

Writeup CTF ADIKARA 2024



Presented By :
Arie Farchan Fyrzatullah

Daftar Isi

Forensic.....	3
Forensweet.....	3
Forensheesh.....	5
Polygrot.....	10
Binary Exploitation.....	13
Buffer overflow #1.....	13
Cryptography.....	15
Safe RSA.....	15
Web Exploit	17
Blaze	17

Forensic

Forensweet

Challenge

25 Solves

✕

Forensweet 🤪

100

My robot always talk strangely when he runs out of battery. He tried to talk something but i don't understand what it's saying.

Submit the flag in uppercase format with proper flag format: ADIKARACTF{}

Author: wzrd

📄 audio.wav

Flag

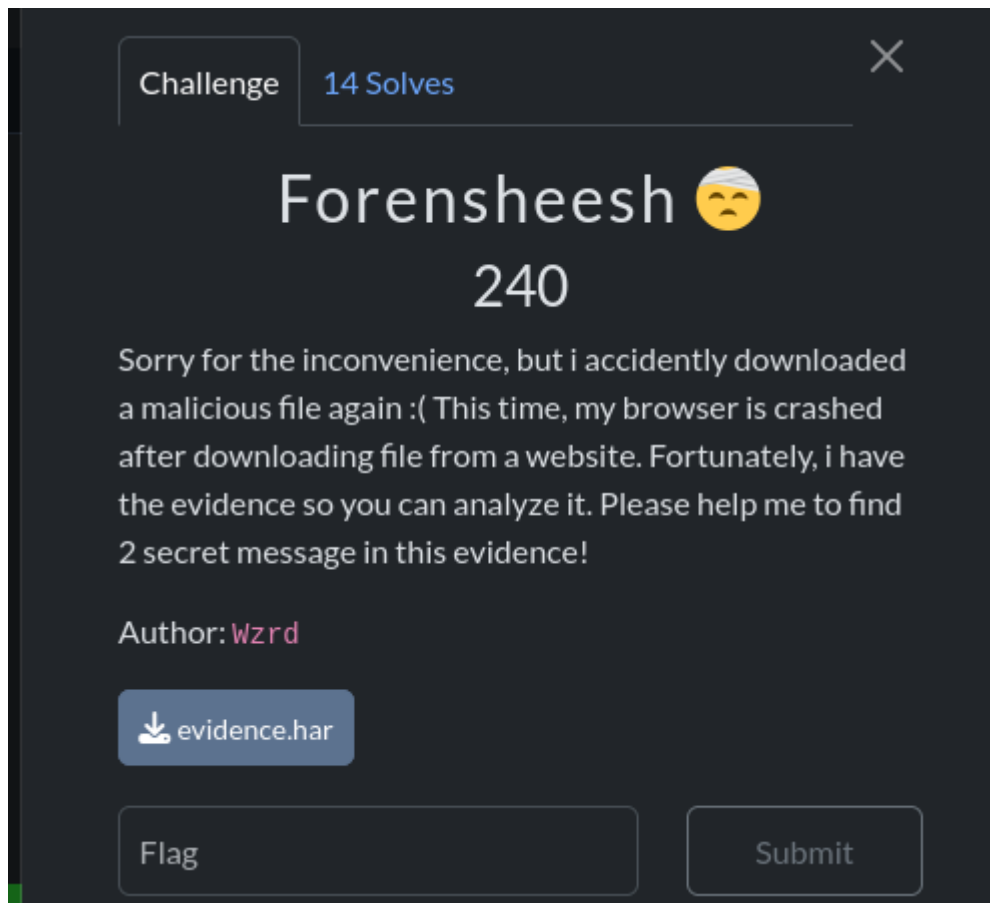
Submit

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

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

Flag : ADIKARACTF{INFODISKONAKHIRTAHUN}

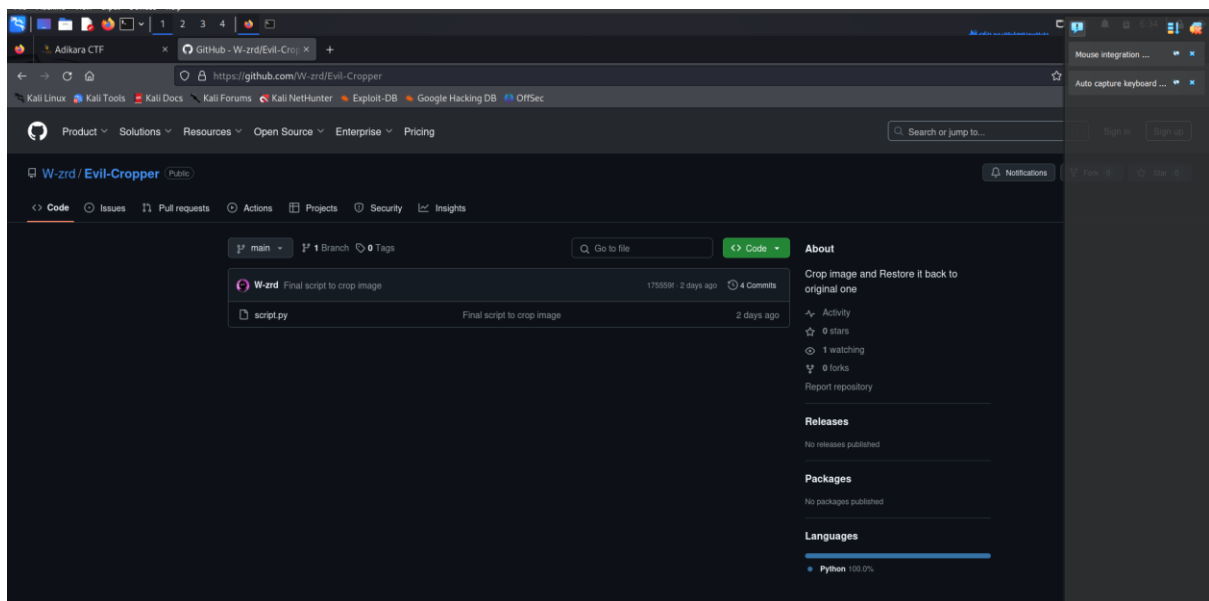
Forensheesh

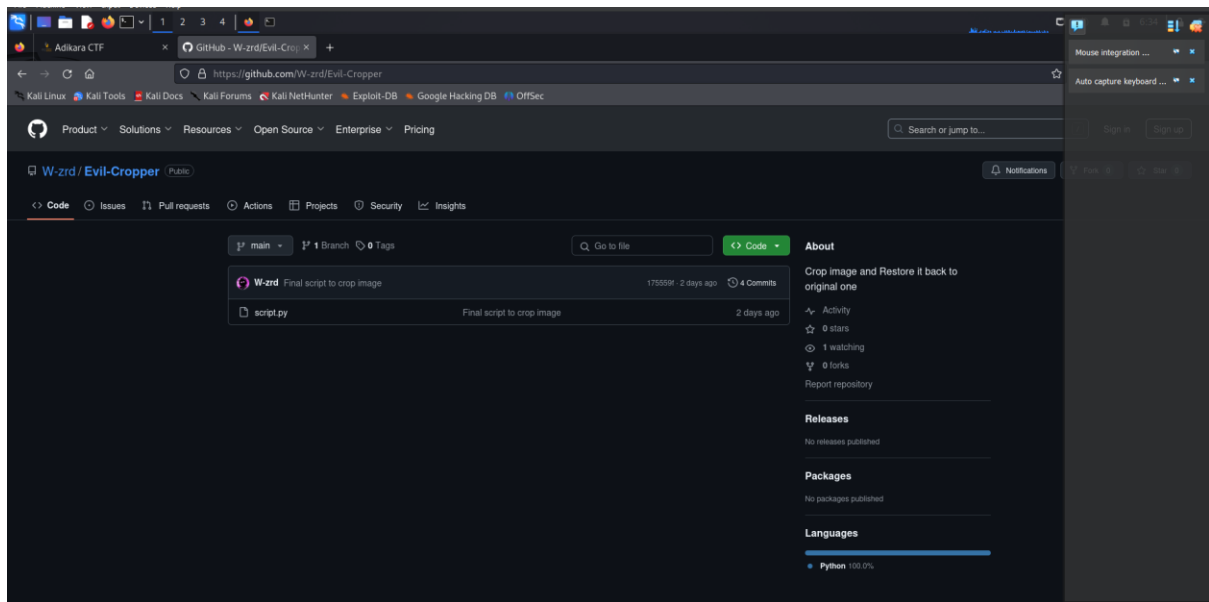


Pada soal ini, diberikan 1 buah file berupa file dengan format har, langsung saya buka saja untuk menganalisanya

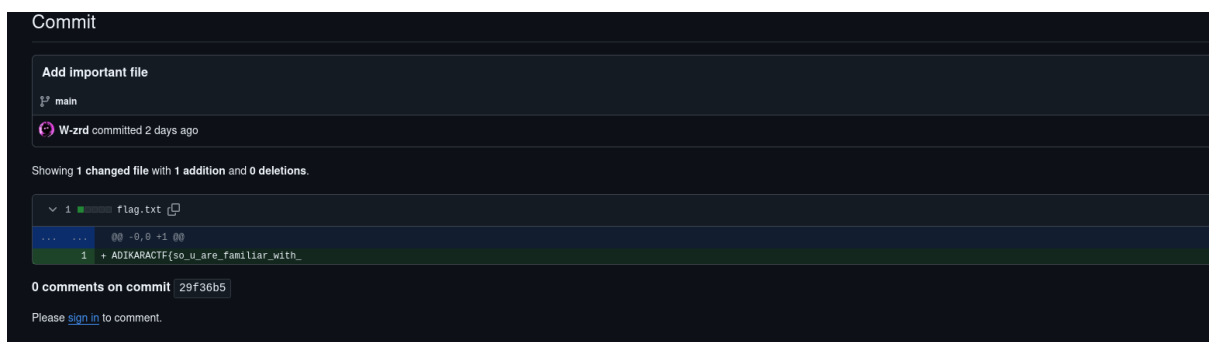
```
File Actions Edit View Help
GNU nano 8.0
{
  "log": {
    "version": "1.2",
    "creator": {
      "name": "WebInspector",
      "version": "537.36"
    },
    "pages": [
      {
        "startedDateTime": "2024-12-19T13:35:30.627Z",
        "id": "page_1",
        "title": "https://github.com/W-zrd/Evil-Cropper",
        "pageTimings": {
          "onContentLoaded": 1556.5420000002632,
          "onLoad": 2750.2620000001385
        }
      }
    ]
  },
}
```

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

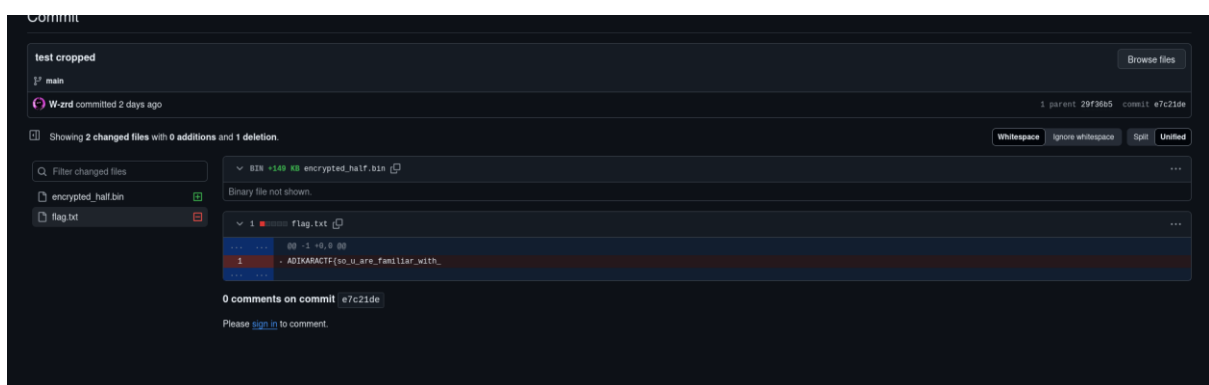




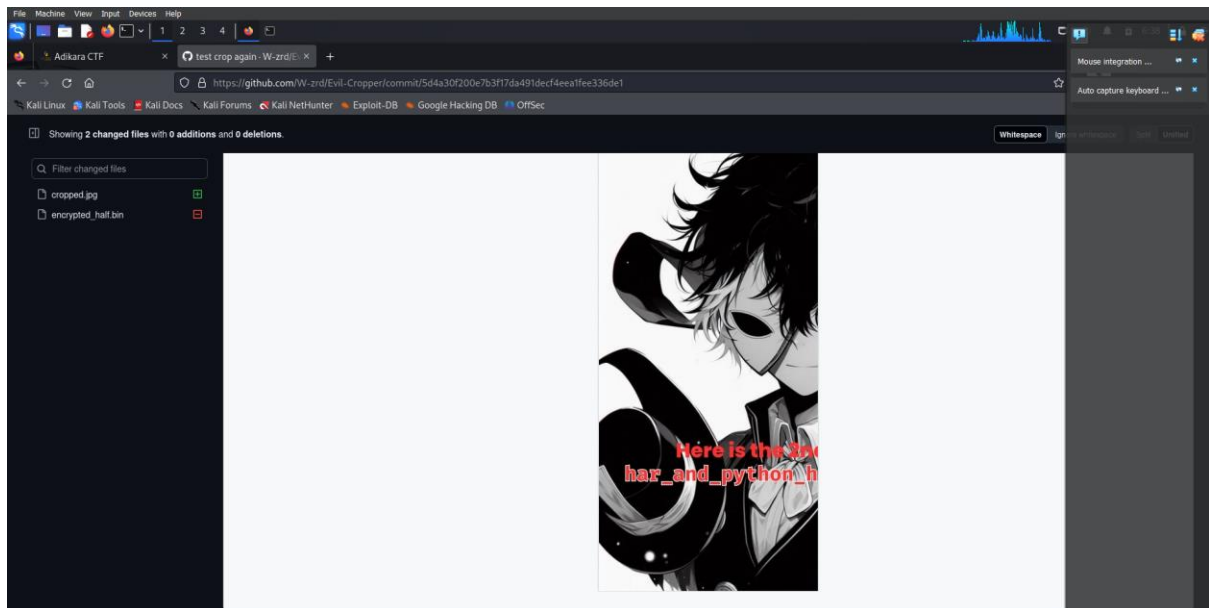
Saya langsung melihat commit histori dan membuka satu persatu untuk menyelesaikan satu satu



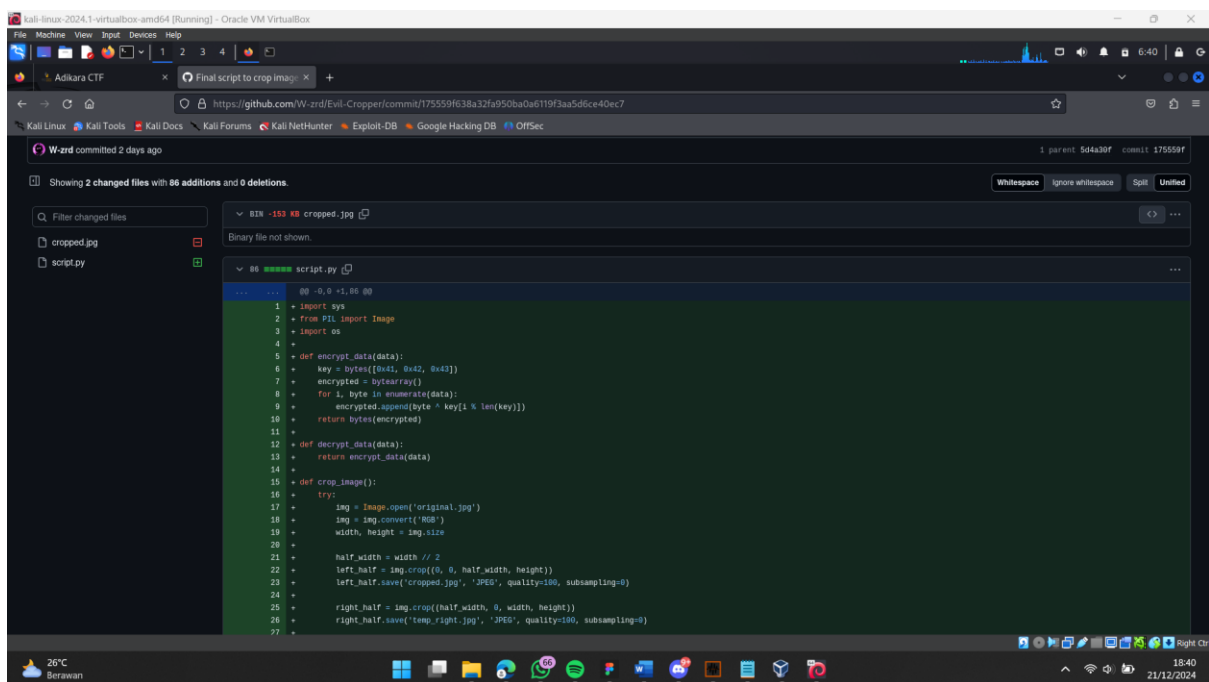
Pada bagian pertama Add important file, saya mendapati potongan flag yaitu **ADIKARACTF{so_u_are_familiar_with_**. Kita tinggal mencari potongan flag lainnya.



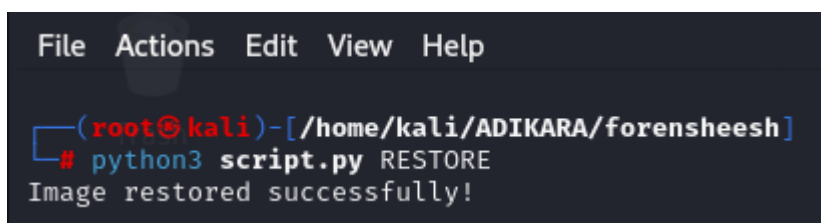
Pada bagian ini, ada file dengan format .bin, sya download apabila dibutuhkan.



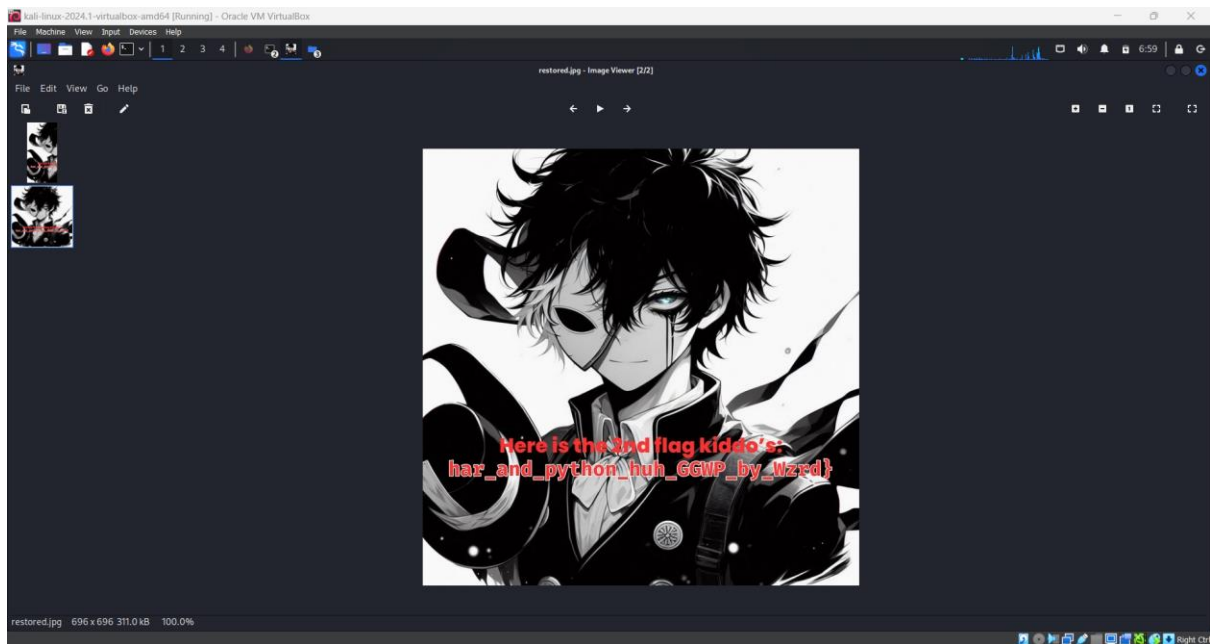
Pada bagian test crop again, saya mendapati cropped image dengan potongan file didalamnya **har_andpython_h**. saya juga mendownload imagenya.



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

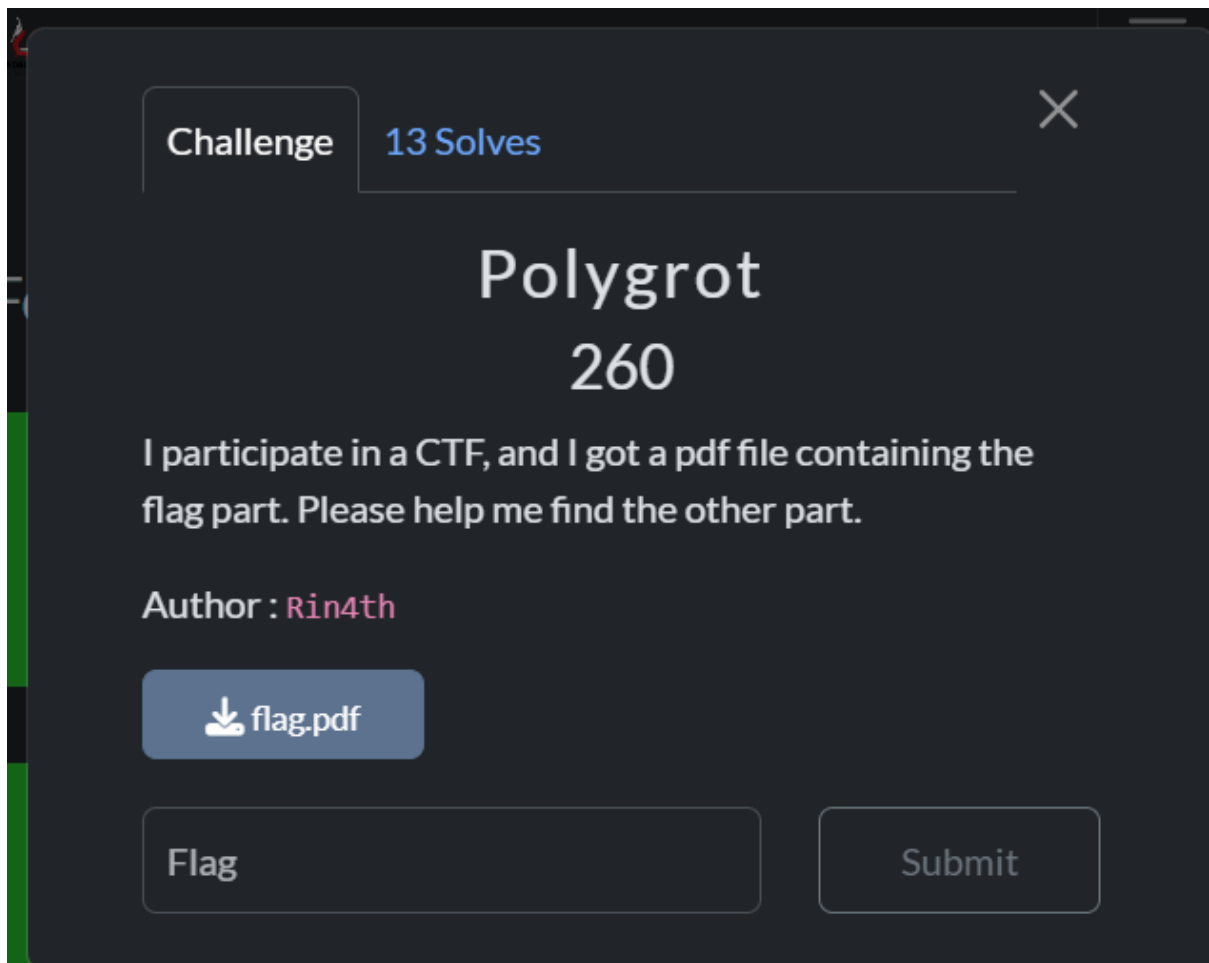


Dan yap, kita dapatkan potongan flag yang lain. `har_andpython_huh_GGWP_Wzrd}`

Kita tinggal gabungkan saja dengan potongan flag sebelumnya

Flag : `ADIKARACTF{so_u_are_familiar_with_har_andpython_huh_GGWP_Wzrd}`

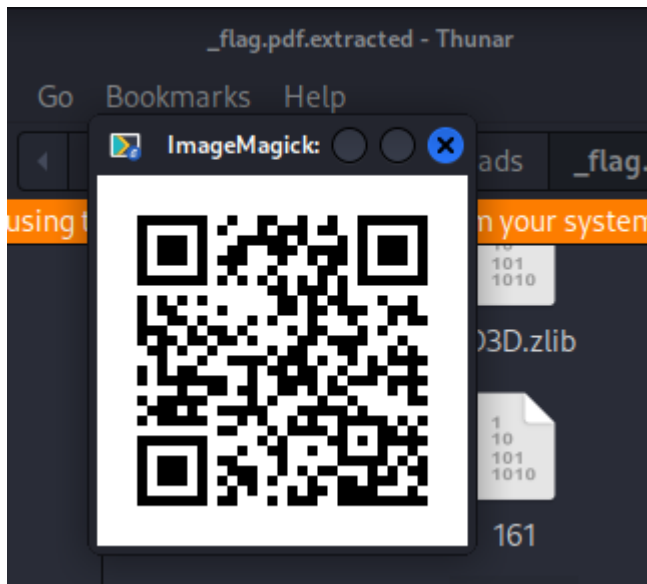
Polygrot



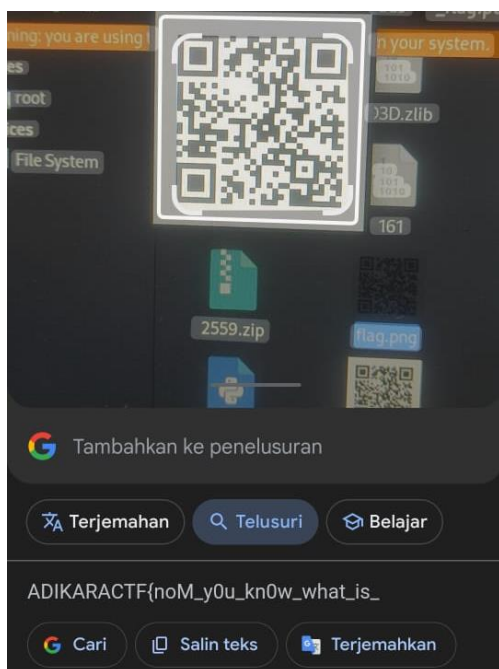
Diberikan challenges seperti berikut. Diberikan 1 buah file dengan format pdf.

polygots?_19adf}

Setelah dibuka terdapat potongan flag `polygots?_19adf}`.



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

Challenge

17 Solves

×

Buffer Overflow #1

180

Can you overwrite the `overflow_me` variable?

`nc 117.53.47.247 50010`

Author: `Moore`

↓ vuln.c

↓ vuln

Flag

Submit

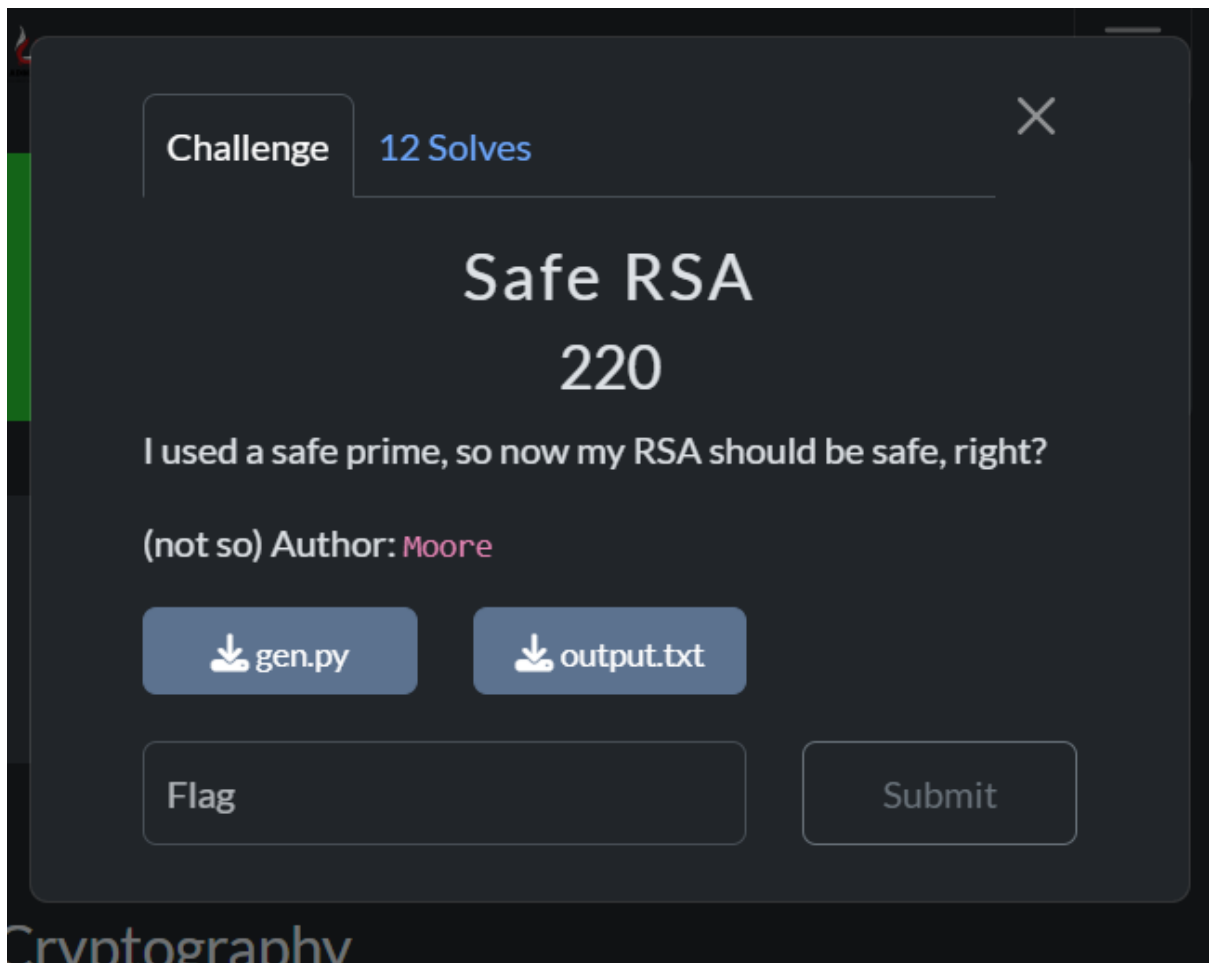
Diberikan sebuah challenge seperti berikut.

```
(root@kali)-[/home/kali/ADIKARA/over1]
# nc 117.53.47.247 50010
1/Downloads/_flag.pdf.extracted
< This is simple buffer overflow vulnerability.
< You have to change value of `overflow_me` variable with this bug.
< On `Buffer Overflow 2` you have to change value to 0xdeadbeef.
< First, `overflow_me` is set to 0x0.< Now, time is yours!
> |ace flag.png? [y]es, [n]o, [A]ll, [N]one, [r]ename: r
new name: mama
inflating: mama
```

Saya langsung connect dan muncul informasi seperti diatas.

Cryptography

Safe RSA



Pada challenge ini kita diberikan 2 buah file.

```
> Users > Fyrza > Downloads > gen.py > ...
1  from Crypto.Util.number import *
2
3  def generate_key():
4      while True:
5          p = getPrime(512)
6          q = 2 * p + 1
7          if isPrime(q):
8              break
9      n = p * q
10     e = 65537
11     d = inverse(e, (p-1)*(q-1))
12     return n, e, d
13
14 n, e, d = generate_key()
15 e = 65537
16
17 flag = open("flag.txt", "rb").read()
18
19 m = bytes_to_long(flag)
20 c = pow(m, e, n)
21
22 print(f"{n =}")
23 print(f"{e =}")
24 print(f"{c =}")
```

Dalam file gen.py terdapat code seperti diatas

```

n = 1414627980887220513187997294909218410456842891295194015074584815518185013457809720501408694397734195717812430836556758035800358255591007769899959974603527546825447848111231493863468518506887
27377614402261954229978269219754312075185083872573296071312565168967164450658906124427063020647048739457948457283284791
e = 65537
c = 958107012020878538417437310931494306555931476834218717992657845675467440270283270060379277568089237428064575166873697240536598014096658094843370465800517857569928714513263102022033874505419
0238905155637221474537758319000878100880684173099253778386118547321637286540549815419269314760633502070855820951147798

```

Dan dalam file output berisi seperti diatas.

```

gen.py 5 factorN.py 1 X
C: > Users > Fyrza > Downloads > factorN.py > ...
1 import math
2
3 n = 14146279808872205131879972949092184104568428912951940150745848155181850134578097205014086943977341957178124308365567580358003582555910077698
4
5 discriminant = 1 + 8 * n
6
7
8 sqrt_disc = int(math.isqrt(discriminant))
9 if sqrt_disc * sqrt_disc == discriminant:
10
11     p = (-1 + sqrt_disc) // 4
12     q = 2 * p + 1
13
14     from sympy import isprime
15     if isprime(p) and isprime(q):
16         print(f"p = {p}")
17         print(f"q = {q}")
18     else:
19         print("p dan q tidak prima.")
20 else:
21     print("Tidak dapat menemukan faktor p dan q.")
22

```

```

PS C:\Users\Fyrza\Downloads> python .\factorN.py
p = 84101961359031945979452537621290226860714543178748530077684118133382987485530203216429576810951971279655223618377812
44778926424658601460559496065941893893
q = 16820392271806389195890507524258045372142908635749706015536823626676597497106040643285915362190394255931044723675562
489557852849317202921118992131883787787
PS C:\Users\Fyrza\Downloads>

```

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

```

> Users > Fyrza > Downloads > gen.py > ...
1 from sympy import mod_inverse
2
3 # Nilai p dan q yang telah ditemukan
4 p = 84101961359031945979452537621290226860714543178748530077684118133382987485530203216429576810951971279655223618377812447789264246586014605594
5 q = 16820392271806389195890507524258045372142908635749706015536823626676597497106040643285915362190394255931044723675562489557852849317202921118
6 n = p * q
7 e = 65537
8
9 # Hitung phi(n)
10 phi_n = (p - 1) * (q - 1)
11
12 # Hitung d
13 d = mod_inverse(e, phi_n)
14
15 # Nilai ciphertext c dari output.txt
16 c = 95810701202087853841743731093149430655593147683421871799265784567546744027028327006037927756808923742806457516687369724053659801409665809484
17
18 # Dekripsi ciphertext
19 m = pow(c, d, n)
20
21 # Ubah hasil dekripsi m kembali menjadi bytes dan kemudian menjadi string
22 from Crypto.Util.number import long_to_bytes
23 flag = long_to_bytes(m)
24
25 # Menampilkan flag
26 print(f"Flag: {flag.decode()}")
27

```

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


```
489557852849317202921118992131883787787  
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

Challenge

7 Solves

×

Blaze

380

I've built a website, but now I'm locked out because I forgot the password. The source code is gone, deleted. Can you recover it from the compiled program and regain access?

Password: 421eecef54272d94ab2e34b76db68245

<http://117.53.47.247:40010/>

Author: b133dz

📄 blaze-src.zip

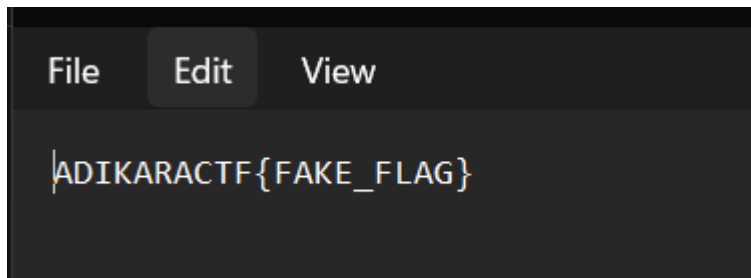
Flag

Submit

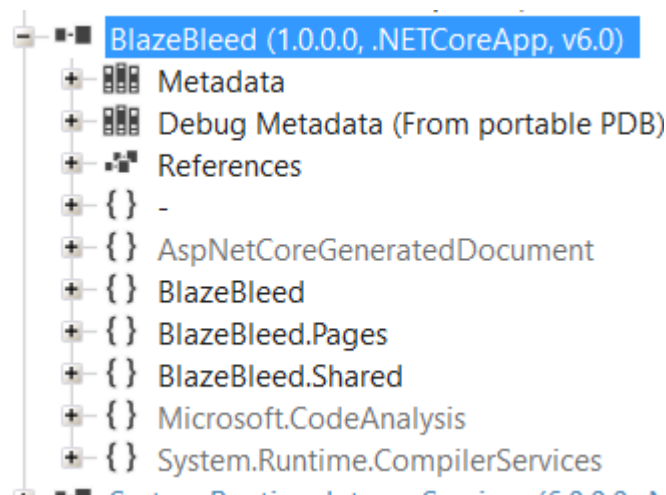
Diberikan file dengan format zip.

Name	Date modified	Type	Size
src	21/12/2024 18:18	File folder	
docker-compose.yml	26/11/2024 14:10	Yaml Source File	1 KB
Dockerfile	26/11/2024 14:11	File	1 KB
flag.txt	26/11/2024 14:11	Text Document	1 KB

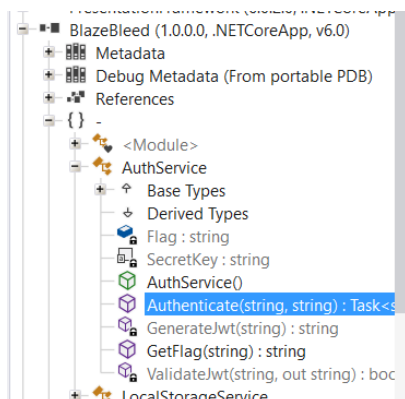
Setelah diextract, terdapat folder seperti diatas dan kita langsung mendapatkan flagnya.



scam bjirrrr.\



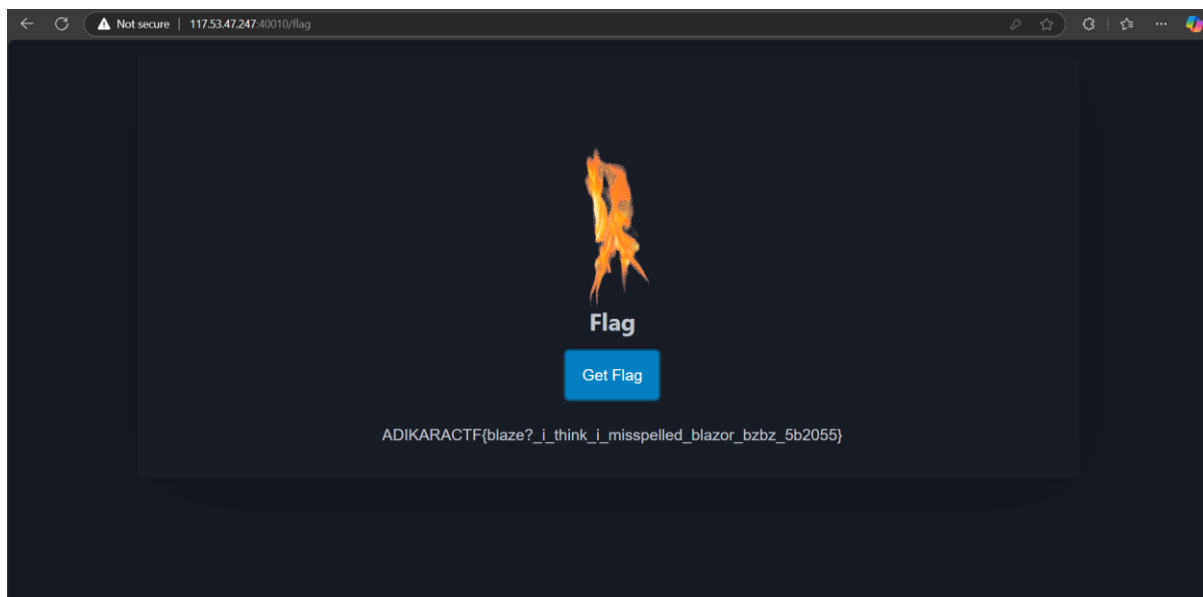
Saya analisis file didalam BlazeBleed.dll dengan menggunakan tools ILSpy, salami terus codenya, bac abaca,cari Dimana kiranya code penting disimpan.



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



akhirnya saya dapatkan ussurnamenya yaitu “admin” dan passwordnya yaitu “isitjustmyimagination?”. Dan saya coba login menggunakan usrnane dan pw tersebut.



Dan yap, kita dapatkan flagnya.

Flag : ADIKARACTF{blaze?_i_think_i_misspelled_blazor_bzbz_5b2055}