Writeup CTF ADIKARA 2024

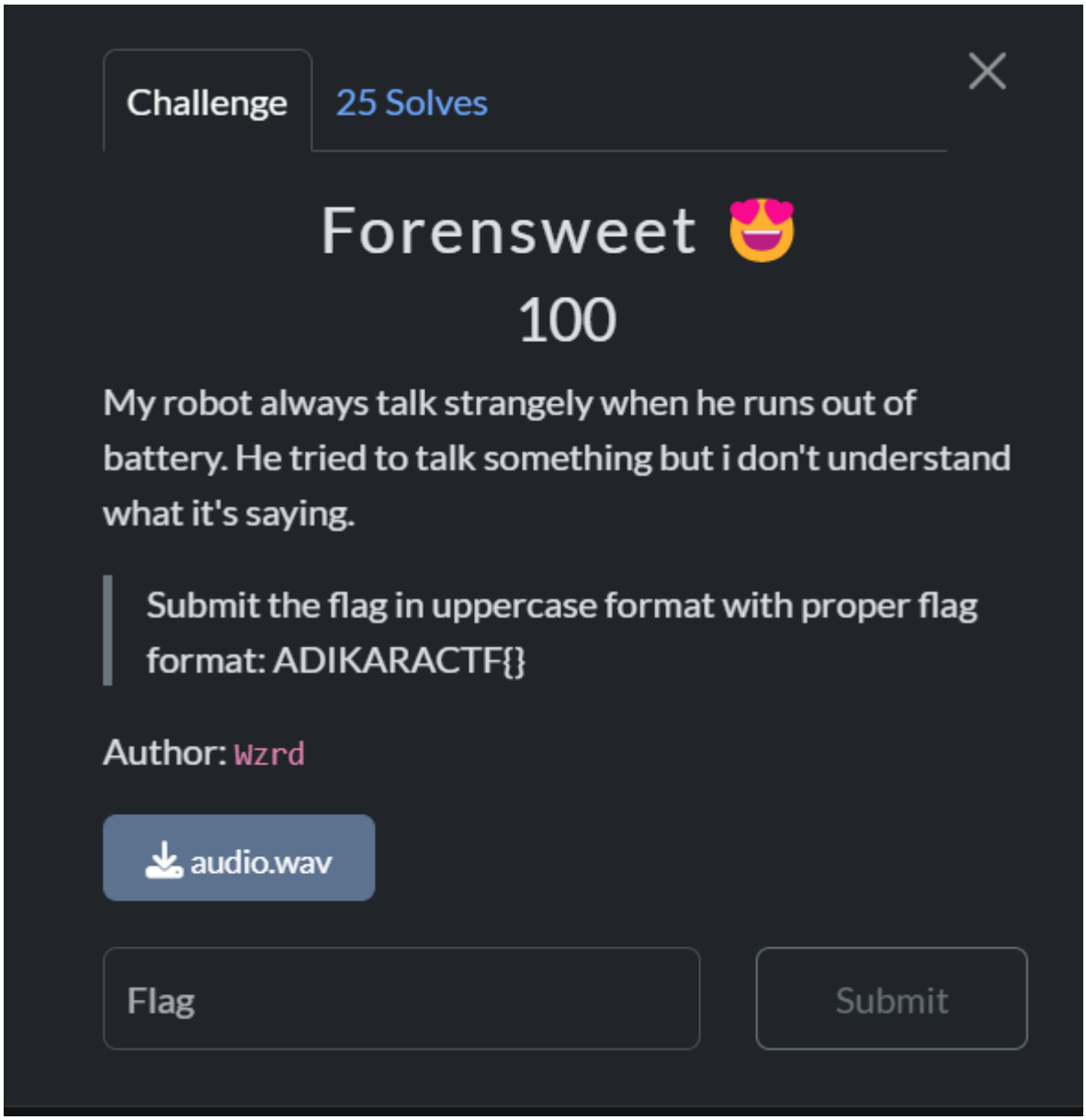
Presented By :

Arie Farchan Fyrzatullah

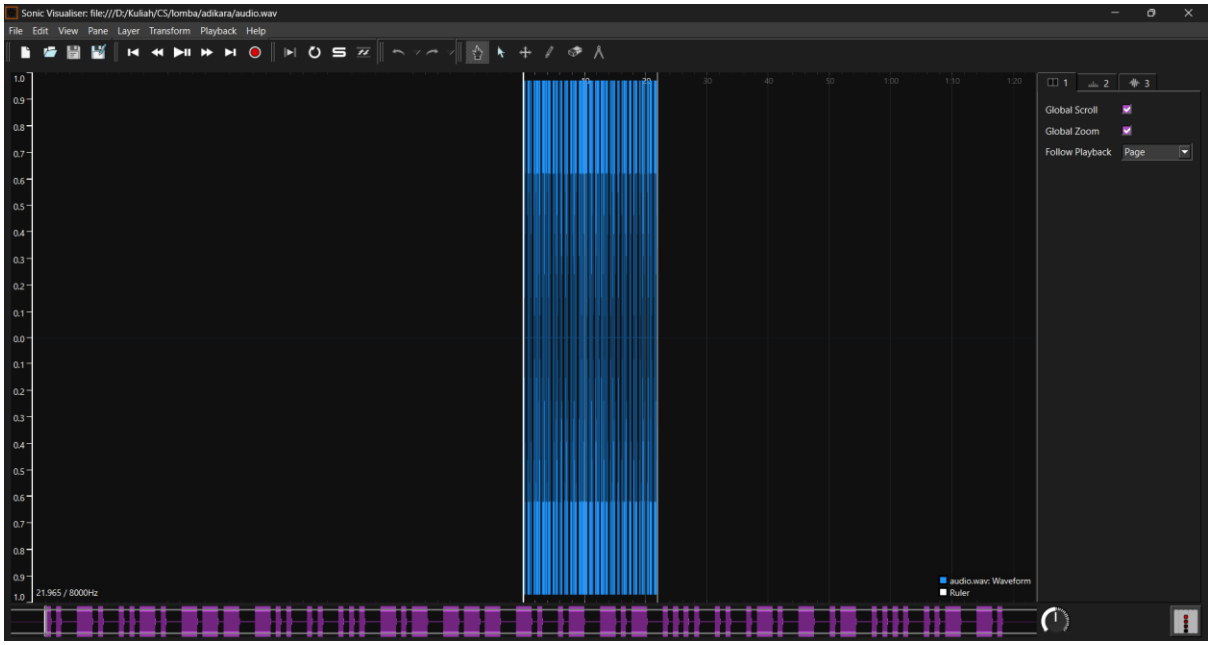
Daftar Isi

Forensic

Forensweet



Diberikan challenges seperti berikut. Diberikan 1 buah file dengan format wav.



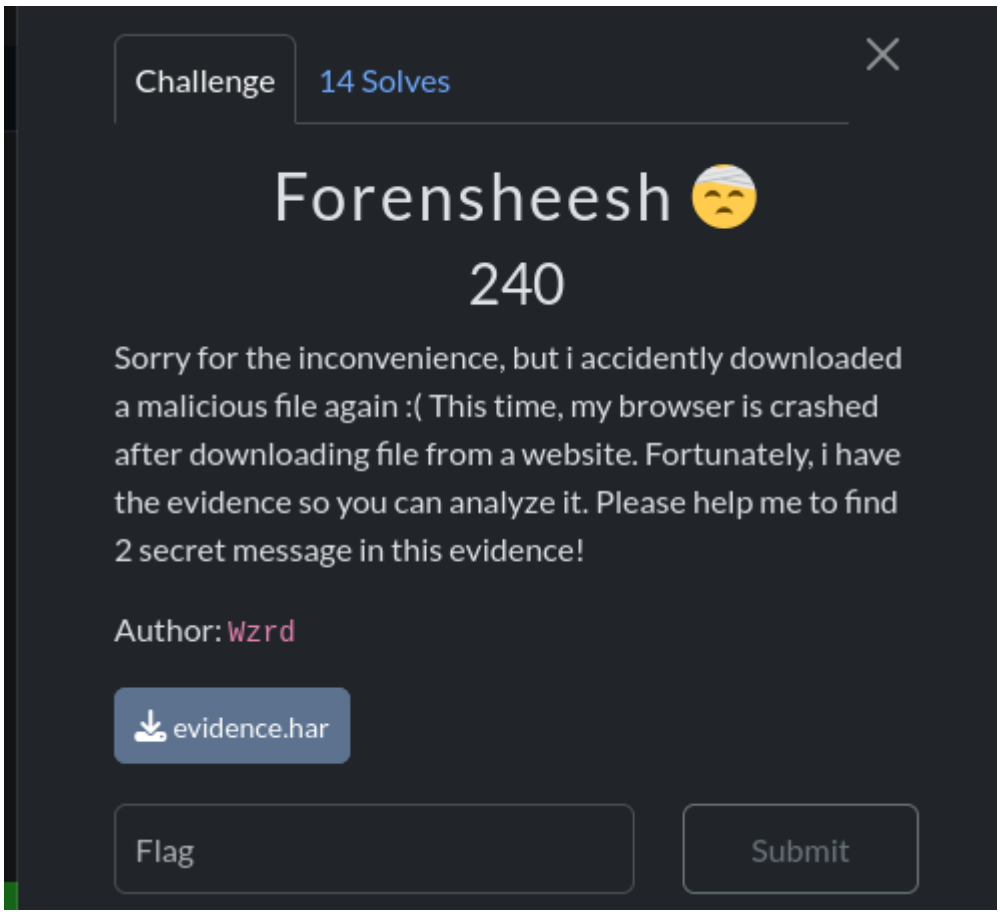
Saya langsung impor kedalam software sonic visualiser untuk melihat apakah ada pesan tersembunyi atau tidak. Jika dilihat, pada bar dibawah merupakan suatu pola, ada panjang dan pendek. Ini mengingatkan saya dengan sandi morse. Saya coba tulis sandinya.

.. -. ..-. --- -.. .. ... -.- --- -. .- -.- ....-. - .- .... ..- -..

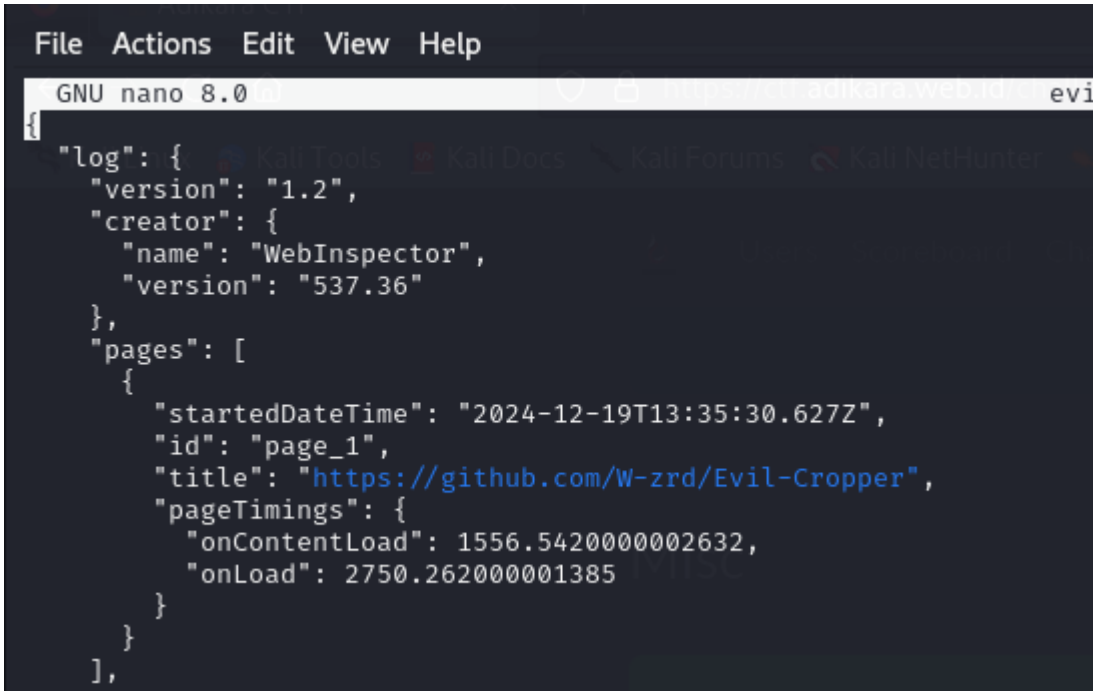
Setelah itu, saya menggunakan morse code translator untuk mencari pesan yang disembunyikan. Dan yap, kita dapat flagnya

Flag : ADIKARACTF{INFODISKONAKHIRTAHUN}

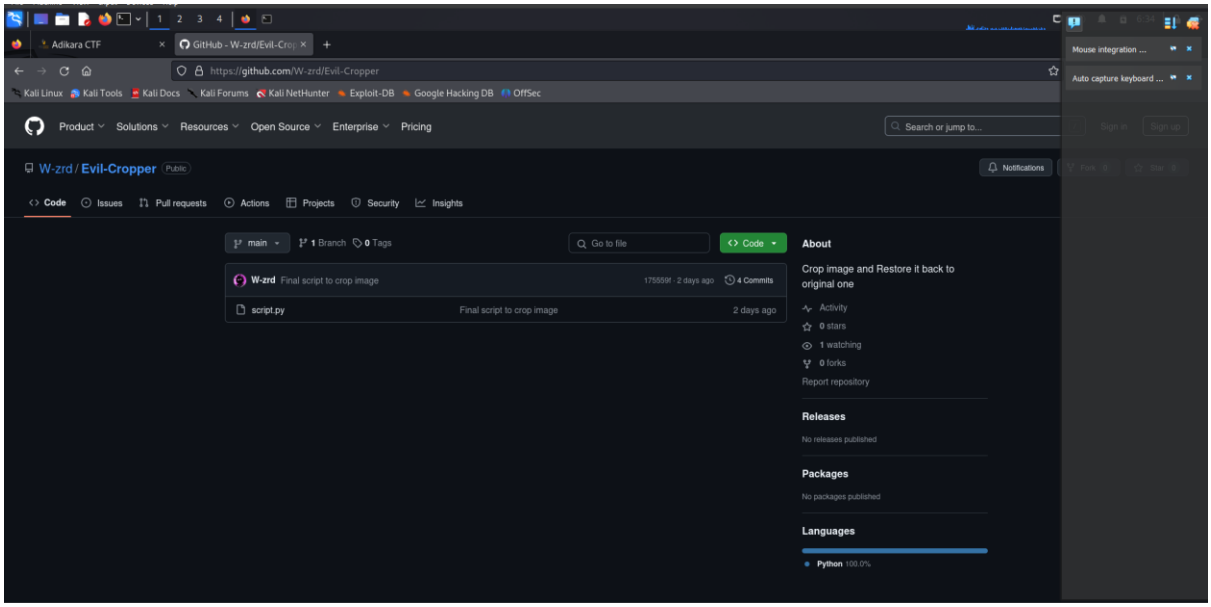
Forensheesh

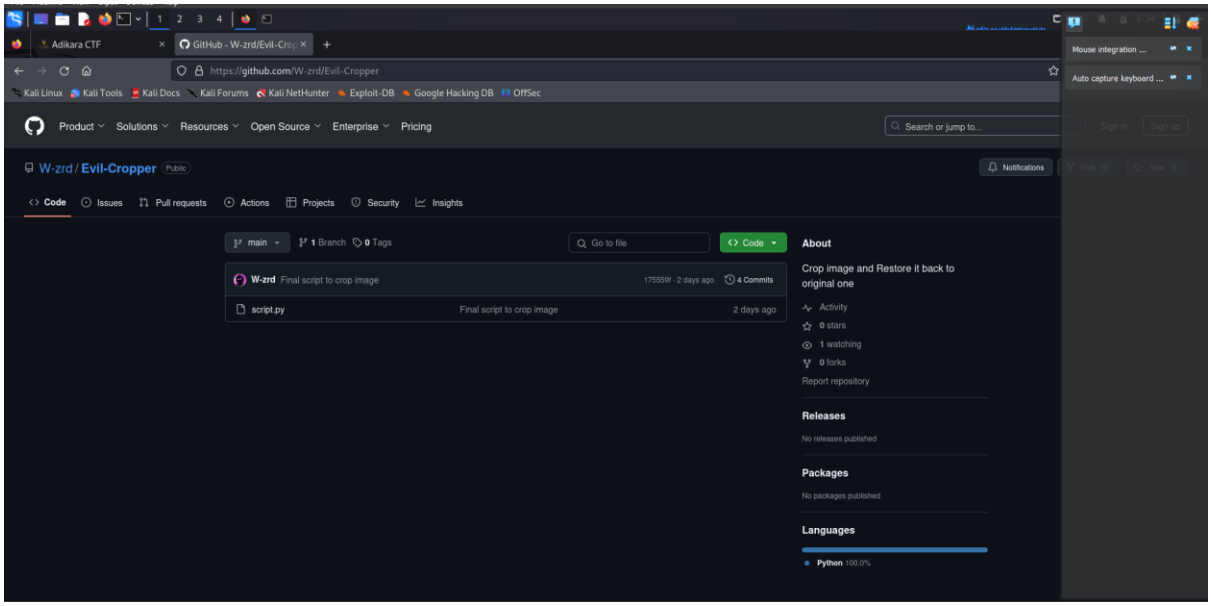


Pada soal ini, diberikan 1 buah file berupa file dengan format har, langsung saya buka saja untuk menganalisanya

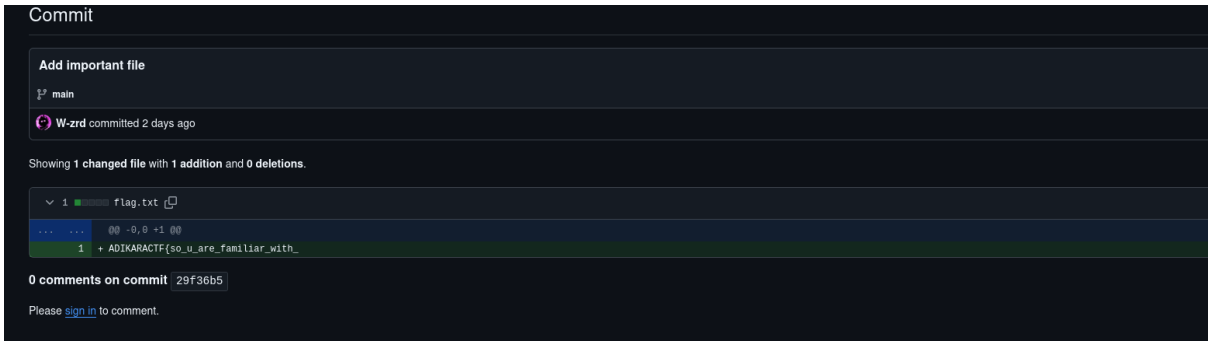


Setelah setelah dianalisa, didalam sini terdapat link github. Langsung saya buka untuk mencari flagnya.

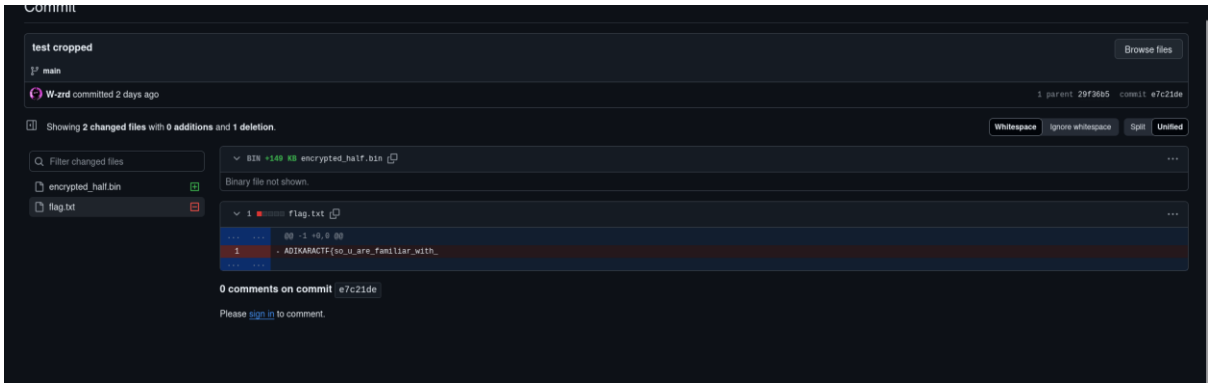




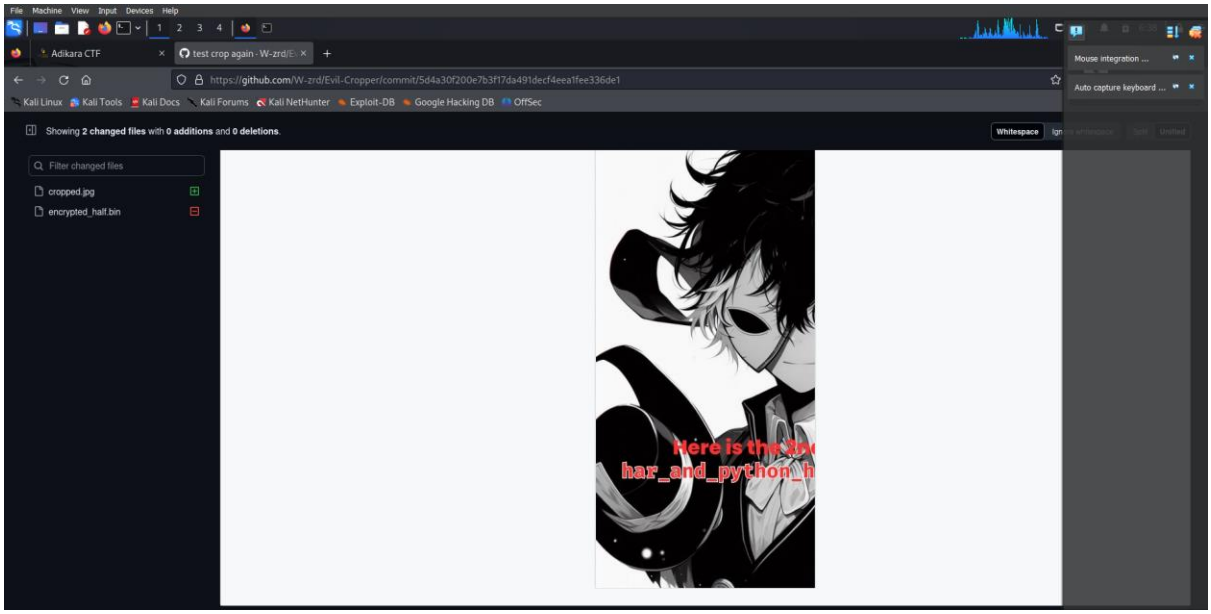
Saya langsung melihat commit histori dan membuka satu persatu untuk menyelesaikan satu satu



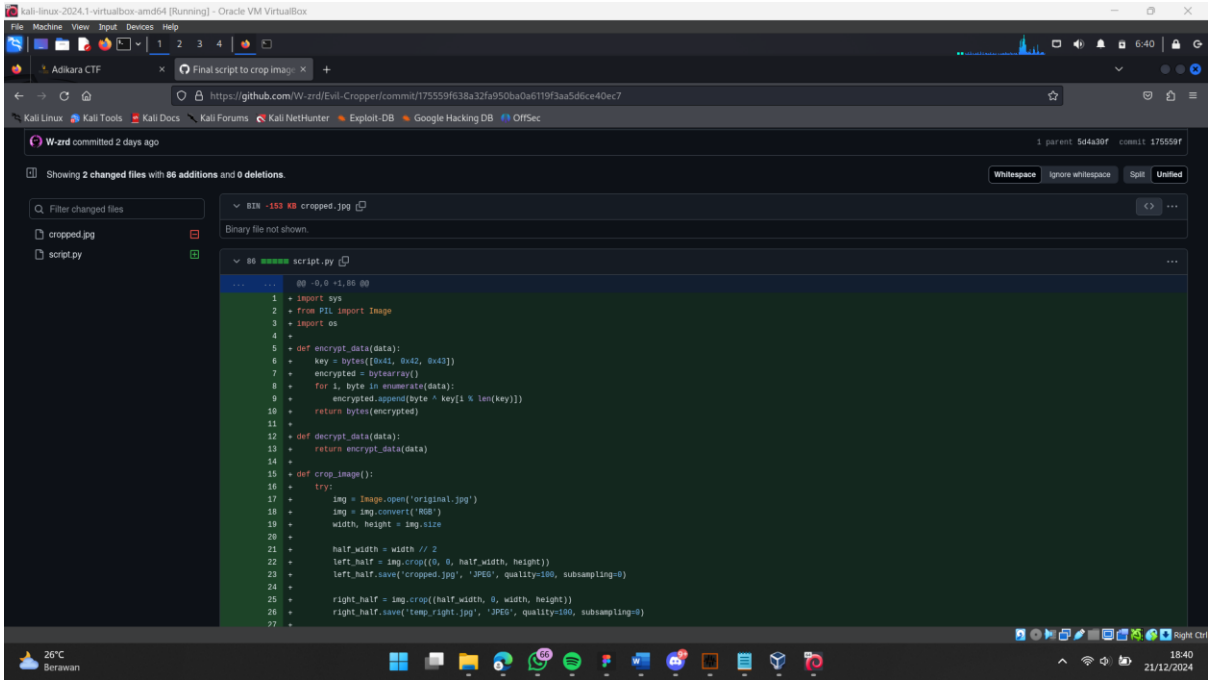
Pada bagian pertama Add important file, saya mendapati potongan flag yaitu ADIKARACTF{so_u_are_familiar_with_ . Kita tinggal mencari potongan flag lainnya.



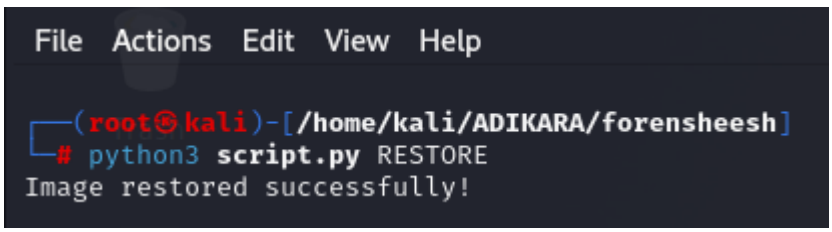
Pada bagian ini, ada file dengan format .bin, sya download apabila dibutuhkan.



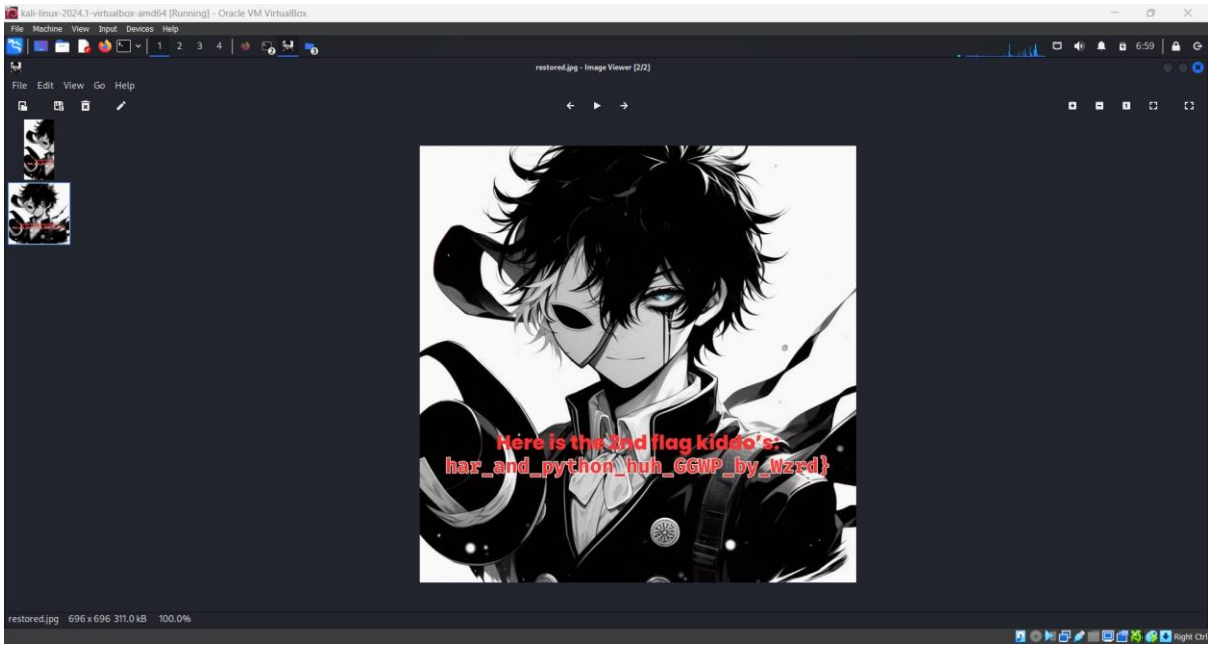
Pada bagian test crop again, saya mendapati cropped image dengan potongan file didalamnya har_andpython_h. saya juga mendownload imagenya.



Di bagian final script to crop image, saya menemukan sebuah script. Sepertinya ini digunakan untuk merestore image tadi.



Tinggal saya restore dengan menggunakan script yang ada. Dan image selesai di restored



Dan yap, kita dapatkan potongan flag yang lain. har_andpython_huh_GGWP_Wzrd}

Kita tinggal gabungkan saja dengan potongan flag sebelumnya

Flag : ADIKARACTF{so_u_are_familiar_with_har_andpython_huh_GGWP_Wzrd}

Polygrot

Diberikan challenges seperti berikut. Diberikan 1 buah file dengan format pdf.

---

polygots?_19adf}

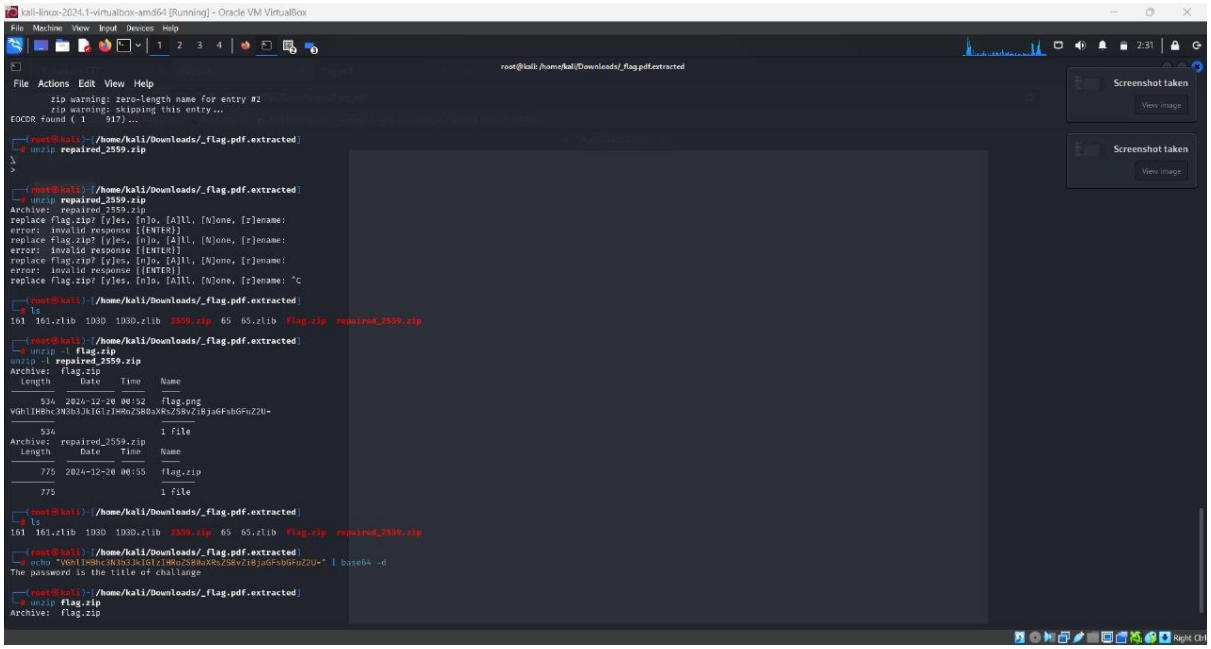
Setelah dibuka terdapat potongan flag polygots?_19adf}.

```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
30            0x1E            PDF document, version: "1.7"
101           0x65            Zlib compressed data, default
353           0x161           Zlib compressed data, default
7485          0x1D3D          Zlib compressed data, default
9561          0x2559          Zip archive data, at least v1.
```

Saya gunakan binwalk untuk menganalisis file. Dan didalamnya ada data zip tersembuni di offset 0x2559.

Setelah itu, saya masuk kedalam direktori hasil extract yaitu _flag.pdf.extracted. dan mel;ihat didalmnya banuak data. Akan tetapi saya fokus kedalam dile 2559.zip.

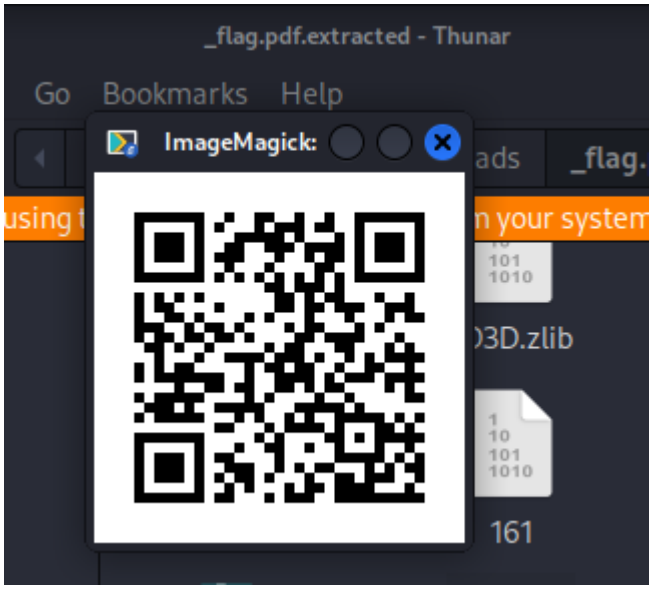
Setelah itu saya extrax 2559.zip dengan command zip -FF 2559.zip --out repaired_2559.zip, karena filenya rusak.



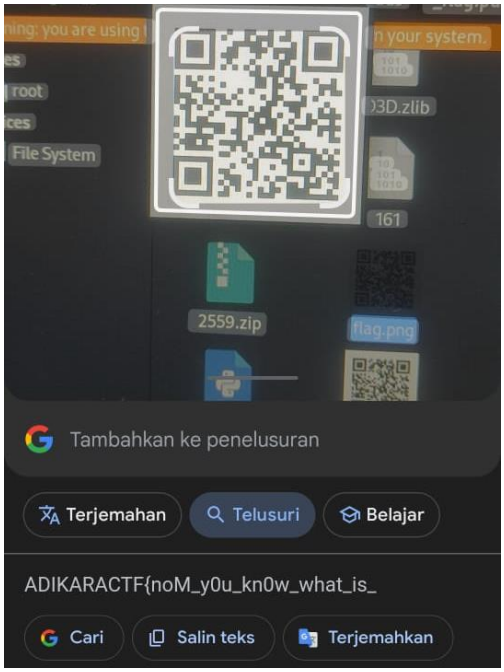
Setelah itu saya melakukan unzip terhadap file hasil repair dan terdapat file degan nama flag.zip. setelah itu saya periksa isi filenya dan mendapati ada string aneh seperti pesan yang tersenkripsi. Saya decrypt pesan tersebut dengan menggunakan base64 dan muncul clue pw dari flag.zip adalah judul dari challengenya yaitu Polygrot

```
┌──(root㉿kali)-[/home/kali/Downloads/_flag.pdf.extracted]
└─# ls
161         1D3D        2559.zip  65.zlib   flag.zip  mama
161.zlib    1D3D.zlib   65        flag.png  hack.py   repaired_2559.zip
```

saya lakukan unzip juga dan memasukkan pw sesuai dengan judul challenge, didalamnya da file dengan nama flag.png



setelah dibuka, terdapat QR code didalamnya, saya memanfaatkan google lens untuk membaca isinya.

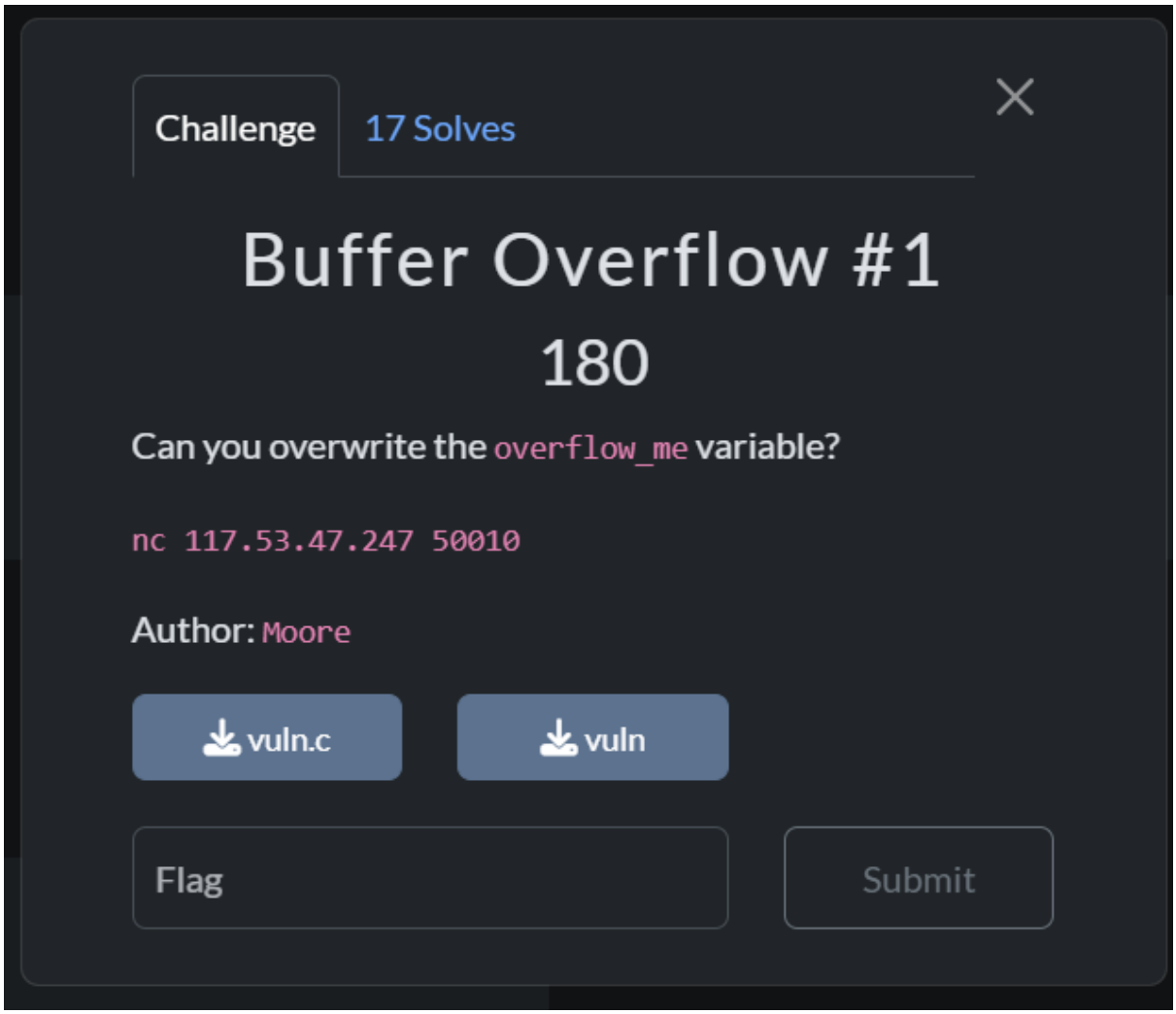


Dan yap, terddapat potongan lain falg didalamnya. ADIKARACTF{noM_y0u_kn0w_what_is_

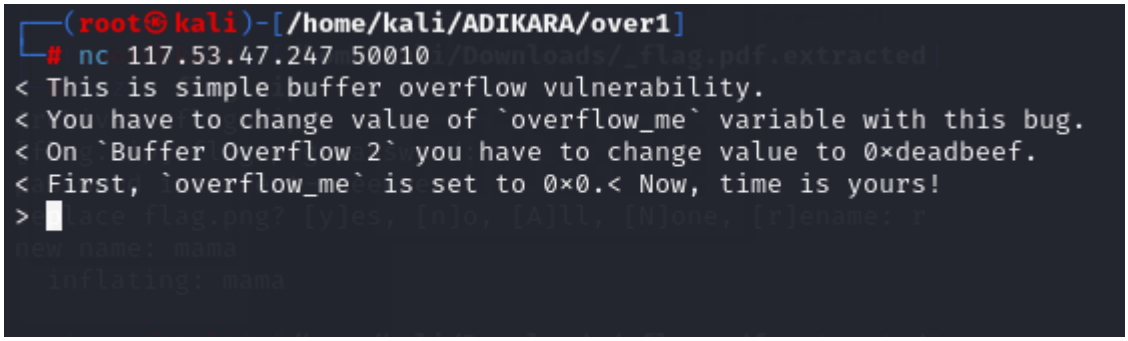
Flag : ADIKARACTF{noM_y0u_kn0w_what_is_polygots?_19adf}

Binary Exploitation

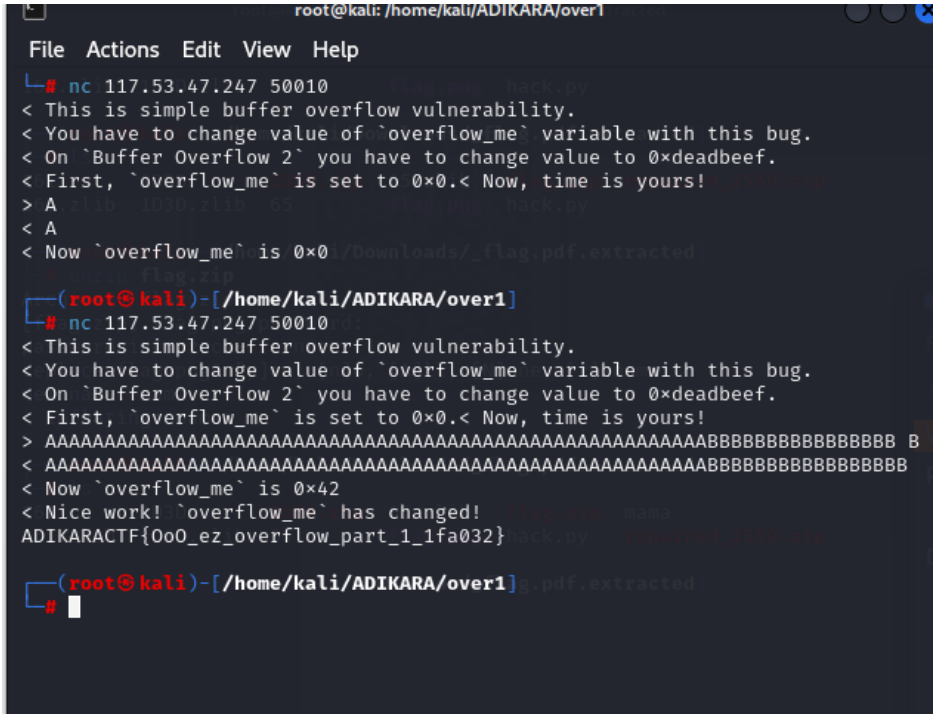
Buffer overflow #1



Diberikan sebuah challenge seperti berikut.



Saya langsung connect dan muncul informasi seperti diatas.

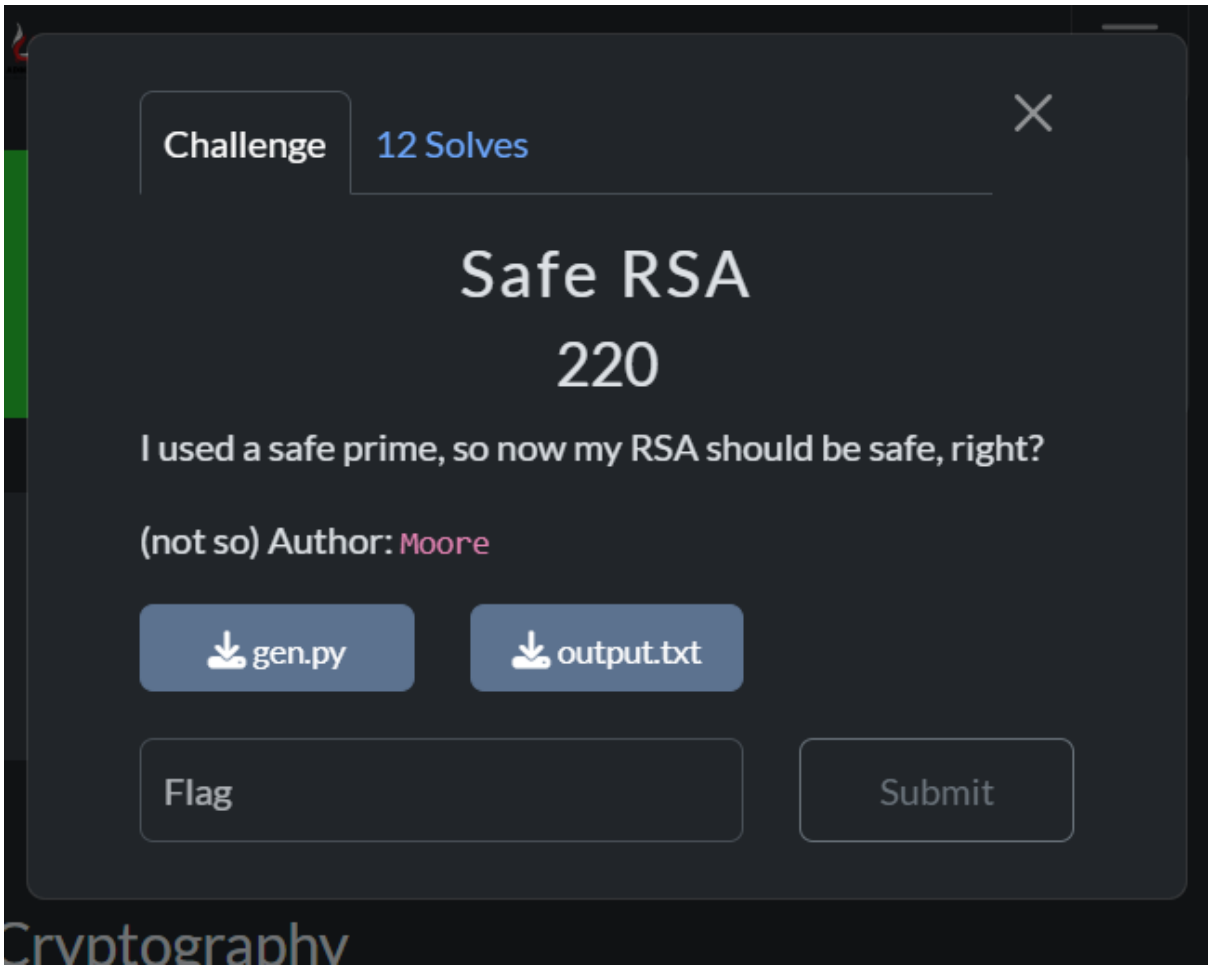


Sselanjutnya saya uji inpunya untuk melihat respon yang diberikan. Saya berkali kali mencoba menemukan ukuran buffer yang tepat. Dan saya temukan ukuran yang tepat, setelah itu, saya mempersiapkan payload untuk menimpa overflow_me dan terdiri dari jumlah padding 40 byte dan 8 byte tambahan ubntuk mencapai overflow_me. Dan yap, kita dapat flagnya.

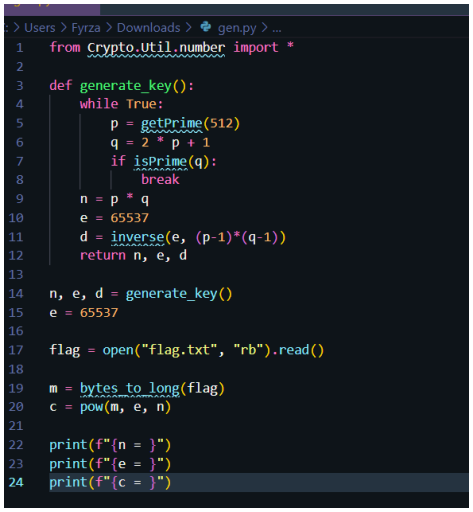
Flag : ADIKARACTF{OoO_ez_overflow_part_1_1fa032}

Cryptography

Safe RSA

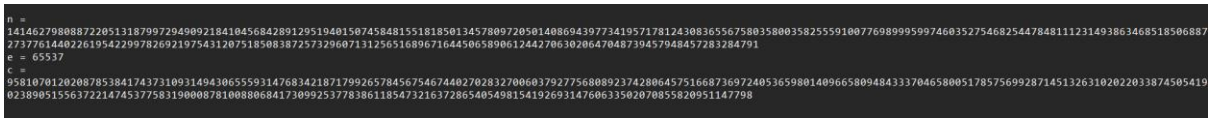


Pada challenge ini kita diberikan 2 buah file.

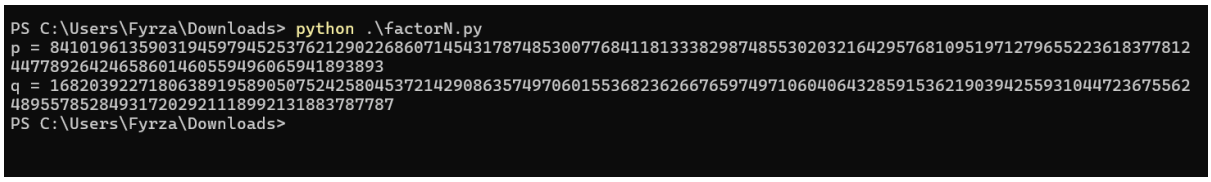


```
Users > Fyrza > Downloads > gen.py > ...
from Crypto.Util.number import *

def generate_key():
    while True:
        p = getPrime(512)
        q = 2 * p + 1
        if isPrime(q):
            break
    n = p * q
    e = 65537
    d = inverse(e, (p-1)*(q-1))
    return n, e, d

n, e, d = generate_key()
e = 65537

flag = open("flag.txt", "rb").read()

m = bytes_to_long(flag)
c = pow(m, e, n)

print(f"{n = }")
print(f"{e = }")
print(f"{c = }")
```

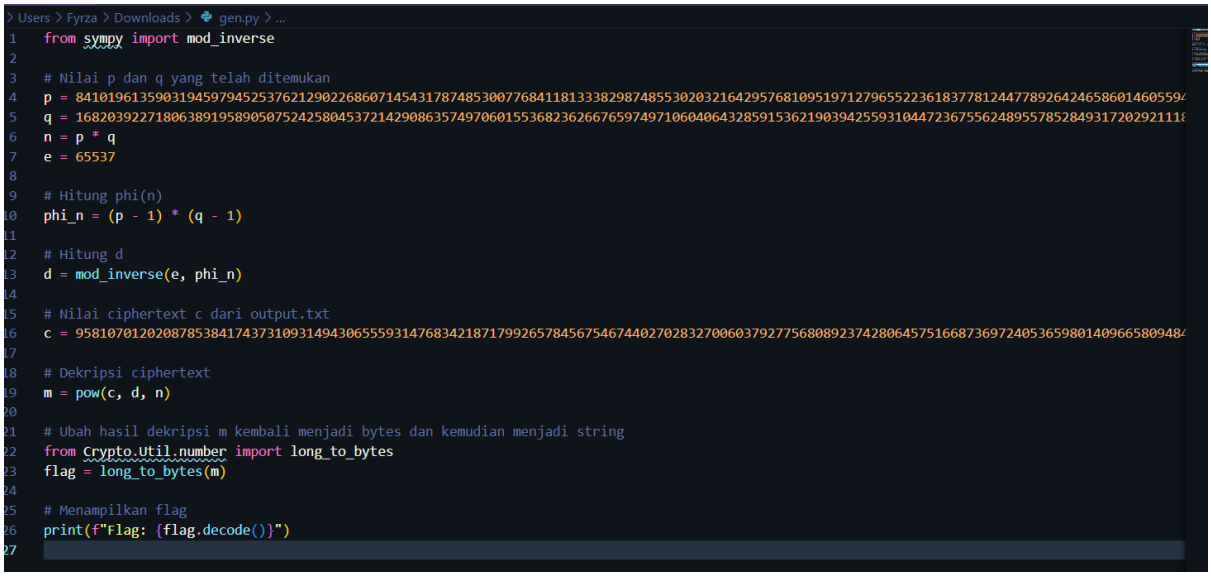
Dalam file gen.py terdapat code seperti diatas



Dan dalam file output berisi seperti diatas.



Untuk memecahkan ini pertama tama saya memfaktorkan bilangan n untuk mendapat nilai p dan q. diatas adlah script untuk mencari nilainya.



Selanjutnya saya mencari nilai dari phi(n) dan menghitung nilai d, setelah didapatkan nilai d, kita dapat mendecrypt pesan dengan rumus m=c^d mod n. diatas adalah scriptnya

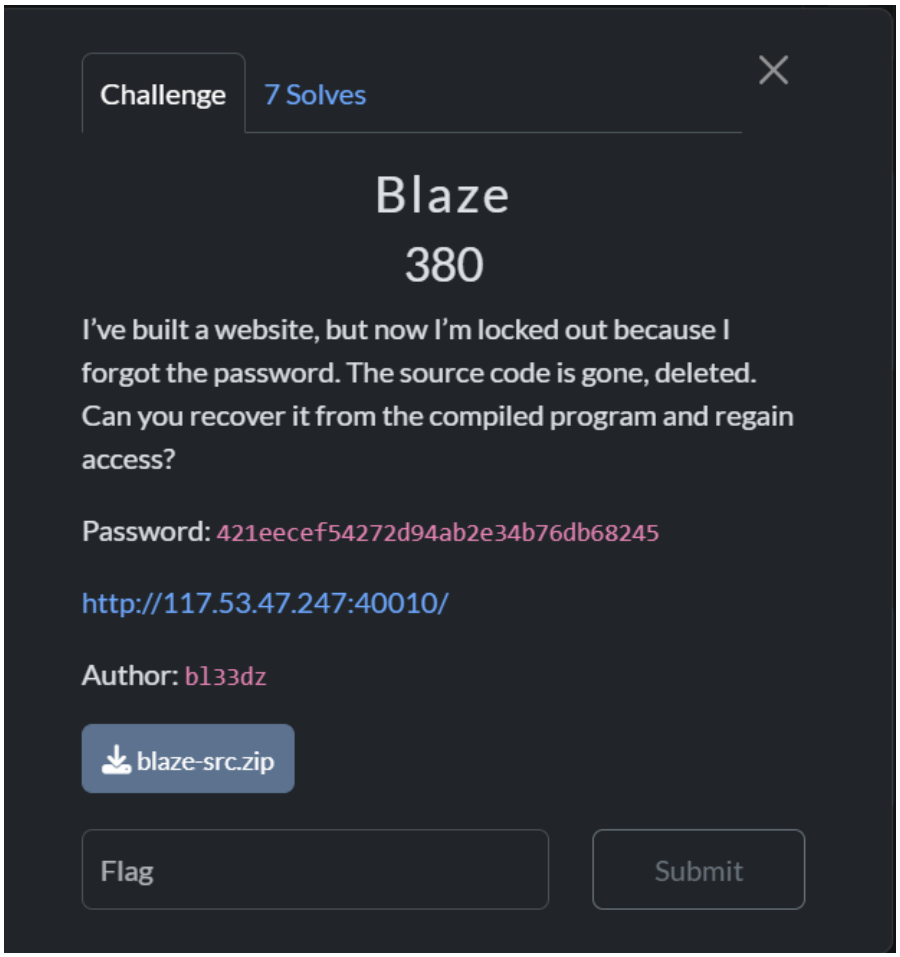
```
PS C:\Users\Fyrza\Downloads> python .\gen.py
Flag: ADIKARACTF{info_nilai_kalkulus_brp_bang_90afc2}
PS C:\Users\Fyrza\Downloads>
```

Dan yap, kita dapat flagnya.

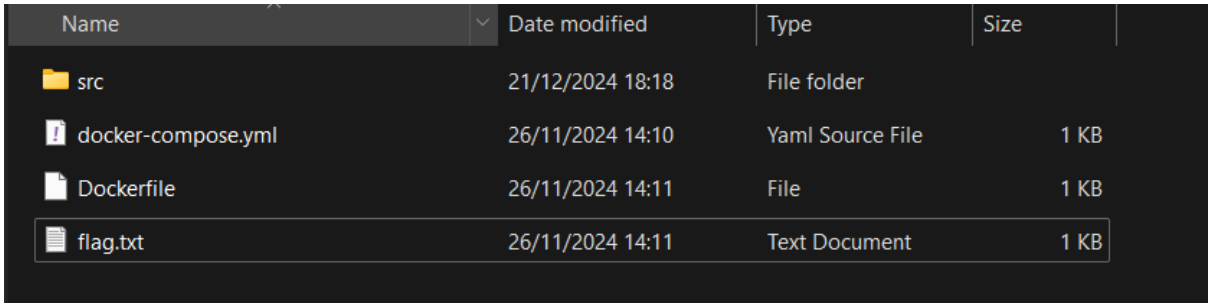
Flag : ADIKARACTF{info_nilai_kalkulus_brp_bang_90afc2}

Web Exploit

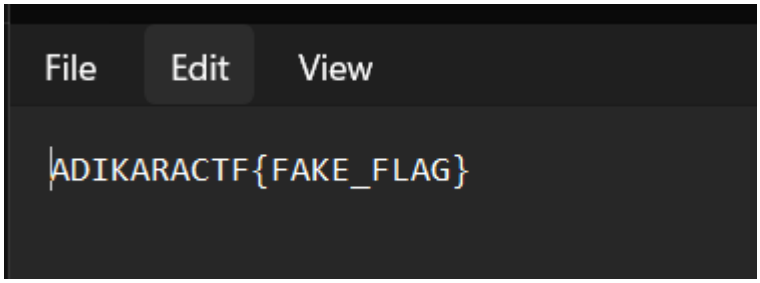
Blaze



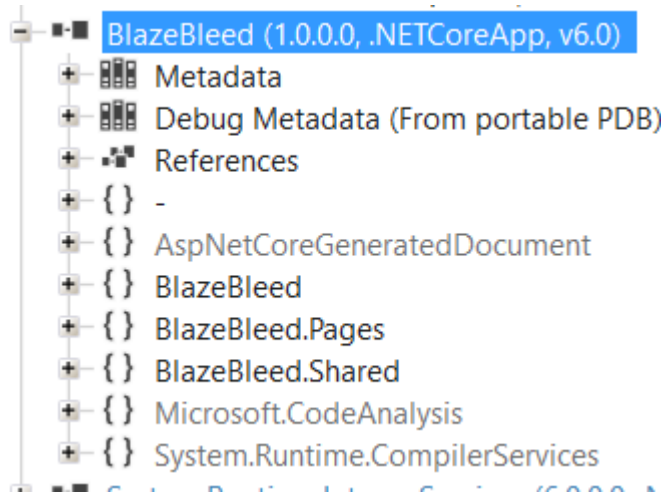
Diberikan file dengan format zip.



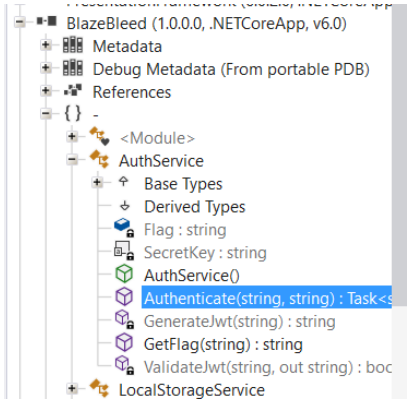
Setelah diextract, terdapat folder seperti diatas dan kita langsung mendaptkan flagnya.



scam bjirrrr.\

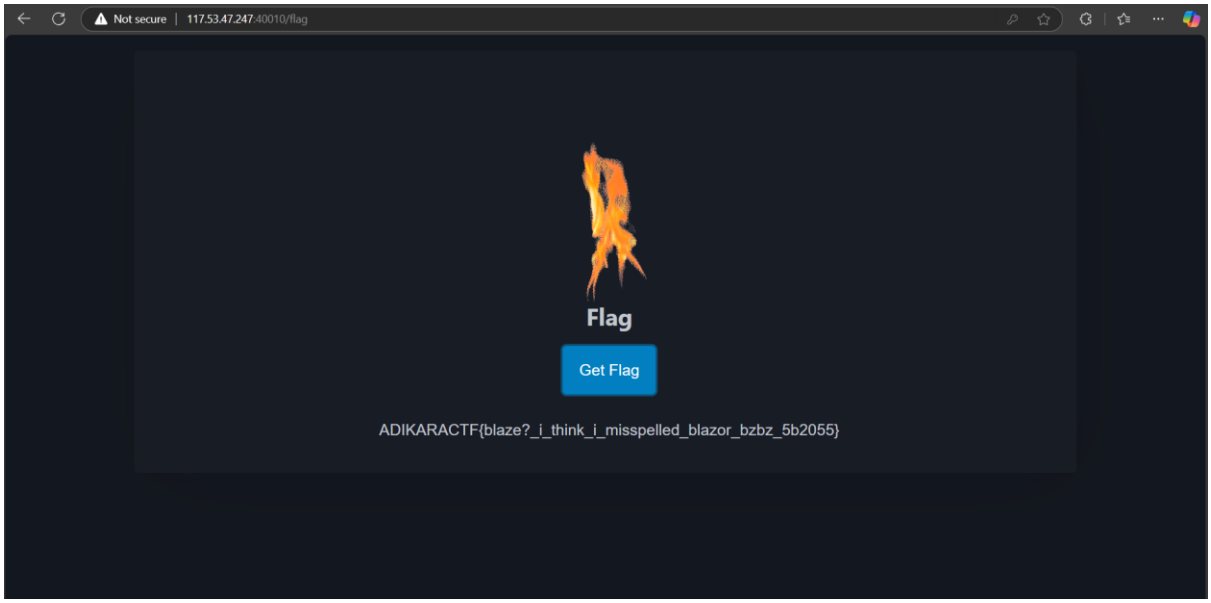


Saya anilisis file didalam BlazeBleed.dll dengan menggunakan tools ILSpy, salami terus codenya, bac abaca,cari Dimana kiranya code penting disimpan.



Saya sedikit curiga dengan bagian ini, siapa tau terdapat informasi berguna.

akhirnya saya daptkan ussernamenya yaitu “admin” dan passwordnya yaitu “isitjustmyimagination?”. Dan saya coba login menggunakan usrname dan pw tersebut.



Dan yap, kita dapatkan flagnya.

Flag : ADIKARACTF{blaze?_i_think_i_misspelled_blazor_bzbz_5b2055}