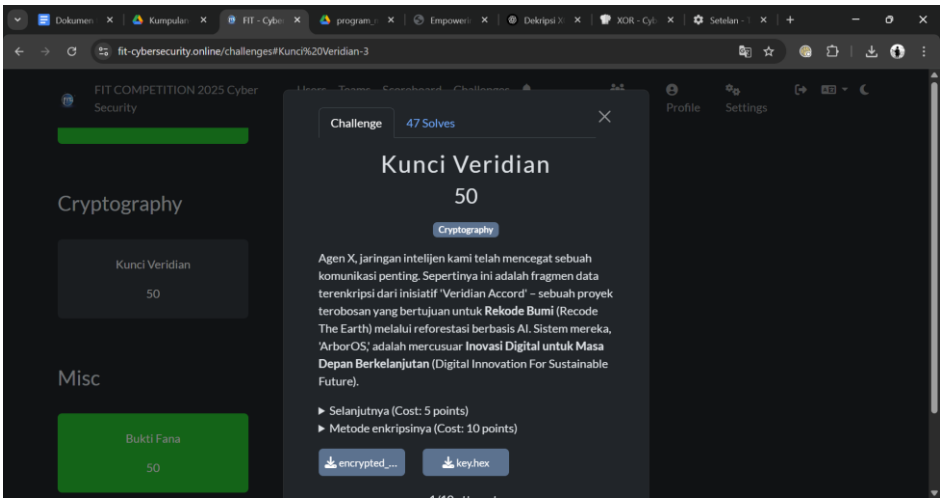
WRITE UP CTF

FIT COMPETITION 2025 :>

Nama Tim : mas yaya tolong rambutnya di kuncir

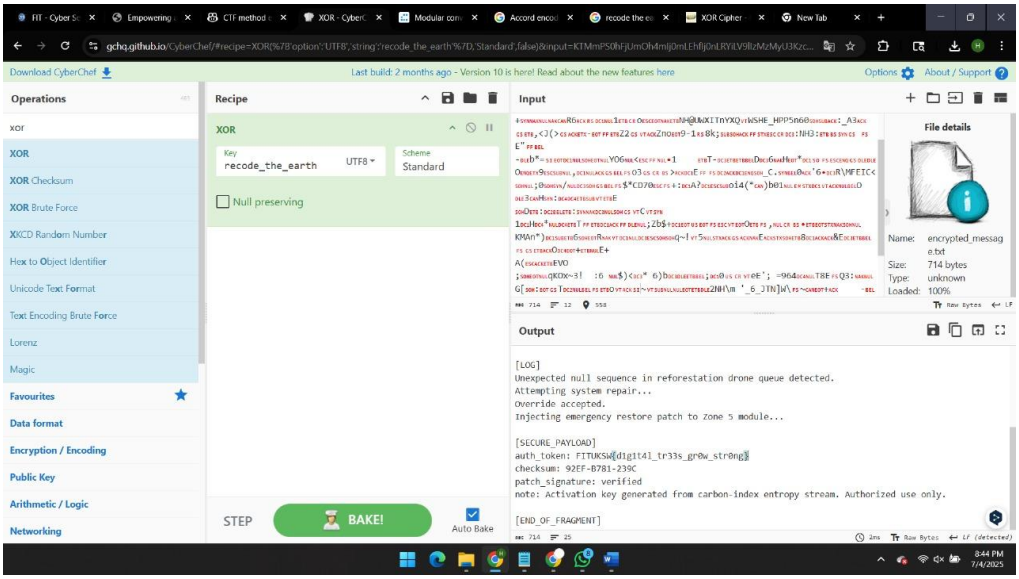
1. [Crypto] Kunci Veridian



Tugas kita adalah mendekripsi pesan tersebut menggunakan file key.hex dan encrypted_message.
Langkah penyelesaian:

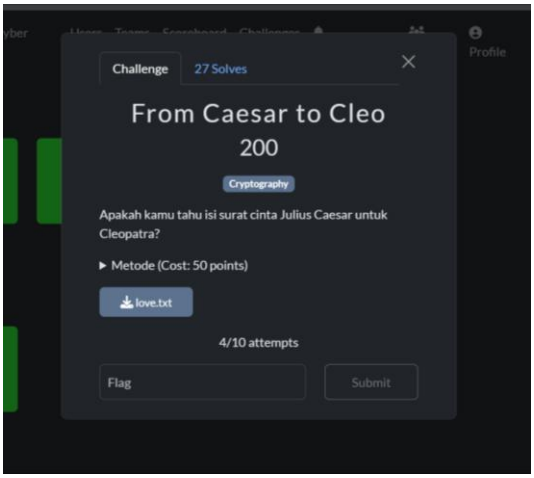
- Deskripsi file key.hex di CyberChef menggunakan operasi **From Hex** dan diperoleh hasil: **recode_the_earth**

- Kemudian unggah file encrypted_message ke CyberChef menggunakan operasi **XOR** dengan kunci yang sudah di dapatkan tadi



- Dan dari hasil deskripsi ditemukan flag: **FITUKSW{d1g1t4l_tr33s_gr0w_str0ng}**

2. [Crypto] From Caesar to Cleo



Diberikan file love.txt yang berisi pesan panjang terenkripsi.Tugas kita adalah mendekripsi isi surat menggunakan metode kriptografi klasik.
langkah penyelesaian:

- Langkah pertama, Kami menggunakan tool dcode.fr dan memilih metode Caesar cipher, Hasil analisis menunjukkan bahwa baris pertama menggunakan Caesar cipher dengan shift mundur 3 huruf: Pb ehoryhg Fohrsdwud → My beloved Cleopatra

- flag ditemukan:
  - find_the_key_of_success_relationship
  - if_you_failed_in_love_take_a_second_chance

- Pada bagian berikutnya terdapat petunjuk: "three steps at a time—but the next will dance in a pattern of 1 to 5"
  Artinya, setiap huruf dienkripsi menggunakan pola shift mundur: 1, 2, 3, 4, 5 secara berulang.

- Setelah proses dekripsi dengan pola tersebut, didapat: Uq qd gwiwoco qpxh → To my eternal love

- Flag ditemukan:
  - you_almost_there
  - the_key_is_TRUST
- Petunjuk selanjutnya, "Let TRUST guide you through the final cipher." Ini menunjukkan penggunaan metode Vigenère cipher dengan key = TRUST.

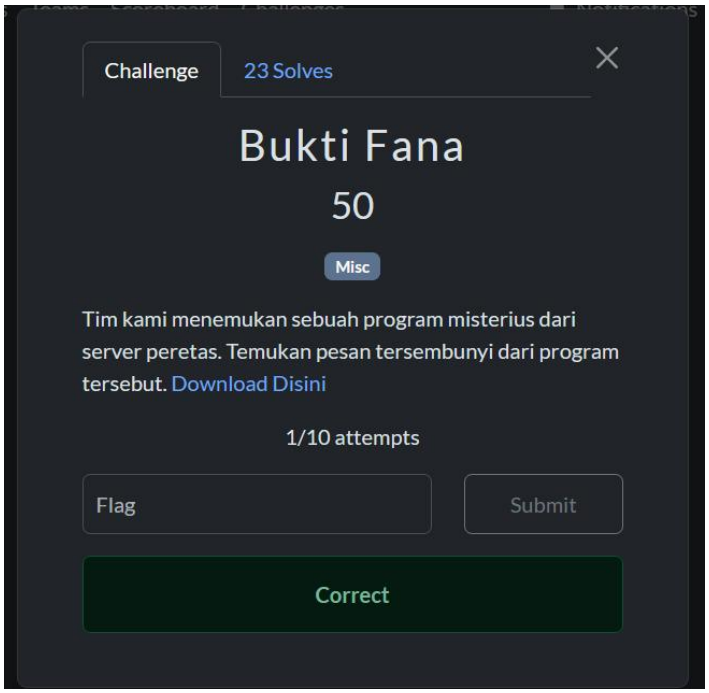
- Setelah didekripsi, teks menjadi: My radiant queen,

The golden sands of Egypt guard our secrets...

- Flag ditemukan:
  - if_you_arrive_here_you_will_get_it
  - vigenere_for_everlasting_love

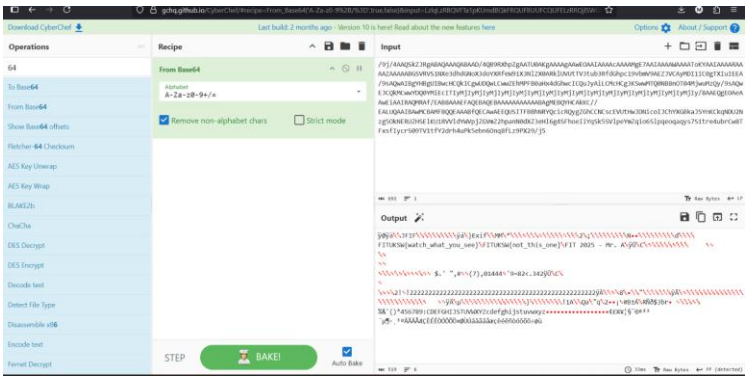
- Flag: **FITUKSW{vigenere_for_everlasting_love}**

3. [Misc] Bukti Fana



Langkah penyelesaian:

- Download File Program yang disediakan di deskripsi soal.
- Setelah dijalankan, program tersebut menunjukkan log aktivitas pada terminal, dan menghasilkan file log dengan nama:`arboros_20250704_203138.log`
- Kami membuka file log tersebut, dan menemukan bagian [DATA] ss_data = yang diikuti oleh string panjang yang terlihat seperti data yang dienkode dalam format **Base64.**
- kami deskripsi menggunakan tool CyberChef menggunakan operasi **From Base64**



- Dari hasil deskripsi diperoleh flag: **FITUKSW{watch_what_you_see}**

4. [Misc] ThePowerOfLogs

Langkah penyelesaian:

- Disedikan file bernama printer_log.txt, dan ketika dibuka file tersebut berisi deretan entri log yang memiliki format seperti ini: `[IO_TRACE] Packet received with tx=423, ty=875, packet=0x7f0000`

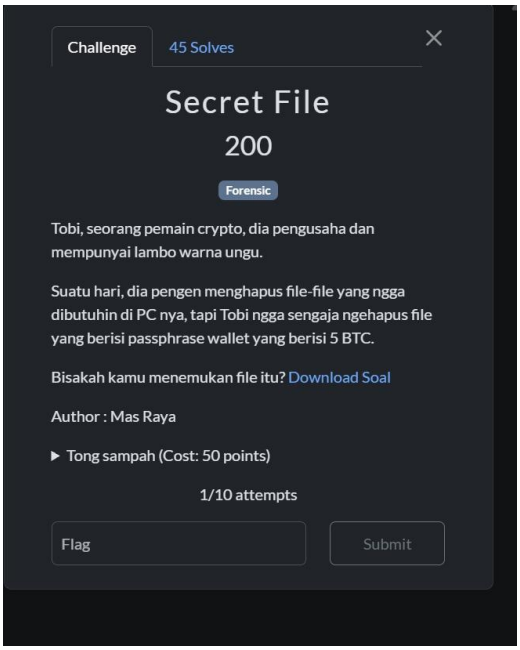
- Dari ini kami bisa simpulkan bahwa setiap baris mewakili sebuah titik piksel (tx dan ty adalah koordinat X dan Y pada gambar, packet adalah nilai warna dalam format heksadesimal 0xRRGGBB)

- kemudian kami gunakan script python untuk membaca koordinat dan warna dari log, lalu menyusun ulang menjadi gambar berukuran 1024x1024 piksel.

- hasil akhirnya disimpan sebagai file hasil_render.png, isinya berupa gambar yang didalanya ada QR code:

- Setelah melakukan pemindaian terhadap QR code tersebut, diperoleh flag: **FITUKSW{r3c0d3_th3_34rth_1s_3451}**

5. [Forensic] Secret File



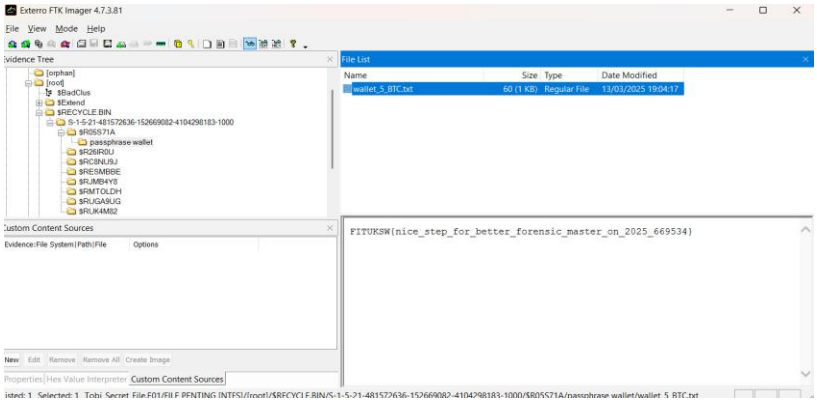
Tugas kita adalah menemukan kembali file yang terhapus tersebut dari file forensik disk image yang diberikan (Tobi_Secret_File.E01)
Langkah penyelesaian:

- Buka file yang sudah dicantumkan pada deskripsi soal menggunakan tool FTK Imager, pilih File > Add Evidence Item, lalu tambahkan file Tobi_Secret_File.E01

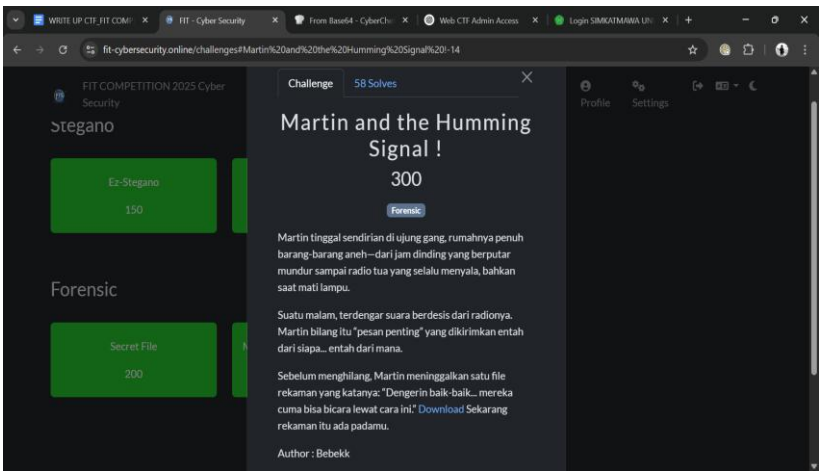
- pada panel kiri, navigasikan ke: `$RECYCLE.BIN > S-1-5-21-...-1000 > $R05571A`

- Di dalamnya terdapat folder **passphrase wallet,** kemudian buka file wallet_5_BTC.txt

- Dan ditemukan flag:
FITUKSW{nice_step_for_better_forensic_master_on_2025_669534}



6. [Forensic] Martin and the Humming Signal

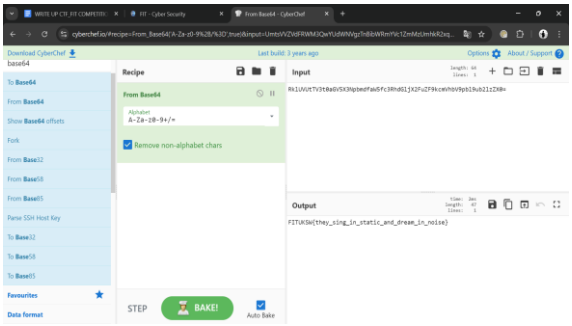


Langkah penyelesaian:

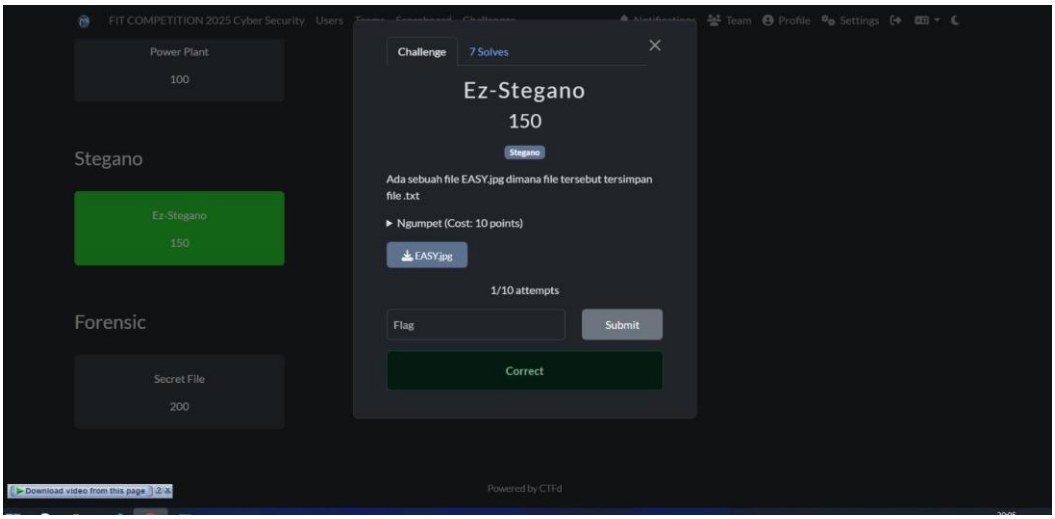
- Unduh file hummingsignal.wav dari deskripsi soal
- File tersebut kami buka menggunakan software Audacity
- Petunjuk pada soal menyebutkan: *"Martin always preferred 'M1'"*. Ini mengarah pada mode Martin M1, yaitu salah satu mode dalam komunikasi SSTV (Slow-Scan Television)
- Kami menggunakan aplikasi MMSSTV (Windows) sebagai dekoder SSTV
- hasilnya menampilkan sebuah QR code:

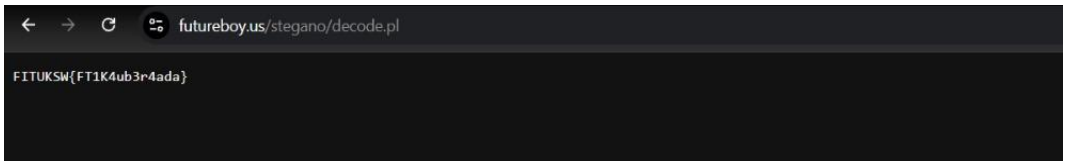
- setelah kami scan QR tersebut muncul pesan terenskripsi: RklUVUtTV3t0aGV5X3NpbmdfaW5fc3RhdGljX2FuZF9kcmVhbV9pbl9ub2lzZX0=

- kami deskripsi menggunakan Cybechef base64, dan hasilnya adalah flag:**FITUKSW{they_sing_in_static_and_dream_in_noise}**



7. [Stegano]Ez-Stegano





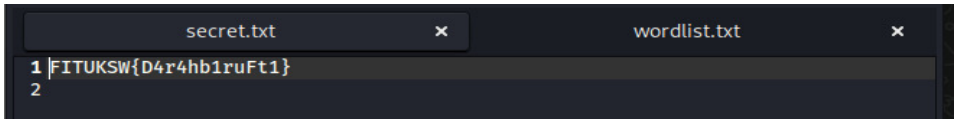
Langkah-langkah:

- Terdapat sebuah file gambar bernama EASY.jpg yang di dalamnya tersimpan sebuah file.txt
- Unduh file EASY.jpg yang disediakan oleh challenge
- kami menggunakan tools online futureboy.us untuk mengekstrak data tersembunyi dalam file gambar
- Hasil diperoleh sebuah flag: **FITUKSW{FT1K4ub3r4ada}**

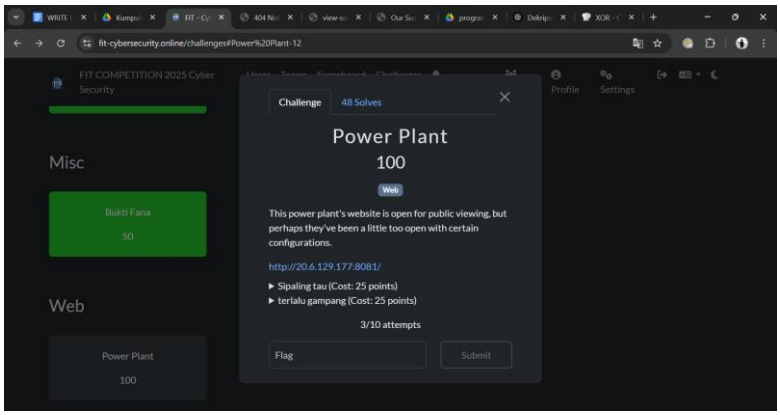
8. [Stegano] Med-Stegano

Langkah penyelesaian:

- Buka soal dan unduh file MEDIUM.jpg
- Dari deskripsi soal, kami mengetahui bahwa terdapat file .txt tersembunyi dalam gambar tersebut
- Kami mencoba mengekstrak file menggunakan steghide dengan beberapa tebakan password: menyesal, pasti, MenyesalPasti, ctf, fitctf, FITUKSW, dll, namun tetap tidak berhasil
- Karena file dikunci, kami memutuskan untuk melakukan brute force, kami install package wordlists
- Kemudian jalankan script `steghide_brute.py` untuk mencoba password dari wordlist secara otomatis
- Setelah beberapa saat, script berhasil menemukan password dan mengekstrak file secret.txt.
- Kami buka file secret.txt dan menemukan flag: **FITUKSW{D4r4hb1ruFt1}**



9. [Web]Power Plant



Langkah penyelesaian:

- Kami memulai dengan mengakses http://20.6.129.177:8081/robots.txt File tersebut mengungkap adanya path tersembunyi: /secret_code.txt

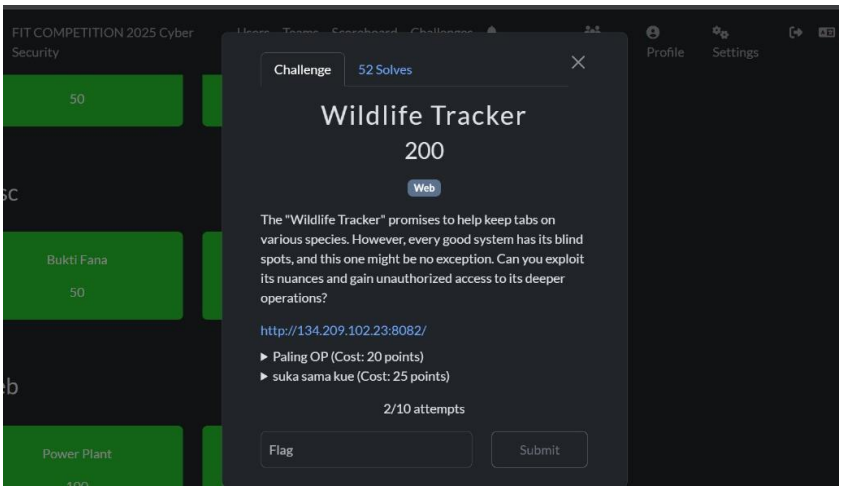
- Kami mencoba langsung mengakses http://20.6.129.177:8081/secret_code.txt, namun file tersebut menampilkan pesan Not Found

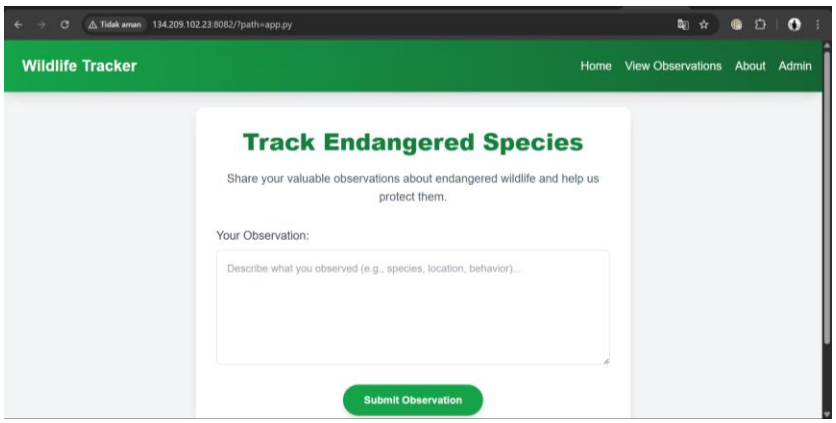
- Selanjutnya, kami melakukan inspeksi elemen pada halaman utama dan menemukan bahwa gambar situs berada di direktori /static/images/power_plant.png. Ini menandakan kemungkinan ada direktori /static/ yang dapat diakses secara langsung

- Berdasarkan temuan tersebut, kami mencoba membuka http://20.6.129.177:8081/static/secret_code.txt

- Akses berhasil, dan kami menemukan flag: **FITUKSW{b3_ec0_fr13ndly}**

10. [Web] Wildlife Tracker





Langkah penyelesaian:

- Kami mengakses website utama dan menemukan menu seperti *Home*, *View Observations*, *About*, dan *Admin*

- Saat mengklik Admin, kami diarahkan ke halaman otentikasi, namun tidak ada respon error saat mengisi kredensial acak – kami curiga autentikasi menggunakan token, bukan sistem login biasa.

- Kami mulai mencoba eksploitasi LFI dan berhasil mengakses `.env` file menggunakan: http://134.209.102.23:8082/?read_file=.env
- Di dalam file `.env`, kami menemukan `SECRET_KEY=wildlife-2025-fit-challenge-secret`

- Kami menduga ini adalah secret untuk JWT (JSON Web Token)

- Setelah itu, kami mencoba membaca file lain dengan LFI dan menemukan bahwa app.py dapat diakses melalui: http://134.209.102.23:8082/?read_file=app.py

- Dari isi app.py diketahui cookie harus admin_token dan Payload admin harus mengandung: {"role": "admin",
  "authorized": true}

- kami membentuk JWT dengan payload:

- Token ini kami tambahkan ke browser sebagai cookie bernama admin_token

- Refresh halaman /admin_dashboard, dan kami berhasil masuk dihalaman admin kami temukan string encoded:
  RklUVUtTV3tiMTBkMXYzcnNxdHlfMW5fdGgzX3cxbGR9Cg==

- Langsung kami deskripsi menggunakan Cyberchef base64 dan hasilnya adalah flag: **FITUKSW{b10d1v3rsqty_1n_th3_w1ld}**