

# **Cyber Security Community**



**Nama Lengkap : Satya Kusuma**

**NIM : 2540124740**

**Discord Username : Q.#0863**

## Web Exploitation: GET aHEAD

GET aHEAD 

 | 20 points 

Tags: picoCTF 2021 Web Exploitation

AUTHOR: MADSTACKS

Hints 

### Description

Find the flag being held on this server to get ahead of the competition <http://mercury.picoctf.net:15931/>

1 2

47,962 solves / 51,835 users attempted (93%)



82% Liked



 picoCTF{FLAG}

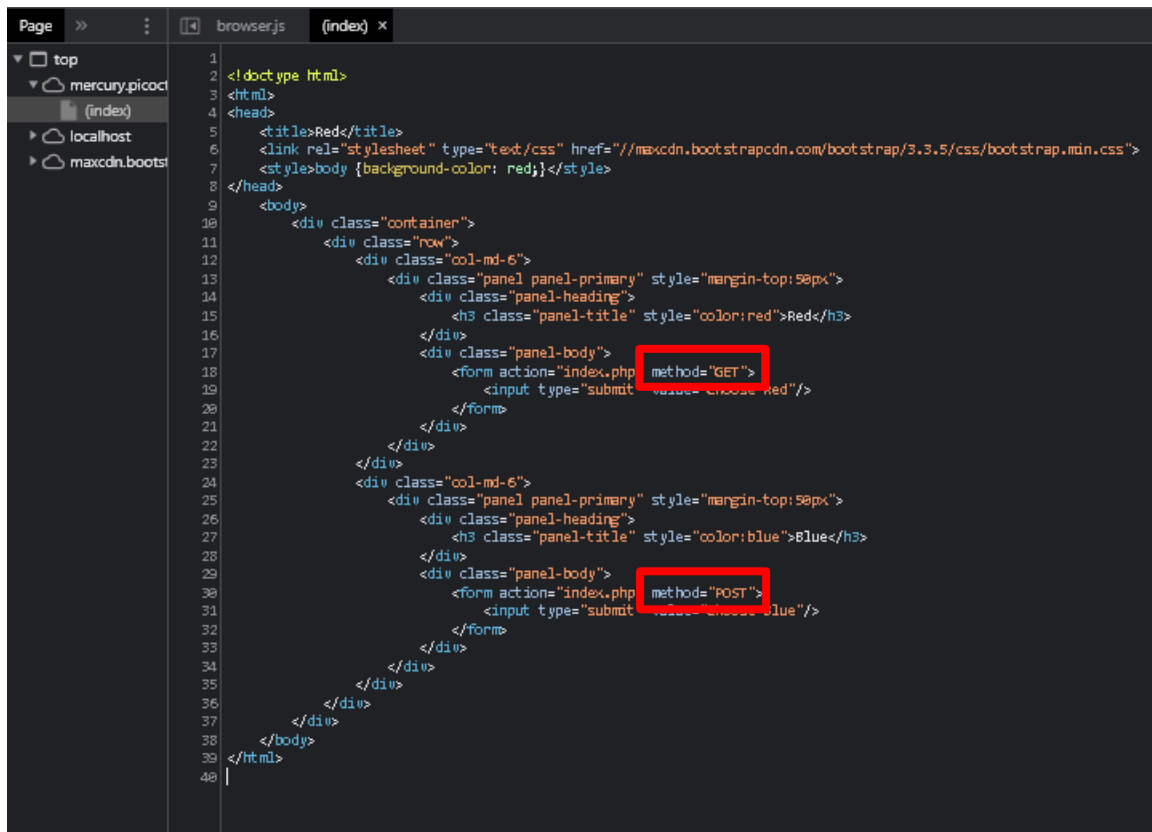
Submit Flag

### Hints:

- Maybe you have more than 2 choices
- Check out tools like Burpsuite to modify your requests and look at the responses

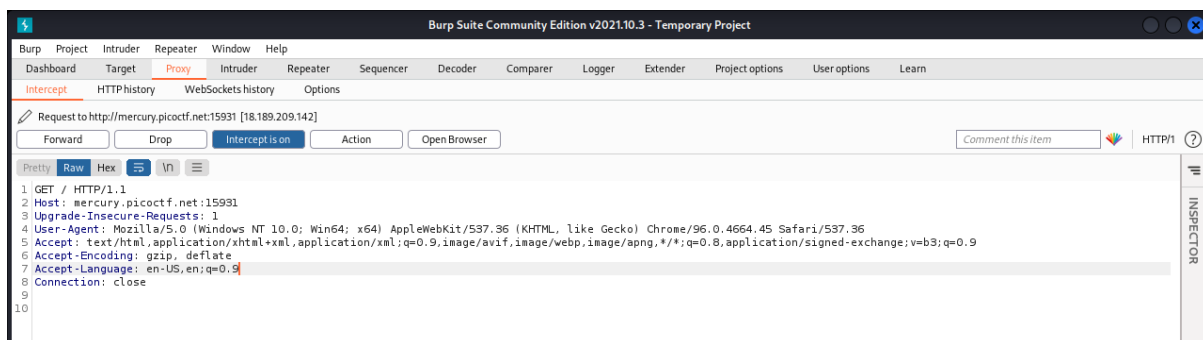
1. Pertama tentunya kita harus membuka websitenya terlebih dahulu. Websitenya akan terbuka seperti gambar dibawah. Disini saya langsung melakukan inspect dan menemukan bahwa di dalam kodenya terdapat GET dan POST method.



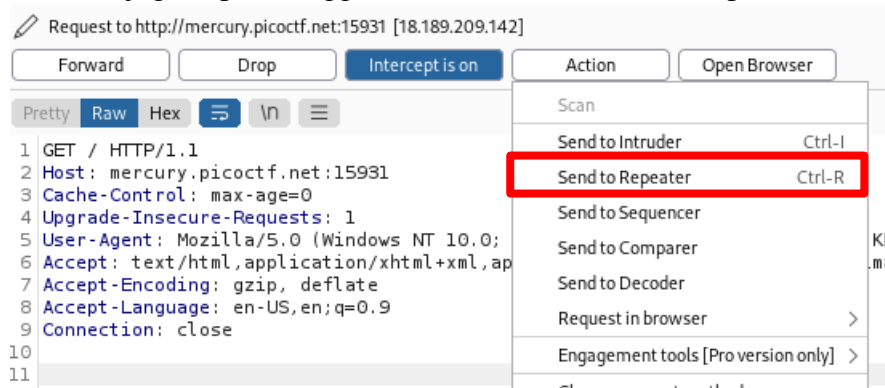


```
1 <!doctype html>
2 <html>
3 <head>
4 <title>Red</title>
5 <link rel="stylesheet" type="text/css" href="//maxcdn.bootstrapcdn.com/bootstrap/3.3.5/css/bootstrap.min.css">
6 <style>body {background-color: red;}</style>
7 </head>
8 <body>
9 <div class="container">
10 <div class="row">
11 <div class="col-md-6">
12 <div class="panel panel-primary" style="margin-top:50px">
13 <div class="panel-heading">
14 <h3 class="panel-title" style="color:red">Red</h3>
15 </div>
16 <div class="panel-body">
17 <form action="index.php" method="GET">
18 <input type="submit" value="Choose Red"/>
19 </form>
20 </div>
21 </div>
22 </div>
23 <div class="col-md-6">
24 <div class="panel panel-primary" style="margin-top:50px">
25 <div class="panel-heading">
26 <h3 class="panel-title" style="color:blue">Blue</h3>
27 </div>
28 <div class="panel-body">
29 <form action="index.php" method="POST">
30 <input type="submit" value="Choose Blue"/>
31 </form>
32 </div>
33 </div>
34 </div>
35 </div>
36 </div>
37 </div>
38 </body>
39 </html>
40
```

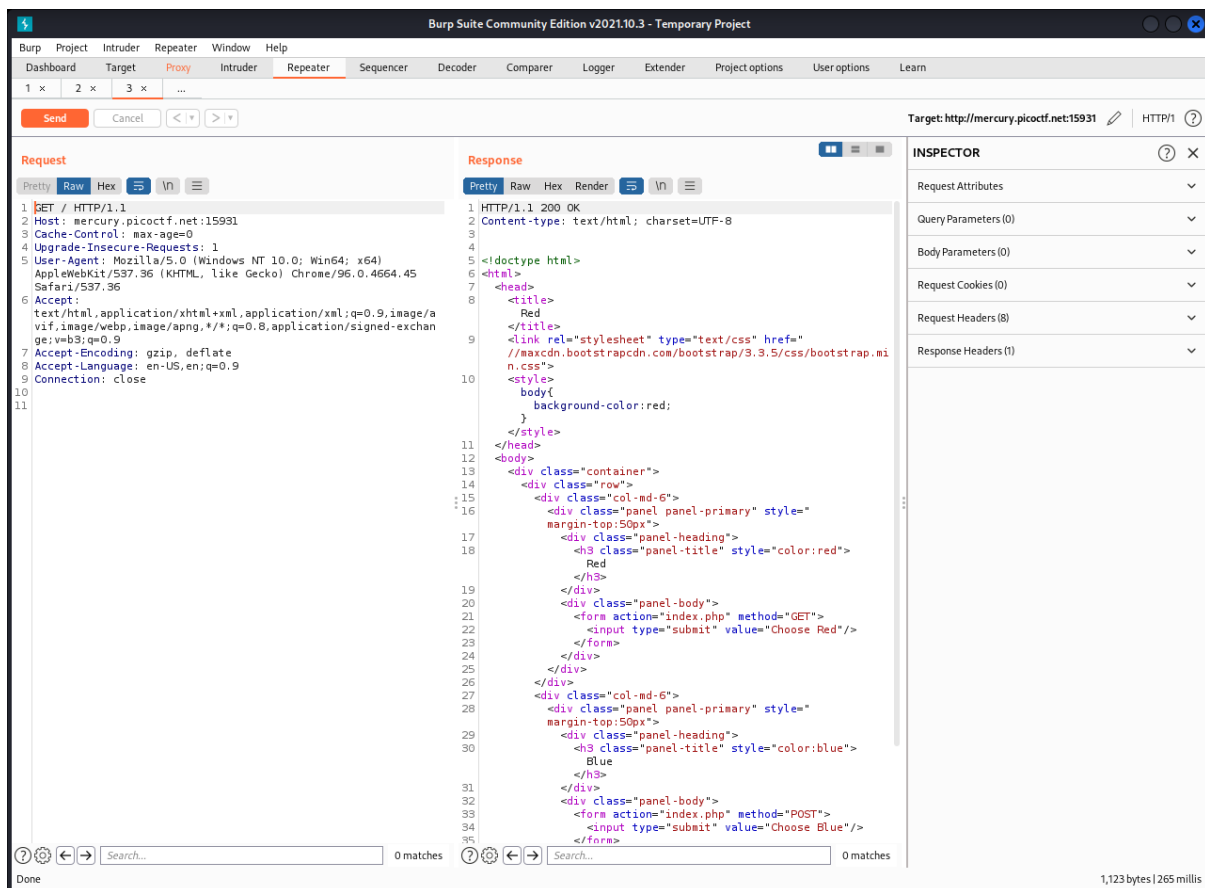
2. Seperti yang ada di hint, saya mencoba untuk menggunakan Burpsuite pada websitenya. (Pastikan Burpsuite -> Proxy -> Intercept is on) Setelah menyalakan burpsuite, refresh website sampai muncul sesuatu pada Burpsuite seperti gambar dibawah.



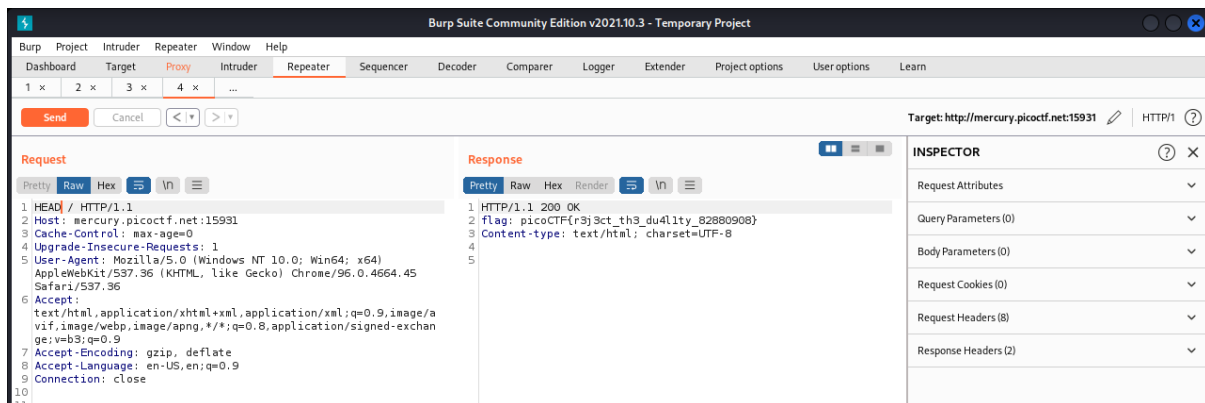
3. Kemudian kita dapat menggunakan shortcut Ctrl + R untuk mengirimnya ke repeater atau kita juga dapat menggunakan Action -> Send to Repeater.



4. Kalau sudah, pindah ke Repeater dan send untuk melihat response.



5. Kemudian, kita dapat mengganti GET yang berada pada kolom kiri menjadi HEAD. Lalu tekan send dan dapat dilihat pada responsnya ditemukanlah flagnya.



FLAG: picoCTF{r3j3ct\_th3\_du4l1ty\_775f2530}


\*GET POST HEAD adalah method HTTP buat ngirim request dari client ke server

- GET: meminta data dari server.
- POST: mengirim data ke server.
- HEAD: mirip sama GET cuman bedanya dia minta header response doang tanpa harus minta body responsnya juga. Biasanya dipake buat ngambil status code atau ukuran filenya sebelum ngedownload file yang lebih gede lagi.

Kenapa pake burpsuite? Soalnya burpsuite bisa intercept request dan bisa ngubah HTTP request (kalo di soal GET jadi HEAD) makanya kita pake burpsuite.

## Cryptography: Mod 26

Mod 26 

 | 10 points 

Tags: picoCTF 2021 Cryptography

AUTHOR: PANDU

Hints 



### Description

1

Cryptography can be easy, do you know what ROT13 is?

`cvpbPGS{arkg_gvzr_V'yy_gel_2_ebhaqf_bs_ebg13_nSkgmDJE}`

136,390 solves / 140,077 users attempted (97%)

 91% Liked 

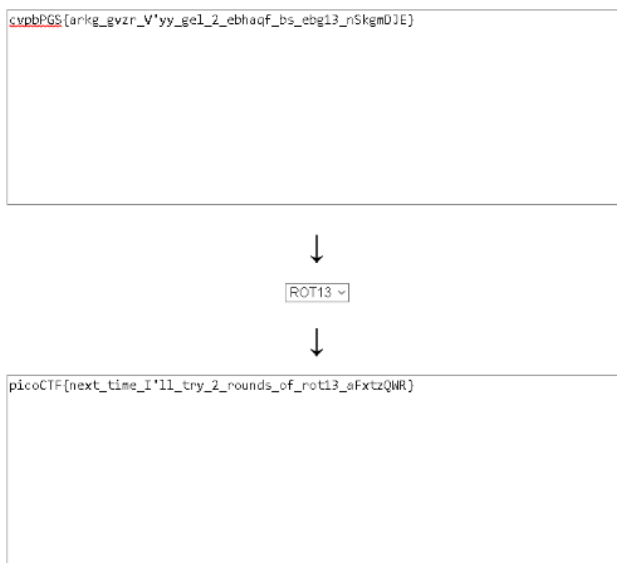
 picoCTF{FLAG}

Submit Flag

1. Seperti yang ada di soal, kita ditanyakan tentang ROT13 dan diberikan string random. Jadi saya langsung mencarinya di internet dan menemukan bahwa ROT13 merupakan sebuah cipher yang mengganti setiap huruf menjadi huruf ke 13 setelah huruf itu sendiri (contoh a -> n, b -> o, c -> p, dan seterusnya). Dan saya juga menemukan bahwa ROT13 ini memiliki online tool, jadi saya menggunakannya dan didapatkan flagnya seperti gambar dibawah.

**rot13.com**

[About ROT13](#)



FLAG: `picoCTF{next_time_I'll_try_2_rounds_of_rot13_aFxtzQWR}`

## Forensic: information

information



👤 | 10 points ✕

Tags: picoCTF 2021 Forensics

AUTHOR: SUSIE

Hints ?

### Description

1 2

Files can always be changed in a secret way. Can you find the flag?

[cat.jpg](#)

64,617 solves / 81,497 users attempted (79%)



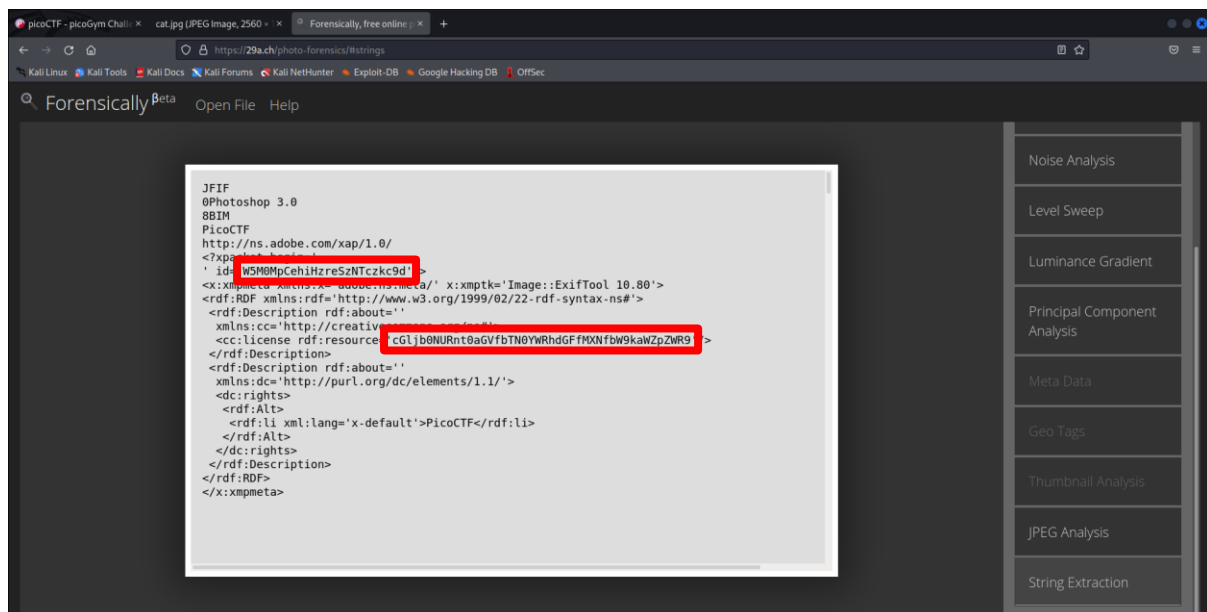
41% Liked



🚩 picoCTF{FLAG}

Submit Flag

1. Pertama kita download dulu fotonya.
2. Selanjutnya saya menggunakan online tools dan mengupload fotonya kemudian melakukan string extraction disana.



3. Pada strings diatas, terdapat 2 strings yang menarik perhatian saya, jadi saya mencoba melakukan decryption Base64 di online tools. Pada strings pertama tidak menghasilkan apapun ketika di decrypt, namun pada strings ke 2 didapatkan flagnya.

The image displays two screenshots of the CyberChef web application, a tool used for performing various cryptographic operations. Both screenshots show the 'From Base64' recipe selected in the 'Recipe' panel, with the 'Remove non-alphabet chars' option checked.

**Top Screenshot:**

- Input:** W5M0MpCehiHzreSzNTczkc9d
- Output:** [.42...16.a\*573.1]

**Bottom Screenshot:**



- Input:** cG1jb0NURlnt0aGVfbTNOYWRhdGF1b3R5bW9kaWZpZm90
- Output:** picoCTF{the\_m3tadata\_1s\_modified}

FLAG: picoCTF{the\_m3tadata\_1s\_modified}



# Binary Exploitation: Stonks

Stonks 

 | 20 points 

Tags: picoCTF 2021 Binary Exploitation

AUTHOR: MADSTACKS



Hints 

## Description

1

I decided to try something noone else has before. I made a bot to automatically trade stonks for me using AI and machine learning. I wouldn't believe you if you told me it's unsecure! [vuln.cnc](https://vuln.cnc)  
[mercury.picoctf.net 33411](https://mercury.picoctf.net/33411)

17,656 solves / 22,988 users attempted (77%)

 58% Liked 

 picoCTF{FLAG}

Submit Flag

1. Pertama download dulu source code vuln.c dan analisis codenya.
2. Setelah dilakukan analisis, terdapat code yang menarik perhatian saya dibagian function buy\_stonks. Code tersebut tidak memiliki format string pada umumnya melainkan langsung menuliskan "user\_buf".

```
int buy_stonks(Portfolio *p) {
    if (!p) {
        return 1;
    }
    char api_buf[FLAG_BUFFER];
    FILE *f = fopen("api", "r");
    if (!f) {
        printf("Flag file not found. Contact an admin.\n");
        exit(1);
    }
    fgets(api_buf, FLAG_BUFFER, f);

    int money = p->money;
    int shares = 0;
    Stok *temp = NULL;
    printf("Using patented AI algorithms to buy stonks\n");
    while (money > 0) {
        shares = (rand() % money) + 1;
        temp = pick_symbol_with_AI(shares);
        temp->next = p->head;
        p->head = temp;
        money -= shares;
    }
    printf("Stonks chosen\n");

    // TODO: Figure out how to read token from file, for now just ask
    char *user_buf = malloc(300 + 1);
    printf("What is your API token?\n");
    scanf("%300s", user_buf);
    printf("Buying stonks with token:\n");
    printf(user_buf);

    // TODO: Actually use key to interact with API

    view_portfolio(p);

    return 0;
}
```

3. Pada bagian sebelumnya terdapat input yang dapat memasukkan 300 strings. Jadi saya mencoba untuk memasukkan “%s” sebanyak 300 kali.

```
Using patented AI algorithms to buy stonks
Stonks chosen
What is your API token?
%%%%%%%%%%
%%%%%%%%%%
%%%%%%%%%%
Buying stonks with token:
timeout: the monitored command dumped core
```

4. Karena tidak memunculkan apapun, jadi saya mencoba menggunakan “%x” untuk menampilkan nilai hexnya.

[illegible]

5. Ternyata didapatkan nilai hexnya, lalu saya mengubahnya ke string.

69 H?  
~? ? ? ? ? 4 ? ? ? ? ? ~ ? ? p ? 5 ? ? ? 67 sc ? o cip {  
FTC0I\_I4\_t5m\_II0m\_y\_y3nc42a6a4I ? ? ? }  
?? : ? ? ? d @ & ? ? ? ? ? \ / ? ? ? p ? ? ? ? ? ? ?  
? ? ? D ? ? ? f ? ? ? ? ? H ? ? ? N @ ? ?  
? K ? ? ~ ? ? ? ~ ? ? ? ? ? Q ? ? ? ? ~ ? ? ? j ?  
? ~ ? ? ? ? ? ? ? E ? ? H ? hsA ` ? ? E ? ? ? E ? ? H ? ? ~  
? ? ? ? ? E ? ? ? ? E ? ? ? 4 0 j ?  
? ? ? S ? ? ]; ? ? ~ ? ? ? ~ ? ? ? ? ? x ? ? ? ? \ O ? ? \ ?  
? ? ? I A ?

6. Terlihat bahwa penulisannya terbalik, jadi saya membalikkan stringnya menjadi 14a6a24cn3y\_y\_m0ll\_m5t\_4I\_10CTF{pico dan dapat dilihat bahwa setelah dibalik pun masih belum tepat susunannya. Disini saya sadar bahwa ada pola yang mana setiap 4 karakter harus dipindahkan ke depan hingga menghasilkan flagnya.

FLAG: picoCTF{I\_l05t\_4ll\_my\_m0n3y\_a24c14a6}

# Reverse Engineering: Transformation

Transformation 

 | 20 points 

Tags: picoCTF 2021 Reverse Engineering

AUTHOR: MADSTACKS

Hints 

## Description

1

I wonder what this really is... 

```
enc ''.join([chr((ord(flag[i]) << 8) + ord(flag[i + 1])) for i in range(0, len(flag), 2)])
```

31,184 solves / 38,637 users attempted (81%)



54% Liked






picoCTF{FLAG}



Submit Flag


1. Pertama download dulu file “enc”, lalu buka filenya dan akan muncul tulisan seperti dibawah.

1 瀝捌宏規は形梶獠楮猿[]搜潦弼彦レ一て魑

2. Kemudian saya mencoba memasukkannya ke cyberchef dan melakukan bruteforce dengan menggunakan resep magic dan menyalakan intensive modenya.

**Recipe**   

**Magic**  

Depth  
3 

☒ Intensive mode ☐ Extensive language support

Crib (known plaintext string or regex)

3. Setelah dilakukan, saya mengecek satu per satu hasilnya dan ditemukan flagnya.

`Encode_text('UTF-16BE (1201)')`

picoCTF{16\_bits\_inst34d\_of\_8\_e141a0f7}

Matching ops: From Base85  
Valid UTF8  
Entropy: 4.43

FLAG: `picoCTF{16_bits_inst34d_of_8_e141a0f7}`