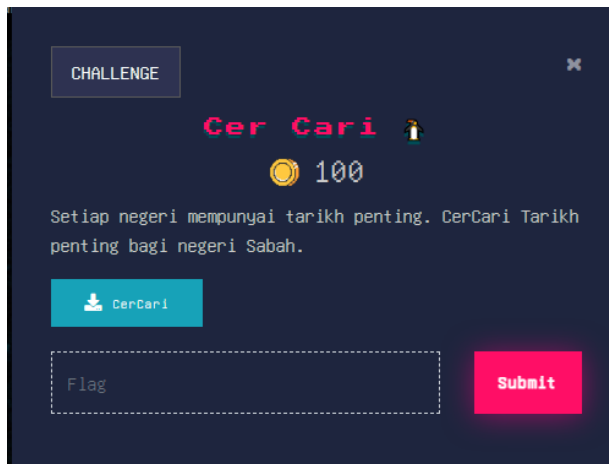


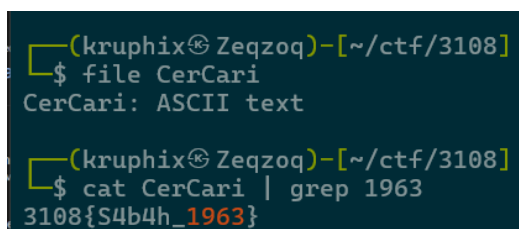
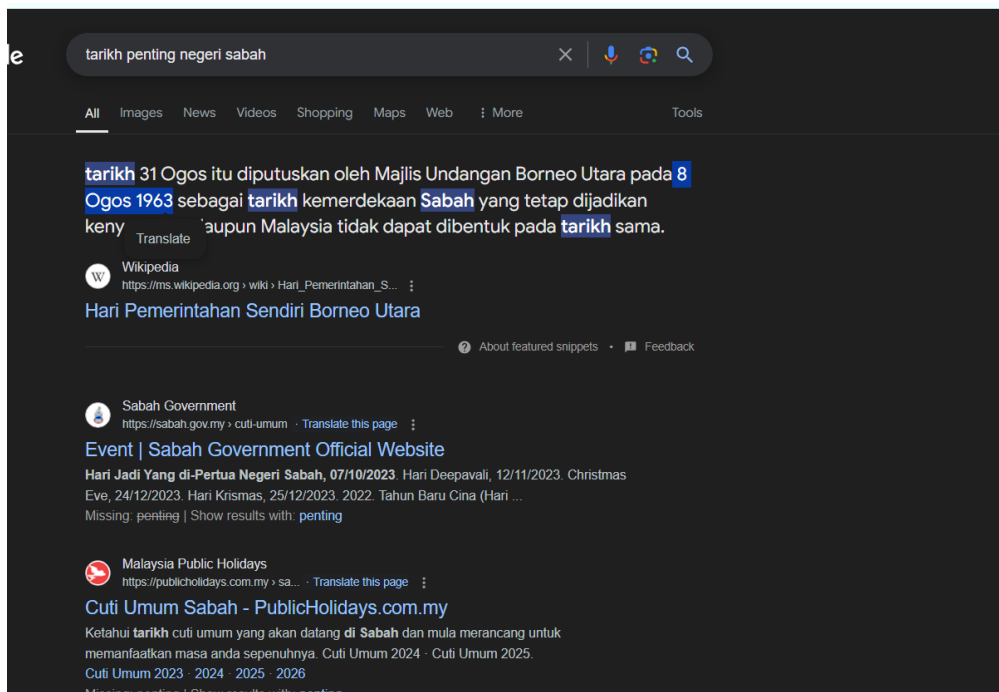
Zeqzoq currently noob writeup

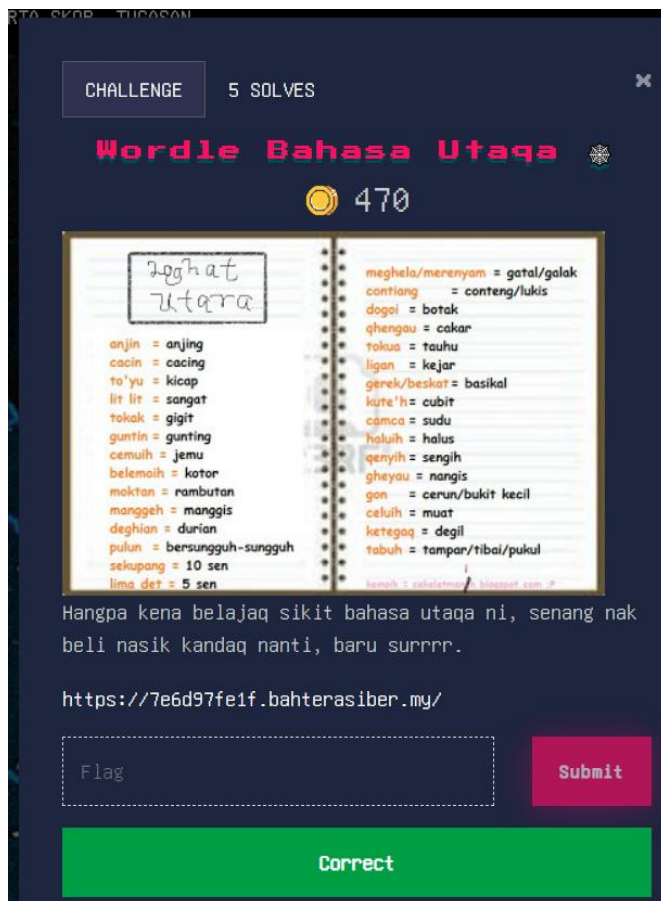
Challenge I solved:

1. Cer Cari
2. Wordle Bahasa Utaqa
3. zZzZz
4. Kontras
5. Jalan jalan Desa
6. Cordini
7. Makanan Popular
8. Sarawak Kita
9. Tinggi Mat
10. Sultan yang Hilang
11. Perigi
12. Bawang
13. Sejarah N9
14. Privacy Matters
15. Sembunyi
16. sembunyi V2
17. Mesej Rahsia
18. Tanpa nama
19. Jauh bono umohnyo
20. Mamu Kasi Tahu
21. Selangorku
22. sambungan Telefon
23. Rawsec
24. Yayasan Digital Malaysia
25. Tinggi lagi
26. Kekacauan Huruf
27. Pandak Lam
28. Syah Sesat



Google the date and grep the date. We use the file command because the CerCari file doesn't have extension. When we run it, we know it is plain text file





Put Sabah because it was sabah question. 2nd A was correct so we search for other word that 4th letter is A and has 5 letter total.



CHALLENGE

zZzZz

100

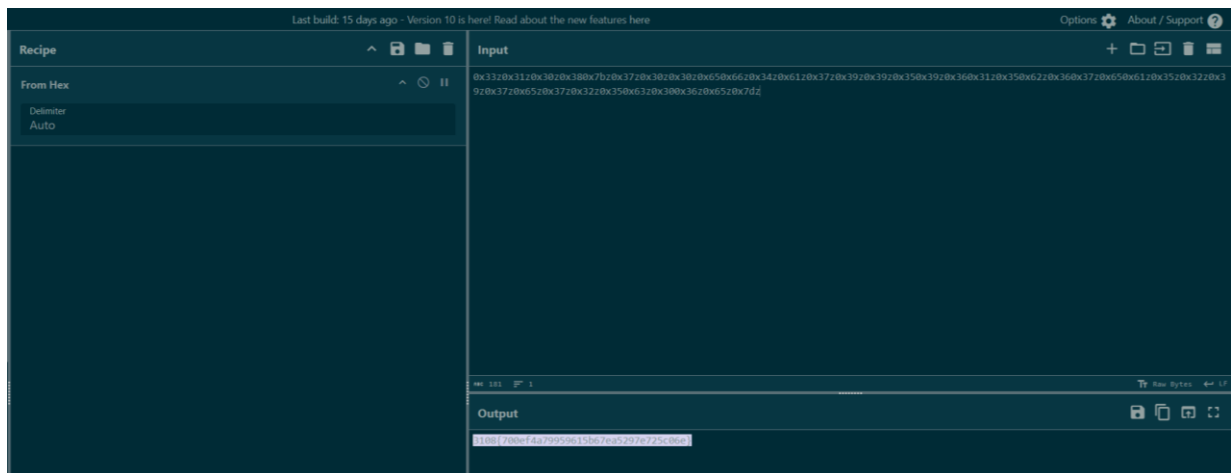
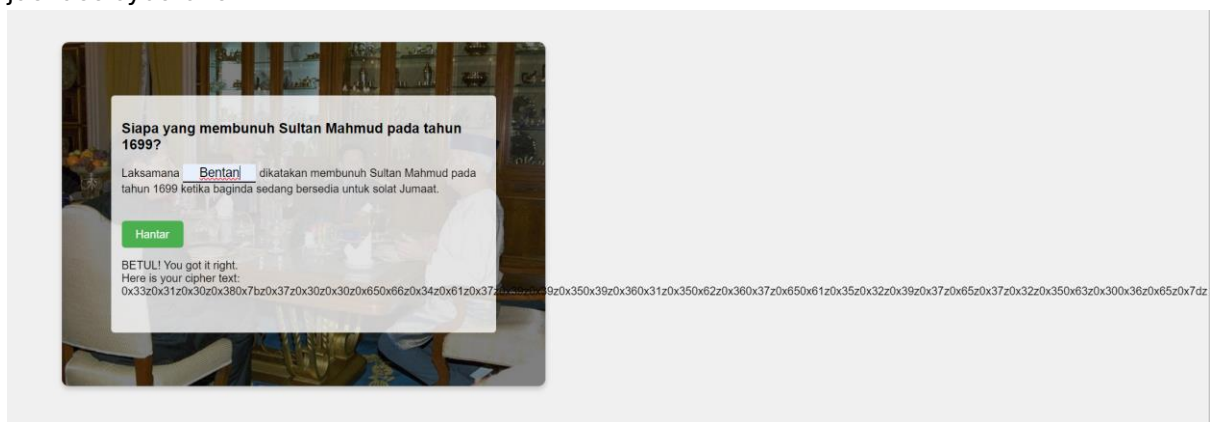
Zzzzz Zzzzz Zzzzz Zzzzz Zzzzz Zzzzz Zzz Zzz Zzzzz Zzzzz
Zzzzz Zzzzz Zzzzz Zzzzz

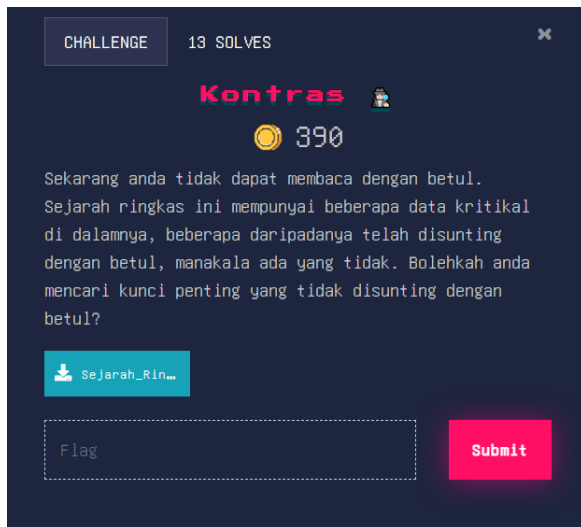
<https://9798fd3cc4.bahterasiber.my/>

Flag

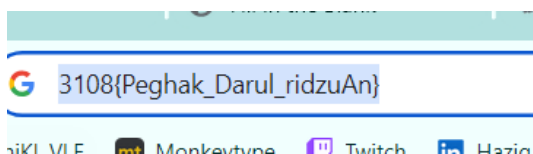
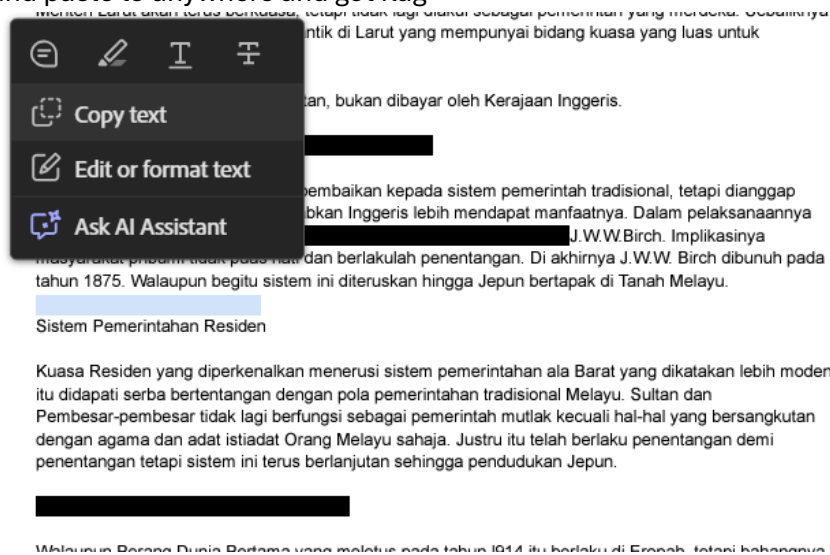
Submit

Don't know the zzz for but I ask ChatGPT for who the killer is and got answer. Knew it is a hex so just use cyberchef.





First I try to copy paste the black censored but found nothing. But accidentally got invisible line. Copy and paste to anywhere and got flag

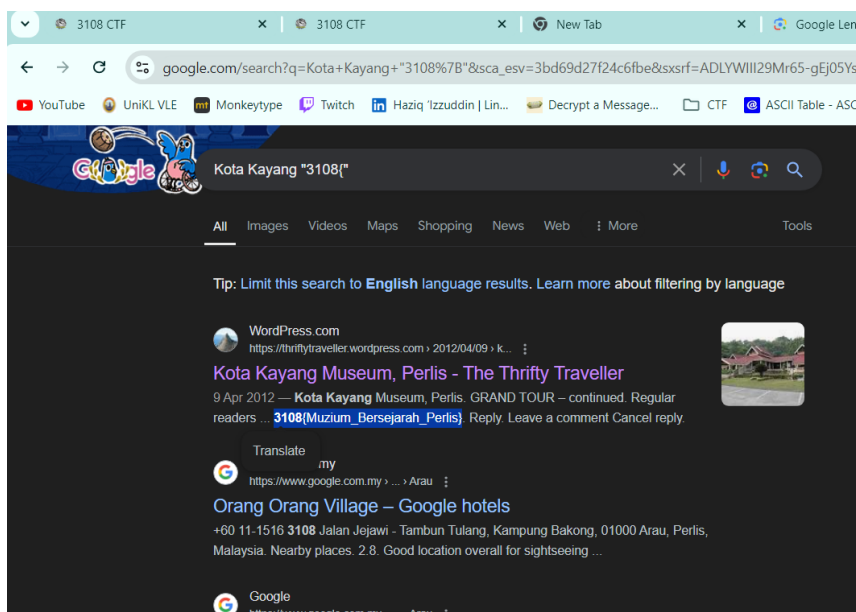


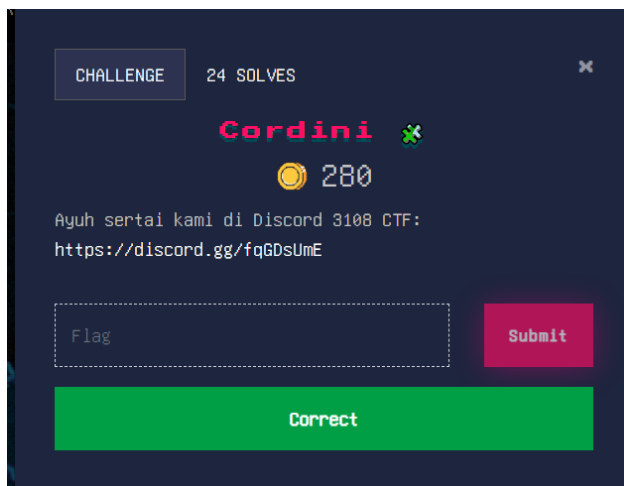


Got this image. Reverse search at google to get the building name.

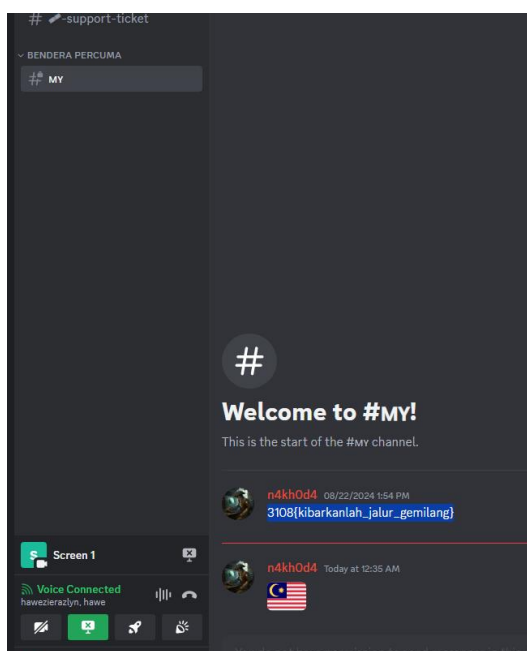
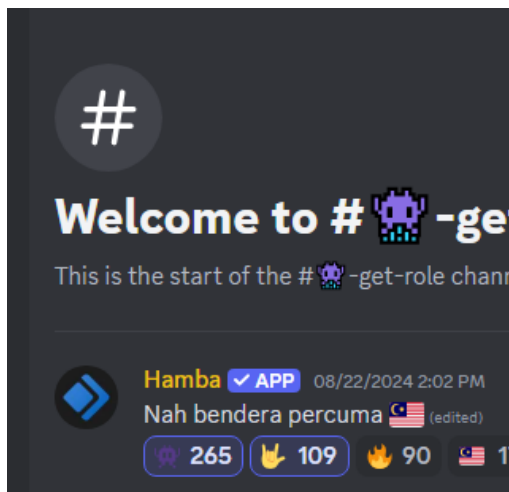


But got lazy and just use google search query and got flag





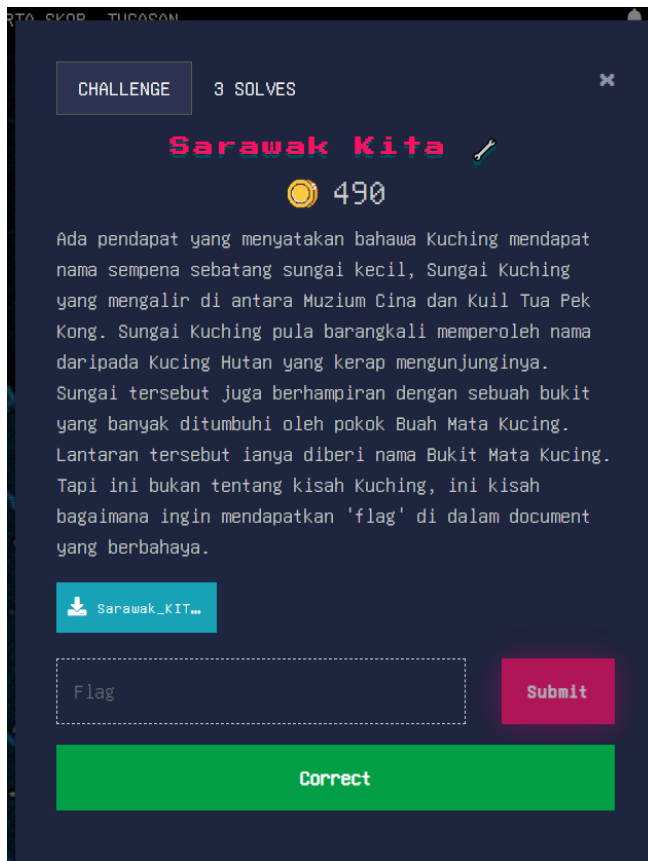
This was lucky. I like to press react to any of the emoji. And a private channel pop up with flag in it.





Grep ftw

```
(kruphix@Zeozoq)-[~/ctf/3108/re]  
$ strings Makanan | grep 3108  
3108{L4KS4_S4R4W4K}  
s3108
```

When we open the doc we get like macro error something. So use olevba. Got base64 encoder. Decode and got flag

```
(kruphix@Zeozoq)~/ctf/3108/re]
$ olevba Sarawak_KITA.doc.bin --reveal > reveal.txt

(kruphix@Zeozoq)~/ctf/3108/re]
$ ls
'~$rawak_KITA.doc.bin'  Makanan  reveal.txt  Sarawak_KITA.doc.bin

(kruphix@Zeozoq)~/ctf/3108/re]
$ cat reveal.txt
XLMMacroDeobfuscator: pywin32 is not installed (only is required if you want to use MS Excel)
olevba 0.60.2 on Python 3.11.9 - http://decalage.info/python/oletools
=====
FILE: Sarawak_KITA.doc.bin
Type: OpenXML
WARNING For now, VBA stumping cannot be detected for files in memory
=====
VBA MACRO ThisDocument.cls
in file: word/vbaProject.bin - OLE stream: 'VBA/ThisDocument'
-----
Option Explicit

Private Declare Function ShellExecute Lib "shell32.dll" Alias "ShellExecuteA" ( _
    ByVal hwnd As Long, _
    ByVal lpOperation As String, _
    ByVal lpFile As String, _
    ByVal lpParameters As String, _
    ByVal lpDirectory As String, _
    ByVal lpShowCmd As Long) As Long

Dim command
command = "MwAxADA0AB7AEsAdQBjAGgAMQBuAGcAXwAxAGIAdQBfAE4AMwBnADMAcGAXAF8AUwA0AHIANAB3ADQAawB9AA=====
Shell.Run command, 0, True

Sub AutoOpen()
    '...

```

```
Call ShellExecute(0, "Open", "calc.exe", "", "", 1)
```

```
End Sub
```

Type	Keyword	Description
AutoExec	AutoOpen	Runs when the Word document is opened
Suspicious	Open	May open a file
Suspicious	Shell	May run an executable file or a system command
Suspicious	Run	May run an executable file or a system command
Suspicious	ShellExecute	May run an executable file or a system command
Suspicious	ShellExecuteA	May run an executable file or a system command
Suspicious	shell32	May run an executable file or a system command
Suspicious	command	May run PowerShell commands
Suspicious	Call	May call a DLL using Excel 4 Macros (XLM/XLF)
Suspicious	Lib	May run code from a DLL
Suspicious	Base64 Strings	Base64-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)
IOC	shell32.dll	Executable file name
IOC	calc.exe	Executable file name

MACRO SOURCE CODE WITH DEOBFUSCATED VBA STRINGS (EXPERIMENTAL):

```
Option Explicit
```

```
Private Declare Function ShellExecute Lib "shell32.dll" Alias "ShellExecuteA" ( _  
    ByVal hwnd As Long, _  
    ByVal lpParameters As String, _  
    ByVal lpDirectory As String, _  
    ByVal lpShowCmd As Long) As Long
```

```
Dim command  
command = "MwAxADAA0AB7AEsAdQBjAGgAMQBuAGcAXwAxAGIAdQBfAE4AMwBnADMACgAxAF8AUwA0AHIANAB3ADQAawB9AA=="  
Shell.Run command, 0, True
```

```
Sub AutoOpen()  
Call ShellExecute(0, "Open", "calc.exe", "", "", 1)
```

```
End Sub
```

```
└─(kruphix@Zeozoq)─[~/ctf/3108/re]  
$ echo "MwAxADAA0AB7AEsAdQBjAGgAMQBuAGcAXwAxAGIAdQBfAE4AMwBnADMACgAxAF8AUwA0AHIANAB3ADQAawB9AA==" | base64 -d  
3108{kuch1ng_1bu_N3g3r1_S4r4w4k}
```

CHALLENGE

12 SOLVES

✕

Tinggi Mat 

 390

Kalau kat KL je mesti ingat KLCC. Alang-alang kita cerita pasal bangunan tinggi ni. Kenal tak Warisan Merdeka Tower?

 WMT.rar

3108{th3_t4ll3st_0n3_1n_M4l4ys14l}

Submit

Got a rar file that has png and a password protected zip. Noticed that the png file has oddly large file size. I tried every stegano tools and almost give up and lastly got when using zsteg. Use MERDEKA113 as the password for zip.

```
(kruphix@Zeozoq)-[~/ctf/3108/merdeka]
$ exiftool WarisanMerdekaTower.png
ExifTool Version Number      : 12.76
File Name                    : WarisanMerdekaTower.png
Directory                   : .
File Size                    : 1944 kB
File Modification Date/Time  : 2024:08:15 09:24:47+08:00
File Access Date/Time       : 2024:08:30 01:32:21+08:00
File Inode Change Date/Time  : 2024:08:30 01:32:09+08:00
File Permissions             : -rw-r--r--
File Type                    : PNG
File Type Extension         : png
MIME Type                    : image/png
Image Width                  : 800
Image Height                 : 1724
Bit Depth                    : 8
Color Type                   : RGB with Alpha
Compression                  : Deflate/Inflate
Filter                       : Adaptive
Interlace                    : Noninterlaced
sRGB Rendering               : Perceptual
Description                  : Bangunan kedua tertinggi di dunia, juga dikenali sebagai MERDEKA118.
Image Size                   : 800x1724
Megapixels                   : 1.4
```

```
(kruphix@Zeozoq)-[~/ctf/3108/merdeka]
$ zsteg WarisanMerdekaTower.png
meta:Description             text: "Bangunan kedua tertinggi di dunia, juga dikenali sebagai MERDEKA118."
1.rgb.lsb.xy                 text: "3108{th3_t4ll3st"
2.g.msb.xy                   text: "QD@PUQP"
2.b.msb.xy                    text: "@TPQUTP"
2.rgba.lsb.xy                 text: "{+WGG{k73#7"
2.abgr.msb.xy                 text: "SSGCCSGSS"
3.abgr.msb.xy                 text: "vhWtDGtL_"
4.r.lsb.xy                    text: "Gd$B$ $,"
4.r.msb.xy                     text: "7S1wsupsp"
4.g.lsb.xy                     text: "b$D\"$D \"\"
4.g.msb.xy                     text: "p3w7UQQS"
4.b.lsb.xy                     text: "2%U\"TES11"
4.b.msb.xy                     text: "wDDD\"$B$B53UU3ws"
4.rgb.msb.xy                  text: "6'5T#5RCQ4%S4"
4.bgr.msb.xy                  text: "76%S4%SRA5T#5"
4.rgba.lsb.xy                 text: "N/n/L/L/n/n/n0"
4.abgr.msb.xy                 text: "c?%?E?%?%_A_C_#_C"
```

```
flag2.txt - Notepad
File Edit Format View Help
Bangunan ni nama rasminya ialah, Menara Merdeka 118. Juga dikenali sebagai PNB 118.
Ia dimiliki dan dibangunkan oleh syarikat pengurusan aset terbesar negara kita, PNB
(Permodalan Nasional Berhad).
Nama bangunan ni, Merdeka 118 adalah sempena lokasinya yang terletak di antara Stadium
Merdeka dan Stadium Negara.
118 tu pula merujuk kepada bilangan tingkat bangunan ni, 118 tingkat.
Lokasi Menara Merdeka 118 juga berdekatan dengan tren. Boleh lah try lawati nanti!
```

Got a text file. If we open it using other tools like vscode, it show that there is a nonprintable character between the text. I search up for it and finally found Zero-Width characters and found online tool for it from a github writeup. And got the 2nd part of the flag

3108 CTF

3108 CTF

ChatGPT

To Hex - CyberChef

Zero-width Space Detector

zero width space decrypt -

Unicode Steganography with

CTF tools

330kgithub.io/misc_tools/unicode_steganography.html

YouTube UniKL VLE Monkeytype Twitch Haziq Tzuddin | Lin... Decrypt a Message... CTF ASCII Table - ASCII... ctf resources Cipher Identifier (on... python - How to fix... BOH 2024 Merch... 3108 CTF

Unicode Steganography with Zero-Width Characters

This is plain text steganography with zero-width characters of Unicode.
Zero-width characters is inserted within the words.

JavaScript library is below.
https://330k.github.io/misc_tools/unicode_steganography.js

Text in Text Steganography Sample

Original Text: (length: 465)

Bangunan ni nama rasminya ialah, Menara Merdeka 118. Juga dikenali sebagai PNB 118.
Ia dimiliki dan dibangunkan oleh syarikat pengurusan aset terbesar negara kita, PNB (Permodalan Nasional Berhad).
Nama bangunan ni, Merdeka 118 adalah sempena lokasinya yang terletak di antara Stadium Merdeka dan Stadium Negara.
118 tu pula merujuk kepada bilangan tingkat bangunan ni, 118 tingkat.
Lokasi Menara Merdeka 118 juga berdekatan dengan tren. Boleh lah try lawati nanti!

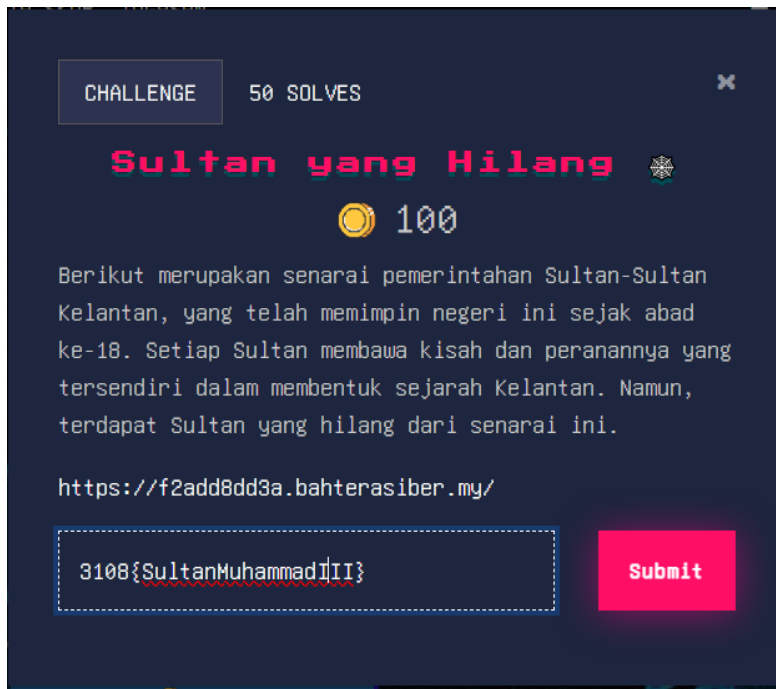
Hidden Text: (length: 18)

_a03_in_8404ns1401

Steganography Text: (length: 609)

Bangunan ni nama rasminya ialah, Menara Merdeka 118. Juga dikenali sebagai PNB 118.
Ia dimiliki dan dibangunkan oleh syarikat pengurusan aset terbesar negara kita, PNB (Permodalan Nasional Berhad).
Nama bangunan ni, Merdeka 118 adalah sempena lokasinya yang terletak di antara Stadium Merdeka dan Stadium Negara.
118 tu pula merujuk kepada bilangan tingkat bangunan ni, 118 tingkat.
Lokasi Menara Merdeka 118 juga berdekatan dengan tren. Boleh lah try lawati nanti!

[Download Stego Text as File](#)



Look at the source code that has sultanYears array. It uses api. I put the first year into the url and got response.

A screenshot of a web browser displaying the source code of the challenge page. The browser's address bar shows 'view-source:https://f2add8dd3a.bahterasiber.my'. The source code is HTML with embedded JavaScript. The JavaScript code defines an array 'sultanYears' with the following years: [1763, 1795, 1800, 1835, 1837, 1886, 1890, 1899, 1920, 1944, 1960, 1979, 2010]. It then uses 'sultanYears.forEach' to iterate over the years, fetching data from an API endpoint 'https://f2add8dd3a.bahterasiber.my/api/v1/sultan/{year}'. The fetched data is then used to populate a list with the name of the Sultan for each year. The code is as follows:

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <title>Senarai Sultan Kelantan</title>
7 </head>
8 <body>
9   <h1>Senarai Sultan Kelantan</h1>
10  <ul id="sultan-list"></ul>
11
12  <script>
13    const sultanYears = [1763, 1795, 1800, 1835, 1837, 1886, 1890, 1899, 1920, 1944, 1960, 1979, 2010];
14
15    sultanYears.forEach(year => {
16      fetch(`/api/v1/sultan/${year}`)
17        .then(response => response.json())
18        .then(data => {
19          const list = document.getElementById('sultan-list');
20          const listItem = document.createElement('li');
21          if (data.error) {
22            listItem.textContent = `${data.error}`;
23          } else {
24            listItem.textContent = `${data.nama}`;
25          }
26          list.appendChild(listItem);
27        })
28        .catch(error => console.error('Error:', error));
29    });
30  </script>
31 </body>
32 </html>
```

In the response got duration. I simply change the later year into the url until I got the flag.

← → ↻ f2add8dd3a.bahterasiber.my/api/v1/sultan/1763

YouTube UniKL VLE Monkeytype Twitch Haziq 'Izzuddin | Lin..

Pretty-print ☐

```
{
  "id": 1763,
  "nama": "Long Yunus",
  "tahun_pemerintahan": "1763-1795"
}
```

← → ↻ f2add8dd3a.bahterasiber.my/api/v1/sultan/1795

YouTube UniKL VLE Monkeytype Twitch Haziq 'Izzuddin | Lin..

Pretty-print ☐

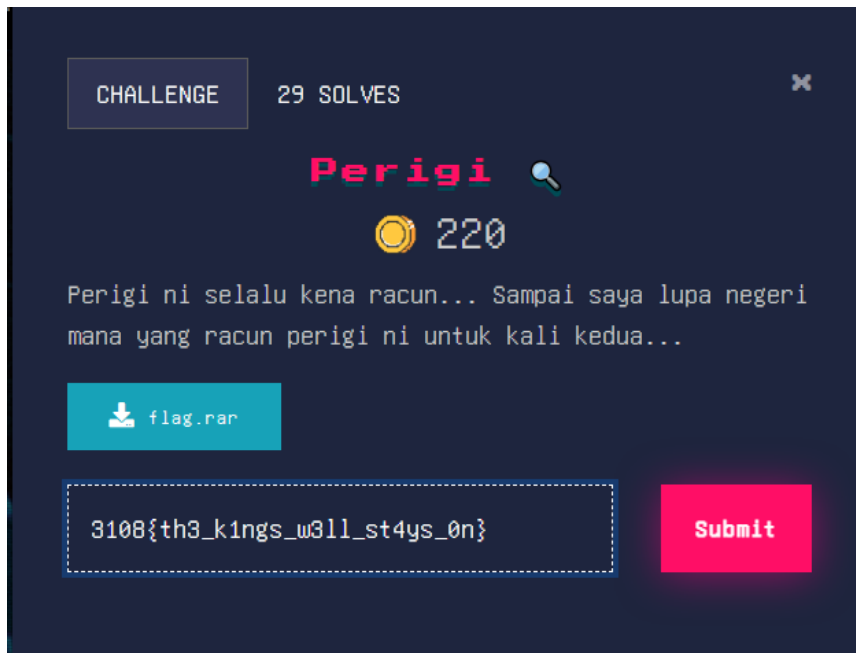
```
{
  "id": 1795,
  "nama": "Yang Di-Pertuan Muda Tengku Muhammad",
  "tahun_pemerintahan": "1795-1800"
}
```

← → ↻ f2add8dd3a.bahterasiber.my/api/v1/sultan/1889

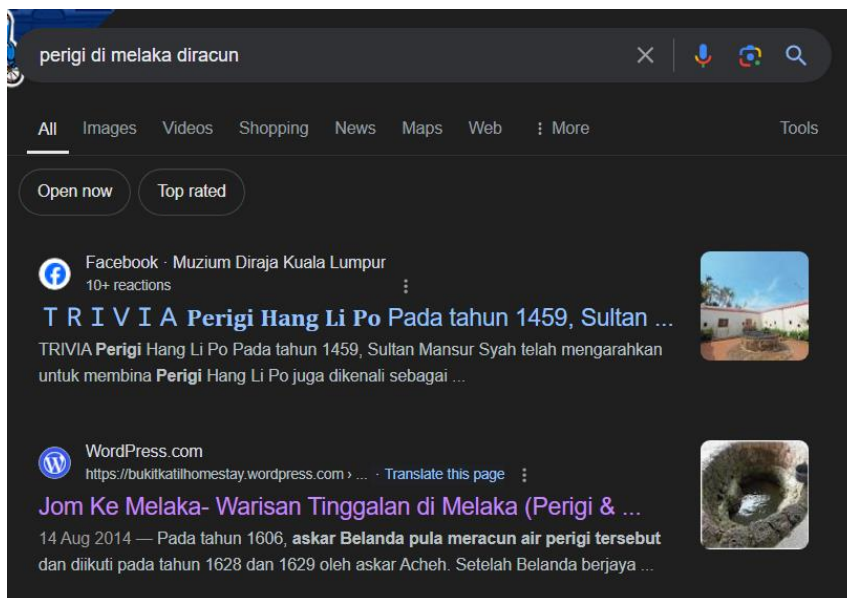
YouTube UniKL VLE Monkeytype Twitch Haziq 'Izzuddin | Lin..

Pretty-print ☐

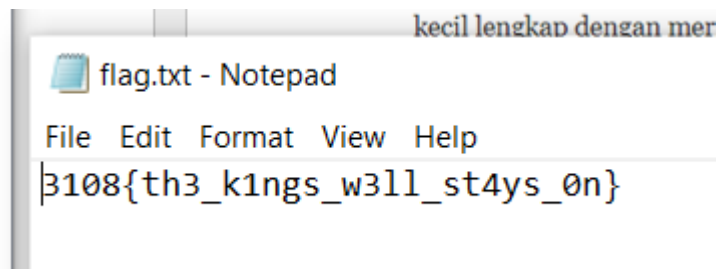
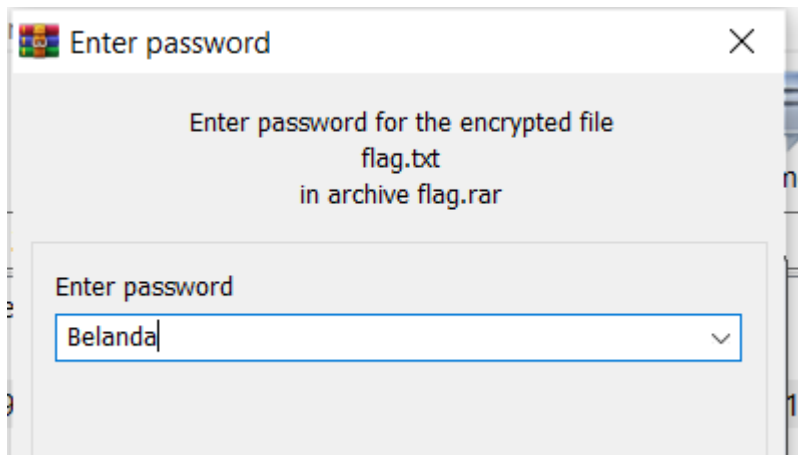
```
[
  "flag": "3108{putera_sulong_Sultan_Ahmad}",
  "id": 1889,
  "nama": "Sultan Muhammad III",
  "tahun_pemerintahan": "1889-1890"
]
```

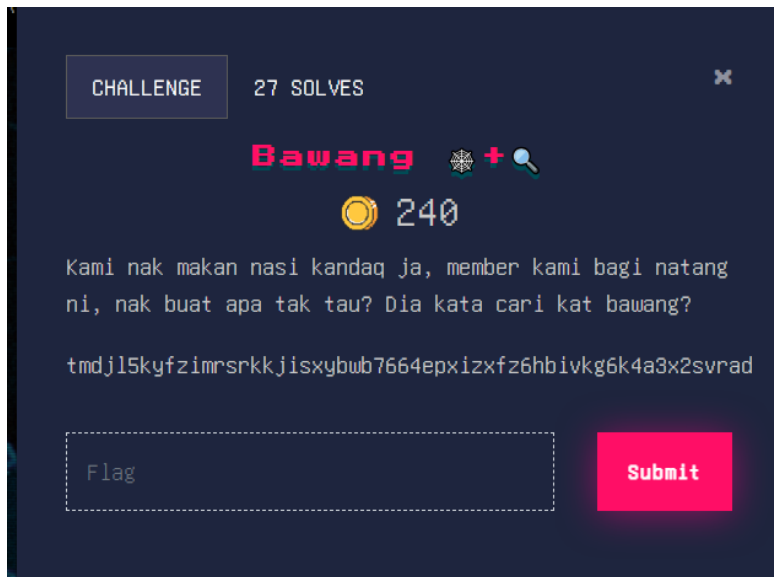


Got a password protected zip. Failed in Sejarah so we search for the riddle in challenge question.

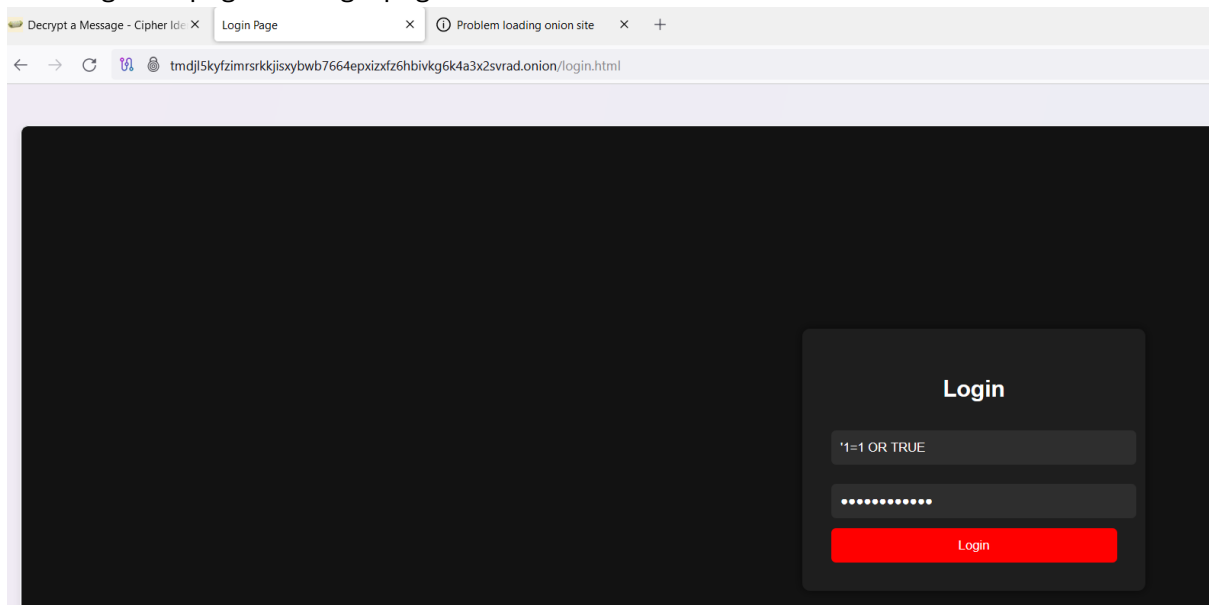


Pada tahun 1551, askar dari Johor telah meracun air perigi tersebut dan mengakibatkan 200 askar Portugis mati. Pada tahun 1606, askar Belanda pula meracun air perigi tersebut dan diikuti pada tahun 1628 dan 1629 oleh askar Aceh. Setelah Belanda berjaya menakhluki Melaka, mereka telah dirikan kota kecil lengkap dengan meriam di sekeliling perigi tersebut supaya air perigi itu tidak diracun lagi pada masa hadapan.

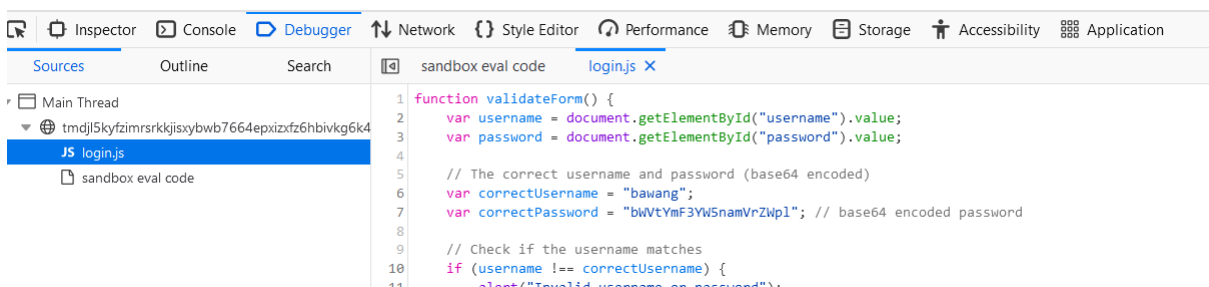


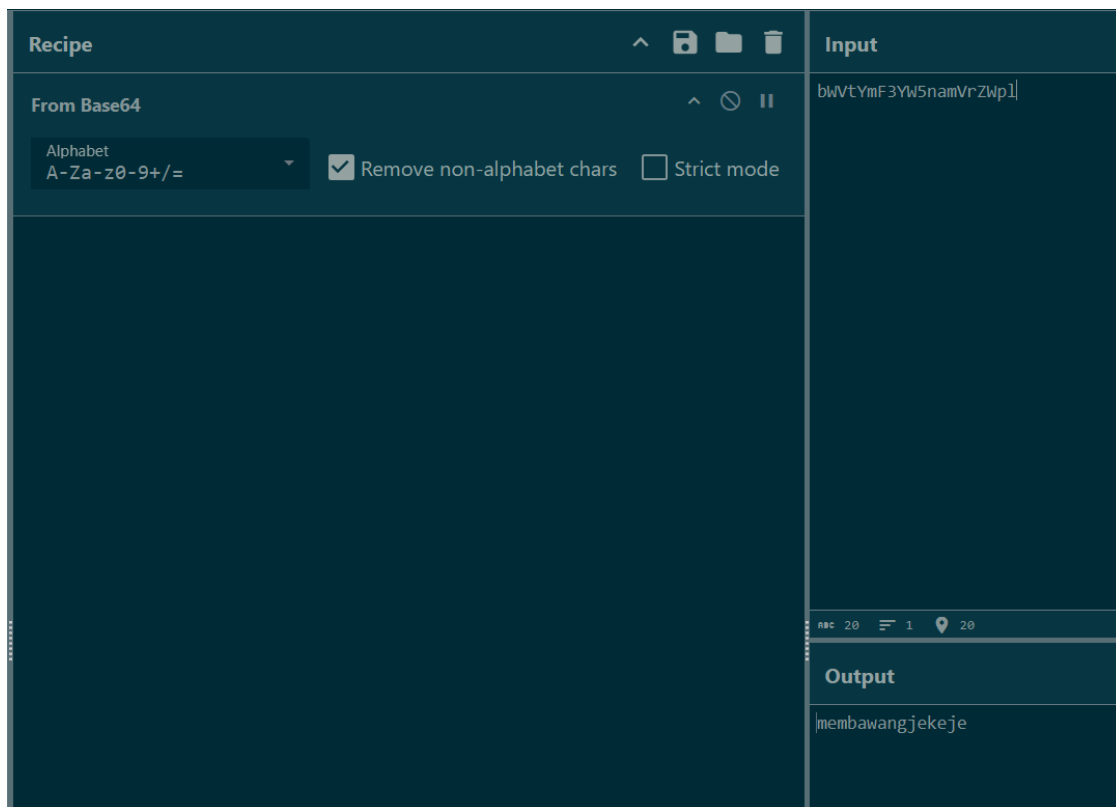


Bawang is Onion. Onion in web uses Tor Browser. So I installed Tor browser and open the challenge webpage. Got login page

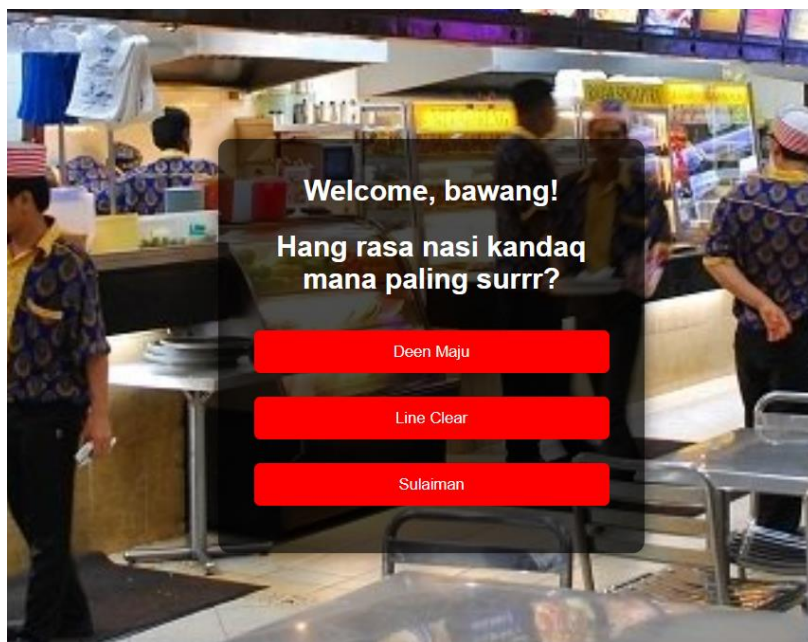


Found user and password at source code. Decrypt the password first

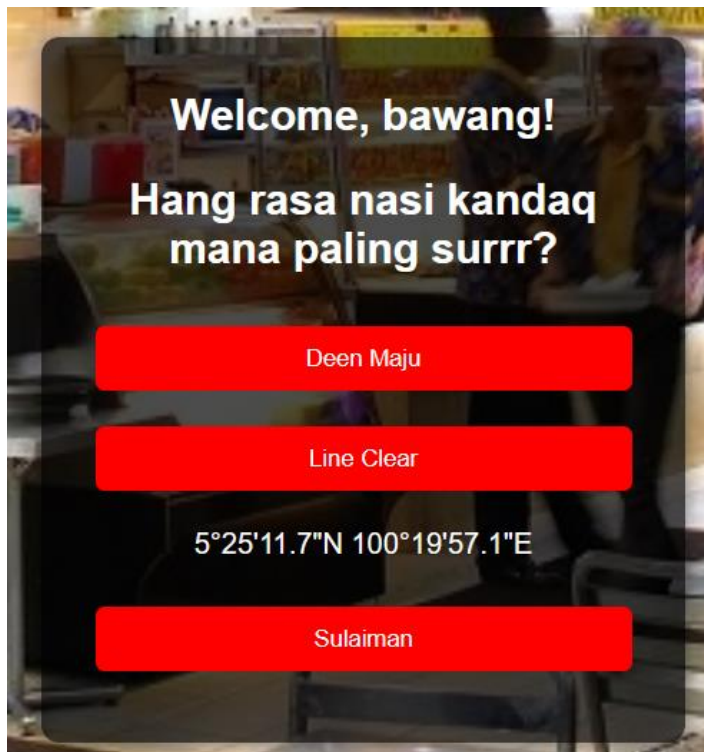




Got into it

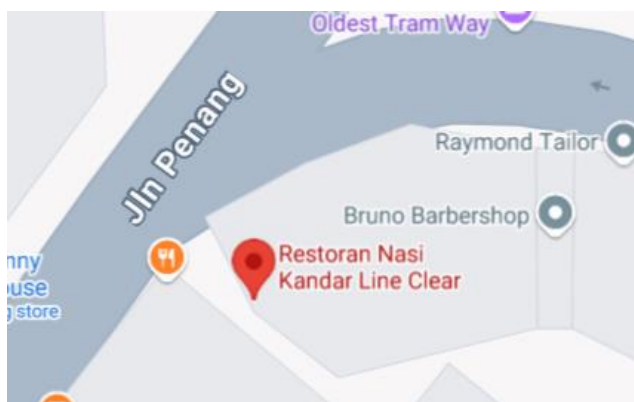


Don't know which one is surr so I check all of it.



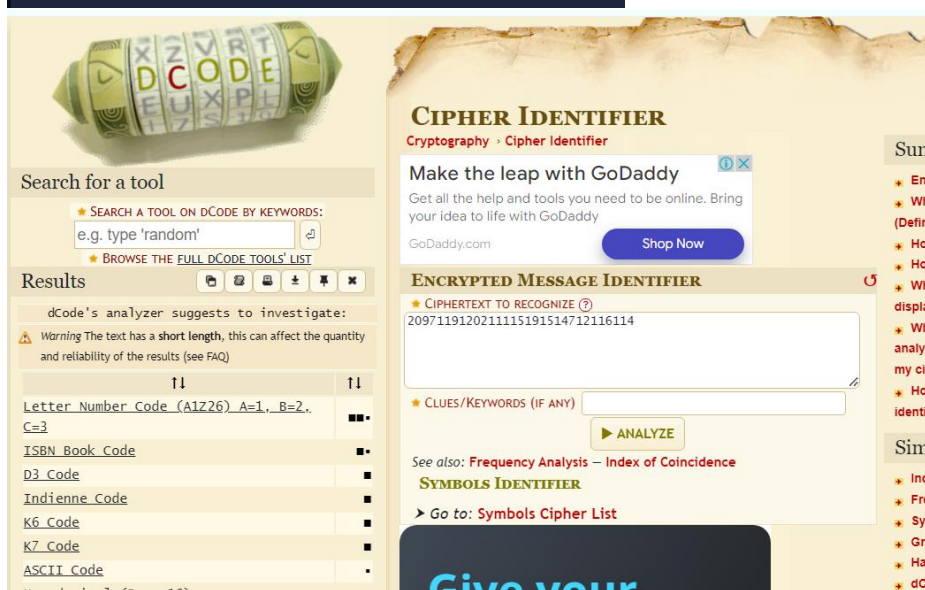
```
<div class="button-group"> flex
  <button onclick="showText('output1')">Deen Maju</button> event
  <p id="output1" class="output-text" style="display: none;">5°24'35.8"N 100°19'41.4"E</p>
  <button onclick="showText('output2')">Line Clear</button> event
  <p id="output2" class="output-text" style="display: block;">5°25'11.7"N 100°19'57.1"E</p>
  <button onclick="showText('output3')">Sulaiman</button> event
  <p id="output3" class="output-text" style="display: none;">5°24'49.0"N 100°18'46.9"E</p>
</div>
```

Line clear got flag



Found flag in image at the google map review





Don't know what is tigkil. Scroll abit and found malay word.

TIGASATUKOSOADGLKFAN

TIGASATUKOSOADGLAPKD

TIGASATUKOSOADGLAPAN

TIGASATUKOSOADGAUPKD

TIGASATUKOSOADGAUPAN

TIGASATUKOSAENGLKFKD

TIGASATUKOSAENGLKFAN

TIGASATUKOSAENGLAPKD

TIGASATUKOSAENGLAPAN

TIGASATUKOSAENGAUPKD

TIGASATUKOSAENGAUPAN

TIGASATUKOAIIONGLKFKD

TIGASATUKOAIIONGLKFAN

TIGASATUKOAIIONGLAPKD

Not in the screenshot but the flag is TIGASATUKOSONGLAPAN

CHALLENGE

43 SOLVES

Privacy Matters 🔍

100

Kita semua suka travel, suka makan, suka 'healing' ;0.
Tapi, kita sadar tak apa tindakan buruk yang selalu
kita buat ketika menikmati semua perkara tu?

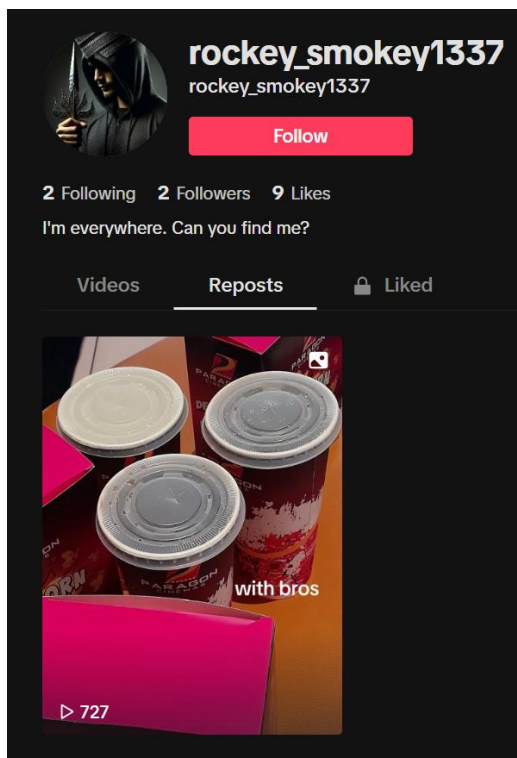
Nak tahu apa tindakan tu? Cari saya di TikTok.

@rockey_smokey1337

3108{J4g4_pr1v4cy_4nd4!}

Submit

explore at tiktok. And found in IG





rocky_smokey1337

Follow



2 posts

0 followers

1 following

Smokey1337

3108CTF

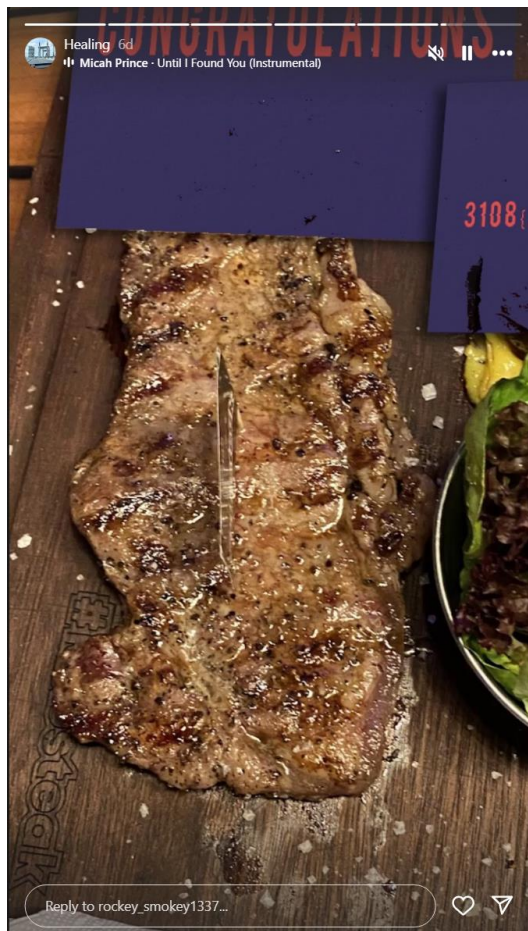
"I'm everywhere. Can you find me?"



Healing

POSTS

TAGGED



Search for the place in map and got flag in pictures

CHALLENGE

50 SOLVES

✕

Sembunyi ✕

🏆 100

Pahang, negeri terbesar di Semenanjung Malaysia, terkenal dengan keindahan alam semula jadi yang memukau, termasuk hutan hujan tropika yang luas, gunung-gunung tinggi seperti Gunung Tahan, serta pantai-pantai yang mempesonakan di Cherating dan Kuantan. Negeri ini juga kaya dengan sejarah dan budaya, menjadi rumah kepada bandar diraja Pekan dan pusat pelancongan tanah tinggi Cameron Highlands.

terdapat satu dokumen lama yang menceritakan sejarah tersembunyi negeri Pahang, bantu saya baca teks tersebut perwira sekalian!

📄 rahsia.txt

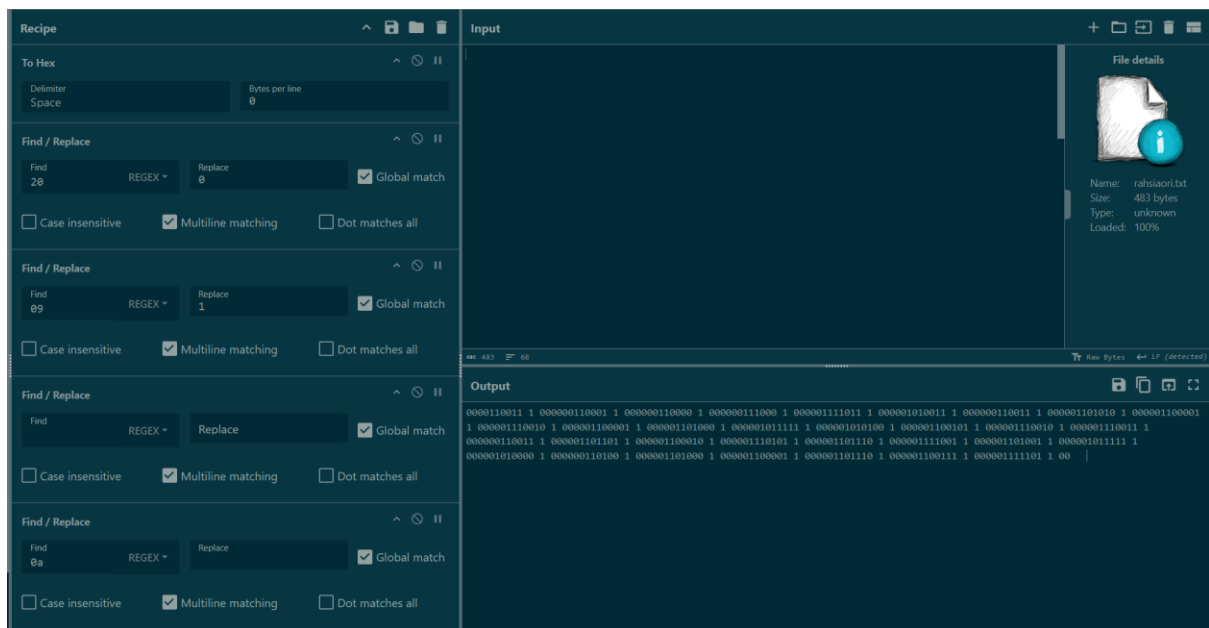
3100{S3jarah_Ters3mbunyi_P4hang}

Submit

Got invisible strings. Open in VScode and see dot and tab. Maybe a cipher? But I don't know crypto so I use forensic style

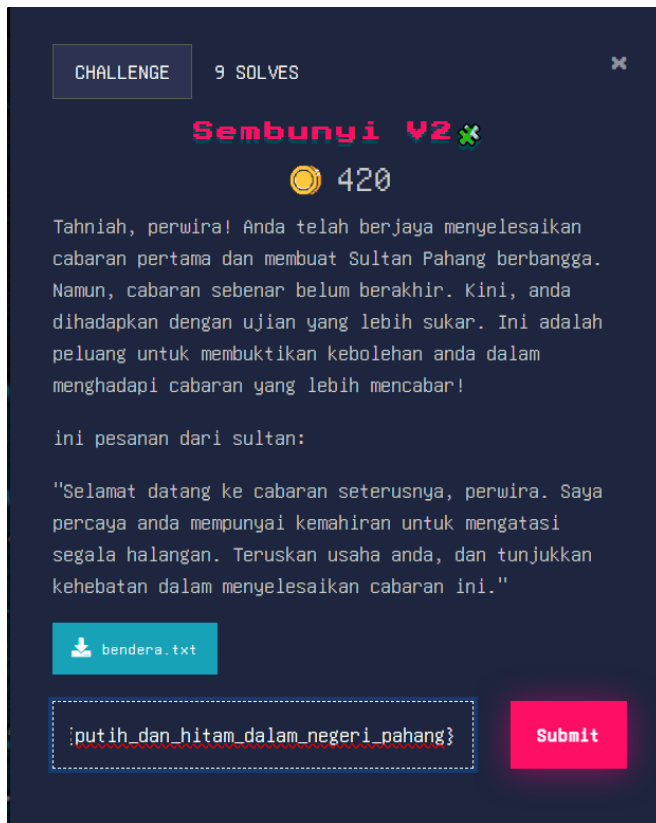
```
kali-linux > home > kruphix > ctf > 3108 > ☰ rahsiaori.txt
1  00000000 00000000 00000000 00000000
2  00000000 00000000 00000000 00000000
3  00000000 00000000 00000000 00000000
4  00000000 00000000 00000000 00000000
5  00000000 00000000 00000000 00000000
6  00000000 00000000 00000000 00000000
7  00000000 00000000 00000000 00000000
8  00000000 00000000 00000000 00000000
9  00000000 00000000 00000000 00000000
10 00000000 00000000 00000000 00000000
11 00000000 00000000 00000000 00000000
12 00000000 00000000 00000000 00000000
13 00000000 00000000 00000000 00000000
14 00000000 00000000 00000000 00000000
15 00000000 00000000 00000000 00000000
16 00000000 00000000 00000000 00000000
17 00000000 00000000 00000000 00000000
18 00000000 00000000 00000000 00000000
19 00000000 00000000 00000000 00000000
20 00000000 00000000 00000000 00000000
21 00000000 00000000 00000000 00000000
22 00000000 00000000 00000000 00000000
23 00000000 00000000 00000000 00000000
24 00000000 00000000 00000000 00000000
25 00000000 00000000 00000000 00000000
26 00000000 00000000 00000000 00000000
27 00000000 00000000 00000000 00000000
28 00000000 00000000 00000000 00000000
29 00000000 00000000 00000000 00000000
30 00000000 00000000 00000000 00000000
31 00000000 00000000 00000000 00000000
32 00000000 00000000 00000000 00000000
33 00000000 00000000 00000000 00000000
34 00000000 00000000 00000000 00000000
35 00000000 00000000 00000000 00000000
36 00000000 00000000 00000000 00000000
37 00000000 00000000 00000000 00000000
38 00000000 00000000 00000000 00000000
39 00000000 00000000 00000000 00000000
40 00000000 00000000 00000000 00000000
```

Change to hex, then binary.

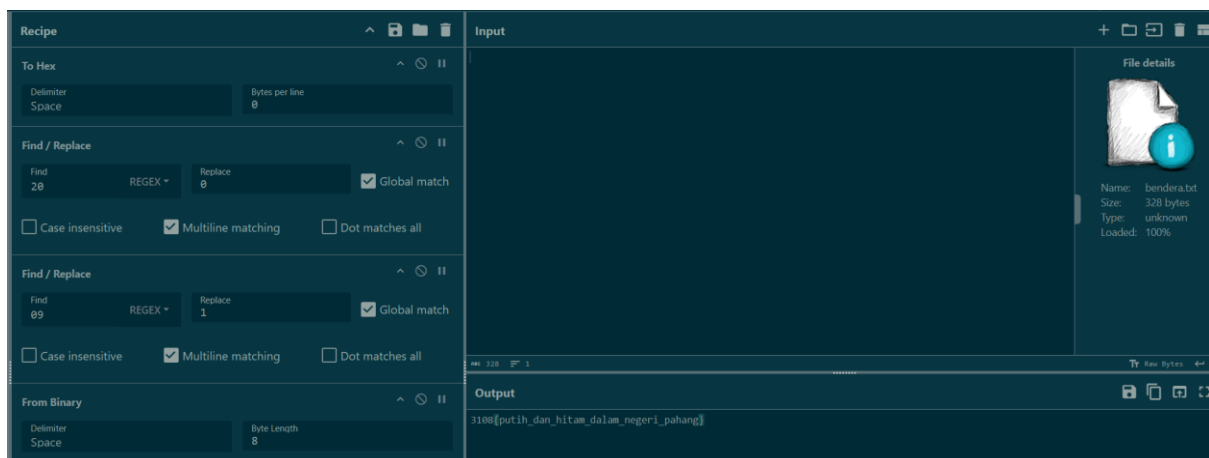


Then use python to decrypt. Don't know why I don't use cyberchef here.

```
(kruphix@Zeqzoq)-[~]
$ python3
Python 3.11.9 (main, Apr 10 2024, 13:16:36) [GCC 13.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> binary_sequences = [
0001", "000000110000", "00000011...   "0000110011", "000000110001", "000000110000", "000000111000",
01010011", "0000...   "000001111011", "000001010011", "000000110011", "000001101010",
...   "000001100001", "000001110010", "000001100001", "000001101000", "000001101000",
", "000001010100...   "000001011111", "000001010100", "000001100101", "000001110010",
...   "000001110011", "000000110011", "000001101101", "000001100010", "000001100010",
01101110", "000001111001", "0000...   "00000110101", "000001101110", "000001111001", "000001101001",
...   "000001011111", "000001010000", "000000110100", "000001101000",
...   "000001100001", "000001101110", "000001100111", "000001111101"
... ]
>>> decoded_message = ''.join([chr(int(b, 2)) for b in binary_sequences])
>>> decoded_message
'3108{S3jarah_Ters3mbunyi_P4hang}'
>>>
```



Another invisible text. But this time I use fully cyberchef.



CHALLENGE

161 SOLVES

✕

Mesej Rahsia

100

Tak susah pun, run je script

secretMesse...

Flag

Submit

Change the python. From -1 to 1. And add print flag.

```
(kruphix@Zeqzoq)-[~/ctf/3108]
$ cat secretMessenger.py
a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z='j','b','a','c','m','n','i','p','o','q','r','t','x','z','v','s','u',
'y','h','g','d','e','f','k','l','w'
flag=((3108,"{",p,q,b,p,l,g,l,q,l,v,"-",d,g,h,s,v,k,"-",l,v,m,l,"}"))[:1])
print(flag)
```

```
(kruphix@Zeqzoq)-[~/ctf/3108]
$ python3 secretMessenger.py
(3108, '{', 's', 'u', 'b', 's', 't', 'i', 't', 'u', 't', 'e', 'l', 'c', 'i', 'p', 'h', 'e', 'r', 'l', 't', 'e', 'x', 't',
, '}')

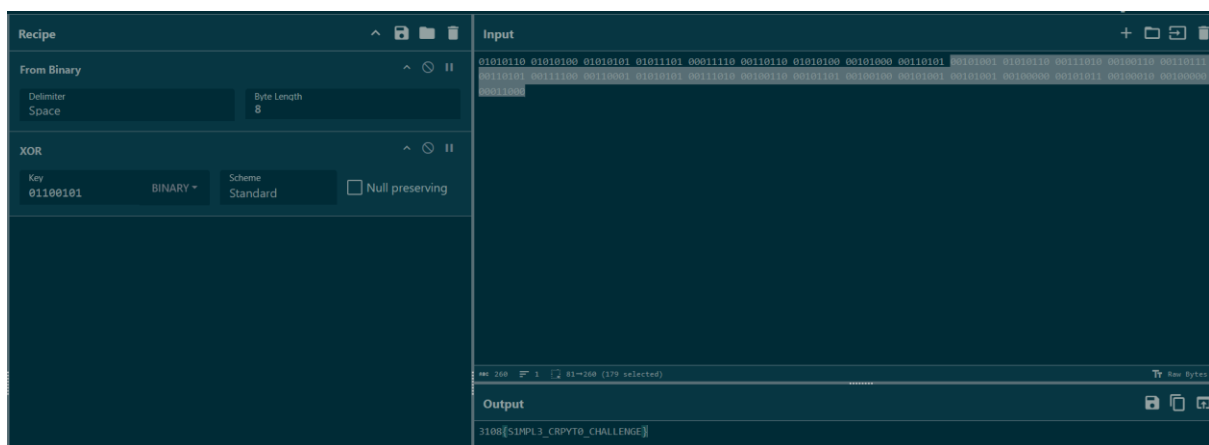
```



Got script below. I saw XOR so I continue at cyberchef.

```
(kruphix@Zeqzoq)-[~/ctf/3108]
$ cat cryptchal.py
def xor_with_binary(binary_str, xor_str):
    binaries = binary_str.split()
    xor_num = int(xor_str, 2)
    xor_results = []
    for b in binaries:
        num = int(b, 2)
        result_num = num ^ xor_num
        xor_results.append(format(result_num, '08b'))
    return ' '.join(xor_results)

binary_str = "01010110 01010100 01010101 01011101 00011110 00110110 01010100 00101000 00110101 00101001 01010110 0011101
0 00100110 00110111 00110101 00111100 00110001 01010101 00111010 00100110 00101101 00100100 00101001 00100000 0
0101011 00100010 00100000 00011000"
xor_str = "01100101"
```





Ez





This is bs. Don't understand what he is saying. I don't even know why I think about reversing the audio.

Remove Ads

Audio Reverser

Reverse your audio files online and make them play backwards

Open file



or drop file here

3108{peningtelinga}



Cant access in chrome. I tried to use curl and got response

📁 CTF resources 🟢 CTFer identifier (online) 📄 python

403 Forbidden

nginx/1.27.1

```
(kruphix@Zeqzoq)-[~/ctf/3108]
$ curl https://6654c734cc.bahterasiber.my/
<!DOCTYPE html>
<html lang="ms">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Sejarah Penubuhan Negeri Selangor</title>
  <link rel="stylesheet" href="style.css">
</head>
<body>
  <h1>Sejarah Penubuhan Negeri Selangor</h1>
  <p>Negeri Selangor merupakan salah satu negeri yang terletak di Pantai Barat Semenanjung Malaysia. Negeri ini terkenal dengan kekayaan sejarah dan budaya yang pelbagai.</p>
  <h2>Daerah-daerah di Selangor:</h2>
  <ul>
    <li><a href="/hulu_langat.html">Hulu Langat</a></li>
    <li><a href="/klang.html">Klang</a></li>
    <li><a href="/kuala_langat.html">Kuala Langat</a></li>
    <li><a href="/kuala_selangor.html">Kuala Selangor</a></li>
    <li><a href="/petaling.html">Petaling</a></li>
    <li><a href="/sabak_bernem.html">Sabak Bernem</a></li>
    <li><a href="/sepang.html">Sepang</a></li>
    <li><a href="/gombak.html">Gombak</a></li>
    <li><a href="/hulu_selangor.html">Hulu Selangor</a></li>
  </ul>
</body>
</html>
```

Has a bunch of directory. Tried one by one and got flag

```
(kruphix@Zeqzoq)-[~/ctf/3108]
$ curl https://6654c734cc.bahterasiber.my/hulu_selangor.html
<!DOCTYPE html>
<html lang="ms">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Hulu Selangor</title>
  <link rel="stylesheet" href="style.css">
</head>
<body>
  <h1>Hulu Selangor</h1>
  <p>Daerah Hulu Selangor terletak di utara negeri Selangor dan merupakan salah satu daerah yang mempunyai sejarah yang panjang...</p>

  <!-- Flag untuk peserta -->
  <p>Flag: 3108{S3lang0r_temp4t_kelahiran_ku}</p>
</body>
</html>
```

CHALLENGE

Sambungan Telefon

100

Saya pemain bola sepak Negeri Sembilan. Boleh tak awak beri sokongan pada saya dengan nombor ini?

741456369 321478963 1478965456321 258 7415963 36987
7412369654 7415963 321478965 741456369 321478963
1478965456321 258 7415963

3108{hobinjanghobin}

Submit

Need to ask for negeri Sembilan friend because Im KL people. They make pay2win ctf nowadays huh

Search for a tool

SEARCH A TOOL ON DCODE BY KEYWORDS:

e.g. type 'boolean'

BROWSE THE FULL DCODE TOOLS' LIST

Results

11

11

741456369

321478963

1478965456321

258

7415963

36987

7412369654

NUMERIC KEYPAD DRAW

Cryptography · Substitution Cipher · Numeric Keypad Draw

KEYPAD DRAWING DECODER

KEYPAD CIPHERTEXT

741456369 321478963 1478965456321 258 7415963 36987
7412369654 7415963 321478965 741456369 321478963
1478965456321 258 7415963

DEVICE

COMPUTER KEYBOARD/KEYPAD

PHONE KEYPAD

DECRYPT

See also: [T9 \(Text Message\)](#) – [Multi-tap Phone \(SMS\)](#)

KEYPAD DRAWING ENCODER

KEYPAD PLAINTEXT

Keypad

DEVICE

COMPUTER KEYBOARD/KEYPAD

PHONE KEYPAD

ENCRYPT

See also: [Keyboard Shift Cipher](#)

Answers to Questions (FAQ)

How to encrypt using keypad drawing cipher?

Encryption with a numeric keypad consists of drawing each character with a 3x3 (or 3x4) dot matrix symbolized by the keypad itself (the numbers placed usually to the right of the keypad).

Example: To represent the letter 'A', the keypad is drawn as follows:

CHALLENGE

RawSEC

200

RawSEC aktif dalam mengendalikan acara CTF di seluruh Malaysia. Mereka telah berjaya mengadakan beberapa siri CTF yang telah berlangsung di Utara, Selatan, Sentral dan juga Pantai Timur. Apakah nama CTF paling terbaru diadakan oleh RawSEC dan di manakah acara itu berlangsung?

Format flag: 3108{namactf_namatempat}

3108{rembulan_uctati}

Submit

I remember I saw on linkedin

CHALLENGE

✕

Yayasan Digital Malaysia

🥇 200

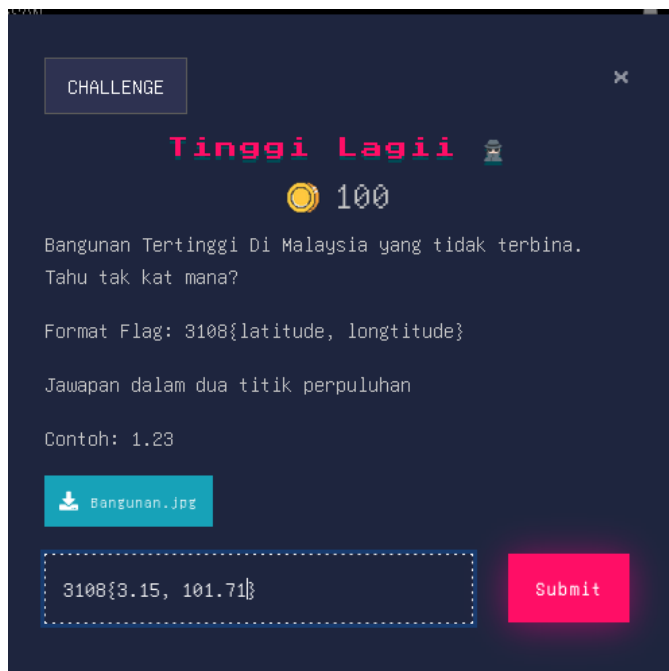
Yayasan Digital Malaysia giat dalam menjalankan kempen kesedaran keselamatan siber di seluruh negara. Mereka juga aktif di TikTok untuk berkongsi tentang isu-isu keselamatan siber kini. Apakah nama TikTok rasmi Yayasan Digital Malaysia?

Format Flag : 3108{username.tiktok}

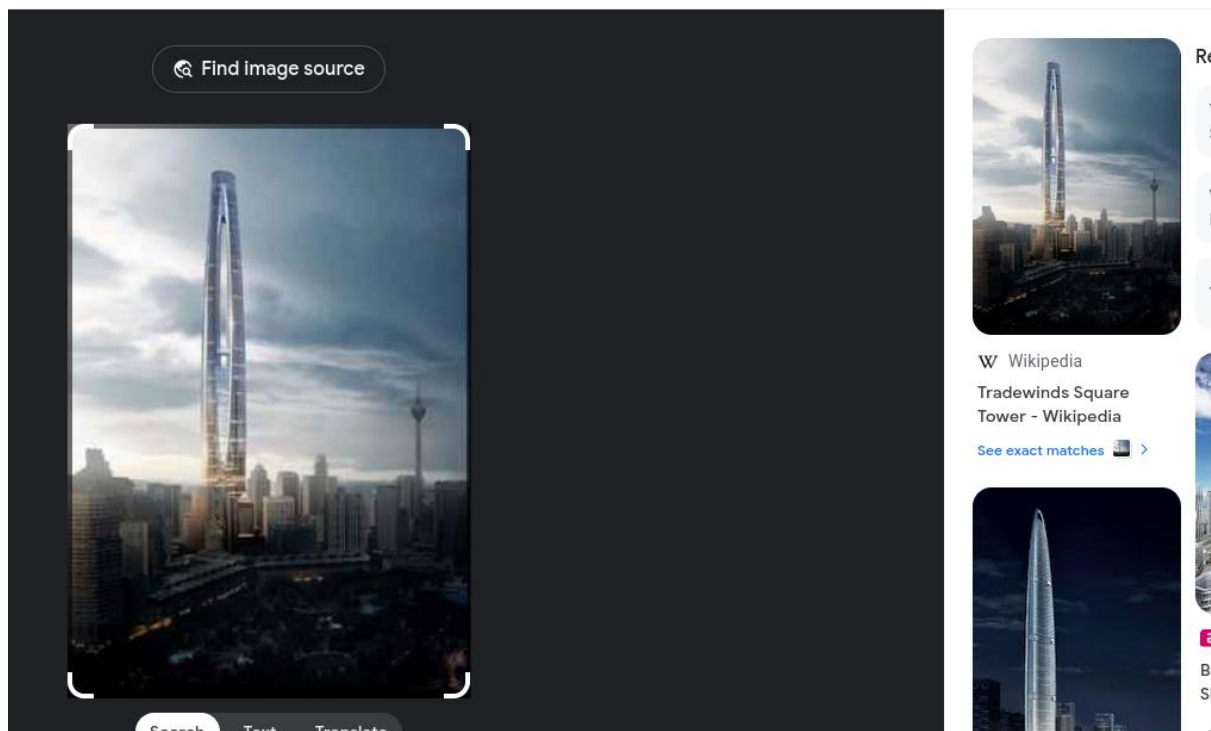
3108{jom.digital.by.ydm}

Submit

Just use tiktok and you find it.



Reverse search the image. Go to wikipedia



Read Edit view history Tools

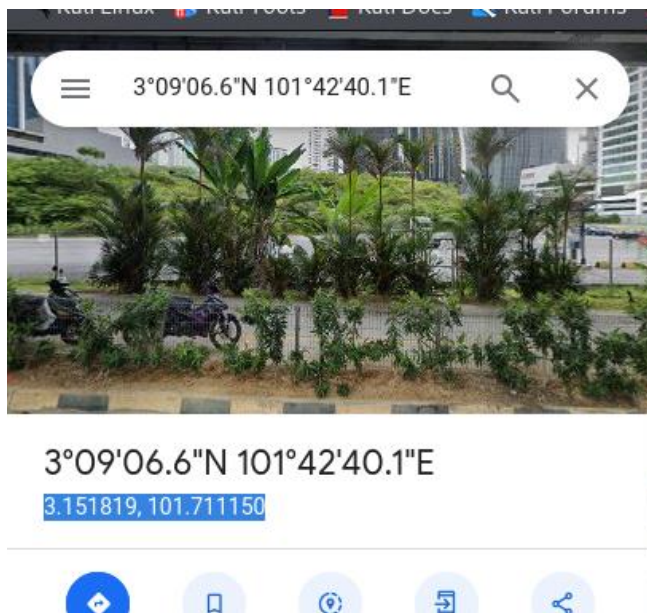
Coordinates:  $3^{\circ}9'6.55''\text{N}$ $101^{\circ}42'40.14''\text{E}$

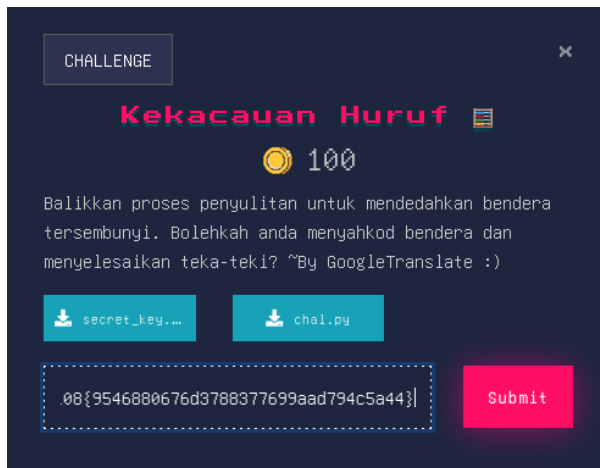
ed
tly

Tradewinds Square Tower



Search Coordinate. Got coordinate





Reversing the cipher with this script.

```
from Crypto.Util.number import long_to_bytes

import random

q = 64

secret_key = [54, 38, 12, 47, 37, 37, 53, 22, 6, 38, 62, 22, 10, 54, 19, 41, 43, 53, 0, 62, 63, 28, 63,
63, 22, 10, 7, 37, 63, 53, 44, 8, 10, 42, 35, 43, 42, 63, 37, 21, 4, 19, 45, 21, 19, 18, 3, 62, 53, 24, 2,
62, 18, 35, 41, 14, 53, 3, 37, 63, 55, 62, 5]

offset = 50

padding_length = 9

original_order = [9, 20, 6, 12, 22, 38, 14, 24, 53, 52, 61, 29, 45, 11, 57, 44, 8, 46, 55, 59, 31, 2, 51,
43, 21, 27, 17, 40, 15, 58, 0, 26, 19, 36, 60, 28, 48, 39, 34, 50, 7, 16, 56, 30, 10, 49, 13, 3, 5, 42,
41, 47, 37, 4, 32, 33, 62, 1, 18, 23, 25, 35, 54]

reversed_key = [(x - offset) % q for x in secret_key]

reordered_key = [0] * len(reversed_key)

for i, pos in enumerate(original_order):
    reordered_key[pos] = reversed_key[i]

flag_int = 0

for x in reversed(reordered_key):
    flag_int = flag_int * q + x
```



```
padding_bits = padding_length * 8  
flag_int >>= padding_bits  
flag_bytes = long_to_bytes(flag_int)  
  
print("Recovered Flag:", flag_bytes.decode())
```

CHALLENGE

36 SOLVES

×

Pandak Lam

150

Dato' Maharaja Lela merupakan tokoh penting dalam sejarah Perak yang terkenal dengan perjuangan beliau terhadap penjajahan British. Anda telah menemui sumber sekunder yang telah diolah dipercayai mengisahkan penyebab beliau menentang terhadap British. Pada akhirnya, beliau dijatuhi hukuman gantung gantung sampai mati.

Sumber_Sekunder.txt

3108{k3b4ngk1tanp4hl4w4n}

Submit

Use Rot13 cipher and find flag

SEARCH A TOOL ON dCODE BY KEYWORDS:

e.g. type 'boolean'

BROWSE THE FULL dCODE TOOLS' LIST

ROT-13 CIPHER

+ Add ROT-13 Cipher to your mobile apps!

Results

SNXGBECRARAG...ALN

Faktor penentangan Dato Maharaja Lela Mengambil hak mengutip cukai. 241ulai1875 Birch memaksa Sultan Abdullah

menguruskan cukai dan melantik penghulu. Memperkenalkan Cukai Baru Birch bertindak sesuka hati dengan memperkenalkan cukai baru

Copy

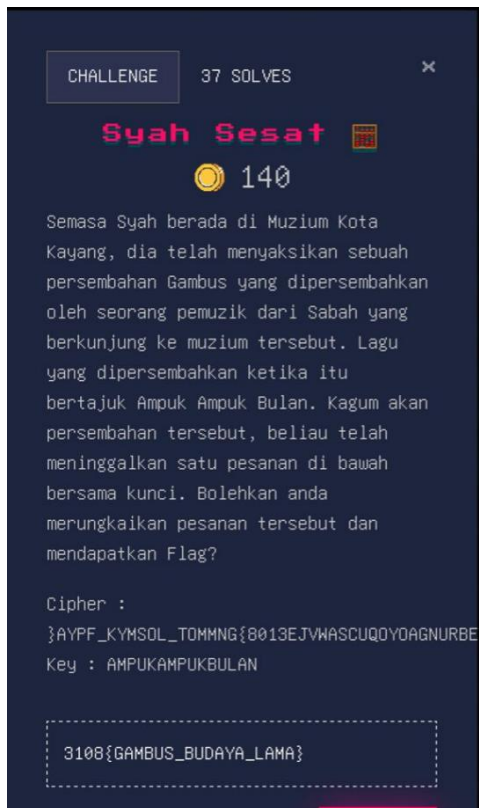
Search with Google

>

an

ermit untuk membalak.

3108k3b4ngk1tanp4hl4w4n Setiap isi rumah perlu membayar 2Dolar sebagai cukai kelamin. Mencabuli Adat Resam Birch dibenci oleh sultan dan pembesar-pembesar Perak apabila mengharamkan sistem perhambaan yang menjadi adat resam Melayu



Use vigenere cipher and found 3108 but in reverse



Use cyberchef to reverse (im using phone)

gchq.github.io

Download CyberChef

Last build: 16 days ago - Version 10 is here! Read about the new featu...

Operations

revers

Reverse

Remove line numbers

Remove Diacritics

ECDSA Signature Conversion

Disassemble x86

Favourites

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Networking

Language

Utils

Date / Time

Extractors

Compression

Hashing

Code tidy

Forensics

Multimedia

Recipe

Reverse

By Character

Input

}AMAL_AYADUB_SUBMAG{8013

24 1

Output

310B{GAMBUS_BUDAYA_LAMA}