Write Up

FR13NDS

#Misc

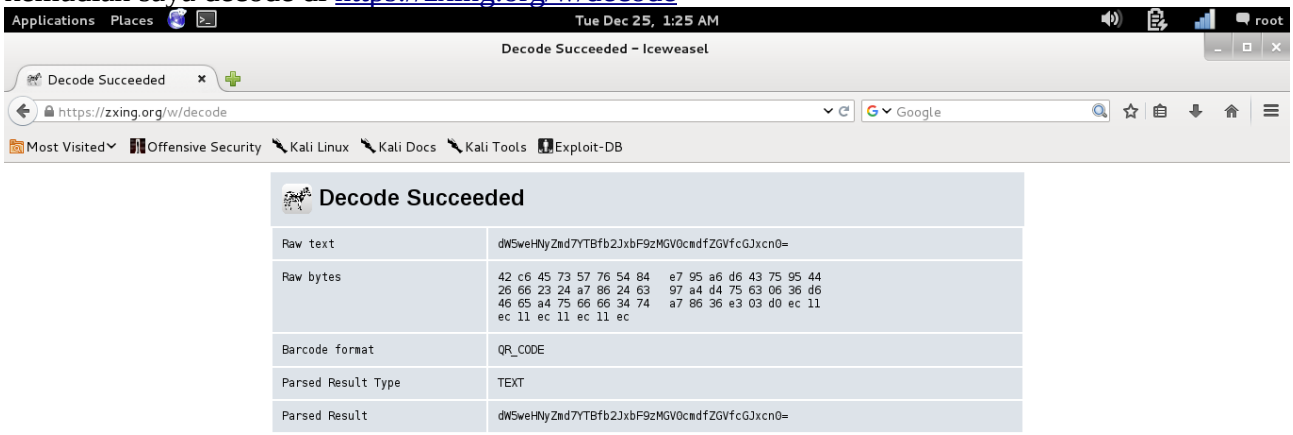
Test Flag (10pts)

hanya copy paste flag : HackFest{test_flag}

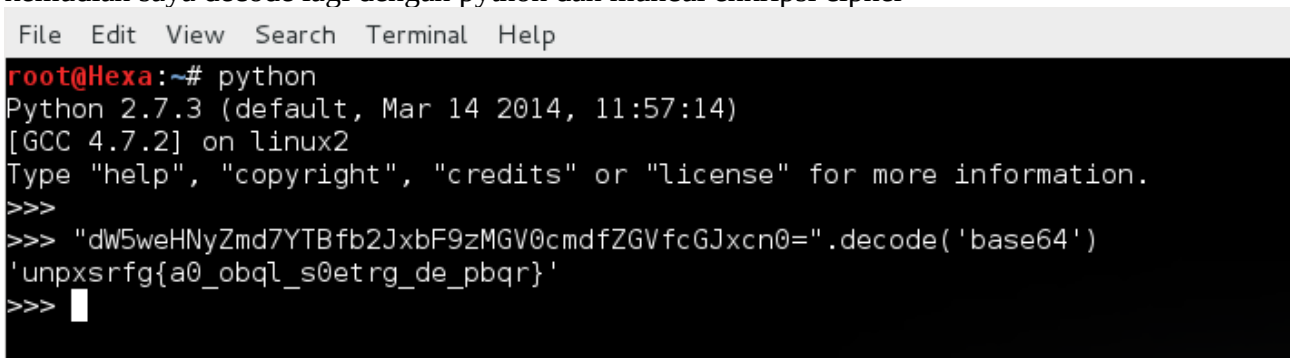
QR Code (364pts)

Diberikan sebuah berkas, dengan nama Flag.png

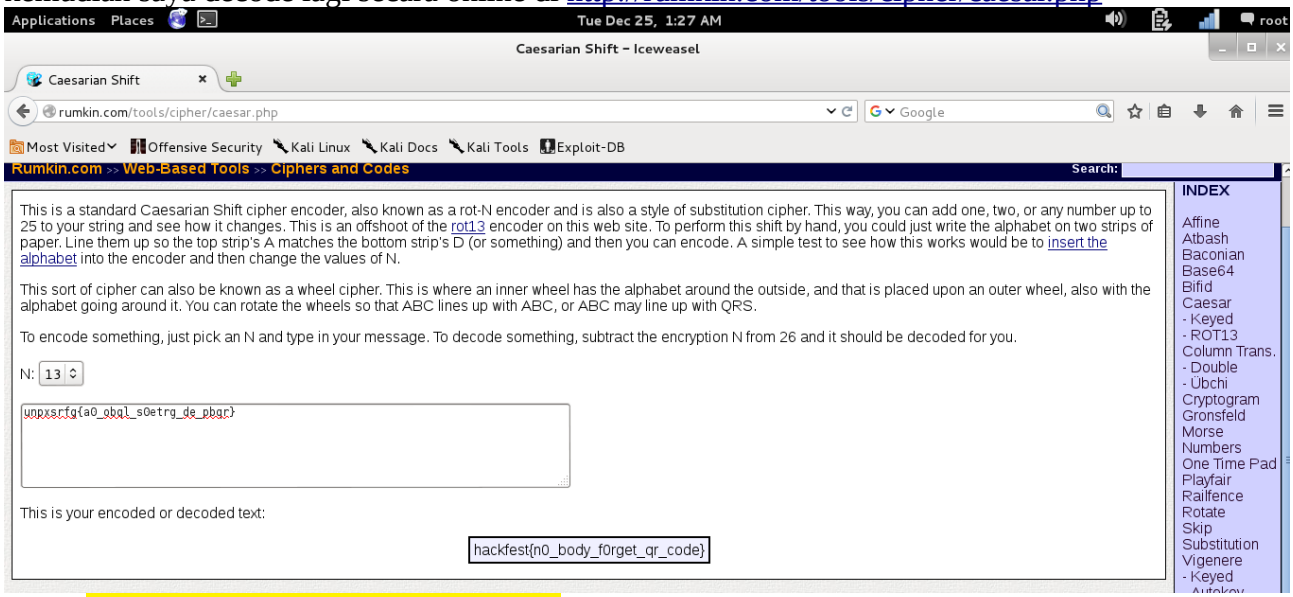
kemudian saya decode di https://zxing.org/w/decode



dan muncul hasil enkripsi base64
dW5weHNyZmd7YTBfb2JxbF9zMGV0cmdfZGVfcGJxcn0=
kemudian saya decode lagi dengan python dan muncul enkripsi cipher

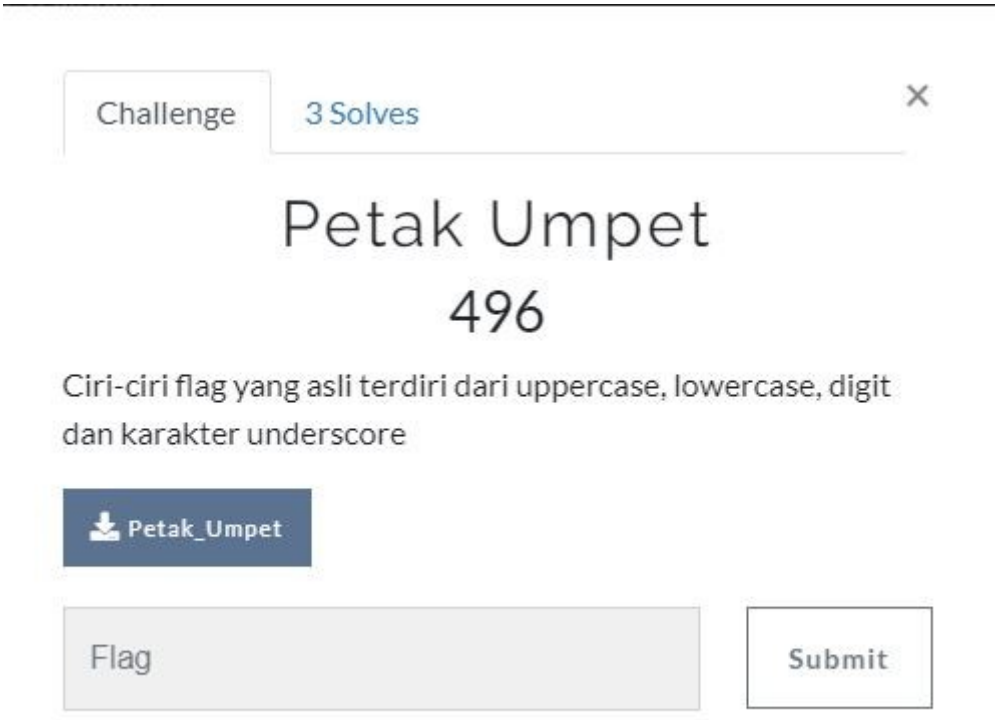


unpxsrfg{a0_obql_s0etrg_de_pbqr}
kemudian saya decode lagi secara online di http://rumkin.com/tools/cipher/caesar.php

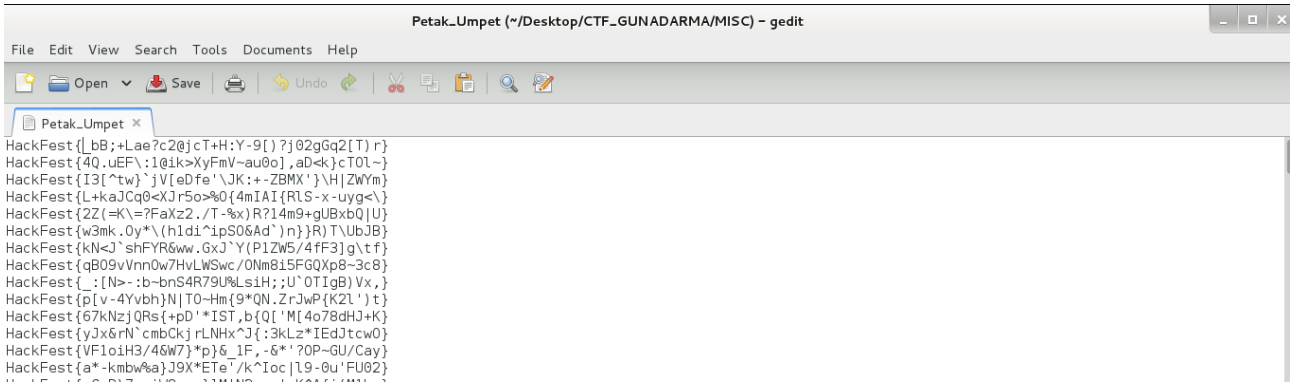


Flag : HackFest{n0_body_f0rget_qr_code}

Petak Umpet (496pts)



diberikan sebuah berkas, dengan nama Petak_Umpet



kemudian saya buka terminal dan memfilter dengan perintah grep seperti pada scrnshoot di bawah ini

```
root@Hexa: ~/Desktop/CTF_GUNADARMA/MISC
File  Edit  View  Search  Terminal  Help
root@Hexa:~/Desktop/CTF_GUNADARMA/MISC# grep -vn '[@|;|+|:|-|.|?|`|~|/|\|(|)|*|&|%|^|=]' Petak_Umpet
3239:HackFest{{C1I8Eol_gthn]n4ZN2qCoMm}QFdmnZCffh}
5473:HackFest{7EdI>8uXo]h8P2lhr0qf'MJ9jOEJAhbTbGx}
```

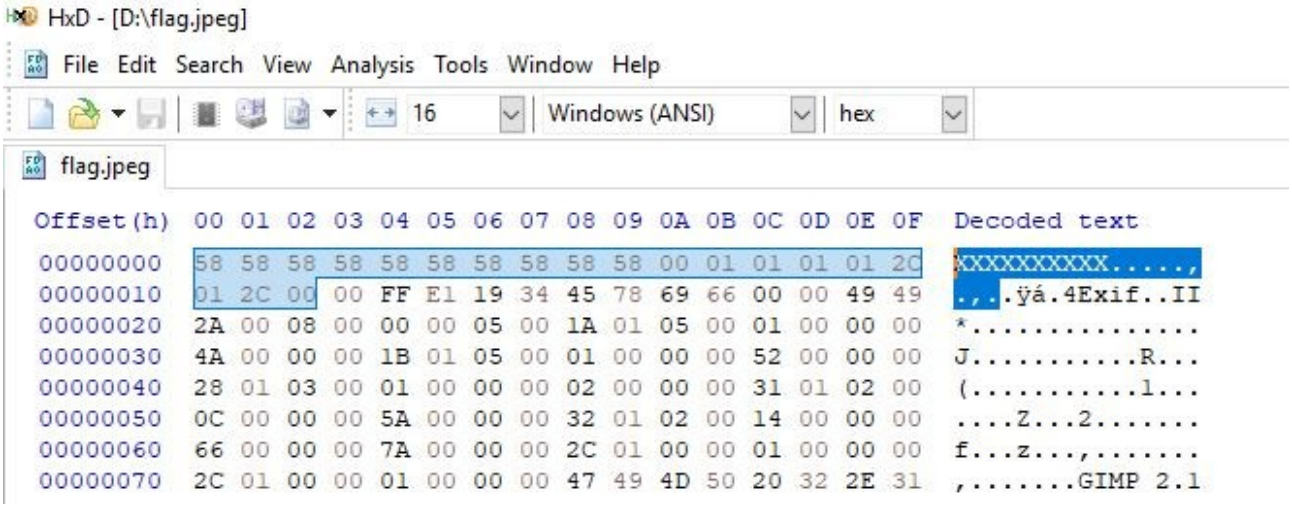
dan flag muncul pada baris ke 68938

Flag : HackFest{tidaaak_semudah_itu_fergusoooo00000}

#Forensic

Tanda Tangan (445pts)

Diberikan sebuah berkas, dengan nama flag.jpg karna nama soal tanda tangan, kemudian saya coba cek dengan HexEditor. Dan benar saja header file salah



saya rubah menjadi

HxD - [D:\CTF_GUNADARMA\FORENSIC\tanda tangan\flag.jpeg]

File Edit Search View Analysis Tools Window Help

16 | Windows (ANSI) | hex

flag.jpeg

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	00	00	01	ÿØÿà..JFIF.....
00000010	00	01	00	00	FF	E1	19	34	45	78	69	66	00	00	49	49	....ÿá.4Exif..II
00000020	2A	00	08	00	00	00	05	00	1A	01	05	00	01	00	00	00	*.....
00000030	4A	00	00	00	1B	01	05	00	01	00	00	00	52	00	00	00	J.....R...
00000040	28	01	03	00	01	00	00	00	02	00	00	00	31	01	02	00	(.....1...
00000050	0C	00	00	00	5A	00	00	00	32	01	02	00	14	00	00	00	....Z...2.....
00000060	66	00	00	00	7A	00	00	00	2C	01	00	00	01	00	00	00	f...z...,.....
00000070	2C	01	00	00	01	00	00	00	47	49	4D	50	20	32	2E	31	,.....GIMP 2.1

kemudian saya save dan mendapatkan flag

Flag : HackFest{F1L3_S1gn4tur3}

Kitty’s BF (496pts)

Diberikan sebuah berkas, dengan nama Kucing.jpg

kemudian saya analisis dengan perintah strings dan grep

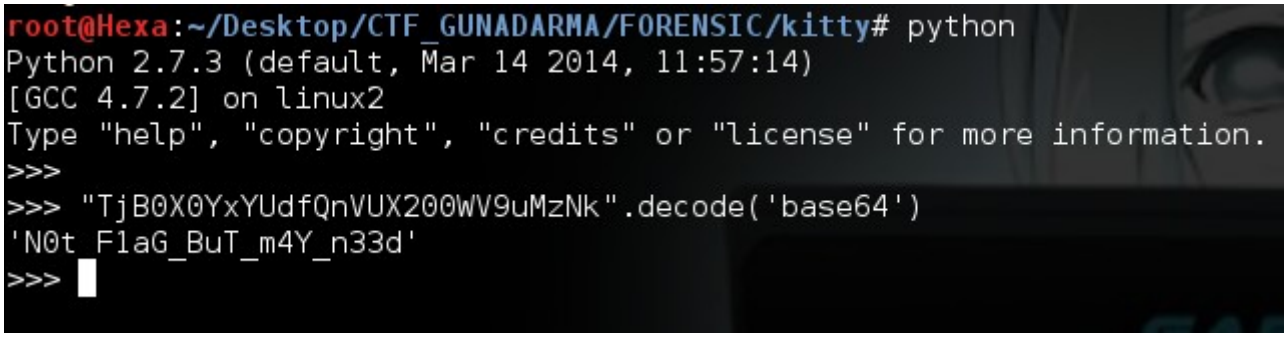
```
File  Edit  View  Search  Terminal  Help
root@Hexa:~/Desktop/CTF_GUNADARMA/FORENSIC/kitty# strings Kucing.jpg | grep -i "
flag"
realflag.txt
realflag.txt
root@Hexa:~/Desktop/CTF_GUNADARMA/FORENSIC/kitty#
```

dan benar saja muncul file txt di dalam file jpg tersebut, kemudian saya rubah format dari file Kucing.jpg menjadi Kucing.zip kemudian extract

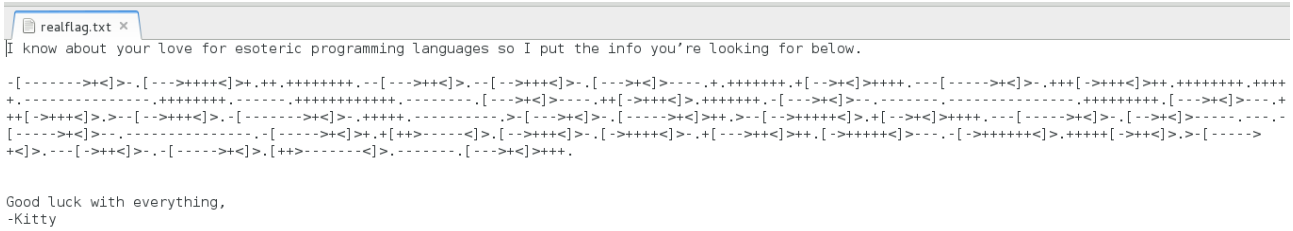
tapi tidak semudah itu :v file masih terpassword, niat mau saya crack make fcrackzip tapi tidak jadi :D saya coba cek dengan exiftool

```
File  Edit  View  Search  Terminal  Help
root@Hexa:~/Desktop/CTF_GUNADARMA/FORENSIC/kitty# exiftool Kucing.zip
ExifTool Version Number         : 8.60
File Name                       : Kucing.zip
Directory                       : .
File Size                       : 220 kB
File Modification Date/Time     : 2018:12:24 06:43:31-05:00
File Permissions                : rw-------
File Type                       : JPEG
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Exif Byte Order                 : Little-endian (Intel, II)
Software                        : Google
Copyright                       : TjB0X0YxYUdfQnVUX200WV9uMzNk
Exif Version                    : 0220
Exif Image Width                : 700
Exif Image Height               : 522
Image Width                     : 700
Image Height                    : 522
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 700x522
root@Hexa:~/Desktop/CTF_GUNADARMA/FORENSIC/kitty#
```

dan benar saja muncul enkripsi base64, kemudian saya decode

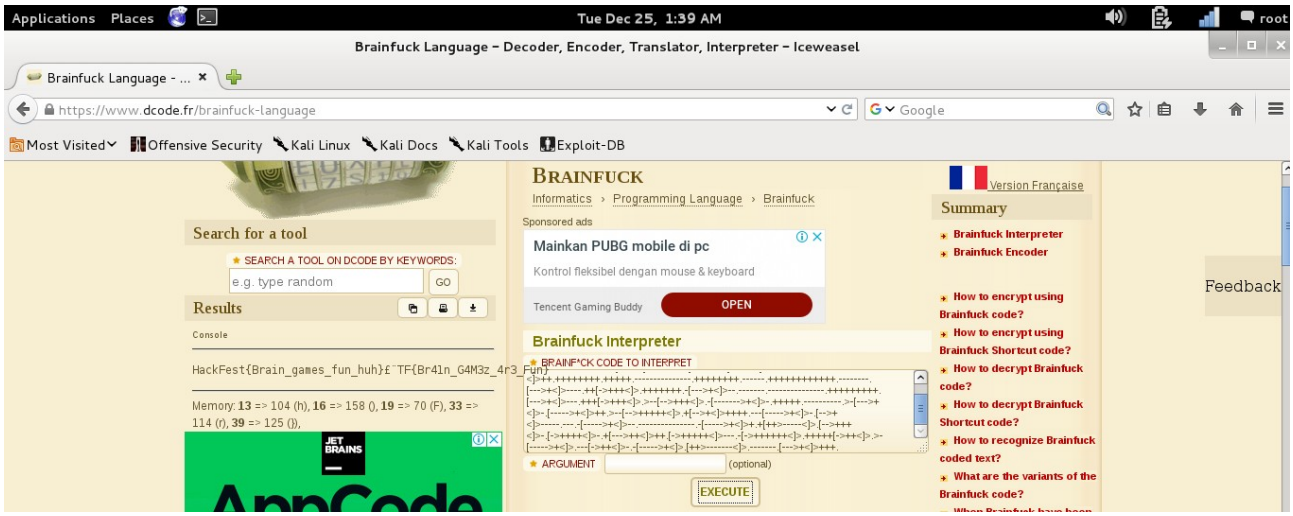


password untuk membuka zip N0t_F1aG_BuT_m4Y_n33d



kemudian saya perhatikan di situ ada kata kunci yang menurut saya clue **"I know about your love for esoteric programming languages so I put the info you're looking for below"** kemudian saya coba cari tau apa itu esoteric languange dan mendapatkan clue lagi yaitu Brainf**k

kemudian saya decode https://www.dcode.fr/brainfuck-language

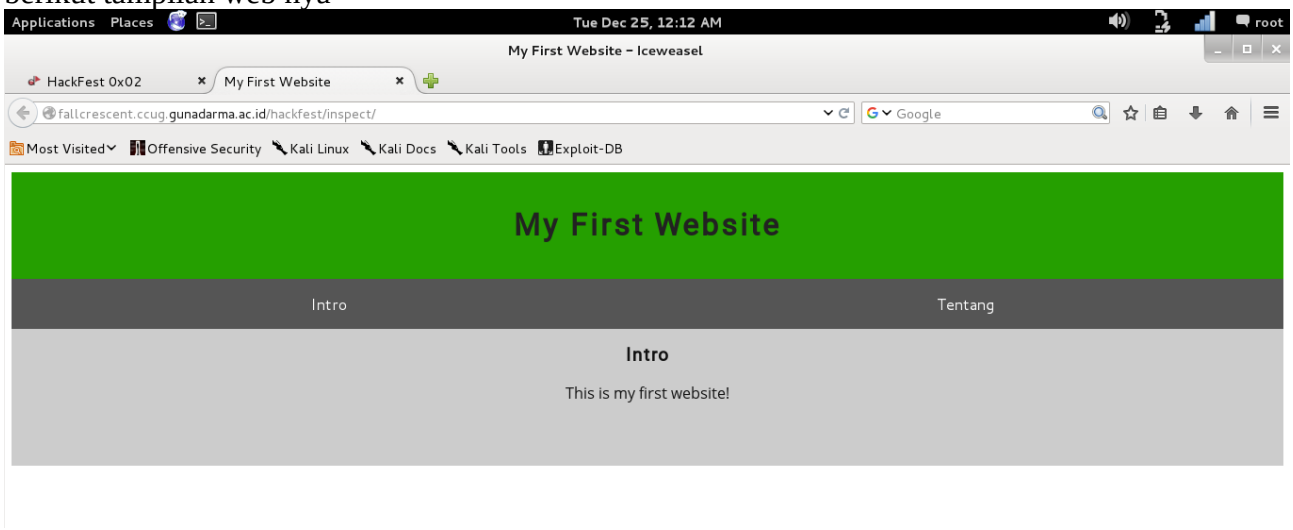


Flag : HackFest{Brain_games_fun_huh}

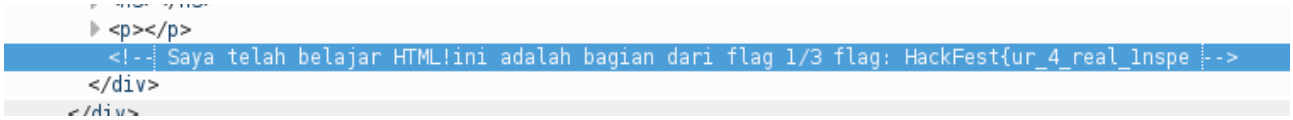
#Web

Inspect Me!(280pts)

di berikan link http://fallcrescent.ccug.gunadarma.ac.id/hackfest/inspect/
berikut tampilan web nya

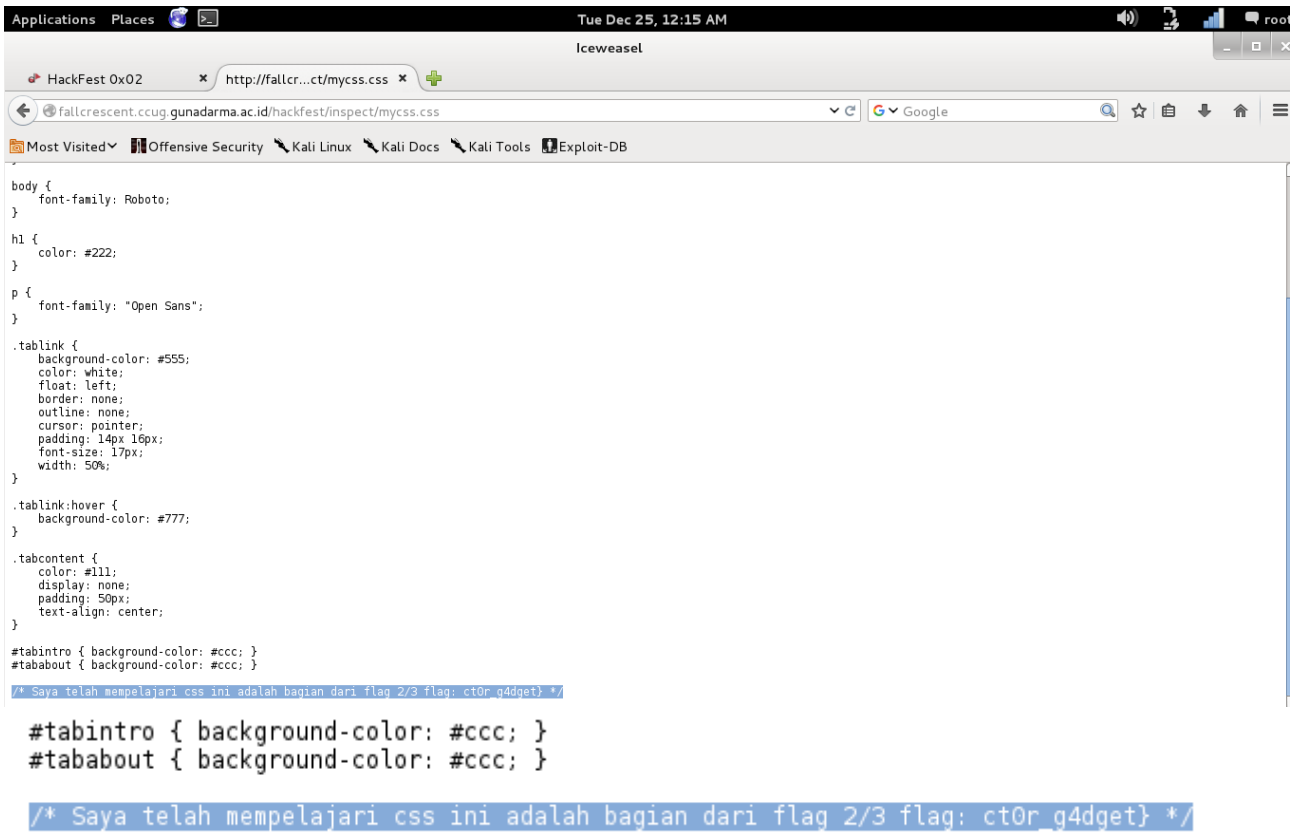


kemudian saya inspect element



dan mendapatkan flag pertama yaitu HackFest{ur_4_real_1nspe
kemudian saya cek lagi ada yang menarik yaitu mycss.css dan myjs.js

kemudian saya tambahkan http://fallcrescent.ccug.gunadarma.ac.id/hackfest/inspect/mycss.css



Flag : HackFest{ur_4_real_1nspect0r_g4dget}

Secara garis besar, saya mengucapkan terima kasih kepada tim FR13NDS yang telah membantu saya menyelesaikan soal dan membuat WriteUp

FR13NDS