

POLY CC CYBER WARRIOR 2025



WRITE UP ROKAM ANALYST

ADAM BIN MOHD AHMAD

**(ADAMAYKO)
01DDT23F1018**

KHIDTISAK A/L PRAKCHUM

**(KHID)
01DDT23F1057**

**PUTERA CARL AIRIEL BIN
ASRA KHAIRIL**

**(TERAZ1)
01DDT 23F1017**

CRYPTOGRAPHY

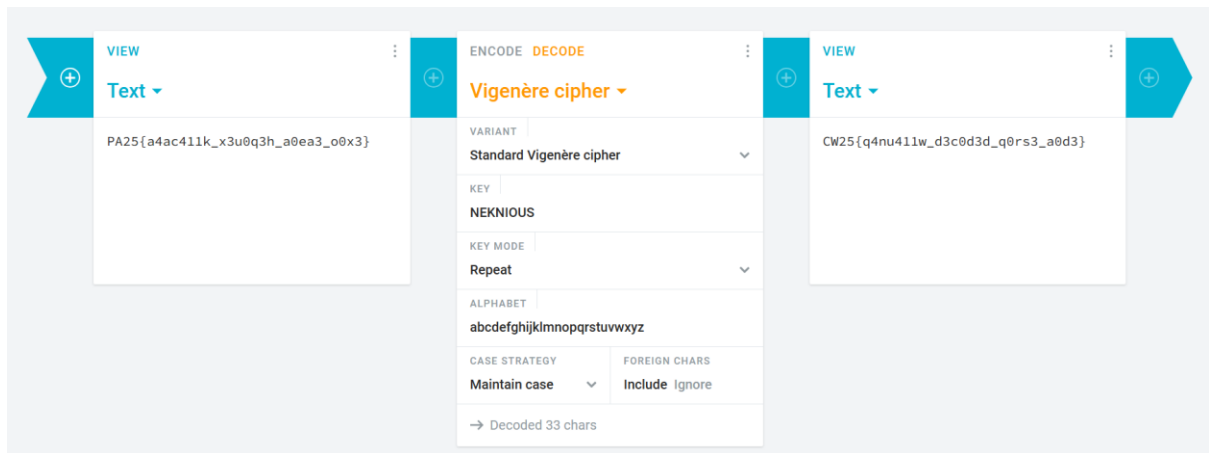
-Roblox Street Light



We need to decode the cipher text using a vigenere cipher with the key is inside the roblox game provide.

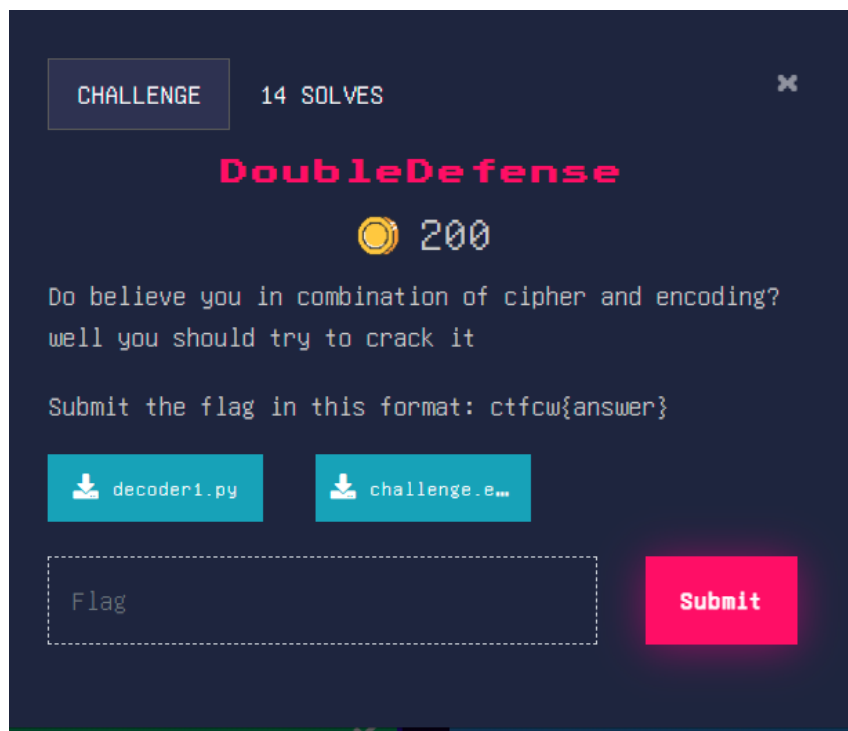


In the roblox game we can see 1 light that is flickering to the pattern of morse code. For us we couldn't get the exact morse code but the closes we can get is NEKNIOUS



Inserting the key we almost got the flag, since our key is almost right we just manually fix the flag which is CW25{m4nu411y_d3c0d3d_m0rs3_c0d3}.

-Double Defense



Both the file is downloaded and put on the same directory

```
(khid@khid)-[~/Downloads]
$ python3 decoder1.py
Decoded Flag: ctfcw{doubl3_secur3}
```

Run the python program and there is the flag.

FLAG: ctfcw{doubl3_secur3}

-Triple Triplet


CHALLENGE 10 SOLVES


Triple triplet

250

Somehow doubling the trouble is not make it harder.
Let's triple it the troublesome.

Submit the flag in this format: ctfcw{answer}

 gen_decode...

 triplet.enc

Flag

Submit

```
1 import base64
2
3 def rot13(s):
4     return s.translate(
5         str.maketrans(
6             "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz",
7             "NOPQRSTUVWXYZABCDEFGHIJKLMnopqrstuvwxyzabcdefghijklm"
8         )
9     )
10
11 def decrypt(filename):
12     with open(filename, "r") as f:
13         data = f.read().strip()
14
15     ascii_chars = data.split()
16     ascii_str = ''.join(chr(int(c)) for c in ascii_chars)
17
18     decoded_b64 = base64.b64decode(ascii_str).decode()
19
20     return rot13(decoded_b64)
21
22 if __name__ == "__main__":
23     flag = decrypt("1")
24     print("Decrypted flag:", flag)
```

Downloading the python script,we get the code shown above,we have to fix the code in order to get the flag

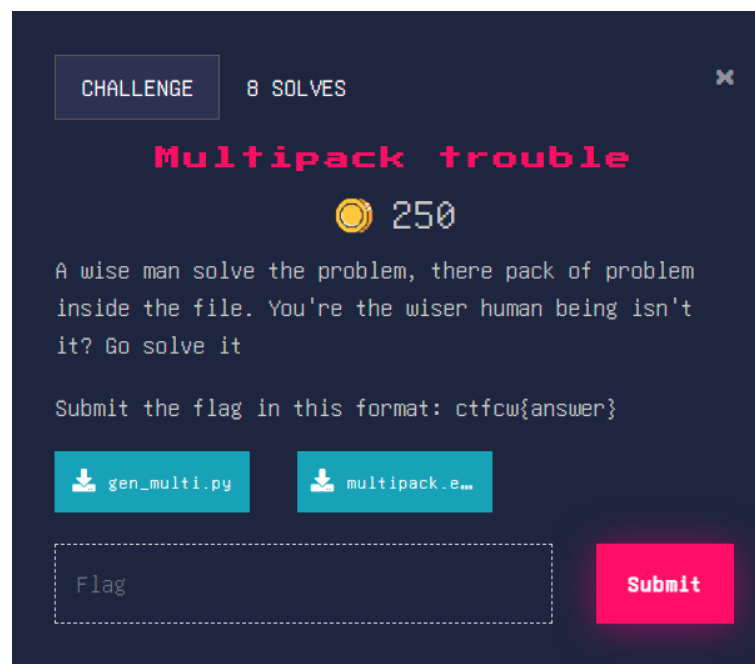
```
1 import base64
2
3 def rot13(s):
4     return s.translate(
5         str.maketrans(
6             "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz",
7             "NOPQRSTUVWXYZABCDEFGHIJKLMnopqrstuvwxyzabcdefghijklm"
8         )
9     )
10
11 def decrypt(filename):
12     with open(filename, "r") as f:
13         data = f.read().strip()
14
15
16     ascii_chars = data.split()
17     ascii_str = ''.join(chr(int(c)) for c in ascii_chars)
18
19
20     decoded_b64 = base64.b64decode(ascii_str).decode()
21
22     return rot13(decoded_b64)
23
24 if __name__ == "__main__":
25     flag = decrypt("triplet.enc")
26     print("Decrypted flag:", flag)
27
```

On line 25,we have to manually insert the file that we wanted to decrypt that is provided in the question.

```
(kali㉿kali)-[~/Downloads]
$ python3 gen_decode.py
Decrypted flag: ctfcw{triple_entente}
```

After we can run the code to get the flag which is ctfcw{triple_entente}

-Multiple trouble



```
1 import binascii
2
3 def vigenere_decrypt(cipher, key):
4     decrypted = []
5     key = key * (len(cipher) // len(key) + 1)
6     for i in range(len(cipher)):
7         c = (ord(cipher[i]) - ord(key[i])) % 256
8         decrypted.append(chr(c))
9     return ''.join(decrypted)
10
11 def decrypt_file(filename, key):
12     with open(x, "r", encoding="latin1") as f:
13         data = f.read()
14
15     b16_str = vigenere_decrypt(data, key)
16
17     ascii_str = binascii.unhexlify(b16_str).decode()
18
19     flag = ''.join(chr(int(ascii_str[i:i+3])) for i in range(0, len(ascii_str), 3))
20     return flag
21
22 if __name__ == "__main__":
23     key = "secure"
24     flag = decrypt_file("x", key)
```

Downloading the python script, we get the code shown above, we have to fix the code in order to get the flag

```
11 def decrypt_file(filename, key):
12     with open(filename, "r", encoding="latin1") as f:
13         data = f.read()
14
```

On line 12 we change the x to file name

```
26     key = "secure"
27     flag = decrypt_file("multipack.enc", key)
```

On line 27, we have to manually insert the file that we wanted to decrypt that is provided in the question.

```
26     key = "secure"
27     flag = decrypt_file("multipack.enc", key)
28     print("Your flag is:", flag)
29
```

Lastly, add a new print line to output the flag

```
(kali@kali)-[~/Downloads]
$ python3 gen_multi.py
Your flag is: ctfcw{multipack_trouble}

(kali@kali)-[~/Downloads]
$
```

After we can run the code to get the flag which is ctfcw{multipack_trouble}

-Quadruple_pack_trouble

CHALLENGE

6 SOLVES

✕

Quadruple_pack_trouble

🏆 300

Challenge by yourself with quadruple pack solving the problem, or you can give up, or you can** substitute** your friend to answer it who can speak the*** ascii*** languages. Choose wisely..

Submit the flag in this format: ctfcw{answer}

📄 decoder.py

📄 quadpack_tr...

Flag

Submit

```

1 def xor_decrypt(data, key):
2     return ''.join(chr(data[i] ^ ord(key[i % len(key)])) for i in range(len(data)))
3
4 def digit_unsubstitute(s):
5     table = str.maketrans("7643985210", "")
6     return s.translate(table)
7
8 def ascii_3digit_decode(s):
9     return ''.join(chr(int(s[i:i+3])) for i in range(0, len(s), 3))
10
11 def decrypt_file(filename, key):
12     with open(filename, "rb") as f:
13         encrypted = f.read()
14
15     substituted = xor_decrypt(encrypted, key)
16
17     ascii_str = digit_unsubstitute(substituted)
18
19     flag = ascii_3digit_decode(ascii_str)
20     return flag
21
22 if __name__ == "__main__":
23     key = "cyber"
24     flag = decrypt_file("x", key)
25     print("Decrypted flag:", flag)

```

Downloading the python script, we get the code shown above, we have to fix the code in order to get the flag

```

4 def digit_unsubstitute(s):
5     table = str.maketrans("7643985210", "0123456789")
6     return s.translate(table)

```

On line 5, Manually enter 0-9 digit for the ASCII process

```

25 if __name__ == "__main__":
26     key = "cyber"
27     flag = decrypt_file("quadpack_trouble.enc", key)
28     print("Decrypted flag:", flag)

```

On line 27, we have to manually insert the file that we wanted to decrypt that is provided in the question.

```

(kali@kali)-[~/Downloads]
$ python3 decoder(1).py
Decrypted flag: ctfcw{multipack_trouble_two}

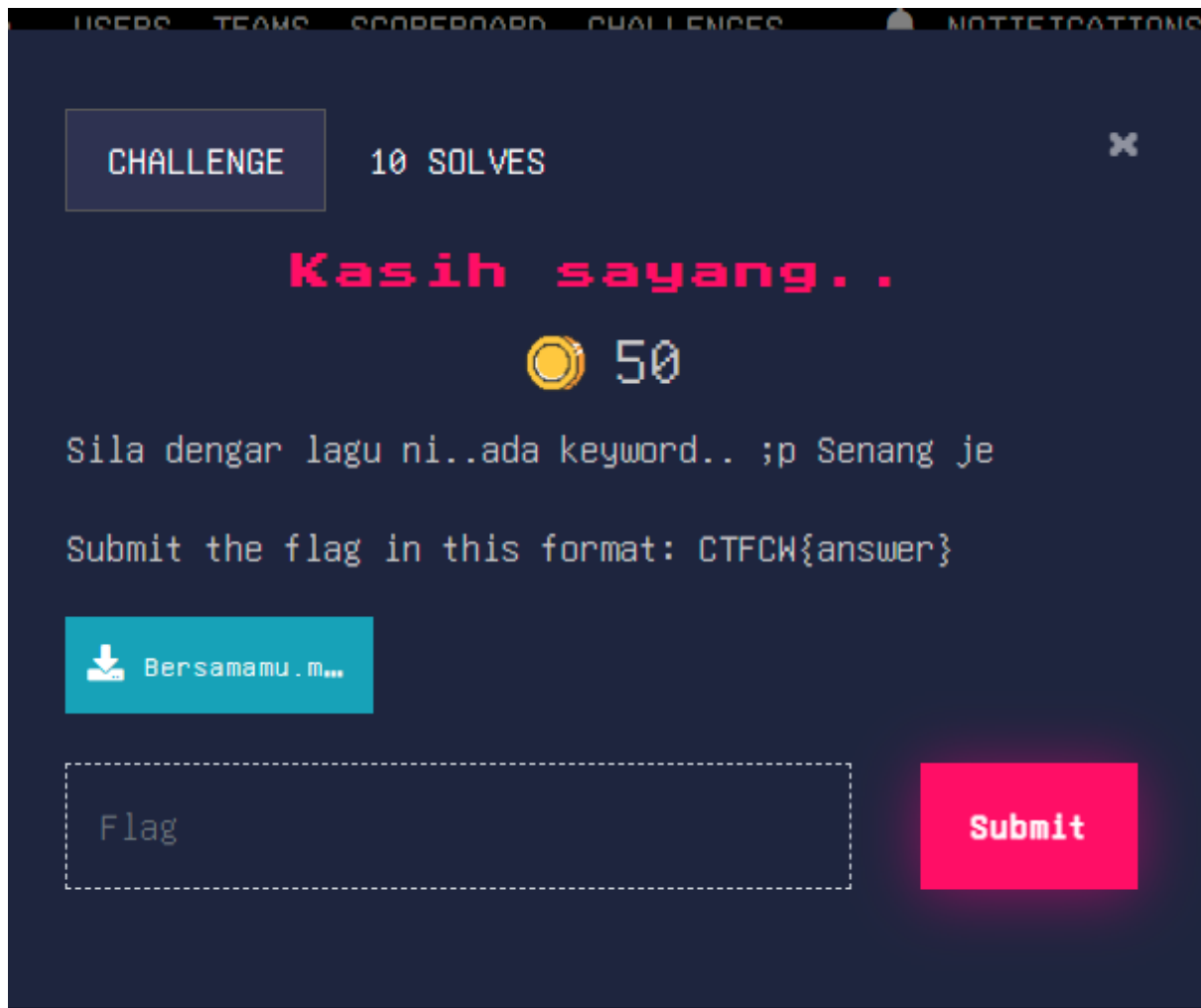
(kali@kali)-[~/Downloads]
$

```

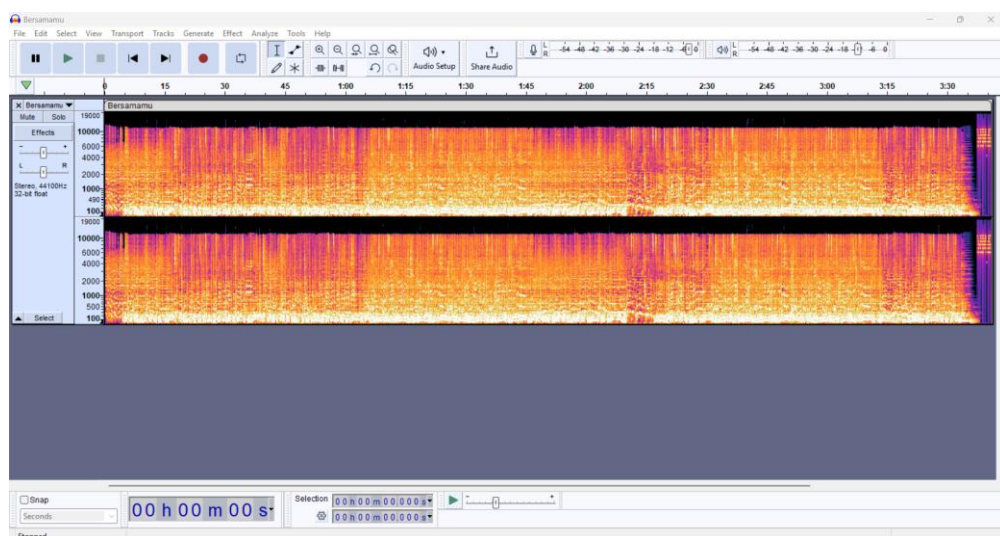
After we can run the code to get the flag which is ctfcw{multipack_trouble_two}

STEGANOGRAPHY

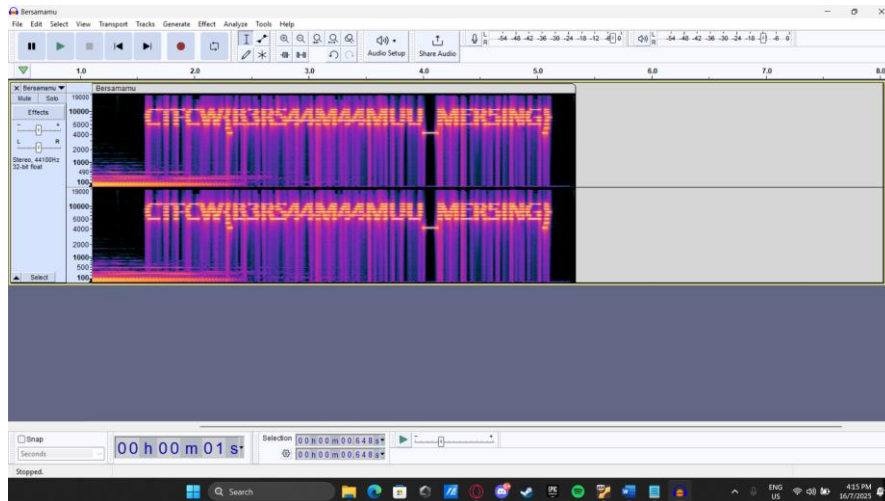
-Kasih Sayang..



We can see the file is .mp4 thus our first step is to see the spectrogram in audacity.



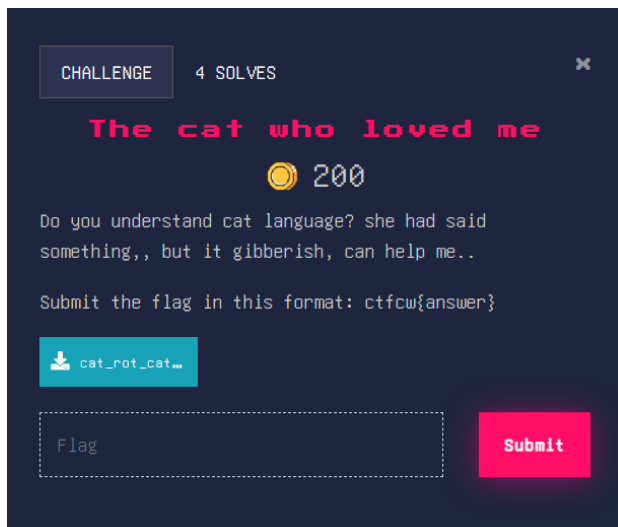
We can see the spectrogram from the audio and from the heatwave we can see at the end of the sound it is different from other.



It will reveal the flag

FLAG: CTFCW{B3RS44M44MUU_MER5ING}

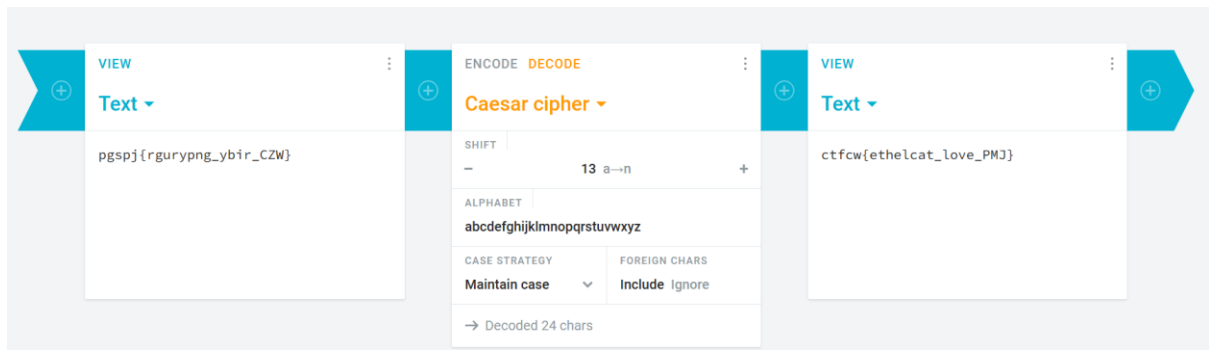
-The Cat Who Loved Me



If we download the image,we will get this picture.

[illegible]

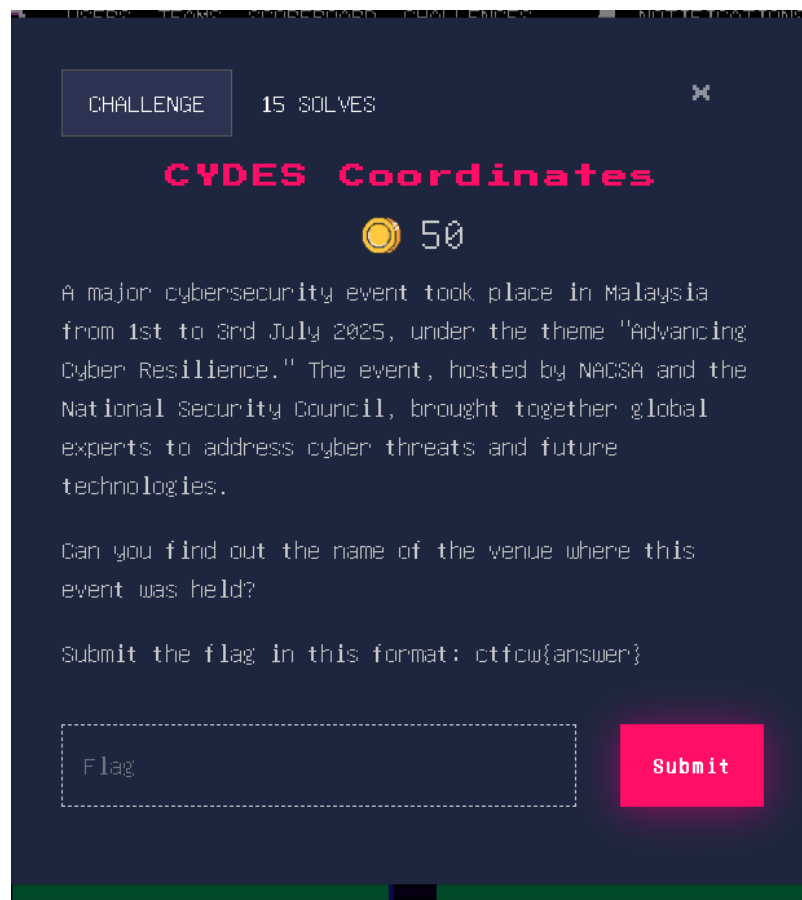
Using the zsteg command we can see the flag format in a jumbled form,we have to decode it first



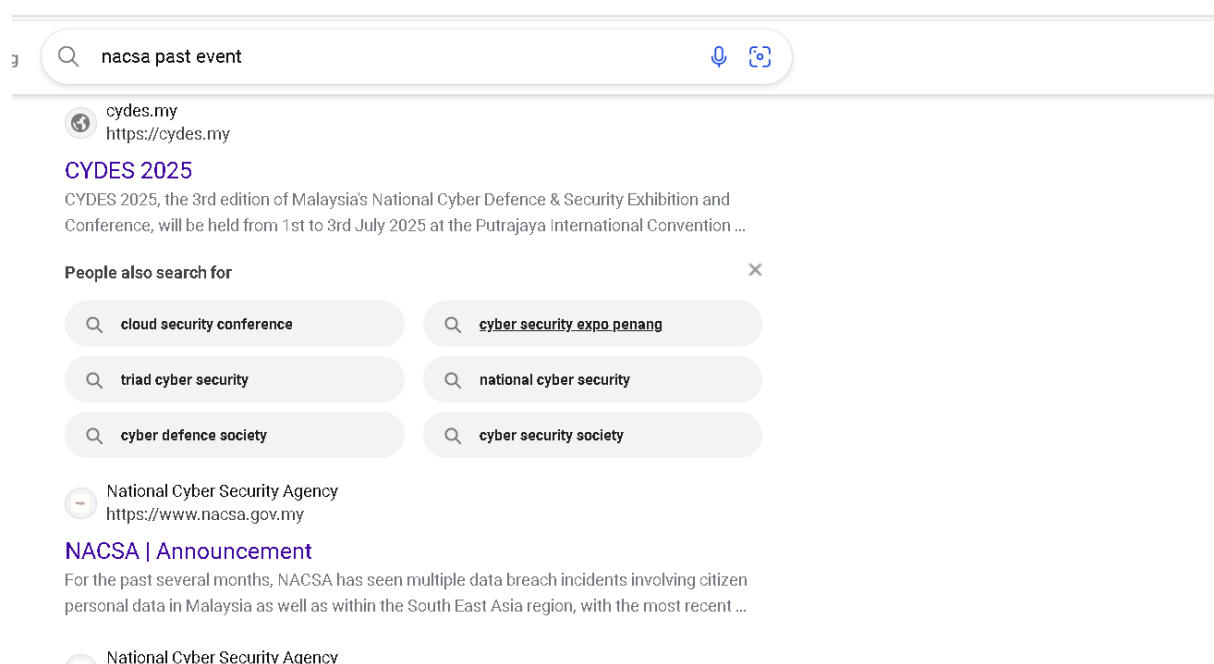
Using the ceasar cipher we will get the flag which is `ctfcw{ethelcat_love_PMJ}`

OPEN SOURCE INTELLIGENT OSINT

-Cydes Coordinates



For Cydes coordinates, the keypoint of question is NACSA and the date and event.



Now,search Nacsa past event since it was the past event happened.

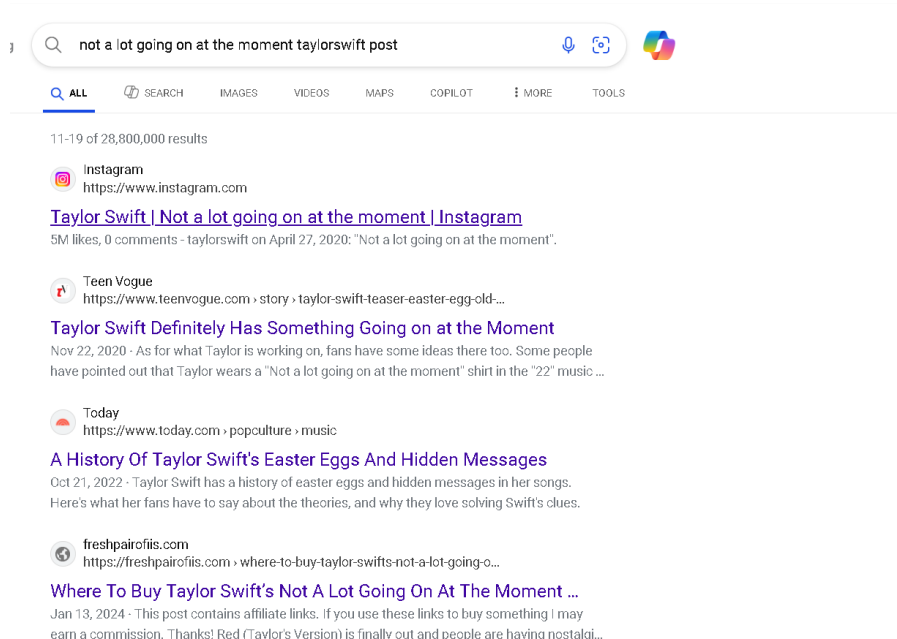


Now we see a past event from nacsa and the date is same with the question.The answer was the venue of the event which is **ctfcw{putrajaya_international_convention_centre (picc),putrajaya}**

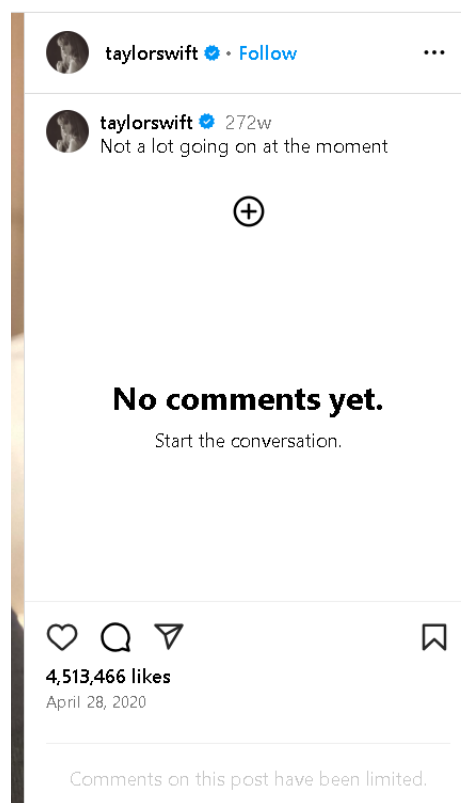
-Not A Lot Going At The



For this question,the main highlighted point is the caption and the artist



Now with the point,we search for “not a lot going at the moment taylor swift post” and we can get the post by taylor swift with the caption



We can see the date here is April 28 2020 and we ned to find what is she doing at that date.From research,we can know that she was completing and album called “Folklore” and the flag was **ctfcw{2020_04_28,folklore}**

-Forgotten Lyrics

CHALLENGE

13 SOLVES

✕

Forgotten Lyrics

50

Before stadium tours and re-recordings, Taylor Swift left her mark in a movie not everyone remembers she was part of. While the spotlight wasn't hers, the lyrics were.

In 2009, a film featured a song performed by another major pop star, one that Swift wrote, quietly, behind the scenes. She even made a brief on-screen appearance, guitar in hand.

Identify the full title of the song Taylor Swift wrote for the film, but did not perform herself, a song that played a key emotional role in the story, even if her name didn't appear in the opening credits.

Flag format: CW25{song_title} Flag Case Sensitive (All lowercase letter)

Flag

Submit

2009 taylor swift song in movie

All

Videos

Short videos

Images

Forums

Shopping

News


More

Tools

AI Overview

The Taylor Swift song featured in the 2009 movie Hannah Montana: The Movie is **"Crazier"**. Swift also co-wrote the movie's closer, "You'll Always Find Your Way Back Home". She made a cameo appearance in the movie, performing "Crazier" during a scene.

You can watch the music video for the song here:



Crazier - Wikipedia

For the song by Gary Numan

For a definition of the term

Wikipedia

Every Taylor Swift Song

FLAG: CW25{youll_always_find_your_back_home}

-No Deal

CHALLENGE 8 SOLVES X

No Deal

100

In March 2025, a cyberattack targeted Malaysia's main airport operator. A top government official publicly announced that no ransom would be paid to the attackers.


Find the full name of the person.

Submit the flag in this format:
ctfcw{xxxx_xxxxx_xxxxxxx}

Submit


march 2025 ransomware attack malaysia airport X 🔍

All News Images Videos Forums Shopping Web More Tools

**Condition Zebra**
<https://condition-zebra.com> › Blog


The Malaysian Airport Ransomware Case

14 Apr 2025 — In March 2025, **Malaysia Airports Holdings Berhad (MAHB)**—operator of **KLIA**—was hit by a ransomware attack that disrupted operations and triggered ...

**Malay Mail**
<https://www.malaymail.com> › malaysia › 2025/03/26

KLIA cyberattack: Sources dispute MAHB and Nacsa's ...

Yesterday, MAHB confirmed that a cybersecurity threat affecting certain computer systems at KLIA was detected on **March 23**, following the ...

**Comparitech**
<https://www.comparitech.com> › Cybersecurity News

Ransomware gang says it hacked the Malaysia's Kuala ...

28 Apr 2025 — The airport announced a cyberattack **disrupted flight information displays, check-in counters, and baggage handling** starting on **March 23, 2025**, ...

Googling about the attack we can see the KLIA ransomware attack that happened in Malaysia on March 2025

klia ransom attack on malaysia airport

All News Images Videos Forums Shopping Web More Tools

Sangfor
<https://www.sangfor.com> › blog › cybersecurity › kuala-...
Kuala Lumpur Airport Cyberattack: Protecting KLIA from ...
 3 Apr 2025 — Cybersecurity **attacks** on the aviation industry are on the rise, underscoring the vulnerabilities of critical infrastructures worldwide.

Dark Reading | Security
<https://www.darkreading.com> › cyberattacks-data-breaches
Malaysian Airport's Ransomware Attack a Warning for Asia
 2 Apr 2025 — The **ransomware attack** on **Kuala Lumpur International Airport** follows several **attacks** against other targets in **Malaysia** and in the region. Last ...

Videos

Kuala Lumpur Airport Under Cyberattack, PM Refuses to Pay ...
 YouTube · Firstpost
 27 Mar 2025

Malaysia's KL International Airport hit by cyber attack, PM rejects \$10M ransom demand, emphasizing strong cyber defense measures.

Kuala Lumpur: Malaysia PM Rejects \$10 Million Ransom ...

Videos

Kuala Lumpur Airport Under Cyberattack, PM Refuses to Pay ...
 YouTube · Firstpost
 27 Mar 2025

Malaysia's KL International Airport hit by cyber attack, PM rejects \$10M ransom demand, emphasizing strong cyber defense measures.

Now googling about the KLIA attack we can see the person who reject the ransomware on the third search which the the Prime Minster for Malaysia (Anwar Ibrahim)

[<<Kembali Ke Senarai](#)

Maklumat Ahli Parlimen



MAKLUMAT

Nama	YAB Dato' Seri Anwar bin Ibrahim
Jawatan dalam Parlimen	Ketua Majlis
Jawatan dalam Kabinet	Perdana Menteri Dan Menteri Kewangan
Parti	PH
Tempat Duduk	A-1
Parlimen	P063
Kawasan	Tambun
Negeri	Perak

CHALLENGE 8 SOLVES X

No Deal

100

In March 2025, a cyberattack targeted Malaysia's main airport operator. A top government official publicly announced that no ransom would be paid to the attackers.

Find the full name of the person.

Submit the flag in this format:
ctfcw{xxxx_xxxxx_xxxxxxx}

ctfcw{seri_anwar_ibrahim}


Submit

Googling his name will get the full name and the flag which is ctfcw{seri_anwar_ibrahim}


-The Dome Of Light

CHALLENGE

6 SOLVES




The Dome of Light

 150

Look at the image. Find out where it was taken and the year the place opened.

Submit the flag in this format: `ctfcw{answer}`

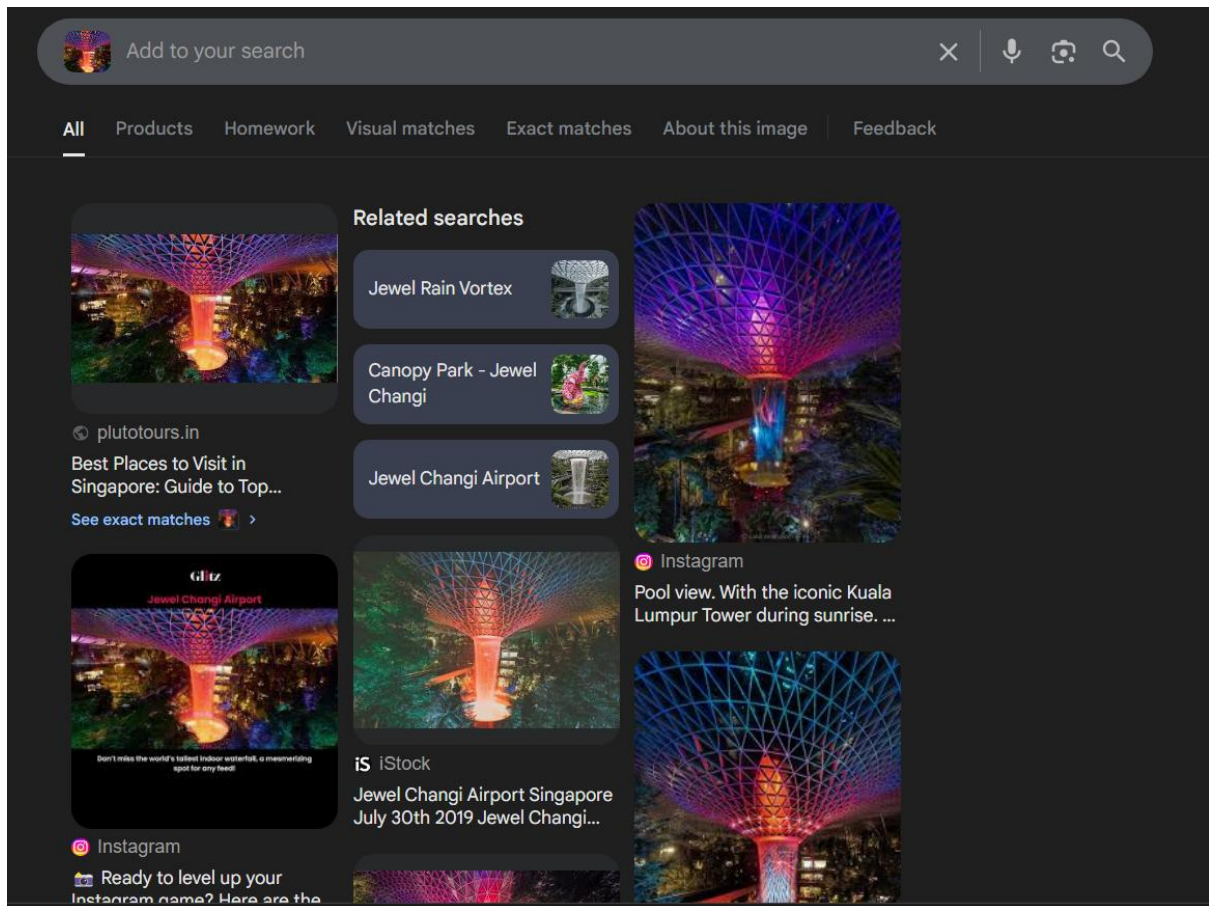
 night-view-...

Flag

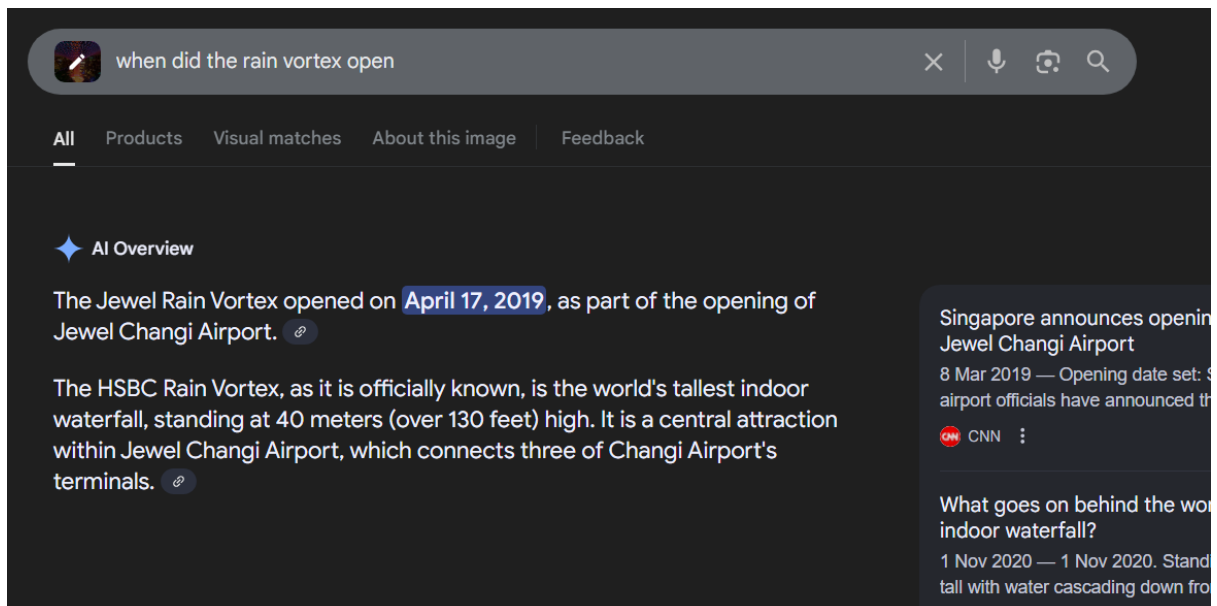
Submit



Downloading the image will the this picture.



By google reverse the picture,we will get this which is the place name (Rain Vortex)



To get the year,we just simply google when did it open and the answer is 2019

CHALLENGE

6 SOLVES


×

The Dome of Light

150

Look at the image. Find out where it was taken and the year the place opened.

Submit the flag in this format: `ctfcw{answer}`

 night-view-...

`ctfcw{rain_vortex_2019}`

Submit

Combining the two answer we will get the flag `ctfcw{rain_vortex_2019}`

-Neon ScrambleLive

CHALLENGE

10 SOLVES

×

Neon Scramble Live

150

A public live webcam shows thousands of people crossing in all directions when the lights turn green, surrounded by commercial buildings and bright neon billboards.

Find the exact GPS coordinates (to 4 decimal places) for the center of this intersection as seen from the live webcam feed.

Submit the flag in this format: `ctfcw{answer}`

Flag

Submit

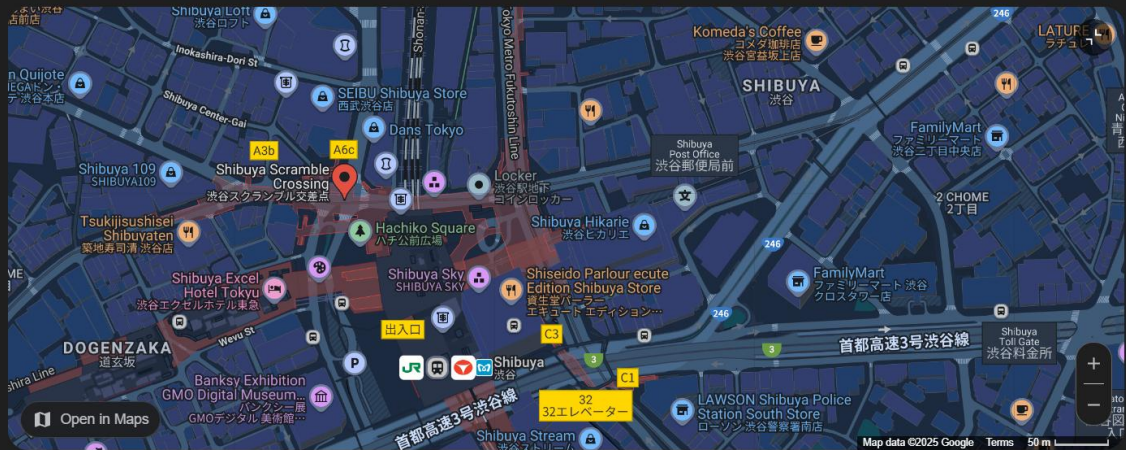
Shibuya Scramble Crossing

4.5 ★ (14K) · Tourist attraction in Shibuya, Japan

Overview

Reviews

Tickets

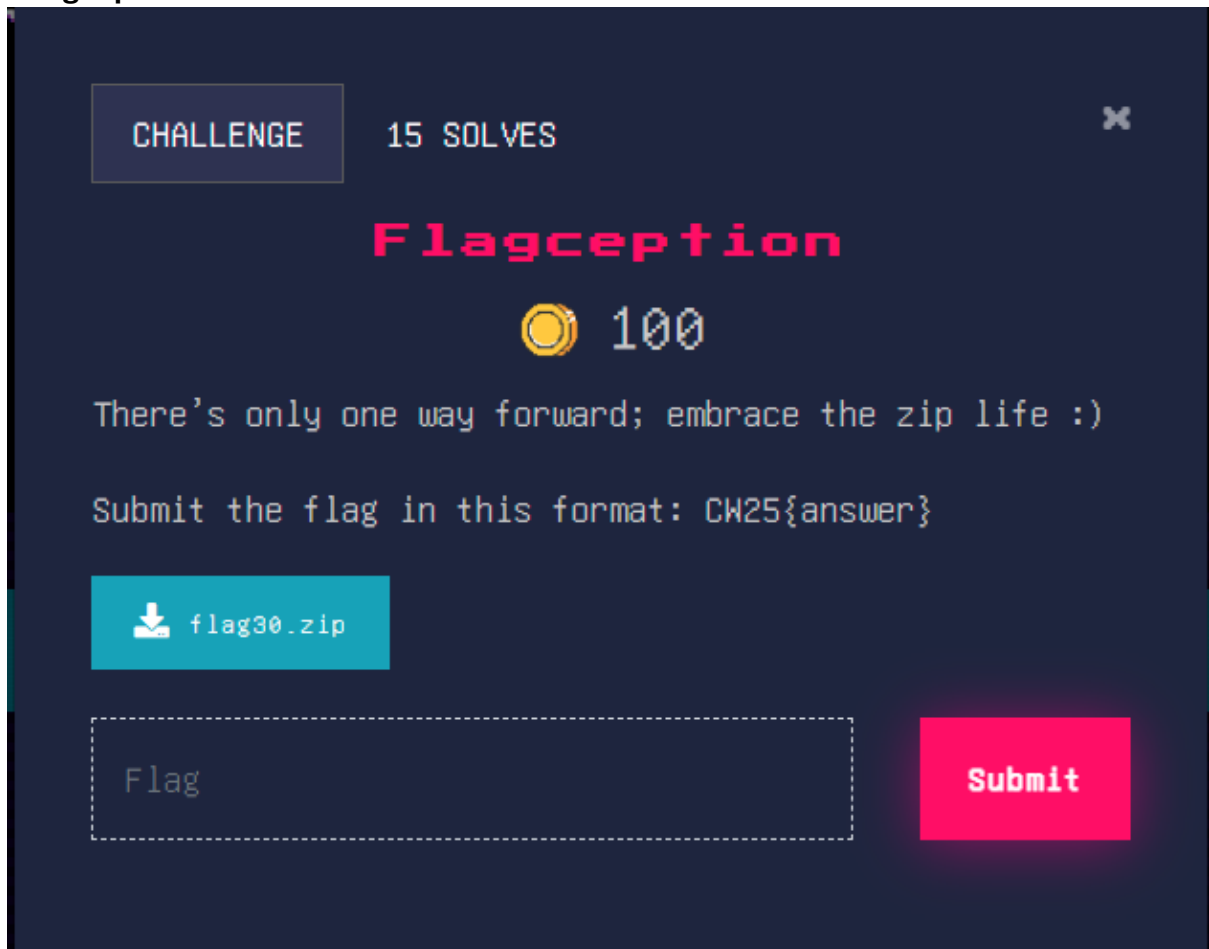


35.6595° N, 139.7006° E

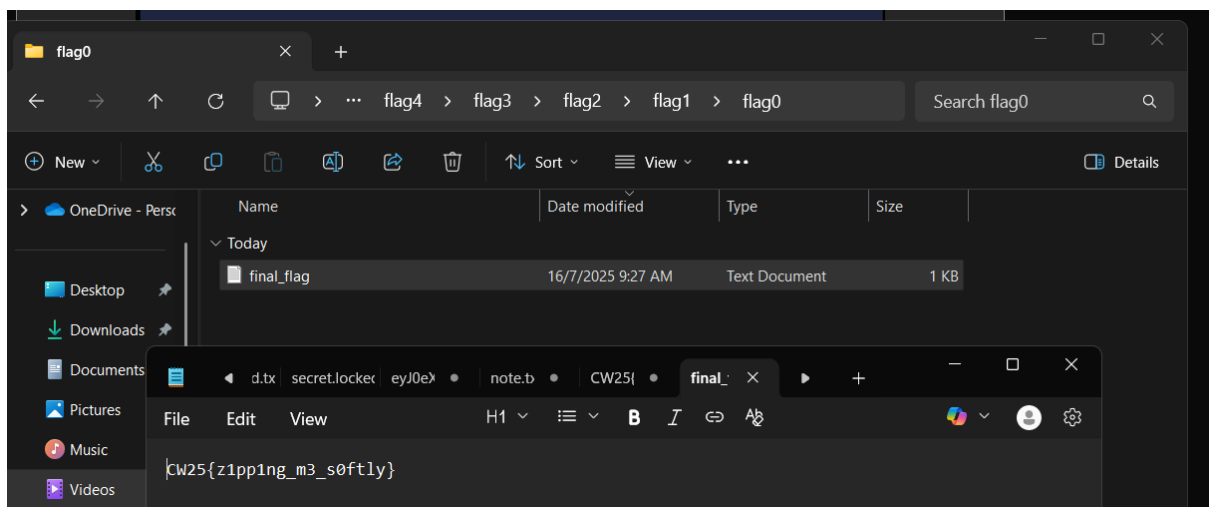
FLAG: ctfcw{35.6595_139.7006}

MISCELLANEOUS (MISC)

-Flagception

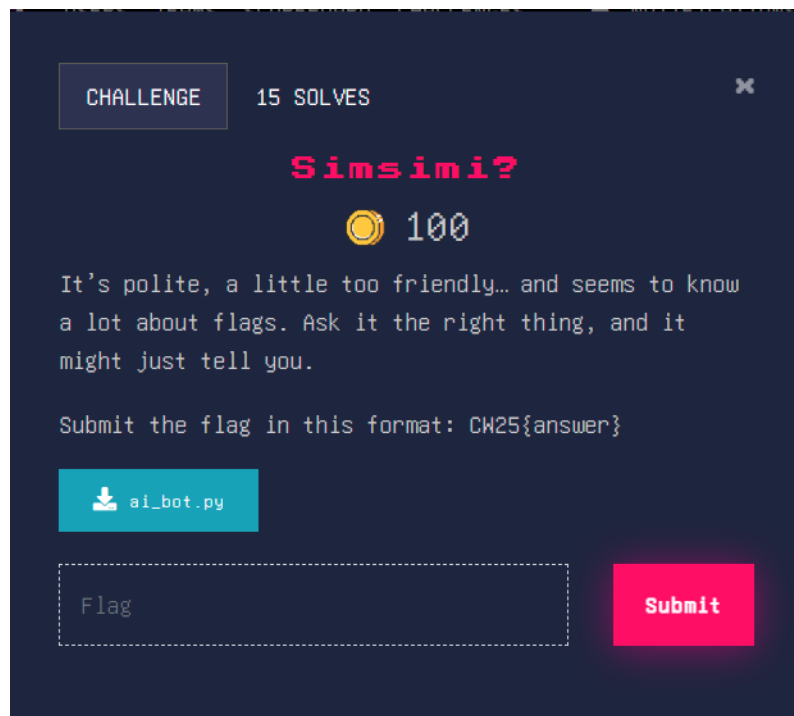


The zip files contain another zip files, and to get the flag , we can make a script or do it manually, in this case we do it manually because it is only 30 files and make a script for it probably takes longer than manually doing it.



FLAG: CW25{z1pp1ng_m3_s0ftly}

-Simsimi?



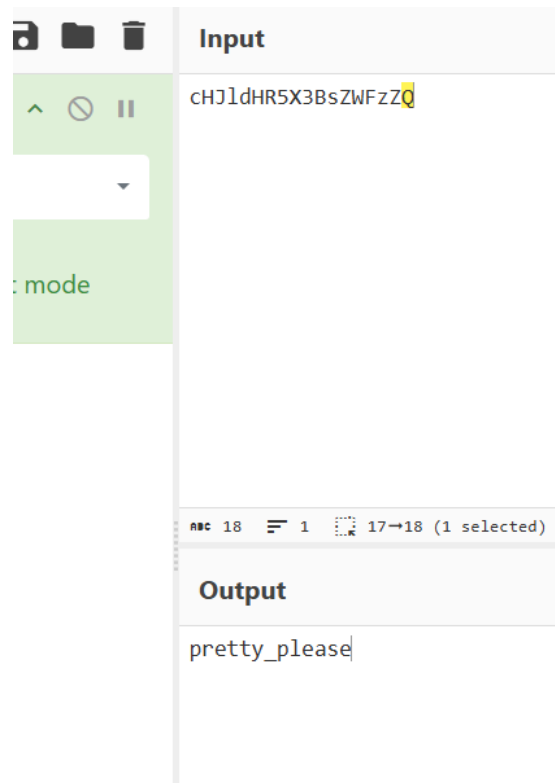
Looking into the code of the bot, the flag is listed in the code in base64 decrypt it and we got the flag

```
elif "flag" in user_input:
    fake_flags = [
        "flag(definitely_not_the_flag)",
        "flag(you thought)",
        "flag(nah bro try again)",
        "flag(omg_stop_trying)"
    ]
    slow_print(f"Bot: Oh you want a flag? Here, take this: {random.choice(fake_flags)}")

elif "pretty please" in user_input or "pls" in user_input:
    real_flag = base64.b64decode("cHJldHR5X3B5ZWZzZ0==").decode()
    slow_print("Bot: ...ugh. Fine. But only because you begged hihi")
    time.sleep(1)
    slow_print(f"Bot: Here's your flag: CW25{real_flag}")
    break

elif "potato" in user_input:
    slow_print("Bot: Are you projecting?")

elif "hello" in user_input or "hi" in user_input:
    responses = ["Yo.", "No.", "I'm busy.", "Hi I guess.", "Sup."]
    slow_print(f"Bot: {random.choice(responses)}")
```

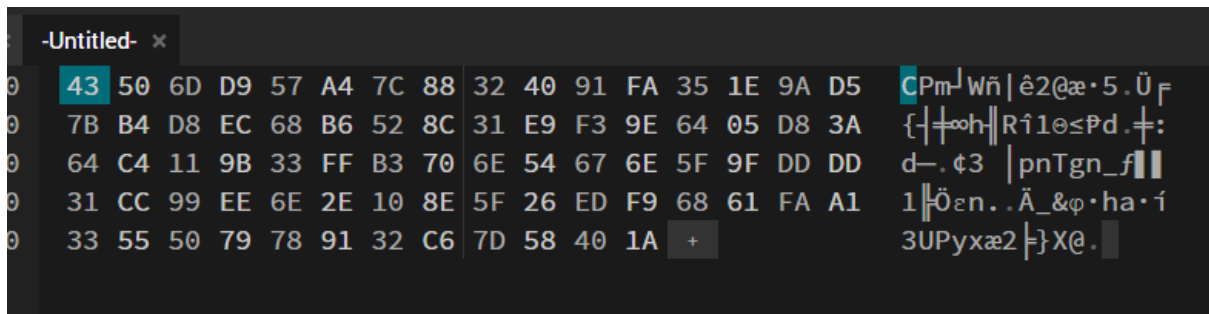
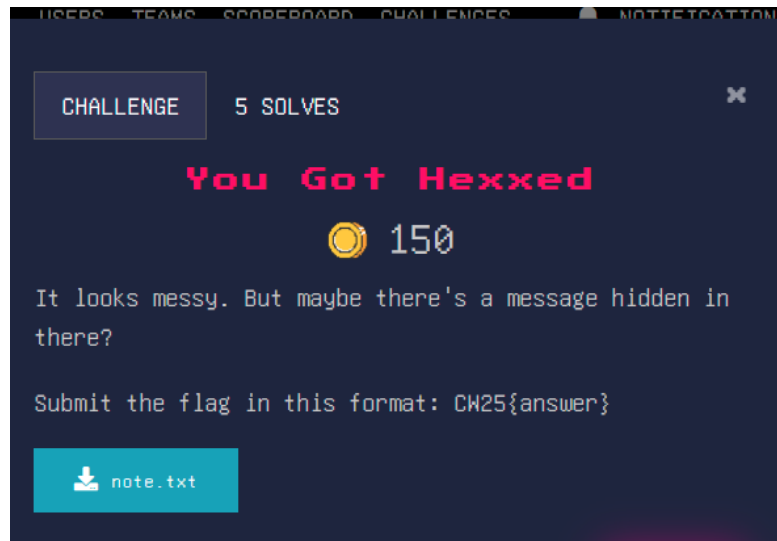


FLAG: CW25{pretty_please}

[illegible]

FLAG: CW25{keyboard_go_brrrrrrrr}

-You Got Hexxed

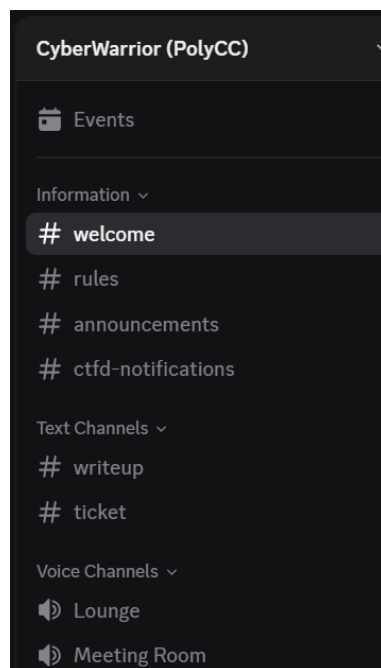
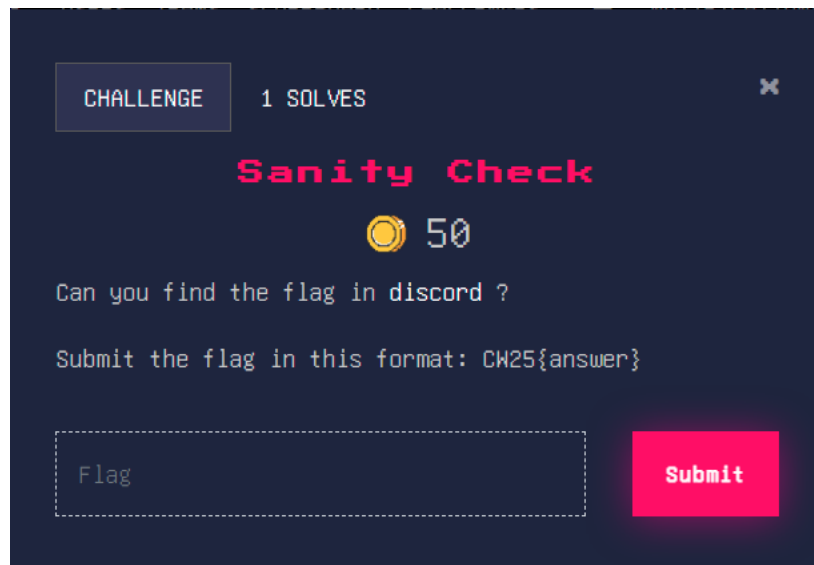


From the hex, just look at the strings and list it out and eventually the flag is easily found

FLAG: CW25{h1dd3n_1n_h3x}

GENERAL

-Sanity Check



By clicking on the “discord” button,you will be invited to the Cyberwarrior official server.





FeiNafali 7:57 AM

^ "Click Create Ticket" for sanity check, state the questions.

EG. Questions: Scanning Machine

Description: Is this the correct flag > CW25{UzRuMXR5X0NoM2Nr} (edited)

Under the ticket section, you can see the user FeiNafali chatted about how to submit a ticket. In the description, we can see the flag but need to decode it first

The screenshot shows a web-based Base64 decoder interface. It consists of three main panels. The left panel, labeled 'VIEW' and 'Text', contains the input string 'UzRuMXR5X0NoM2Nr'. The middle panel, labeled 'ENCODE' and 'DECODE', has 'Base64' selected as the encoding variant. Below this, it shows 'Base64 (RFC 3548, RFC 4648)' and a button to 'Decoded 12 bytes'. The right panel, labeled 'VIEW' and 'Text', displays the decoded output 'S4n1ty_Ch3ck'.

Decoding it with Base64, we will get the flag CW25{S4n1ty_Ch3ck}.