0180  65 70 2d 61 6c 69 76 65  0d 0a 52 65 66 65 72 65   ep-alive ··Refere
0190  72 3a 20 68 74 74 70 3a  2f 2f 31 37 32 2e 31 36   r: http: //172.16
01a0  2e 32 35 34 2e 31 3a 38  30 39 30 2f 68 74 74 70   .254.1:8 090/http
01b0  63 6c 69 65 6e 74 2e 68  74 6d 6c 0d 0a 0d 0a 6d   client.h tml····m
01c0  6f 64 65 3d 31 39 31 26  75 73 65 72 6e 61 6d 65   ode=191& username
01d0  3d 4c 69 61 6d 5f 32 34  26 70 61 73 73 77 6f 72   =Liam_24 &passwor
01e0  64 3d 50 25 34 30 73 73  77 30 72 64 21 32 30 32   d=P%40ss w0rd!202
01f0  34 26 61 3d 31 37 32 35  31 36 33 39 38 39 36 38   4&a=1725 16398968
0200  30 26 70 72 6f 64 75 63  74 74 79 70 65 3d 30      0&produc ttype=0
```

```
secret_pass.pcapng        Packets: 88 · Displayed: 4 (4.5%)        Profile: Default
```

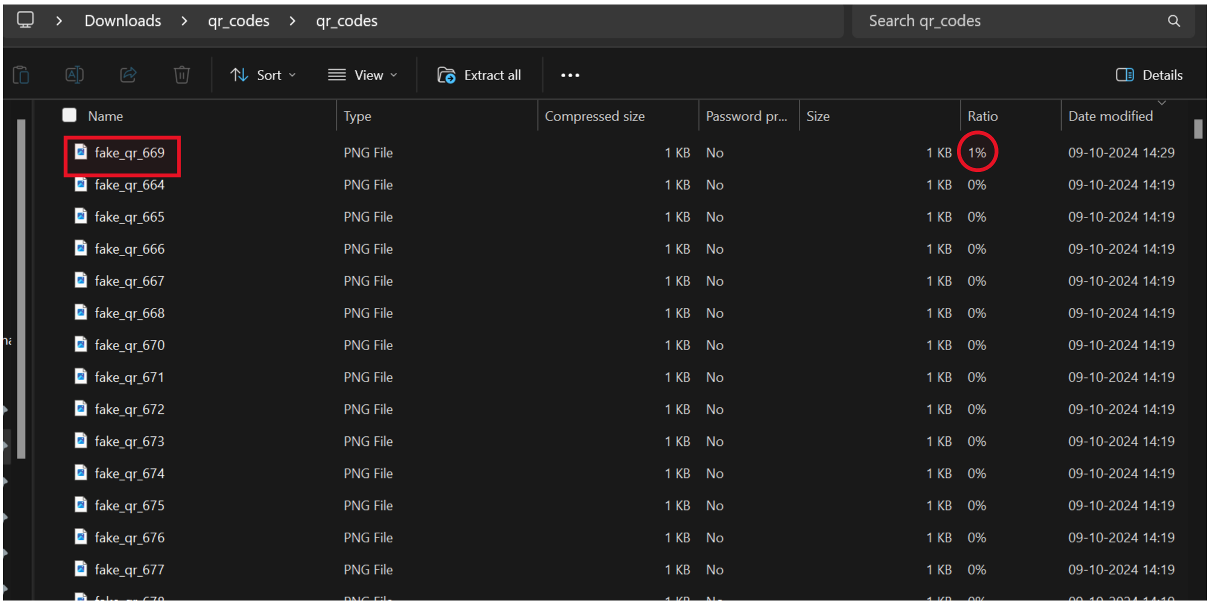
Flag obtained : root@localhost{Liam_24_P%40ssw0rd!2024}

2. PLAY WITH QRs

Problem: find the correct qr to get the flag

Steps:

1. Download the given zip file in the task
2. Check for the ratio in file manager that differs from others.

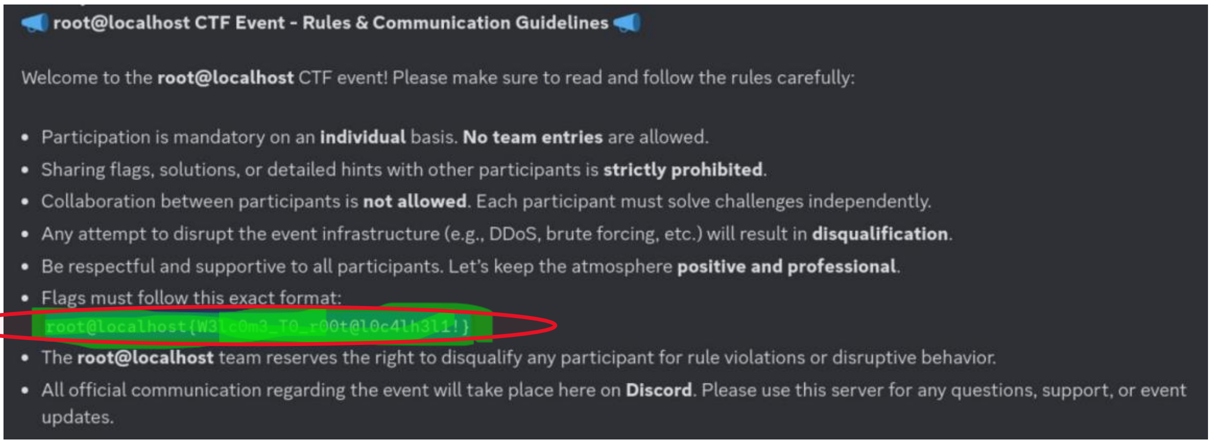


Name	Type	Compressed size	Password pr...	Size	Ratio	Date modified
fake_qr_669	PNG File	1 KB	No	1 KB	1%	09-10-2024 14:29
fake_qr_664	PNG File	1 KB	No	1 KB	0%	09-10-2024 14:19
fake_qr_665	PNG File	1 KB	No	1 KB	0%	09-10-2024 14:19
fake_qr_666	PNG File	1 KB	No	1 KB	0%	09-10-2024 14:19
fake_qr_667	PNG File	1 KB	No	1 KB	0%	09-10-2024 14:19
fake_qr_668	PNG File	1 KB	No	1 KB	0%	09-10-2024 14:19
fake_qr_670	PNG File	1 KB	No	1 KB	0%	09-10-2024 14:19
fake_qr_671	PNG File	1 KB	No	1 KB	0%	09-10-2024 14:19
fake_qr_672	PNG File	1 KB	No	1 KB	0%	09-10-2024 14:19
fake_qr_673	PNG File	1 KB	No	1 KB	0%	09-10-2024 14:19
fake_qr_674	PNG File	1 KB	No	1 KB	0%	09-10-2024 14:19
fake_qr_675	PNG File	1 KB	No	1 KB	0%	09-10-2024 14:19
fake_qr_676	PNG File	1 KB	No	1 KB	0%	09-10-2024 14:19
fake_qr_677	PNG File	1 KB	No	1 KB	0%	09-10-2024 14:19

Flag obtained : root@localhost{7h3_q6_!s_fun}

3. WELCOME

Statement : Welcome to root@localhost! To get started, check the very first announcements made in the system. Hidden within these early messages lies a clue to kickstart your journey.



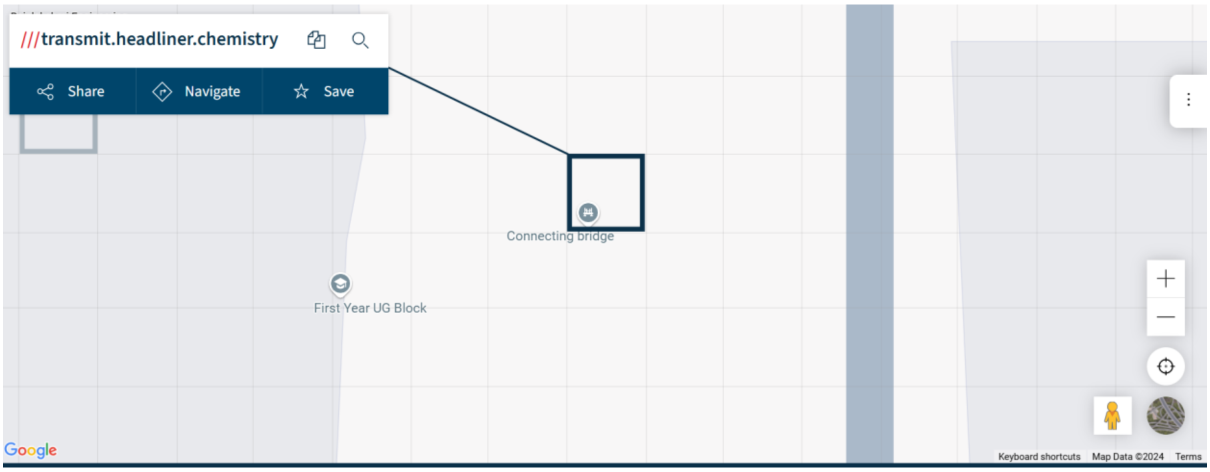
📢 **root@localhost CTF Event - Rules & Communication Guidelines** 📢

Welcome to the **root@localhost** CTF event! Please make sure to read and follow the rules carefully:

- Participation is mandatory on an **individual** basis. **No team entries** are allowed.
- Sharing flags, solutions, or detailed hints with other participants is **strictly prohibited**.
- Collaboration between participants is **not allowed**. Each participant must solve challenges independently.
- Any attempt to disrupt the event infrastructure (e.g., DDoS, brute forcing, etc.) will result in **disqualification**.
- Be respectful and supportive to all participants. Let's keep the atmosphere **positive and professional**.
- Flags must follow this exact format:
  `root@localhost{W3lc0m3_T0_r00t@l0c4lh3l1!}`
- The **root@localhost** team reserves the right to disqualify any participant for rule violations or disruptive behavior.
- All official communication regarding the event will take place here on **Discord**. Please use this server for any questions, support, or event updates.

OSINT

1. WEAK
   Problem: What is one of the most commonly used passwords in the world, often considered weak and insecure?
   Flag: 12345678
2. Locate the bridge:
   Problem: Your task is to find the connection bridge in Rajalakshmi Engineering College using What3Words. Once you locate it, note down the three words assigned to that location.
   Steps:
   1. Open what3words.
   2. Search "Rajalakshmi engineering college" in the search panel.
   3. Locate the connection bridge and note down the 3 related description words shown
   4. Put the words in flag format.



///transmit.headliner.chemistry

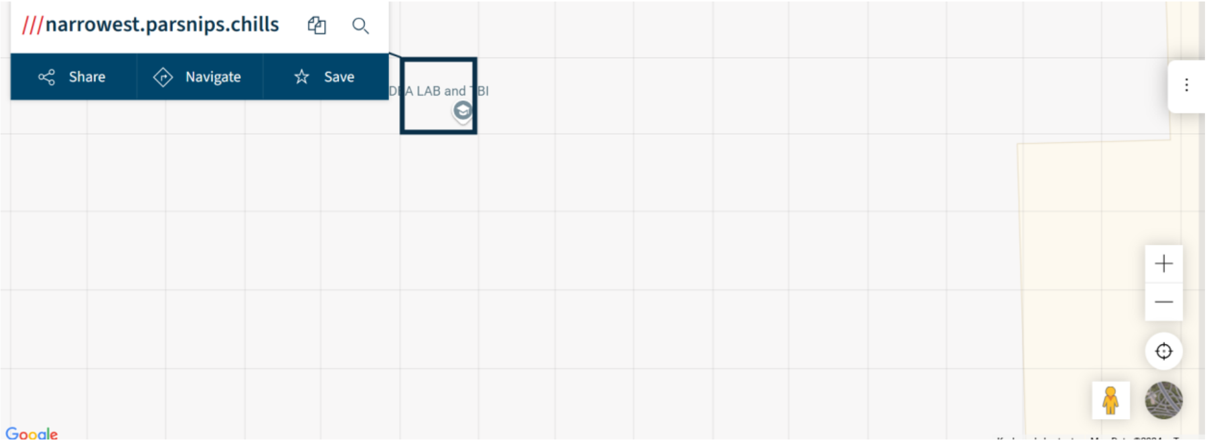
2. find the lab

Problem:

In this challenge, your mission is to locate the Idea Lab in Rajalakshmi Engineering College using What3Words. Navigate to the specific location, and retrieve the three words corresponding to it.

Steps:

1. Open what3words.
2. Search “Rajalakshmi engineering college” in the search panel.
3. Locate the idea lab and note down the 3 related description words shown
4. Put the words in flag format.



///narrowest.parsnips.chills

4. the magnetic epicenter

Problem: A certain point in Tamil Nadu is often considered to align closely with the Earth's magnetic equator. Your task is to locate this point and retrieve its what3words address.

Steps:

Search for the “certain point in Tamil Nadu is often considered to align closely with the Earth's magnetic equator.”

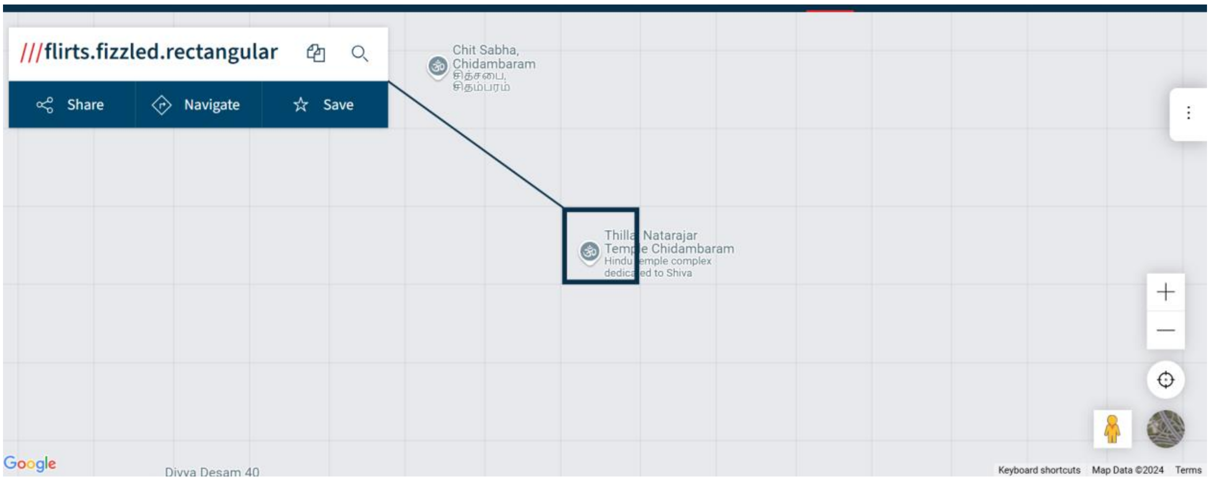
It will result in “Chidambaram Temple”

Open what3words.

Search “Chidambaram Temple” in the search panel.

Locate the idea lab and note down the 3 related description words shown

Put the words in flag format.



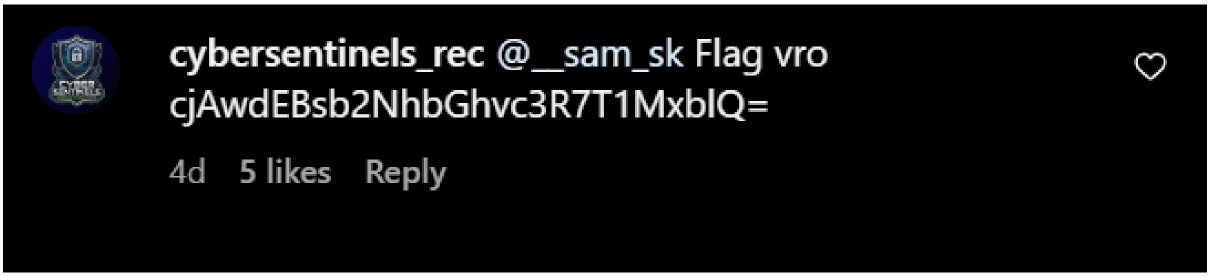
///flirts.fizzled.rectangular

5. the cyber sentinels hunt

Problem :

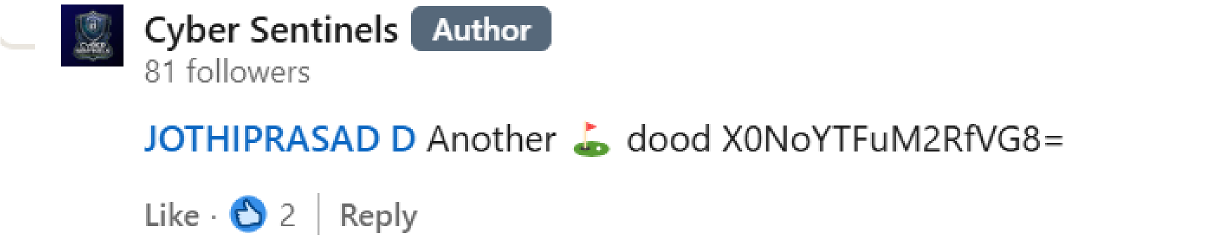
The Cyber Sentinels have left a trail of breadcrumbs across the web. Your mission is to follow their digital footprints across Instagram, LinkedIn, and Discord to uncover the flag hidden in three parts. Are you ready to decode their secrets?

1st: Instagram



cybersentinels_rec @__sam_sk Flag vro cjAwdEBsb2NhbGhvc3R7T1MxblQ=

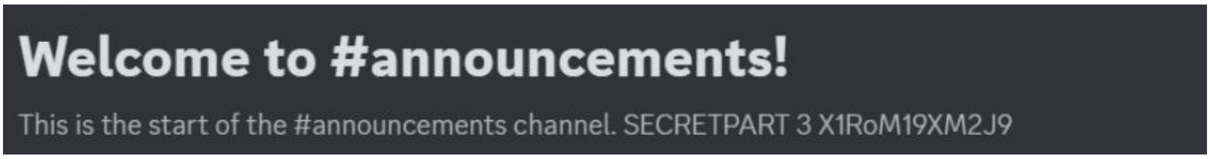
Linkedin :



Cyber Sentinels Author
81 followers

JOTHIPRASAD D Another ⛳ dood X0NoYTFuM2RfVG8=

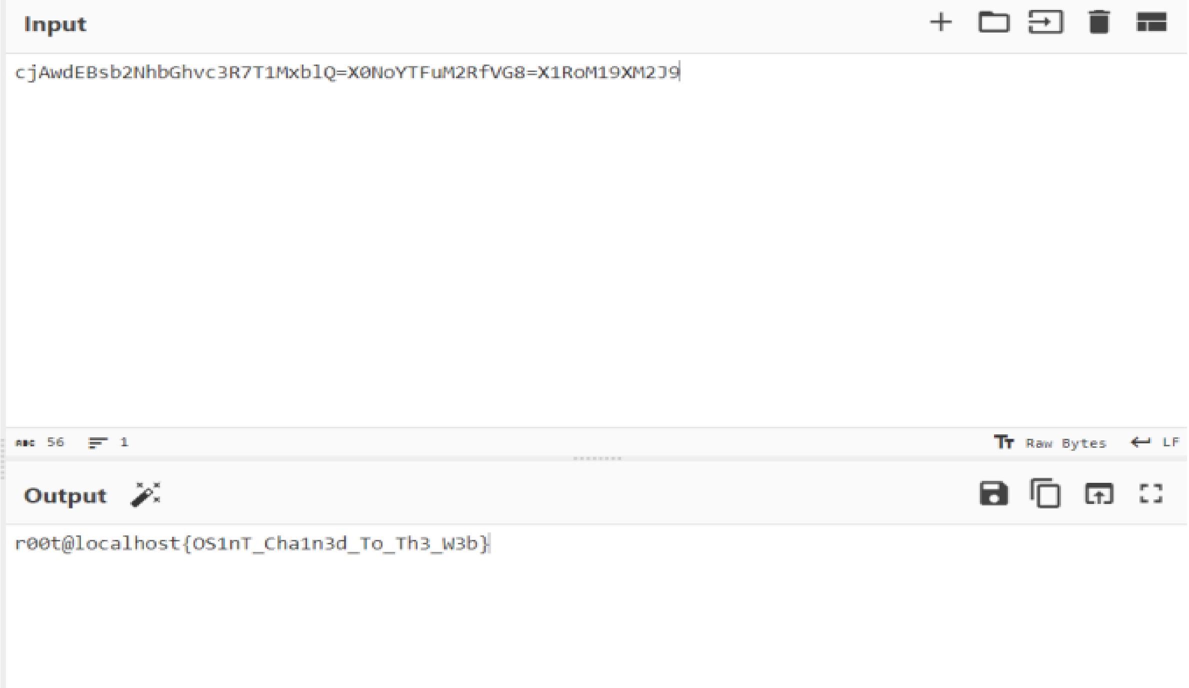
Discord :



Welcome to #announcements!

This is the start of the #announcements channel. SECRETPART 3 X1RoM19XM2J9

Giving the values on base64 to decode and flag is obtained



```
cjAwdEBsb2NhbGhvc3R7T1MxblQ=X0NoYTFuM2RfVG8=X1RoM19XM2J9
```

```
r00t@localhost{OS1nT_Cha1n3d_To_Th3_W3b}
```

WEB

Easy web

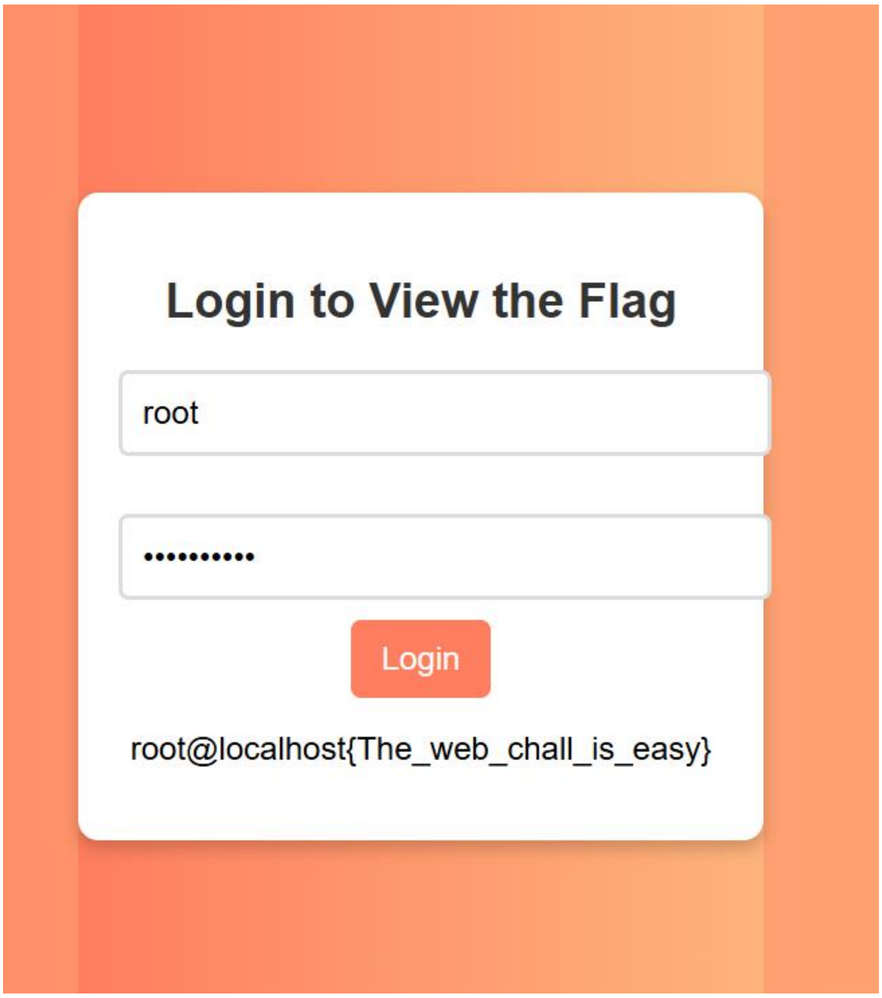
Steps:

At login page when we open the link, right click and select “view page source” .

At the elements column, there will be a script.js file.

Open the file and you can see the username and password.

Use the credentials to login the page and obtain the flag.



Login to View the Flag

root

••••••••••

root@localhost{The_web_chall_is_easy}

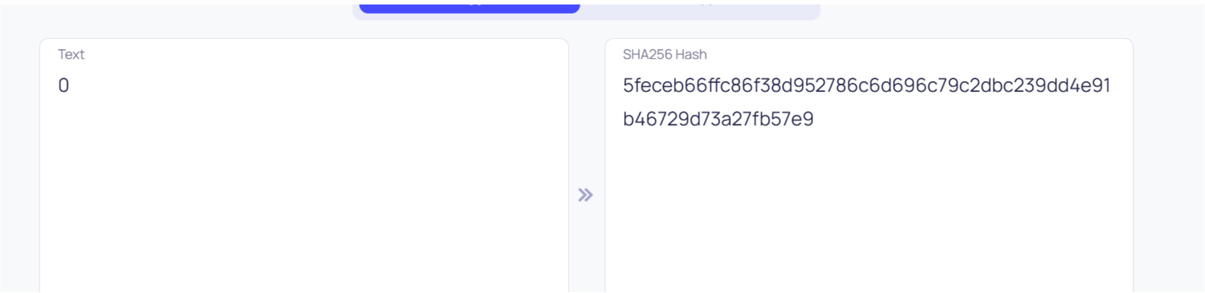
Idoor :

Open the link and you will see the fake flag

Camera= some hash values will be given.

That appears to be hashed value of 20

When we put hashed value of 0 we can obtain the flag.

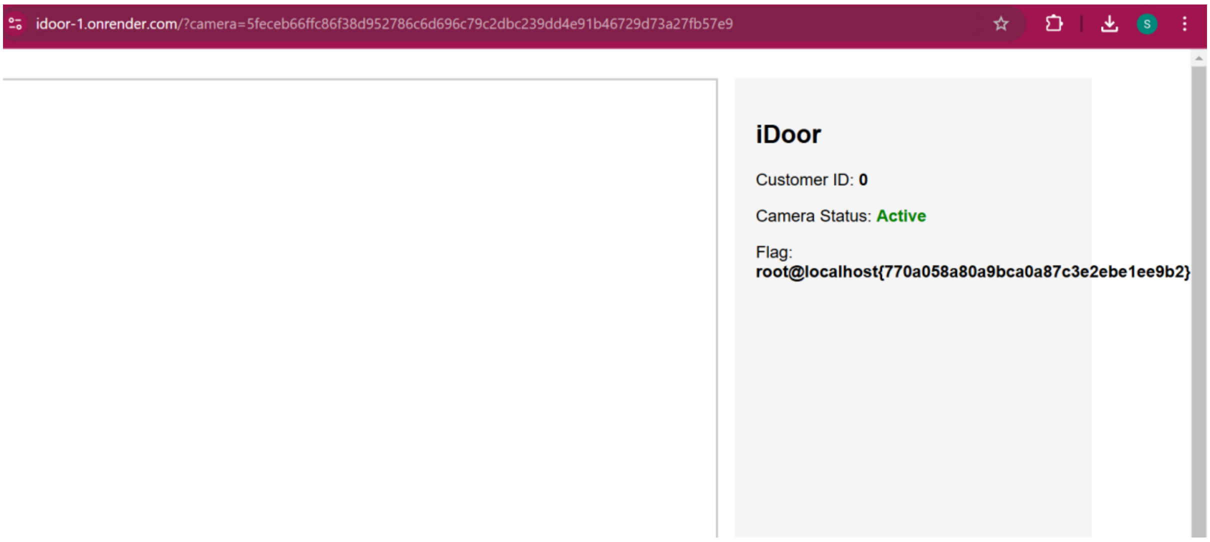


Text

0

SHA256 Hash

5feceb66ffc86f38d952786c6d696c79c2dbc239dd4e91b46729d73a27fb57e9



idoor-1.onrender.com/?camera=5feceb66ffc86f38d952786c6d696c79c2dbc239dd4e91b46729d73a27fb57e9

iDoor

Customer ID: **0**

Camera Status: **Active**

Flag:
root@localhost{770a058a80a9bca0a87c3e2ebe1ee9b2}

Stegnography:

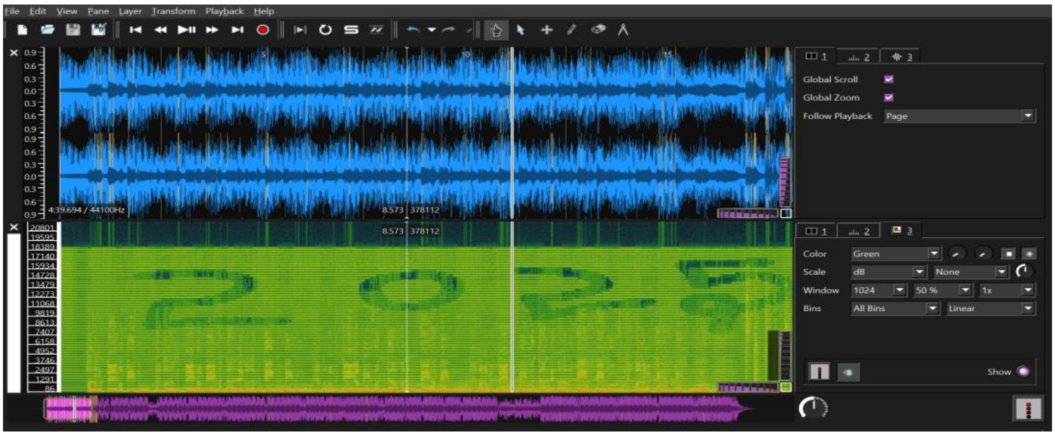
Echo of time :

Open the sonic visualizer

Open the downloaded mp3 in sonic visualizer.

Add spectogram in the song layer from the pane column

You will see the flag



Global Scroll ☑
Global Zoom ☑
Follow Playback Page

Color Green
Scale dB None
Window 1024 50 % 1x
Bins All Bins Linear

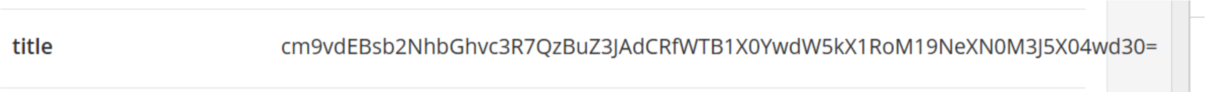
Hidden truth:

Download the png picture

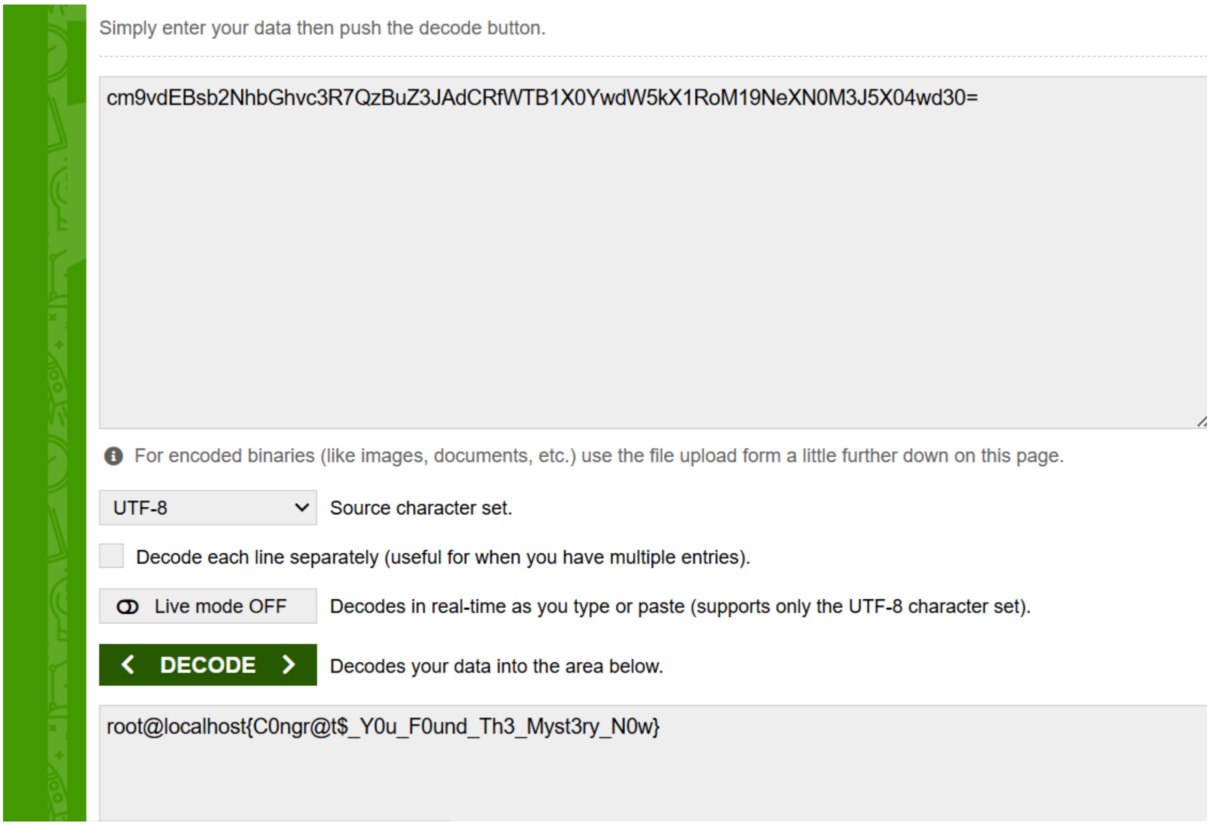
Using meta2go upload the picture and see the details description box

Hashed value will be provided in the title column

Using base64 obtain the flag



title cm9vdEBsb2NhbGhvc3R7QzBuZ3JAdCRfWTB1X0YwdW5kX1RoM19NeXN0M3J5X04wd30=



Simply enter your data then push the decode button.

```
cm9vdEBsb2NhbGhvc3R7QzBuZ3JAdCRfWTB1X0YwdW5kX1RoM19NeXN0M3J5X04wd30=
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

□ Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

DECODE Decodes your data into the area below.

```
root@localhost{C0ngr@t$_Y0u_F0und_Th3_Myst3ry_N0w}
```