Write Up WRECK-IT 6.0

Junior Qualifier

Team 3xplo1t3r

Team Members:

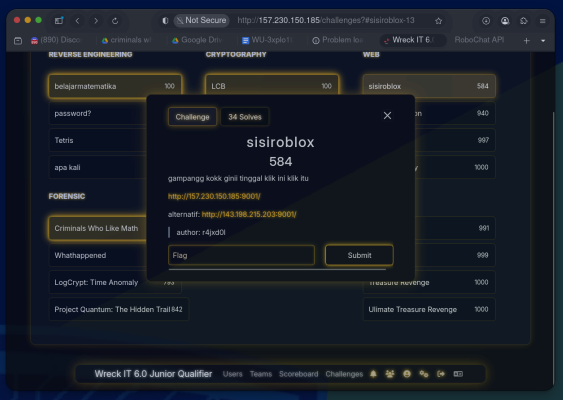
Rayhan (Rosemary1337)

Rado (Frigg1337)

Table of Contents

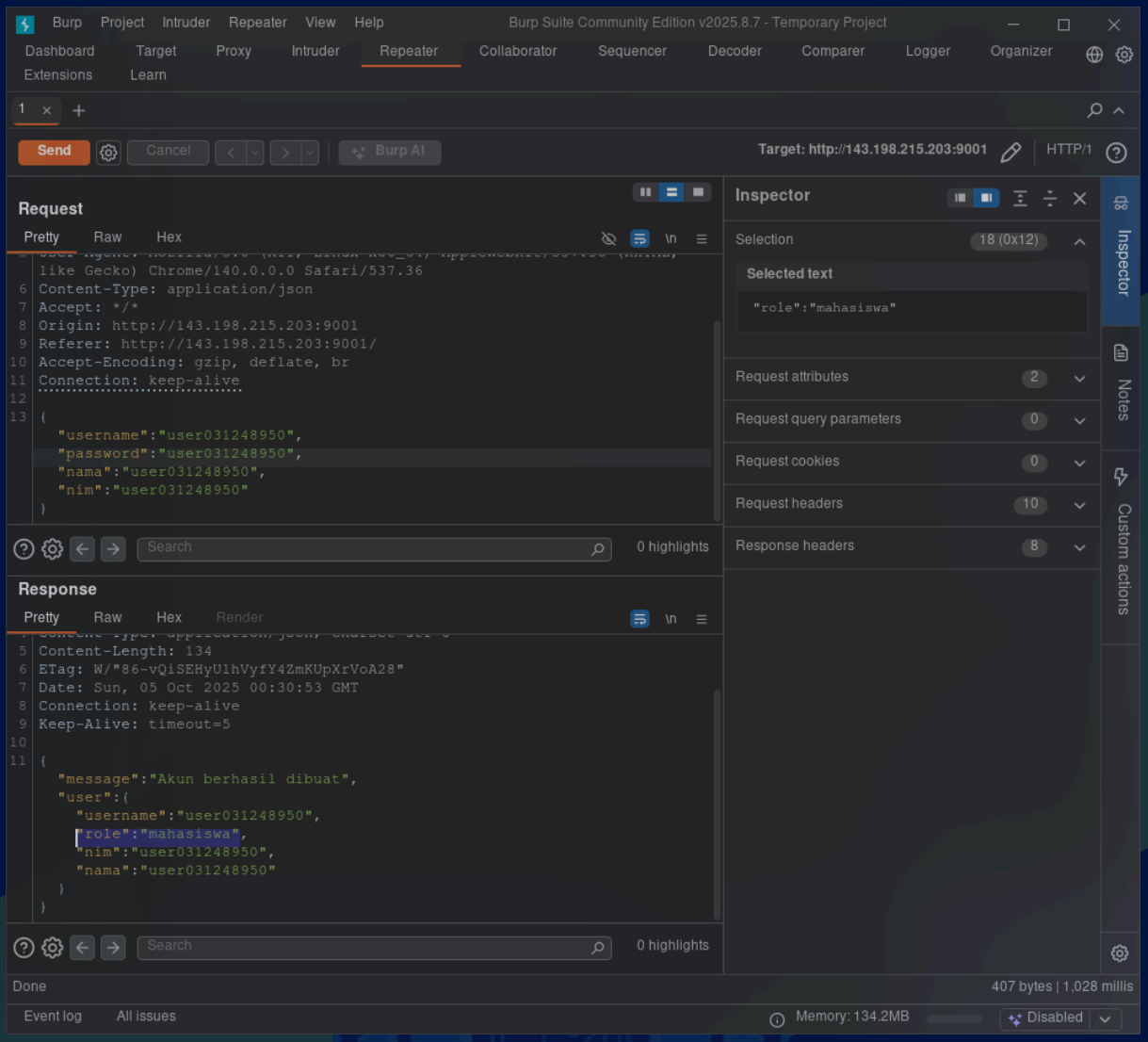
Web Exploitation

Sisiroblox

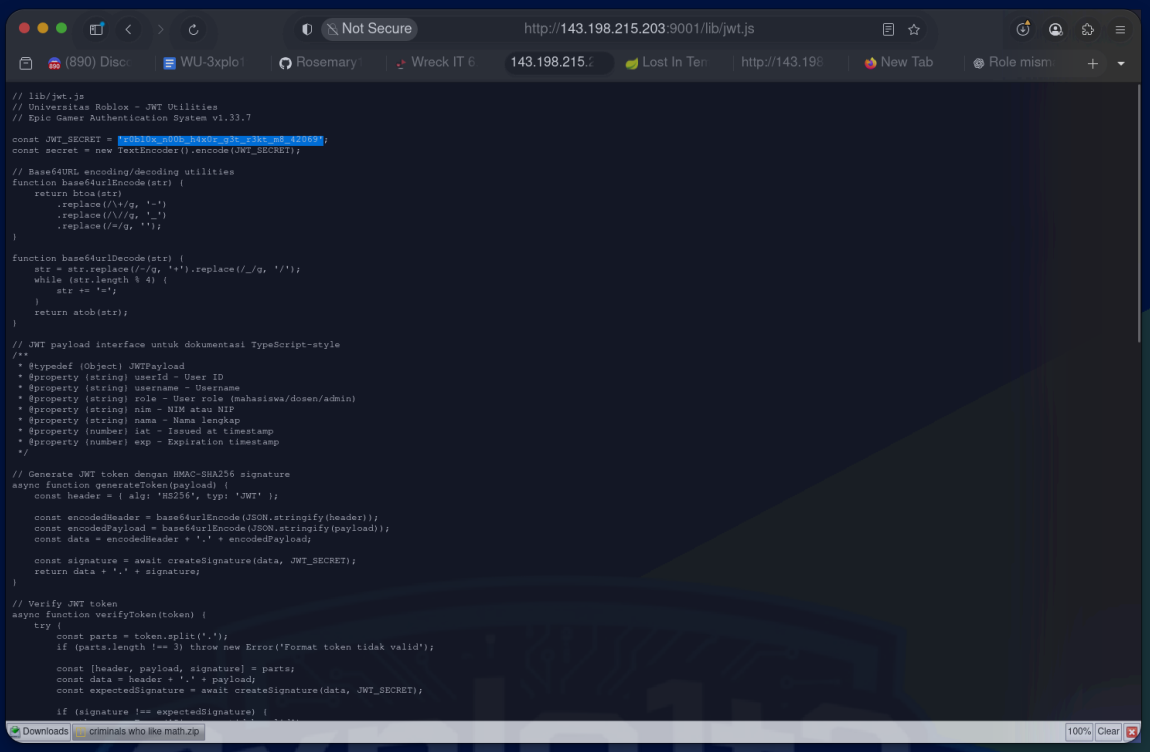


Solution

Disini saya diberikan website berjudul "SIAKAD Noobmaster69" saya explore websitenya, setelah saya explore beberapa menit ternyata jalan untuk menemukan flag sepertinya adalah register dan login, pertama saya coba SQLi dengan menggunakan beberapa payload milik saya, ternyata tidak bisa. Lanjut saya coba untuk register dan memeriksa requestnya via Repeater(Burpsuite), nah di Responsenya ada yang sedikit aneh, disini saya menemukan "role":"mahasiswa", tetapi saat Requestnya tidak ada role apapun



Kemudian saya ganti rolenya manual ke “dosen” dan “admin”, ternyata tidak bisa, saya telusuri ternyata ada path /lib/jwt.js yang digunakan untuk JWT Token



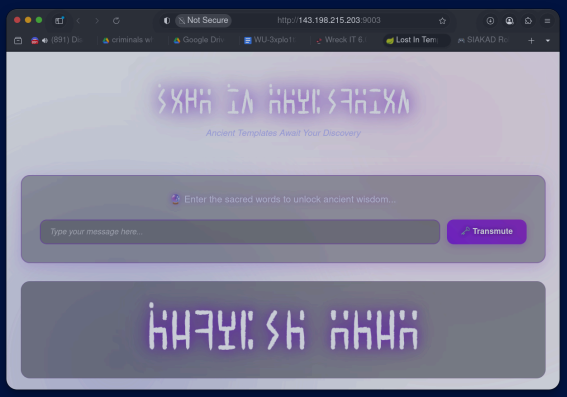
Nah sepertinya dari sini, kalau mengubah role tanpa jwt itu tidak bisa, kemudian saya buat token admin melalui script python, berikut source codenya:

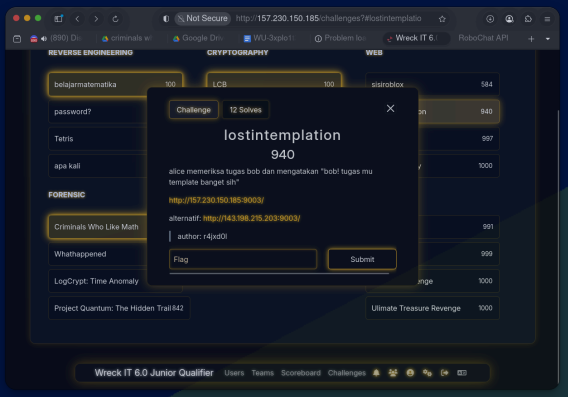
```python
import jwt
import time

SECRET = "r0bl0x_n00b_h4x0r_g3t_r3kt_m8_42069"

payload = {
    "userId": “R1337_2",
    "username": "Rosemary1337",
    "role": "admin",
    "nim": "0000",
    "nama": "Rosemary1337",
    "iat": int(time.time()),
    "exp": int(time.time()) + 3600
}

token = jwt.encode(payload, SECRET, algorithm="HS256")
print("[+] Token admin valid:")
print(token)
```

Dari script ini saya mendapatkan token admin, lalu saya kirim request manual ke path yang memungkinkan, misal ke /api/manage/users yang biasanya digunakan di web lainnya, lanjut menggunakan curl:
curl -H "Authorization: Bearer

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOiJhZG1pbi0xMjM0Iiw
idXNlcm5hbWUiOiJhZG1pbiIsInJvbGUiOiJhZG1pbiIsIm5pbSI6IjAwMDAiLCJuYW1
hIjoiQWRtaW5pc3RyYXRvciIsImlhdCI6MTc1OTU3NTYwOSwiZXhwIjoxNzU5NTc5MjA
5fQ.rEJQctzTazfpQ8JUd-21Vw1rE__6zOGBNgC7LfWmPlY"
http://143.198.215.203:9001/api/manage/users
Ternyata responsenya mengembalikan ke html awal bukan json, mungkin disini tokennya salah/gimana saya juga kurang tahu, karena biasanya di real website itu bisa. Sempat saya coba beberapa kali, sambil menunggu website challenge down 504. Saya coba -+ 10 menit menunggu website challenge up, dan disini ga dapet apa apa hehehe,
selanjutnya saya skip dan ganti ke challenge lainnya.

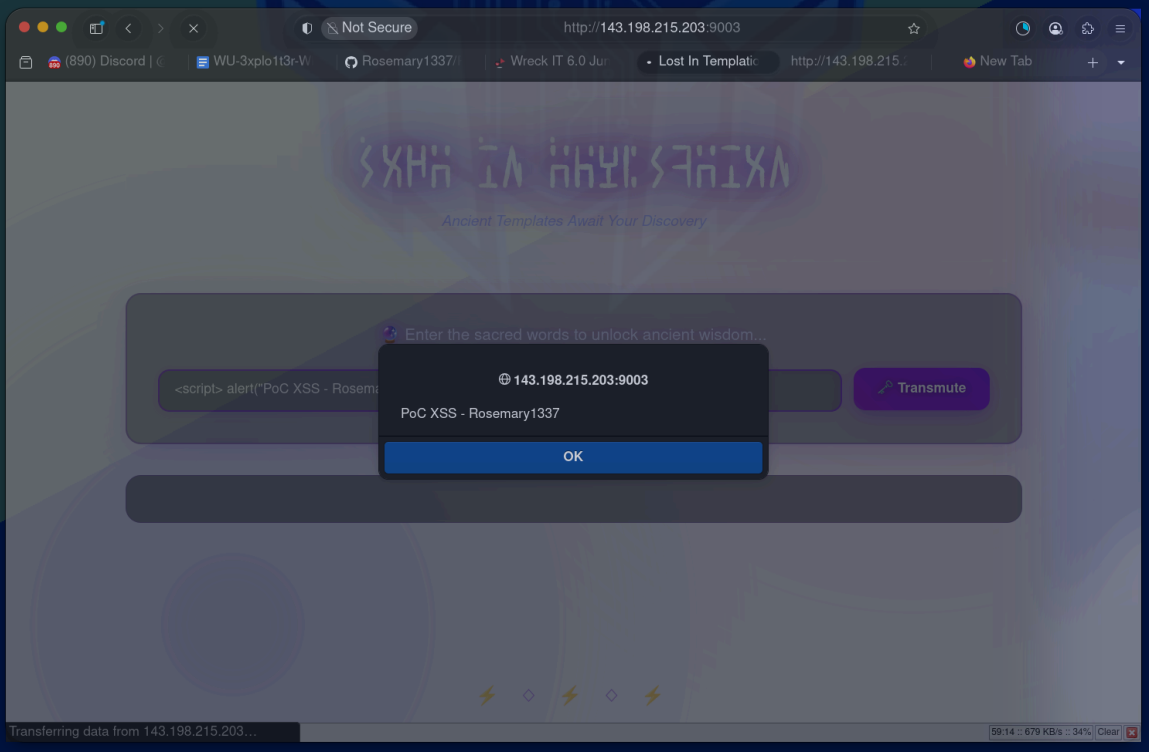
Lostintemplation





Solution

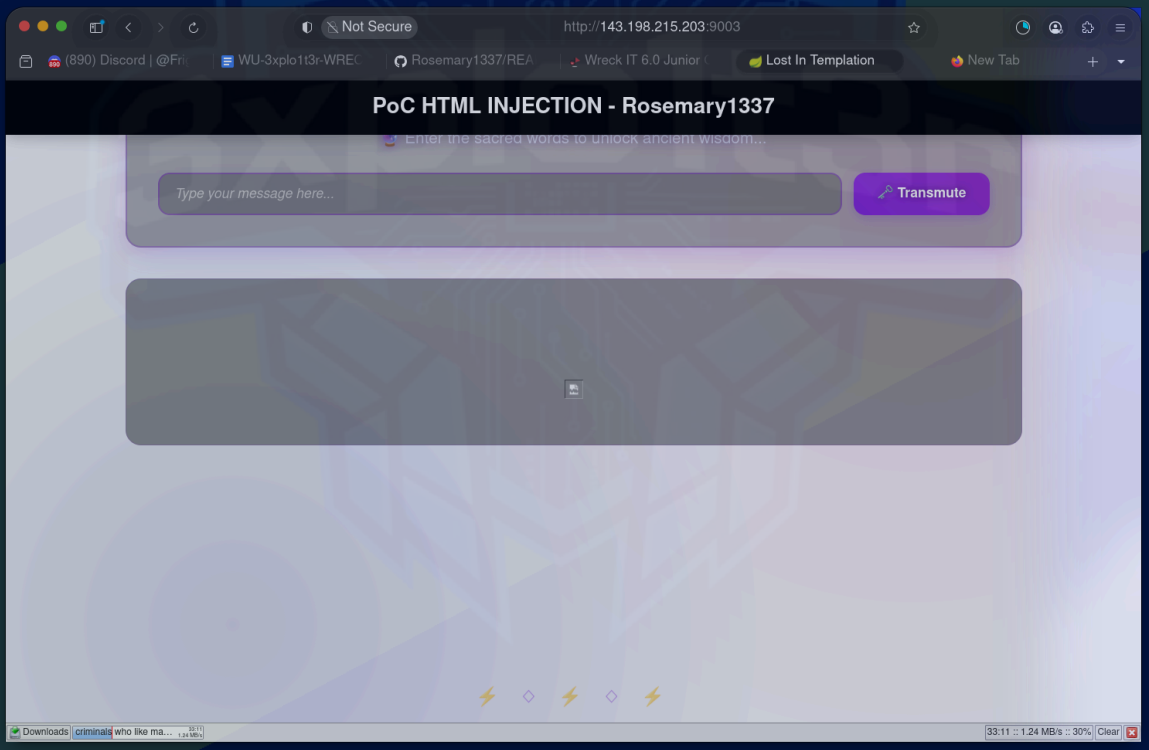
Jadi disini diberikan suatu website dengan ip dan port tertera di gambar, jadi website itu menampilkan teks sesuai yang kita input, misal input “test” outputnya juga “test” hanya saja beda font, dari sini saya iseng masukin payload basic XSS dan ternyata valid XSS dengan memakai payload: <script> alert("PoC XSS - Rosemary1337");</script>



Kemudian saya coba beberapa payload, tetapi tidak ada yang bisa

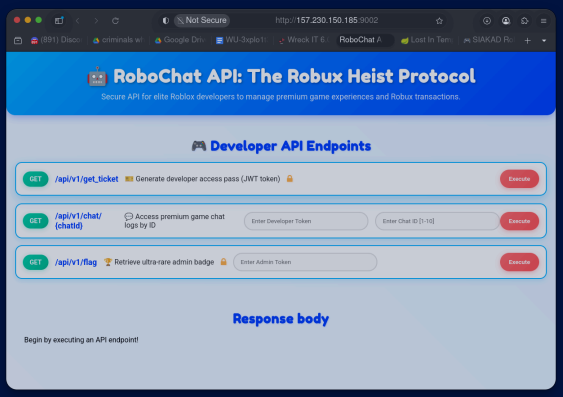
melihat dimana letak “flag” nya, jadi saya coba pakai payload lain, pertama saya pakai payload HTML Injection, dan ternyata valid juga pakai payload:

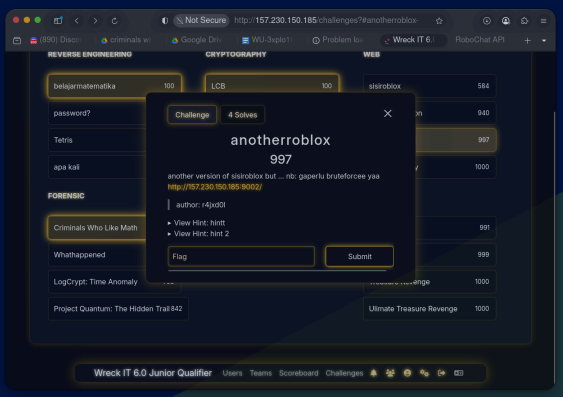
```
<img src=x onerror="document.querySelectorAll('header, nav,
.sidebar, .ads,
.cookie-banner').frgba(0,0,0,0.25)';b.textContent='PoC HTML
INJECTION -
Rosemary1337';document.body.prepend(b);window.scrollTo(0,0);"></h2>o
rEach(n⇒n.style.display='none');document.body.style.paddingTop='0';
var
b=document.createElement('div');b.style.cssText='position:fixed;left
:0;right:0;top:0;z-index:999999;padding:18px;text-align:center;font-
size:28px;font-weight:800;background:black;color:white;box-shadow:0
4px 20px rgba(0,0,0,0.25)';b.textContent='PoC HTML INJECTION -
Rosemary1337';document.body.prepend(b);window.scrollTo(0,0);">
```



dan saya coba lagi beberapa payload milik saya, ternyata sama juga, tidak ada yang bisa menemukan lokasi flag, lalu saya coba payload umum SSTI dan tidak ada yang valid, sampai disitu saya coba lagi beberapa payload yang sudah saya kumpulkan dari Write Up orang orang di medium, saya coba satu satu ternyata tetap tidak ada yang valid. Sampai disini saya skip challenge ini dan pindah ke challenge lain karena sudah -+ 20 menit saya coba di chall wkwkwk

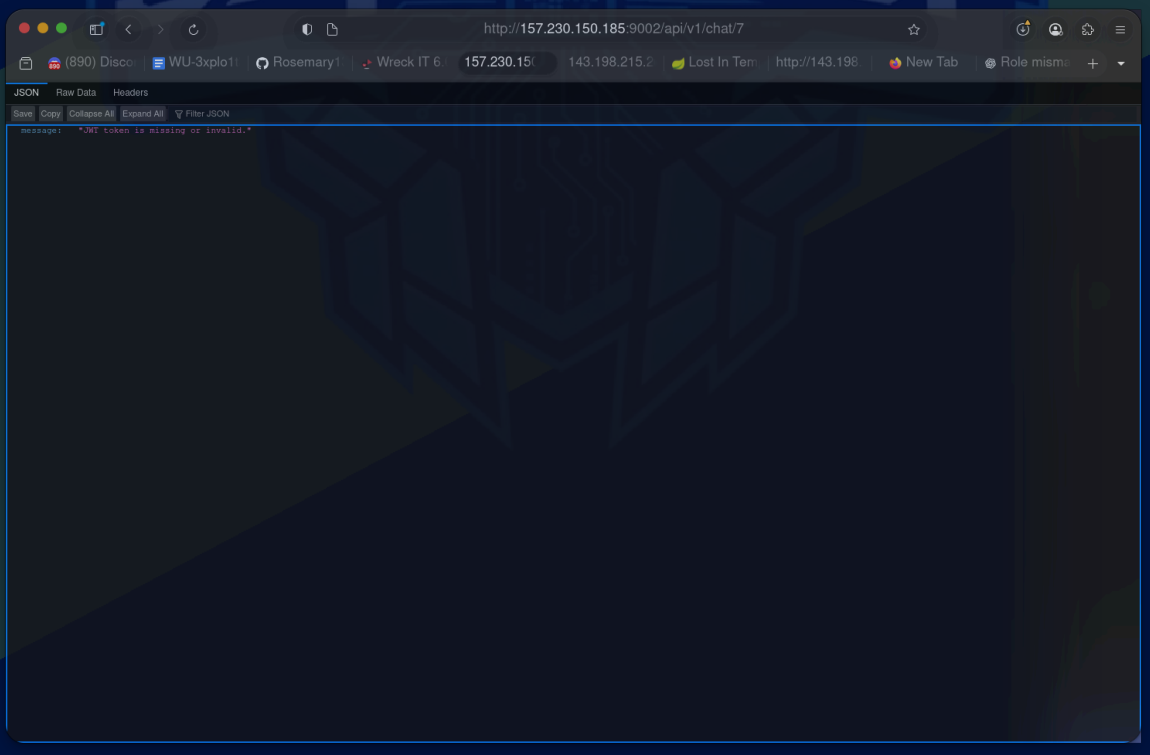
Anotherroblox



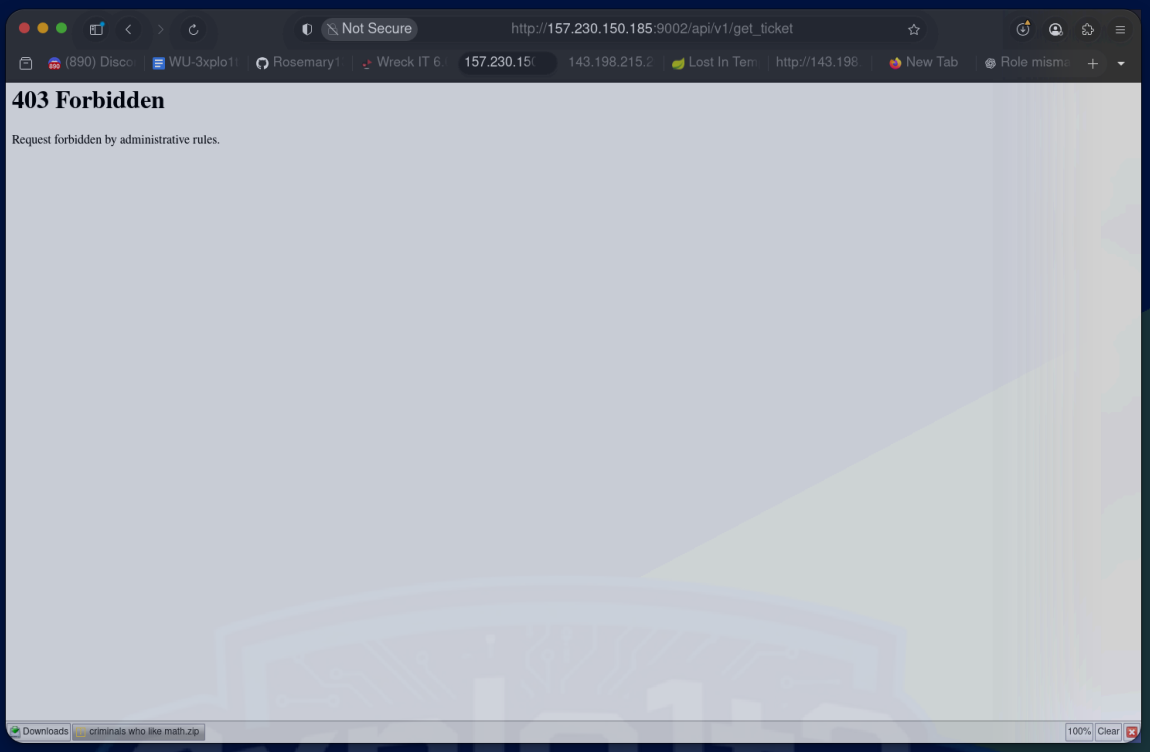


Solution

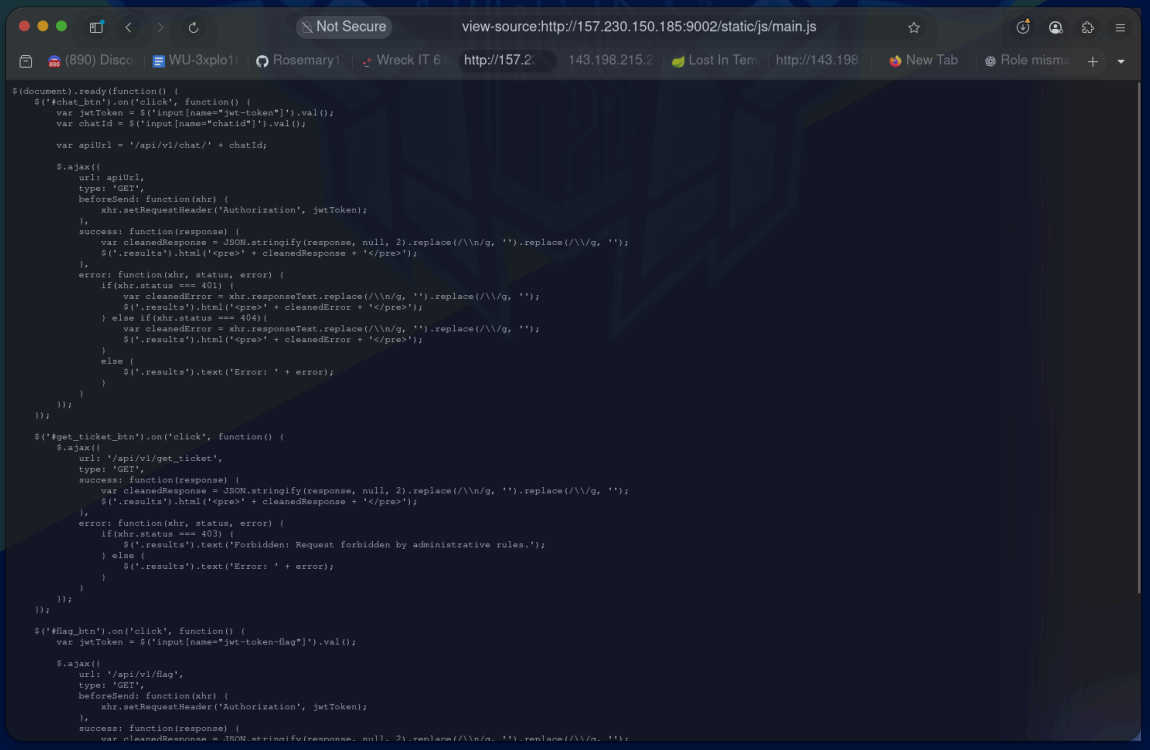
Jadi disini diberikan website API Endpoints, lagi lagi JWT wkwkwk, saya coba akses manual di path /api/v1/chat/{chatid}, saya coba 1-10 butuh token semua



Saya coba yang lainnya, saya pergi ke path /api/v1/get_ticket, baik manual atau tekan Execute, Tapi response tetap 403

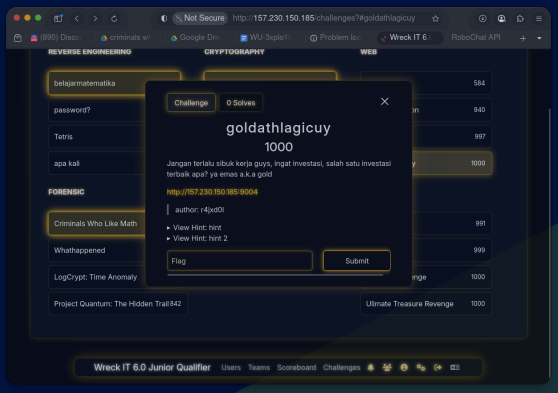


Jadi saya muter muter disitu aja, saya coba explore path path nya, saya inspect pagenya untuk menemukan tanda tanda abnormal, saya selidiki setiap file js nya



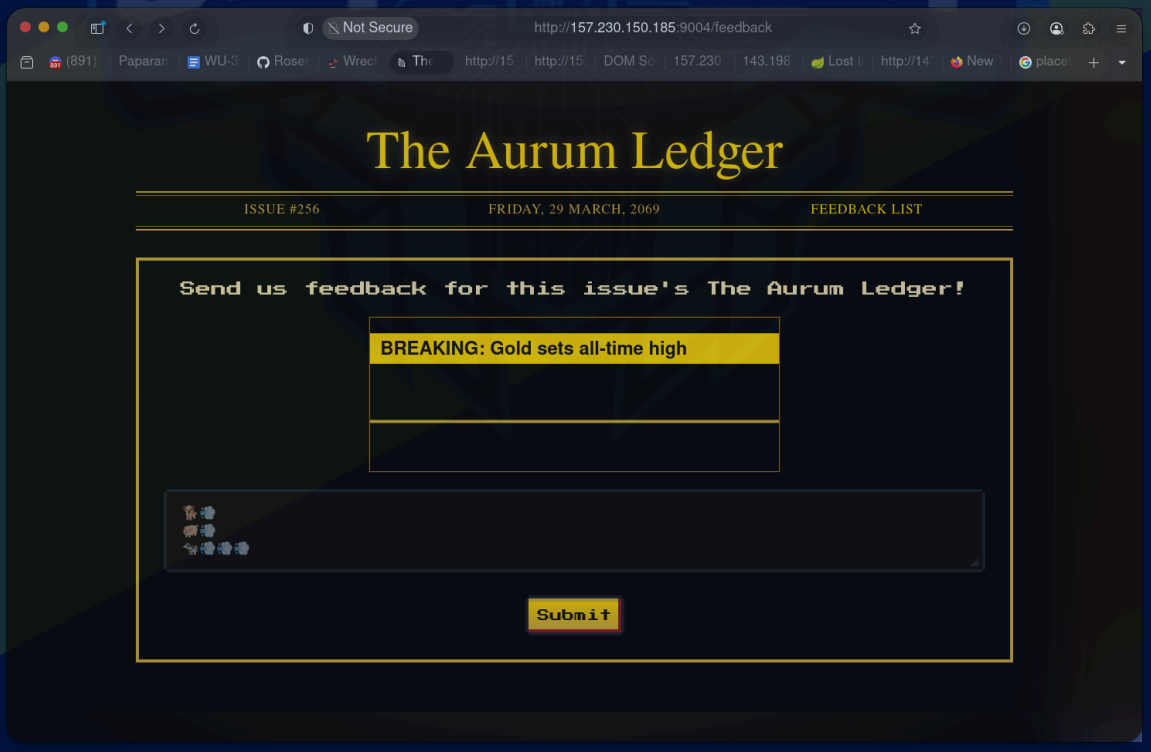
Tanpa sadar muter muter disini mulu 15 menit, karena pusing ya mending sekip laah

Goldathlagicuy

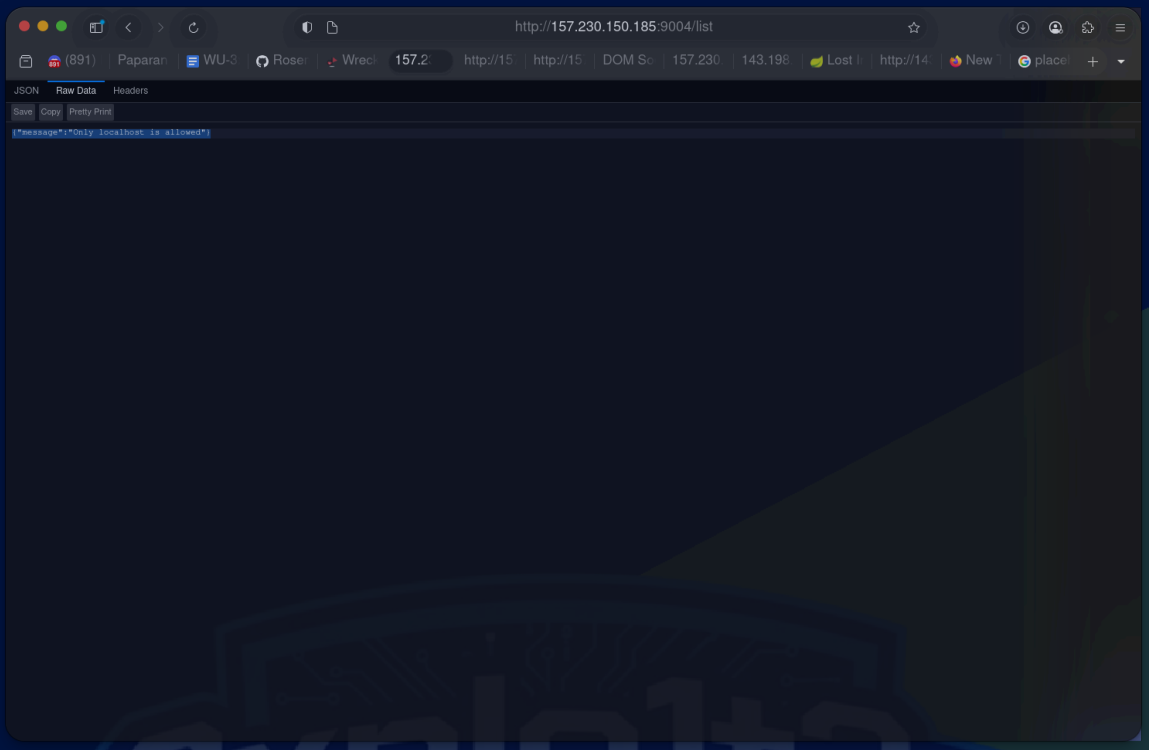


Solution

Diberikan website berjudul "The Aurum Ledger" setelah saya teliti dan eksplorasi lebih dalam ada path /feedback, saya langsung pergi kesana dan tampilannya berbeda dari homepage, seperti cursornya, font, dan placeholder input feedbacknya aneh banget



Saya view source dan menemukan lagi path /list untuk menampilkan feedback. Dari sini sepertinya logikanya itu input feedback lalu lihat list, sayangnya di list itu begini:



Jadi selain localhost gabisa, dan saya ga yakin soalnya gaada yang bisa solve wkwkwk, walaupun udah ada hint:
View Hint: hint

emas(x)ssss

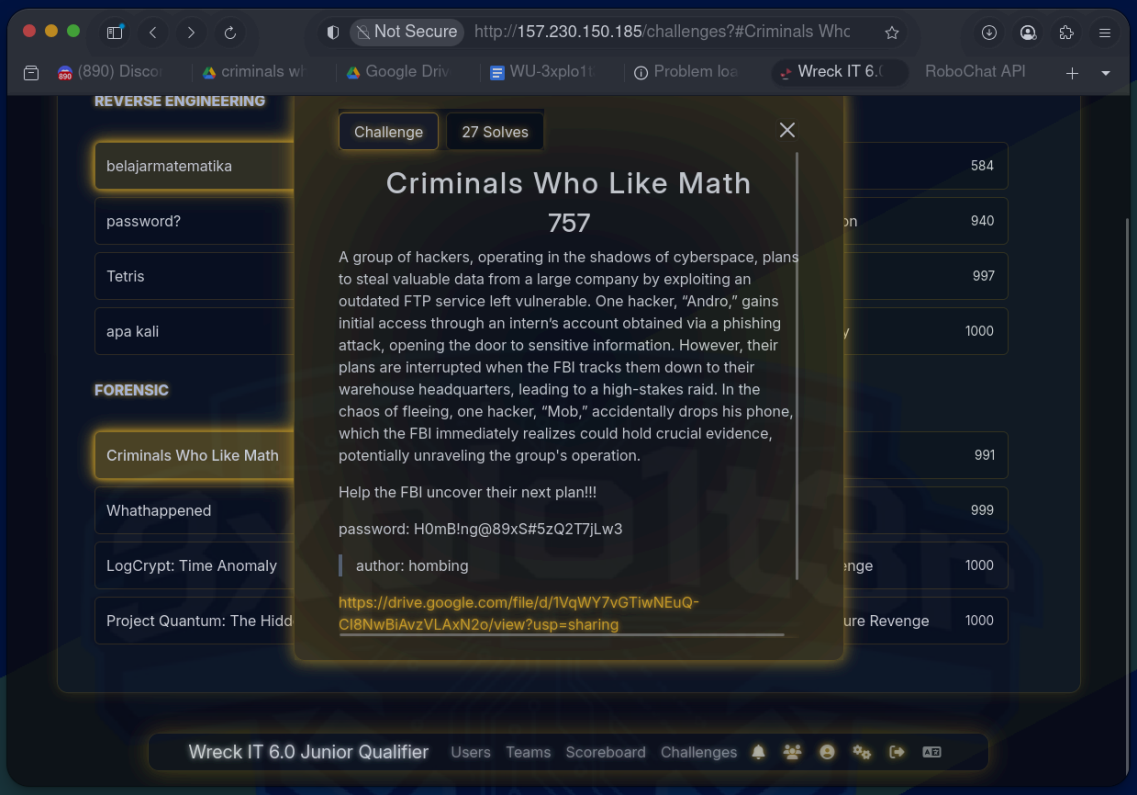
View Hint: hint 2

Eksfiltrasi flag harus baca halaman internal lalu kirim hanya flagnya (CSP mencegah koneksi langsung ke domain luar)

Karena belum ada yang bisa solve jadi saya skip aja deh daripada anu

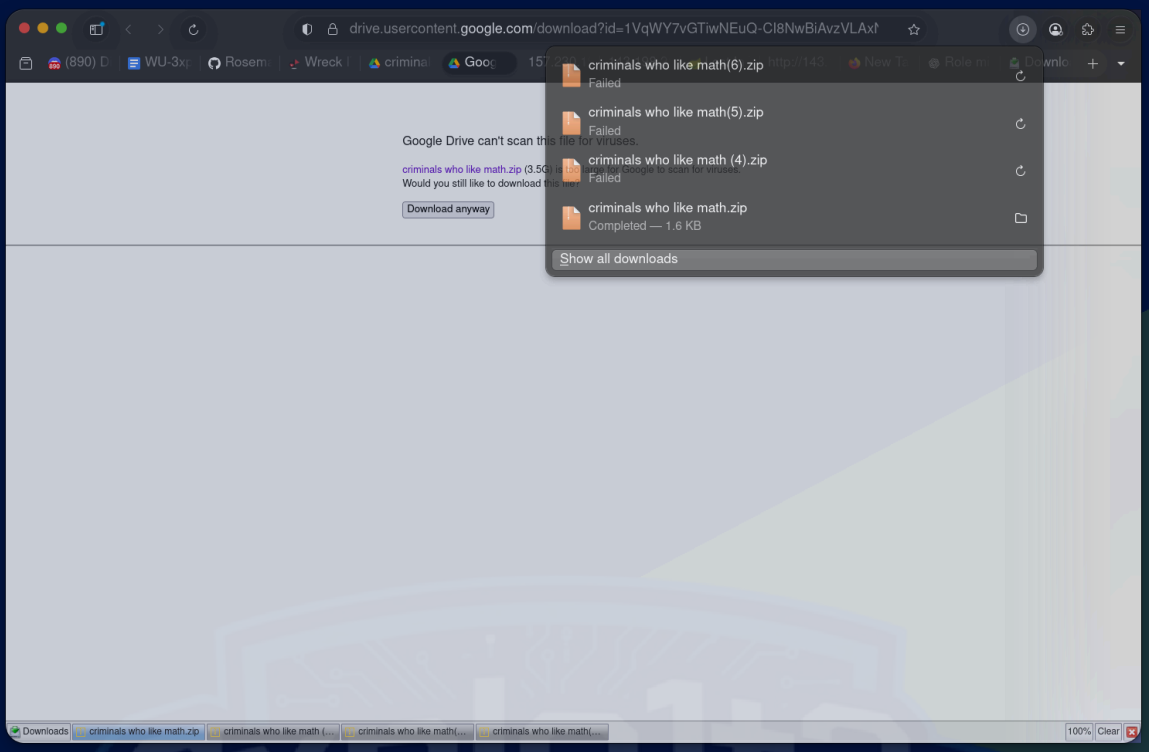
Forensic

Criminals Who Like Math

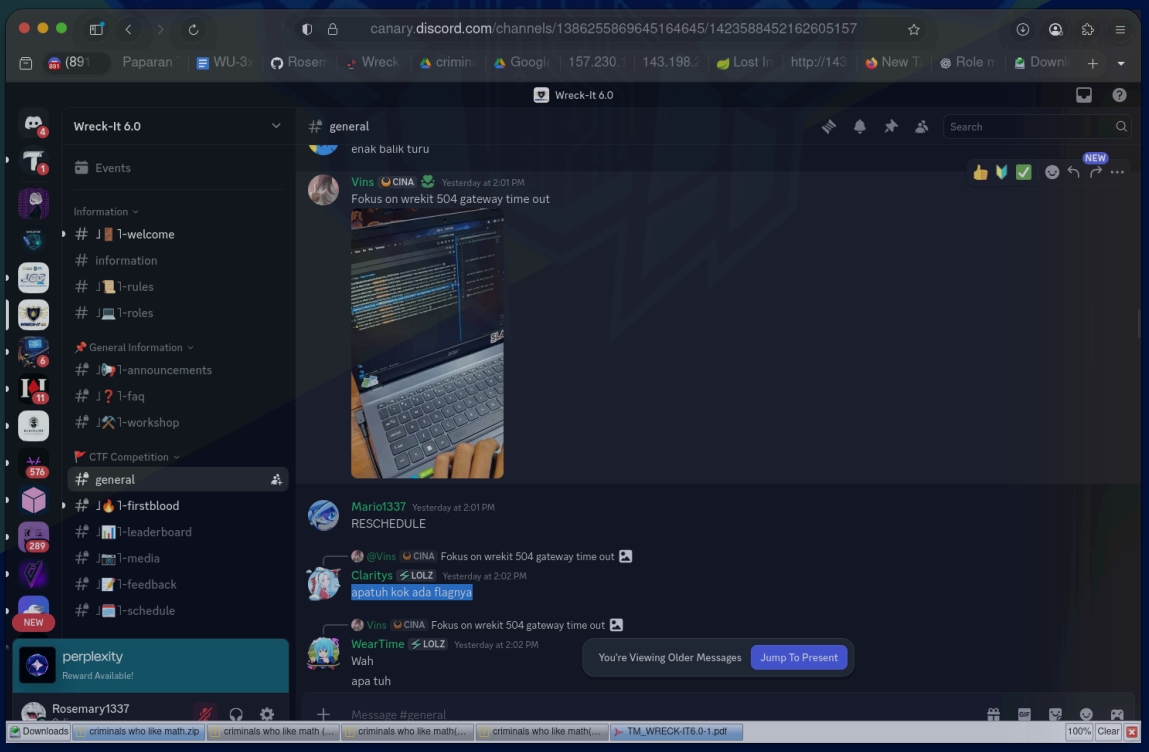


Solution

Disini diberikan link google drive mengarah ke file "criminals who like math.zip" nah disini saya coba download, saat file yang didownload sudah mencapai 2.6GB itu error, berhenti sendiri



Sudah 7x saya coba, ketika hampir selesai itu failed, awalnya sih saya b aja di chall ini, ya saya pikir udah deh skip aja, eh pas nunggu web utamanya down di discord malah ada yang berbagi wkwkwk

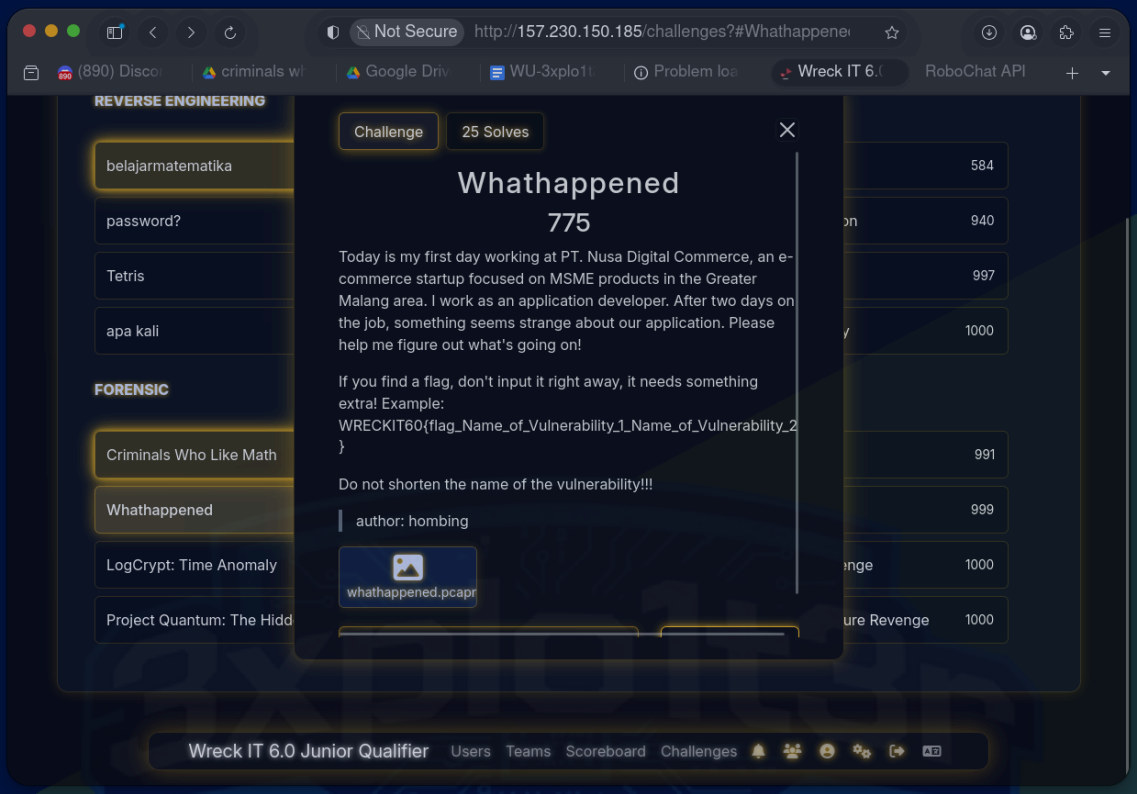


ya saya input aja flagnya, kata panitia kan dilarang berbagi, karena

disini dia yang berbagi, dan kita ga kerjasama, ga kenal tiba tiba bagi flag ya gapapa dong:v

FLAG:WRECKIT60{M1ss10n_D4t4_Exf1ltr4t10n}

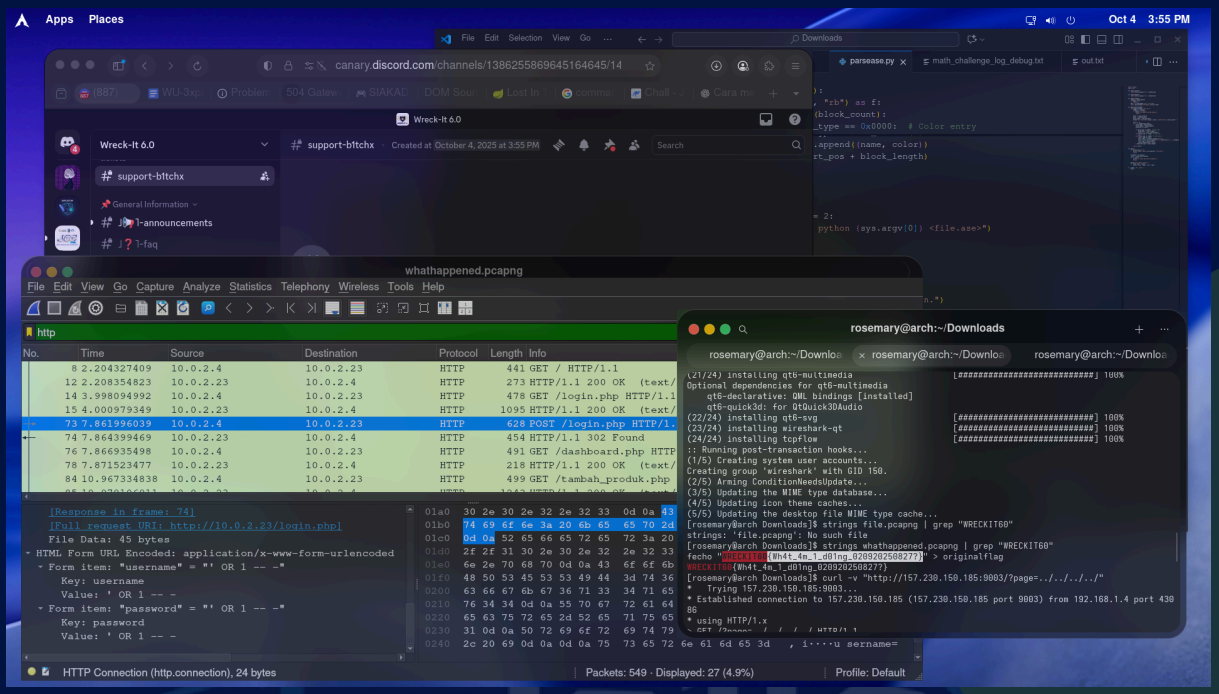
Whathappened



Solution

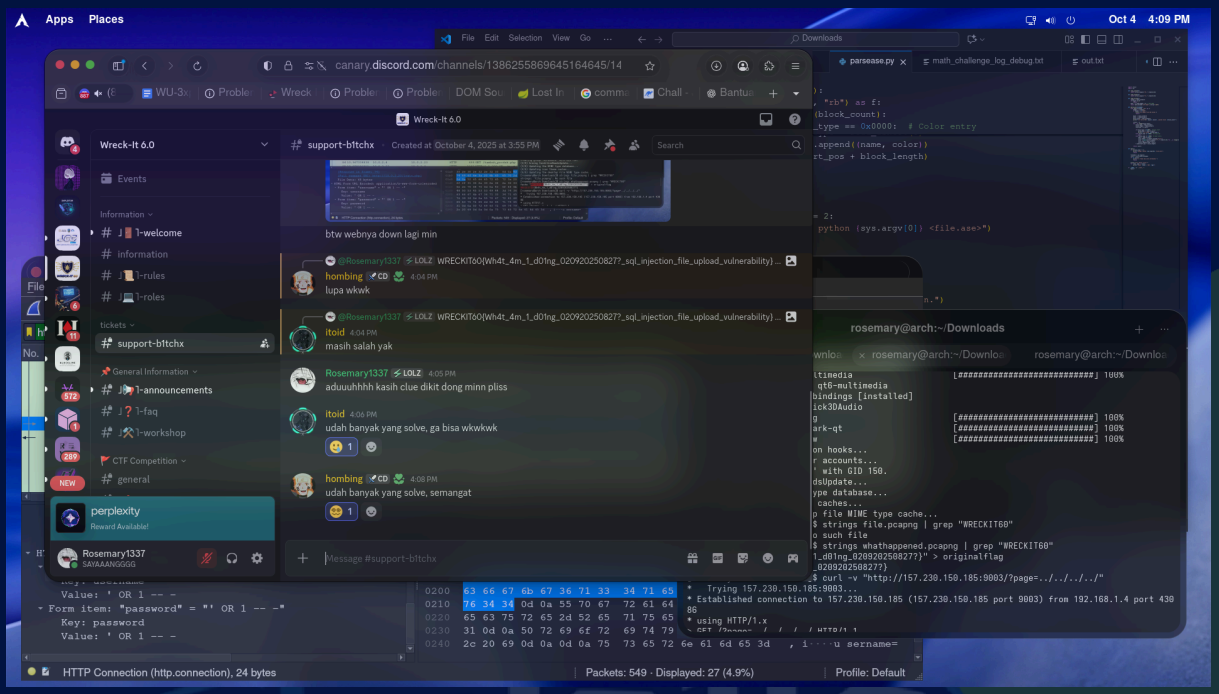
Langsung saja pertama saya diberikan file pcapng, langsung saya buka lewat Wireshark, dari desc challengenya kita bisa menyimpulkan yaitu: 1. Membuka file pcap untuk mencari log yang aneh 2. Flag tidak hanya satu, tapi digabung dengan nama vulnerability yang kita temukan. Nah dari situ saya gunakan strings dan grep untuk mencari

flag dengan pola kata “WRECKIT60”



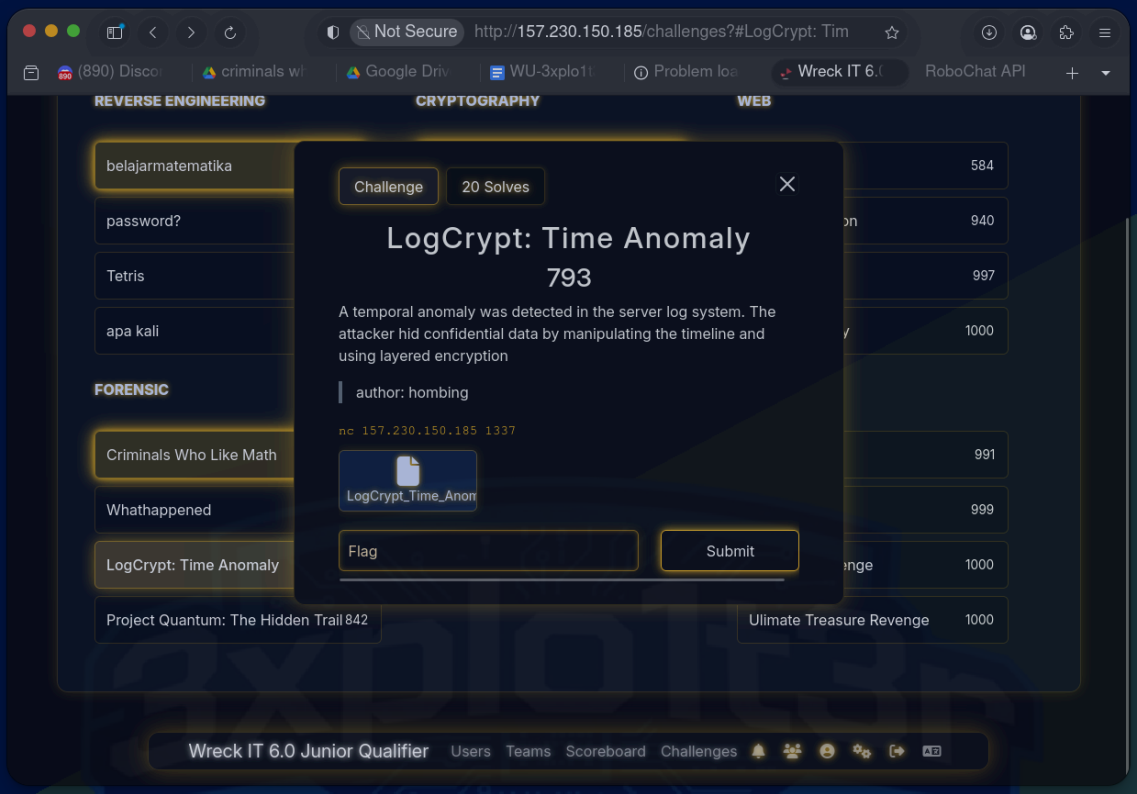
Nah seperti yang bisa kita lihat di bagian kanan, di console/terminal ada langkah langkah saya menemukan originalflag, yaitu dengan cara strings whathappened.pcapng | grep “WRECKIT60” Nah darisitu tampil outputnya adalah fecho "WRECKIT60{Wh4t_4m_1_d01ng_020920250827?}" > originalflag Dan ini adalah originalflag nya, langkah kedua saya pakai wireshark, seperti yang bisa dilihat digambar, dari situ saya menyadari 2 hal yaitu ada user yang login dengan kredensial yang tidak asing, yaitu ‘ OR – - nah sudah jelas ini adalah payload dari SQL Injection, kedua saya menemukan user yang mengakses tambah_produk dan dia meng input file dengan ekstensi .php . darisini saya tau ini adalah File Upload Vulnerability/Unrestricted File Upload, jadi saya atur pola flag menjadi WRECKIT60{Wh4t_4m_1_d01ng_020920250827_SQL_Injection_Unrestricted_File_Upload} tetapi salah, saya coba banyak pola lain seperti SQL_Injection dan File_Upload_Vulnerability tetap salah sampai saya

sudah pusing dan akhirnya saya tanya panitia wkwkwk



Sampai sini saya sudah menyerah, sudah saya coba sampai 25x pola yang memungkinkan tapi gaada satupun yang benar, kemudian saya skip dulu untuk soal ini dan lanjut ke soal yang lain.

LogCrypt: Time Anomaly



Solution

Disini saya diberikan file 7z yang berisi beberapa file log, setelah ini saya coba connect ke IP dan PORT yang diberikan, ternyata berisi soal, pertama adalah

Question 1: There was a coordinated attack from 5 different IP addresses. How many minutes were there between the first and last attacks from IP address 203.0.113.89?

>

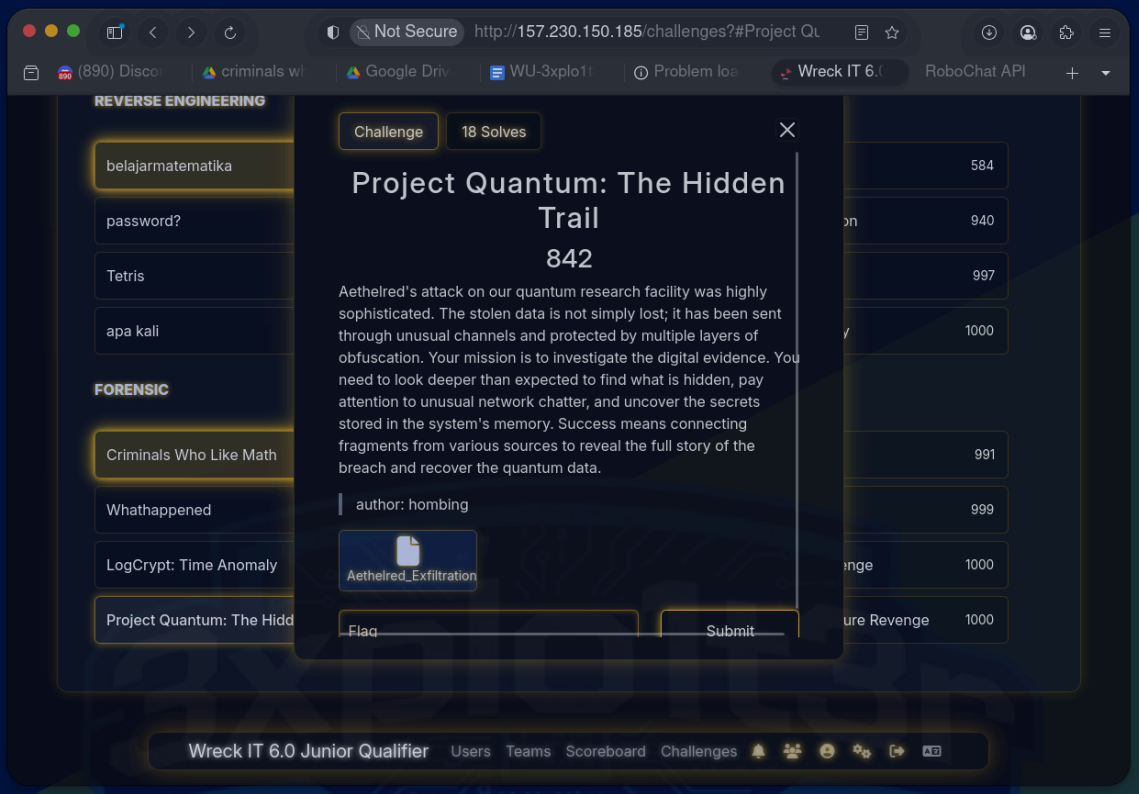
Dan saya cari manual di VScode(CTRL+F) saya masukkan ipnya, saya cari satu satu di filenya dan ketemu di file access.log, kemudian saya hitung berapa selisih waktu antara serangan pertama sampai terakhir, 15/Dec/2023:10:15:00 sampai 15/Dec/2023:11:00:00 nah sudah diketahui selisihnya 45 menit, saya masukkan dan benar, lanjut ke soal kedua, disuruh mencari decode dari base64 yang ada di field User-Agent, jadi saya cari lagi " == " karena biasanya b64 pakai 2 sama dengan untuk penutup, ternyata tidak ada, lanjut saya cari " = " hanya 1, dan ketemu 21 yang sama, kebetulan saya mulai cari dari bawah dan ternyata ada dibawah juga stringnya wkwkwk, dari string

U2Vzc2lvbk1EOjc0MjgxMzktVGltZW91dDozNjAwLVVzZXI6YWRtaW4= bisa kita decode menjadi SessionID:7428139-Timeout:3600-User:admin, saya input dan lanjut ke soal 3, di soal 3 saya sempat kebingungan, dari terminal VScode saya pakailah qwen code, saya coba karena dia bisa langsung interaksi dengan filenya, saya paste pertanyaannya dan dapat jawaban 15055. Saya input dan lanjut ke pertanyaan 4, sayangnya disini saya jawabnya sudah -3 menit sebelum jam 19.00, jadi tidak sempat untuk menjawab nomor 4 hehehe.

```
Question 1: There was a coordinated attack from 5 different IP
addresses. How many minutes were there between the first and last
attacks from IP address 203.0.113.89?
> 45
Correct! Moving to the next question.

Question 2: What is the original content of the Base64 encoded
message in the User-Agent field?
> SessionID:7428139-Timeout:3600-User:admin
Correct! Moving to the next question.

Question 3: What is the total response size of the 10 requests
showing an arithmetic pattern?
> 15055
Correct! Moving to the next question.

Question 4: Decode the hexadecimal path. What is the encoded word?
>
```

Dan disini waktu habis sebelum ketemuan sama flag:(

Project Quantum: The Hidden Trail

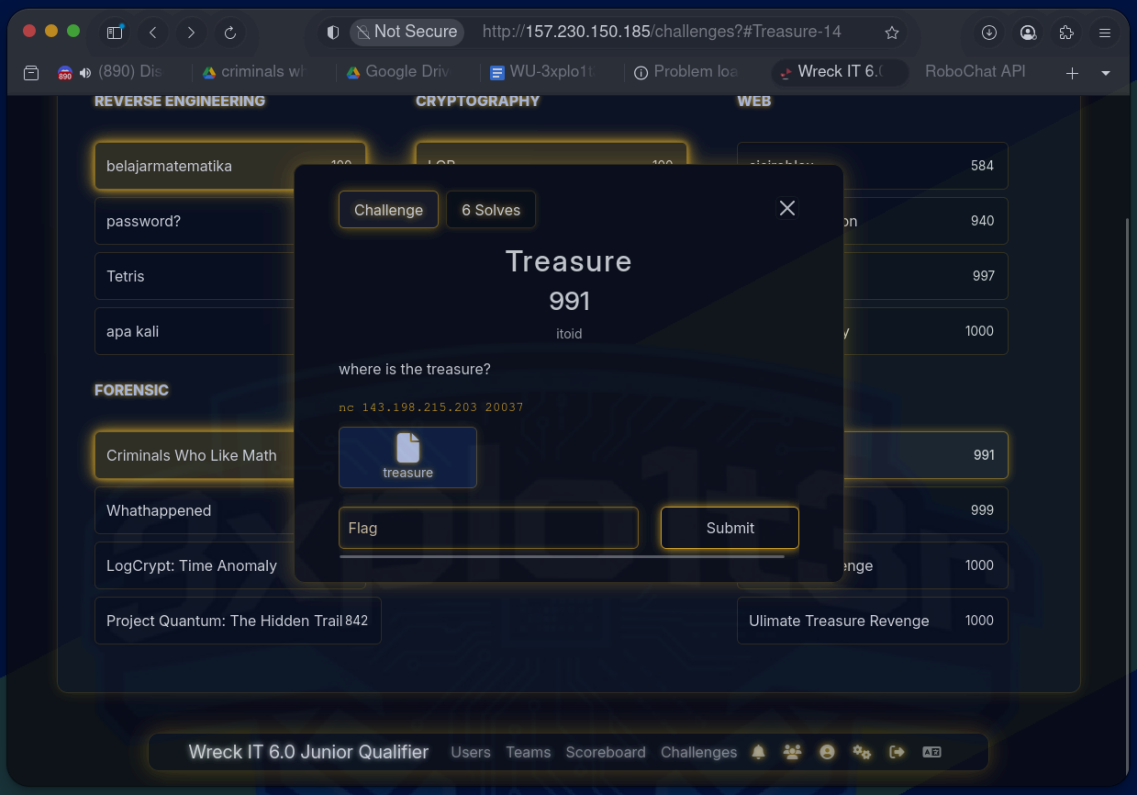


Solution

Diberikan satu file 7z berukuran 50mb, didalamnya ada file file seperti log, vmem, dan lainnya, di README.md bisa disimpulkan kalau harus ambil kunci dari RAM.vmem lalu pulihkan file gambar dari Server-Prod-Quantum.dd, lalu rekonstruksi exfil dari network traffic.log, tetapi karena keterbatasan waktu (waktu tidak mencukupi) saya belum bisa menemukan flagnya.

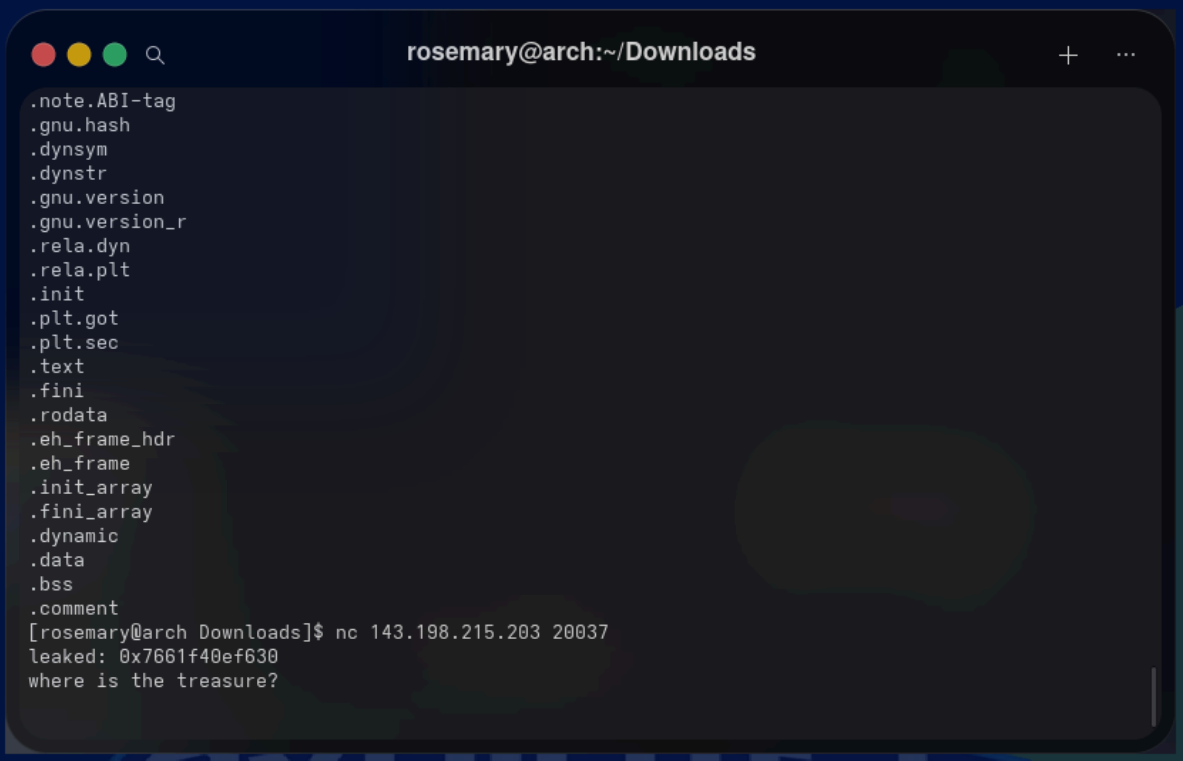
PWN

Treasure



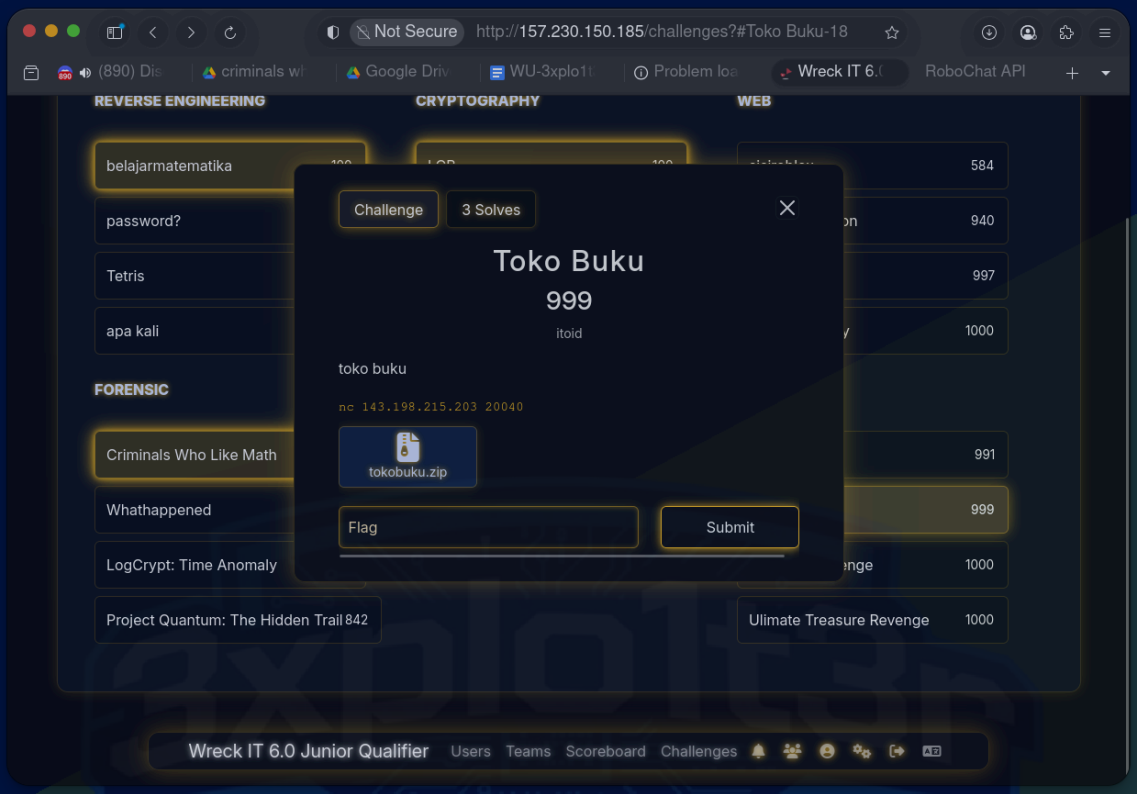
Solution

Jadi disini kita disuruh connect ke ip dan port yang sudah disediakan, dan isinya adalah:



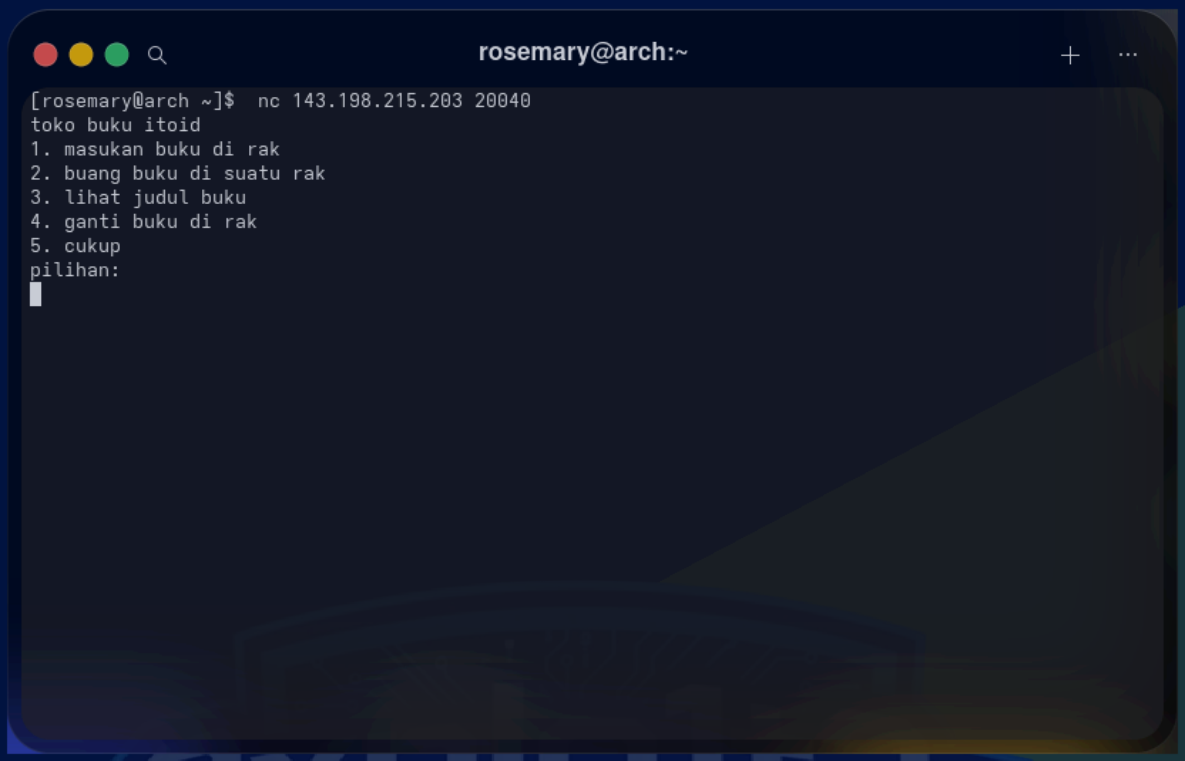
Binary/network service langsung mencetak sebuah alamat saat terhubung:
leaked: 0x7661f40ef630
Dan berubah setiap koneksi, Dari strings terlihat juga entri ./flag dan teks where is the treasure? tanda bahwa tujuan akhir adalah membaca file ./flag di server. Intinya server ngasih leak, karena kelihatannya ini chall susah setelah saya coba, saya skip ke chall lain (chall kak itoid susah bjir)

Toko Buku

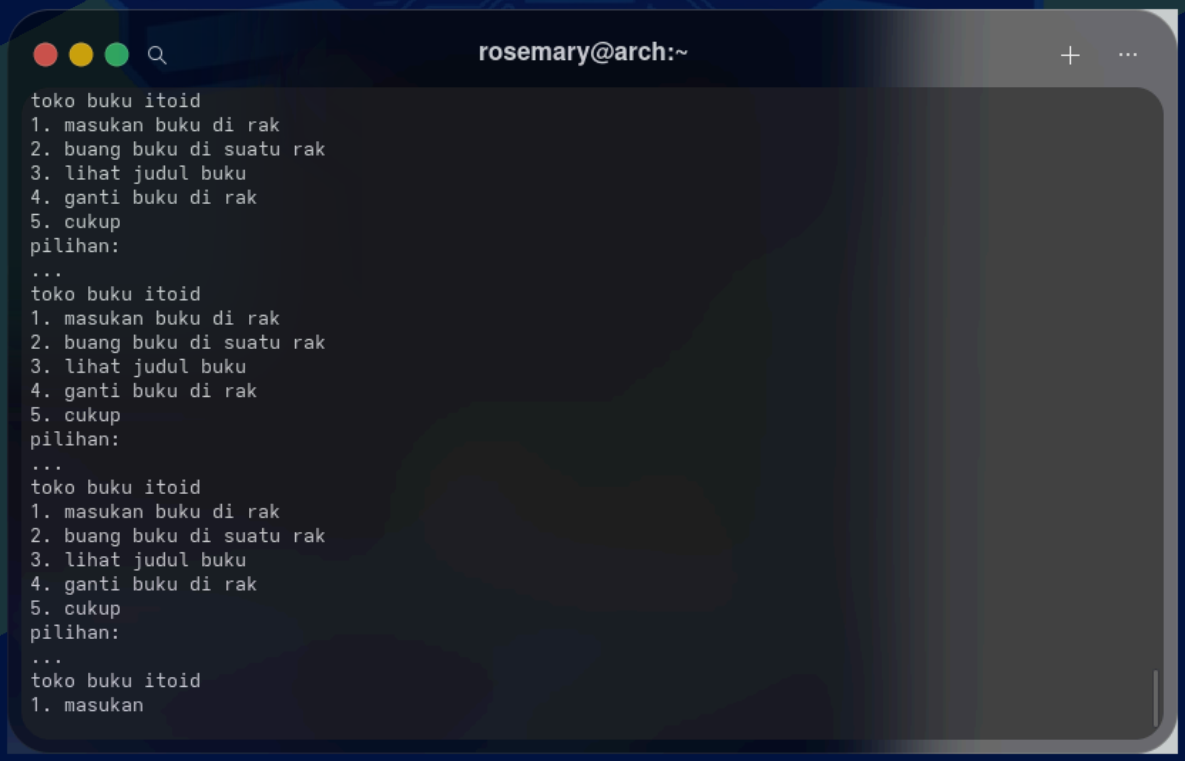


Solution

Disini kita disuruh connect ke ip dan portnya, setelah connect ternyata isinya adalah toko buku

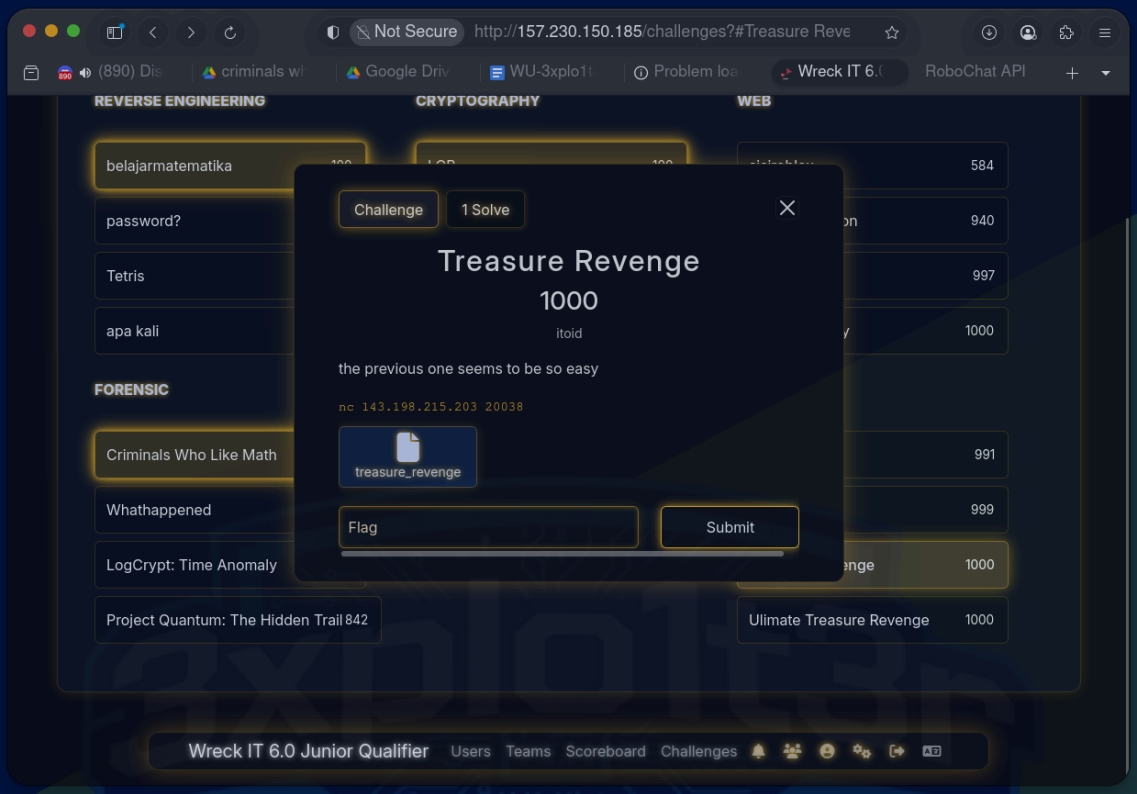


Dari sini saya coba coba sampai 30 menitan buat cari logika dan cara kerjanya buat dapetin flag



disini dia crash saat kita input string, jadi hanya bisa input integer, jadi saya kembali ke desc challengenya, kemudian saya download file yang berisi 2 lib dan 1 file executable, karena yang sudah solve sedikit, dan soal kak itoid susah susah jadi saya skip

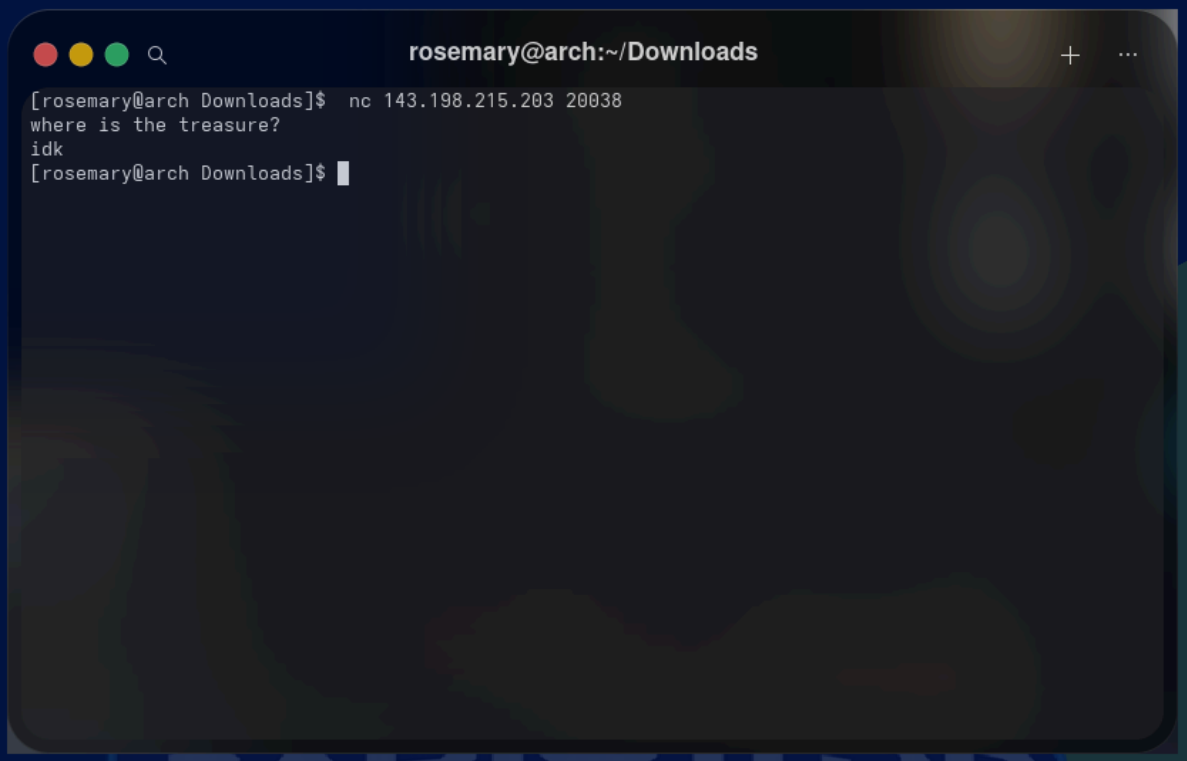
Treasure Revenge



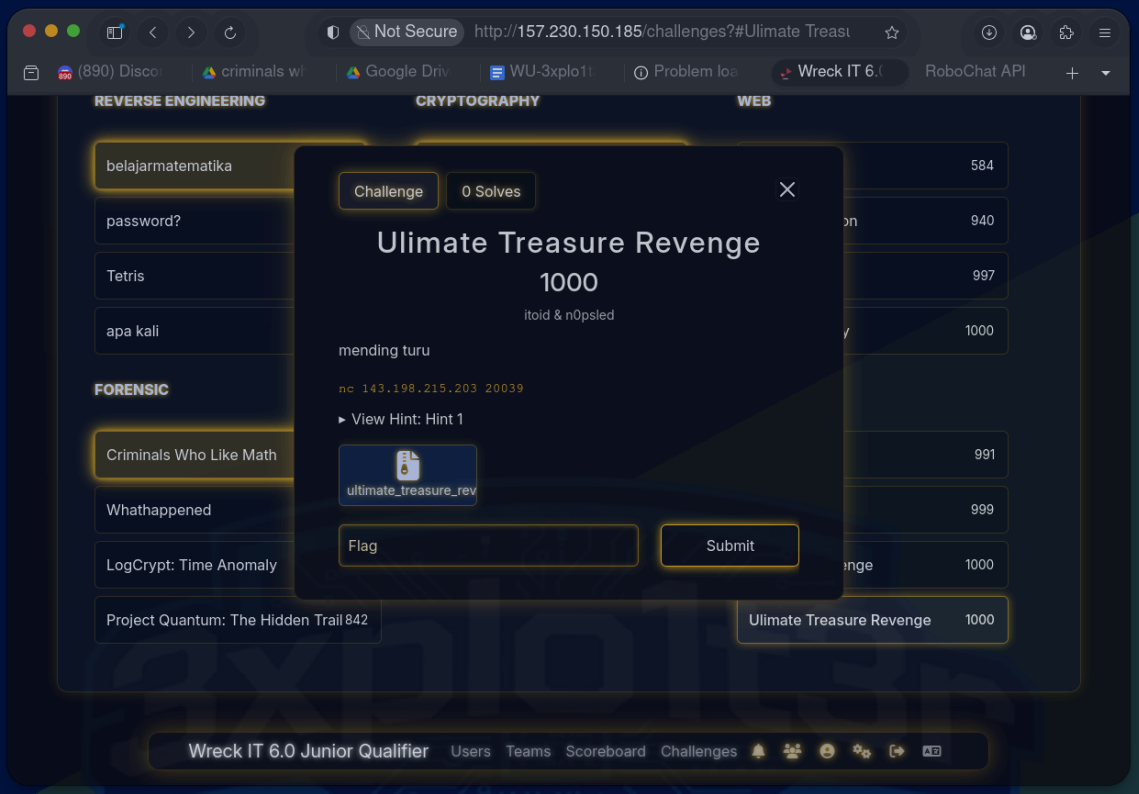
Solution

Yah ini sama kaya chall “Treasure” yang lebih susah dari chall Treasure wkwkwk, jadi setelah connect ke ip dan portnya langsung

saya skip damn



Ultimate Treasure Revenge

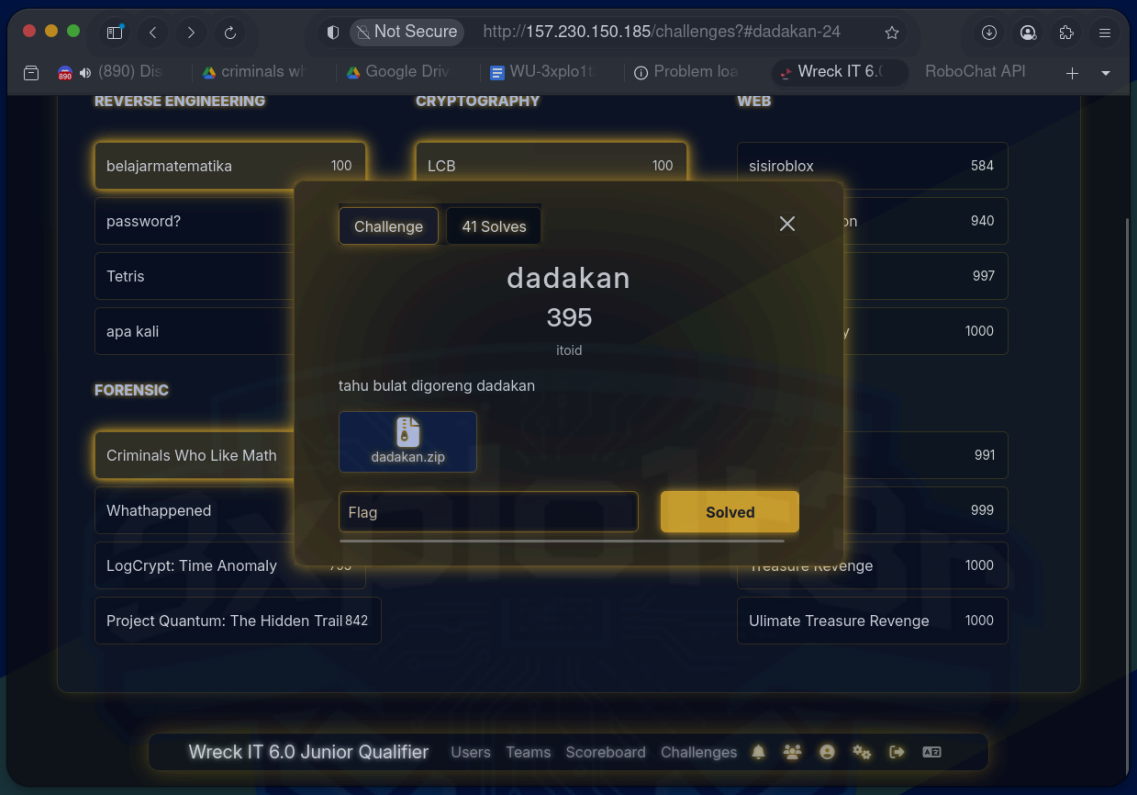


Solution

Udah bener desc challengenya, jadi langsung skip tanpa pikir panjang

Cryptography

Dadakan



Solution

Challenge ini meminta kita untuk mendapatkan flag yang disembunyikan didalam output sebuah skrip (chall.py) dengan membalikkan rangkaian transformasi dan PRNG yang digunakan.

File yang tersedia :

- chall.py
- Outputt.txt

Saya memulai dengan melihat isi file chall.py dan menemukan bahwa skrip membutuhkan secret.py,lalu saya membuat secret.py dummy berisi flag = b'FLAG{test_dummy}' agar skrip bisa dijalankan.setelah itu saya menjalankan chall.py untuk menyimpan output ke out.txt untuk dianalisis.
Saya melihat beberapa angka penting: nilai S, K^S, M^…, A_perm^…,

B_perm^…, dan 624 angka Z.

Selanjutnya saya membuat skrip recovery_flag.py yang membalik proses transformasi PRNG, rotasi, dan permutasi. Tujuannya adalah mendapatkan:

- S, K, M
- A_perm, B_perm, r

Setelah saja jalankan scriptnya,menghasilkan output:

```
S = 0x543c5310
K = 0x95f99222
M = 0x1f687fdd
A_perm = 449
B_perm = 63
r = 242
```

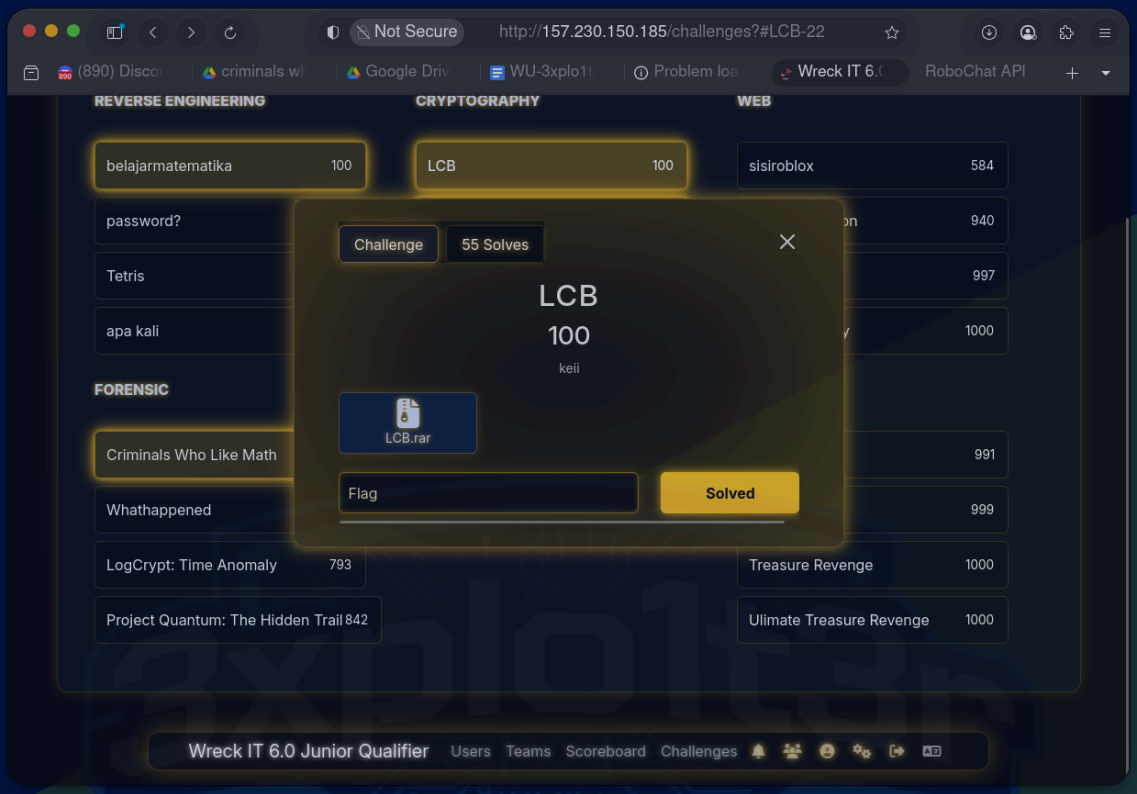
Untuk verifikasi dan melihat teks yang mudah dibaca, saya juga menjalankan debug_recover.py yang menampilkan potongan-potongan printable dari state_bytes sehingga posisi flag terlihat. Karena penyelenggara menyediakan outputs.txt di dalam ZIP, saya mengekstrak file tersebut lalu menjalankan recover_flag.py pada outputs.txt untuk mendapatkan hasil nyata (bukan dummy). Dengan extract_flag.py saya mengekstrak substring antara { dan } dari state_bytes yang sudah dikembalikan.

FLAG:WRECKIT60{this_is_a_super_long_ctf_flag_constructed_for_testing_state_embedding_and_solver_robustness__it_contains_letters_numbers_and_underscores_to_keep_parsing_simple_and_reliable__remember_that_the_best_attacks_start_with_clean_models_and_precise_inversions__keep_hacking_friend_h4h4_1t01d_1s_h3r3_t0_m4k3_y0ur_d4y_b3tt3r_h4h4h4h4h4h4h4h4h4h4h4_:p}

Script yang saya gunakan :

https://github.com/Rafaa-kn/WRECKIT60---dadakan-/tree/main

LCB



Solution

Diberikan file LCB.rar, setelah saya ekstrak berisi cipher.py, generator.py, dan folder dist, saya coba baca generator.py, teryata logikanya adalah membuat folder dist/ untuk output ciphertext, dan buat banyak pasangan plaintext ke ciphertext dari cipher linear, dari situ saya ekstrak lagi file LCB.rar nya di folder yang berbeda, saya run generator.py yang terletak di folder yang berbeda, dan dia menghasilkan output folder dist/ baru beserta isinya, dari sini agak janggal karena saat di ekstrak pertama kali itu sudah ada folder dist/. Lalu saya coba untuk buat solver dari ciphertext original didalam folder dist/. Berikut scriptnya:

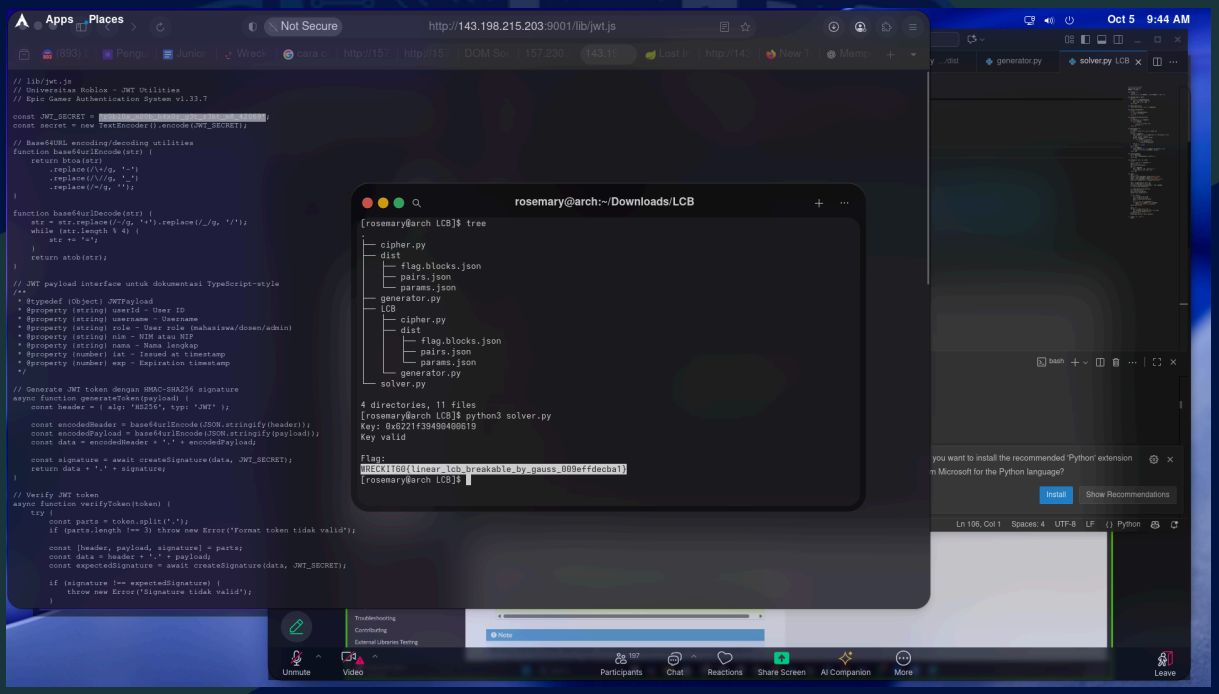
```
#!/usr/bin/env python3
import json, sys, os
MASK64 = (1<<64)-1


def rol64(x, r):
    r %= 64
```

```
    return ((x << r) & MASK64) | ((x & MASK64) >> (64 - r))


def permute_bits(x, perm):
    out = 0
    for i, src in enumerate(perm):
        bit = (x >> (63 - src)) & 1
        out = (out << 1) | bit
    return out


def u64_to_bits_le(x):
    return [(x >> i) & 1 for i in range(64)]


def bits_le_to_u64(bits):
    x = 0
    for i,b in enumerate(bits):
        if b: x |= (1<<i)
    return x


def build_matrix_from_rots(rot):
    n = 64
    A = [[0]*n for _ in range(n)]
    for i in range(n):
        for r in rot:
            j = (i - (r % 64)) % 64
            A[i][j] ^= 1
    return A


def gf2_solve(A, b):
    n = len(A)
    M = [r[:] + [b_i] for r, b_i in zip(A, b)]
    row = 0
    for col in range(n):
        sel = next((r for r in range(row, n) if M[r][col]), None)
        if sel is None: continue
        M[row], M[sel] = M[sel], M[row]
        for r in range(n):
            if r != row and M[r][col]:
                for c in range(col, n+1):
                    M[r][c] ^= M[row][c]
        row += 1
        if row == n: break
    sol = [0]*n
    for r in range(n):
```

```
        lead = next((c for c in range(n) if M[r][c]), None)
        if lead is not None: sol[lead] = M[r][n]
    return sol


def inverse_perm(p):
    inv = [0]*len(p)
    for i, src in enumerate(p): inv[src] = i
    return inv


def decrypt(ct, key, rot, perm):
    k = 0
    for r in rot: k ^= rol64(key, r)
    pperm = ct ^ k
    inv = inverse_perm(perm)
    out = 0
    for i in range(64):
        bit = (pperm >> (63 - inv[i])) & 1
        if bit: out |= (1 << (63 - i))
    return out


def main():
    base = "dist"
    params = json.load(open(f"{base}/params.json"))
    pairs = json.load(open(f"{base}/pairs.json"))
    flags = json.load(open(f"{base}/flag.blocks.json"))
    perm, rot = params["perm"], params["rotations"]


    pt0 = int(pairs[0]["pt_hex"],16)
    ct0 = int(pairs[0]["ct_hex"],16)
    kcontrib = (permute_bits(pt0,perm) ^ ct0) & MASK64
    b = u64_to_bits_le(kcontrib)


    A = build_matrix_from_rots(rot)
    sol = gf2_solve(A,b)
    key = bits_le_to_u64(sol)
    print(f"Key: 0x{key:016x}")


    for p in pairs:
        pt = int(p["pt_hex"],16)
        ct = int(p["ct_hex"],16)
        pperm = permute_bits(pt,perm)
        k = 0
```

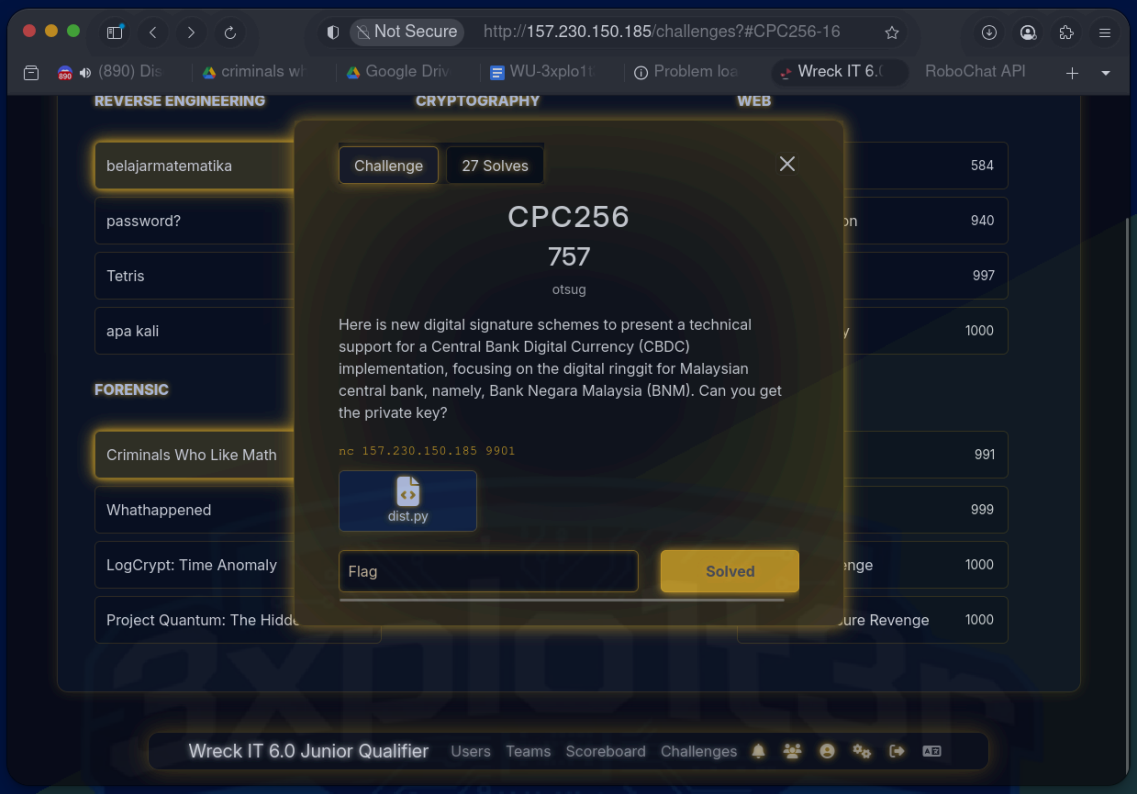
```
        for r in rot: k ^= rol64(key,r)
        if (pperm ^ k) & MASK64 != ct & MASK64:
            print("Key salah"); sys.exit(1)
    print("Key valid")


    data = b""
    for blk in flags["blocks_hex"]:
        pt = decrypt(int(blk,16), key, rot, perm)
        data += pt.to_bytes(8,"big")
    print("\nflag:")
    print(data.rstrip(b'\x00').decode())


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

Dan saya jalankan langsung ketemu flagnya



FLAG:WRECKIT60{linear_lcb_breakable_by_gauss_009effdecba1}

CPC256



Solution

Tantangan ini meminta kita memulihkan kunci privat λ dari dua tanda tangan yang memakai nonce lemah — cukup bandingkan dua tanda tangan untuk menemukan λ.

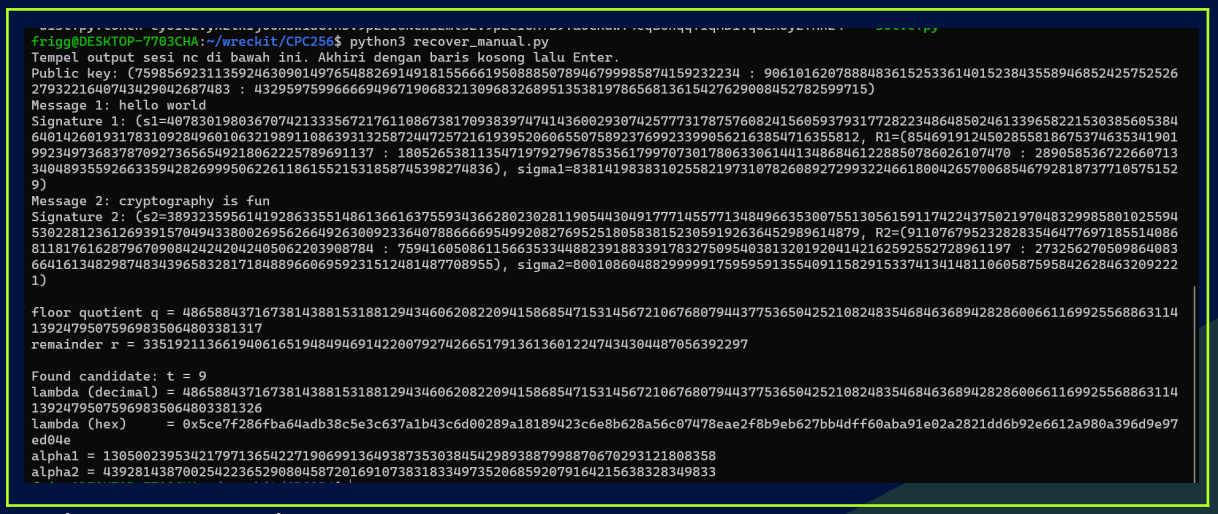
Saya mencoba masuk ke `nc 157.230.150.185 9901` dan saya mendapatkan public key, dua pesan, dua tanda tangan lengkap, dan prompt untuk menebak private key λ.

Saya menggunakan script manual_recover.py:

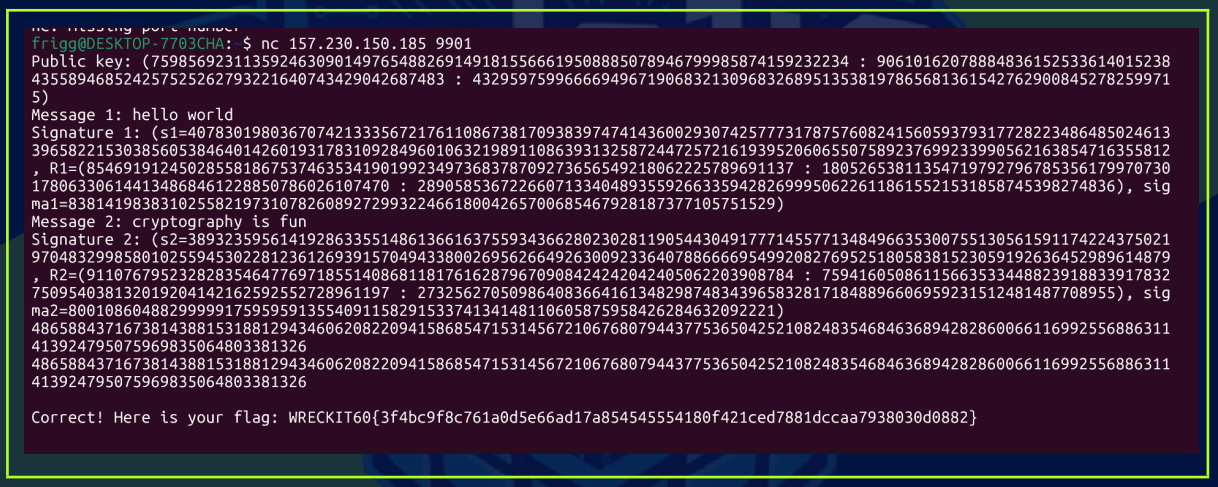
```
import re

def extract_and_compute(text):
    try:
        s1 = int(re.search(r"s1=([0-9]+)", text).group(1))
        s2 = int(re.search(r"s2=([0-9]+)", text).group(1))
        sigma1 = int(re.search(r"sigma1=([0-9]+)", text).group(1))
```

```
        sigma2 = int(re.search(r"sigma2=([0-9]+)", text).group(1))
    except Exception as e:
        print("Gagal mengekstrak integer dari teks. Pastikan kamu
menempel seluruh blok signature.")
        print("Error:", e)
        return

    diff_s = s1 - s2
    diff_sigma = sigma1 - sigma2
    q, r = divmod(diff_s, diff_sigma)
    print("floor quotient q =", q)
    print("remainder r =", r)
    # search small neighborhood
    for t in range(-1000, 1001):
        lam = q + t
        a1 = s1 - sigma1 * lam
        a2 = s2 - sigma2 * lam
        if 1 <= a1 < 2**256 and 1 <= a2 < 2**256:
            print("\nFound candidate: t =", t)
            print("lambda (decimal) =", lam)
            print("lambda (hex)     =", hex(lam))
            print("alpha1 =", a1)
            print("alpha2 =", a2)
            return
    print("Tidak ditemukan kandidat dalam rentang pencarian. Coba
pastikan teks yang kamu paste benar.")

if __name__ == "__main__":
    print("Tempel output sesi nc di bawah ini. Akhiri dengan baris
kosong lalu Enter.")
    lines = []
    while True:
        try:
            line = input()
        except EOFError:
            break
        if line.strip() == "":
            break
        lines.append(line)
    banner = "\n".join(lines)
    extract_and_compute(banner)
```

Script akan menghasilkan:



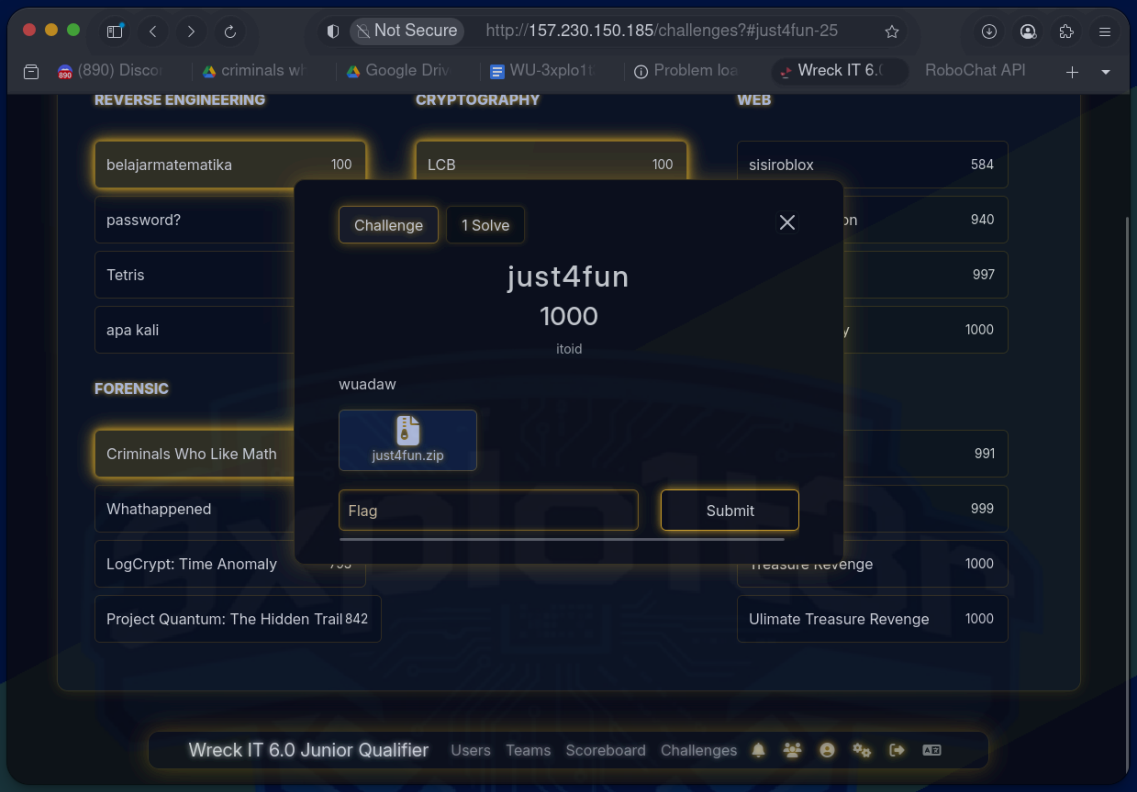
Dari output script tersebut.saya copy 4865884371673814388153188129434606208220941586854715314567210676807944377536504252108248354684636894282860066116992556886311413924795075969835064803381326.dan sya coba input ke nc 157.230.150.185 9901.



Dan saya berhasil mendapatkan flag nya.

FLAG:WRECKIT60{3f4bc9f8c761a0d5e66ad17a854545554180f421ced7881dccaa7938030d0882}

Just4fun

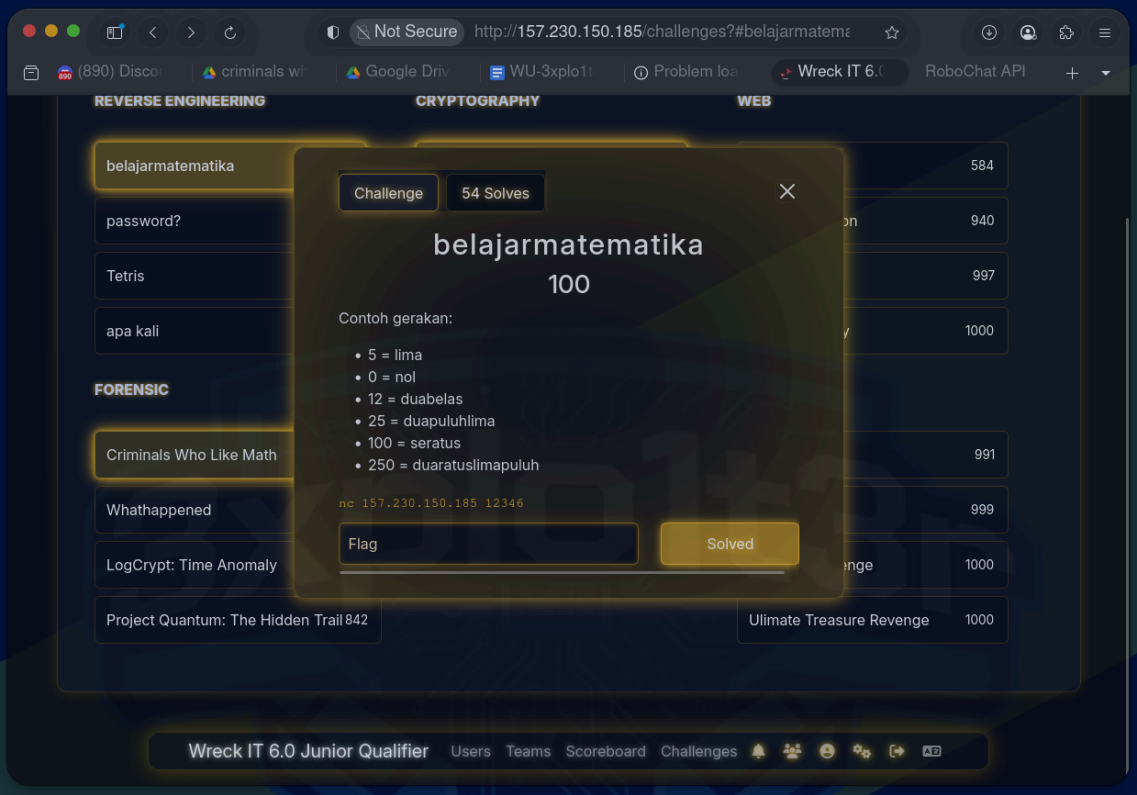


Solution

Lagi lagi soalnya kak itoid, dari sini kita udah putus asa aja sih ga berharap lebih, mendingan kerjain yang mudah mudah aja hehehe

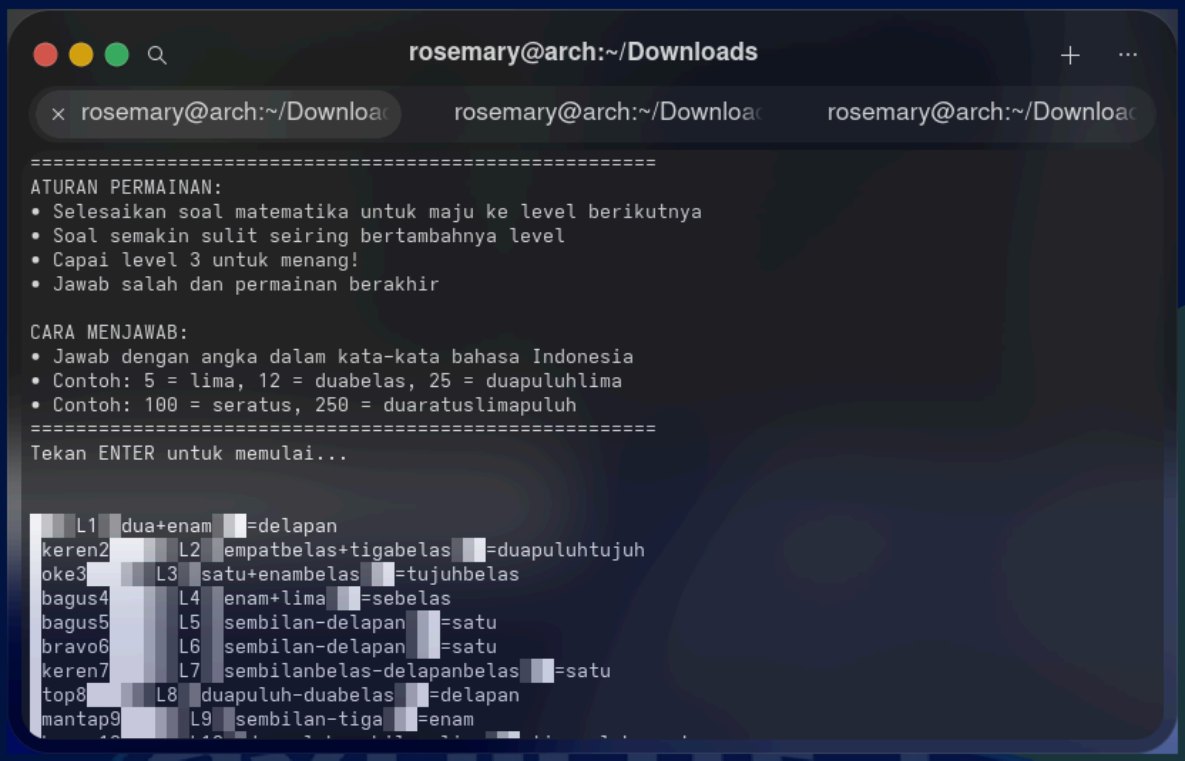
Reverse Engineering

Belajarmatematika

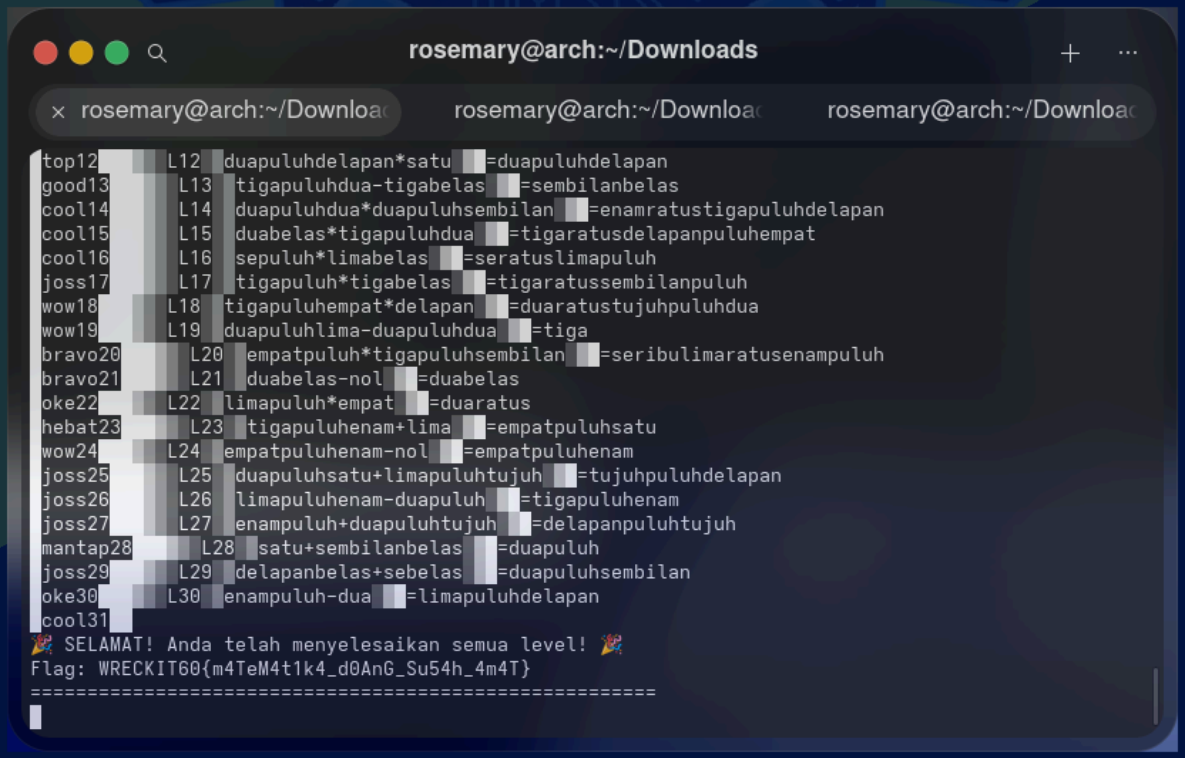


Solution

Disini saya diberikan host dan port dan disuruh connect ke host dan port tersebut, setelah saya connect isinya adalah soal matematika, berikut adalah screenshot dari isi soal:

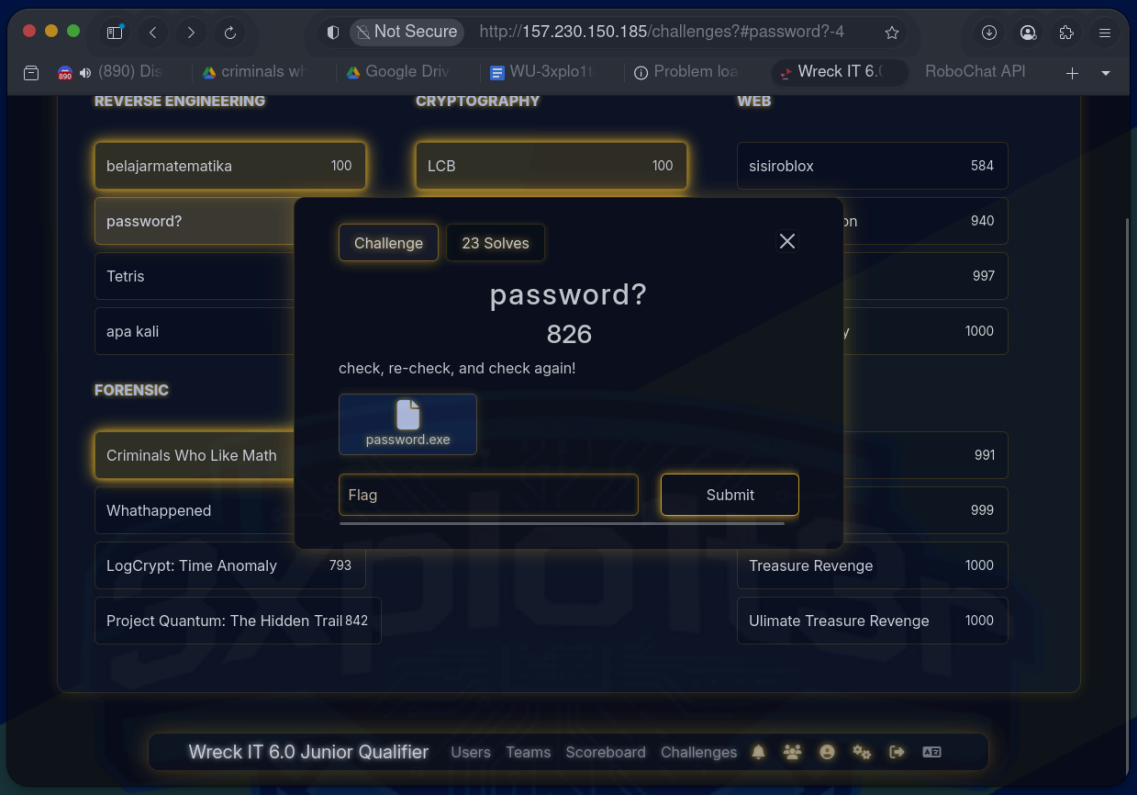


Dari sini saya tahu ini bukan soal biasa, ya karena yang seharusnya angka 1 menjadi string "satu", jadi pas websitenya 504 tadi, daripada gabut saya coba lah kerjakan satu satu tanpa bantuan apapun, dan setelah mencoba cukup lama saya menemukan flag di L30:



FLAG:WRECKIT60{m4TeM4t1k4_d0AnG_Su54h_4m4T}

Password?

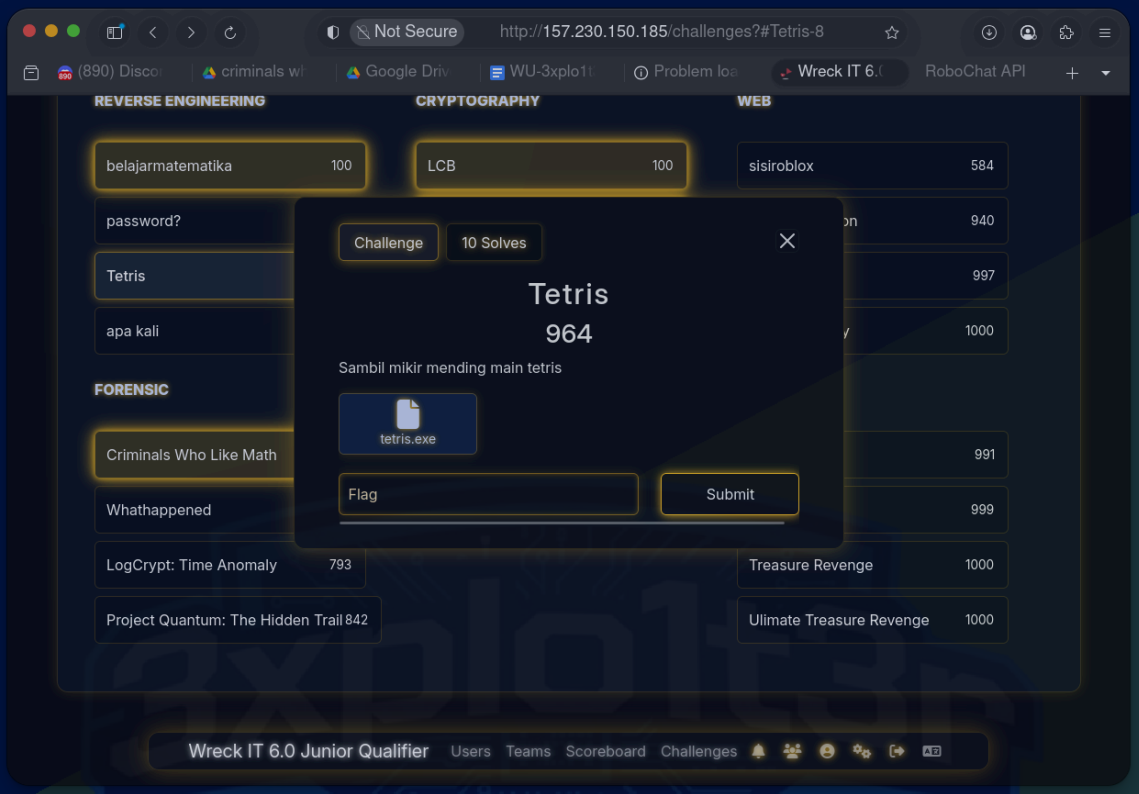


Solution

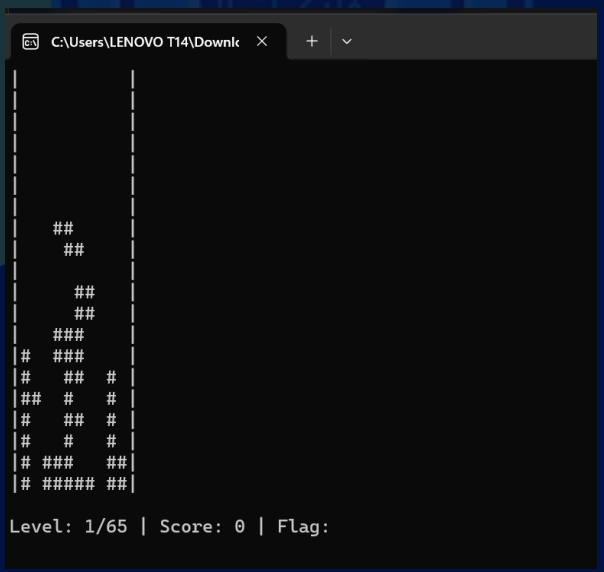
Di tantangan ini diberikan sebuah file dengan format exe yang ketika saya membukanya saya terhubung ke sebuah terminal dan disuruh memasukkan sebuah password.ketika saya mencoba memasukkan password yang salah maka akan terpental keluar program.

Tetapi karena keterbatasan waktu saya tidak berhasil menyelesaikan tantangan ini.

Tetris

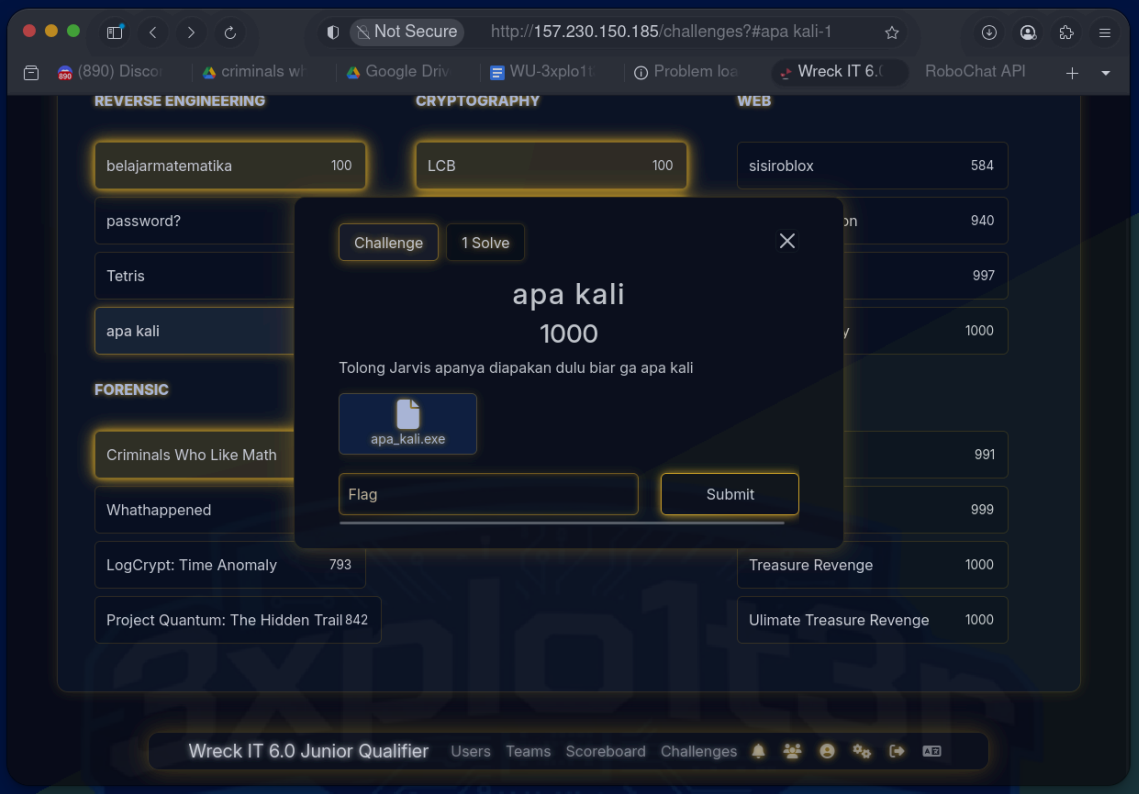


Solution



Karena terbatasnya waktu saya gagal menyelesaikan tantangan ini.

Apa Kali



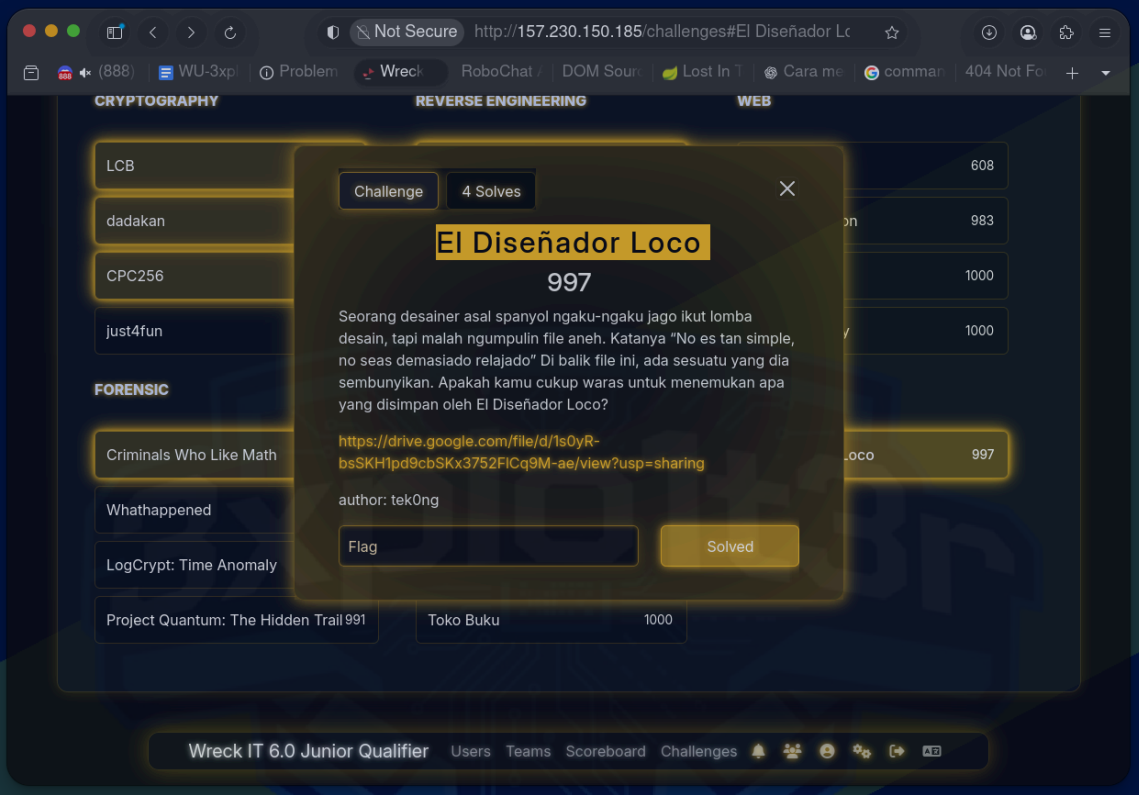
Solution

Pada tantangan ini diberikan sebuah file dengan format exe.ketika saya buka maka akan langsung diarahkan ke sebuah program yang meminta inputan .dan ketika saya menginputkan suatu kalimat program akan langsung tertutup.

Saya gagal menyelesaikan tantangan ini.

Miscellaneous

El Diseñador Loco



Solution

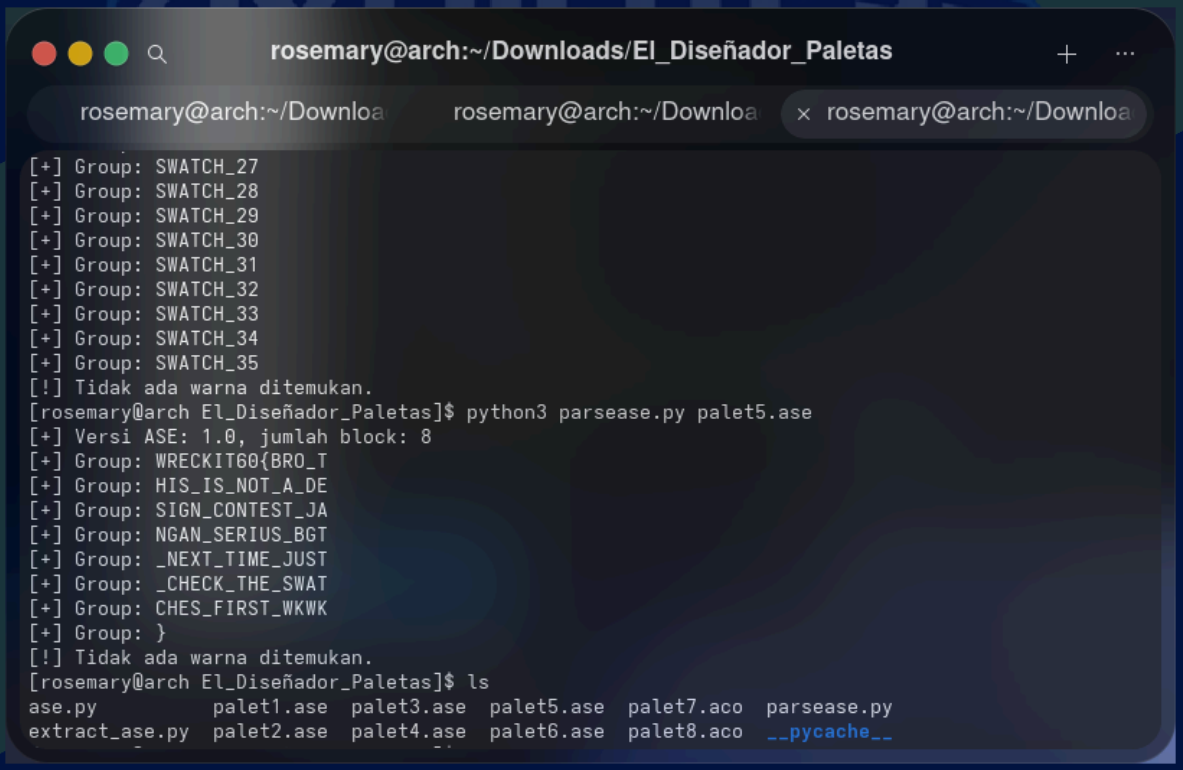
Disini saya diberikan sebuah file psd bernama Chall.psd, setelah saya dapat hint dari panitia, hintnya "Kau pikir aku akan meninggalkan warnaku di kanvas? Tidak. Warnaku hidup di tempat lain." dan dikasih file dari panitia berisi file .aco dan .ase, kemudian saya buat script python parsease.py untuk parse(menguraikan) file .ase nya, berikut kodenya:

```
import struct
import sys


def read_uint16(f):
   return struct.unpack(">H", f.read(2))[0]

def read_uint32(f):
```

```
    return struct.unpack(">I", f.read(4))[0]

def read_string(f):
    length = read_uint16(f)
    if length == 0:
        return ""
    data = f.read(length * 2)  # UTF-16BE
    return data.decode("utf-16be").rstrip("\x00")

def parse_ase(filename):
    with open(filename, "rb") as f:
        header = f.read(4)
        if header != b"ASEF":
            print("[!] Bukan file ASE valid.")
            return

        major = read_uint16(f)
        minor = read_uint16(f)
        block_count = read_uint32(f)
        print(f"[+] Versi ASE: {major}.{minor}, jumlah block:
{block_count}")

        colors = []
        for _ in range(block_count):
            block_type = read_uint16(f)
            block_length = read_uint32(f)
            start_pos = f.tell()


            if block_type == 0x0001:  # Group start
                group_name = read_string(f)
                print(f"[+] Group: {group_name}")
            elif block_type == 0x0002:  # Group end
                pass
            elif block_type == 0x0000:  # Color entry
                name = read_string(f)
                color_model = f.read(4).decode("ascii")
                color = tuple(struct.unpack(">f", f.read(4))[0] for
_ in range(3))
                color_type = read_uint16(f)
                colors.append((name, color))
            f.seek(start_pos + block_length)


        return colors


def main():
```

```
    if len(sys.argv) != 2:
        print(f"Usage: python {sys.argv[0]} <file.ase>")
        return

    filename = sys.argv[1]
    colors = parse_ase(filename)
    if not colors:
        print("[!] Tidak ada warna ditemukan.")
        return

    print("\n[+] Daftar warna:")
    for name, rgb in colors:
        print(f"Nama: {name} | RGB: {rgb}")

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

Kemudian saya jalankan python3 parsease.py palet1.ase sampai palet5.ase, nah di palet5.ase saya menemukan flagnya



FLAG:WRECKIT60{BRO_THIS_IS_NOT_A_DESIGN_CONTEST_JANGAN_SERIUS_BGT_NEXT_TIME_JUST_CHECK_THE_SWATCHES_FIRST_WKWK}

Thank You

The journey matters more than the flag.