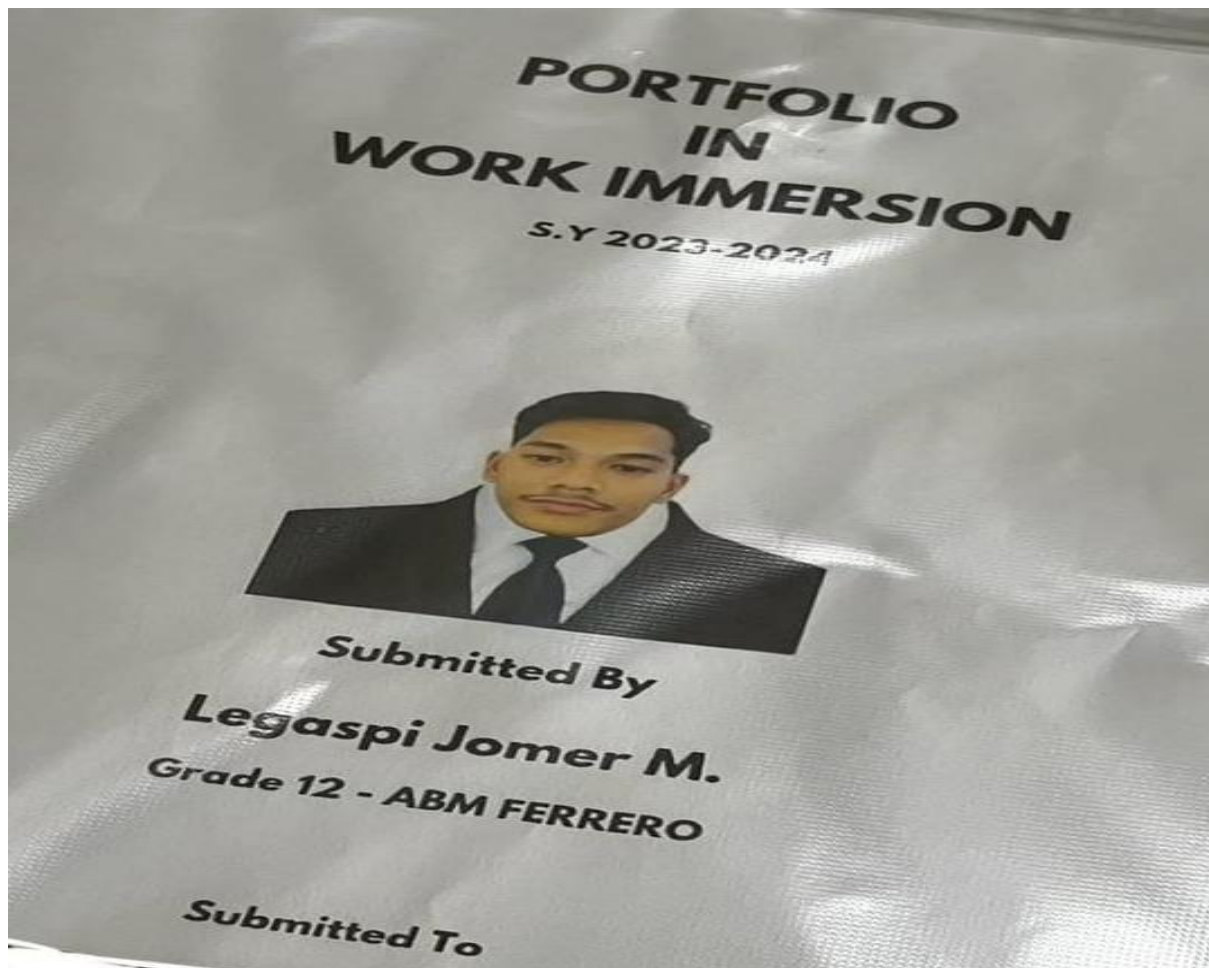


Write-Up Freepass POROS 2025



Author : broken

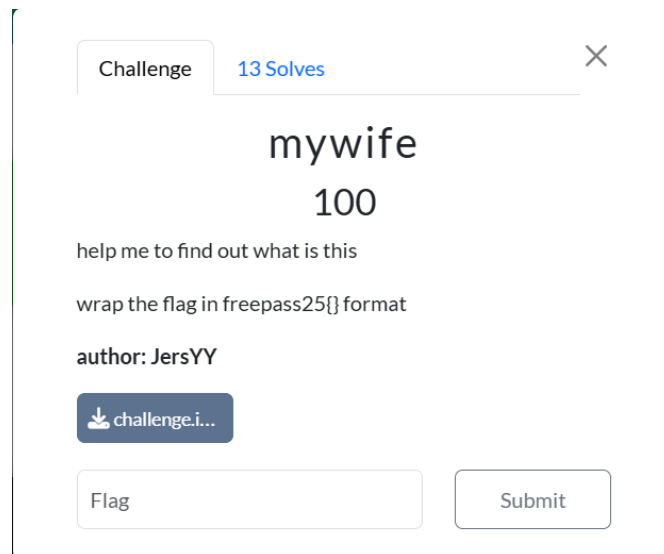
Mohammad Iqbal Bagas Permana

245140701111024

Teknologi Informasi

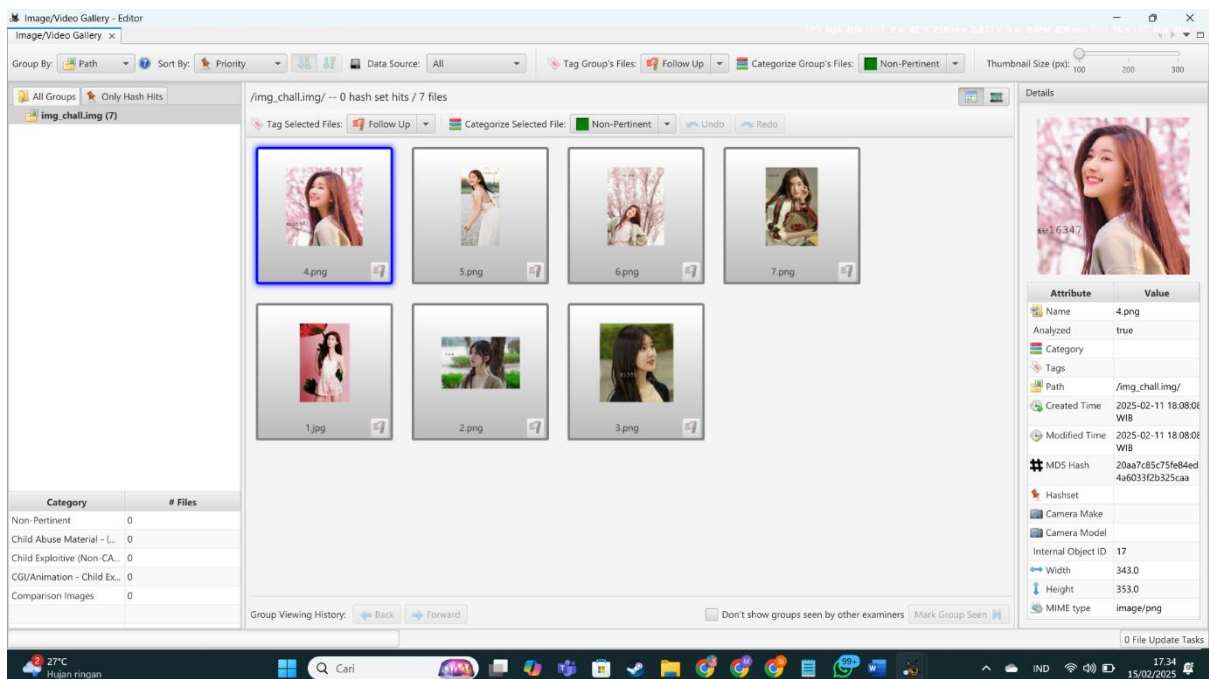
Forensics

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

Challenge 6 Solves X

tiny
400

My friend just gave me a secret image that only certain people can see. Can you see it?

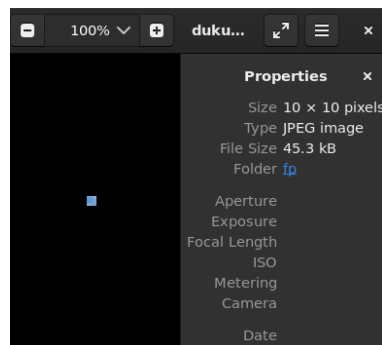
wrap the flag in freepass25{} format , example: flag{a-z} > freepass25{a-z}

author : JersYY

↓ chall.jpg

Flag Submit

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

The screenshot shows the HxD hex editor interface. The file 'dukun.jpg' is open. The hex view shows the following data at offset 0000D90:

```

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Teks yang dinon-sandikan
0000D90 00 0A 00 0A 03 01 11 00 02 11 01 03 11 01 FF C4 .....yA
0000D91 00 1D 00 00 02 03 01 01 01 01 00 00 00 00 00 .....yA
0000D92 00 00 00 05 06 04 07 08 03 02 09 01 00 FF C4 .....yA
0000D93 34 10 00 02 02 02 01 04 01 04 01 04 01 04 02 4.....!...m1
0000D94 03 00 01 02 03 04 05 11 06 12 21 00 07 13 22 31 ..2A#..BQa..$3.q
0000D95 08 14 32 41 23 09 15 42 51 61 16 17 24 33 18 71 CR.yA.....
0000D96 43 52 81 FF C4 00 1E 01 00 01 04 03 01 01 01 00 ..yA.?.....
0000D97 00 00 00 00 00 00 00 00 00 05 03 04 06 07 02 08 09 ..yA.?.....
0000D98 01 00 0A FF C4 00 3F 11 00 02 01 03 03 03 03 03 ..yA.?.....
0000D99 02 04 05 03 02 05 05 00 01 02 03 04 05 11 06 12 ..yA.?.....
0000D9A 21 00 07 31 08 13 22 09 32 41 14 51 15 23 42 61 !..1..".2A.Q.#Ba
  
```

The value 0A000A is highlighted in blue at offset 0000D90. The text 'Teks yang dinon-sandikan' is visible in the right pane.

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-Header] 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 0.00708
[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
[File] Coded Character Set       : UTF8
[File] Envelope Record Version   : 4
[File] Date Created              : 2021:03:11
[File] Digital Creation Date     : 2021:03:11
[File] Digital Creation Time     : 21:26:05-04:00
[File] Application Record Version : 4
[File] Time Created              : 21:26:05-04:00
[File] Keywords                  : Who!People!in Pic!Alex Mustelier
[File] IPTC Digest               : 49e81a2fa795a7a56ac703c85b560ab3
[File] Image Width               : 2912
[File] Image Height              : 4368

```



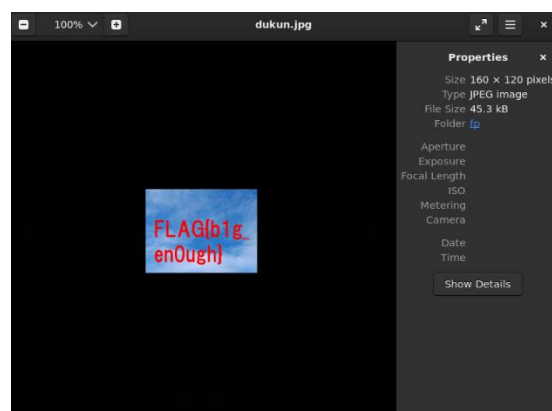
Saya mencoba lagi untuk menemukan sumber lainnya dan menemukan :

```

[ICC_Profile, ICC_Profile, Image] cppt - 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 0.00708
[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

Challenge

12 Solves

×

EliteCodeCipher

100

pemanasan kasih soal elit tipis tipis lah ya...

wrap the flag in freepass25{} format author : JersYY

 chall.py

Flag

Submit

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 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

$$y^2 = x^3 + Ax + B \mod M$$

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 python untuk menemukan n .

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

```

from sage.all import *
from Crypto.Util.number import *

M = 17459102747413984477
A = 2
B = 3

E = EllipticCurve(GF(M), [A, B])

G = E(15579091807671783999, 4313814846862507155)
P = E(11773164984492924924, 14526984146008997354)

n = discrete_log(P, G)

flag = long_to_bytes(n)
print(flag)

```

```

-----
TypeError                                 Traceback (most recent call last)
Cell In[1], line 13
    10 G = E(Integer(15579091807671783999), Integer(4313814846862507155))
    11 P = E(Integer(11773164984492924924), Integer(14526984146008997354))
--> 13 n = discrete_log(P, G)
    15 flag = long_to_bytes(n)
    16 print(flag)
File /ext/sage/10.4/src/sage/groups/generic.py:924, in discrete_log(a, base, ord, bounds,

```

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

```

from sage.all import *
from Crypto.Util.number import *

M = 17459102747413984477
A = 2
B = 3

E = EllipticCurve(GF(M), [A, B])

G = E(15579091807671783999, 4313814846862507155)
P = E(11773164984492924924, 14526984146008997354)

n = discrete_log(P, G, operation="+")

flag = long_to_bytes(n)
print(flag)

```

```

b'ecc_ygy!'

```

Dan voilà, Flagnya adalah `freepass25{ecc_ygy!}`

Web Exploitation

1. Guess What?

Challenge 25 Solves X

Guess What?

100

Yuk main tebak-tebakan sama acuu 🤖, Kalo bener acuu kasih hadiah deh, hehehe...

Author: anakmamah

<http://10.34.4.150:9000>

Flag Submit

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

```
Elements Console Sources Network Performance Memory >> 1 ⚙️
<html>
  <head></head>
  <body> == $0
    <h1>Guessing Challenge</h1>
    <p>Guess what the answer is, if you can get it right, i'll give you a prize</p>
    <form method="POST">...</form>
    <!-- ?source -->
  </body>
</html>
```

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 :

Md5 hash calculated hash digest	Md5 value Reversed hash value
25203fcbba1a52a482fe46e34507dd69	POROSJUARA
Copy Hash	Copy Value
	Blame this record

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

← → ↻ ⚠ Not secure 10.34.4.150:9000

Congratulations! here's your Prize: **freepass25{online_tools_can_sometimes_be_very_helpful_semangat_brok_123456789}**

dan voilà Flagnya adalah

freepass25{online_tools_can_sometimes_be_very_helpful_semangat_brok_123456789}

2. Binary Whisper

Challenge 10 Solves X

Binary Whisper

176

Di balik tirai web, tersembunyi sebuah naskah kuno. Jalannya berliku, terpecah oleh titik dan garis. Buka gerbang rahasia, tembus batas yang tak terlihat, Tapi jangan tertipu—apa yang kau temukan hanyalah bayangan yang terdistorsi.

"MDEwMTAwMTAgMDEwMDAwMTEgMDEwMDAxMDE=" Ia berteriak dalam bahasa mesin, namun maknanya terasa ganjil. Apakah ini akhir, atau pertanda untuk menyelam lebih dalam? Temukan kebenaran di balik topeng, sebelum waktumu habis!

"Kesuksesan bukan hanya milik mereka yang cepat, tetapi juga mereka yang teliti dan tak pernah menyerah." - ChatGPT

flag file's name: **flag{random 20 length number}.txt**

Note: format flag tetap "freepass25[a-Z]" yaa, bukan nama file!

Author: **anakmamah**

<http://10.34.4.150:55100>

Flag Submit

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

From Base64

Alphabet
A-Za-z0-9+/=

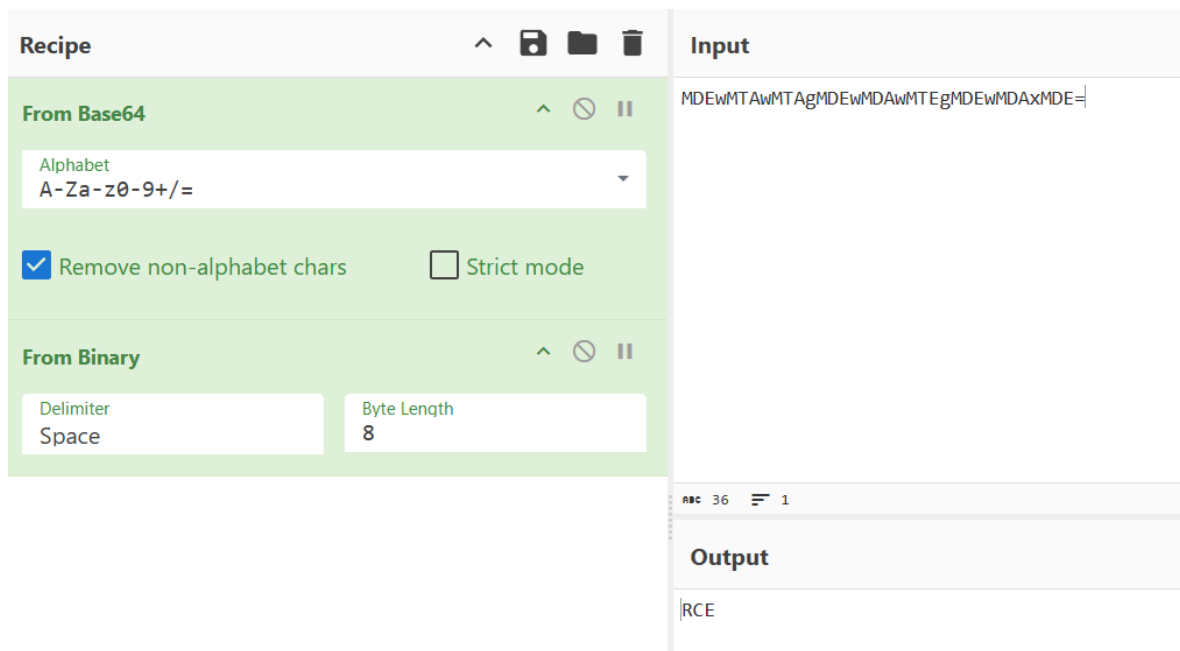
☒ Remove non-alphabet chars ☐ Strict mode

MDEwMTAwMTAgMDEwMDAwMTEgMDEwMDAxMDE=

Output

01010010 01000011 01000101

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(" ");
  };
}
```

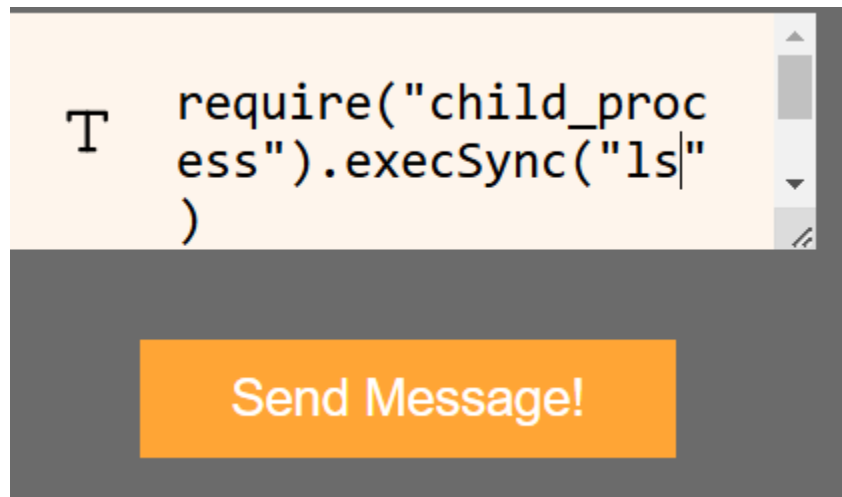
Disini terdapat forbiddenwords dan yang membuat saya curiga adalah forbidden words hanya berlaku pada input di bagian message, kecurigaan saya diperkuat dengan adanya eval(message) yang dimana hal ini digunakan untuk mengeksekusi string sebagai kode JavaScript sehingga ketika kita memasukkan input kode 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

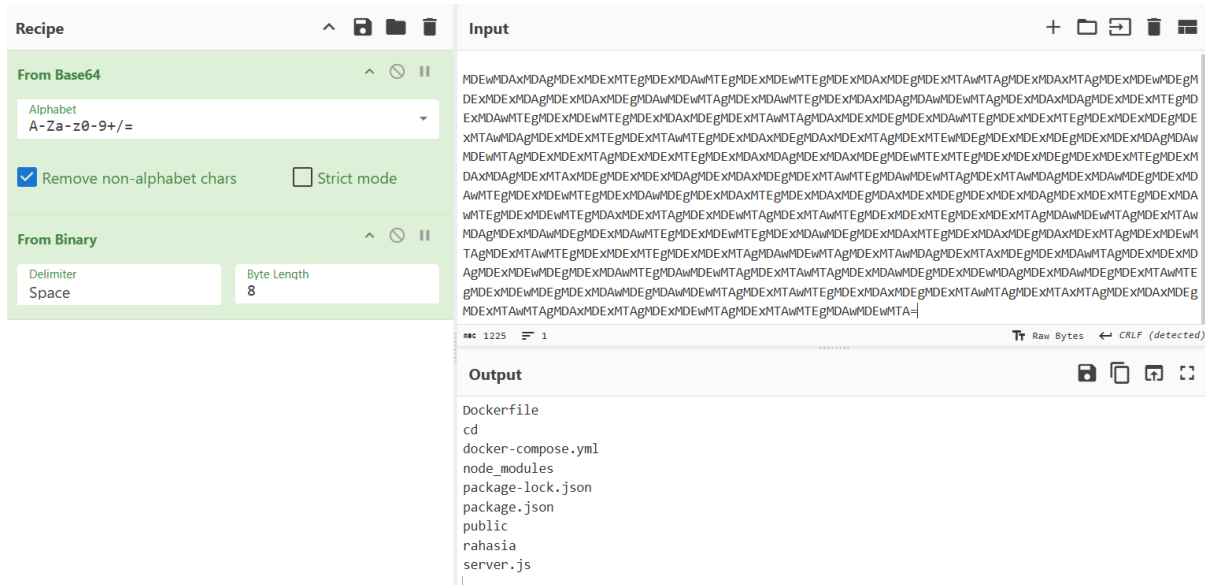
Output:

MDAxMTAwMTAgMDAxMTAxMDE=

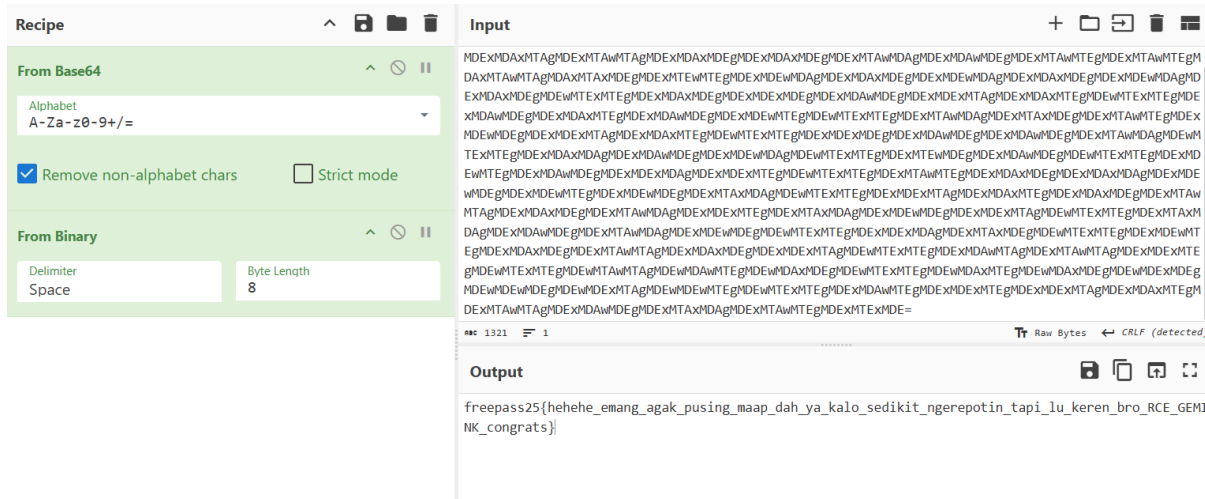
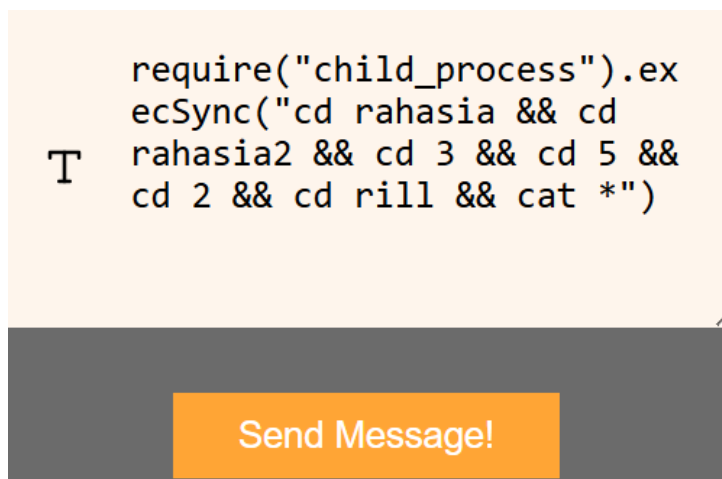
Dan ketika saya decode menjadi angka 25, Sepertinya ini merupakan kerentanan (Server Side Template Injection) SSTI dan saya mencoba untuk mencari input command lain dan menemukan `require("child_process").execSync()` yang dapat mengeksekusi ke dalam direktori server. Langsung saja kita coba :



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_ngerepo  
tin_tapi_lu_keren_bro_RCE_GEMINK_congrats}
```

3. Atmin Raja Iblis

Challenge

6 Solves

×

Atmin Raja Iblis

400

Atmin adalah raja iblis yang sesungguhnya... Kamu harus membantu saya mengambil flagnya dari sang raja iblis 🤩. Tetapi saya harus menemukan kunci yang tepat terlebih dahulu untuk dapat membuka ruangan rahasia.

Author: anakmamah

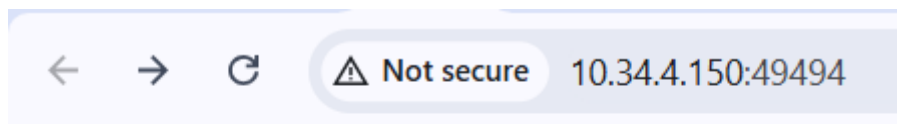
<http://10.34.4.150:49494>

⬇ server.js

Flag

Submit

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



There's nothing here, umm...

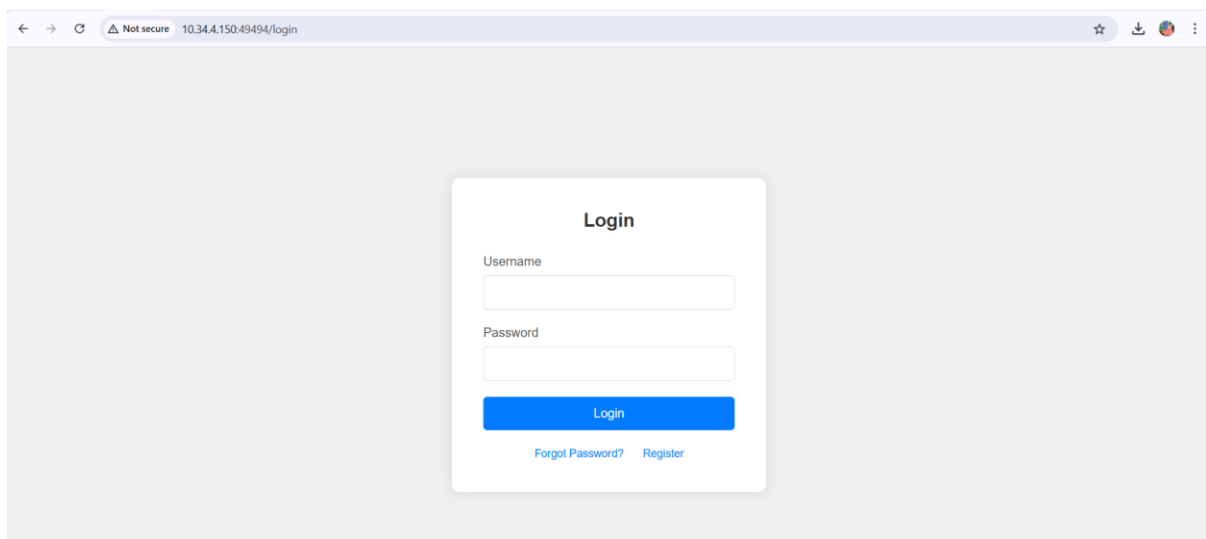
Maybe u could find another way

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

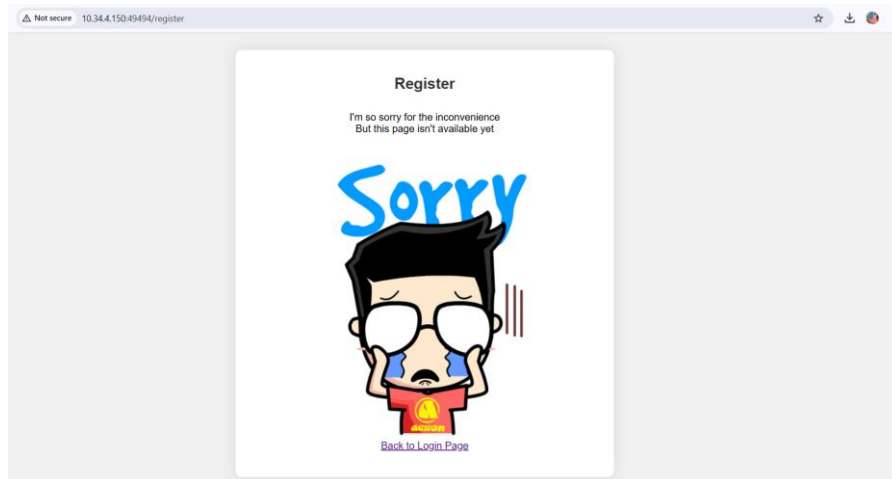
Sepertinya source code merupakan kunci bagaimana kita akan solve challenge ini.

```
169
170 router.get("/flag", authenticate, async (req, res) => {
171   const token = req.cookies.authToken;
172
173   try {
174     const response = await axios.post("http://localhost:49494/graphql", {
175       query: `
176         query {
177           getProfile(token: "${token}") {
178             id
179             username
180             role
181           }
182         }
183       `,
184     });
185
186     const user = response.data.data.getProfile;
187     const decoded = jwt.verify(token, JWT_SECRET);
188
189     if (decoded.role !== "administrator") {
190       return res.send(
191         <h1>Welcome, ${user.username}</h1>
192         <p>Role: ${user.role}</p>
193       );
194     }
195
196     res.sendFile(path.join(__dirname, "profile.html"));
197   } catch (error) {
198     console.error(error);
199     res.status(500).send("An error occurred while fetching the profile");
200   }
201 });
202
203 router.get("/register", (req, res) => {
204   res.sendFile(path.join(__dirname, "public", "register.html"));
205 });
206
207 app.use(
208   "/graphql",
209   (req, res, next) => {
210     if (req.method !== "POST") {
211       return res.status(405).send("Only POST requests are allowed");
212     }
213     next();
214   }
215 );
```

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

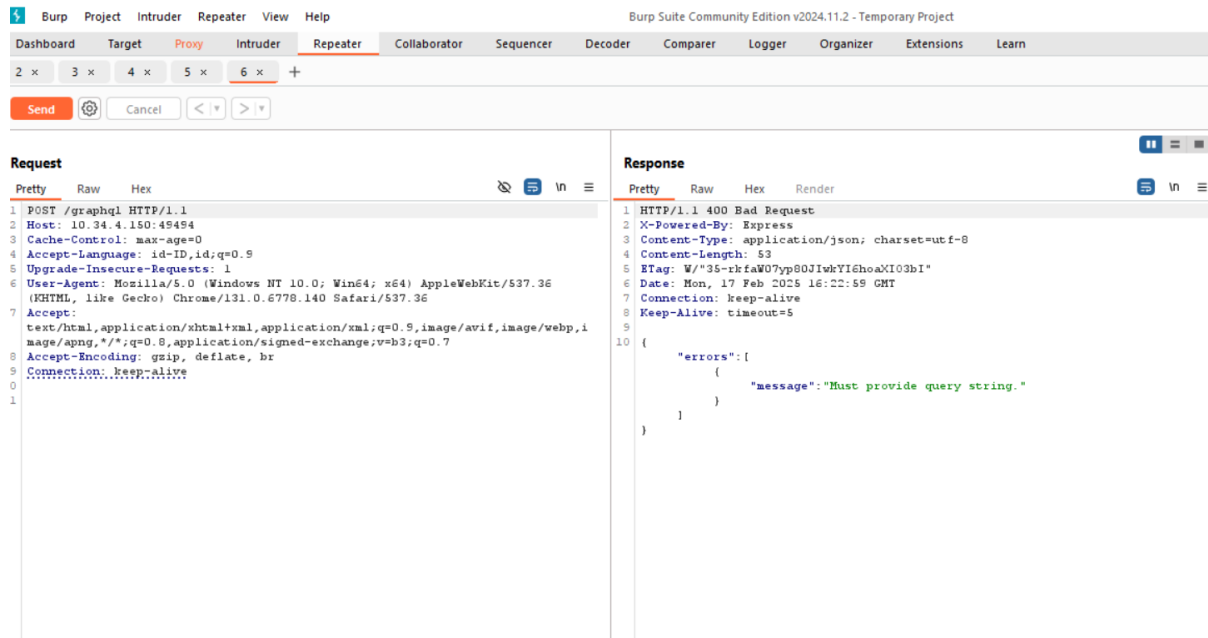


Dan saya mencoba /graphql



Only POST requests are allowed

Menarik, saya akan buka website ini dengan menggunakan 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

Request		Response	
Pretty	Raw	Pretty	Raw
<pre> 1 POST /graphql HTTP/1.1 2 Host: 10.34.4.150:49494 3 Content-Type: application/json 4 Cache-Control: max-age=0 5 Accept-Language: id-ID,id;q=0.9 6 Upgrade-Insecure-Requests: 1 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.140 Safari/537.36 8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i mage/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 9 Accept-Encoding: gzip, deflate, br 10 Connection: keep-alive 11 Content-Length: 93 12 13 { 14 "query": 15 "mutation (register(username: \"broken\", password: \"waduuh\"))" 16 } 17 18 19 20 </pre>		<pre> 1 HTTP/1.1 200 OK 2 X-Powered-By: Express 3 Content-Type: application/json; charset=utf-8 4 Content-Length: 52 5 ETag: W/"34-q7jqtGu299F1I0RuBSitx0dIv8" 6 Date: Mon, 17 Feb 2025 14:47:48 GMT 7 Connection: keep-alive 8 Keep-Alive: timeout=5 9 10 { 11 "data": { 12 "register": "User registered successfully" 13 } 14 } </pre>	

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



Welcome, broken

Role: user

Jadi saya mencoba cara lain dengan query login

Request		Response	
Pretty	Raw	Pretty	Raw
<pre> 1 POST /graphql HTTP/1.1 2 Host: 10.34.4.150:49494 3 Content-Type: application/json 4 Cache-Control: max-age=0 5 Accept-Language: id-ID,id;q=0.9 6 Upgrade-Insecure-Requests: 1 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.140 Safari/537.36 8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i mage/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 9 Accept-Encoding: gzip, deflate, br 10 Connection: keep-alive 11 Content-Length: 88 12 13 { 14 "query": "mutation (login(username: \"broken\", password: \"waduuh\"))" 15 } 16 17 18 19 </pre>		<pre> 1 HTTP/1.1 200 OK 2 X-Powered-By: Express 3 Content-Type: application/json; charset=utf-8 4 Content-Length: 178 5 ETag: W/"b2-/VtKML1C7qIaNLNtQ/Rgpnc7FmA" 6 Date: Mon, 17 Feb 2025 16:53:58 GMT 7 Connection: keep-alive 8 Keep-Alive: timeout=5 9 10 { 11 "data": { 12 "login": 13 "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZiZCIGMtZmInJmVhGU0iOiJlc2VyIiwiaWF0IjoxNzE5ODU0MjM1M4LCJleHAiOiJlM3MhK4MTk1Mzh9.YWw16o-ij2fywI2ZF2J8FTkC-IGbUMDYoiR1PHBaEA4" 14 } 15 } </pre>	

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