WRECK IT 6.0

JUNIOR QUALIFICATION 2025

Nama Team : Un Grr

Anggota :

- Rafl
- 0xSpectre
- F3N4South

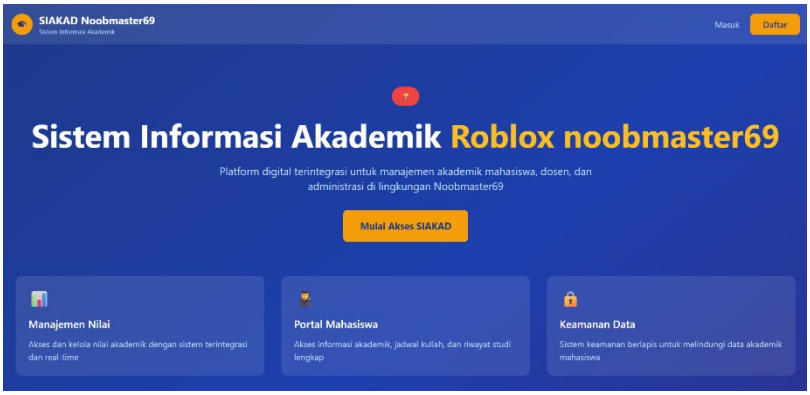
DAFTAR ISI

WEB

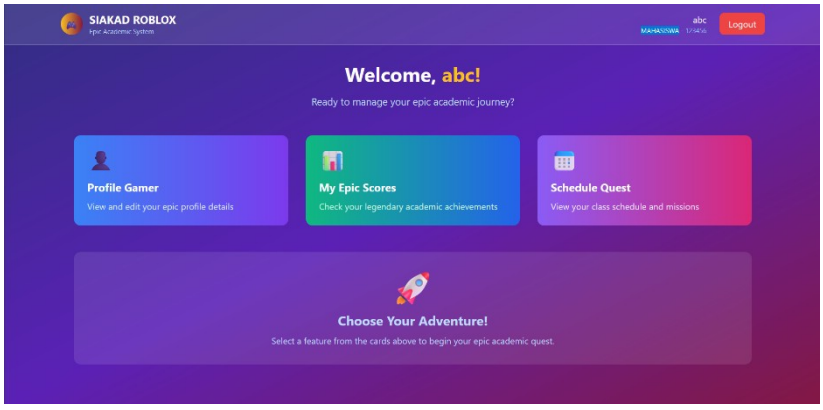
sisiroblox

Langkah Penyelesaian :

Pada chall ini, kami diarahkan menuju sebuah website SIAKAD Roblox.

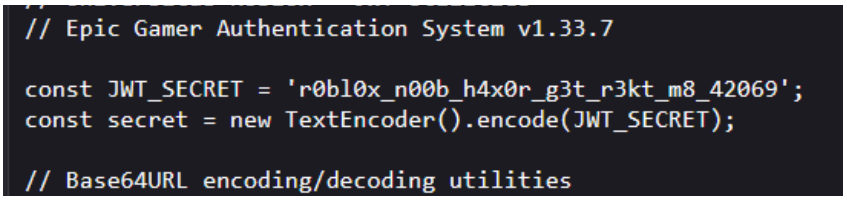


Setelah masuk ke web, saya daftar dan mendapatkan role mahasiswa.



Saat saya mengecek source code dari webnya saya menemukan clue yang mengarah pada JWT Token.

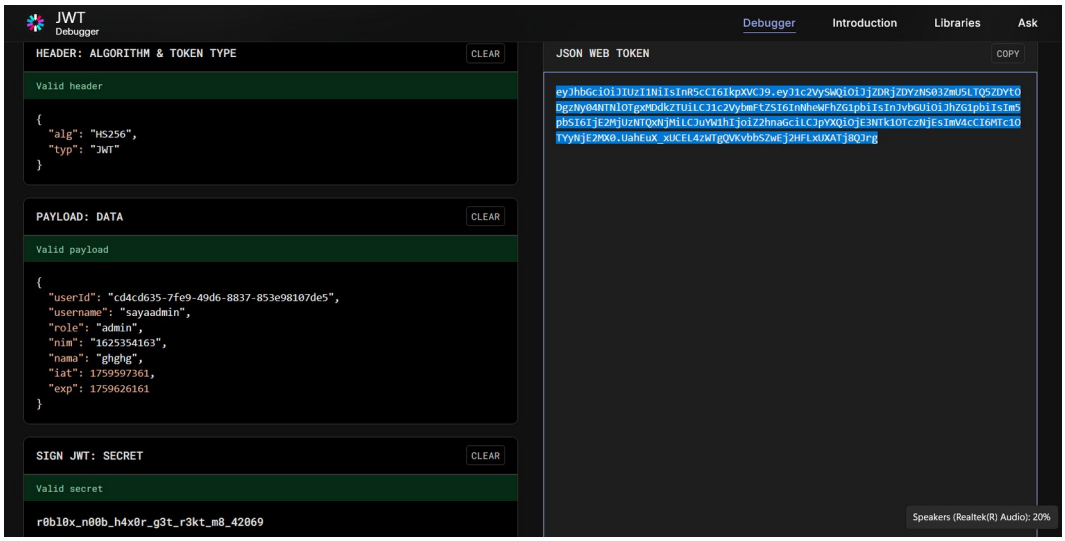
Didalam jwt.js terdapat JWT Secret seperti pada gambar.



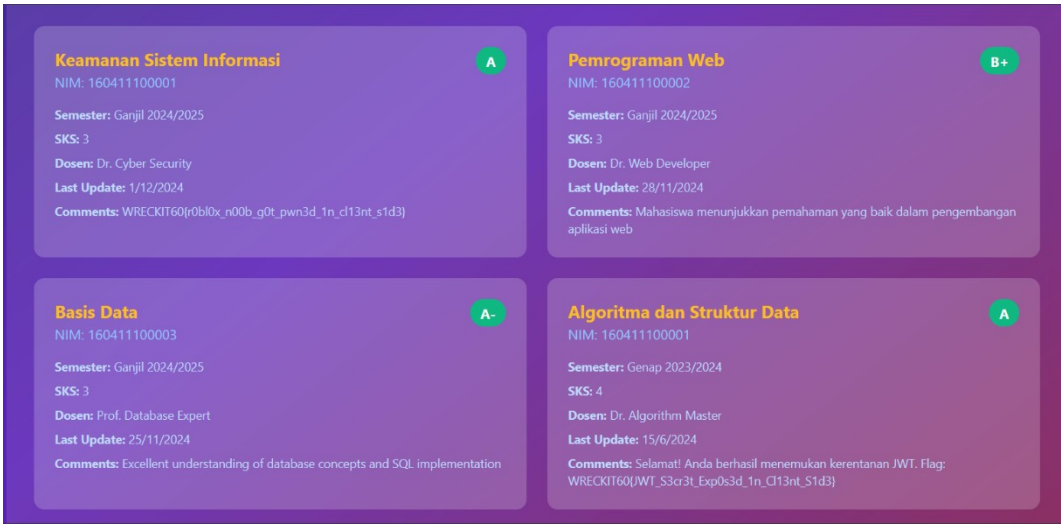
```
// Epic Gamer Authentication System v1.33.7

const JWT_SECRET = 'r0bl0x_n00b_h4x0r_g3t_r3kt_m8_42069';
const secret = new TextEncoder().encode(JWT_SECRET);

// Base64URL encoding/decoding utilities
```

Kemudian saya melakukan inspeksi kepada webnya dan menemukan authToken.

AuthToken yang ditemukan saya ambil dan saya input ke JWT.io dan saya melakukan modifikasi terhadap role yang awalnya “mahasiswa” menjadi “admin”. Selain itu, JWT Secret yang saya temukan saat inspeksi saya input ke secret dan menghasilkan output berupa JWT Token yang sudah dimodifikasi.



Hasil output JWT Token saya pakai untuk menggantikan token yang belum dimodifikasi untuk mendapatkan akses admin, dan flagnya.

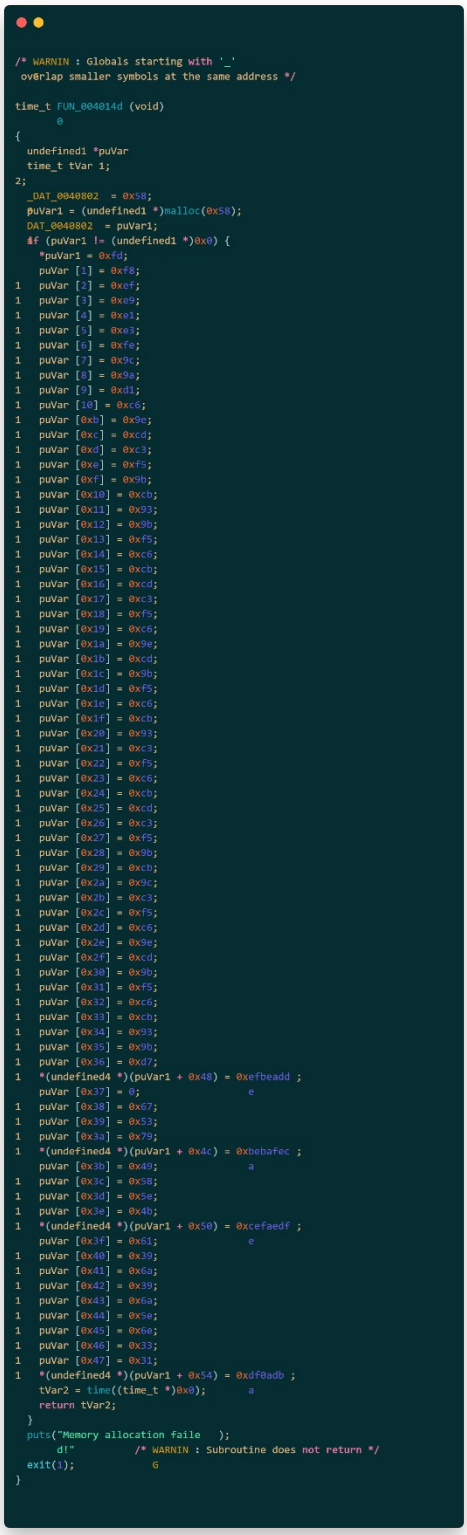


Flag :

WRECKIT60{r0bl0x_n00b_g0t_pwn3d_1n_cl13nt_s1d3}

REVERSE ENGINEERING

1.password?



```
/* WARNIN : Globals starting with '_'
 ov6rlap smaller symbols at the same address */

time_t FUN_004014d (void)
      0
{
  undefined1 *puVar
  time_t tVar 1;
2;
  _DAT_0040802  = 0x58;
  puVar1 = (undefined1 *)malloc(0x58);
  DAT_0040802  = puVar1;
  if (puVar1 != (undefined1 *)0x0) {
    *puVar1 = 0xfd;
    puVar [1] = 0xf8;
1   puVar [2] = 0xef;
1   puVar [3] = 0xe9;
1   puVar [4] = 0xe1;
1   puVar [5] = 0xe3;
1   puVar [6] = 0xfe;
1   puVar [7] = 0x9c;
1   puVar [8] = 0x9a;
1   puVar [9] = 0xd1;
1   puVar [10] = 0xc6;
1   puVar [0xb] = 0x9e;
1   puVar [0xc] = 0xcd;
1   puVar [0xd] = 0xc3;
1   puVar [0xe] = 0xf5;
1   puVar [0xf] = 0x9b;
1   puVar [0x10] = 0xcb;
1   puVar [0x11] = 0x93;
1   puVar [0x12] = 0x9b;
1   puVar [0x13] = 0xf5;
1   puVar [0x14] = 0xc6;
1   puVar [0x15] = 0xcb;
1   puVar [0x16] = 0xcd;
1   puVar [0x17] = 0xc3;
1   puVar [0x18] = 0xf5;
1   puVar [0x19] = 0xc6;
1   puVar [0x1a] = 0x9e;
1   puVar [0x1b] = 0xcd;
1   puVar [0x1c] = 0x9b;
1   puVar [0x1d] = 0xf5;
1   puVar [0x1e] = 0xc6;
1   puVar [0x1f] = 0xcb;
1   puVar [0x20] = 0x93;
1   puVar [0x21] = 0xc3;
1   puVar [0x22] = 0xf5;
1   puVar [0x23] = 0xc6;
1   puVar [0x24] = 0xcb;
1   puVar [0x25] = 0xcd;
1   puVar [0x26] = 0xc3;
1   puVar [0x27] = 0xf5;
1   puVar [0x28] = 0x9b;
1   puVar [0x29] = 0xcb;
1   puVar [0x2a] = 0x9c;
1   puVar [0x2b] = 0xc3;
1   puVar [0x2c] = 0xf5;
1   puVar [0x2d] = 0xc6;
1   puVar [0x2e] = 0x9e;
1   puVar [0x2f] = 0xcd;
1   puVar [0x30] = 0x9b;
1   puVar [0x31] = 0xf5;
1   puVar [0x32] = 0xc6;
1   puVar [0x33] = 0xcb;
1   puVar [0x34] = 0x93;
1   puVar [0x35] = 0x9b;
1   puVar [0x36] = 0xd7;
1   *(undefined4 *)(puVar1 + 0x48) = 0xefbeadd ;
    puVar [0x37] = 0;                 e
1   puVar [0x38] = 0x67;
1   puVar [0x39] = 0x53;
1   puVar [0x3a] = 0x79;
1   *(undefined4 *)(puVar1 + 0x4c) = 0xbebafec ;
    puVar [0x3b] = 0x49;              a
1   puVar [0x3c] = 0x58;
1   puVar [0x3d] = 0x5e;
1   puVar [0x3e] = 0x4b;
1   *(undefined4 *)(puVar1 + 0x50) = 0xcefaedf ;
    puVar [0x3f] = 0x61;              e
1   puVar [0x40] = 0x39;
1   puVar [0x41] = 0x6a;
1   puVar [0x42] = 0x39;
1   puVar [0x43] = 0x6a;
1   puVar [0x44] = 0x5e;
1   puVar [0x45] = 0x6e;
1   puVar [0x46] = 0x33;
1   puVar [0x47] = 0x31;
1   *(undefined4 *)(puVar1 + 0x54) = 0xdf0adb ;
    tVar2 = time((time_t *)0x0);      a
    return tVar2;
  }
  puts("Memory allocation faile   );
       d!"          /* WARNIN : Subroutine does not return */
  exit(1);            G
}
```

Langkah Penyelesaian :

Pada chall ini, diberikan sebuah file dengan format exe. Karena ini adalah chall reverse, saya langsung coba masukan password.exe ke ghidra, dan saya mendapatkan sebuah notasi heksadesimal seperti gambar disamping. Setelah itu saya meminta tolong pada ChatGPT untuk dibuatkan sebuah code python yang saya gunakan untuk mendecode notasi heksadesimal tersebut.

```
data = [
 0xfd,0xf8,0xef,0xe9,0xe1,0xe3,0xfe,0x9c,0x9a,0xd1,
 0xc6,0x9e,0xcd,0xc3,0xf5,0x9b,0xcb,0x93,0x9b,0xf5,
 0xc6,0xcb,0xcd,0xc3,0xf5,0xc6,0x9e,0xcd,0x9b,0xf5,
 0xc6,0xcb,0x93,0xc3,0xf5,0xc6,0xcb,0xcd,0xc3,0xf5,
 0x9b,0xcb,0x9c,0xc3,0xf5,0xc6,0x9e,0xcd,0x9b,0xf5,
 0xc6,0xcb,0x93,0x9b,0xd7
]

key = data[0] ^ ord('W')

decoded = ''.join(chr(b ^ key) for b in data)
print("Key: 0 {:02X}".format(key))
print(%Decode    , decoded)
      d:"
```

Dari baris code tersebut, didapatlah output berupa flag.

```
Key: 0xAA
Decoded: WRECKIT60{l4gi_1a91_lagi_l4g1_la9i_lagi_1a6i_l4g1_la91}
PS C:\Users\rafel\Code>
```

Flag :

WRECKIT60{l4gi_1a91_lagi_L4g1_la9i_lagi_1a6i_l4g1_La91}

Namun seharian ini terdapat banyak masalah pada server web Wreck IT, yang membuat saya dan team tidak dapat mengsubmit flag ini dengan tepat waktu.