

3108 CTF : KEMBARA TUAH 2024

Writeup by Soul





Soul
15th place
4360 points

MALAYSIA

3108

Cordini

Maklum Balas

KELANTAN

Sultan yang Hilang

SELANGOR

Mesej Rahsia

Tanpa Nama 3

Selangorku

PAHANG

Sembunyi

Sembunyi V2

WILAYAH PERSEKUTUAN

Tinggi Mat

Tinggi Lagii

PERLIS

Jalan Jalan Desa

Syah Sesat

MELAKA

Perigi

Pahlawan Lagenda

TERENGGANU

Privacy Matters

Ngaji

SABAH

Cer Cari

Asal Nama Sabah

JOHOR

zZzZz

SARAWAK

Sarawak Kita

KEDAH

Langkawi Di Hati

PULAU PINANG

Bawang

MALAYSIA

3108

CHALLENGE 636 SOLVES X

3108

10

Untuk CTF tahun ini, kami berpendapat bahawa hanya satu soalan akan dikeluarkan.

Kami hanya ingin tahu, Adakah anda sayang negara anda Malaysia?

Jawab Ya jika benar, Tidak jika salah

<https://www.youtube.com/watch?v=oIDeGj83us8>

Flag Submit

For this just answer “ya” or “tidak” .

CORDINI

CHALLENGE 271 SOLVES X

Cordini *

100

Ayuh sertai kami di Discord 3108 CTF:

<https://discord.gg/fqGDsUmE>

Flag Submit

First join the discord server, react at channel get-role and you will get the flag .

Welcome to #MY!

This is the start of the #my channel.

August 22, 2024



n4kh0d4 08/22/2024 1:54 PM
3108{kibarkanlah_jalur_gemilang}

August 30, 2024



n4kh0d4 08/30/2024 12:35 AM

Maklum Balas

CHALLENGE

226 SOLVES



Maklum Balas

200

Sila isi maklum balas bagi membantu menaik taraf CTF 3108 akan datang. Terima kasih.

Flag percuma di akhir maklum balas.

<https://forms.gle/W7HG9ZmKnLnt2RBt6>

Flag

Submit

Just submit the google form and get the flag .

Borang Maklum Balas 3108 CTF 2024

Terima kasih pewira atas maklum balas anda. Semoga bertemu lagi di lain masa.
3108{MalaysiaMadaniJiwaMerdeka}

[Submit another response](#)

KELANTAN

Sultan yang Hilang

The image shows a challenge interface from a CTF competition. At the top left is a 'CHALLENGE' button. To its right, '187 SOLVES' is displayed. On the far right is a close button (an 'X').

The challenge title is 'Sultan yang Hilang' in a stylized font, accompanied by a small globe icon. Below the title is a yellow circular icon with a question mark and the number '100'.

The challenge description reads:

Berikut merupakan senarai pemerintahan Sultan-Sultan Kelantan, yang telah memimpin negeri ini sejak abad ke-18. Setiap Sultan membawa kisah dan peranannya yang tersendiri dalam membentuk sejarah Kelantan. Namun, terdapat Sultan yang hilang dari senarai ini.

A URL is provided below the description:
<https://f2add8dd3a.bahterasiber.my/>

At the bottom left is a 'Flag' input field, and at the bottom right is a red 'Submit' button.

Open the web server .click ctrl + u to view page source .

```

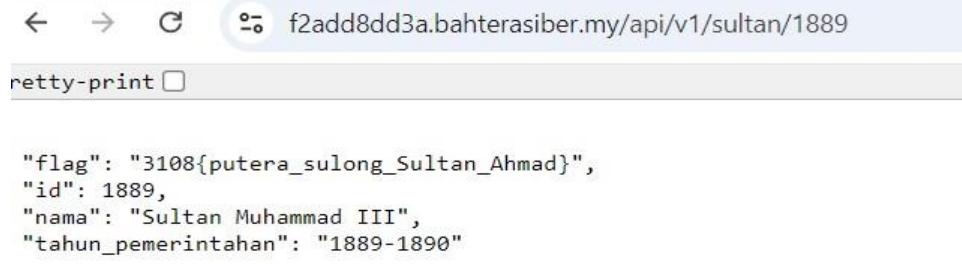
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Senarai Sultan Kelantan</title>
</head>
<body>
    <h1>Senarai Sultan Kelantan</h1>
    <ul id="sultan-list"></ul>

    <script>
        const sultanYears = [1763, 1795, 1800, 1835, 1837, 1886, 1890, 1899, 1920, 1944, 1960, 1979, 2010];

        sultanYears.forEach(year => {
            fetch(`/api/v1/sultan/${year}`)
                .then(response => response.json())
                .then(data => {
                    const list = document.getElementById('sultan-list');
                    const listItem = document.createElement('li');
                    if (data.error) {
                        listItem.textContent = `${data.error}`;
                    } else {
                        listItem.textContent = `${data.nama}`;
                    }
                    list.appendChild(listItem);
                })
                .catch(error => console.error('Error:', error));
        });
    </script>
</body>
</html>

```

Follow the path given api/v1/sultan/year and need to change the year 1 by 1. After doing some research I get the year that was not in source code which is 1889. after you change the year with 1889 you will get the flag .



```

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

```

SELANGOR

Mesej Rahsia



```
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',
flag=(3108,"",p,q,b,p,l,g,l,q,l,v,"",d,g,h,s,v,k,"",l,v,m,l,"")[:-1]
```

They give file.py. I use cyberchef to decode it and get the flag.

Recipe

Substitute

Plaintext: abcdefghijklmnopqrstuvwxyz

Ciphertext: jbacmnipoqrxtzvsuyh...

Ignore case

Input: 3108{pqbpqlglqlv_dghsvk_lvml}

Output: 3108{substitute_cipher_text}

Tanpa Nama 3



They give file python

```
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 00111110 00110110 01010100 00101000 00110101 00101001 01010110 00111010 00100110 00110111 00110101 00111100 00110001 010
xor_str = "01100101"
```

When I analyze the code it didn't print result or output so I put print on the last line and get the flag

3108{S1MPL3_CRPYT0_CHALLENGE} .

SELANGORKU



Go to website and it says 403 forbidden.check inspect element it only accept user-agent:curl .

```
(kali㉿kali)-[~/Downloads/3108CTF/selangor]
└─$ curl https://6654c734cc.bahterasiber.my/
!DOCTYPE html


    
    
    Sejarah Penubuhan Negeri Selangor
    <link rel="stylesheet" href="style.css">


    <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="/kuala_langat.html">Kuala Langat</a></li>
        <li><a href="/kuala_selangor.html">Kuala Selangor</a></li>
        <li><a href="/semantan.html">Semantan</a></li>
        <li><a href="/sabak_bernuar.html">Sabak Bernuar</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>

```

Using curl we get some directory there. After I try I get the flag at directory `hulu_selangor.html` .

```
(kali㉿kali)-[~/Downloads/3108CTF/selangor]
└─$ 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">

<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>

</html>
```

PAHANG

Sembunyi

CHALLENGE 147 SOLVES

Sembunyi *

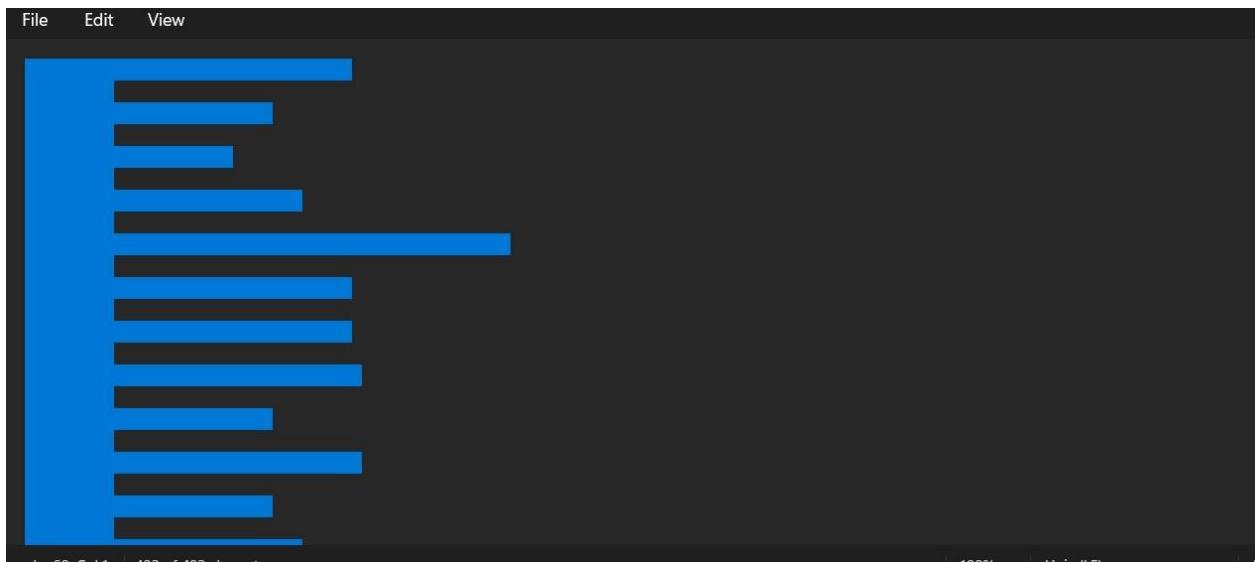
100

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](#)

Given the file .txt but when I open it its nothing but when I ctrl a they look like something there .



So I use white space decoder and get the flag .

code

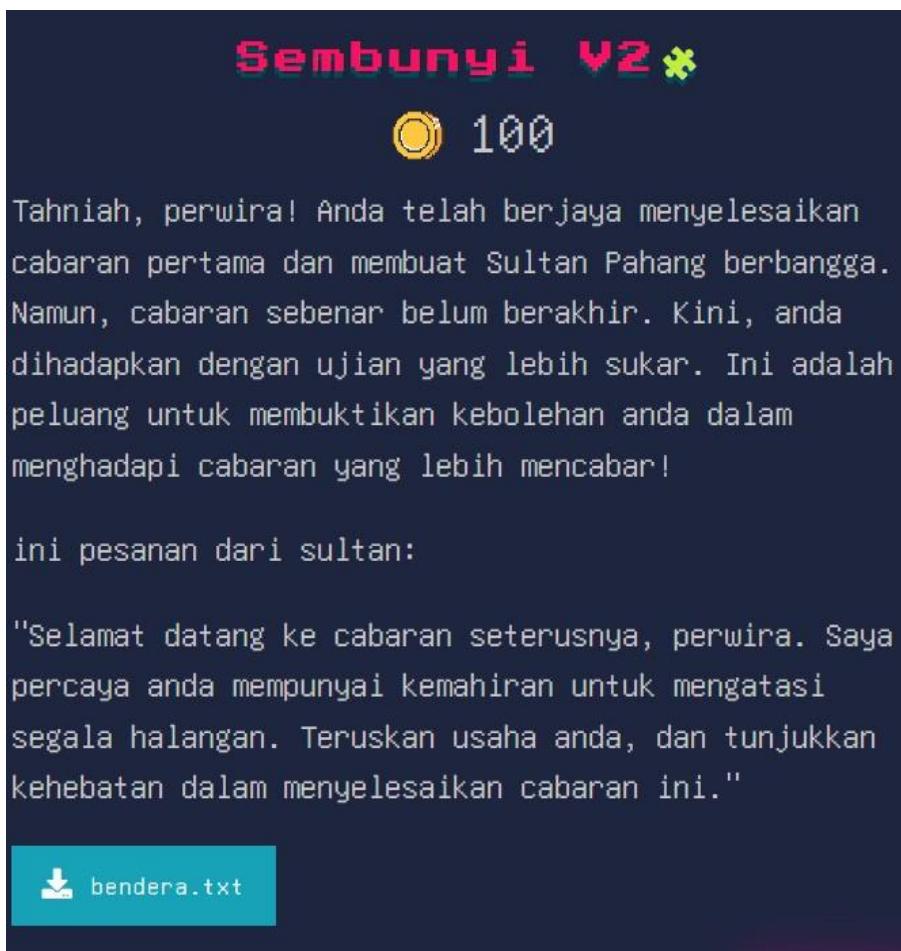
input

Timeout(5s)

output

```
3108{S3jarah_Ters3mbunyi_P4hang}
```

Sembunyi v2



Same as sembunyi but this I cannot use the decoder I use before put it on gpt with a correct prompt it will give code here .

```
File Actions Edit View Help
GNU nano 8.1
file = open("bendera.txt", "r").read()
result = ""
for char in file:
    if ord(char) == 32:
        result += "0"
    else:
        result += "1"
print(result)
```

And print output like this

```
01101101001100101101101101011010110111011010000101111010011100000  
1110101011001000111010001100100110111011000010110000101101011001110  
111101101000001011101100110001101111100101000001110111011010010111001101  
1011010011100001110011011000010010110110010101111001000000001011001000  
1010101110010011110101011110101111010010000001010111100111101011111010  
110011011110101
```

go to cipher identifier to decode it and get the flag .

```
⚠️ Output limited to printable characters (other chars replaced by ⚡)  
↑↓ ↑↓  
BIN 3108{putih_dan_hitam_dalam_negeri_paha  
/8 ng}
```

WILAYAH PERSEKETUAN

Tinggi mat



Extract the file using command unrar x filename .

```

└─(kali㉿kali)-[~/Downloads/3108CTF/_WMT.rar.extracted]
└─$ ls
43.rar flag2.rar flag2.txt WarisanMerdekaTower.png _WarisanMerdekaTower.png.extracted

└─(kali㉿kali)-[~/Downloads/3108CTF/_WMT.rar.extracted]
└─$ cat flag2.txt
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!
└─(kali㉿kali)-[~/Downloads/3108CTF/_WMT.rar.extracted]
└─$ 

```

You can see many file there but when I try to open file flag2.txt it ask for password ,Based on warisanmerdekatower.png I try to submit the password MERDEKA118

but it didn't give real flag just a normal text but using steg online I get half of the flag .

_On3_1n_M4l4ys14!}



And I think another half in the picture warisanmerdekatower.png so I use zsteg to see if have hidden message there .

```

└─(kali㉿kali)-[~/Downloads/3108CTF/_WMT.rar.extracted]
└─$ zsteg WarisanMerdekaTower.png
meta Description .. text: "Bangunan kedua tertinggi di dunia, juga dikenali sebagai MERDEKA118."
b1,rgb,lsb,xy .. text: "3108{th3_t4ll3st"
b2,g,msb,xy .. text: "QD@PUOP"
b2,b,msb,xy .. text: "@t@PQUTP"
b2,rgba,lsb,xy .. text: "{+WGG{k73#7"
b2,abgr,msb,xy .. text: "SSGCCSGSS"
b3,abgr,msb,xy .. text: "vhWtDGtL_"
b4,r,lsb,xy .. text: "Gd$B$ $,"
b4,r,msb,xy .. text: "7Siwsupsp"
b4,g,lsb,xy .. text: "b$D\"$D \""
b4,g,msb,xy .. text: "p3w7UQQS"
b4,b,lsb,xy .. text: "2%U\"TES11"
b4,b,msb,xy .. text: "wDDD\"$B53UU3ws"
b4,rgb,msb,xy .. text: "6'5T#5RCQ4%$4"
b4,bgr,msb,xy .. text: "76%$4%SRA5T#5"
b4,rgba,lsb,xy .. text: "N/n/L/L/n/n/n0"
b4,abgr,msb,xy .. text: "c?%?E?%?%_A_C_#_C"

```

And I get the full after combined it and get the flag 3108{th3_t4ll3st_0n3_1n_M4l4ys14!} Tinggi Lagii .

Tinggi Lagii

◎ 100

Bangunan Tertinggi Di Malaysia yang tidak terbina.

Tahu tak kat mana?

Format Flag: 3108{latitude, longitude}

Jawapan dalam dua titik perpuluhan

Contoh: 1.23

 Bangunan.jpg

For this just use gpt



what is the latitude and longitude



The latitude and longitude coordinates for the location in the image, rounded to two decimal places, are:

[Copy code](#)

{3.15, 101.71}

These coordinates correspond to the Merdeka 118 building in Kuala Lumpur, Malaysia. Let me know if you need any further assistance!

··· [Copy](#) [Share](#) [Upvote](#) [Downvote](#) [Flag](#)

As a format flag you will get the flag 3108{3.15, 101.71}

Perlis

Jalan Jalan Desa



Open the file and get the picture like this .



As the question give hint that syah left his review just search in google like this And directly get the flag.

"kota kayang museum" "3108"

All Images Maps Videos News Web Shopping More Tools

WordPress.com
<https://thriftytraveller.wordpress.com> › 2012/04/09 › kot... :

Kota Kayang Museum, Perlis - The Thrifty Traveller
9 Apr 2012 — **Kota Kayang Museum**, Perlis. GRAND TOUR – continued. Regular readers ... 3108{Muzium_Bersejarah_Perlis}. Reply. Leave a comment Cancel reply.

google.com.my

Syah Sesat

CHALLENGE 165 SOLVES X

Syah Sesat ⓘ

100

Semasa Syah berada di Muzium Kota Kayang, dia telah menyaksikan sebuah persembahan Gambus yang dipersembahkan oleh seorang pemuzik dari Sabah yang berkunjung ke muzium tersebut. Lagu yang dipersembahkan ketika itu bertajuk Ampuk Ampuk Bulan. Kagum akan persembahan tersebut, beliau telah meninggalkan satu pesanan di bawah bersama kunci. Bolehkan anda merungkaikan pesanan tersebut dan mendapatkan Flag?

Cipher :

3AYPF_KYMSOL_TOMMNG{8013EJVWASCUQOYDAGNURBETMYUIBMTNHGMALKGZTXUBDP

Key : AMPUKAMPUKBULAN



Copy the cipher use cipher Identifier and you will get the flag it was vigene cipher .

Arrange from back and get the flag 3108{GAMBUS_BUDAYA_LAMA}

MELAKA

Perigi

Extract file flag.rar but it ask for password.and the question actually give a hint siapa racun kali kedua after doing research I find that the Belanda was do that so I input the password Belanda and directly get the flag .

CHALLENGE

133 SOLVES



Perigi 🔍

🟡 100

Perigi ni selalu kena racun... Sampai saya lupa negara mana yang racun perigi ni untuk kali kedua...

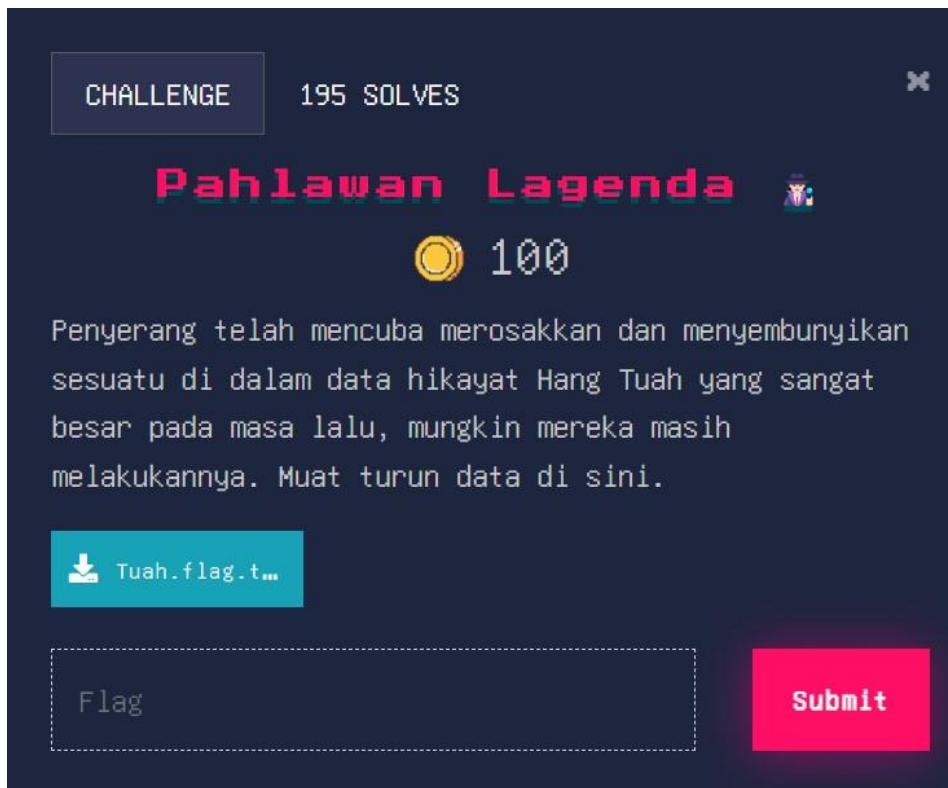
flag.rar

Flag

Submit

```
└─(kali㉿kali)-[~/Downloads]
$ cat flag.txt
3108{th3_k1ngs_w3ll_st4ys_0n}
```

Pahlawan Legenda

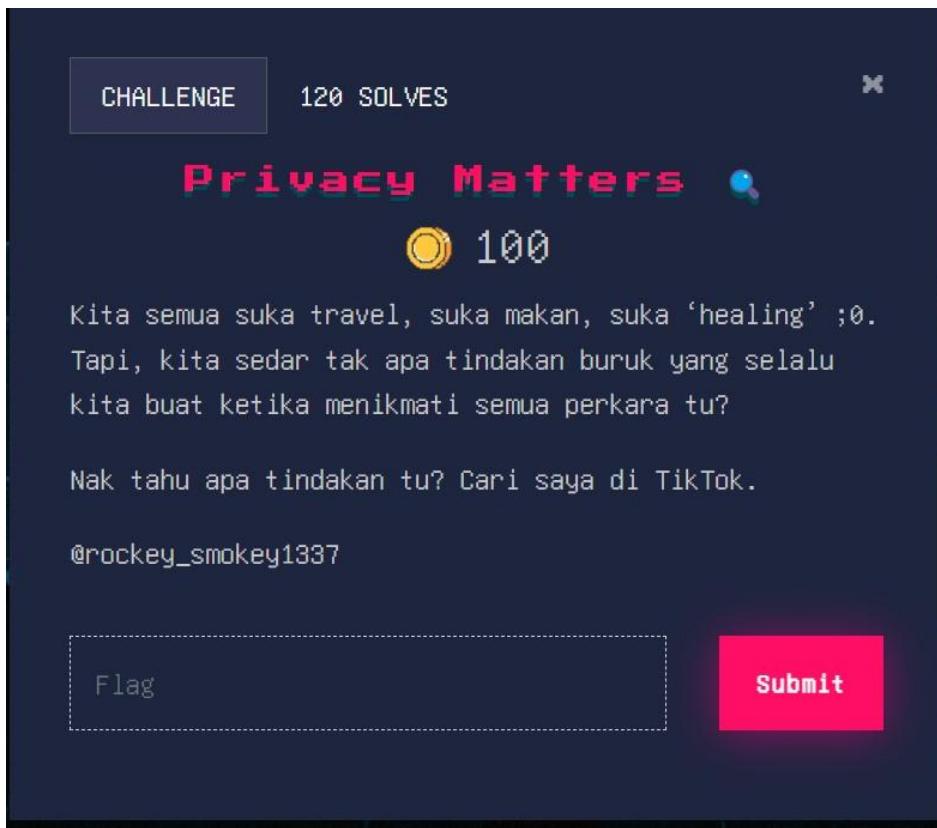


Download file tuah flag .txt using ctrl f and I find the flag .

```
Kami nak makan nasi ka • rahsia (1).txt rahsia (1).txt Untitled Tuah.flag.txt
File Edit View
The ambiguity and variability in the portrayal of the monarch are conditioned not so much by the author's style, as by the unjustified to expect this character, an immobile module of the plot, to possess strict integrity and consistency, as it is to try to construct a consistent picture of the monarch on the basis of different stories in the 'Mirrors', which aim at resolving a specific, unconnected problem in each instance. Any reasonable and justified actions taken by the monarch in the hikayat not only point to his greatness, but also enable Hang Tuah to display his courage and statesmanship. Conversely, his weaknesses and whims make it possible to represent 'in persons' such important notions as the need for a monarch to listen to his wise counsellors, to avoid rashness and to turn a deaf ear to slander. Even more importantly, these weaknesses help to test a subject's loyalty to his sovereign. Were it not for Hang Tuah's willingness to carry out any assignment for his sovereign, both on the latter's orders and voluntarily (and irrespective of whether it involves a matter of importance to the state or such absurd requests as to pick some fruits from a palm tree about to collapse, to rescue a horse from a cesspit, or to bring news from the next world), he would not have become a living embodiment of this loyalty, implicit and absolute, precisely because only then can such loyalty, according to medieval Malay ideas, ensure peace, order and prosperity for the whole state. 3108{gr3p_15_@w3s0m3_14ks4m4n4} As for the consequences of
```

TERENGGANU

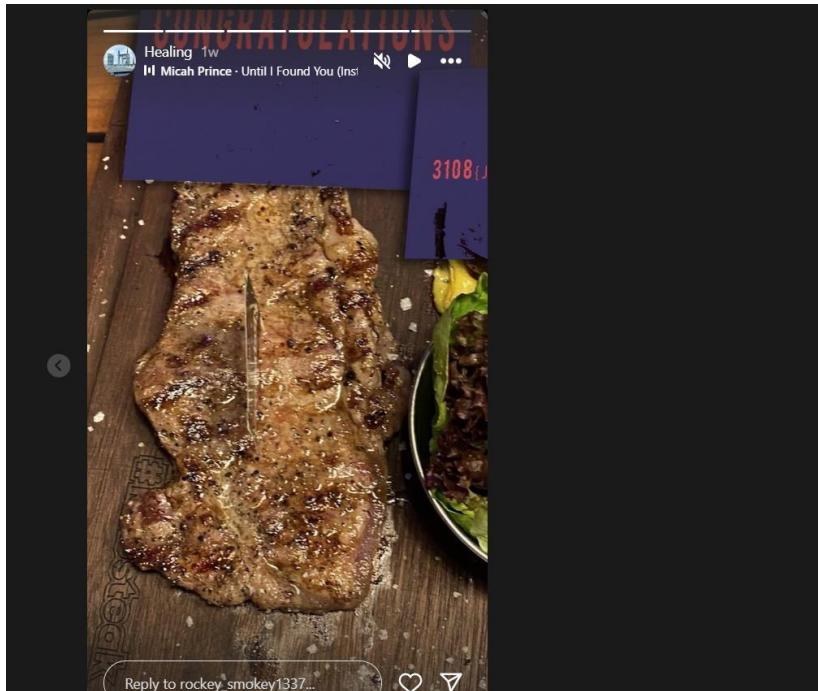
Privacy Matters



Given the username of someone @rockey_smokey1337. when I check repost and read the comment I find clue that rockey also have ig account.

The screenshot shows a TikTok post by user **p3tualang1337**. The post has 6 likes, 4 comments, and 0 saves. It includes a link: <https://www.tiktok.com/@p3tualang1337/photo/7406...>. The comments section shows:

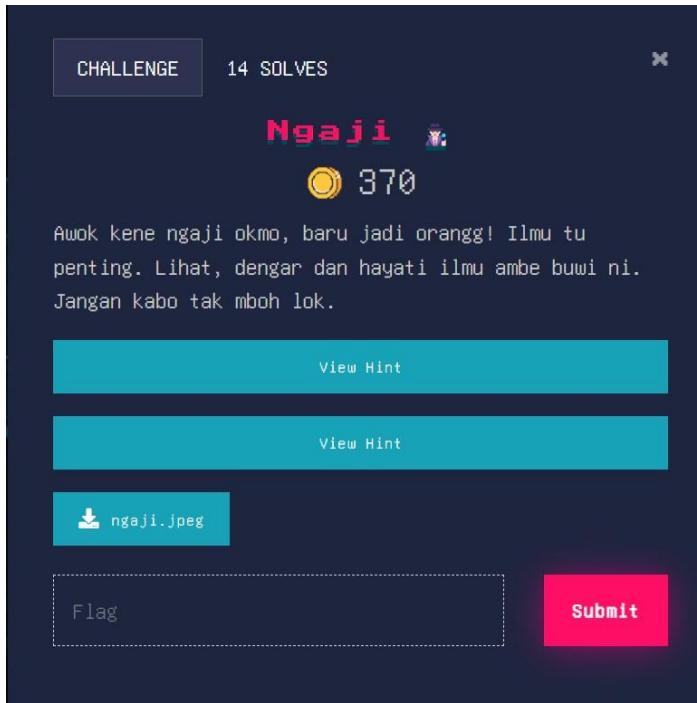
- rockey_smoke1337** Boek bro, nanti post kat ig jgn lupa tag aku @rockey_smoke1337 8-23 Reply
- p3tualang · Creator** baik bosku 8-23 Reply
- zeqzoz** comment tanda hadir part 2 3dano... Reply



But the problem is the highlight not giving full picture. based on the information I try to search steak in Terengganu and found kbbsteak near the bridge and check for the review I get the full picture.



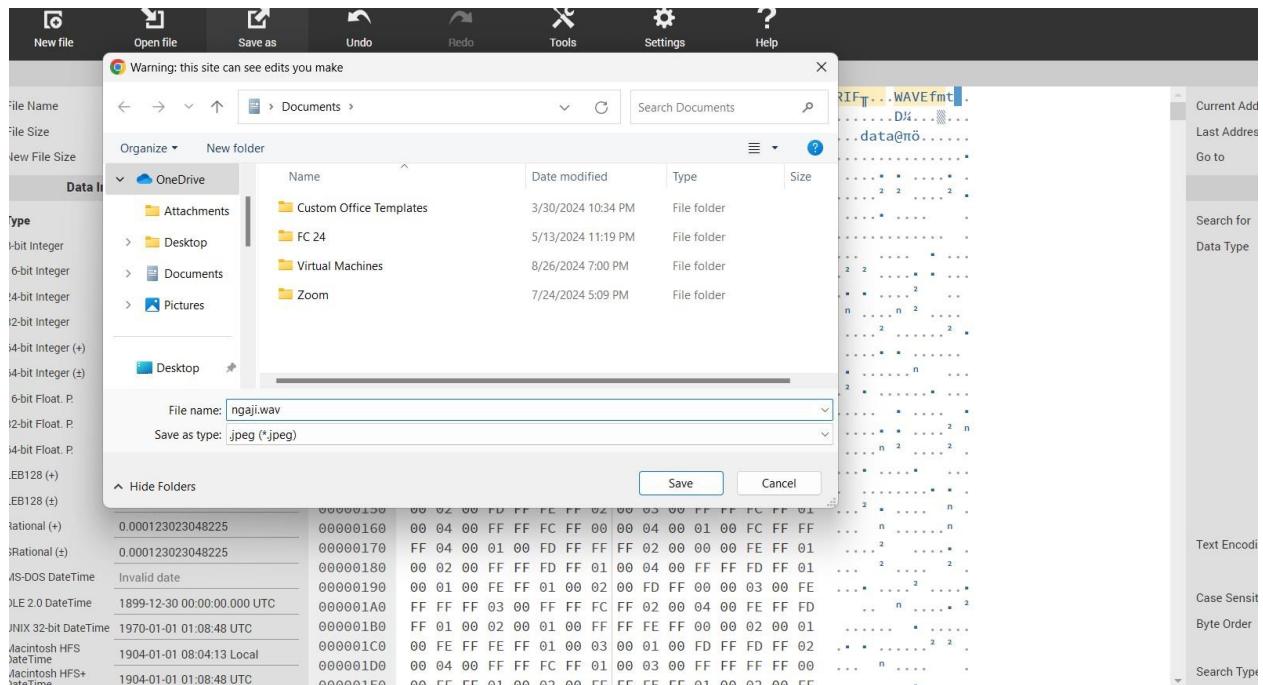
Ngaji



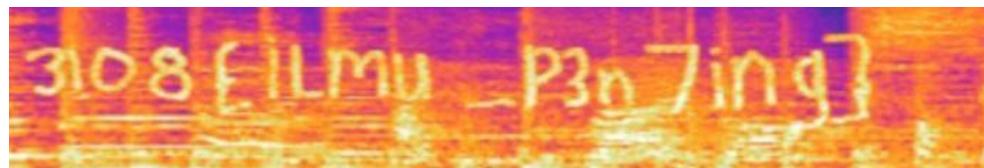
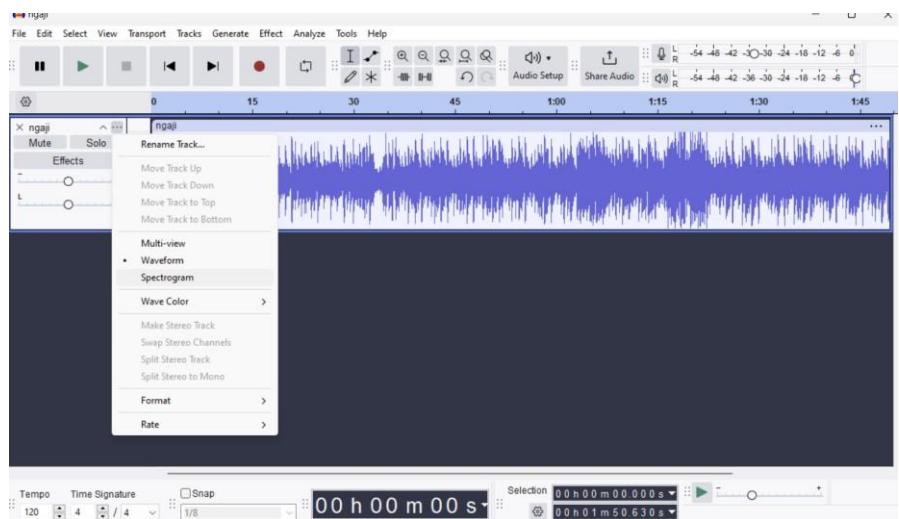
They give 2 hint tuan hamba perlu dengar bukan lihat .I find a jpeg file but cannot open but its corrupted when I check the file hex I found ...fmt after do some research that fmt was associated with wav.modify the hex with this 00000000 52 49 46 46 D2 04 00 00 57 41 56 45 66 6D 74 20 and save as ngaji.wav .

The screenshot shows the Immunity Debugger interface with the assembly and registers panes visible. The assembly pane displays the modified hex dump of the file, which includes the string "...fmt" at address 0x00000000. The registers pane shows various CPU registers like EIP, ECX, and ESP.

Type	Unsigned (+)	Signed (±)
8-bit Integer	255	-1
16-bit Integer	55551	-9985
24-bit Integer	16767231	-9985
32-bit Integer	4009744639	-285222657
64-bit Integer (+)	41908499587782911	
64-bit Integer (±)	41908499587782911	
16-bit Float P	-159.875	
32-bit Float P	-3.9590505e+28	
64-bit Float P	7.436695160365996e-306	
LEB128 (+)	91366535195775	
LEB128 (±)	91366535195775	
Rational (+)	410.936299485	
SRational (±)	-29.2308747188	
MS-DOS Date/Time	Invalid date	
OLE 2.0 Date/Time	1899-12-30 00:00:00.000 UTC	
UNIX 32-bit Date/Time	2097-01-23 01:57:19 UTC	
Macintosh HFS Date/Time	2031-01-23 09:57:19 Local	
Macintosh HFS+ Date/Time	2031-01-23 01:57:19 UTC	
UTF-8 Character	Invalid data	



After that open file in audacity change to spectrogram and check for the diagram we found the flag .



SABAH

Cer Cari

CHALLENGE 363 SOLVES X

Cer Cari

100

Setiap negeri mempunyai tarikh penting. CerCari Tarikh penting bagi negeri Sabah.

 CerCari

Flag

Submit



After open the file we can see that theres many (sabah and year) and we don't know which one is the answer.goggle it Tarikh penting sabah and found 1963.

Tarikh penting bagi negeri Sabah.

tarikh 31 Ogos itu diputuskan oleh Majlis Undangan Borneo Utara pada 8 Ogos 1963 sebagai tarikh kemerdekaan Sabah yang tetap dijadikan kenyataan walaupun Malaysia tidak dapat dibentuk pada tarikh sama.

Wikipedia
https://ms.wikipedia.org › wiki › Hari_Pemerintahan_Se... :
Hari Pemerintahan Sendiri Borneo Utara

And get the flag which contain year 1963 .

Asal nama sabah

CHALLENGE 32 SOLVES

Asal Nama Sabah

Setiap negeri mempunyai asal nama negeri tersebut. Begitu juga dengan negeri Sabah. Sabah juga mempunyai nama asal negeri tersebut yang popular di kalangan masyarakat tempatan.

Asal_Nama_S...

Flag Submit

Since it was exe file I decompile and open it on ghidra to check the function .

```
1 Decompile: check_flag - (Asal_Nama_Sabah.exe)
2 void check_flag(char *param_1)
3 {
4     int iVar1;
5     size_t sVar2;
6     undefined6 local_46;
7     undefined2 uStack_40;
8     undefined6 uStack_3e;
9     undefined8 local_38;
10    undefined8 local_30;
11    undefined8 local_28;
12    undefined5 local_20;
13    undefined3 uStack_1b;
14    undefined5 uStack_18;
15    int local_10;
16    uint local_c;
17
18    local_38 = 0x3935643530356435;
19    local_30 = 0x6532353530326131;
20    local_28 = 0x3233643339323734;
21    local_20 = 0x3365336335;
22    uStack_1b = 0x39353L;
23    uStack_18 = 0x633L3932;
24    local_46 = 0x7361616d616e;
25    uStack_40 = 0x6c61;
26    uStack_3e = 0x6861626173;
27    sVar2 = strlen((char *)&local_46);
28    local_10 = (int)sVar2;
29    for (local_c = 0; local_c < 0x25; local_c = local_c + 1) {
30        *(byte *)((long)&local_38 + (long)(int)local_c) =
31            *(byte *)((long)&local_38 + (long)(int)local_c) ^
32            *(byte *)((long)&local_46 + (long)((int)local_c % (int)sVar2));
33    }
34
35    iVar1 = strcmp(param_1, (char *)&local_38);
36    if (iVar1 == 0) {
37        printf("Correct! The flag is: %s\n", &local_38);
38    }
}
```

I using gpt to help me analyze the code and it give this .

Based on the decompiled code snippet you provided, here's an analysis of what the code is doing:

Code Breakdown:

1. Variable Initialization:

- `local_38`, `local_30`, `local_28`, etc., are initialized with large hexadecimal values. These variables will likely undergo transformation during the execution of the function.

2. String Length Calculation:

- `sVar2 = strlen((char *)&local_46);` calculates the length of the string starting at `local_46`.

3. Loop:

- The loop runs from `local_c = 0` to `local_c < 0x25` (which is 37 in decimal).
- Inside the loop, each byte of `local_38` is transformed using a bitwise XOR operation with values derived from `local_38` and `local_46`.

It say the match value of local 38 and when I run the exe I get the flag .

- This loop likely modifies the contents of `'local_38'`, turning it into a string that should match the input flag.

4. String Comparison:

- After the loop, the function compares the transformed `local_38` with the input string (`param_1`) using `strcmp`.
 - If the strings match (`iVar1 == 0`), the function prints "Correct! The flag is: %s\n", where `%s` is the content of `local_38`.

Conclusion:

- The input that would make `strcmp` return 0 (indicating the strings match) must be the one that, after the transformation process, equals the value in `local_38`.

Given the decompilation and analysis, the input for this function to produce the correct output is:

Input: "asalnamasabah"

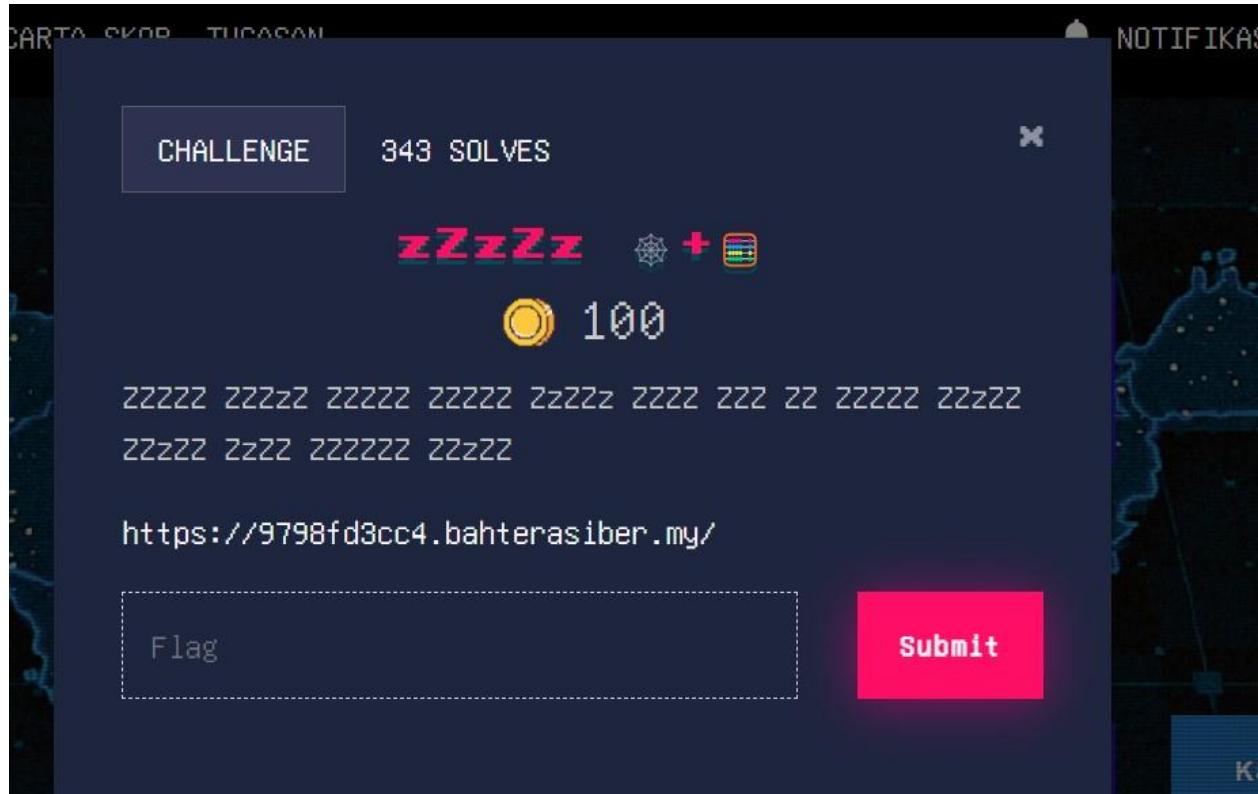
This is the string that, when processed through the loop, matches the expected value of `local_38`.

• • ◻ ◻ ▲ ▾

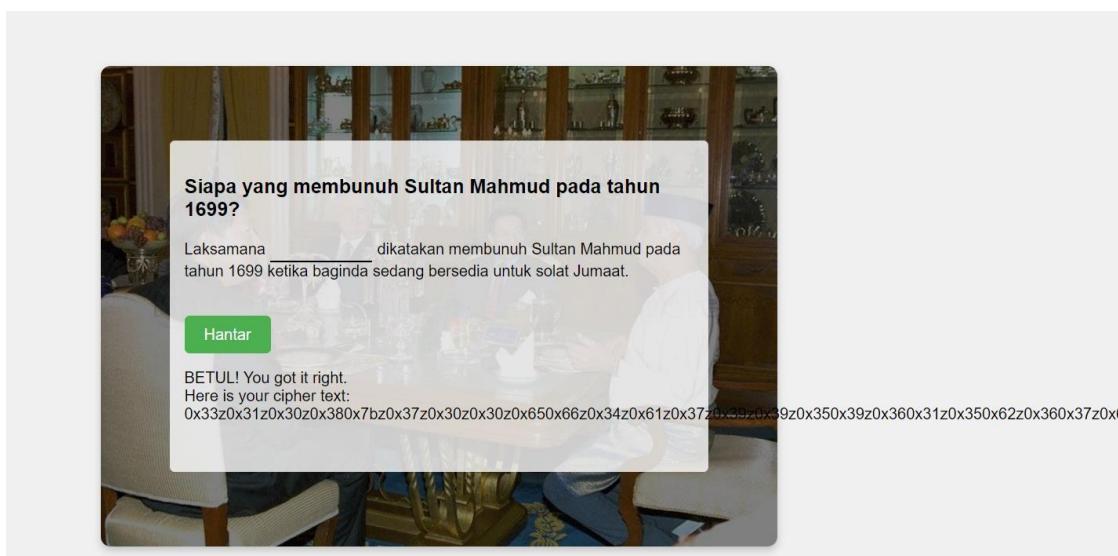
The flag is 3108{S4B4H_S4PP4H}

JOHOR

zZzZz



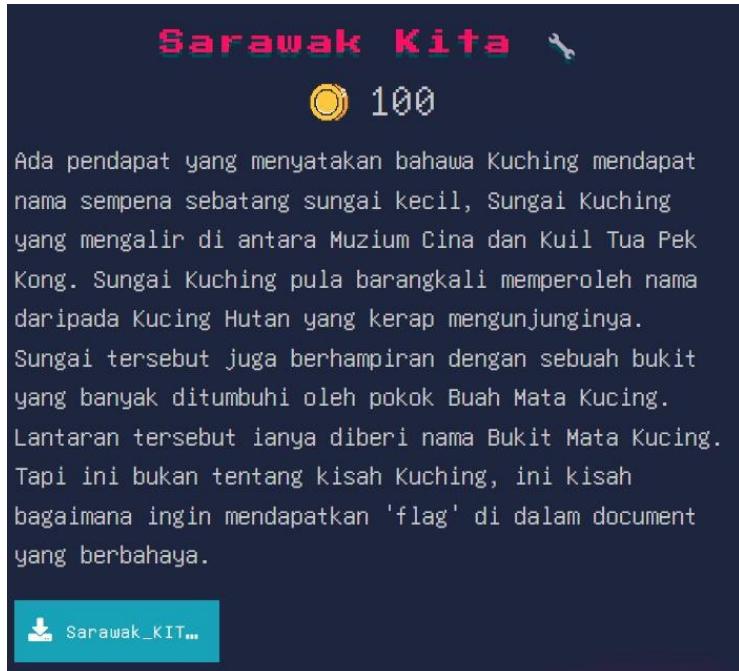
Go to website page and answer the question which the answer is Bentan .



Decode this using hex and you get the flag .

SARAWAK

Sarawak kita



Since the file .bin use binwalk -e to extract it .

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	Zip archive data, at least v2.0 to extract, compressed size: 422, uncompressed size: 1503, name: [Content_Types].xml
991	0x3DF	Zip archive data, at least v2.0 to extract, compressed size: 243, uncompressed size: 590, name: _rels/.rels
1795	0x703	Zip archive data, at least v2.0 to extract, compressed size: 310, uncompressed size: 1071, name: word/_rels/document.xml.rels
2427	0x97B	Zip archive data, at least v2.0 to extract, compressed size: 2236, uncompressed size: 19007, name: word/document.xml
4710	0x1266	Zip archive data, at least v2.0 to extract, compressed size: 3402, uncompressed size: 8704, name: word/vbaProject.bin
8161	0x1FE1	Zip archive data, at least v1.0 to extract, compressed size: 785631, uncompressed size: 785631, name: word/media/image1.png
793843	0xC1CF3	Zip archive data, at least v2.0 to extract, compressed size: 192, uncompressed size: 277, name: word/_rels/vbaProject.bin.rels
794095	0xC1DEF	Zip archive data, at least v2.0 to extract, compressed size: 1686, uncompressed size: 6992, name: word/theme/theme1.xml
795832	0xC24B8	Zip archive data, at least v2.0 to extract, compressed size: 376, uncompressed size: 817, name: word/vbaData.xml
796254	0xC265E	Zip archive data, at least v2.0 to extract, compressed size: 734, uncompressed size: 1662, name: word/settings.xml
797035	0xC296B	Zip archive data, at least v2.0 to extract, compressed size: 378, uncompressed size: 716, name: docProps/app.xml
797723	0xC2C1B	Zip archive data, at least v2.0 to extract, compressed size: 1966, uncompressed size: 15628, name: word/styles.xml
799734	0xC33F6	Zip archive data, at least v2.0 to extract, compressed size: 327, uncompressed size: 637, name: docProps/core.xml
800372	0xC3674	Zip archive data, at least v2.0 to extract, compressed size: 444, uncompressed size: 1312, name: word/fontTable.xml
800864	0xC3860	Zip archive data, at least v2.0 to extract, compressed size: 187, uncompressed size: 260, name: word/webSettings.xml
802076	0xC3D1C	End of Zip archive, footer length: 22

I reviewing all the contain in the file until I found something interesting in vbaproject.bin .

```
793843 0xC1CF3 Zip archive data, at least v2.0 to extract, compressed size: 192, uncompressed size: 277, name: word/_rels/vbaProject.bin.rels
794095 0xC1DEF Zip archive data, at least v2.0 to extract, compressed size: 1686, uncompressed size: 6992, name: word/theme/theme1.xml
795832 0xC24B8 Zip archive data, at least v2.0 to extract, compressed size: 376, uncompressed size: 817, name: word/vbaData.xml
796254 0xC265E Zip archive data, at least v2.0 to extract, compressed size: 734, uncompressed size: 1662, name: word/settings.xml
797035 0xC296B Zip archive data, at least v2.0 to extract, compressed size: 378, uncompressed size: 716, name: docProps/app.xml
797723 0xC2C1B Zip archive data, at least v2.0 to extract, compressed size: 1966, uncompressed size: 15628, name: word/styles.xml
799734 0xC33F6 Zip archive data, at least v2.0 to extract, compressed size: 327, uncompressed size: 637, name: docProps/core.xml
800372 0xC3674 Zip archive data, at least v2.0 to extract, compressed size: 444, uncompressed size: 1312, name: word/fontTable.xml
800864 0xC3860 Zip archive data, at least v2.0 to extract, compressed size: 187, uncompressed size: 260, name: word/webSettings.xml
802076 0xC3D1C End of Zip archive, footer length: 22

[(kali㉿kali)-[~/Downloads/skibidi]
$ ls
Sarawak_KITA.doc.bin _Sarawak_KITA.doc.bin.extracted

[(kali㉿kali)-[~/Downloads/skibidi]
$ cd _Sarawak_KITA.doc.bin.extracted

[(kali㉿kali)-[~/Downloads/skibidi]/_Sarawak_KITA.doc.bin.extracted]
$ ls
*.zip '[Content_Types].xml' docProps _rels word

[(kali㉿kali)-[~/Downloads/skibidi]/_Sarawak_KITA.doc.bin.extracted]
$ cd word

[(kali㉿kali)-[~/Downloads/skibidi]/_Sarawak_KITA.doc.bin.extracted/word]
$ ls
document.xml fontTable.xml media _rels settings.xml styles.xml theme vbaData.xml vbaProject.bin webSettings.xml
[(kali㉿kali)-[~/Downloads/skibidi]/_Sarawak_KITA.doc.bin.extracted/word]
$ ]
```

Using strings I found base 64 after file calc.exe .

```
[(kali㉿kali)-[~/Downloads/skibidi]/_Sarawak_KITA.doc.bin.extracted/word]
$ strings vbaProject.bin
ShellExecuteA
?LB!
Open
calc.exe
MwAxADA0AB7AEsAdQBjAGgAMQBuAGcAXwAxAGIAAdQBFAE4AMwBnADMAcgAxAF8AUwA0AHIANAB3ADQAwB9AA=""'
ent.Do
Attribut
e VB_Nam
e = "Thi
sDocumen
1Normal
VGloba!
Spac
Crea
tabl
Pre decla
BExp
Temp
lateDeri
$Custom
10pt
.lici
H Func
ShellEx
Lib "
32.dll
" Alias
A" (-
ByVa
l hwnd A
s Long,
lpOpera
Paramters
Direct
Show
Dim commband
AxADA0A
B7AEsAdQ
BjAGgAMQ
BuAGcAX
fAE4A
MwBnADM
```

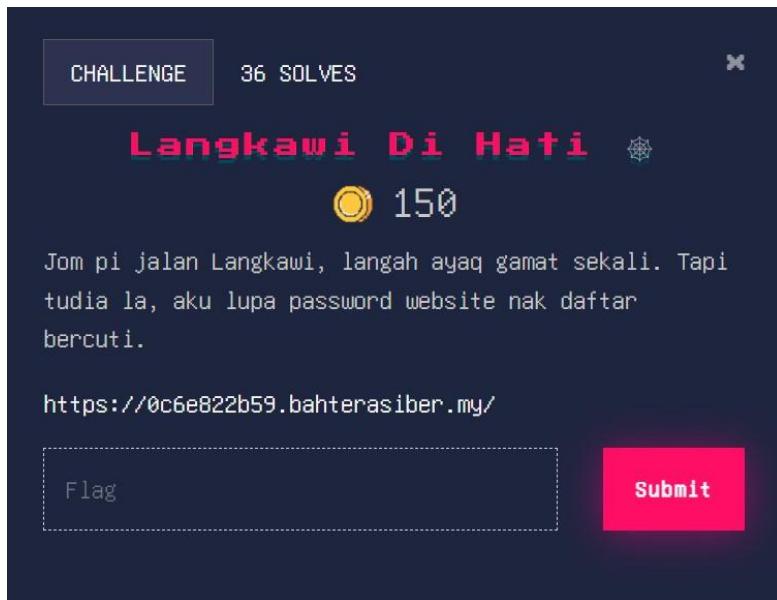
I try to decode it it was base 64 and I get the flag but need to arrange it first.

```
MwAxADAAOAB7AEsAdQBjAGgAMQBuAGcAXwAxAGIAAdQBFAE4AMwBnADMAcgAxAF8AUwA0AHIANAB3ADQaawB9AA=
```

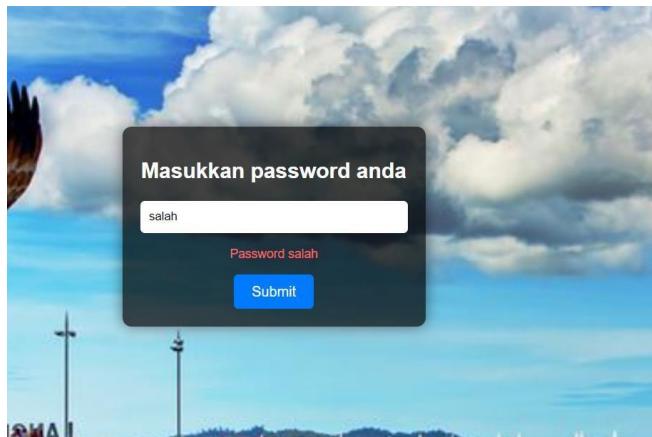
A screenshot of a terminal window. At the top, there's a status bar with 'abc 88' and a file count of '1'. On the right, there are icons for 'Raw Bytes' and 'LF'. Below the status bar, the word 'Output' is centered. The main area shows the decoded base64 string: '3NUL1NUL0NUL8NUL{NULKNUlUNULCNUlhNUL1NULnNULgNUL_ _NUL1NULbNULU_ _NULNNUl3NULgNUL3NULrNUL1NUL_ _NULsNUL4NULrNUL4NULWNUl4NULkNUL}NUL'. The text is mostly black with some red and white highlights.

KEDAH

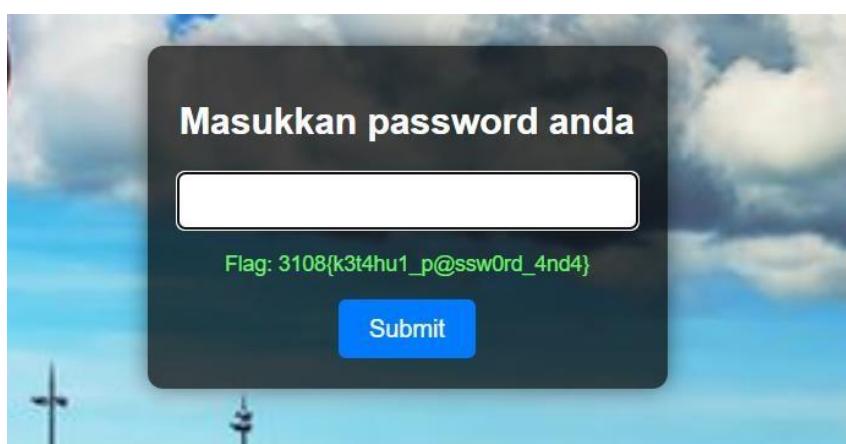
Langkawi di Hati



Open the web page and just follow what the web page say



Do it until you reach $10 + 9$ equal 21 and get the flag

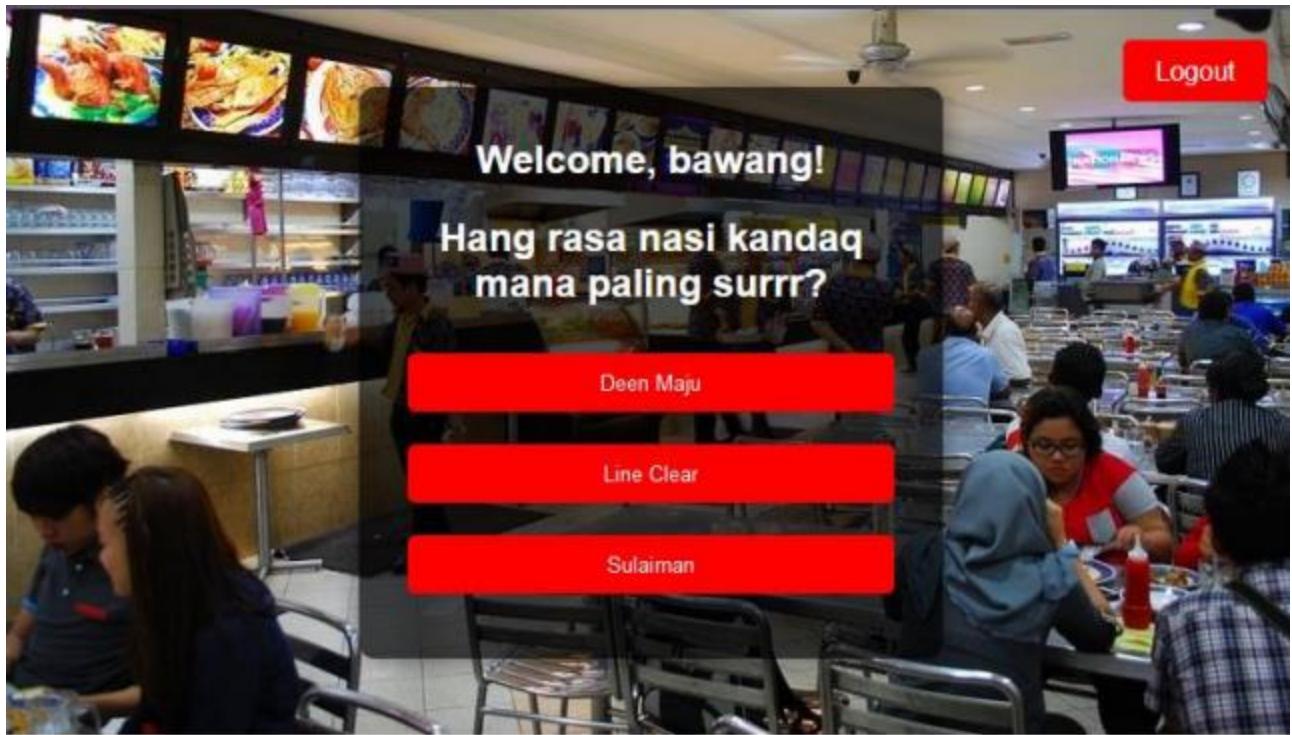


PULAU PINANG

Bawang

The screenshot shows a challenge interface. At the top left is a button labeled "CHALLENGE". To its right is the text "89 SOLVES" and a close button (an "X"). Below this is the challenge title "Bawang" in a large, stylized font, followed by a gear icon and a plus sign. A circular progress bar icon with the number "100" is shown below the title. The main text of the challenge is in Indonesian: "Kami nak makan nasi kandaq ja, member kami bagi natang ni, nak buat apa tak tau? Dia kata cari kat bawang?". Below the text is a long string of characters: "tmdj15kyfzimrsrkkjisxybwb7664epxizxfz6hbivkg6k4a3x2svrad". At the bottom left is a dashed-line text input field labeled "Flag". At the bottom right is a solid pink "Submit" button.

Copy the text open it on tor browser login as bawang and password membawangjekeje.the password from base 64 I decode it and get membawangjekeje. It wil the web page like this.search one by 1 review and will get the flag on nasi kandar line clear.



After do osint I found the flag

Restoran Nasi Kandar Line Clear
Beside 161 & 177 Penang Road, George Town, 10000 George Town, Pulau Pinang, Malaysia

4.0 ★★★★☆ 5,201 reviews

Dine in | Lunch

Ajai 1 review · 1 photo

★★★★☆ a week ago NEW

Look for the flag my friend XD, but repentance is good, I don't want it.
3108 CTF

Food: 5/5 | Service: 5/5 | Atmosphere: 5/5

Translated by Google See original (Malay)

padvisor.com.my > Restaurant_Review-g2...



