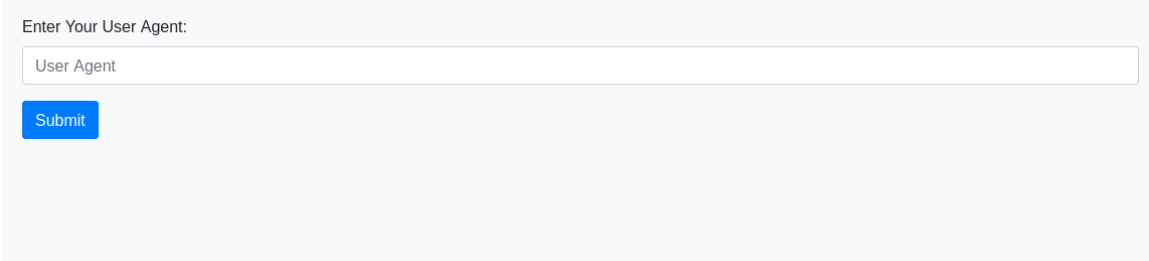
WU CYBER STRIKE ID CTF 2024

By : Sironcy (Rafi)

1. Hacker wanna be

Diberikan sebuah website dengan sebuah input berupa user agent

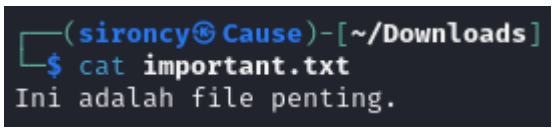


Setelah membaca hint **Hacker wanna be "tni-prima"** saya berpikir mungkin ada kaitannya user agent dengan tni-prima, lalu saya memodifikasi request saya menggunakan Burpsuite untuk mengganti user agent menjadi tni-prima dan berhasil mendapatkan Flagnya.

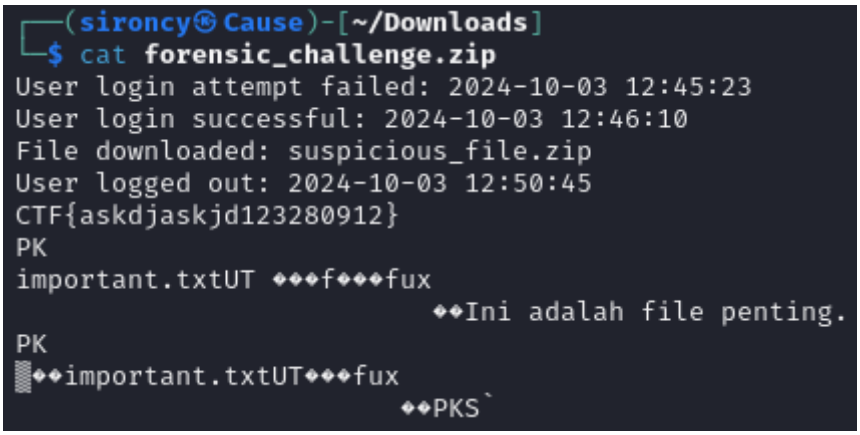
FLAG : **FLAG{_s!MpL3_us3r_4g3nT_}**

2. Log yang Tersembunyi

Diberikan sebuah file zip bernama forensic_challenge.zip, ketika kita mengekstraknya, kita hanya memperoleh sebuah text file yang isinya tidak berguna.



Kemudian saya mencoba untuk menggunakan command cat pada file zipnya untuk mengecek saja, dan ternyata mengandung Flagnya.



FLAG : **CTF{askdjaskjd123280912}**

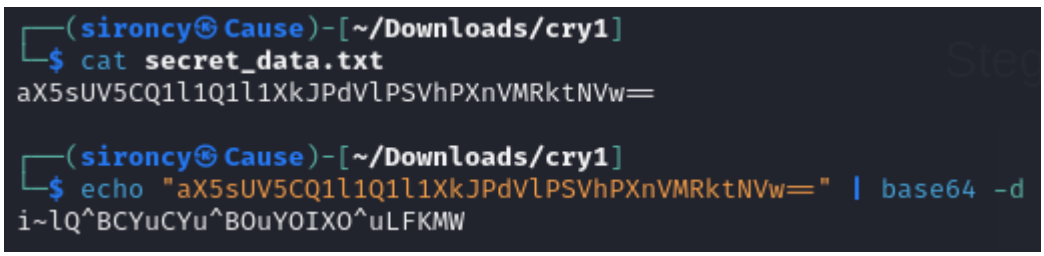
3. Eksplorasi Gambar Terenkripsi

Kita diberi sebuah file png, dengan nama ctf.png. Ketika saya cek image tersebut saya tidak menemukan informasi apapun, lalu saya berpikiran untuk mengecek metadata file tersebut menggunakan exiftool dan exiv2 tetapi tidak ada juga, lalu berlanjut ke binwalk, hexdump, xxd, saya juga tidak menemukan apapun. Kemudian saya mencoba tool **zsteg** dan akhirnya berhasil menemukan hidden Flagnya.

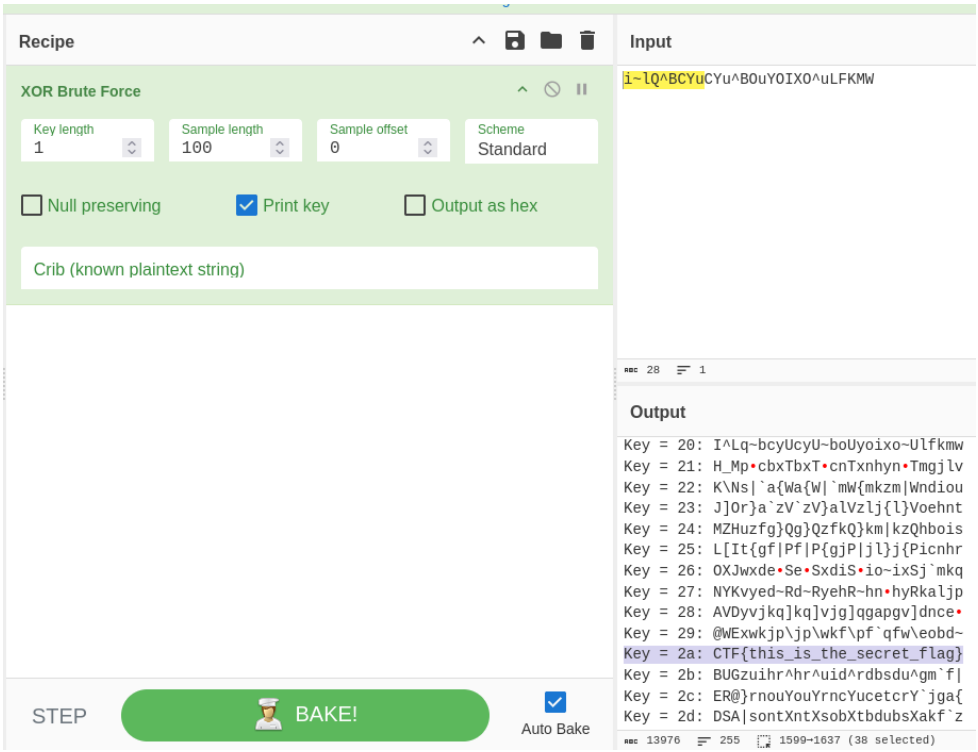
FLAG : **CTF{hidden_flag}**

4. Eksplorasi File Terenkripsi

Kita diberikan sebuah file zip dengan nama secret_data.zip, setelah diekstrak kita mendapatkan sebuah file yang mengandung file berisi teks yang diencode menggunakan base64. Kita coba decode dan mendapatkan teks enkripsi yang belum diketahui menggunakan metode apa.



Saya mencoba semua metode dekripsi yang ada pada situs cyberchef untuk menemukan Flagnya, dan akhirnya berhasil ditemukan pada enkripsi metode XOR dengan key = 2a.



FLAG : **CTF{this_is_the_secret_flag}**

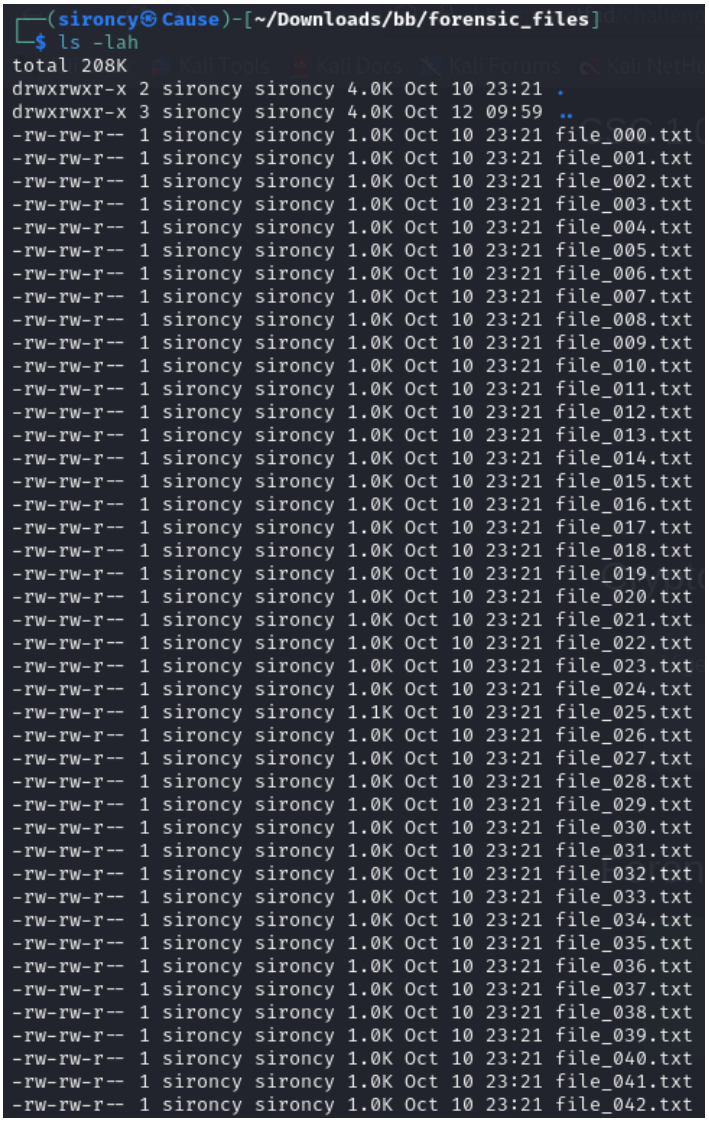
5. Tersembunyi

Diberikan sebuah zip file dengan nama forensic_challenge2.zip, setelah diekstrak kita mendapat dua file, terdapat string menarik pada file secret_message.txt yang tampaknya seperti encoding base64, lalu saya coba mendecodenya dan mendapatkan Flagnya.

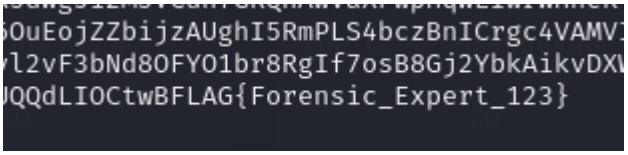
FLAG : **CTF{123Srypto}**

6. Mystery in the Files

Diberikan file zip bernama barangbukti.zip ketika diekstrak kita mendapatkan sebuah directory dengan 50 file, saya coba untuk menampilkan semua file dengan perintah **ls -lah** yang akan menampilkan semua file termasuk hidden files dengan format list, serta ukurannya. Setelah dicermati terdapat satu file dengan ukuran yang berbeda dari file lain, yaitu file **file_025.txt**.



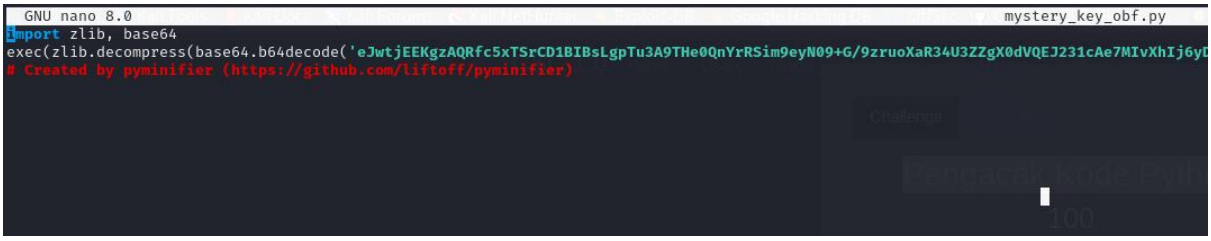
Setelah dilihat isi file tersebut mengandung Flag yang kita cari.



FLAG : **FLAG{Forensic_Expert_123}**

7. Pengacak Kode Python

Diberikan sebuah program python yang berfungsi mendecode string dari base64 lalu mendekompresinya dari zlib, ternyata setelah dijalankan program tidak berfungsi.



Dengan bantuan internet saya membuat program yang serupa, ketika dijalankan berfungsi dengan baik dan mereveal Flagnya.

```
┌──(sironcy㉿Cause)-[~/Downloads]
└─$ cat obs.py
import zlib
import base64

compressed_data = 'eJwtjEEKgzAQRfc5xTSRCD1BIBsLgpTu3A9THe0QnYrRSim9eyN09+G/9zruoXaR34U3ZZgX0
RD8o'

def flag(data):
    decoded_data = base64.b64decode(compressed_data)
    decompressed_data = zlib.decompress(decoded_data)
    print(decompressed_data.decode('utf-8'))

if __name__ == '__main__':
        flag(compressed_data)
```

```
┌──(sironcy㉿Cause)-[~/Downloads]
└─$ python3 obs.py
def I(key):
B=print
a=input
 w="reverse_engineering_rocks"
 if key==w:
  B("Flag: CTF{flag_anda_disini}")
 else:
  B("Kunci salah, coba lagi!")
if __name__=="__main__":
 T=a("Masukkan kunci: ")
 I(T)
```

FLAG : **CTF{flag_anda_disini}**