

Writeup Pemanasan Gemastik 15

H4ckM3

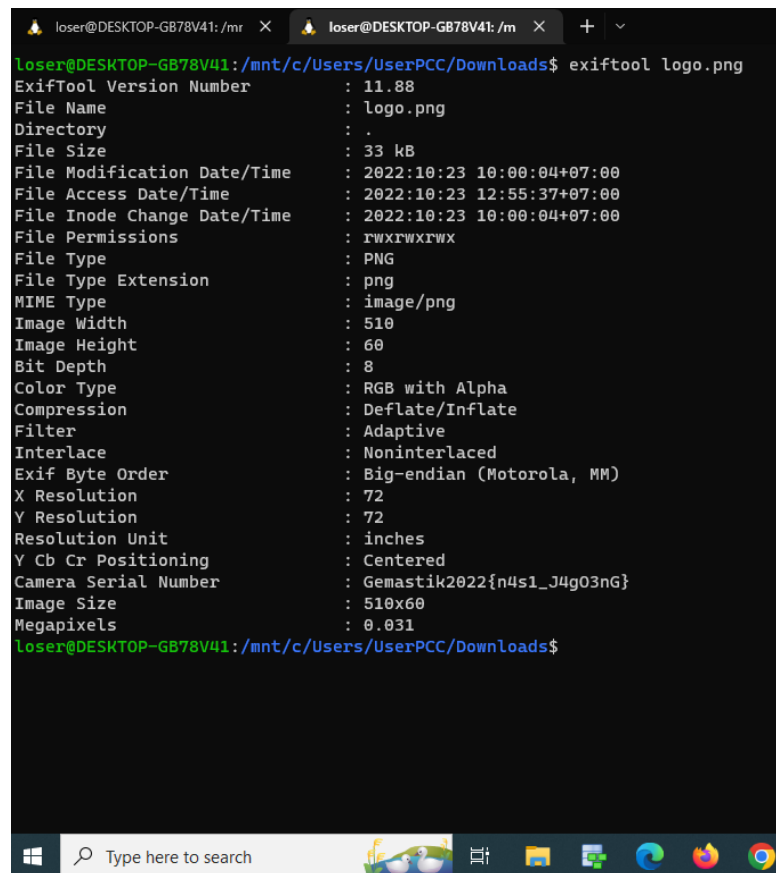
Forensics

1. So Meta..

diberikan sebuah gambar logo.png linknya [disini](#)

penyelesaian:

1. dari judul So Meta.. saya langsung berpikir ada sesuatu yang disembunyikan pada meta file, untuk mengekstrak meta saya gunakan tools exiftool



```
loser@DESKTOP-GB78V41: /mnt/c/Users/UserPCC/Downloads$ exiftool logo.png
ExifTool Version Number      : 11.88
File Name                    : logo.png
Directory                   : .
File Size                   : 33 kB
File Modification Date/Time  : 2022:10:23 10:00:04+07:00
File Access Date/Time       : 2022:10:23 12:55:37+07:00
File Inode Change Date/Time  : 2022:10:23 10:00:04+07:00
File Permissions             : rwxrwxrwx
File Type                   : PNG
File Type Extension         : png
MIME Type                   : image/png
Image Width                 : 510
Image Height                : 60
Bit Depth                   : 8
Color Type                  : RGB with Alpha
Compression                 : Deflate/Inflate
Filter                      : Adaptive
Interlace                   : Noninterlaced
Exif Byte Order              : Big-endian (Motorola, MM)
X Resolution                 : 72
Y Resolution                 : 72
Resolution Unit              : inches
Y Cb Cr Positioning          : Centered
Camera Serial Number         : Gemastik2022{n4s1_J4gO3nG}
Image Size                  : 510x60
Megapixels                   : 0.031
loser@DESKTOP-GB78V41: /mnt/c/Users/UserPCC/Downloads$
```

2. didapatkan flag pada Camera Serial Number:
Gemastik2022{n4s1_J4gO3nG}

2. Where is my flag??

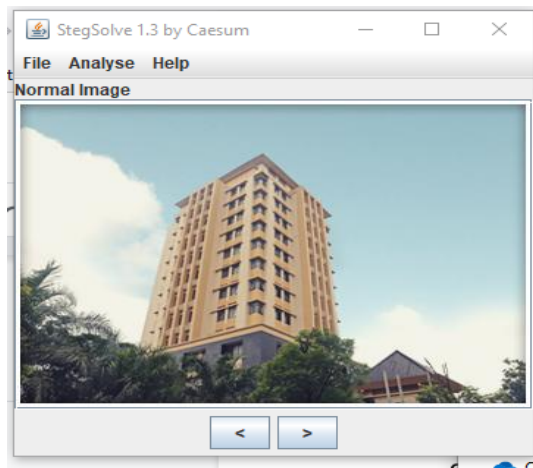
description:

I lost my flags there... i can only hope no one will hack me

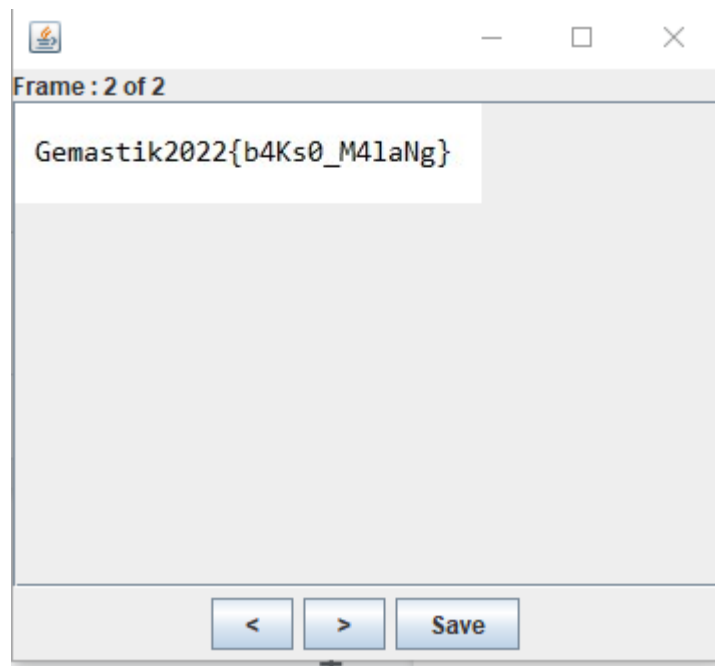
[profile.jpg](#)

penyelesaian:

1. saya menggunakan tools stegsolve untuk menyelesaikan chall ini.



2. kemudian saya coba analisis frame menggunakan menu analyse pilih frame browser, dan benar saja ada 2 frame dan pada frame yang kedua terdapat flagnya



Flagnya: Gemastik2022{b4Ks0_M4lNg}

Kriptografi

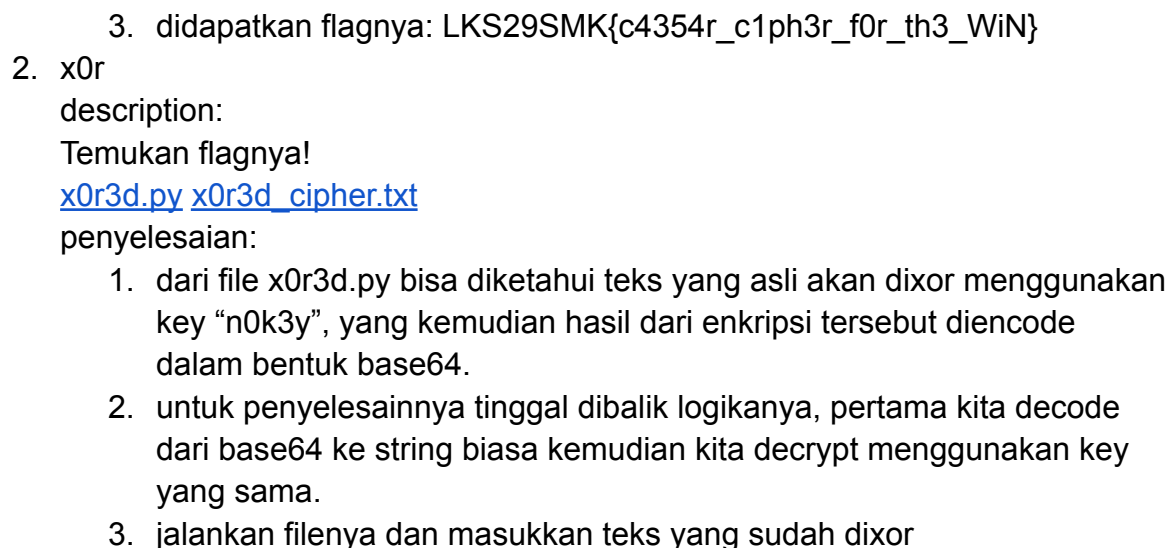
1. Thanks God, it's easy

description:

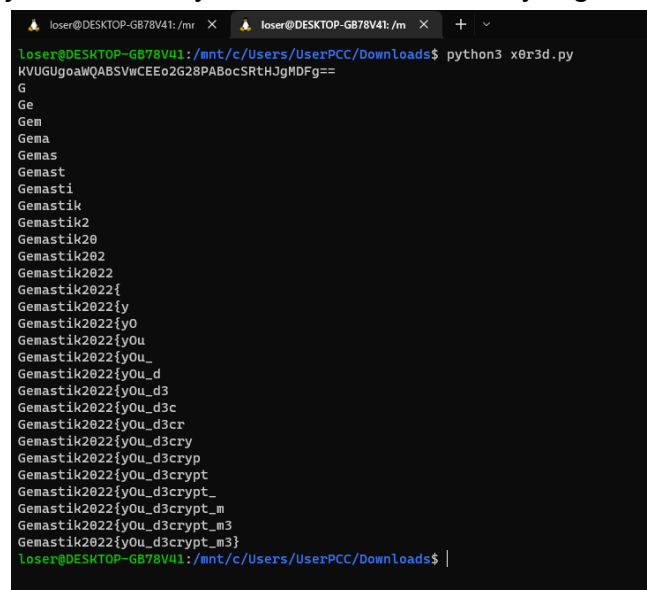
VUC29CWU{m4354b_m1zr3b_p0b_dr3_GsX}

penyelesaian:

1. dari soal yang diberikan diketahui adalah caesar cipher, selanjutnya lakukan decode menggunakan tools online dcode.fr
2. kemudian decrypt dengan metode bruteforce



4. yeavy dapet flagnya: Gemastik2022{yOu d3crypt m3}



3. Encoder-Decoder

description:

Pecahkan encrypted textnya!

[jatim-enc.py](#) [encrypted.txt](#)

penyelesaian:

1. disediakan file encrypter dan file yang berisi string yang sudah dienkripsi.
2. dair file `jatim-enc.py` bisa diketahui logikanya string awal akan dibalik kemudian diubah ke dalam bentuk unicode selanjutnya dixor dengan heksadesimal `0x50` kemudian ditambah 9 dan hasilnya dikalikan dengan string 'X' setelah itu ditambahkan - diakhir
3. untuk penyelesaiannya kita balik logikanya kita pecah menjadi array terlebih dahulu dengan delimiter -, supaya - ini nantinya tidak ikut kedalam array. selanjutnya kita balik arraynya agar yang tadi diakhir kembali ke posisi awal. selanjutnya kita hitung jumlah 'X' nya dan dikurangi 9 lalu dixor dengan heksadesimal `0x50` kemudian ubah dari unicode menjadi character.
4. selanjutnya jalankan decrypt nya dengan inputan file yang sudah dienkripsi.

```
loser@DESKTOP-GB78V41:/mnt/c/Users/UserPCC/Downloads$ python3 jatim-enc.py
G
Ge
Gem
Gema
Gemast
Gemasti
Gemastik
Gemastik2
Gemastik20
Gemastik202
Gemastik2022
Gemastik2022{
Gemastik2022{t
Gemastik2022{tH
Gemastik2022{tHa
Gemastik2022{tHan
Gemastik2022{tHanK
Gemastik2022{tHanKs
Gemastik2022{tHanKs_
Gemastik2022{tHanKs_f
Gemastik2022{tHanKs_f0
Gemastik2022{tHanKs_f0r
Gemastik2022{tHanKs_f0r_
Gemastik2022{tHanKs_f0r_f
Gemastik2022{tHanKs_f0r_f1
Gemastik2022{tHanKs_f0r_f1n
Gemastik2022{tHanKs_f0r_f1nd
Gemastik2022{tHanKs_f0r_f1nd1
Gemastik2022{tHanKs_f0r_f1nd1n
Gemastik2022{tHanKs_f0r_f1nd1ng
Gemastik2022{tHanKs_f0r_f1nd1ng_
Gemastik2022{tHanKs_f0r_f1nd1ng_m
Gemastik2022{tHanKs_f0r_f1nd1ng_m3
Gemastik2022{tHanKs_f0r_f1nd1ng_m3}
None
loser@DESKTOP-GB78V41:/mnt/c/Users/UserPCC/Downloads$
```

5. taraaa flagnya: `Gemastik2022{tHanKs_f0r_f1nd1ng_m3}`

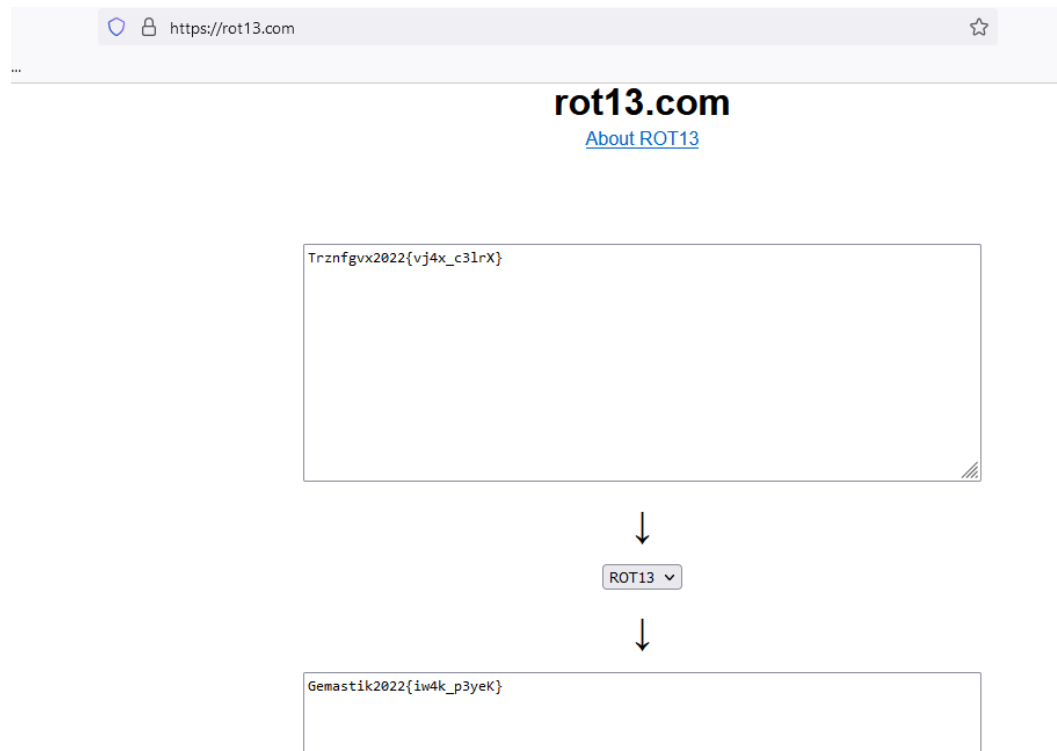
4. Heavy Rotation 13

description:

Trznfgvx2022{vj4x_c3lrX}

penyelesaian:

1. dari judul yang diberikan saya beranggapan soal yang diberikan adalah encode metode ROT 13
2. untuk penyelesaiannya decode menggunakan tools online rot13.com



3. dapat flagnya dong: Gemastik2022{iw4k_p3yeK}

Web

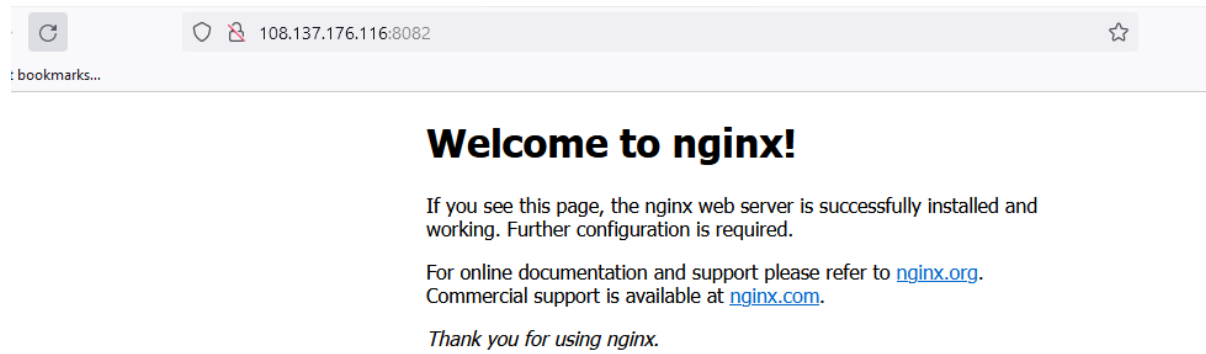
1. Duh!

description:

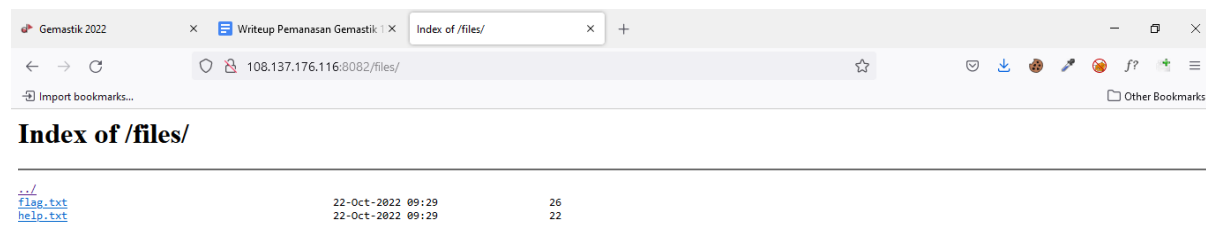
108.137.176.116:[8081-8083]

penyelesaian:

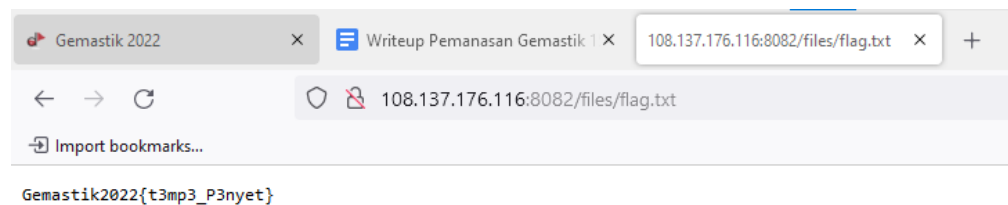
1. diberikan sebuah alamat ip dan range port dari 8081 sampai 8083
2. ketika saya kunjungi ternyata hanya port 8082 dan 8083 yang bisa diakses lewat browser.
3. saya fokus pada port 8082 terlebih dahulu.



4. ternyata hanya menampilkan halaman default nginx
5. saya coba masukkan directory files/



6. terdapat 2 file pada directory files/ yaitu flag.txt dan help.txt
7. dan ternyata flagnya ada difile flag.txt



8. submit flagnya: Gemastik2022{t3mp3_P3nyet}

— Terima kasih —