NETSA SKILL CHALLENGE CTF

24 MAY 2025

Writeup by: Triple A Battery

Team members:

1. Ammar Saifuddin
2. Aida Sakinah
3. Eusoff Aminurrashid

Contents

Steganography

Welcome to CTF


```
# Function to extract and decode message from a specific bit position in the red channel

def extract_message_from_bit(bit_position):
    bits = []
    for pixel in img.getdata():
        red = pixel[0]
        bit = (red >> bit_position) & 1
        bits.append(str(bit))

    # Convert bits to characters
    message = ''
    for i in range(0, len(bits), 8):
        byte = bits[i:i+8]
        if len(byte) < 8:
            break
        char = chr(int(''.join(byte), 2))
        message += char

    return message

# Try bits 1, 2, and 3 of red channel
messages = {bit: extract_message_from_bit(bit)[:500] for bit in range(1, 4)}
messages
```

Result

```
{1:
'netsa{Fl@g!sHidd3n}\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
```

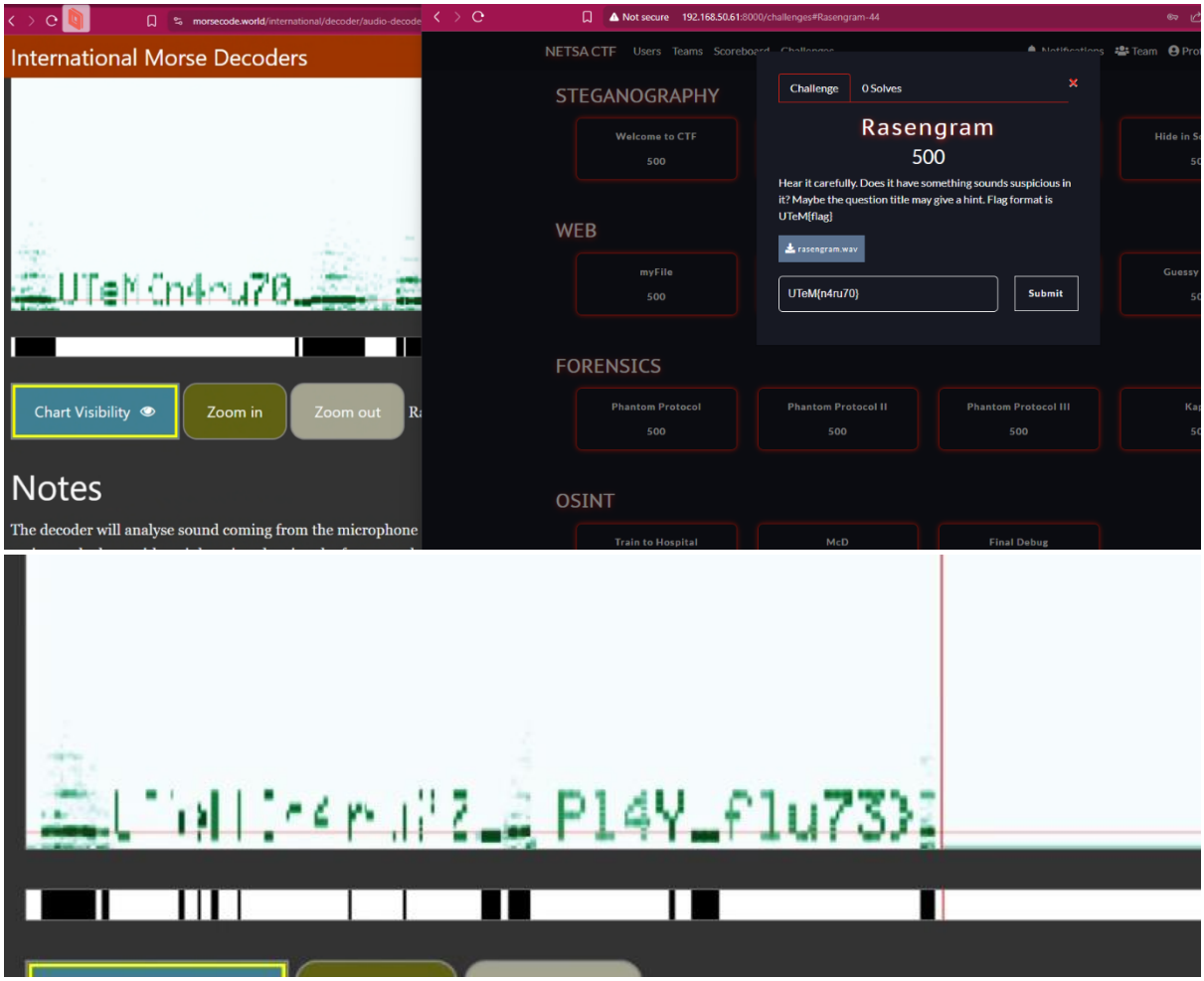
```
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
';
```

The message hidden in the second least significant bit (bit 1) of the red channel is:

Flag: netsa{Fl@g!sHidd3n}

Rasengram

(epic Naruto flute song with morse code)



Song is around 1 minutes 30 seconds. Listen or look at the audio wave to determine where each morse code starts and end. In this audio, there is 2 parts.

Put the audio file in morse decoder and it will show in the chart.

Flag: UTeM{n4ru70_Pl4Y_flu7e}

Cryptography

Baby RSA

Baby RSA

175

escription: We've implemented a secure communication system using RSA encryption, but something seems off about the size of our encryption key. Can you help us recover the original message from the ciphertext?

You are given the following RSA parameters:

n(the modulus): 1057169

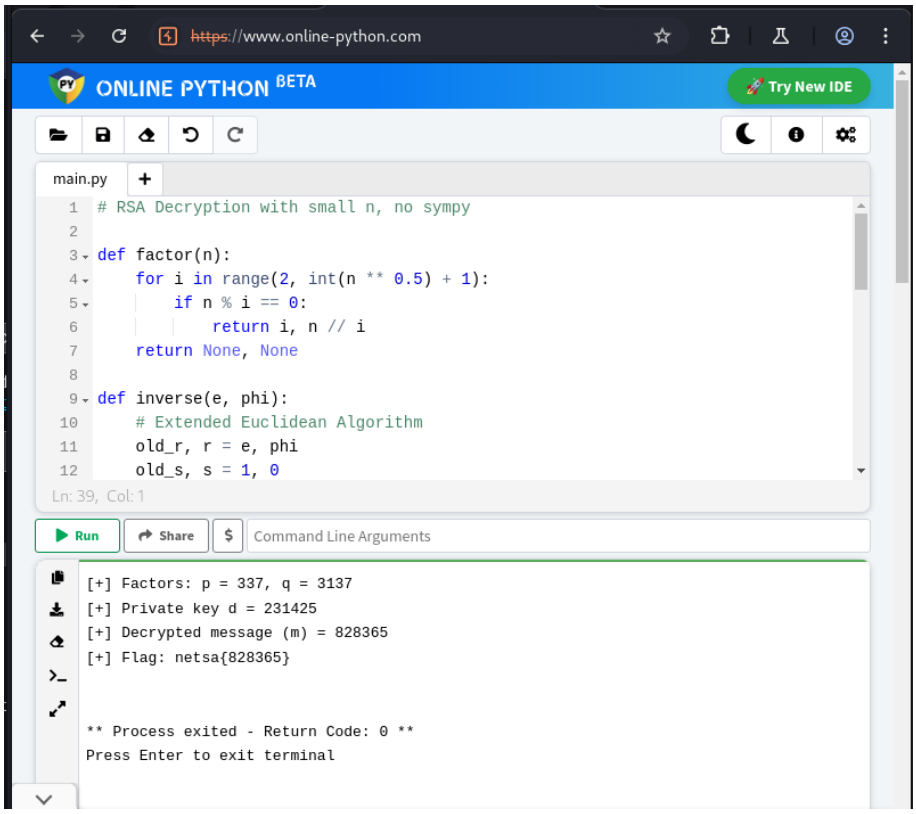
e (the public exponent): 65537

c (the ciphertext): 586132

Your task is to:

Compute the private key d

Flag Format netsa{Decimal}

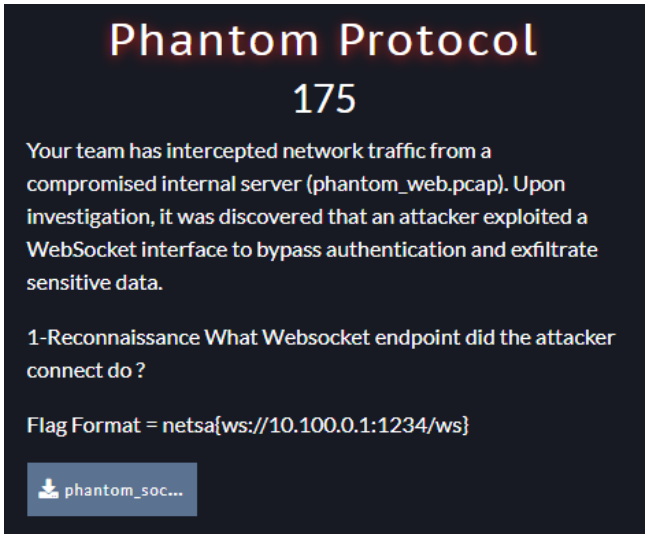


A simple python code was made to calculate the value of m

Flag: netsa{828365}

Forensics

Phantom Protocol



Forgor

Flag: forgor

Phantom Protocol II

Phantom Protocol II

212

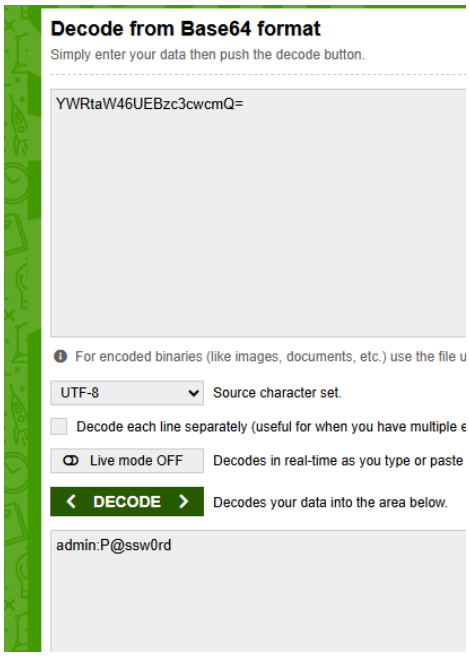
From Question Phantom Protocol ,What Credentials did the attacker use to authenticate ?

Flag Format : netsa{username:password}

Same Wireshark file as the predecessor.


```
{"cmd":"users"}
{
  "active_connections": 1,
  "your_ip": "192.168.244.132",
  "username": "anonymous",
  "note": "Admin can see more details"
}
{"auth":"YWRtaW46cGFzc3dvcmQ="}
{
  "status": "failed",
  "hint": "Invalid credentials"
}
{"auth":"YWRtaW46cGFzc3dvcmQxMjM="}
{
  "status": "failed",
  "hint": "Invalid credentials"
}
{"auth":"YWRtaW46UEBzc3dvcmQ="}
{
  "status": "failed",
  "hint": "Invalid credentials"
}
{"auth":"YWRtaW46UEBzc3cwcmQ="}
{
  "status": "success",
  "role": "admin",
  "token": "RkxBRzogbmV0c2Fze3diM19TMGNrM3RfUzRuZGJveDF9",
  "message": "Try exploring commands to find the real flag"
}
{"cmd":"debug_logs"}
```

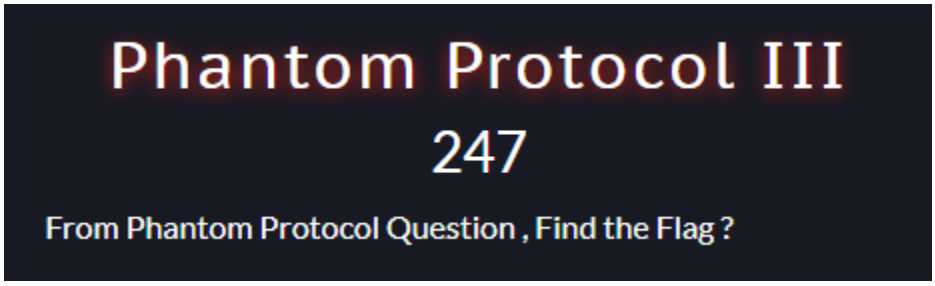

Authentication token.



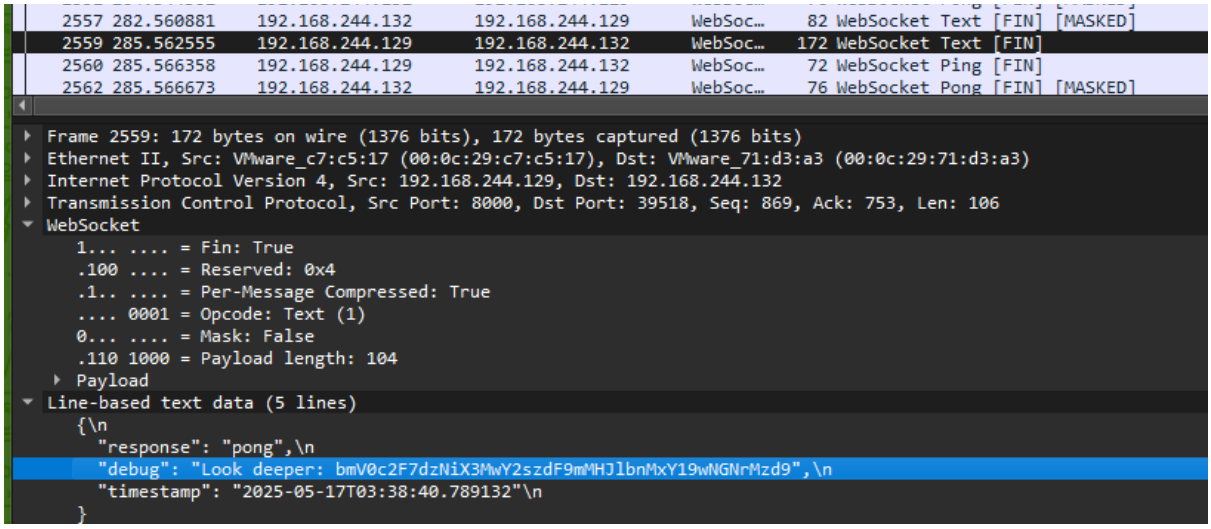
Decode Base64 format.

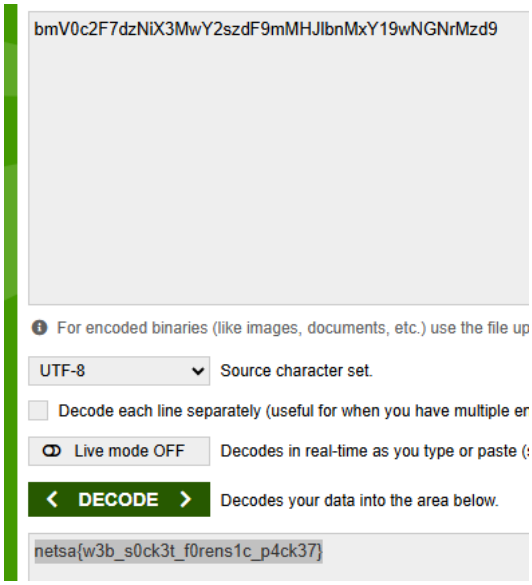
Flag: netsa{admin:P@ssw0rd}

Phantom Protocol III



Search for WebSocket protocol





Base64.

Flag: netsa{w3b_s0ck3t_f0rens1c_p4ck37}

IOT

4 Bytes to Freedom

4 Bytes to Freedom

136

Access logs have been wiped. No tags left behind. The only clue? Four strange bytes buried deep in memory. The flag is the obfuscated UID.

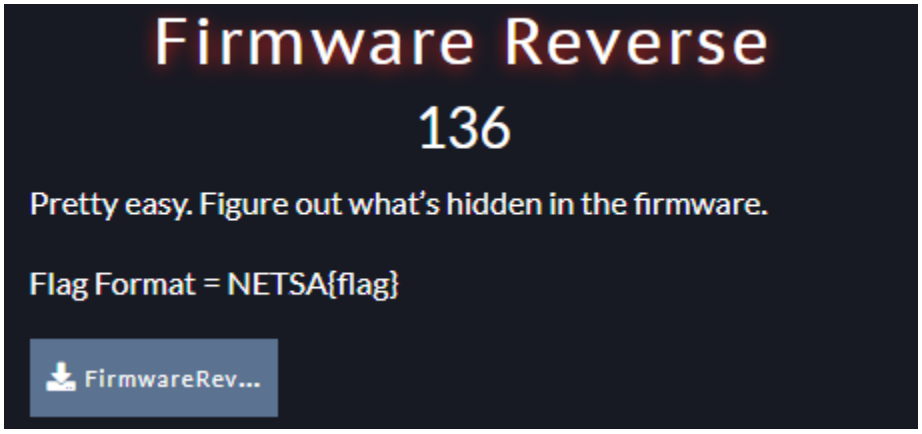
Flag format: NETSA{FLAG}

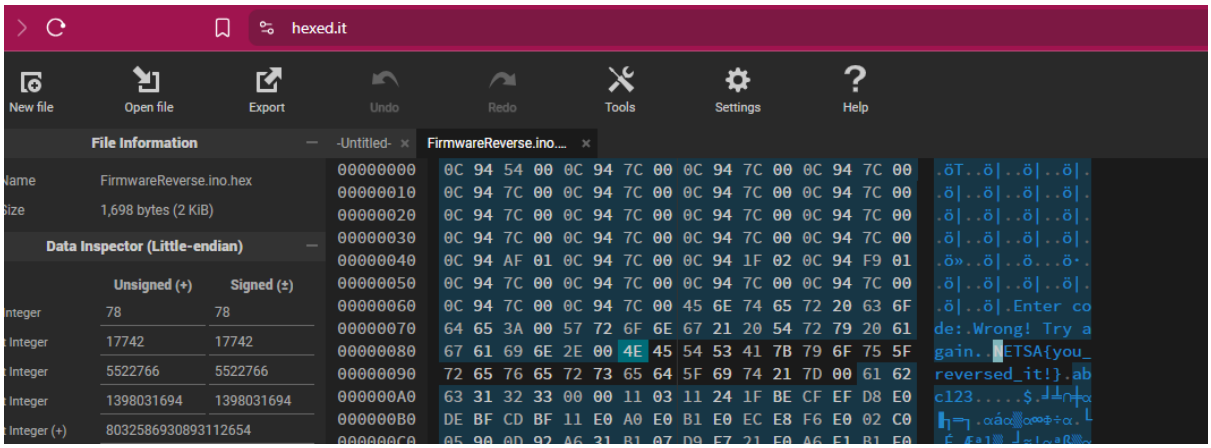
```
#include <EEPROM.h>
byte key[4] = {0xAA, 0xBB, 0xCC, 0xDD};
byte obfuscatedUID[4] = {0x74, 0x16, 0x0C, 0x03};

void setup() {
  Serial.begin(9600);
  for (int i = 0; i < 4; i++) {
    EEPROM.write(i, obfuscatedUID[i]);
  }
  Serial.println("Obfuscated UID written to EEPROM.");
}
void loop() {
```

Author forgor

Flag: netsa{??} cant do anything if he forgor

Firmware Reverse





Hex editor. Answer straight forward.

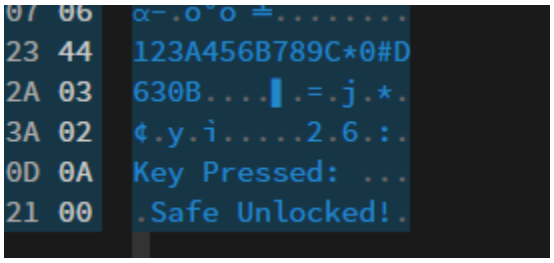
Flag: NETSA{you_reversed_it!}

Trace

A video of Arduino module blinking. Blinking = morse code.

Flag: NETSA{SILENT}

Blink Logic

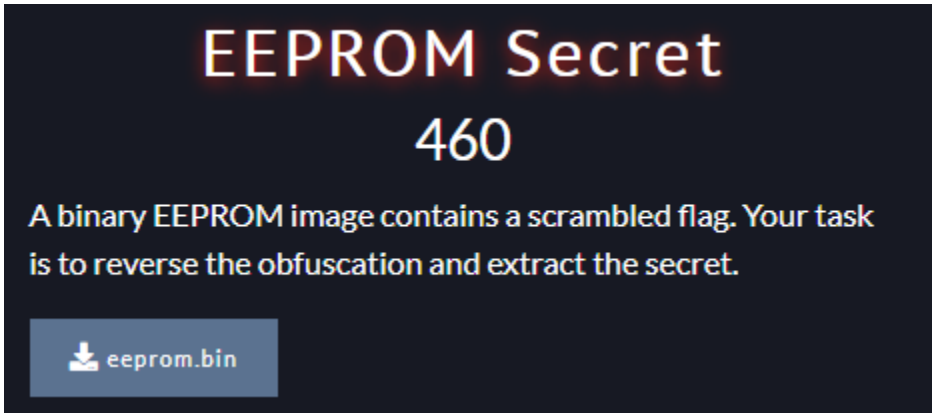


Follow the instructions.

Check hex editor last digits.

Flag: NETSA{630B}

EEPROM Secret



Author forgor

Flag: netsa{??} D:

OSINT

McD

This McD is in Farmlim, Penang.

Flag: netsa{farlim}

Train to Hospital

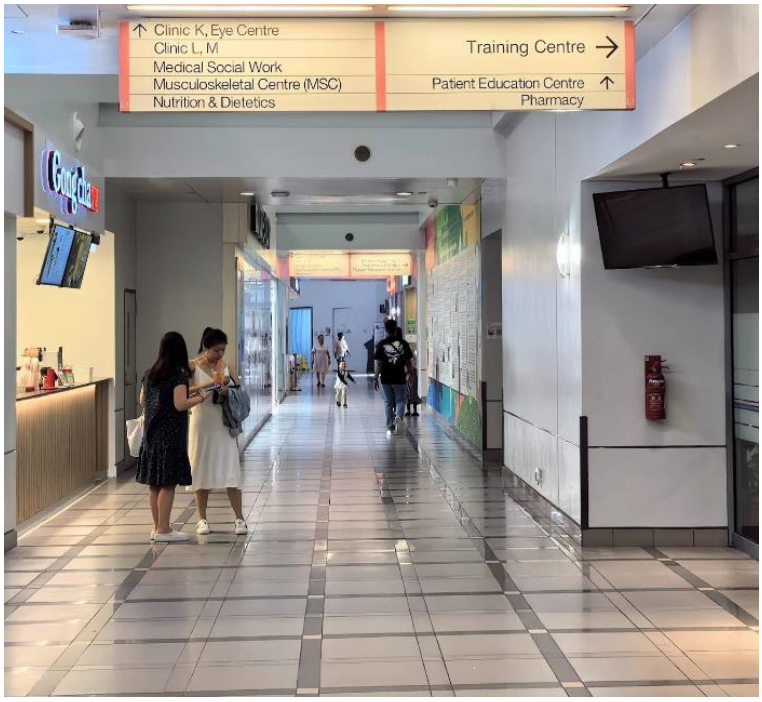
Train to Hospital

247

Your friend Jeam Wong just became a proud father in a hospital somewhere in Singapore. He sent you a quick photo from the hospital and invited you to visit. Locate the nearest MRT station to the hospital so you can visit the happy family !

Flag format: netsa{Location_Of_The_Station}

021d911e-b...



Gongcha in a hospital. :D

Flag: netsa{Little_India}

Final Debug

Final Debug

364

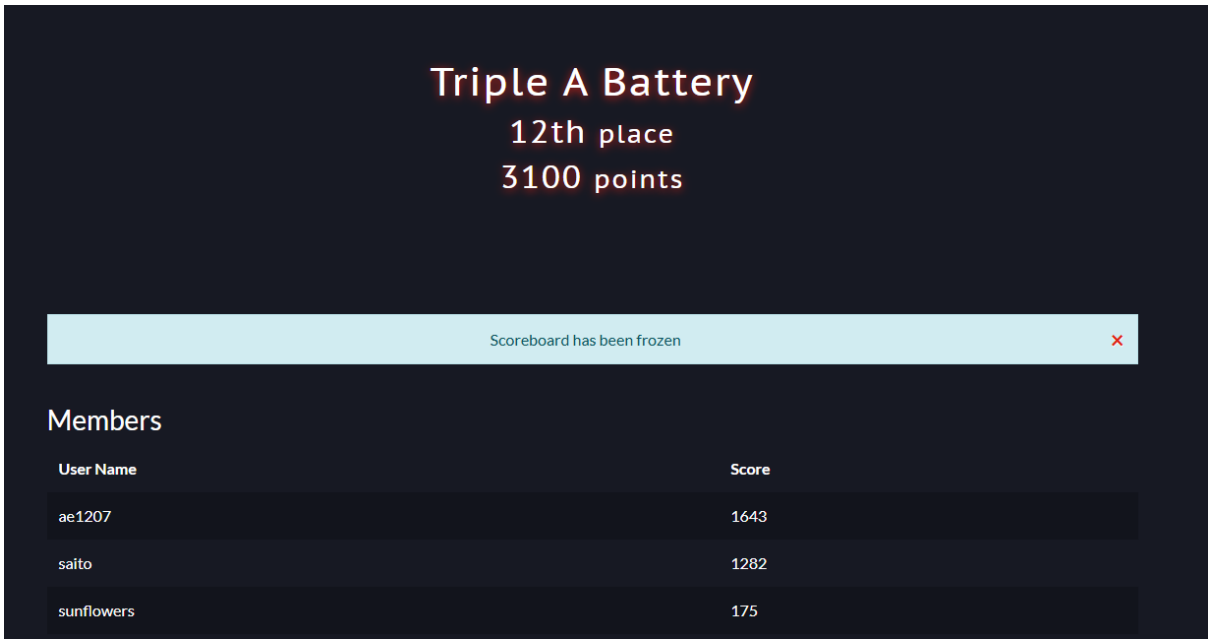
One of our former developers did not leave peacefully. After we fired her, she disappeared and took something valuable with her. Recently, she has been active online under the name pyth0n_l0v3rz, posting strange messages and small clues. We need your help to find and recover what she took — maybe it contains your flag.

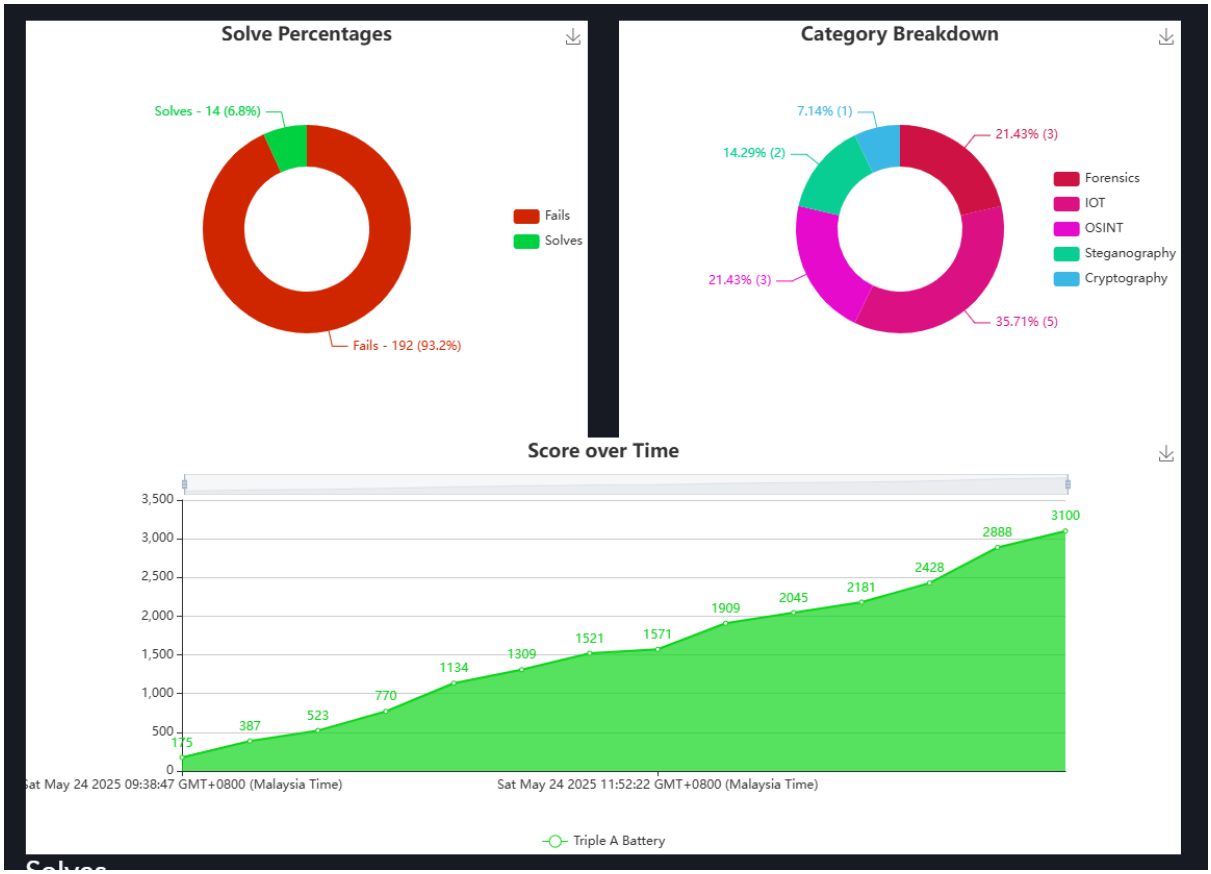
Flag Format : netsa{}

Find at GitHub. Author said it

Flag: netsa{??} (he forgor)

Triple A Battery as a Team





Solves

Challenge	Category	Value	Time
Phantom Protocol II	Forensics	212	May 24th, 2:55:11 PM
EEPROM Secret	IOT	460	May 24th, 2:54:54 PM
Phantom Protocol III	Forensics	247	May 24th, 2:45:45 PM
4 Bytes to Freedom	IOT	136	May 24th, 2:41:05 PM
Phantom Protocol	Forensics	136	May 24th, 2:10:09 PM
Final Debug	OSINT	338	May 24th, 11:53:55 AM
Welcome to CTF	Steganography	50	May 24th, 11:52:22 AM
Train to Hospital	OSINT	212	May 24th, 11:36:59 AM
Baby RSA	Cryptography	175	May 24th, 10:33:22 AM
Blink Logic	IOT	364	May 24th, 10:29:53 AM
Trace	IOT	247	May 24th, 10:23:07 AM
Firmware Reverse	IOT	136	May 24th, 10:11:04 AM
McD	OSINT	212	May 24th, 10:10:01 AM
Rasengram	Steganography	175	May 24th, 9:38:47 AM