

Write Up

Internal 22 – Cyber tahun 2024

Nama Team:

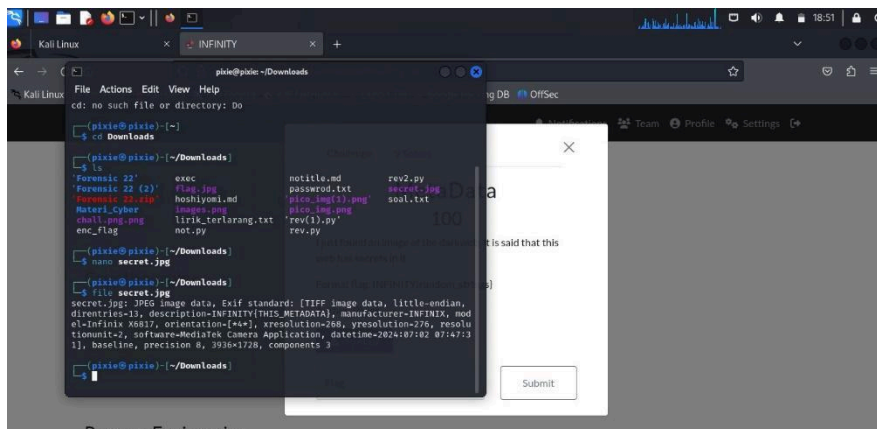
INFINITY USER 4

Anggota:

- Zuleyka Arum Adnin
- Lu'luah Nafisa
- Aliska Rizki Nur Anggraeni

Digital Forensic

A. Metadata

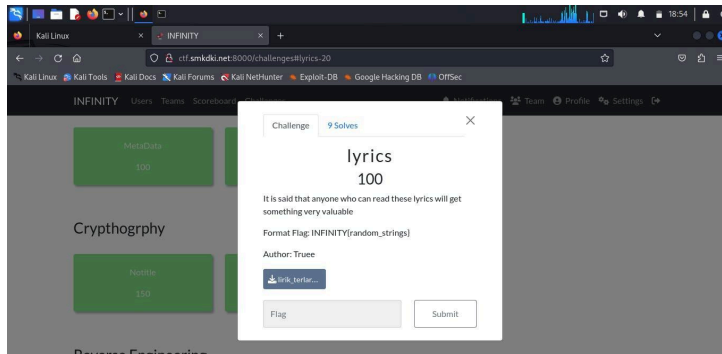


1. Pada soal Meta data terdapat sebuah file yang mana, file tersebut berjenis file PNG. Pada meta data kita harus mengetahui detail dari file PNG tersebut, maka dari itu kami menggunakan tools file.

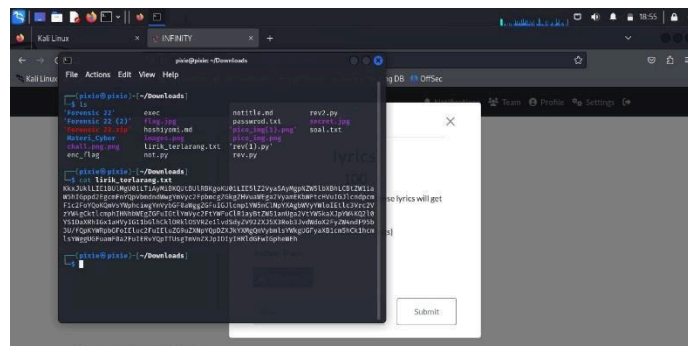
2. Setelah dilakukan file, maka didapatkan flag seperti gambar diatas

Flag: INFINITY{THIS_METADATA}

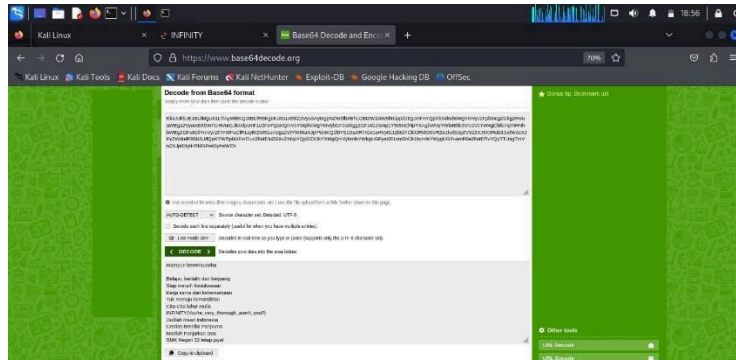
B. Lyrics



1. Pada soal lyrics terdapat sebuah file yang mana, file tersebut berjenis txt.



2. Kami mencoba untuk membaca file tersebut dengan command cat, dan didapat sebuah kata acak yang tentunya tidak bisa dibaca oleh manusia. Maka dari itu kami akan mendecode kata acak tersebut.



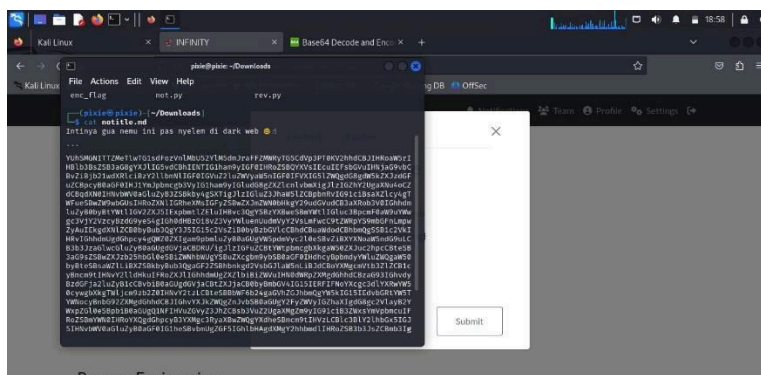
3. Buka base64 di Firefox, lalu paste kata acak yang sudah di salin dari file lirik_terlarang.txt tersebut

4. Dan kami mendapat flag diantara sebuah lirik seperti gambar diatas

Flag: INFINITY{You're_very_thorough_aren't_you? }

Cryptography

A. Notitle

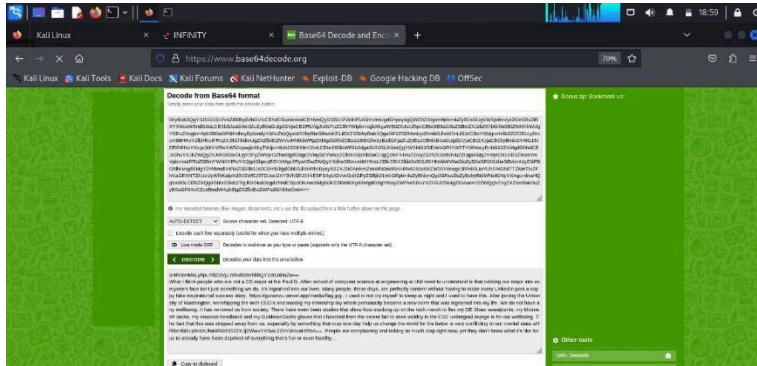


1. Pada soal lyrics terdapat sebuah file yang mana, file tersebut berjenis md.

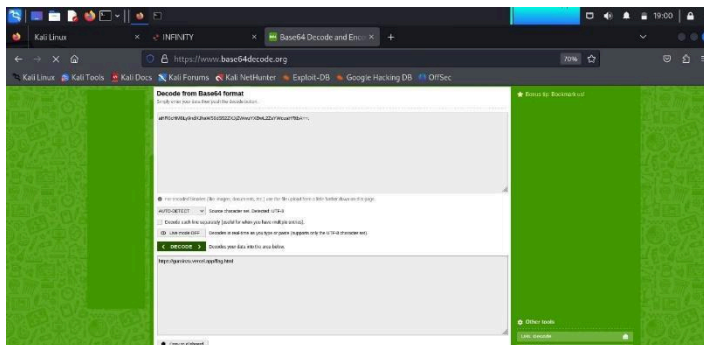
2. Kami mencoba untuk membaca file tersebut dengan command cat, dan didapat sebuah kata acak yang tentunya tidak bisa dibaca

oleh manusia. Maka dari itu kami akan mendecode kata acak tersebut

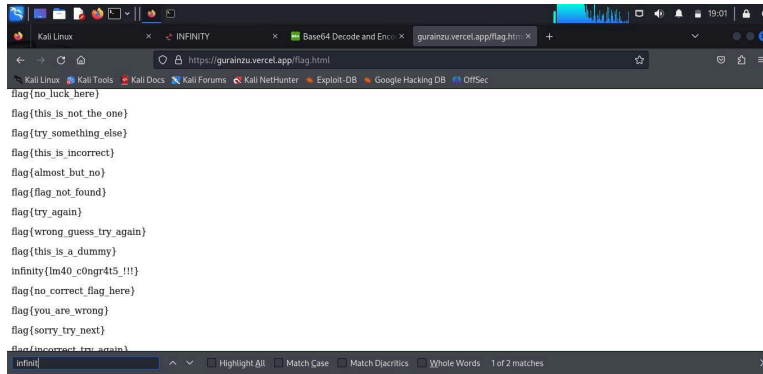
3. Buka base64 di Firefox, lalu paste kata acak yang sudah di salin dari file notitle.md tersebut.



4. Lalu didapat sebuah paragraf yang didalamnya terdapat sebuah kata acak lagi yang tentunya harus di decode kembali.



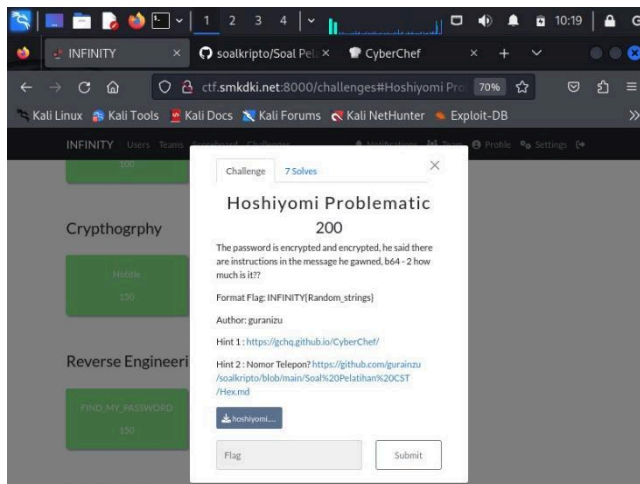
5. Setelah mendecode, kami mendapat sebuah alamat URL yang mengarah ke flag tersebut.



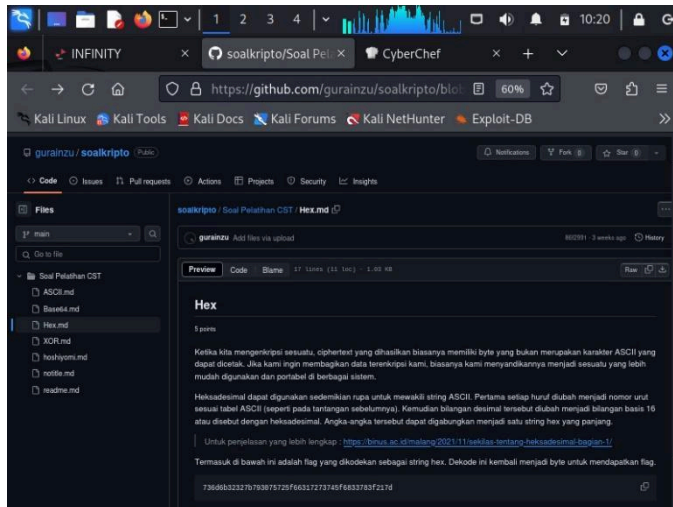
6. Saat dibuka, terdapat banyak kata², maka kami menggunakan Ctrl + f untuk menemukan sebuah kata yang kami cari, yaitu infinity

Flag: INFINITY {lm40_c0ngr4t5_!!!}

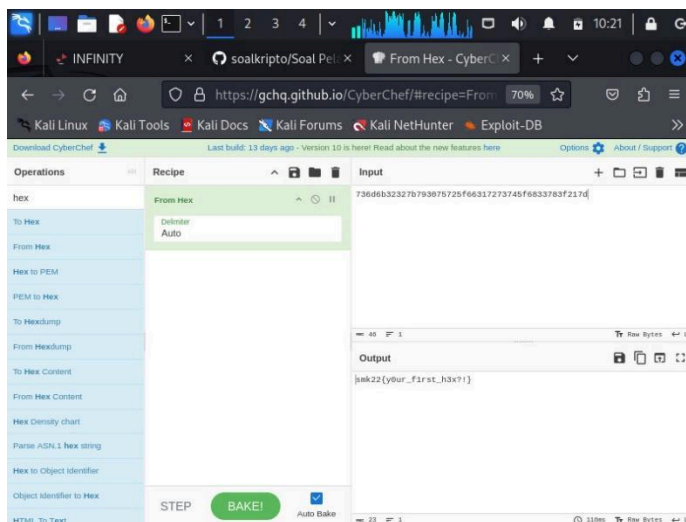
B. Hoshiyomi Problematic



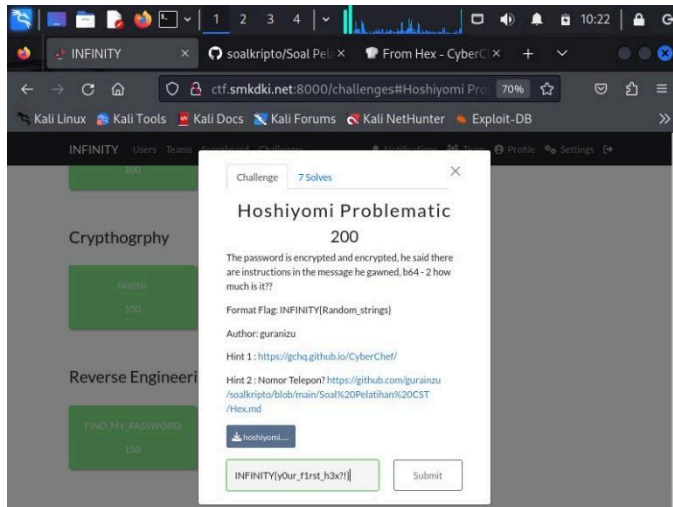
1. Pada soal hoshiyomi problematic terdapat 2 hint.



2. Pada hint 2 terdapat kata acak yang tidak bisa dibaca oleh manusia, maka dari itu kami akan mendecode kata acak tersebut.



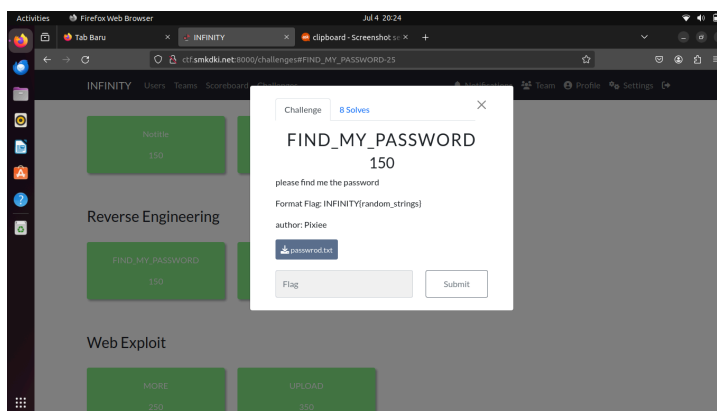
3. Buka link yang terdapat pada hint 1 untuk mendecode kata acak yang terdapat pada hint 2, decode kata acak tersebut menggunakan from hex. Setelah mendecode, keluarlah sebuah flag yang kita cari.



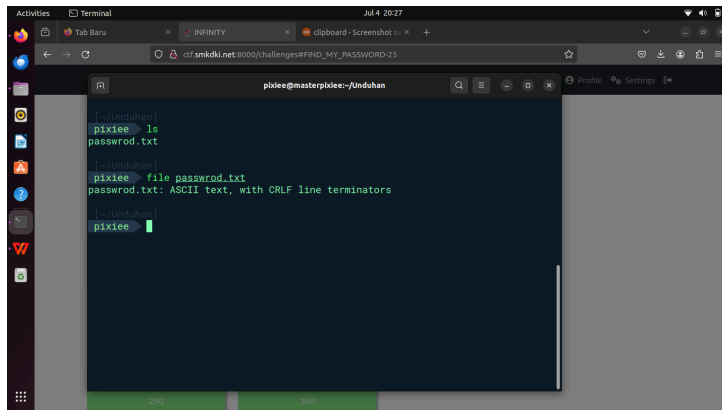
4. Ubah kata smk22 menjadi INFINITY
Flag : INFINITY{y0ur_f1rst_h3x?!}

Reverse Engineering

A. FIND_MY_PASSWORD



1. Pada soal find my password terdapat sebuah file yang berjenis txt

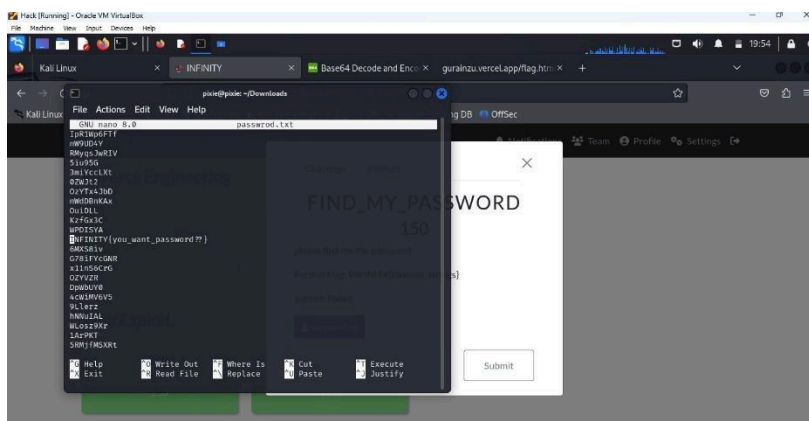


```
[~/Unduhan]
pixiee> ls
password.txt

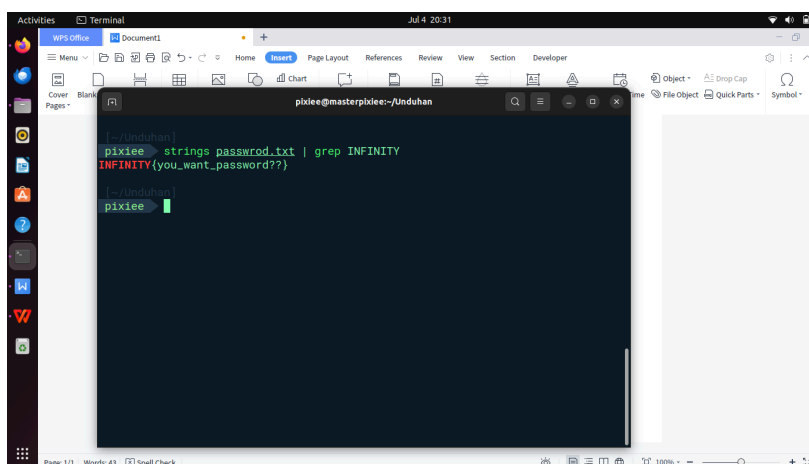
[~/Unduhan]
pixiee> file password.txt
password.txt: ASCII text, with CRLF line terminators

[~/Unduhan]
pixiee>
```

2. Lalu kami mencoba untuk membuka file tersebut dengan command nano



3. Dan didapat sebuah password acak yang sangat banyak jumlahnya



4. Format flag yang sedang kami cari ialah infinity, maka kami akan mencari kata infinity di antara password acak tersebut dengan cara ctrl + f. Lalu ketik infinity, dan didapat flag seperti gambar diatas.

Flag: INFINITY{you_want_password??}

B. Static

```
1 {Brx_uh_vr_juhdw_krz_gr_brx_nqrz_wkh_ydoxh_uhyhuvdo??}
2
3 It is said that this word is cursed, every sentence in it is shifted to 3 from the original letter, can you restore ??
4
5 jika kalian sudah berhasil tambahkan INFINITY di sebelum tanda kurawal
```

1. Diberikan soal seperti dan ada kata yang ke encrypt katnya setiap kata di shift menjadi 3 dari kata aslinya

```
soal.txt
1 def unshift_char_correct(char):
2     if 'a' <= char <= 'z':
3         return chr((ord(char) - ord('a') - 3) % 26 + ord('a'))
4     elif 'A' <= char <= 'Z':
5         return chr((ord(char) - ord('A') - 3) % 26 + ord('A'))
6     else:
7         return char
8
9 encrypted_string = _____
10
11
12 original_string = ''.join(unshift_char_correct(char) for char in encrypted_string)
13
14 print("This Your Flag:", original_string)
```

2. Dan diberikan script python untuk mengerjakanya disini sebenarnya kita hanya tinggal menaruh kata yang ter encrypt ke dalam variabel encrypted_string

```
GNU nano 6.2 rev.py
1 def unshift_char_correct(char):
2     if 'a' <= char <= 'z':
3         return chr((ord(char) - ord('a') - 3) % 26 + ord('a'))
4     elif 'A' <= char <= 'Z':
5         return chr((ord(char) - ord('A') - 3) % 26 + ord('A'))
6     else:
7         return char
8
9 encrypted_string = "{Brx_uh_vr_juhdw_krz_gr_brx_nqrz_wkh_ydoxh_uhyhuvdo??}"
10
11 original_string = ''.join(unshift_char_correct(char) for char in encrypted_string)
12
13 print("This Your Flag:", original_string)
```

3. menjadi seperti ini

```
pixiee -> python3 rev.py  
This Your Flag: {You_re_so_great_how_do_you_know_the_value_reversal??}
```

4. lalu ketika di RUN akan muncul flagnya

Flag : INFINITY

{You_re_so_great_how_do_you_know_the_value_reversal??}

Web Exploitation

A. MORE

Challenge 6 Solves X

MORE

250

I've just created a website and you're definitely looking for vulnerabilities on my website, look for hints to help you

Servers here: 192.168.3.22

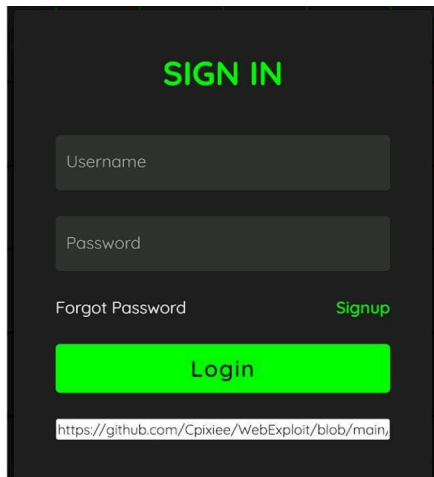
Formarts Flags: INFINITY{random_string}

Author: Pixiee

► View Hint

Flag Submit

1. Pada soal more terdapat sebuah IP address yang mengarah pada sebuah website



2. Kami mencoba untuk membukanya, dan didapatkan sebuah website seperti pada gambar diatas
3. Kami mencoba untuk melihat page source website tersebut dan mencoba mencari hint yang tersembunyi di website ini.
4. Kami menemukan hint pertama pada halaman style. css, pada hint pertama kami diarahkan untuk menemukan hint kedua lalu kami lanjut mencari hint kedua
5. Kami menemukan hint kedua pada halaman docker.py, hint kedua mengarahkan kami pada sebuah direktori secret.flag.
6. Kami mencoba merubah alamat URL website ini menjadi 192.168.3.22/secret.flag
7. Kami menemukan sebuah alamat URL pada halaman secret.flag

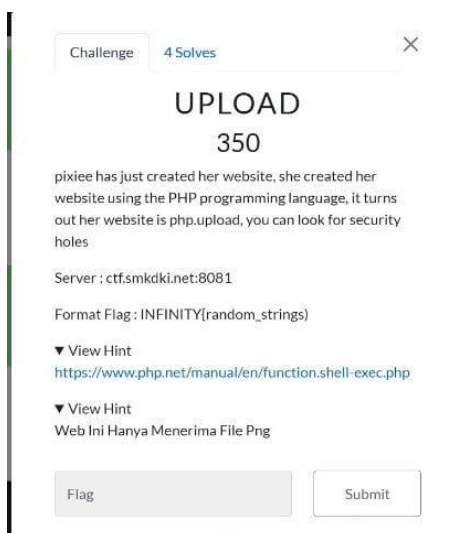
8. Kami mencoba untuk membuka alamat URL yang diberikan pada secret.flag, dan kami menemukan sebuah halaman seperti pada gambar diatas

9. Kami menemukan banyak payload SQL injection, lalu kami menggunakan Ctrl + f agar menemukan apa yang sedang kami cari

10. Kami mencari infinity dan di dapatkan flag seperti pada gambar diatas.

Flag: INFINITY {P4manas4n_DULU_G4_s333hhh_4400482}

B. UPLOAD



1. Pada soal upload terdapat sebuah alamat website yang harus kita kunjungi atau kami buka

A screenshot of a code editor with a dark background. The file name 'exploit.php' is visible in the top left corner. The code is as follows:

```
1 <?php
2 $output = shell_exec('cat flag.txt');
3
4 echo "<pre> $output </pre>";
5 ?>
```

2. Saat kami membuka alamat tersebut, terdapat sebuah halaman browse dan upload seperti gambar diatas

3. Kami diberikan 2 hint pada soal ini, hint yang pertama kami diberikan alamat URL yang mengarah kepada website PHP dan pada hint ke 2 kami diberikan petunjuk, bahwa hanya file PNG lah yang dapat diterima oleh website upload tersebut

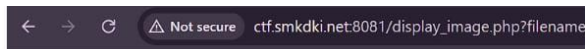
4. Hal pertama yang kami lakukan adalah membuat sebuah file di dalam CMD kali Linux dengan command nano flag.png. Mengapa kami menggunakan .png? Karena pada website upload tersebut terdapat sebuah filter, yang dimana hanya file tertentu yang dapat dikirim.

5. Langkah selanjutnya kami menyalin sebuah format yang ada pada hint 1 yang mengarah pada website php, pada hint 1 terdapat sebuah format atau syntax yang mengandung "ls" Atau list. List ini berfungsi untuk mengetahui file apa saja yang ada pada website upload.

6. Maka langsung saja kami save file yang sudah kami buat lalu kami kembali ke halaman website upload dan menekan browse lalu memasukkan file yang sudah kami buat tadi.

7. Setelah kami tekan upload, maka munculah beberapa file yang ada dalam website seperti pada gambar diatas.

8. Setelah itu, kami mengubah "ls" pada file flag.png menjadi "cat flag.txt"



Uploaded File

INFINITY{Your_picture_is_as_good_as_Leonardo_Davinci??_Is_it_you}

9. Lalu kami upload kembali file tersebut seperti pada gambar diatas, dan di dapatkan flag pada halaman website upload ini

Flag: INFINITY

{Your_picture_is_as_good_as_Leonardo_Davinci??_Is_it_you }