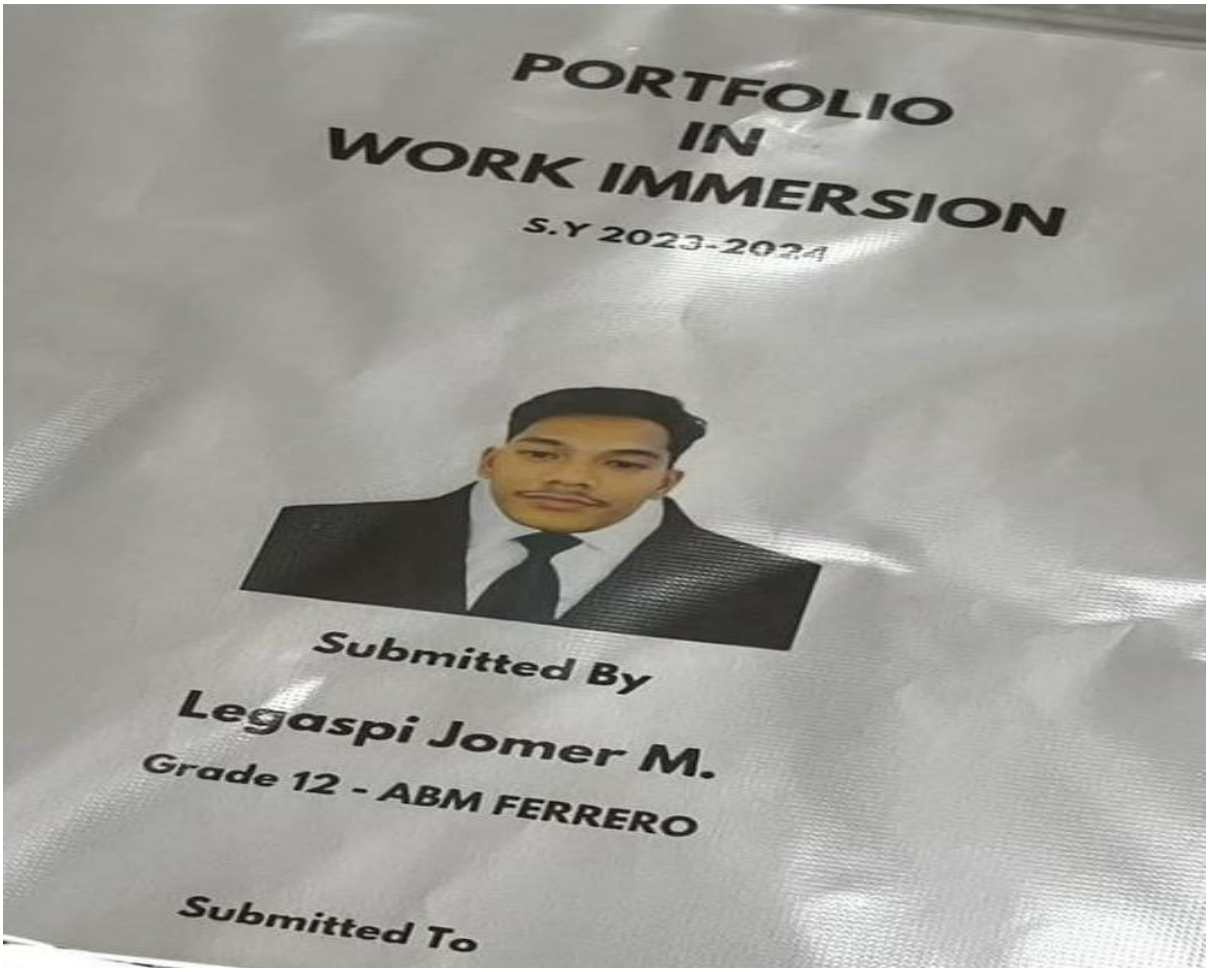
Write-Up Freepass POROS 2025



Author : broKen

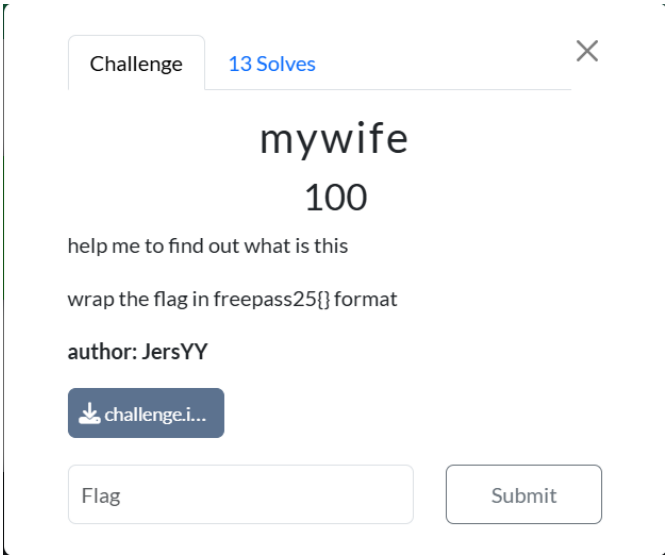
Mohammad Iqbal Bagas Permana

245140701111024

Teknologi Informasi

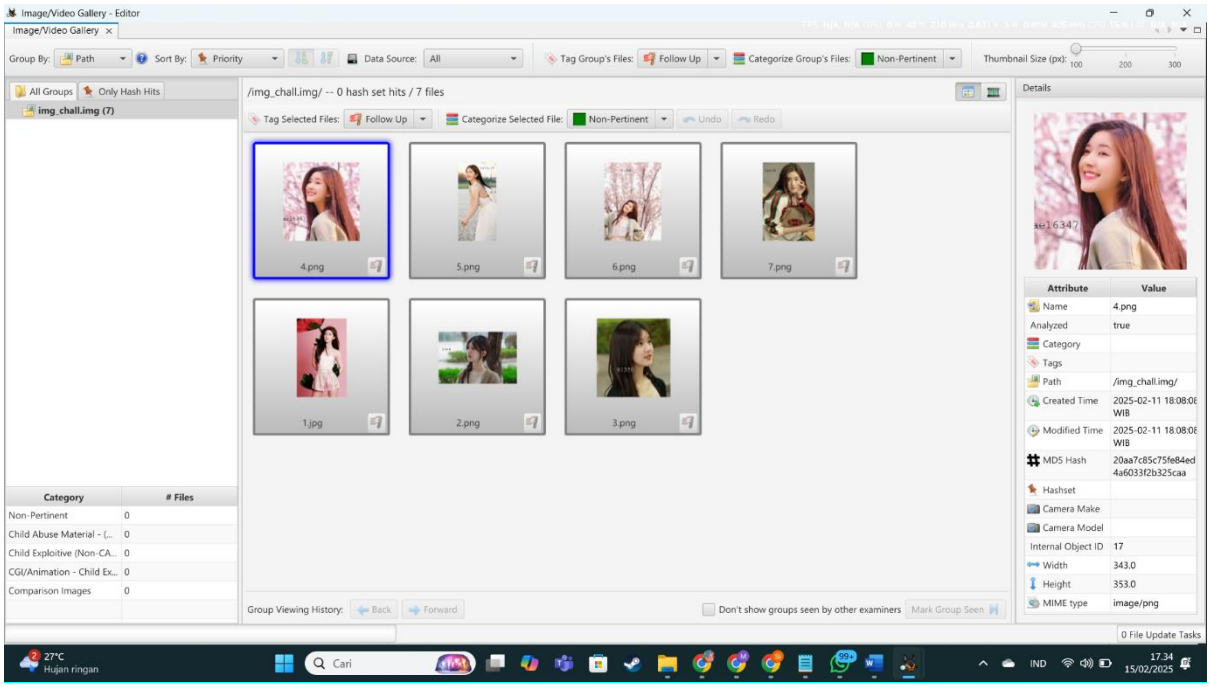
Forensics

1. **Mywife**



Pada challenge ini, diberikan sebuah file .img. Dan ini merupakan challenge disk analysis dan biasanya dalam CTF, tipe file ini dapat dibuka dengan menggunakan Autopsy.

Jadi mari kita langsung saja buka menggunakan Autopsy.

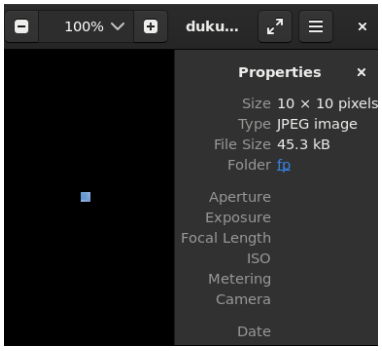


Dan benar saja, ketika kita buka dengan Autopsy terdapat beberapa gambar yang berisi teks yang kemungkinan adalah flag. Langsung saja kita wrap teks yang ada pada png tersebut dan voilà, flagnya adalah

freepass25{2ace91350ae16347fd38a3554844fe04}

2. **Tiny**

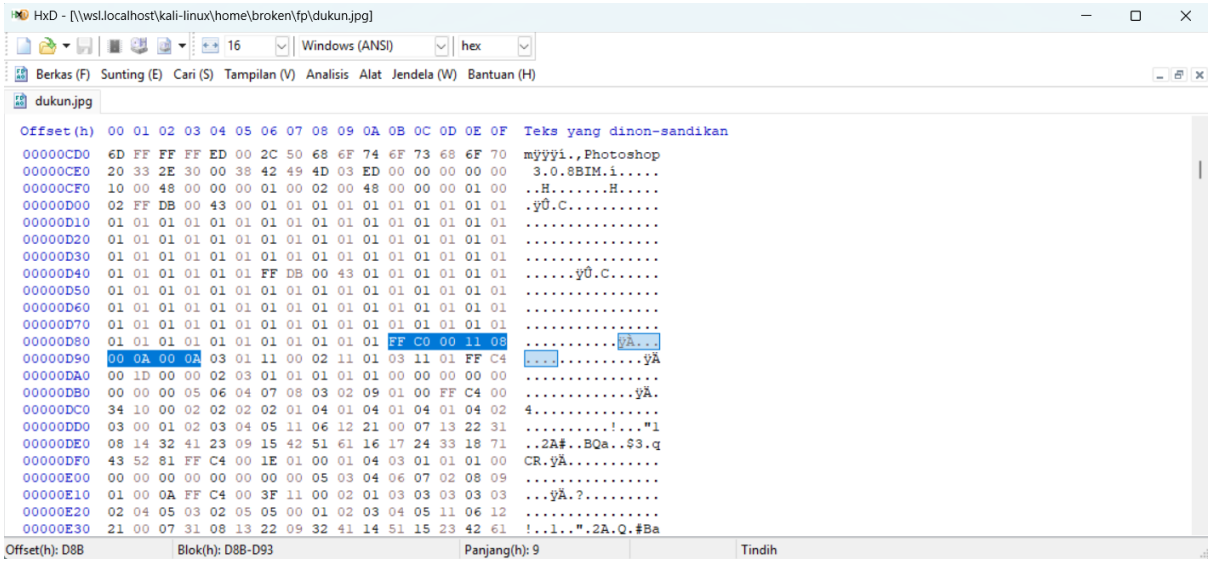
Pada chall ini diberikan sebuah chall .jpg. Langsung saja kita download file tersebut dan melakukan inspeksi lebih dalam. Pertama-tama, saya melakukan eog pada file jpg tersebut.



dan menariknya, file tersebut hanya berukuran 10x10. Dan saya berpikir mungkin ini adalah challenge hexedit dengan mengubah size pixel file tersebut.

Langsung saja kita buka file dengan Hxd dan mencari bagian hex mana yang merupakan size jpg tersebut dengan mencari header yang menunjukkan bagian resolusi.

Langsung saja kita filter nilai hex ffc0 pada Hxd dan saya menemukan ini



Menurut informasi gambar yang saya berikan sebelumnya, dapat kita asumsikan 0A adalah hex untuk nilai 10.

Mari kita ubah hex size tersebut. Pertama saya ubah size ke ukuran 1000x1000 dan sepertinya size ini masih terlalu besar untuk jpg ini. Jadi saya mencoba pendekatan dengan size yang lebih kecil, tetapi ketika saya melihat jpg tersebut sepertinya harus memiliki size yang tepat karena saya mengganti file ini berkali-kali isinya scrambled dan tidak dapat dibaca.

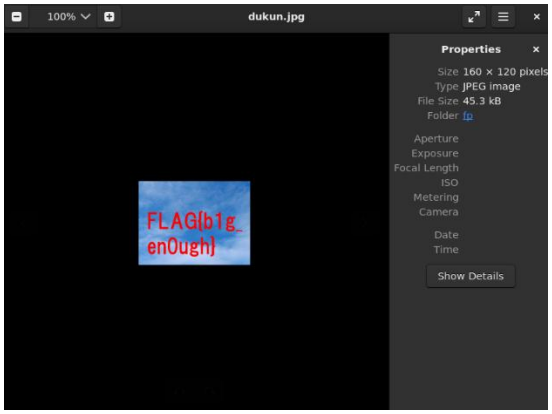
Karena tak kunjung menemukan size yang tepat, saya mencoba menggunakan tools lain untuk inspeksi apakah ada size asli dari jpg ini. Saya telah mencoba tools seperti String, StegSolve, binwalk dan tidak menemukan hal yang menarik. Dan akhirnya saya memutuskan untuk mencari ukuran asli file ini di internet dengan mencari info info yang penting dari exiftool seperti data profile seperti ID, Creator, date time dll. Dan telah mendapatkan beberapa metadata yang sesuai tapi untuk size masih belum tepat.

```
[ICC-header]    Profile Creator                 : Hewlett-Packard
[ICC-header]    Profile ID                      : 0
[ICC_Profile]   Profile Copyright               : Copyright (c) 1998 Hewlett-Packard Company
[ICC_Profile]   Profile Description             : sRGB IEC61966-2.1
[ICC_Profile]   Media White Point               : 0.95045 1 1.08905
[ICC_Profile]   Media Black Point               : 0 0 0
[ICC_Profile]   Red Matrix Column               : 0.43607 0.22249 0.01392
[ICC_Profile]   Green Matrix Column             : 0.38515 0.71687 0.09708
[ICC_Profile]   Blue Matrix Column              : 0.14307 0.06061 0.7141
[ICC_Profile]   Device Mfg Desc                 : IEC http://www.iec.ch
[ICC_Profile]   Device Model Desc               : IEC 61966-2.1 Default RGB colour space - sRGB
[ICC_Profile]   Viewing Cond Desc               : Reference Viewing Condition in IEC61966-2.1
[ICC-view]      Viewing Cond Illuminant         : 19.6445 20.3718 16.8089
[ICC-view]      Viewing Cond Surround           : 3.92889 4.07439 3.36179
[ICC-view]      Viewing Cond Illuminant Type    : D50
[ICC_Profile]   Luminance                       : 76.03647 80 87.12462
[ICC-meas]      Measurement Observer            : CIE 1931
[ICC-meas]      Measurement Backing             : 0 0 0
[ICC-meas]      Measurement Geometry            : Unknown
[ICC-meas]      Measurement Flare               : 0.999%
[ICC-meas]      Measurement Illuminant          : D65
[ICC_Profile]   Technology                      : Cathode Ray Tube Display
[ICC_Profile]   Red Tone Reproduction Curve     : (Binary data 2060 bytes, use -b option to extract)
[ICC_Profile]   Green Tone Reproduction Curve   : (Binary data 2060 bytes, use -b option to extract)
[ICC_Profile]   Blue Tone Reproduction Curve    : (Binary data 2060 bytes, use -b option to extract)
[File]          Current IPTC Digest             : 49e81a2fa795a7a56ac703c85b560ab3
[IPTC]          Coded Character Set             : UTF8
[IPTC]          Envelope Record Version         : 4
[IPTC]          Date Created                    : 2021:03:11
[IPTC]          Digital Creation Date           : 2021:03:11
[IPTC]          Digital Creation Time           : 21:26:05-04:00
[IPTC]          Application Record Version      : 4
[IPTC]          Time Created                    : 21:26:05-04:00
[IPTC]          Keywords                        : Who|People|In Pic|Alex Mustelier
[Photoshop]     IPTC Digest                     : 49e81a2fa795a7a56ac703c85b560ab3
[File]          Image Width                     : 2912
[File]          Image Height                    : 4368
```

Saya mencoba lagi untuk menemukan sumber lainnya dan menemukan :

```
[ICC_Profile, ICC_Profile, Image] cprt - Profile Copyright: Copyright (c) 1998 Hewlett-Packard Company
[ICC_Profile, ICC_Profile, Image] desc - Profile Description: sRGB IEC61966-2.1
[ICC_Profile, ICC_Profile, Image] wtpt - Media White Point: 0.95045 1 1.08905
[ICC_Profile, ICC_Profile, Image] bkpt - Media Black Point: 0 0 0
[ICC_Profile, ICC_Profile, Image] rXYZ - Red Matrix Column: 0.43607 0.22249 0.01392
[ICC_Profile, ICC_Profile, Image] gXYZ - Green Matrix Column: 0.38515 0.71687 0.09708
[ICC_Profile, ICC_Profile, Image] bXYZ - Blue Matrix Column: 0.14307 0.06061 0.7141
[ICC_Profile, ICC_Profile, Camera] dmnd - Device Mfg Desc: IEC http://www.iec.ch
[ICC_Profile, ICC_Profile, Camera] dmdd - Device Model Desc: IEC 61966-2.1 Default RGB colour space - sRGB
[ICC_Profile, ICC_Profile, Image] vued - Viewing Cond Desc: Reference Viewing Condition in IEC61966-2.1
[ICC_Profile, ICC-view, Image] 8 - Viewing Cond Illuminant: 19.6445 20.3718 16.8089
[ICC_Profile, ICC-view, Image] 20 - Viewing Cond Surround: 3.92889 4.07439 3.36179
[ICC_Profile, ICC-view, Image] 32 - Viewing Cond Illuminant Type: D50
[ICC_Profile, ICC_Profile, Image] lumi - Luminance: 76.03647 80 87.12462
[ICC_Profile, ICC-meas, Image] 8 - Measurement Observer: CIE 1931
[ICC_Profile, ICC-meas, Image] 12 - Measurement Backing: 0 0 0
[ICC_Profile, ICC-meas, Image] 24 - Measurement Geometry: Unknown (0)
[ICC_Profile, ICC-meas, Image] 28 - Measurement Flare: 0.999 %
[ICC_Profile, ICC-meas, Image] 32 - Measurement Illuminant: D65
[ICC_Profile, ICC_Profile, Image] tech - Technology: Cathode Ray Tube Display
[ICC_Profile, ICC_Profile, Image] rTRC - Red Tone Reproduction Curve: (Binary data 2060 bytes)
[ICC_Profile, ICC_Profile, Image] gTRC - Green Tone Reproduction Curve: (Binary data 2060 bytes)
[ICC_Profile, ICC_Profile, Image] bTRC - Blue Tone Reproduction Curve: (Binary data 2060 bytes)
[Composite, Composite, Image]  - Image Size: 160x120
```

Dan setelah saya coba Image size website tersebut dan ternyata

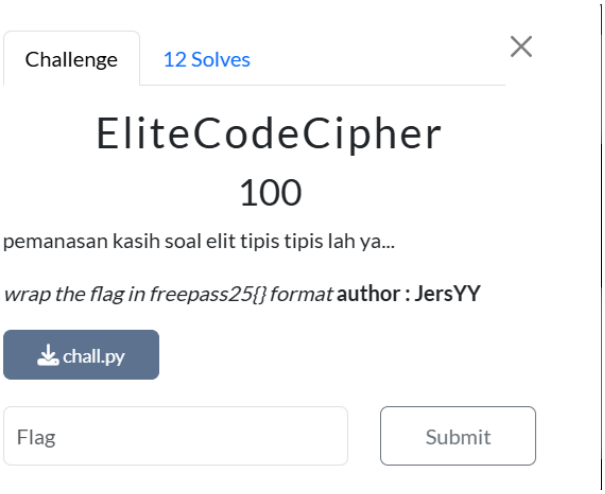


Voilà size benar dan challenge solved

Flag : freepas25{b1g_en0ugh}

Cryptography

1. EliteCodeCipher



Pada chall ini diberikan sebuah file python dan langsung saja kita buka file tersebut. Sebelum kita lanjut lebih dalam tentang ECC (EllipticCurve), mari kita pahami bagaimana logika matematika dasar untuk menemukan flag.

Jika kita perhatikan, untuk mendapatkan flag, kita memerlukan variabel $\boldsymbol{n}$ yang dapat kita dapatkan dari persamaan $P = n * G$. Dan kita harus menggunakan aturan ECC untuk mencari variabel n pada persamaan tersebut karena, P dan G bukan menggunakan perhitungan biasa, melainkan menggunakan perhitungan ECC dengan input garis x dan y.

Berikut adalah rumus ECC dalam kode ini

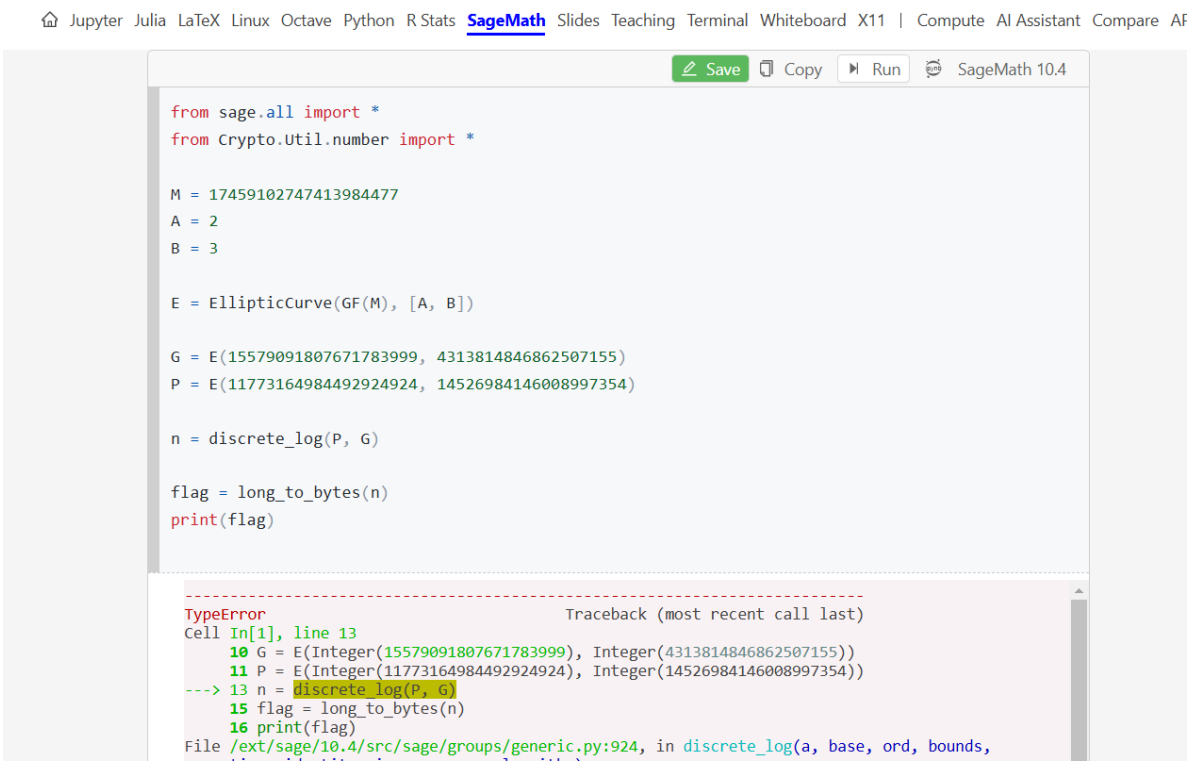
$$y2 = x3 + Ax + B \ mod \ M$$

Yang dimana : A dan B adalah konstanta, M adalah Kurva hingga, sedangkan y dan x adalah input koordinat yang akan dimasukkan.

Saya tidak akan menjelaskan terlalu detail tentang perhitungannya tetapi intinya semua variabel yang diperlukan untuk perhitungan persamaan tersebut telah dipenuhi (Termasuk koordinat x dan y untuk masing-masing variabel P dan G). Dan untuk mencari nilai n pada hasil persamaan yang melibatkan ECC tersebut, kita dapat menggunakan discrete_log yang ada di SageMath.

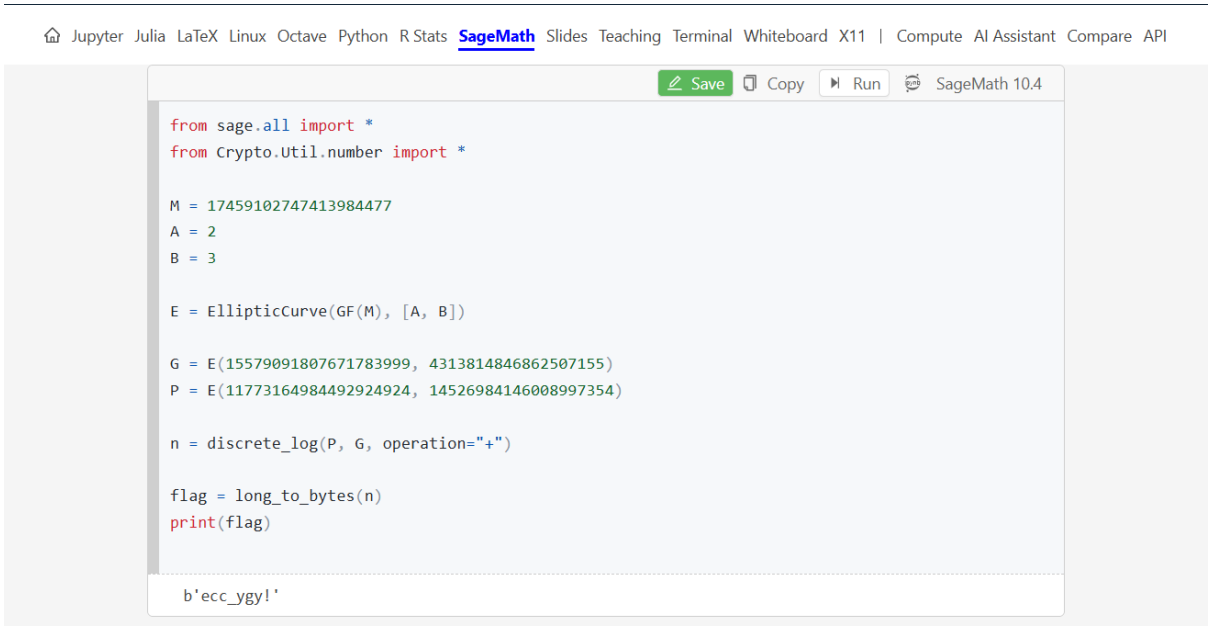
Berikut script kode pyhton untuk menemukan n.

(Saya menggunakan decoder online karena Tidak memiliki Library Sagemath yang terinstall)



Kode pertama saya ketika saya run mengalami error, dan sepertinya terdapat kesalahan pada baris ke 13 di perhitungan discrete_log. Dan setelah saya research lagi apa kesalahannya, ternyata dalam ECC kita harus menggunakan *operation* = " + " untuk perhitungan ECC agar kita melakukan penjumlahan titik dan bukan perkalian biasa.

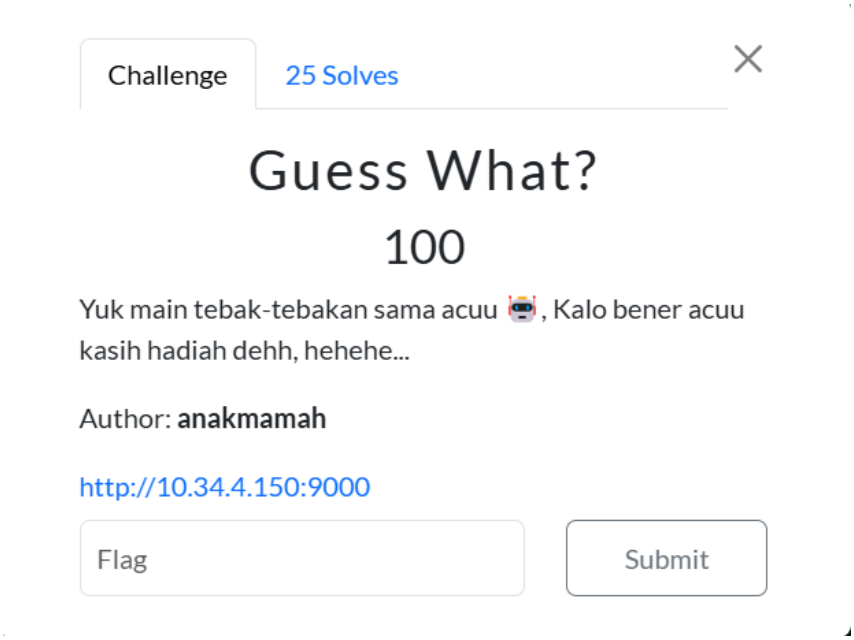
Dan setelah saya benarkan kodenya dan saya mendapatkan



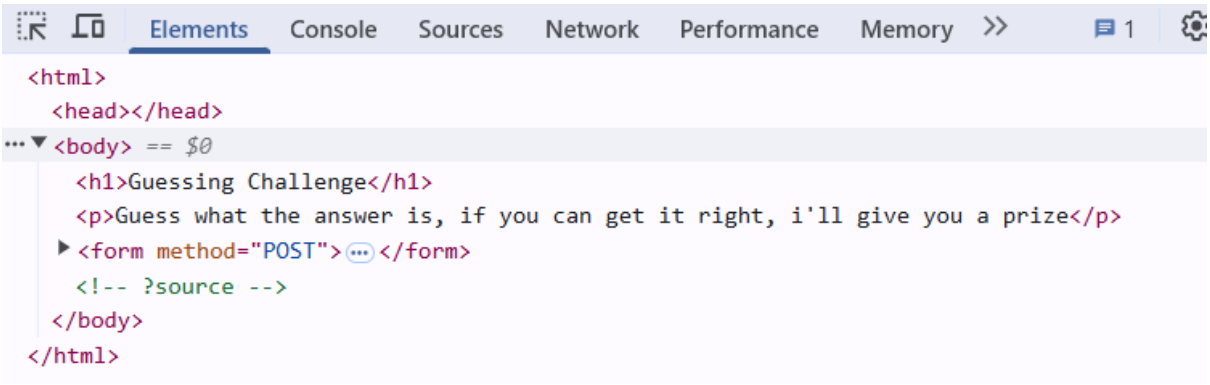
Dan voilà, Flagnya adalah freepass25{ecc_ygy!}

Web Exploitation

1. **Guess What?**



Pada Challenge ini diberikan sebuah link website, dan kita akan coba masuk terlebih dahulu. Ketika saya coba memasukkan sesuatu pada box answer sepertinya tidak memberikan apapun dan saya mulai inspect website ini. Dan saya menemukan comment yang menarik yaitu



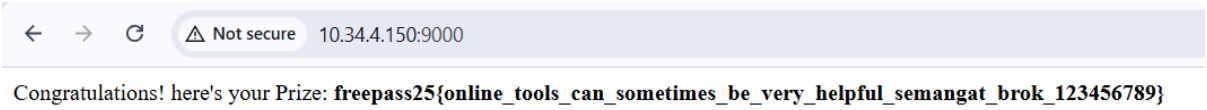
Terdapat hint ?source, mari kita coba memasukkan /?source ke alamat website tersebut. Dan kita akan mendapatkan cara untuk mendapatkan flag tersebut.

```
$hash1 = md5($input1);
$reversed = "25203fcbba1a52a482fe46e34507dd69";

if ($hash1 == $reversed) {
    echo "Congratulations! here's your Prize: <strong>" . $flag . "</strong>";
```

Dalam kode tersebut dituliskan jika $hash1 == $reversed, maka kita akan mendapatkan flag. Dan karena $hash1 adalah input answer kita yang di

hash dengan md5, maka kita harus decode hash md5 yang ada pada $reversed dan menginputnya pada answer. Saya mencoba berbagai website decoder online untuk md5 hash dan akhirnya saya menemukan satu website decoder yang works dan ternyata setelah di decode :

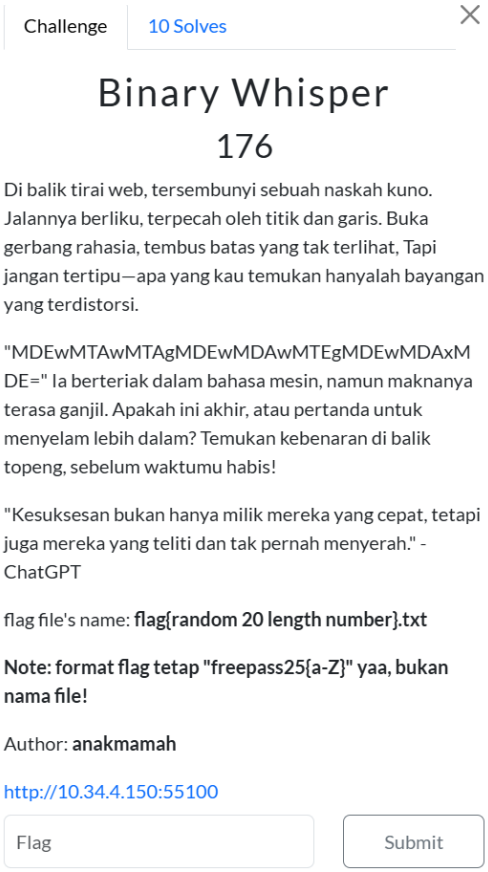
Hash tersebut memiliki value “POROSJUARA” dan langsung saja kita masukkan String tersebut ke dalam input answer pada website



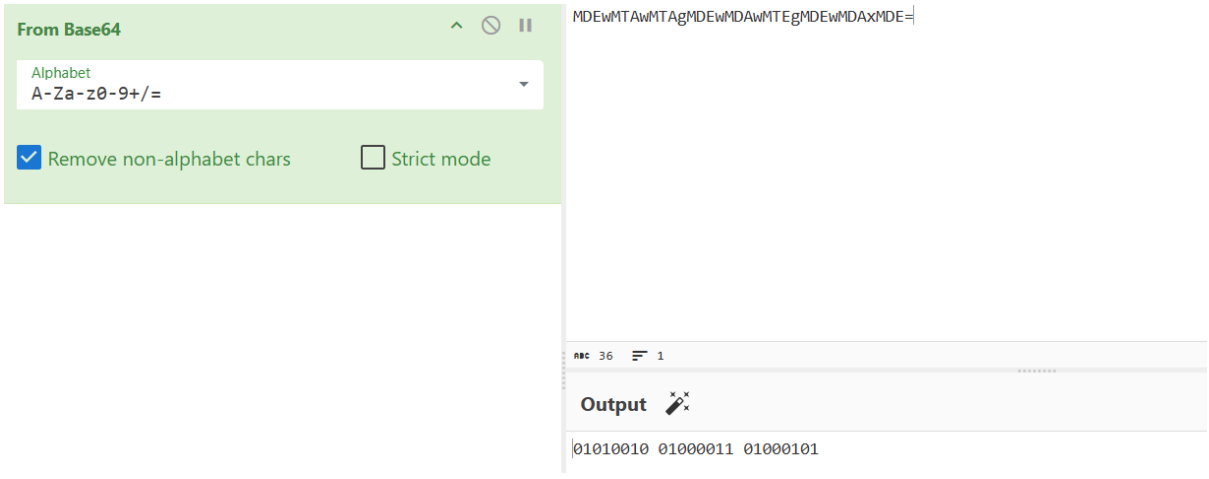
dan voilà Flagnya adalah

freepass25{online_tools_can_sometimes_be_very_helpful_semangat_brok_123456789}

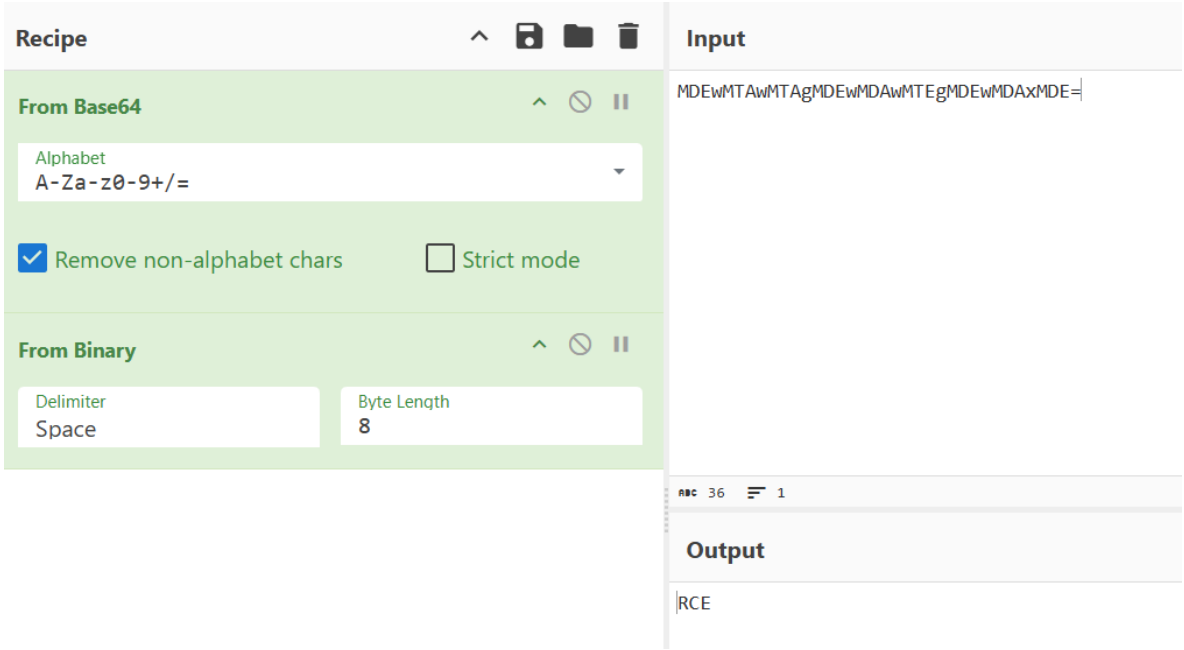
2. **Binary Whisper**



Pada challenge ini diberikan deskripsi yang panjang dan sebuah link website, dan di deskripsi tersebut terdapat kode yang sepertinya merupakan base64, langsung saja kita decode



Ternyata hasilnya biner, mari kita decode lagi



Dan hasilnya tertulis RCE. (Remote Control Execution) RCE sendiri yaitu Salah satu jenis kerentanan website dengan melakukan input kode dari jarak jauh. Tetapi, sebelum melangkah lebih jauh tentang RCE, saya mencoba untuk melakukan inspect pada web tersebut. Dan saya menemukan

```
<!-- /view-server ini apaa yaaaa??? -->
```

Dan setelah saya coba, saya menemukan suatu hal yang menarik

```
if (containsForbiddenWords(message)) {
  return res
    .status(400)
    .send("Error: Forbidden content detected in the message.");
}

try {
  const result = eval(message);
  const binaryString = (text) => {
    return text
      .toString()
      .split("")
      .map((char) => char.charCodeAt(0).toString(2).padStart(8, "0"))
      .join(" ");
  };
```

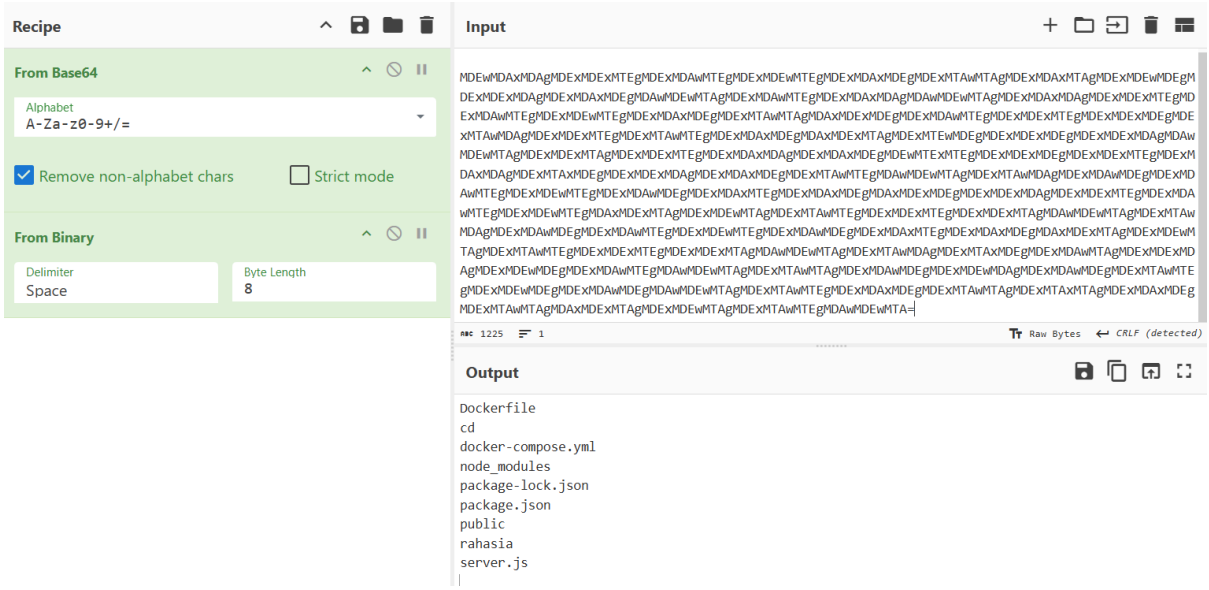
Disini terdapat forbiddenwords dan yang membuat saya curiga adalah forbidden words hanya berlaku pada input di bagian message, kecurigaan saya diperkuat dengan adanya eval(message) yang dimana hal ini digunakan untuk mengeksekusi string sebagai kode JavaScript sehingga ketika kita memasukkan input kode string ke dalam input message, maka kode tersebut akan dieksekusi. Hal ini juga diperkuat dengan hint chall ini yaitu RCE.

Maka, saya melanjutkan pengerjaan chall ini dengan mencari tahu apa saja cara untuk mengeksploitasi hal ini, Saya mencoba input dengan {{5*5}} dan menghasilkan

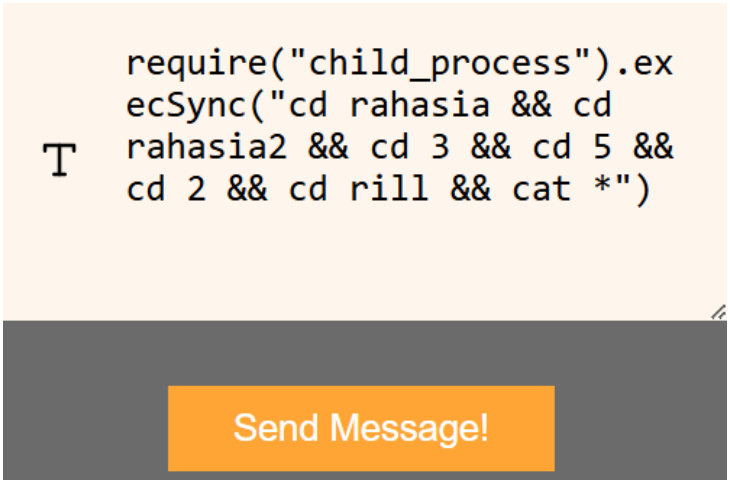
Output:
MDAxMTAwMTAgMDAxMTAxMDE=

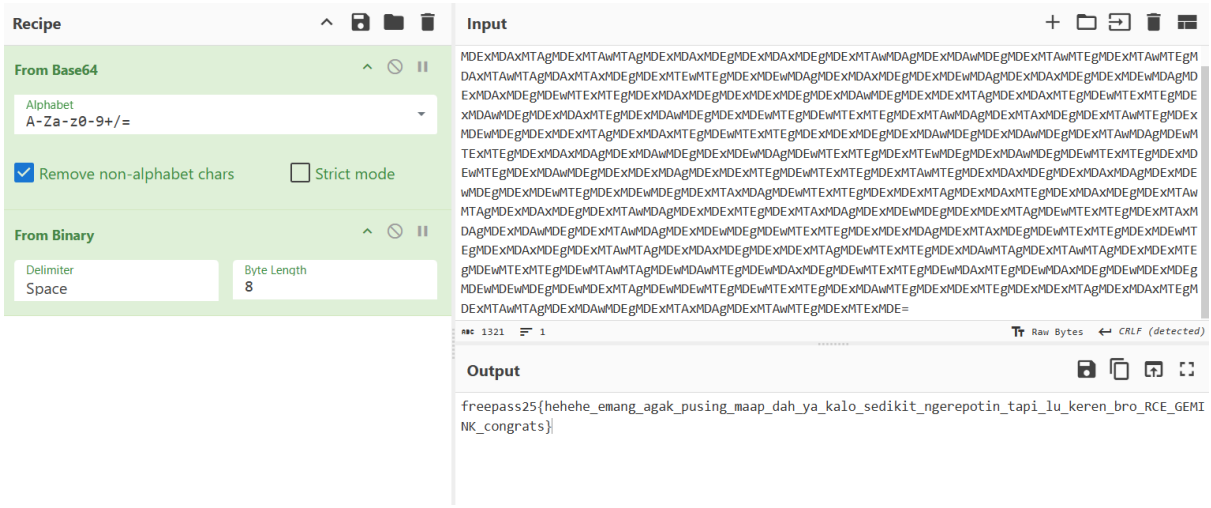
Dan ketika saya decode menjadi angka 25, Sepertinya ini merupakan kerentanan (Server Side Template Injection) SSTI dan saya mencoba untuk mencari input command lain dan menemukan require("child_process").execSync() yang dapat mengeksekusi ke dalam direktori server. Langsung saja kita coba :

Ketika saya send Message :



Dan terdapat beberapa direktori, dan saya akan langsung saja ke direktori yang benar, karena direktorinya sangat banyak dan nested.

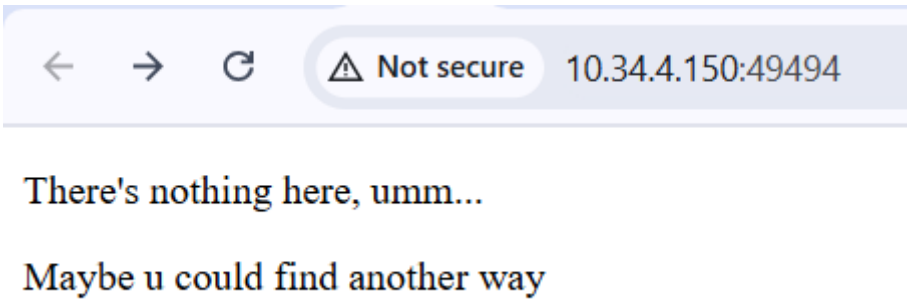




Dan voilà flagnya adalah
freepass25{hehehe_emang_agak_pusing_maap_dah_ya_kalo_sedikit_ngerepotin_tapi_lu_keren_bro_RCE_GEMINK_congrats}

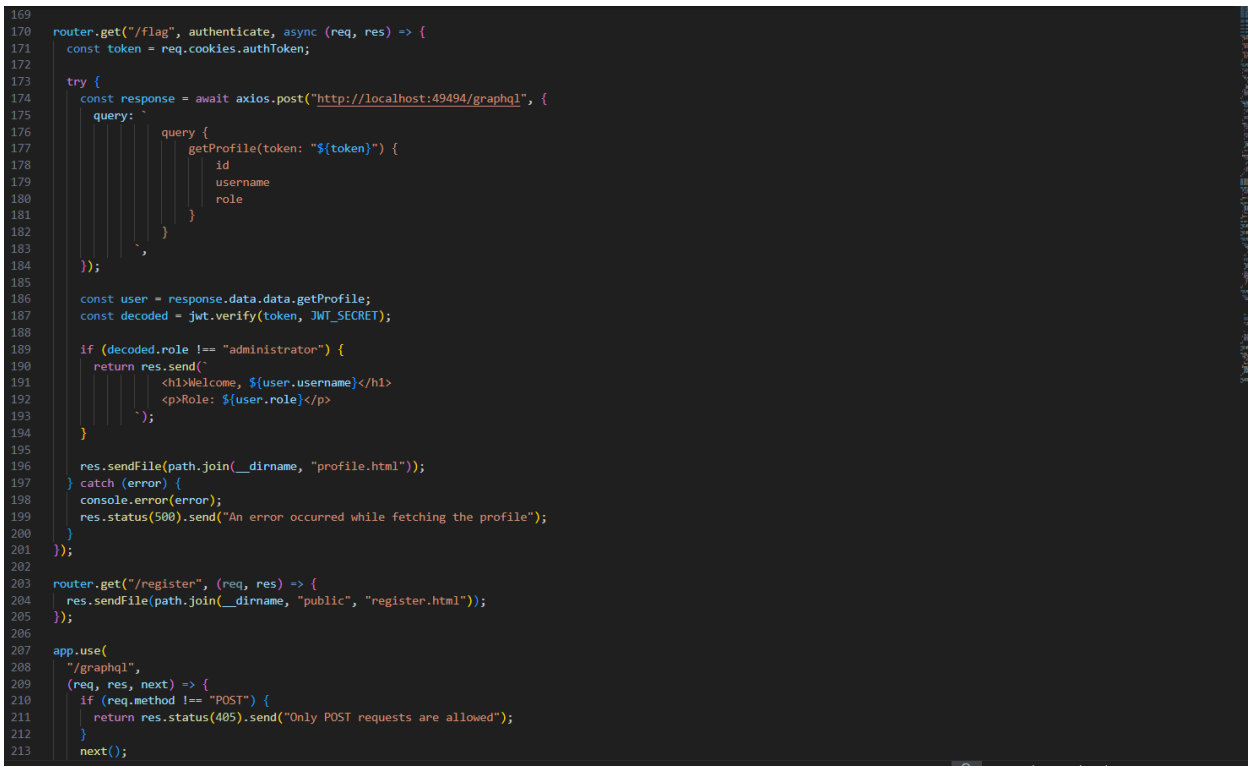
3. **Atmin Raja Iblis**

Pada chall ini diberi sebuah challenge yang berisi link website dan source code javascript dari server tersebut dan langsung saja kita buka.



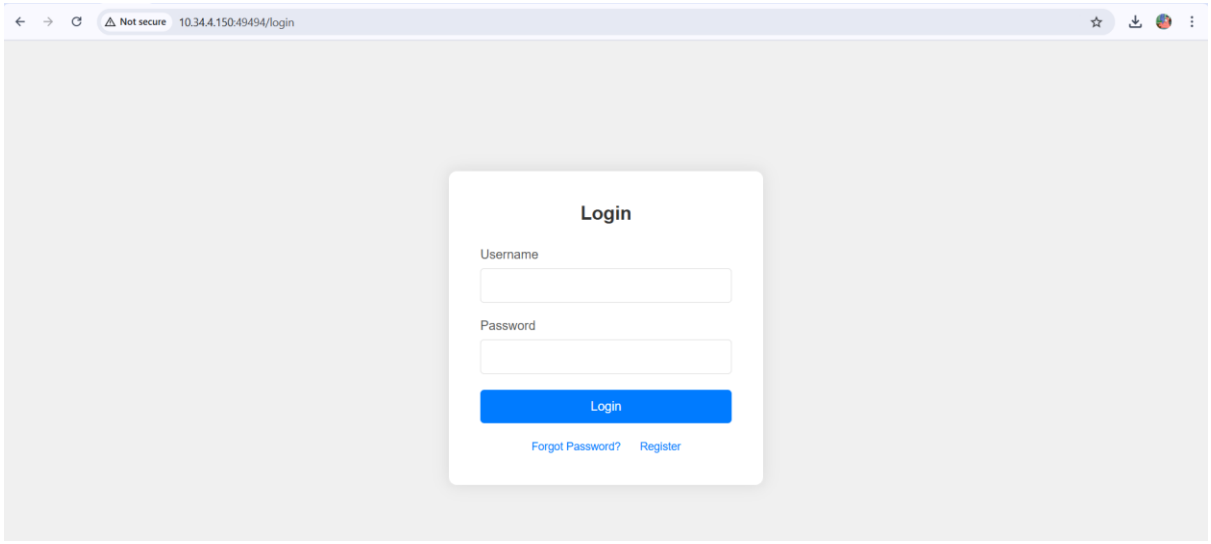
Dan sepertinya nothing here, dan ketika saya inspect juga tidak menemukan hal yang menarik, jadi mari kita check source code yang diberikan.

Sepertinya source code merupakan kunci bagaimana kita akan solve challenge ini.

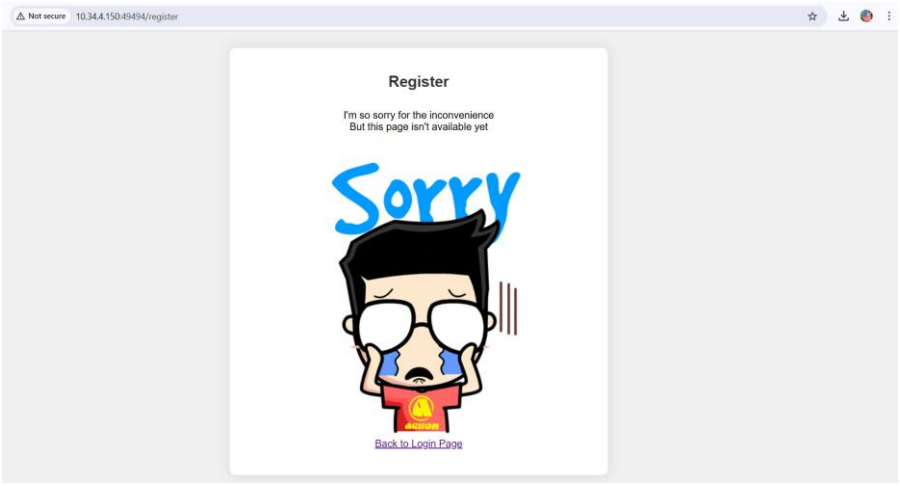


```
router.get("/flag", authenticate, async (req, res) => {
  const token = req.cookies.authToken;

  try {
    const response = await axios.post("http://localhost:49494/graphql", {
      query: `
              query {
                getProfile(token: "${token}") {
                  id
                  username
                  role
                }
              }
            `,
    });

    const user = response.data.data.getProfile;
    const decoded = jwt.verify(token, JWT_SECRET);

    if (decoded.role !== "administrator") {
      return res.send(`
              <h1>Welcome, ${user.username}</h1>
              <p>Role: ${user.role}</p>
            `);
    }

    res.sendFile(path.join(__dirname, "profile.html"));
  } catch (error) {
    console.error(error);
    res.status(500).send("An error occurred while fetching the profile");
  }
});

router.get("/register", (req, res) => {
  res.sendFile(path.join(__dirname, "public", "register.html"));
});

app.use(
  "/graphql",
  (req, res, next) => {
    if (req.method !== "POST") {
      return res.status(405).send("Only POST requests are allowed");
    }
    next();
```

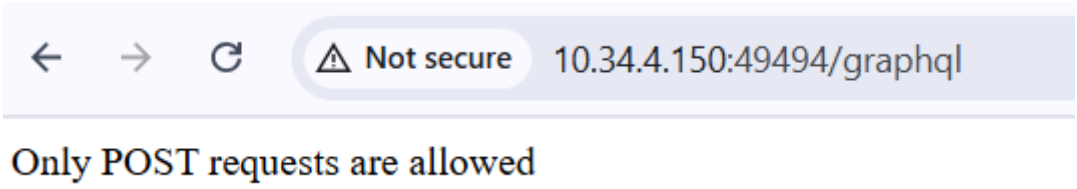
Terdapat sesuatu yang menarik ada /flag, /register, dan /graphql dan ada JWT secret, sepertinya ini adalah challenge terkait JWT token. Ketika saya check /flag



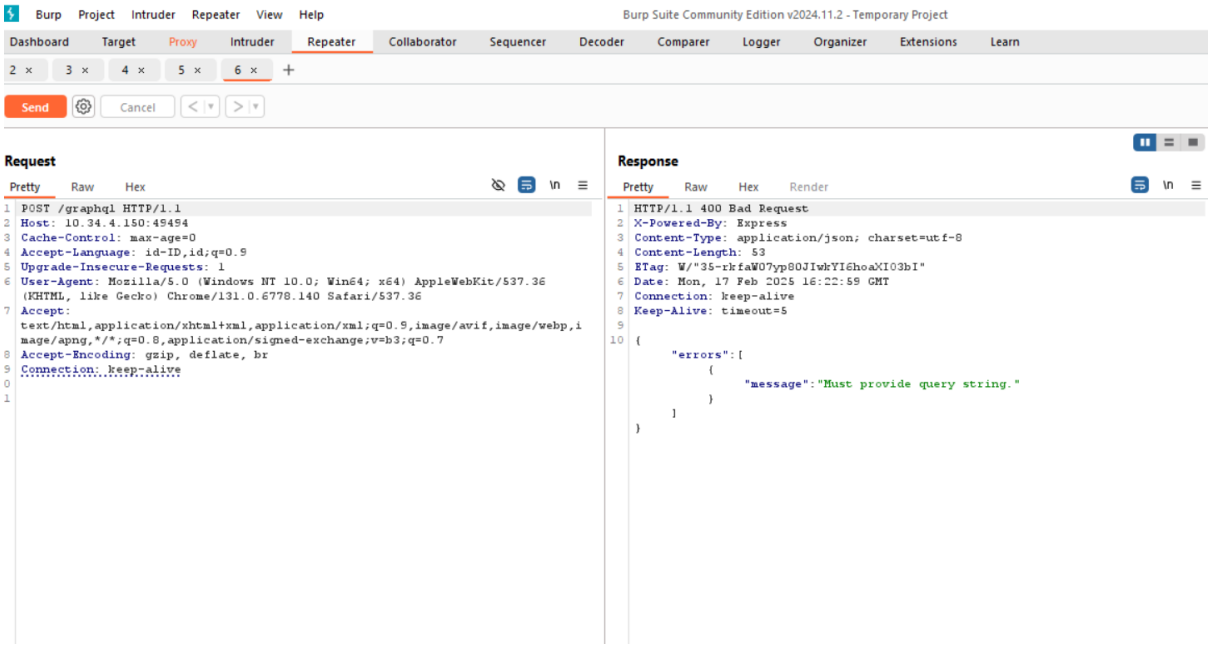
Ternyata saya di direct langsung ke halaman login, untuk/register, hanya mendapatkan ini



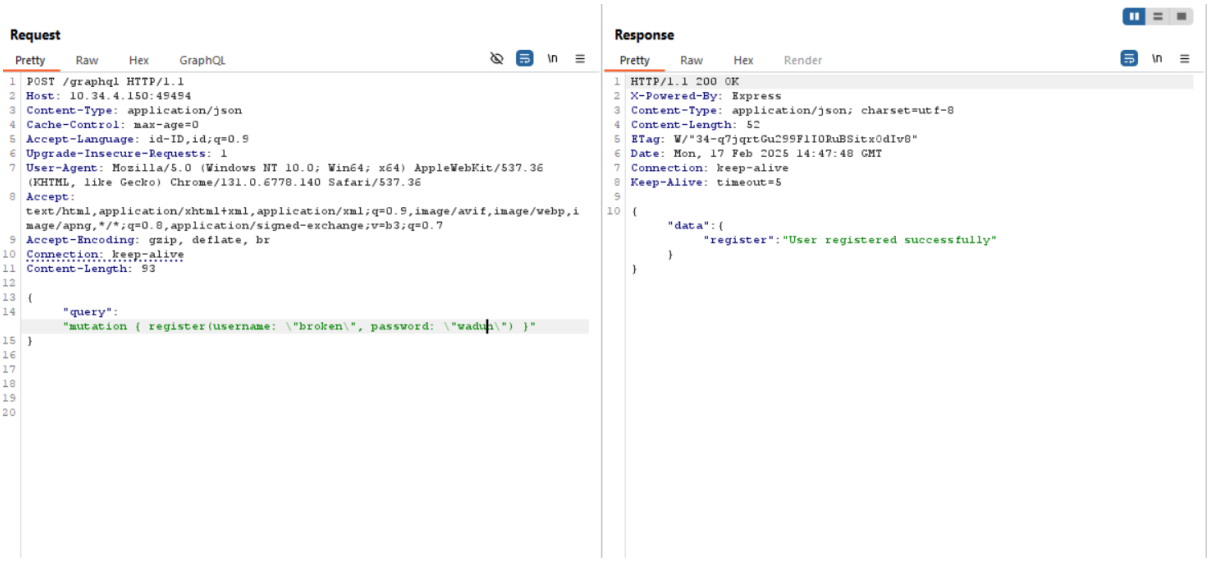
Dan saya mencoba /graphql



Menarik, saya akan buka website ini dengan menggunkan burpsuite

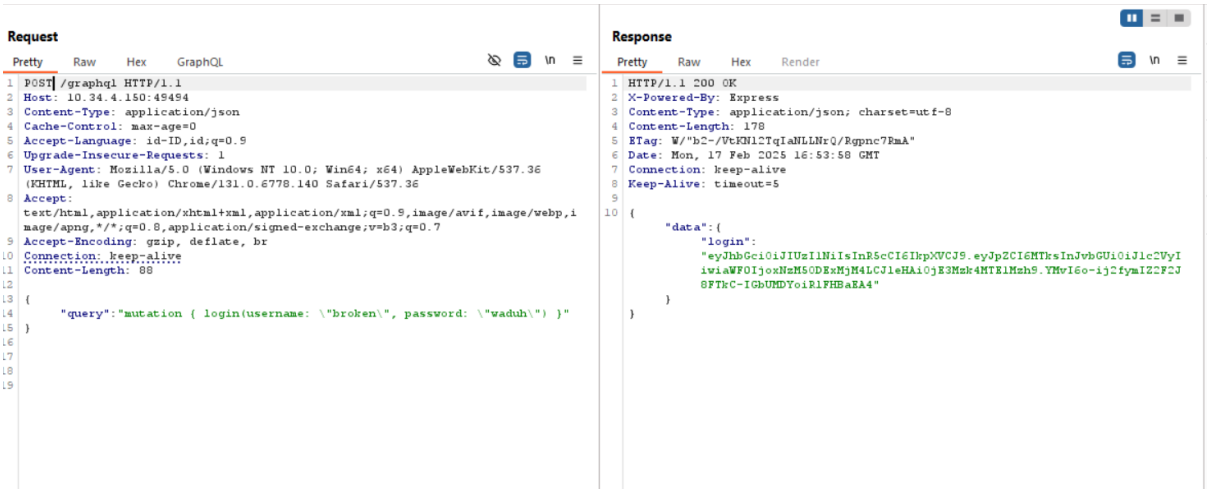


Dan website memberikan output Must provide query string. Sepertinya dalam chall ini kita harus menginput query di burpsuite untuk melangkah ke depan. Jadi saya research lebih lanjut mengenai query ini dan saya akan mulai dengan register



Dan disini register saya berhasil dengan user dan password yang telah saya berikan, tetapi ketika saya login, website tidak memberikan saya apapun melainkan

Jadi saya mencoba cara lain dengan query login



Dan saya mendapatkan JWT token untuk user, dan m

freepass25{graphql_jwt_basic_exploitation_right_goodluck_bro_fre

epassnya}

mas gasempet tulis wu saya jelaskan di presentasi saja ya