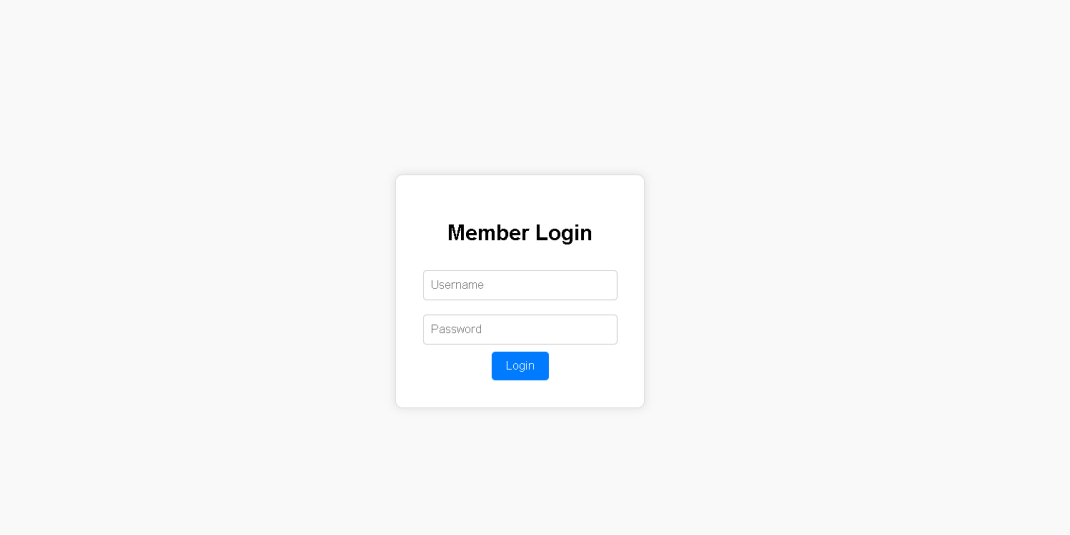
CTF CYBER WARRIOR 2025

TEAM ROKAM ANALYST WRITE UP
30/5/2025

MEMBERS:
adamayko
khid
Teraz1

WEB EXPLOITATION

1)Invalid Credentials

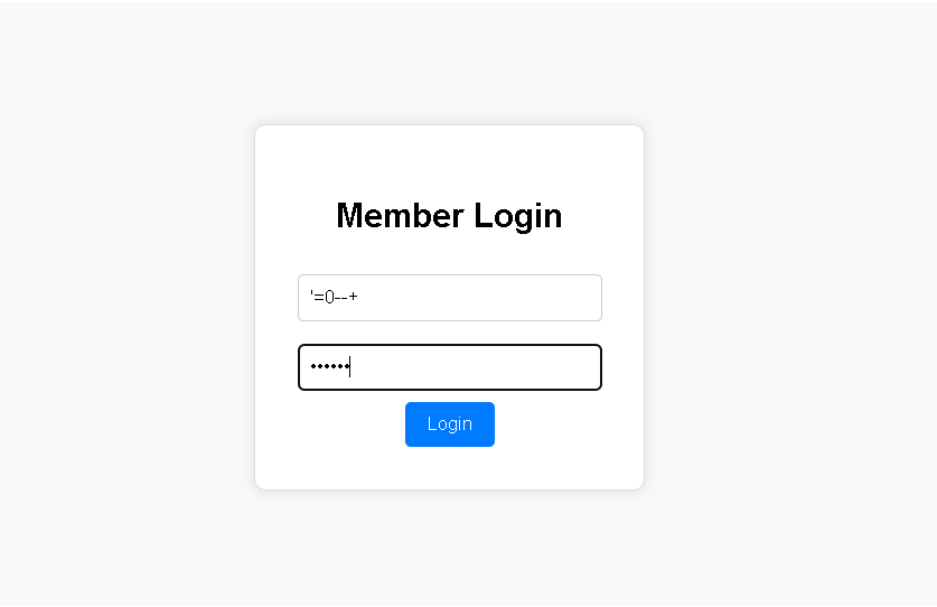


This is the main webpage for invalid credentials.As we can see the page need to be a login using username and password.For the solution we can use the swl injection method.

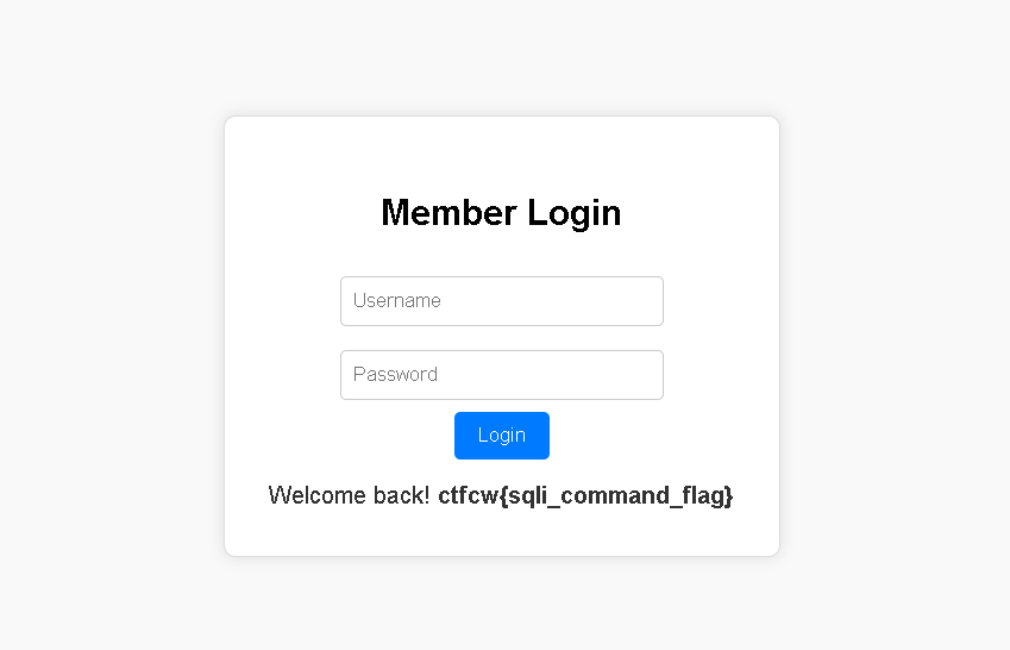
Generic SQL Injection Payloads

```
'
''
`
``
,
"
""
/
//
\
\\
;
' or "
-- or #
' OR '1
' OR 1 -- -
" OR "" = "
" OR 1 = 1 -- -
' OR '' = '
'='
'LIKE'
'=0--+
 OR 1=1
' OR 'x'='x
' AND id IS NULL; --
''''''''''''UNION SELECT '2
%00
/*…*/
+               addition, concatenate (or space in url)
||              (double pipe) concatenate
%               wildcard attribute indicator
```

Now open a sql injection payload list from any source and try each combination to the username and password.

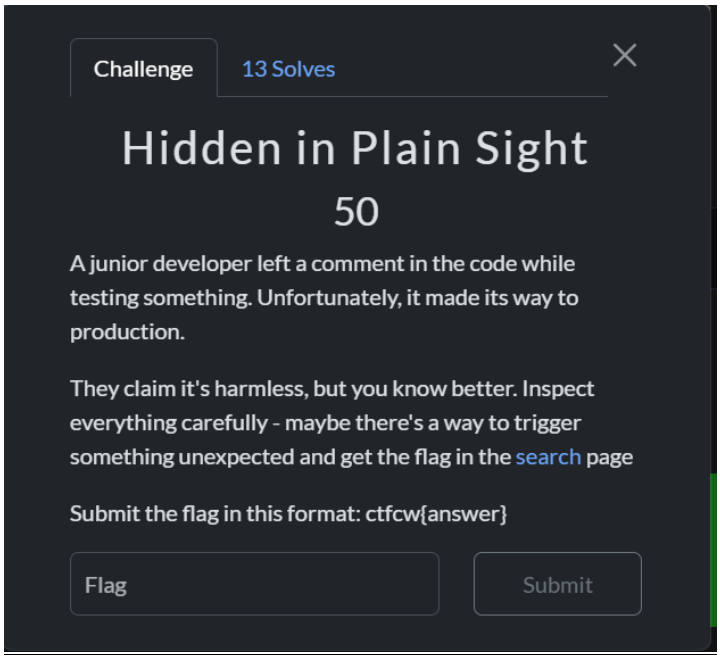


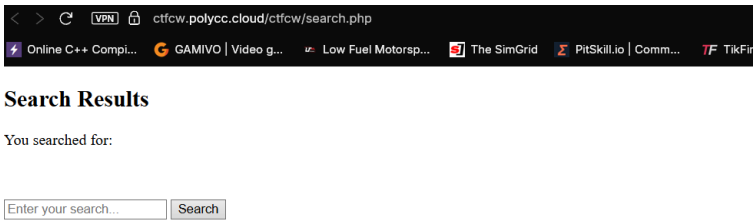
After trying the each combination.A suitable combination to bypass login system is '**=0--+**.By pressing login,the flag will be show.



The flag is **ctfcw{sqli_command_flag}.**

2)Hidden In Plain Sight





This is the search page from the link provided.

First, open the page source,

```
Line wrap
<!DOCTYPE html>
<html>
<head>
    <title>Search</title>
    <!--assets/pc.js -->
</head>
<body>
    <h2>Search Results</h2>
    <p>You searched for: </p>
    <br><br>
    <form method="GET" action="">
        <input type="text" name="query" placeholder="Enter your search..." required>
        <input type="submit" value="Search">
    </form>
</body>
</html>
```

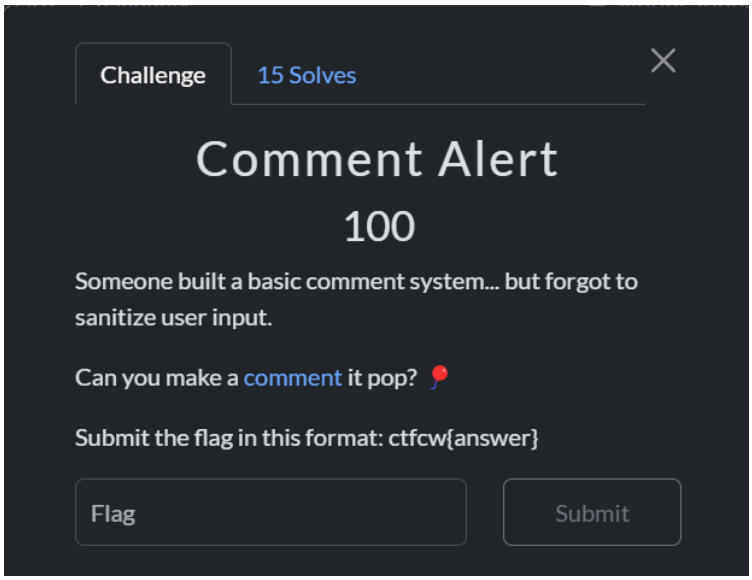
This is the page source, highlighted in green is some type or file directory that can be put in our link.

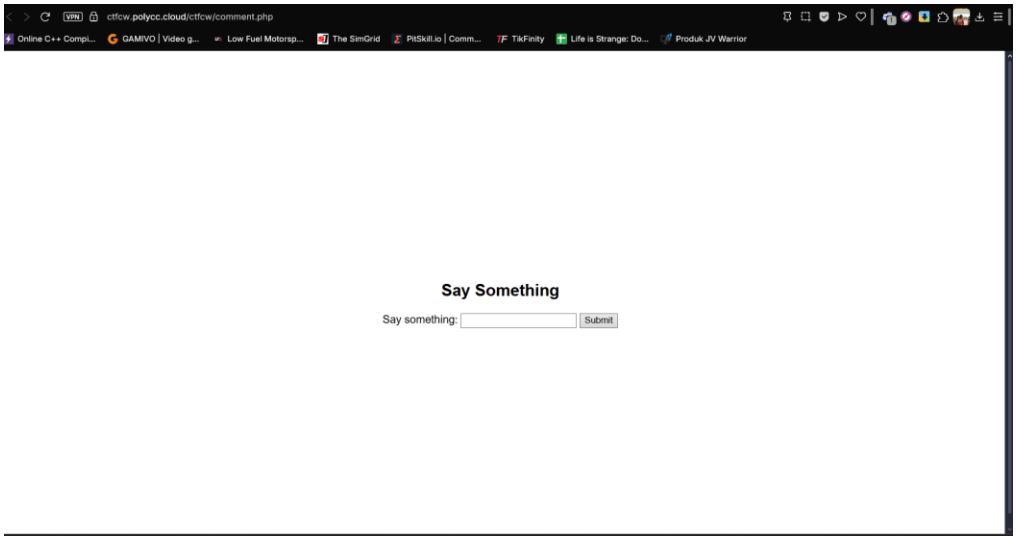
```
VPN  ctfcw.polycc.cloud/ctfcw/assets/pc.js
Online C++ Compi...   GAMIVO | Video g...   Low Fuel Motorsp...

// assets/pc.js
alert("ctfcw{reflected_xss_master}");
```

After putting the directory on the link, the flag will be shown

ctfcw{reflected_xss_master}

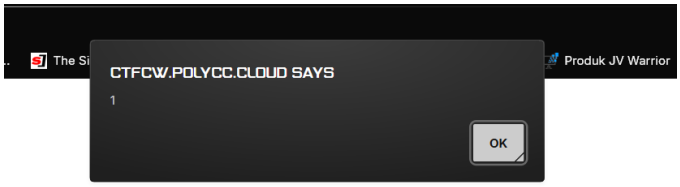
3)Comment Alert





This is the website open using the link provided.

Basic approach during ctf if there are website like this is trying to exploit the XSS, in this case I tried with the script <script>alert(1)</script> because the question mentioned something about pop, this script basically will activate pop up.



Upon submitting it, the pop-up will pop and when press “OK”

ctfcw{popup_trigger}

You said:

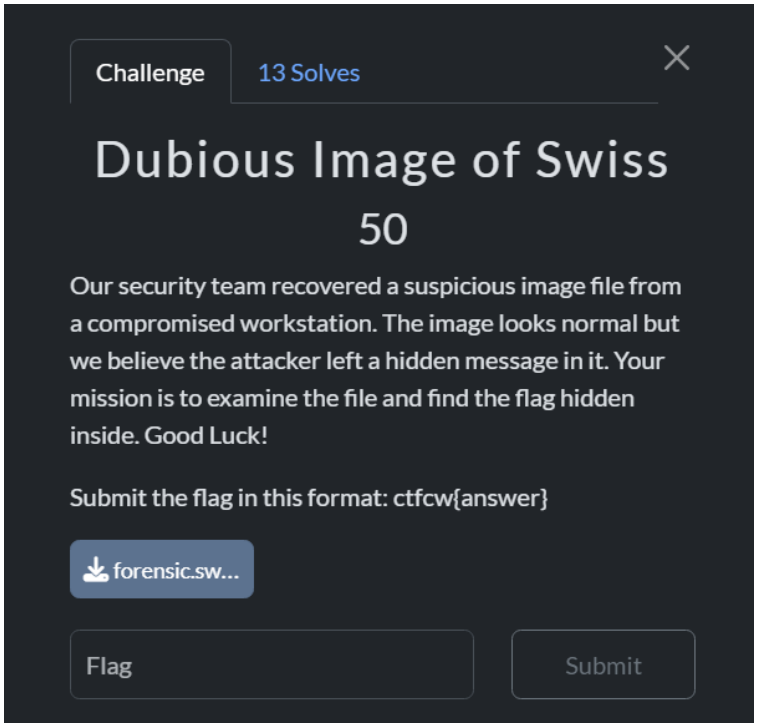
Say Something

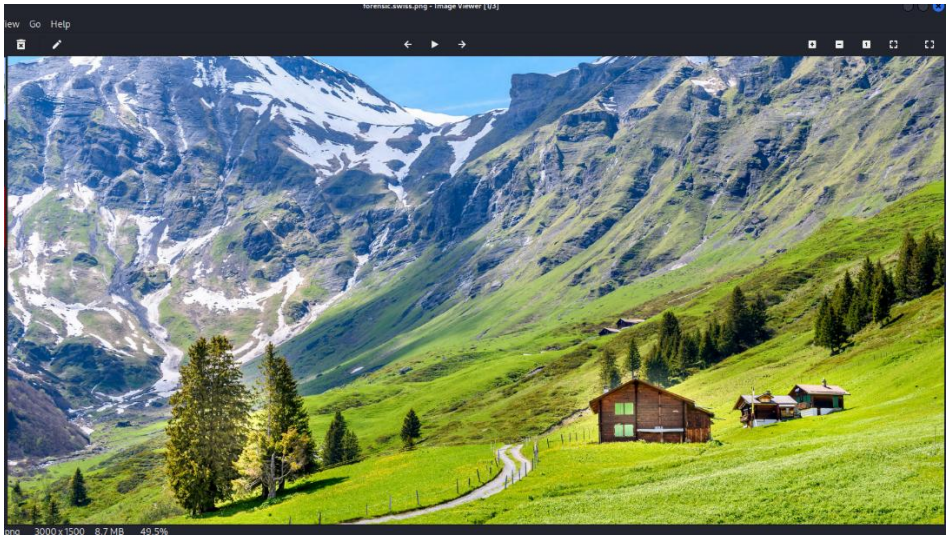
Say something: Submit

The Flag will be shown: **ctfcw{popup_trigger}**

<u>DIGITAL FORENSICS</u>

1)Dubious Image of Swiss





When we install the file,we have been given a png file shown above

```
┌──(kali㉿kali)-[~/Downloads]
└─$ exiftool forensic.swiss.png
ExifTool Version Number         : 13.25
File Name                       : forensic.swiss.png
Directory                       : .
File Size                       : 8.7 MB
File Modification Date/Time     : 2025:05:29 20:39:05-04:00
File Access Date/Time           : 2025:05:29 20:39:11-04:00
File Inode Change Date/Time     : 2025:05:29 20:39:05-04:00
File Permissions                : -rw-rw-r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 3000
Image Height                    : 1500
Bit Depth                       : 8
Color Type                      : RGB with Alpha
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
SRGB Rendering                  : Perceptual
Image Size                      : 3000×1500
Megapixels                      : 4.5
```

Using exiftool,we can see the metadata for the png file.After using the exiftool we can see nothing interesting or related to the flag itself

```
┌──(kali㉿kali)-[~/Downloads]
└─$ zsteg forensic.swiss.png
b1,b,lsb,xy         .. file: OpenPGP Secret Key
b1,rgb,lsb,xy       .. text: "ctfcw{book_the_ticket_flight}"
b1,rgb,msb,xy       .. file: OpenPGP Public Key
b1,bgr,lsb,xy       .. /var/lib/gems/3.3.0/gems/zsteg-0.2.13/lib/zsteg/checke
r/wbstego.rb:41:in `to_s': stack level too deep (SystemStackError)
```

Challenge 13 Solves

Dubious Image of Swiss

50

Our security team recovered a suspicious image file from a compromised workstation. The image looks normal but we believe the attacker left a hidden message in it. Your mission is to examine the file and find the flag hidden inside. Good Luck!

Submit the flag in this format: ctfcw{answer}

forensic.sw...

ctfcw{book_the_ticket_flight}

Submit

We can use another tool such as zsteg.Using zsteg we can see in the b1,rg,lsb,xy section flag which is “ctfcw{book_the_ticket_flight}”.

Miscellaneous (MISC)

1)Protected Secrets

Challenge 6 Solves

Protected Secrets

50

We found a zipped folder named protected.zip, and it's locked with a password. Inside, there's a file named flag.txt, but we can't open it without the correct password. Can you figure out the password and extract the flag?

Hint: *kamus dalam talian*

Submit the flag in this format: ctfcw{answer}

protected.zip

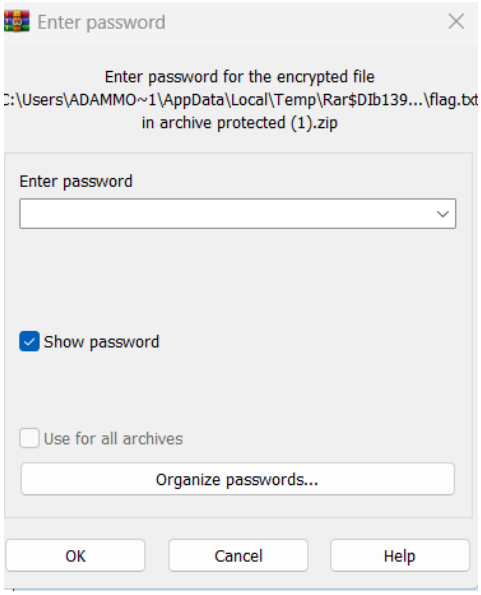
Flag Submit

protected	30/5/2025 10:07 AM	WinRAR ZIP archive	1 KB

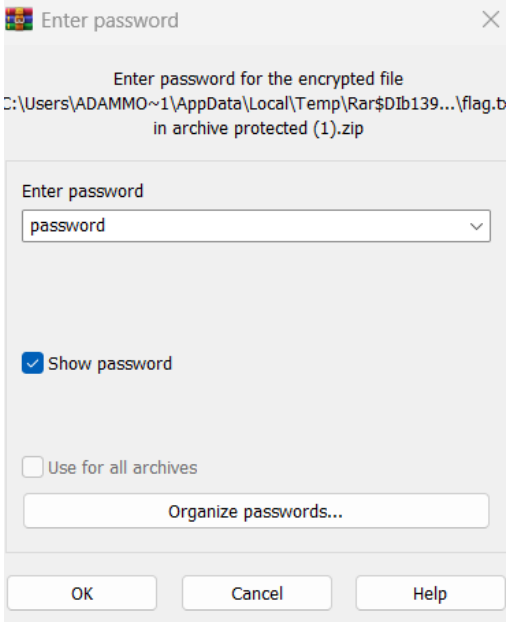
When we install the file,we have been given a file shown above.

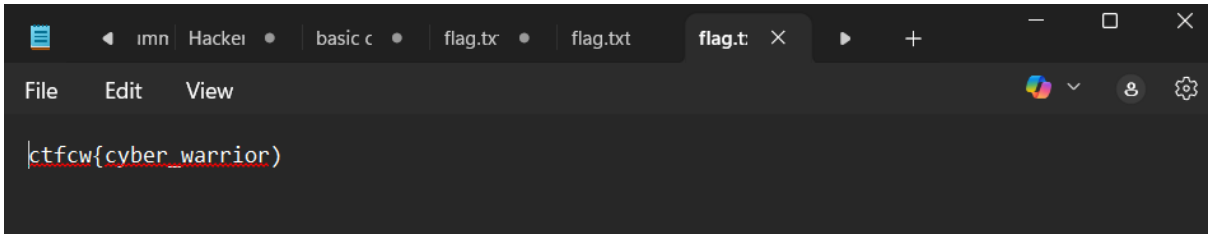
Name	Size	Packed	Type	Modified	CRC32
..			File folder		
flag.txt *	20	38	Text Document		4EF37DAF

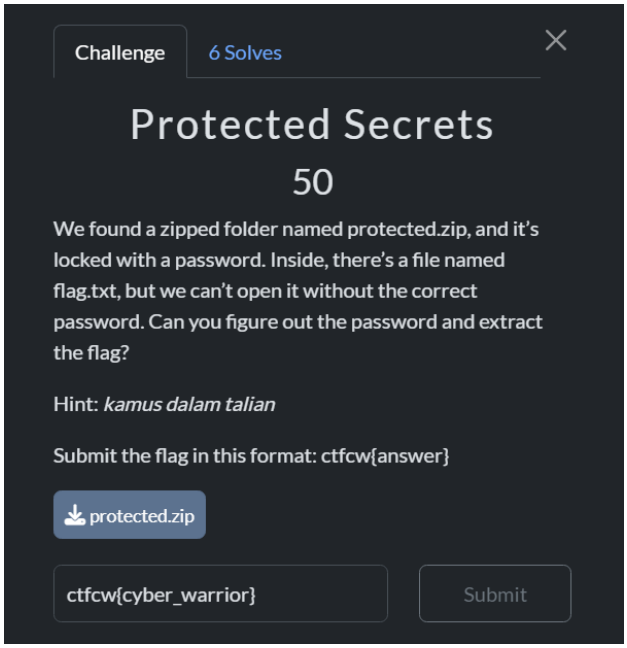
Opening the zip file we can see theres a text file called flag.txt



Opening the text file,we can see the text file is protected with a password.

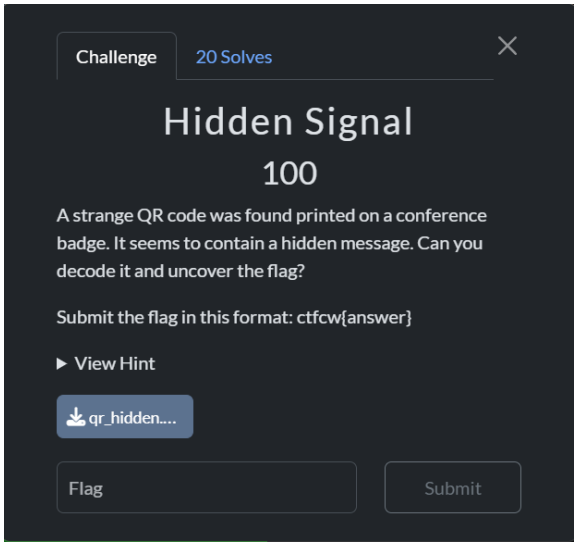






For our situation,we brute force the password manually using common password.For this text file,the password for it is password.Inside the text file is the flag it self which is "ctfcw{cyber_warrior}"

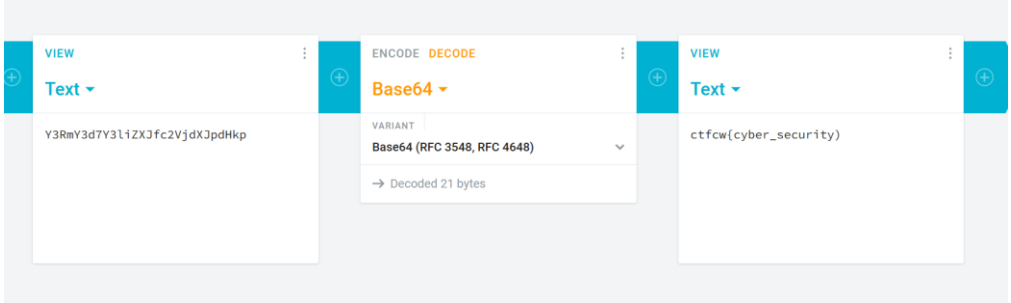
2)Hidden Signal



This is the QR code from the download button,

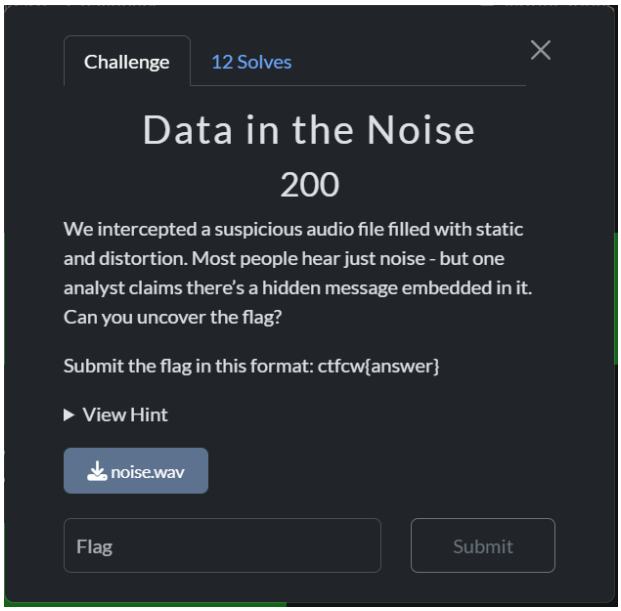
Upon scanning it, this is the output: Y3RmY3d7Y3liZXJfc2VjdXJpdHkp

From the encrypted text, we convert it with Base64 and we will get the flag.

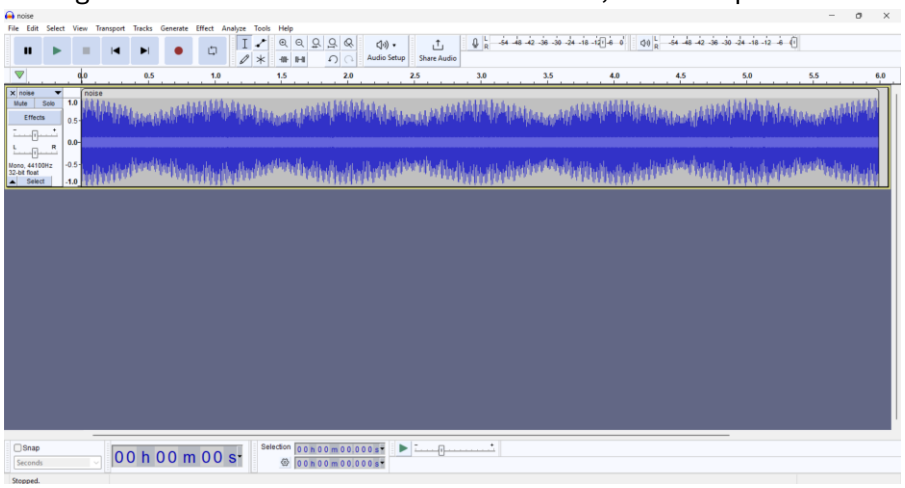


ctfcw{cyber_security}

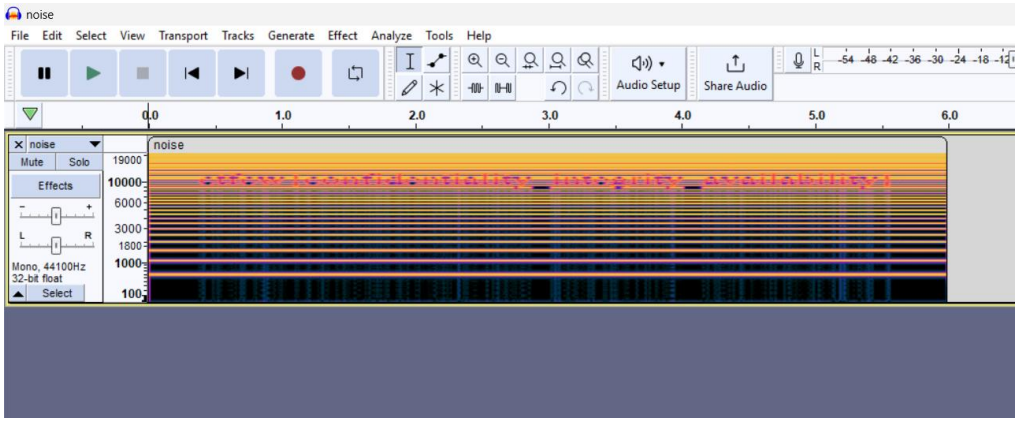
3)Data in the Noise



Seeing it is a .mav file that mean it is a audio file, we will export it to Audacity.



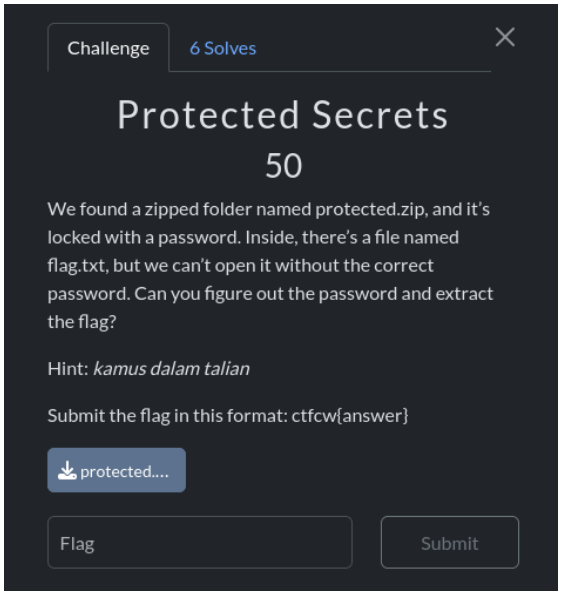
At first, the audio itself didn't give any flag, but when we use the Spectrogram to see the heatwave of the audio, the flag is hidden in the spectrogram.

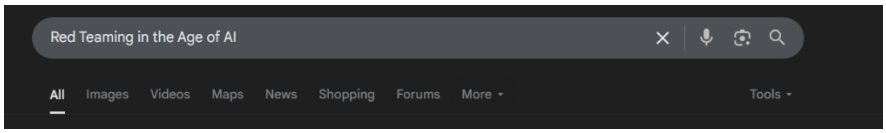


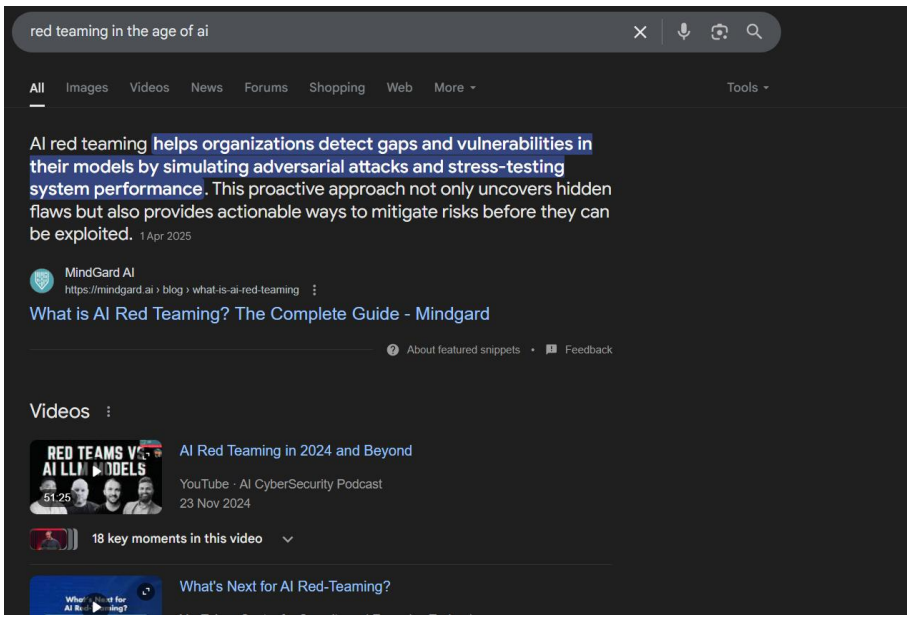
The flag can be seen : **ctfcw{confidentiality_integrity_availability}**

Open Source Intelligence(OSINT)

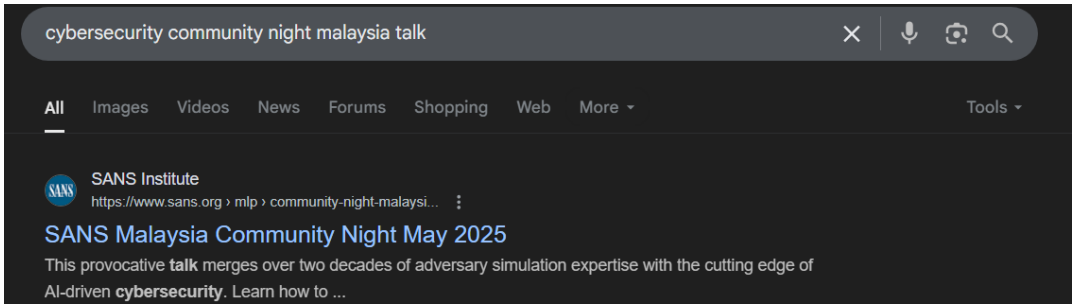
1)Red Team Rendezvous







When search “red teaming in the age of ai” we couldn’t find anything interesting



If we search up “cybersecurity community night malaysia talk”,we can see an article on the website “SANS Institute”

Thank you for your interest in our community nights. **This event is at capacity** – please send an email to SEA@sans.org to confirm if spots are available. Alternatively, you can go on our waitlist.

SANS Community Nights are a great way to stay in touch with your local InfoSec community and to hear the latest in technical wizardry, industry intelligence, and thought leadership from our amazing instructors.

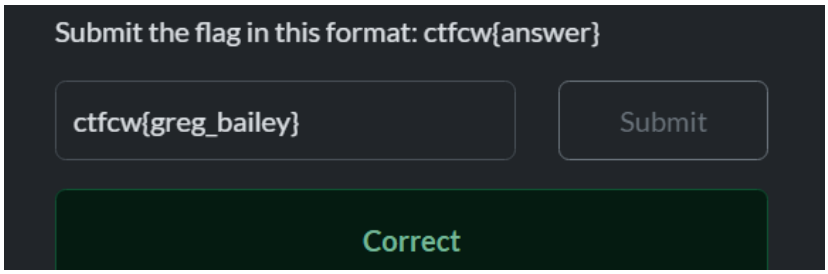
Join us at our next Community Event in Kuala Lumpur, Malaysia!

Monday, May 19th

7:00 pm – 8:00 pm
Registration

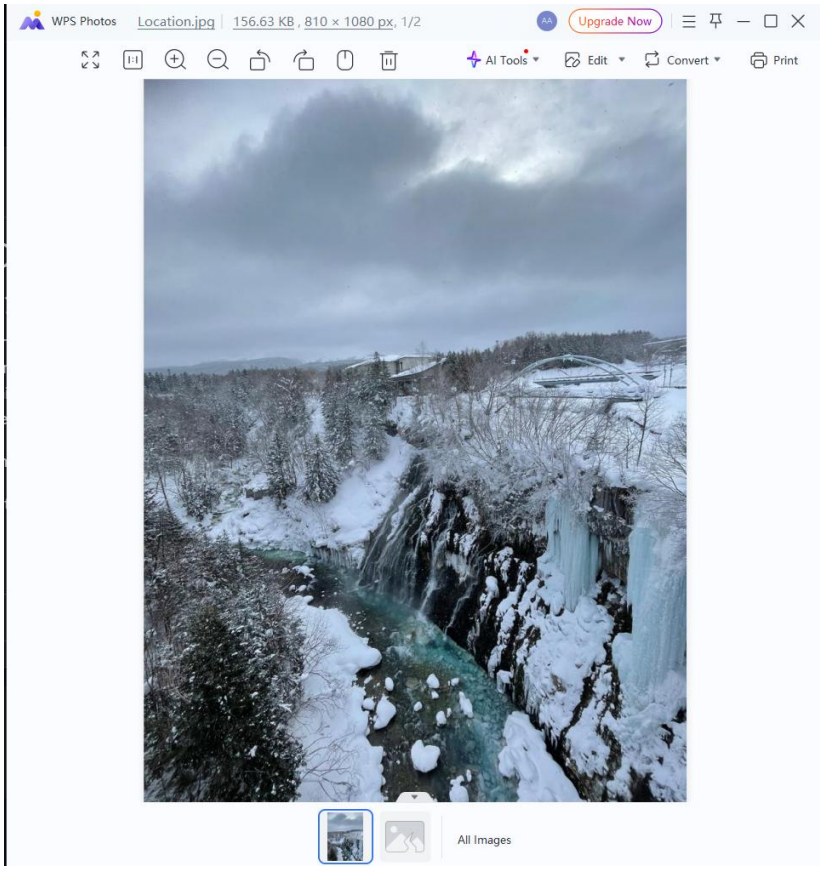
8:00 pm - 9:00 pm
Presentation by Greg Bailey

Title: Operationalizing a Red Team in the Age of AI
Presenter: Greg Bailey

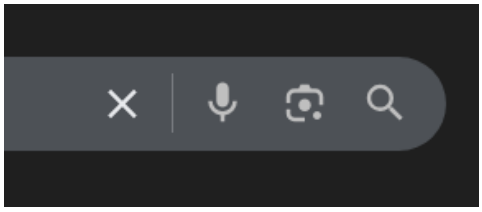


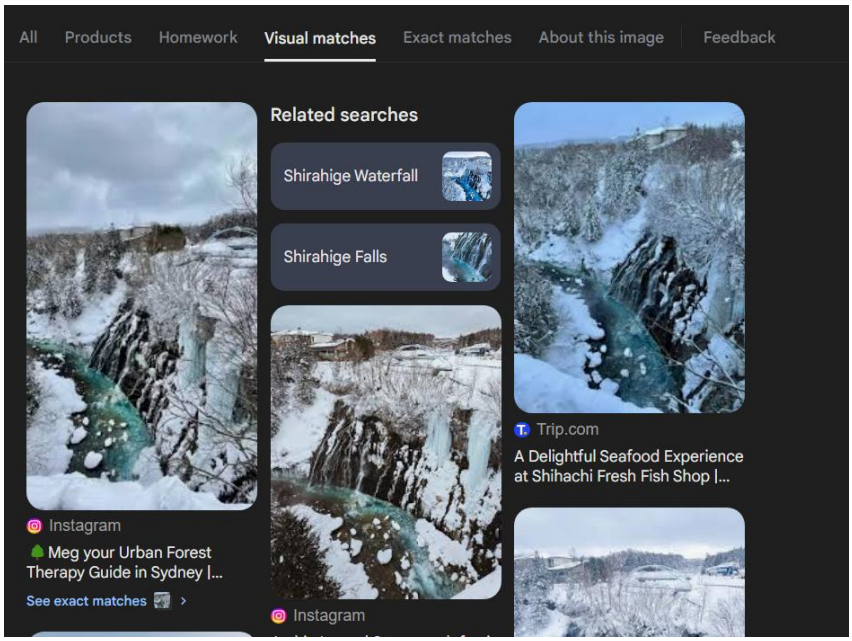
We can see the presenter name in the below,convert that into the flag format we get out flag is “ctfcw{Greg_Bailey}”

2)Frozen Coordinates

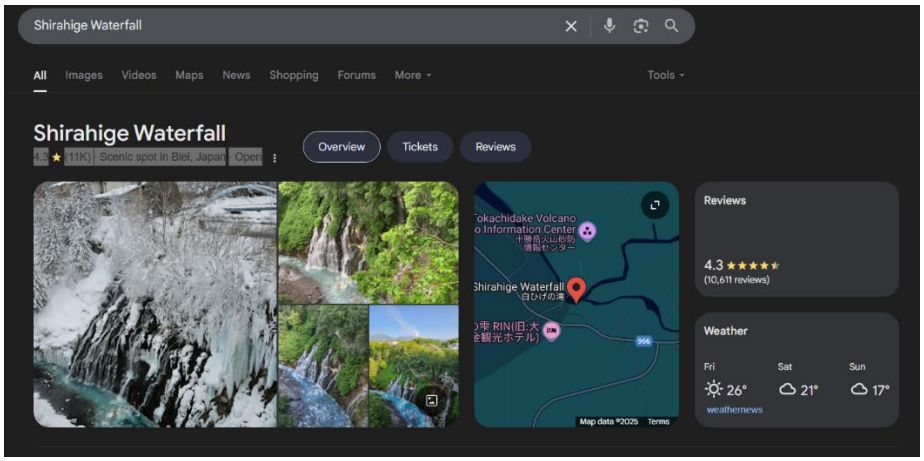


When we install the file,we have been given a png file shown above.

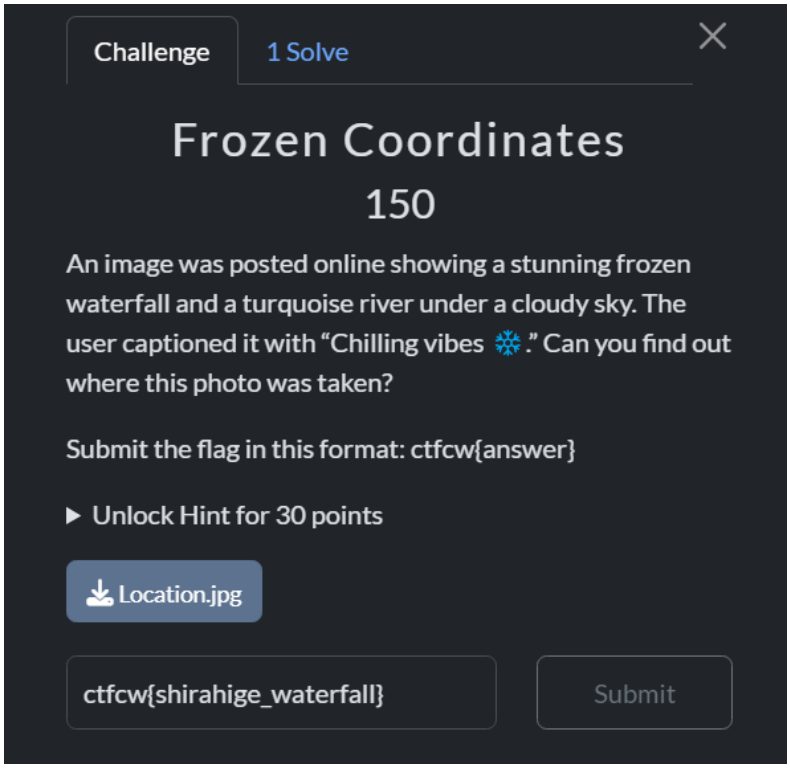




Using google image reverse search,we can see the exact picture and 2 related searches which is “shirahige waterfall” and “shirahige falls”



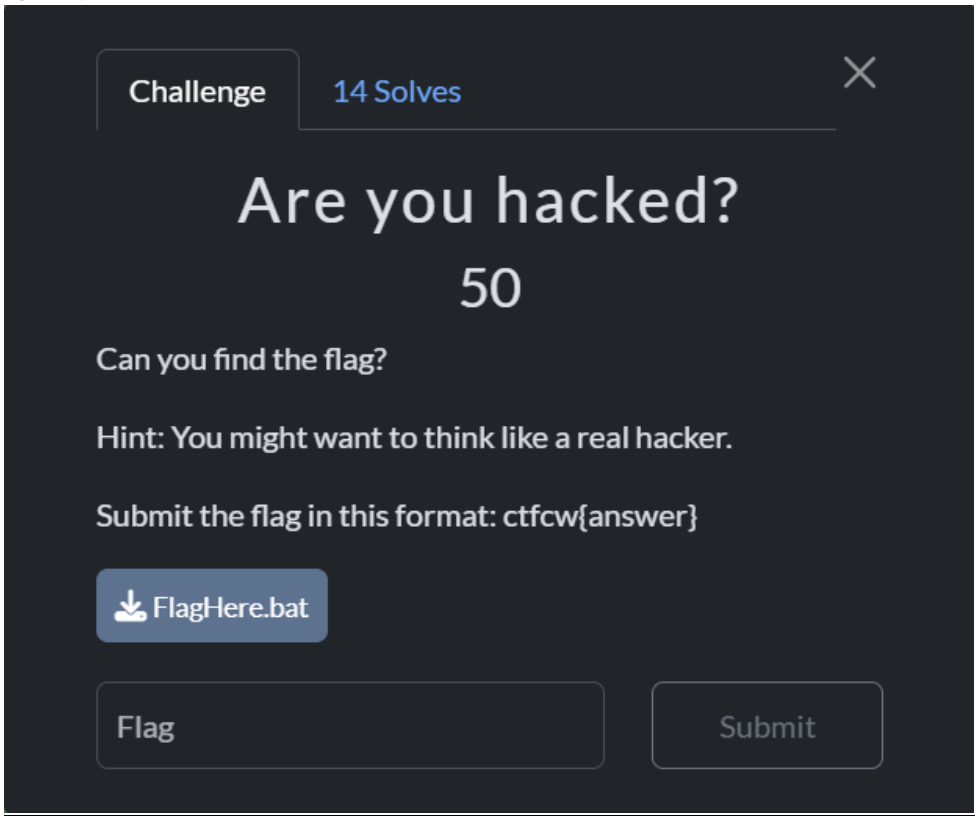
Clicking on the shirahige waterfall,we can see the exact picture that have been given to us so that will be our answer

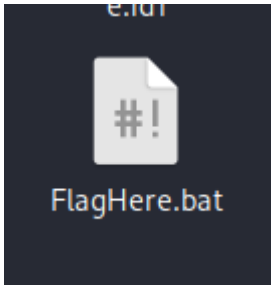


Converting the answer to flag format we get "ctfcw{shirahige_waterfall}"

Reverse Engineering

1)Are you hacked?



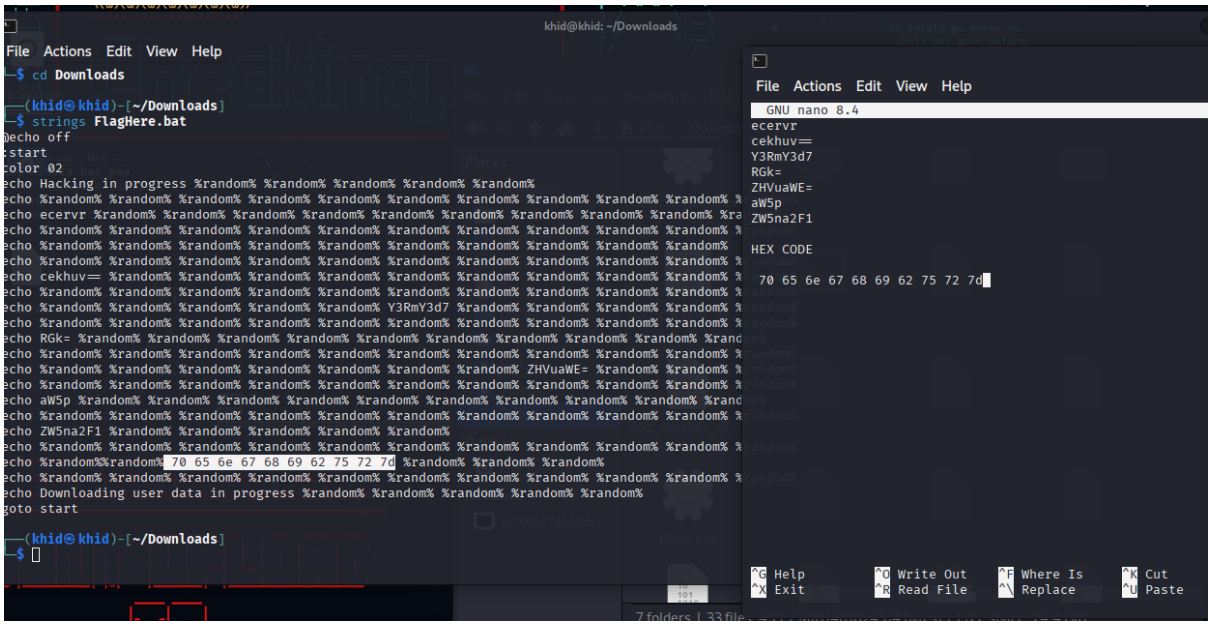


The .bat file is downloaded in Kali Linux, First thing when reverse engineering is to analyse the strings of the file.

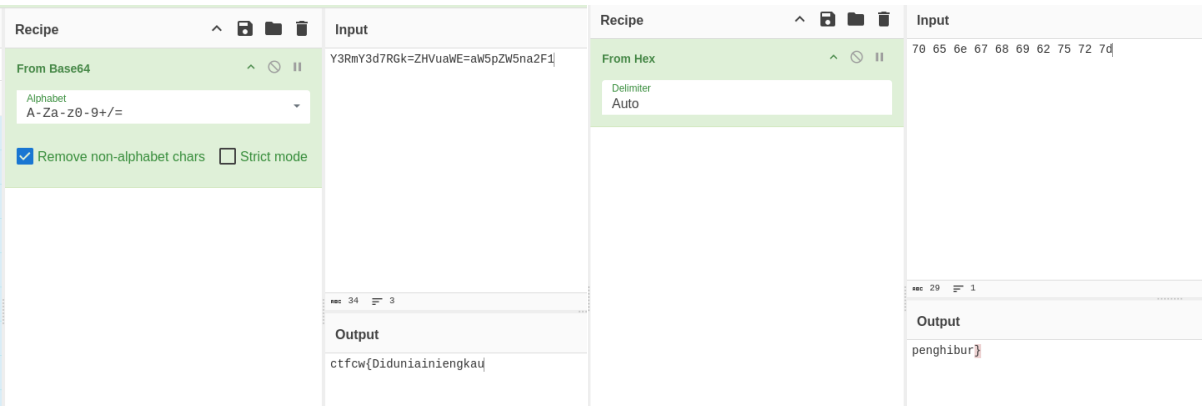
```
┌──(khid㉿khid)-[~/Downloads]
└─$ strings FlagHere.bat
@echo off
:start
color 02
echo Hacking in progress %random% %random% %random% %random% %random%
echo %random% %random% %random% %random% %random% %random% %random% %random% %random% %random% %random%
echo ecervr %random% %random% %random% %random% %random% %random% %random% %random% %random% %random%
echo %random% %random% %random% %random% %random% %random% %random% %random% %random% %random% %random%
echo %random% %random% %random% %random% %random% %random% %random% %random% %random% %random%
echo %random% %random% %random% %random% %random% %random% %random% %random% %random% %random% %random%
echo cekhuv== %random% %random% %random% %random% %random% %random% %random% %random% %random% %random%
echo %random% %random% %random% %random% %random% %random% %random% %random% %random% %random% %random%
echo %random% %random% %random% %random% %random% Y3RmY3d7 %random% %random% %random% %random% %random%
echo %random% %random% %random% %random% %random% %random% %random% %random% %random% %random% %random%
echo RGk= %random% %random% %random% %random% %random% %random% %random% %random% %random% %random%
echo %random% %random% %random% %random% %random% %random% %random% %random% %random% %random% %random%
echo %random% %random% %random% %random% %random% %random% %random% ZHVuaWE= %random% %random% %random%
echo %random% %random% %random% %random% %random% %random% %random% %random% %random% %random% %random%
echo aW5p %random% %random% %random% %random% %random% %random% %random% %random% %random% %random%
echo %random% %random% %random% %random% %random% %random% %random% %random% %random% %random% %random%
echo ZW5na2F1 %random% %random% %random% %random% %random%
echo %random% %random% %random% %random% %random% %random% %random% %random% %random% %random% %random%
echo %random%%random% 70 65 6e 67 68 69 62 75 72 7d %random% %random% %random%
echo %random% %random% %random% %random% %random% %random% %random% %random% %random% %random% %random%
echo Downloading user data in progress %random% %random% %random% %random% %random%
goto start
```

From all the strings, we can see parts of encrypted message from Base64 and Hex.

Compile all the encrypted and write it down somewhere

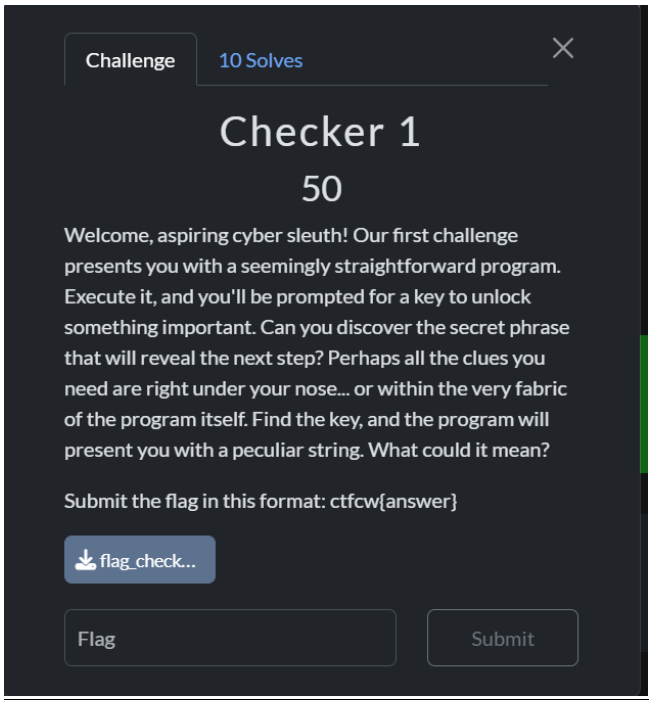


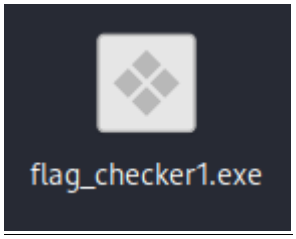
Next we need to try decrypt it in sequence from top to bottom, and the output will show the flag



The flag is **ctfcw{Diduniainiengkaupenghibur}**

2)Checker 1

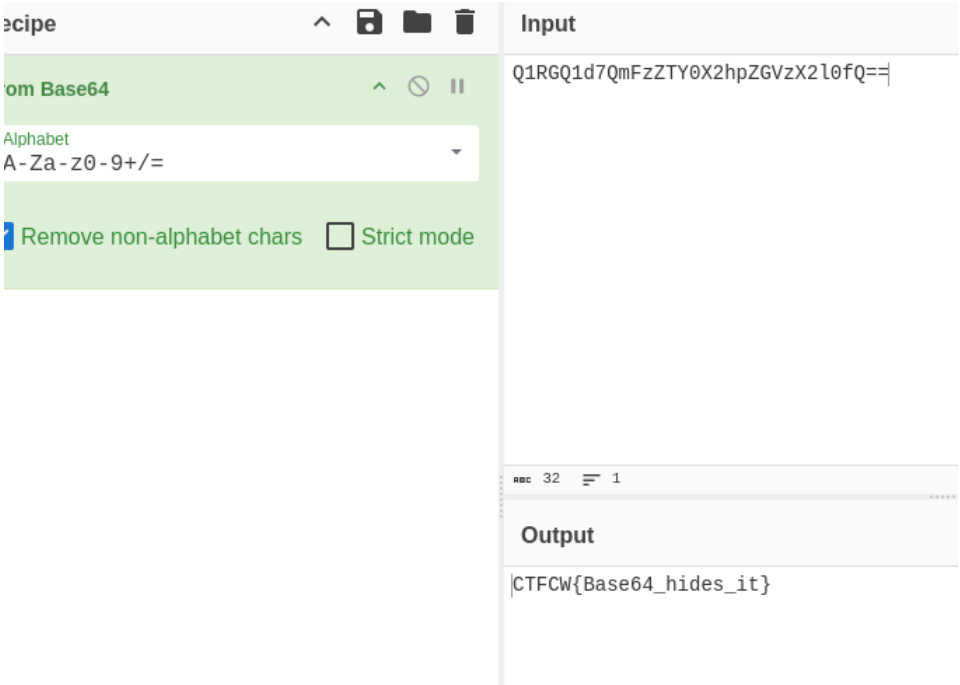




The file provided is downloaded in Kali linux.

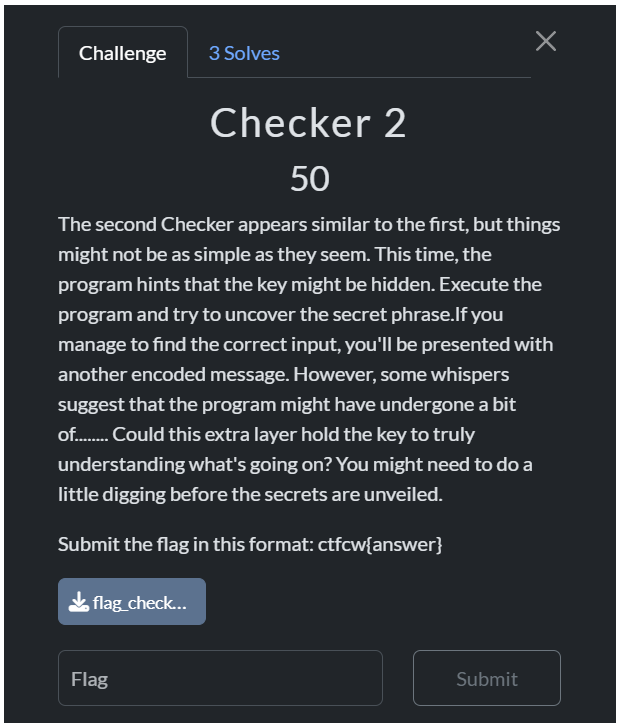
```
*****************************************
*              FLAG CHECKER v1.1        *
Enter the secret key to reveal the encoded flag:
Q1RGQ1d7QmFzZTY0X2hpZGVzX2l0fQ==
reveal
Correct key!
Encoded Flag:
Decode this to get the real flag!
Incorrect key. Keep trying!
basic_string: construction from null is not valid
;*3$"
zPLR
GCC: (Debian 14.2.0-16) 14.2.0
Scrt1.o
__abi_tag
```

Upon reading the strings of the .exe, the string contain encrypted flag, decrypt it using Base64, the output is the flag.



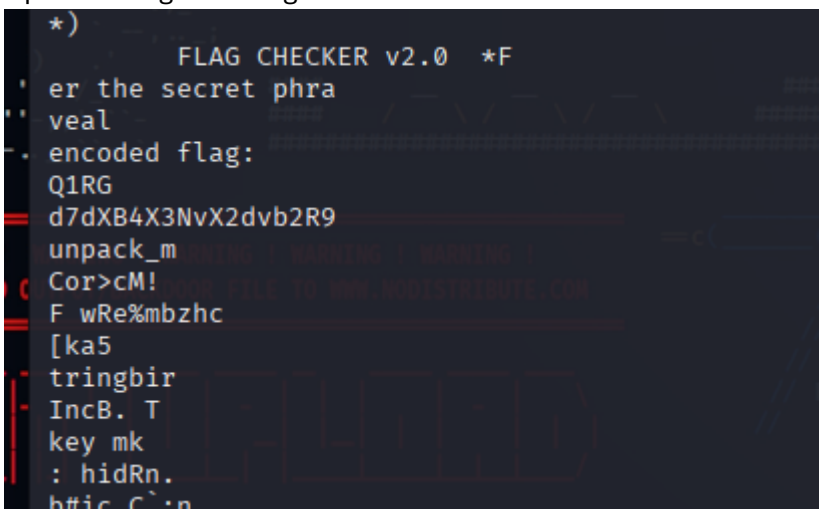
The flag is : **CTFW{Base64_hides_it}**

3)Checker 2



The file provided is downloaded in Kali Linux.

Upon reading the strings of the .EXE



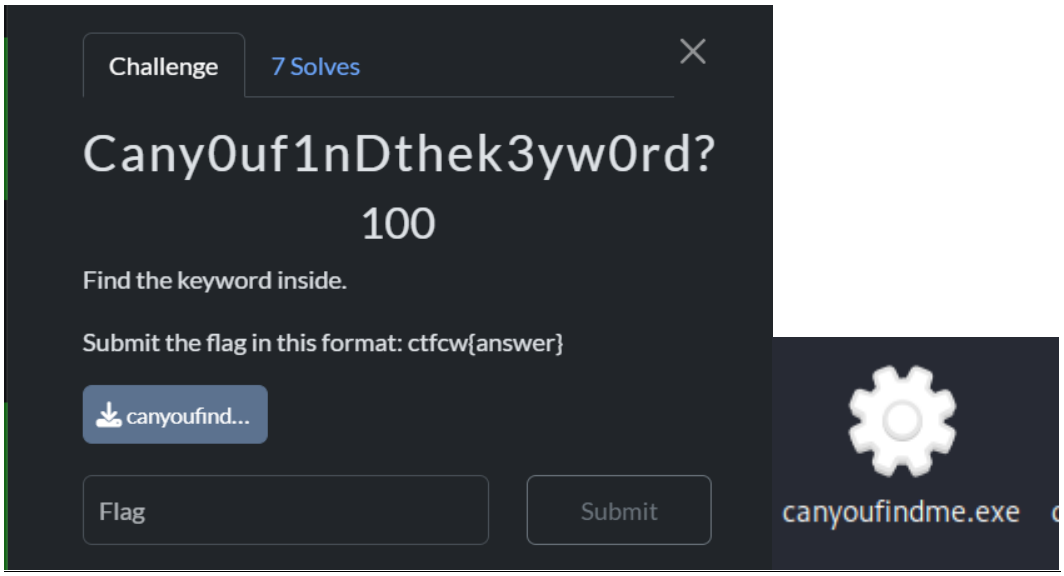
There are encoded flag which is : Q1RGd7dXB4X3NvX2dvb2R9

The flag looks like Base64, upon decrypting the flag, this is the output:

CTF{upx_so_good}

ctfw{upx_so_good}

<u>4) Cany0uf1nDthek3yw0rd?</u>



The file is downloaded in Kali Linux,

Upon reading the strings for the .exe.

```
libgcj-16.dll
_Jv_RegisterClasses
Enter the password:
%99s
no_password
Correct! Here's your flag: ctfcw{%s}
Wrong password.
Mingw runtime failure:
  VirtualQuery failed for %d bytes at address %p
  Unknown pseudo relocation protocol version %d.
  Unknown pseudo relocation bit size %d.
glob-1.0-mingw32
```

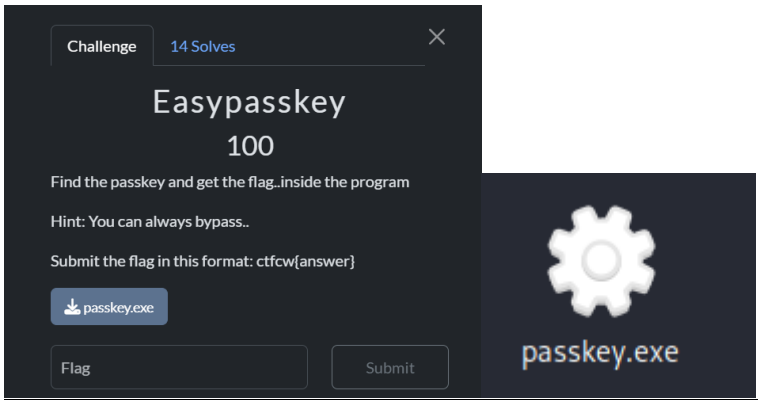
We can see the password is no_password.

```
C:\Users\User\Downloads>canyoufindme.exe
Enter the password: no_password
Correct! Here's your flag: ctfcw{no_password}

C:\Users\User\Downloads>
```

The flag can be found when we input the password into the .exe

Flag: **ctfcw{no_password}**

5)Easypasskey

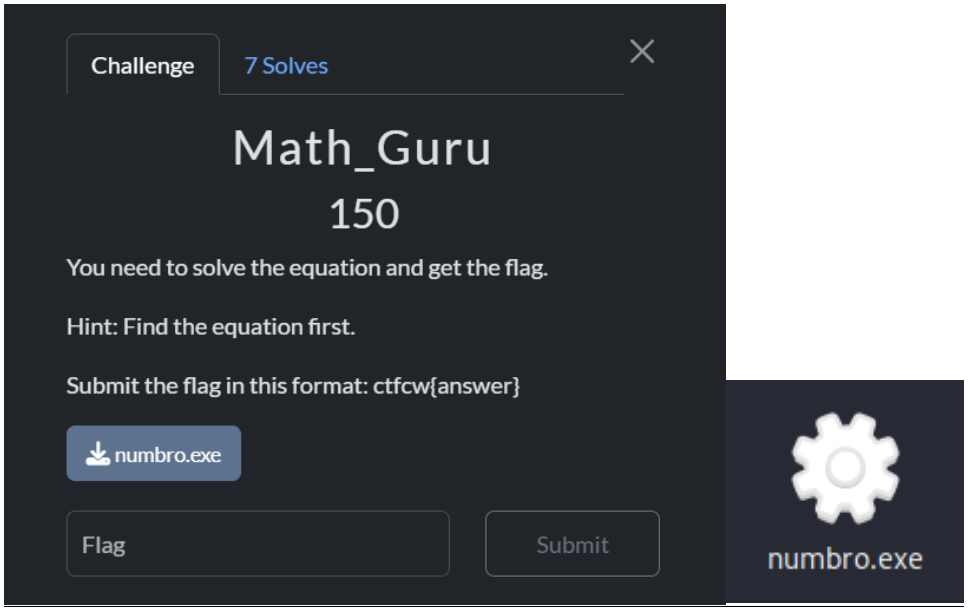


The file is downloaded in Kali Linux, and the strings of the .exe the flag can be found

```
%49s
nopassword
Correct! Flag: ctfcw{crack_easy_win}
Wrong answer. Try again.
pause
Mingw runtime failure:
  VirtualQuery failed for %d bytes at address %p
  Unknown pseudo relocation protocol version %d.
  Unknown pseudo relocation bit size %d.
glob-1.0-mingw32
GCC: (GNU) 6.3.0
GCC: (GNU) 6.3.0
```

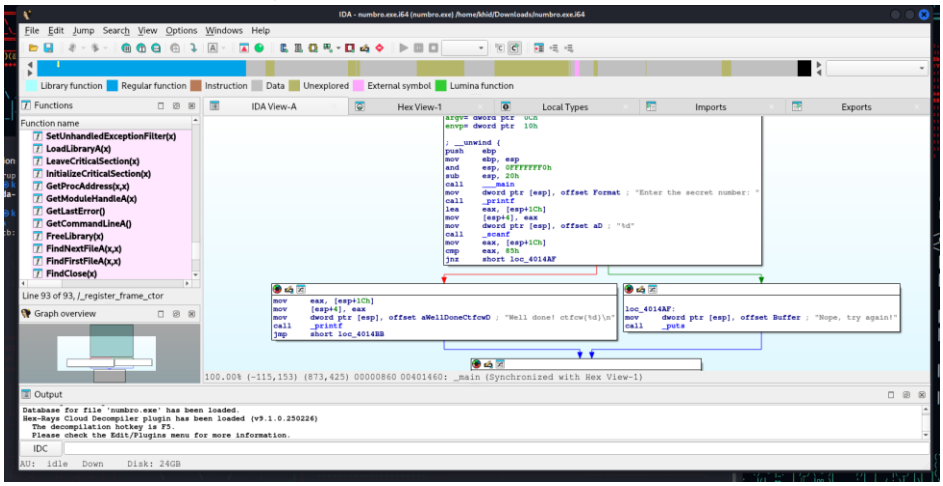
Flag : **ctfcw{crack_easy_win}**

6)Math_Guru



The file is downloaded in Kali Linux.

Next the .exe file is exported to IDA Free.



The equation is listed in the source code and calculating it will resulted in 133.

```
C:\Users\User\Downloads>numbro.exe
Enter the secret number: 133
Well done! ctfcw{133}
Press any key to continue . . .
```

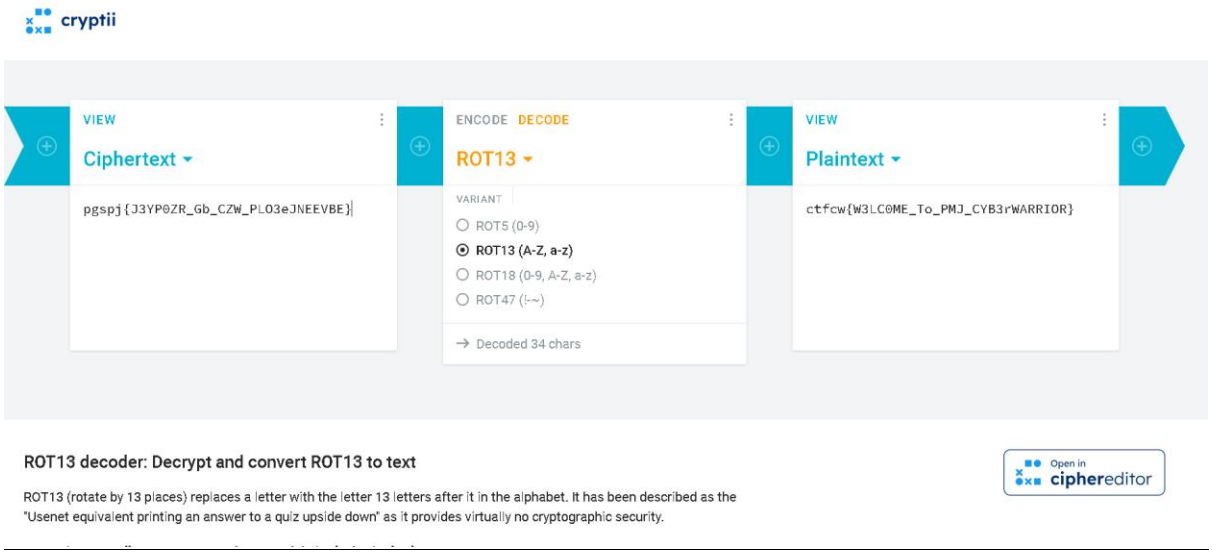
Put the 133 as the secret number and the flag is **ctfcw{133}**

Cryptography

1)ROT13

```
pgspj{J3YP0ZR_Gb_CZW_PLO3eJNEEVBE}
```

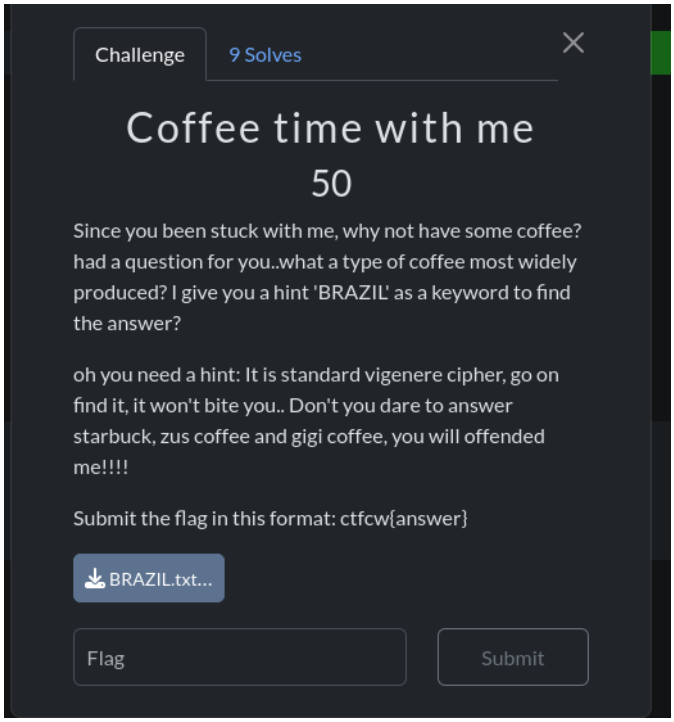
By downloading the text file we can get an encrypted text is **pgspj{J3YP0ZR_Gb_CZW_PLO3eJNEEVBE}.**

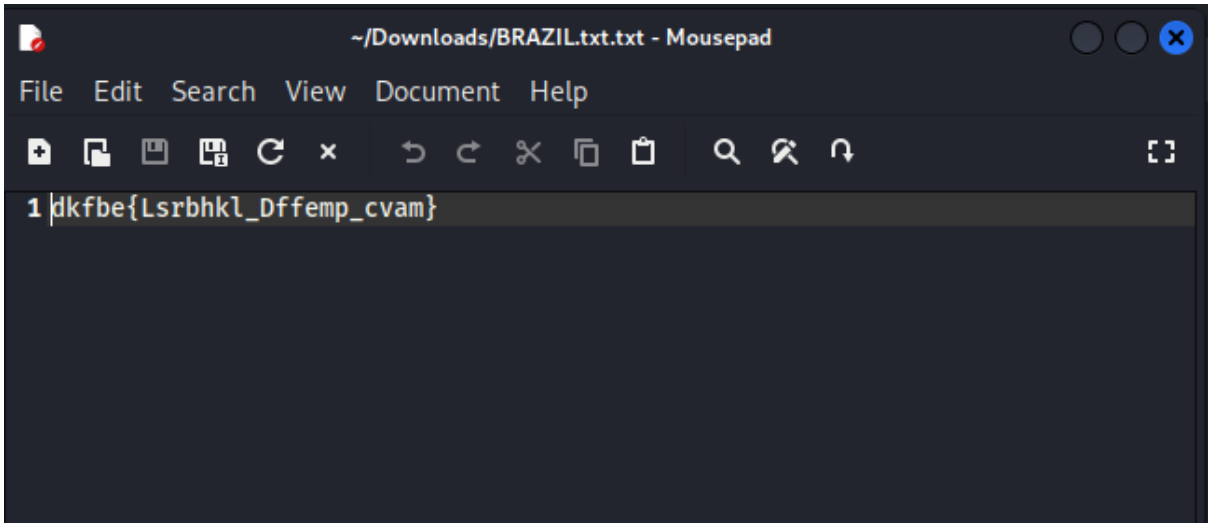


Now,by using any website or app that can decode the encrypted text especially for rot13 cryptographic.Entering the ciphertext which is the encrypted text.Set to decode and choose rot13 since this was the rot 13 encryption.The result will be show the flag.

For the rot13,the flag } was **ctfcw{W3LC0ME_To_PMJ_CYB3rWARRIOR**

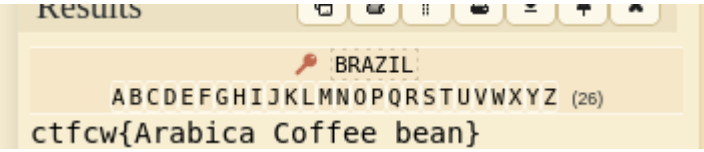
2)Coffee time with me

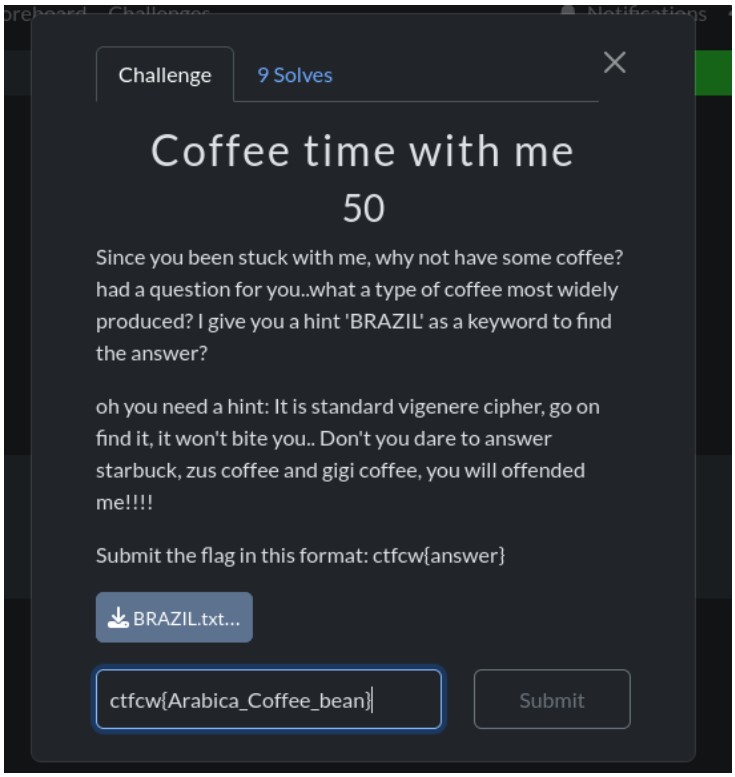




When we install the file,we have been given a text file shown above.

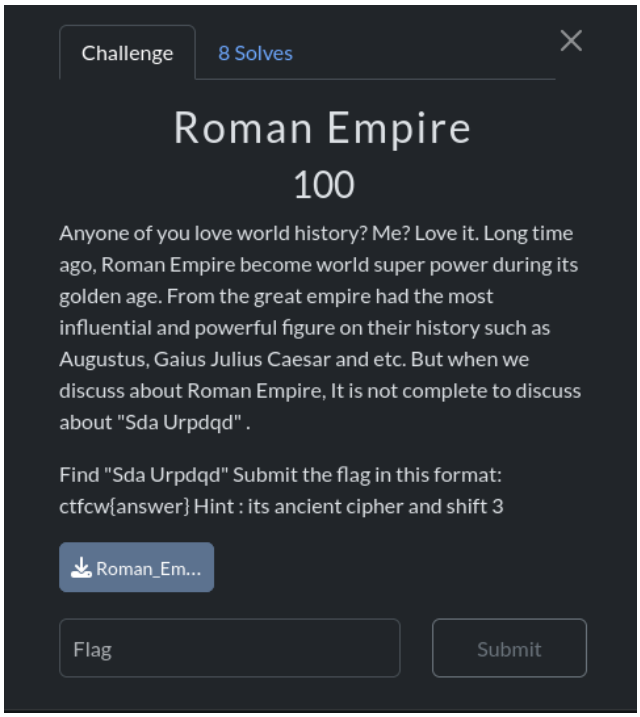
The hint in the question is using a vigenere cipher and the keyword is “BRAZIL”.Putting the information we have into an online vigenere decoder with the key being “BRAZIL”.

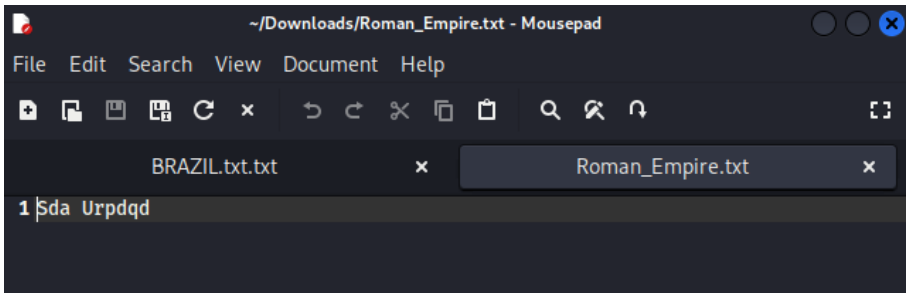




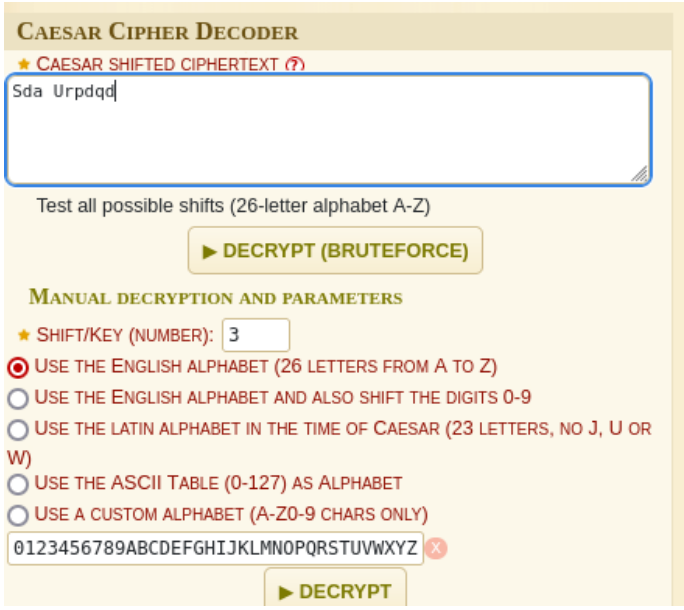
When we decoded,we got the flag which is “ctfcw{Arabica_coffee_bean}”

3)Roman Empire

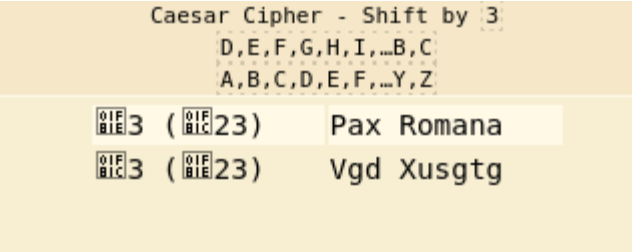


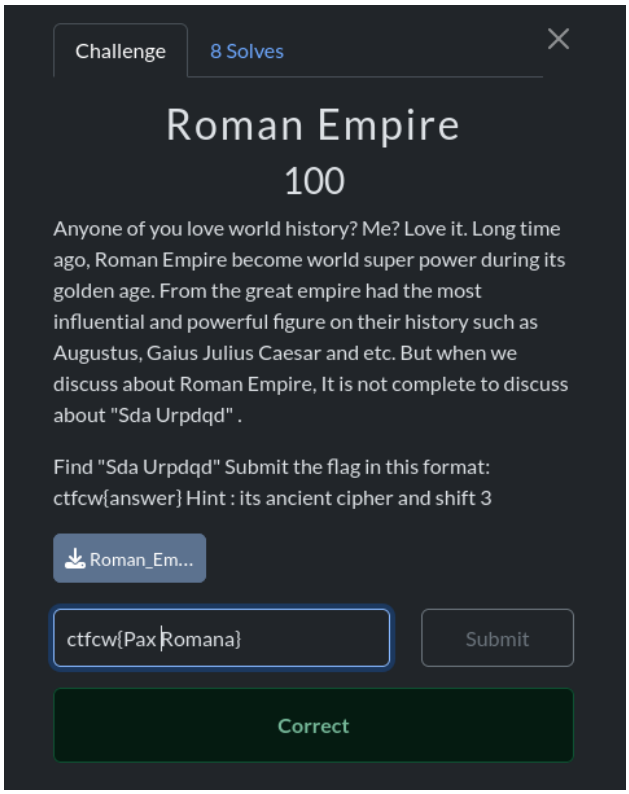


When we install the file,we have been given a text file shown above.



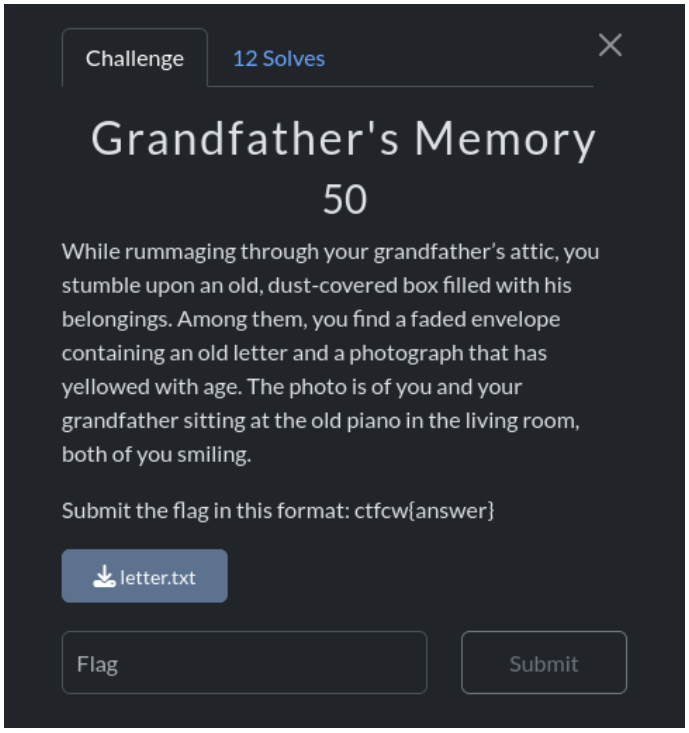
The hint in the question is using a ancient cipher which is ceasar cipher and the shift is 3.Putting the information we have into an online ceasar cipher decoder with the shift being 3

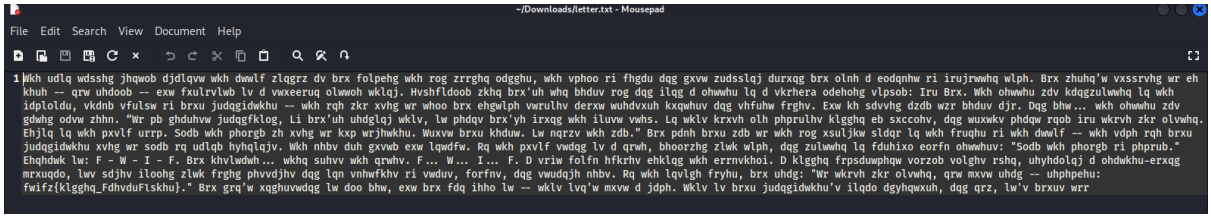




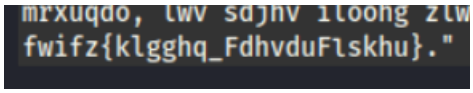
When we decoded,we got the answer which is “Pax Romana” and convert it into flag format we got “ctfcw{Pax Romana}”

4)Grandfathers Memory

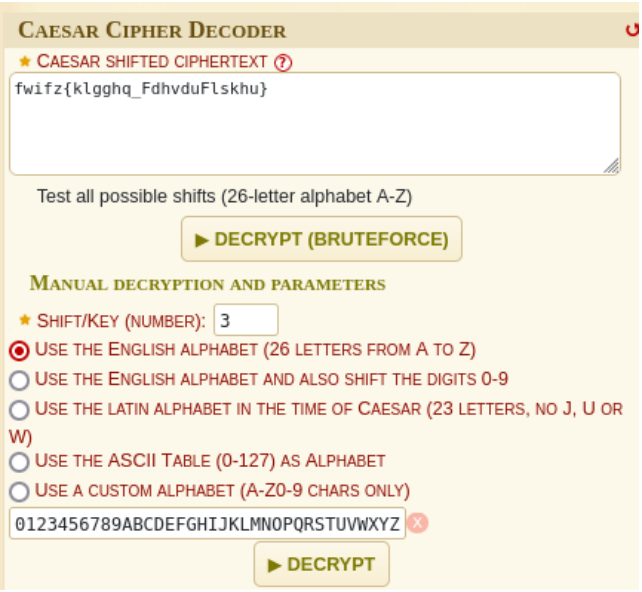




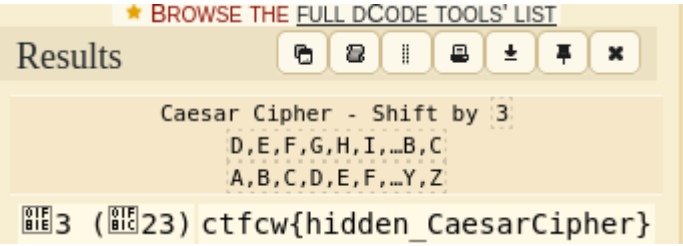
When we install the file,we have been given a text file shown above.



To make the job easier,we will only decrypt the part of the letter since it has the shape of the flag.



We test it using ceaser cipher with the shift being 3

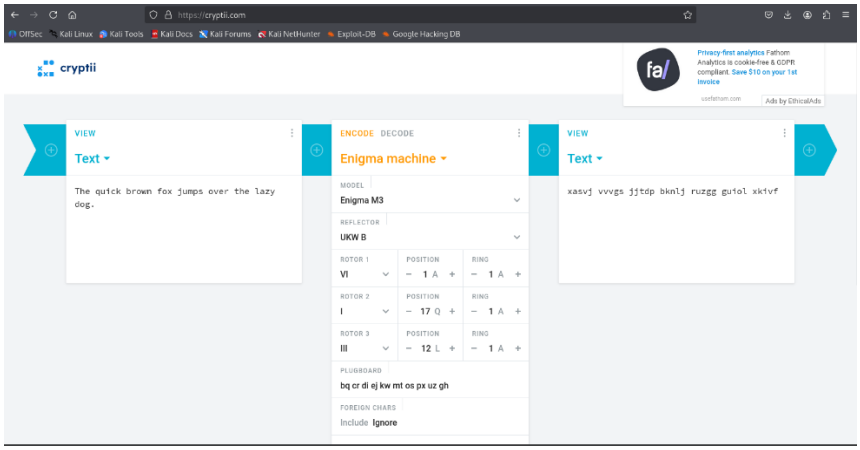


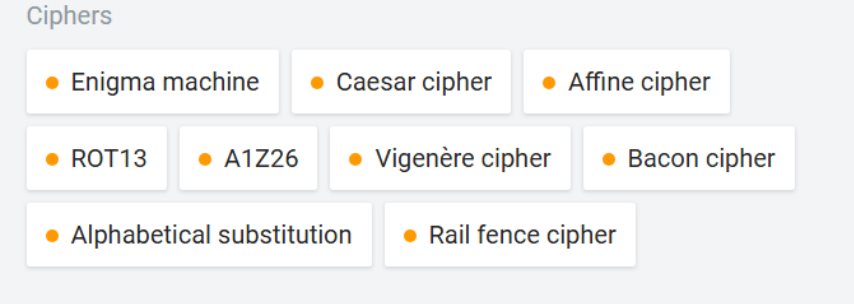
When we decoded,we got the flag which is “ctfcw{hidden_CaesarCipher}”

5)Cipher no hint

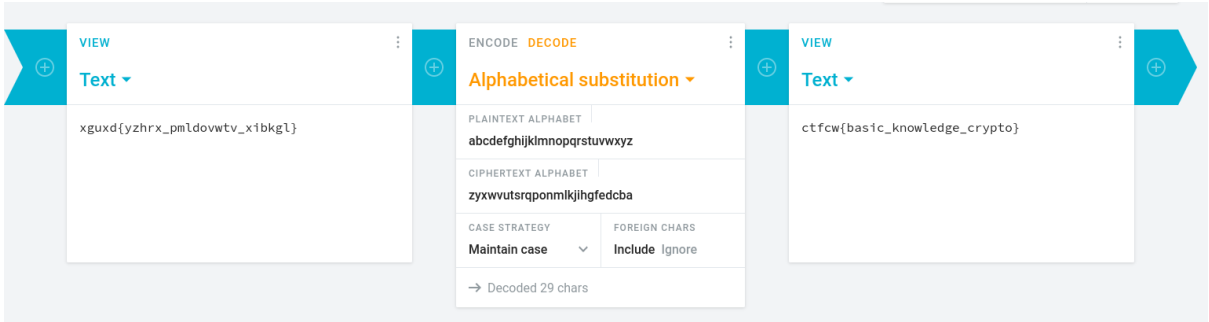

```
1 xguxd{yzhrx_pmldovwtv_xibkgl}
```

When we install the file,we have been given a text file shown above.





Since there are no hint on which cipher is this,we are trying 1 by 1 cipher using the website cryptii.

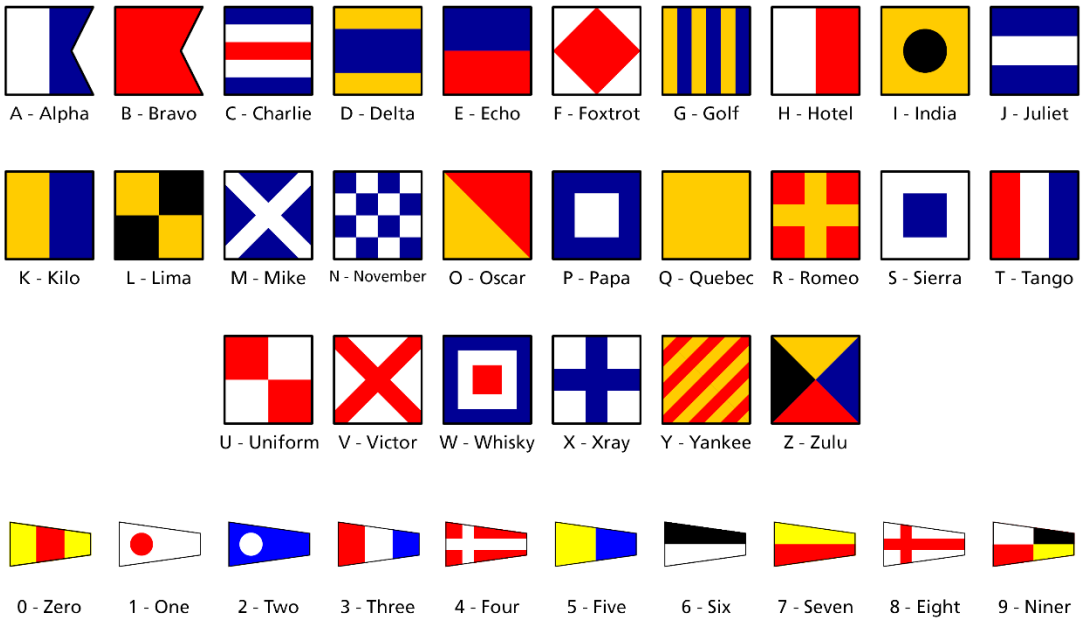


After testing 1 by 1 cipher we can see that the cipher for this is Alpahabetical substitution and we got the flag which is “ctfcw{basic_knowledge_crypto}”

6)Grandfather's Picture

This is the picture from the download link.

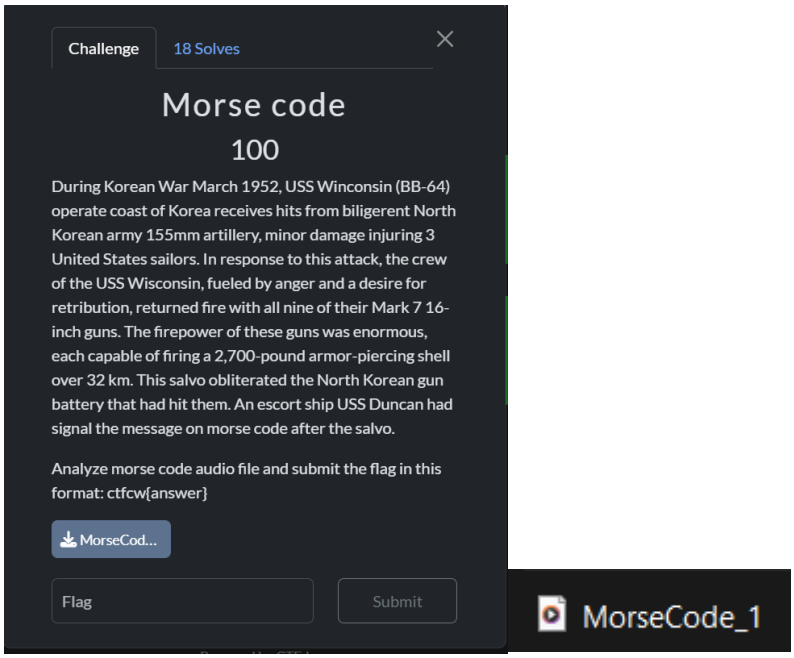
Upon looking at the picture, we can see that it uses navy signal code.



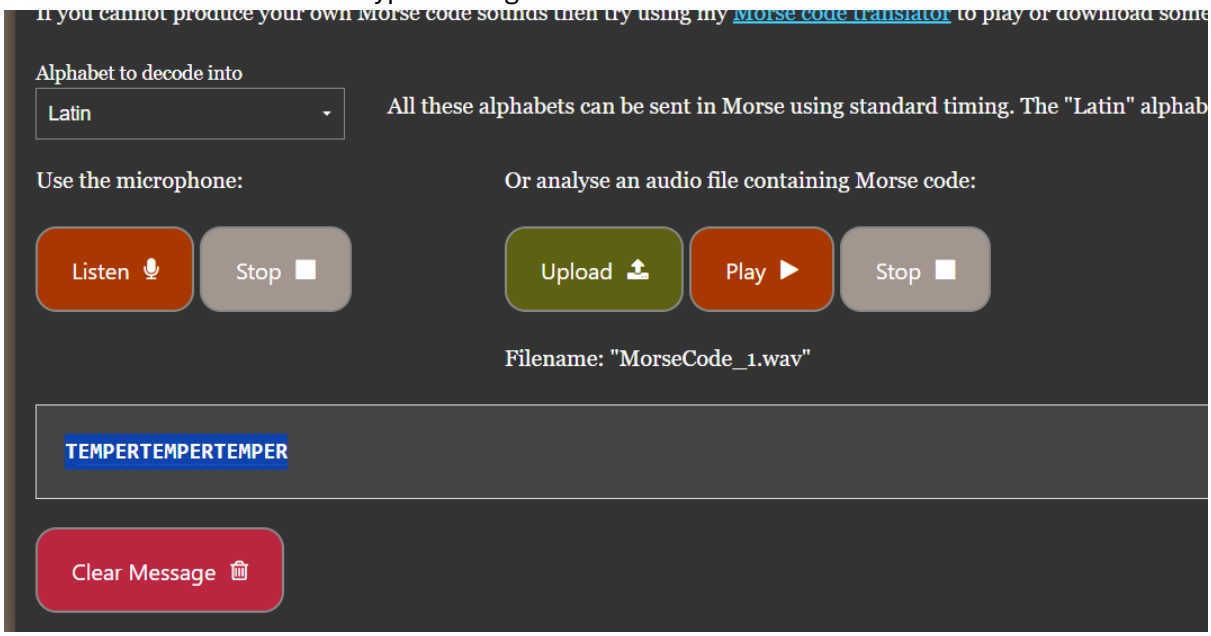
So when translating the picture, it will reveal the flag

Flag: **ctfcw{navysignalscode}**

7)Morse Code

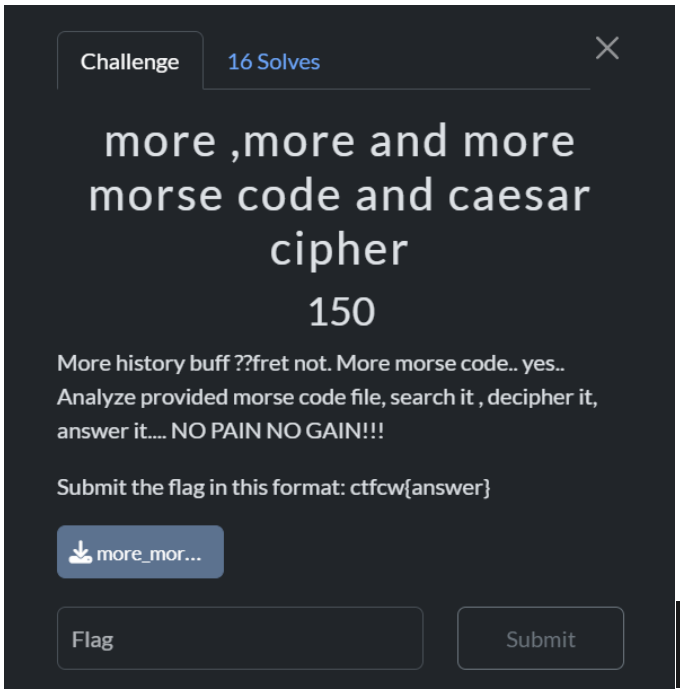


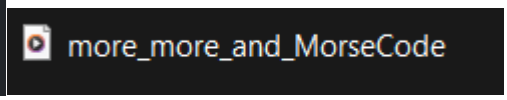
The audio morse code is decrypted using online tools



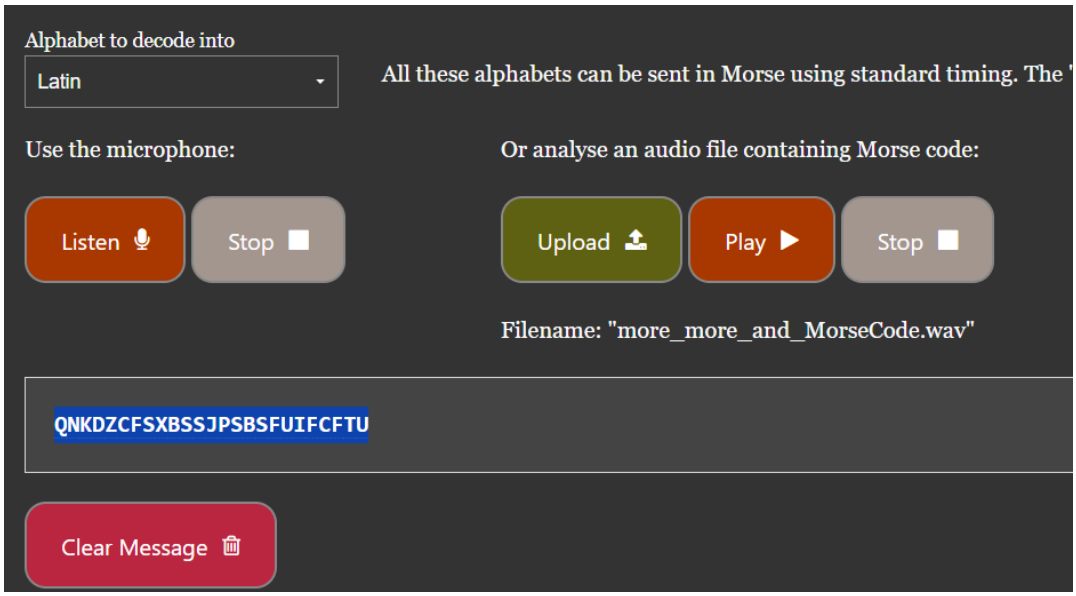
The flag is **ctfcw{TEMPERTEMPERTEMPER}**

8) more ,more and more morse code and caesar cipher

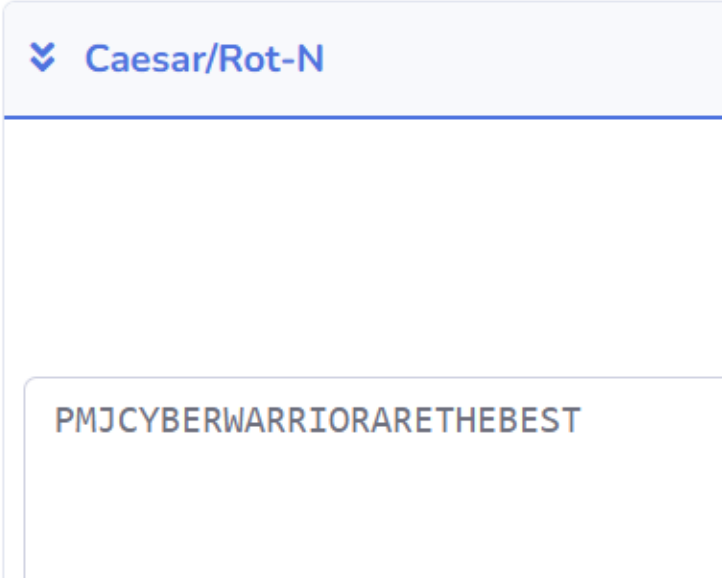




The morsecode audio is decoded using online morsecode .wav to text.



Now the encoded flag is decoded by using Caesar cipher



The flag is: **ctfcw{PMJCYBERWARRIORARETHEBEST}**