Write Up LEST2024

Killualemonade

Table of Contents

babyXor

Cryptography

i think its super easy

Author : BosToken

Attachment:
chall.py

Lampiran:

app.py

```
import random

flag = 'LEST2024{REDACTED}' #This is dummy flag
key_1 = [random.randint(1, 200) for _ in range(2)]
key_2 = [random.randint(1, 500) for _ in range(2)]

def enc(src, key):
    res = []
    for a, b in enumerate(src):
        if (a % 2 == 0):
            res.append(ord(b) ^ key[0])
        else:
            res.append(ord(b) ^ key[1])
    return res

res_1 = enc(flag, key_1)
res_2 = enc(flag, key_2)
print(res_2)

# output : [359, 216, 376, 201, 281, 173, 281, 169, 336, 229,
324, 239, 372, 254, 323, 252, 327, 241, 280, 243, 364, 248, 372,
240, 330, 214, 280, 194, 358, 248, 372, 245, 287, 237, 379, 228,
342]
```

Solusi:

tinggal di bruteforce xor hingga menemukan flag dengan awalan LEST2024

Solvernya:

solve.py

```
def dec(enc_res, key):
    res = []
    for a, b in enumerate(enc_res):
        if (a % 2 == 0):
            res.append(chr(b ^ key[0]))
        else:
            res.append(chr(b ^ key[1]))
    return ''.join(res)

def is_printable(s):
    return all(32 <= ord(c) <= 126 for c in s)

encrypted_result = [359, 216, 376, 201, 281, 173, 281, 169, 336,
229, 324, 239, 372, 254, 323, 252, 327, 241, 280, 243, 364, 248,
372, 240, 330, 214, 280, 194, 358, 248, 372, 245, 287, 237, 379,
228, 342]

for key1 in range(1, 501):
    for key2 in range(1, 501):
        decrypted = dec(encrypted_result, [key1, key2])
                                if    is_printable(decrypted)    and
decrypted.startswith('LEST2024'):
            print(f"Flag: {decrypted}")
            break
```

Hasilnya:

Flag: LEST2024{xor_chall3nGe_maK3_Me_h4pPy}

Alan Mathison

Cryptography

You should know after read my information. drmpuq_xc_upxs_atpvv Format flag LEST2024{flag}

Author : BosToken

Attachment:
Information.txt

Lampiran:

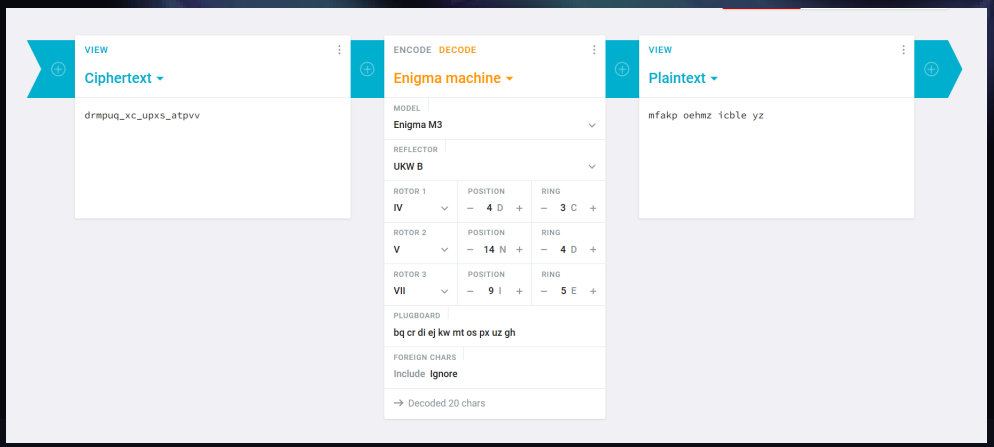
Information.txt

```
M3 UKWB
Rotor : IV, Postion : 4, Ring : 3
Rotor : V, Position : 14, Ring : 4
Rotor : VII, Position : 9, Ring : 5
```

Solusi:

kita hanya perlu mendecrypt sesuai dengan apa yang diberikan pada file information.txt.

Disini saya menggunakan cryptii untuk mendecryptnya



Flag : LEST2024{mfakp oehmz icble yz}

Crackme

Reverse Engineering

crack this code without needing to crack your monitor!

Author : moonap

Attachment:
crackme

Solusi:

Diberikan sebuah file, lalu langsung kita gunakan ghidra untuk menyelidiki file tersebut

```
strcat(param_9,(char *)param_6);
strcat(param_9,(char *)param_7);
strcat(param_9,(char *)param_8);
if (lVar1 != *(long *)(in_FS_OFFSET + 0x28)) {
                    /* WARNING: Subroutine does not return */
  __stack_chk_fail();
}
return;
```

disini saya menemukan sesuatu yang janggal yaitu, param_9 didapatkan ketika menggabungkan (concat) dari param_6 - param_9

Langsung saja kita eksekusi

Solver :

solve.py

```
import struct

def hex_to_str(val, length):
        return ''.join([chr((val >> (8 * i)) & 0xFF) for i in
range(length)])
param_1 = [
    0x6b2068616b617041, 0x2075617420756d61, 0x6973656e6f646e69,
    0x6e75706d656d2061, 0x796e616220696179, 0x6b6100
]
```

```
param_2      =      [0x702d6961746e6170,      0x6179206961746e61,
0x6861646e6920676e, 0x3f]
param_3 = [0x6e616b6b7573614d, 0x203a67616c6620]
param_4 = [0x6173207373706f4f, 0x67616c662068616c, 0x21]
param_5 = [0x616c462077776f57, 0x2172616e65622067, 0x00]
param_6      =      [0x373133315750464f,      0x605c7a7130756678,
0x675c4a5c48603771, 0x00]
param_7      =      [0x737c7e3142797459,      0x6442767e296f7e42,
0x7c2e75426f6f6872, 0x6f]
param_8      =      [0x7d7d66656d507b7b,      0x6c3f506767673b63,
0x3a6a6e6d3c3e396a, 0x72]

param_6_str = ''.join([hex_to_str(val, 8) for val in param_6])
param_2_str = ''.join([hex_to_str(val, 8) for val in param_2])
param_1_str = ''.join([hex_to_str(val, 8) for val in param_1])
for i in range(len(param_6_str)):
    if i >= len(param_6_str) or param_6_str[i] == '\0':
        break
    param_6_str = (param_6_str[:i] +
                                        chr(ord(param_6_str[i])  ^
ord(param_2_str[0x17]) ^ ord(param_1_str[7])) +
                   param_6_str[i+1:])

param_7_str = ''.join([hex_to_str(val, 8) for val in param_7])
param_4_str = ''.join([hex_to_str(val, 8) for val in param_4])
for i in range(len(param_7_str)):
    if i >= len(param_7_str) or param_7_str[i] == '\0':
        break
    param_7_str = (param_7_str[:i] +
                    chr(ord(param_7_str[i]) ^ ord(param_4_str[6])
^ ord(param_1_str[0x14])) +
                   param_7_str[i+1:])

param_8_str = ''.join([hex_to_str(val, 8) for val in param_8])
param_3_str = ''.join([hex_to_str(val, 8) for val in param_3])
for i in range(len(param_8_str)):
    if i >= len(param_8_str) or param_8_str[i] == '\0':
        break
    param_8_str = (param_8_str[:i] +
                   chr(ord(param_8_str[i]) ^ ord(param_4_str[10])
^ ord(param_3_str[0xc])) +
                   param_8_str[i+1:])

param_9 = param_6_str + param_7_str + param_8_str

print("param_9:", param_9)
```

Hasil:

```
param_9: LEST2024{ev3ry_cr4cK_I_d�������Did_,can_cr4ck_yourr_h3ar������tt_bjirrl4hhh_0ce613bae5}������
```

Flag:

param_9:
LEST2024{ev3ry_cr4cK_I_dDid_,can_cr4ck_yourr_h3artt_bjirrl4hhh_0ce613bae5}

Scramble Pyre

Reverse Engineering

irregular, like your life. so make it orderly

Author : moonap

Lampiran
`scramble.pyre.pyc`

Solusi:

Diberikan sebuah file pyc, langsung saja kita decompile

```
┌──(jersyy㉿Steven)-[~/KALIBER/Forensics]
└─$ pycdc scramble-pyre.pyc
# Source Generated with Decompyle++
# File: scramble-pyre.pyc (Python 2.7)


def logo():
    print '\nScramble Python\n'


def main():
    inputUser = raw_input('Ayo cek flagnya mas: ')
    splitString = list(inputUser)
    flage = []
    for i in range(0, len(splitString)):
        flag = ord(splitString[i]) + 13877459 + 332291
        flage.append(flag)

    if len(flage) == 53:
        if flage[41] == 14209845 and flage[14] == 14209862 and flage[4] == 14209800 and flage[38] == 14209799 and flage[0] == 14209826 and flage[26] == 1420
9860 and flage[25] == 14209798 and flage[17] == 14209855 and flage[32] == 14209801 and flage[27] == 14209845 and flage[51] == 14209851 and flage[40] == 1420
9851 and flage[48] == 14209804 and flage[20] == 14209845 and flage[16] == 14209858 and flage[29] == 14209802 and flage[35] == 14209871 and flage[11] == 1420
9849 and flage[45] == 14209847 and flage[3] == 14209834 and flage[15] == 14209799 and flage[13] == 14209859 and flage[44] == 14209849 and flage[12] == 14209
861 and flage[19] == 14209853 and flage[47] == 14209852 and flage[39] == 14209859 and flage[1] == 14209819 and flage[52] == 14209875 and flage[43] == 142098
48 and flage[36] == 14209845 and flage[46] == 14209852 and flage[23] == 14209866 and flage[42] == 14209806 and flage[9] == 14209850 and flage[10] == 1420980
1 and flage[28] == 14209869 and flage[31] == 14209866 and flage[49] == 14209847 and flage[24] == 14209854 and flage[21] == 14209862 and flage[22] == 1420987
1 and flage[7] == 14209802 and flage[33] == 14209845 and flage[18] == 14209860 and flage[50] == 14209800 and flage[5] == 14209798 and flage[6] == 14209800 a
nd flage[37] == 14209866 and flage[8] == 14209873 and flage[30] == 14209865 and flage[34] == 14209859 and flage[2] == 14209833:
            print 'Benar mas, itu flagnya.'
        else:
            print 'Itu bukan flagnya mas.'
    else:
        print 'Itu bukan flagnya mas.'

if __name__ == '__main__':
    logo()
    main()
```

setelah itu kita rapihkan sedikit

`scramble.pyre.py`

```
def logo():
    print('\nScramble Python\n')

def main():
    inputUser = raw_input('Ayo cek flagnya mas: ')
    splitString = list(inputUser)
    flage = []
```

```
    for i in range(0, len(splitString)):
        flag = ord(splitString[i]) + 13877459 + 332291
        flage.append(flag)

    if len(flage) == 53:
        if (flage[41] == 14209845 and flage[14] == 14209862 and
            flage[4] == 14209800 and flage[38] == 14209799 and
            flage[0] == 14209826 and flage[26] == 14209860 and
            flage[25] == 14209798 and flage[17] == 14209855 and
            flage[32] == 14209801 and flage[27] == 14209845 and
            flage[51] == 14209851 and flage[40] == 14209851 and
            flage[48] == 14209804 and flage[20] == 14209845 and
            flage[16] == 14209858 and flage[29] == 14209802 and
            flage[35] == 14209871 and flage[11] == 14209849 and
            flage[45] == 14209847 and flage[3] == 14209834 and
            flage[15] == 14209799 and flage[13] == 14209859 and
            flage[44] == 14209849 and flage[12] == 14209861 and
            flage[19] == 14209853 and flage[47] == 14209852 and
            flage[39] == 14209859 and flage[1] == 14209819 and
            flage[52] == 14209875 and flage[43] == 14209848 and
            flage[36] == 14209845 and flage[46] == 14209852 and
            flage[23] == 14209866 and flage[42] == 14209806 and
            flage[9] == 14209850 and flage[10] == 14209801 and
            flage[28] == 14209869 and flage[31] == 14209866 and
            flage[49] == 14209847 and flage[24] == 14209854 and
            flage[21] == 14209862 and flage[22] == 14209871 and
            flage[7] == 14209802 and flage[33] == 14209845 and
            flage[18] == 14209860 and flage[50] == 14209800 and
            flage[5] == 14209798 and flage[6] == 14209800 and
            flage[37] == 14209866 and flage[8] == 14209873 and
            flage[30] == 14209865 and flage[34] == 14209859 and
            flage[2] == 14209833):
            print('Benar mas, itu flagnya.')
        else:
            print('Itu bukan flagnya mas.')
    else:
        print('Itu bukan flagnya mas.')

if __name__ == '__main__':
    logo()
    main()
```

Lalu kita reverse saja

Solver:

solve.py

```
def get_original_char(flag_value):
    return chr(flag_value - 14209750)
flage = [0] * 53

flage[41] = 14209845
flage[14] = 14209862
flage[4] = 14209800
flage[38] = 14209799
flage[0] = 14209826
flage[26] = 14209860
flage[25] = 14209798
flage[17] = 14209855
flage[32] = 14209801
flage[27] = 14209845
flage[51] = 14209851
flage[40] = 14209851
flage[48] = 14209804
flage[20] = 14209845
flage[16] = 14209858
flage[29] = 14209802
flage[35] = 14209871
flage[11] = 14209849
flage[45] = 14209847
flage[3] = 14209834
flage[15] = 14209799
flage[13] = 14209859
flage[44] = 14209849
flage[12] = 14209861
flage[19] = 14209853
flage[47] = 14209852
flage[39] = 14209859
flage[1] = 14209819
flage[52] = 14209875
flage[43] = 14209848
flage[36] = 14209845
flage[46] = 14209852
flage[23] = 14209866
flage[42] = 14209806
flage[9] = 14209850
flage[10] = 14209801
flage[28] = 14209869
flage[31] = 14209866
flage[49] = 14209847
```

```
flage[24] = 14209854
flage[21] = 14209862
flage[22] = 14209871
flage[7] = 14209802
flage[33] = 14209845
flage[18] = 14209860
flage[50] = 14209800
flage[5] = 14209798
flage[6] = 14209800
flage[37] = 14209866
flage[8] = 14209873
flage[30] = 14209865
flage[34] = 14209859
flage[2] = 14209833

original_flag = ''.join(get_original_char(flag) for flag in flage)
print(f' {original_flag}')
```

Flag:

LEST2024{d3comp1ling_pyth0n_w4st3_my_t1me_8bcaff6a2e}

mywife

Forensic

help me to find out what is this

Format flag: Kaliber{*.}

Author : moonap

Attachment:
mywife.dd

Solusi:

Diberikan sebuah disk langsung saja kita eksekusi menggunakan Foremost

Setelah itu didapatkan:

```
┌──(jersyy㉿Steven)-[~/KALIBER/Forensics/foremost_output_new]
└─$ l
audit.txt  jpg/  png/
```

lalu di cek satu persatu hingga mendapatkan:

Flag:
Kaliber{sh3_is_beaut1ful,_isn't_she?}

yes she is :v

The Vanishing Code

Forensic

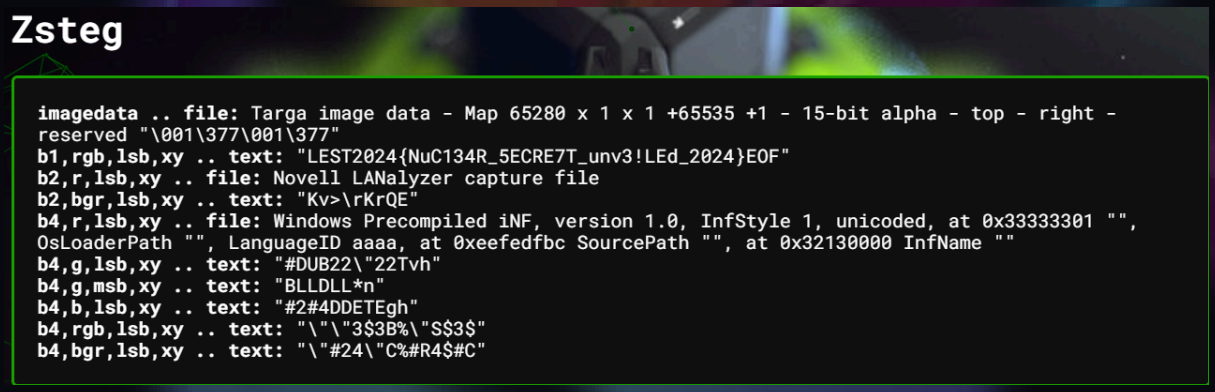
In 2024, a crucial message about a top-secret World War III operation was hidden within an image by a secret agent. This message isn't easily accessible, as each bit of the message has been concealed within the pixels of the image, and it can only be retrieved through a very specific method. Your task is to uncover the hidden message within the image named "secret".

Author: shalord
Attachment:
secret,png

Solusi:

disini saya coba menggunakan tools online yaitu Aperi'Solve dan mendapatkan flagnya

yang mana menggunakan zsteg



Flag:

`LEST2024{NuC134R_5ECRE7T_unv3!LEd_2024}`

HIDden spell

Forensic

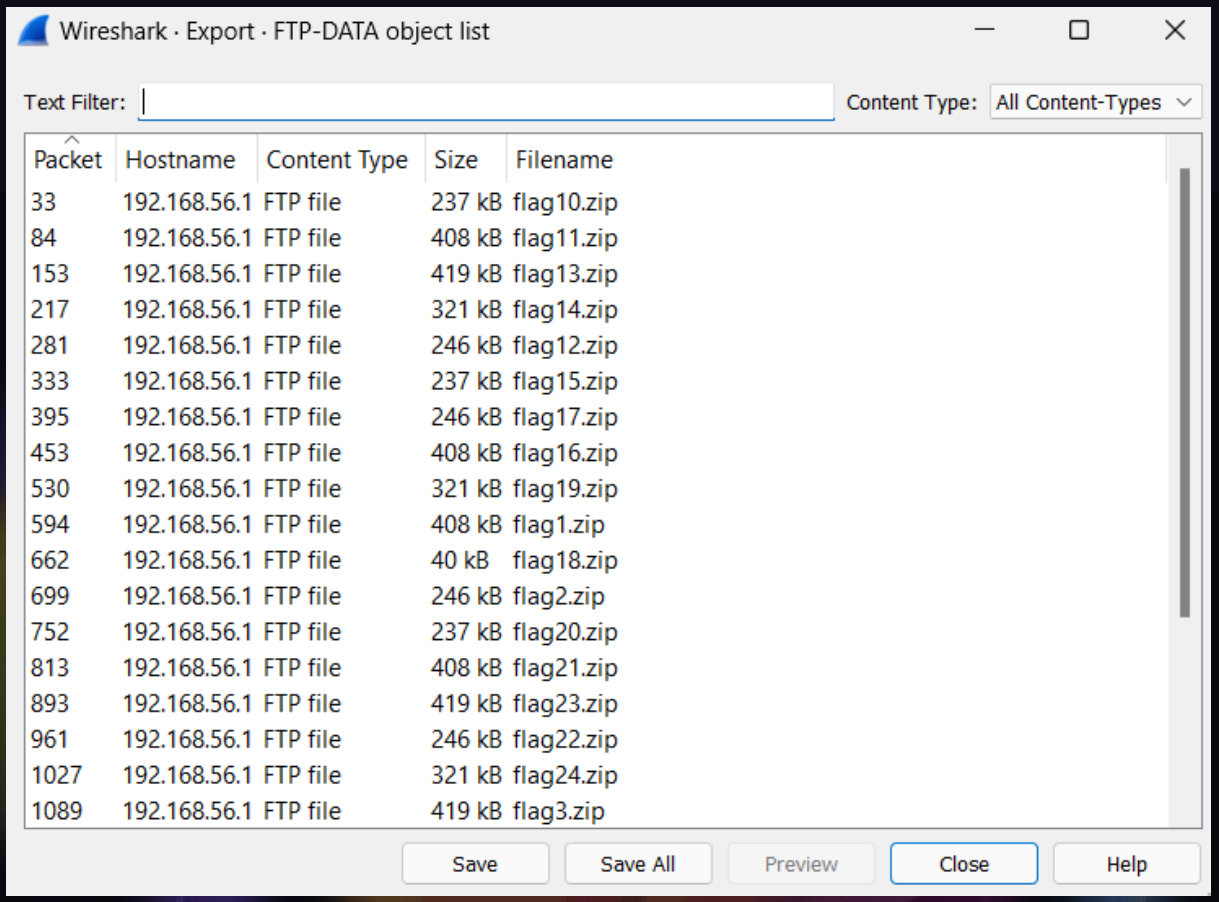
Amidst the bustling currents of packets coursing through diverse spells, your task is to uncover a singular book housing secret spell . Beware it could be anywhere where eyes could see.

Author : p0t4rr

Attachment:
`HIDden.pcapng`

Solusi:

Saat kita cek chall.pcapng menggunakan Wireshark, kita dapat lihat ada komunikasi FTP tanpa enkripsi. Kita bisa langsung export file yang ada dalam melalui File -> Export Objects -> FTP-DATA lalu klik Save All.



Sekarang kita mempunyai 25 File Flag.zip

Setelah ditelusuri 1 per satu, flag yang asli terdapat pada file Flag18,zip

tetapi kita membutuhkan password untuk membukanya, setelah menelusuri lebih dalam terdapat protokol USB yang mana dapat kita gunakan

Sumber :

https://ctftime.org/writeup/26887

https://help.ivanti.com/wl/help/en_US/Velocity/2.0.7/admin/keyboardCodes.htm?Highlight=key%20codes

Ternyata pw.zip hanya rabbit hole….

Hasil:

```
0b              H
17              T
17              T
13              P
16              S
020033000000000
38              /
38              /
13              P
04              A
16              S
17              T
08              E
05              B
0c              I
11              N
37              .
06              C
12              O
01              M
38              /
16              S
06              C
1f              2
14              Q
2000a           G
24              7
20015           r
1a              W

https://pastebin.com/sc2qG7Rw
```

Setelah itu kita masuk ke link diberikan file mega dan setelah di download kita perlu mengconvert dari country flag ship cipher menjadi password

Pass : VOLDEEEMORTTTT

Flag : LEST2024{Int3rc3pt3d_tr4nsmIssion_sUuccEsszzz}

Alien sound

Forensic

Anomaly sound? format flag LEST2024{.*}

Author : shalord

Attachment:
`Alien.wav`

Solusi:

Diberikan sebuah .wav file disini saya langsung mencoba spectogram dari wav tersebut dan didapatkan flag

Flag : LEST2024{YEEA_Y@N6_32_E2_AJ4H}

btw @nya susah diliat bang :v

Wika Wika

Forensic

Bocil kematian telah menamatkan game Cyberpunk_077, dan menyanyikan anthem kebangsaannya. Bisakah kamu mendapatkan hadiah rahasia dari game ini ?

Author : shalord

Lampiran

secret.gif

Solusi:

KIta ubah gif tersebut menjadi potongan img dan didapatkan flagnya

```
collage.png     secret.gif.010  secret.gif.023  secret.gif.036  secret.gif.049  secret.gif.062  secret.gif.075  secret.gif.088  secret.gif.101
report.xml      secret.gif.011  secret.gif.024  secret.gif.037  secret.gif.050  secret.gif.063  secret.gif.076  secret.gif.089  secret.gif.102
secret.gif      secret.gif.012  secret.gif.025  secret.gif.038  secret.gif.051  secret.gif.064  secret.gif.077  secret.gif.090  secret.gif.103
secret.gif.000  secret.gif.013  secret.gif.026  secret.gif.039  secret.gif.052  secret.gif.065  secret.gif.078  secret.gif.091  secret.gif.104
secret.gif.001  secret.gif.014  secret.gif.027  secret.gif.040  secret.gif.053  secret.gif.066  secret.gif.079  secret.gif.092  secret.gif.png
secret.gif.002  secret.gif.015  secret.gif.028  secret.gif.041  secret.gif.054  secret.gif.067  secret.gif.080  secret.gif.093  secret.gif:Zone.Identifier
secret.gif.003  secret.gif.016  secret.gif.029  secret.gif.042  secret.gif.055  secret.gif.068  secret.gif.081  secret.gif.094
secret.gif.004  secret.gif.017  secret.gif.030  secret.gif.043  secret.gif.056  secret.gif.069  secret.gif.082  secret.gif.095
secret.gif.005  secret.gif.018  secret.gif.031  secret.gif.044  secret.gif.057  secret.gif.070  secret.gif.083  secret.gif.096
secret.gif.006  secret.gif.019  secret.gif.032  secret.gif.045  secret.gif.058  secret.gif.071  secret.gif.084  secret.gif.097
secret.gif.007  secret.gif.020  secret.gif.033  secret.gif.046  secret.gif.059  secret.gif.072  secret.gif.085  secret.gif.098
secret.gif.008  secret.gif.021  secret.gif.034  secret.gif.047  secret.gif.060  secret.gif.073  secret.gif.086  secret.gif.099
secret.gif.009  secret.gif.022  secret.gif.035  secret.gif.048  secret.gif.061  secret.gif.074  secret.gif.087  secret.gif.100
```

Flag:

`LEST2024{meN@MA7KAn_cY83RPUNk_077}`

`Cukup ngedukun…`

Welcome

Misc

Flag : Tulis sendiri

Chall paling susah :v

Feedback

Feedback

https://lest.kaliber.or.id/testimonial

feedback.

Solusi: flag didapatkan pada link feedback

Flag : LEST2024{th4nkSz_Fo0r_p4rtIc1patE}