

WRITE UP CTF ICYPTION 2020 dari TEAM SIJA

Write Up Recon

any information on this website?

100

<http://180.250.135.6:8080/src/>

you will find quite interesting information using superuser accounts

diberikan sebuah URL website dan saya klik login

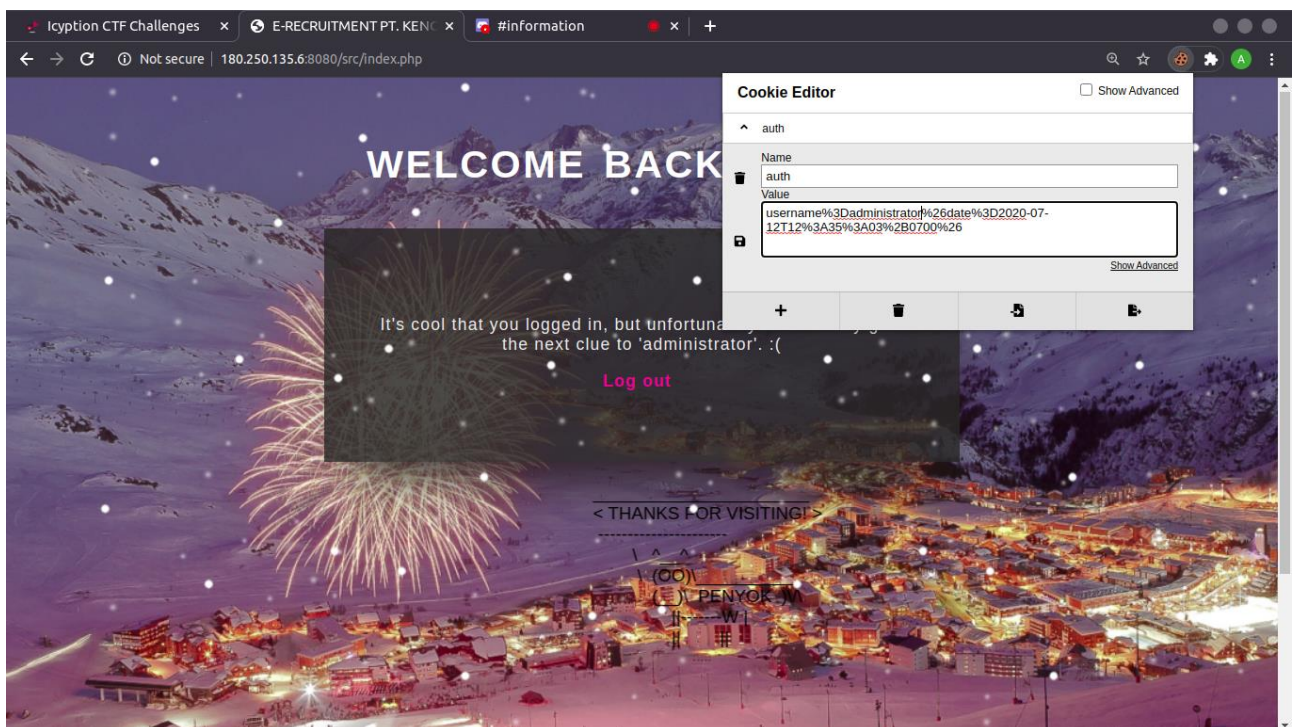
lalu saya inspect element dan ada string berupa base64 <!--

VkhKNUIHZDFaWE4wTDJkMVpYTjBDZz09Cg== --> lalu saya decode 2x dan mendapat hasilnya yaitu Try guest/guest

lalu saya login dengan username password guest

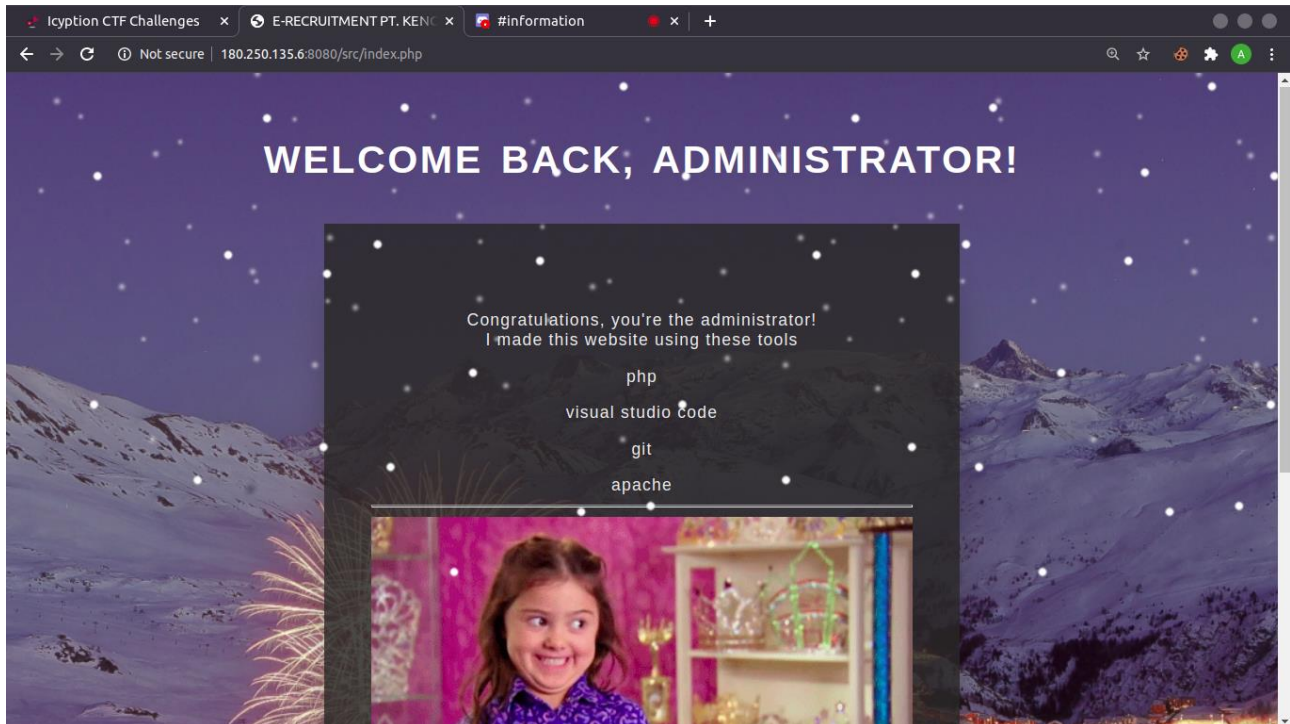
lalu berhasil login kemudian saya klik here dan mendapat clue 'administrator'

lalu saya mengubah cookie dengan cookie editor



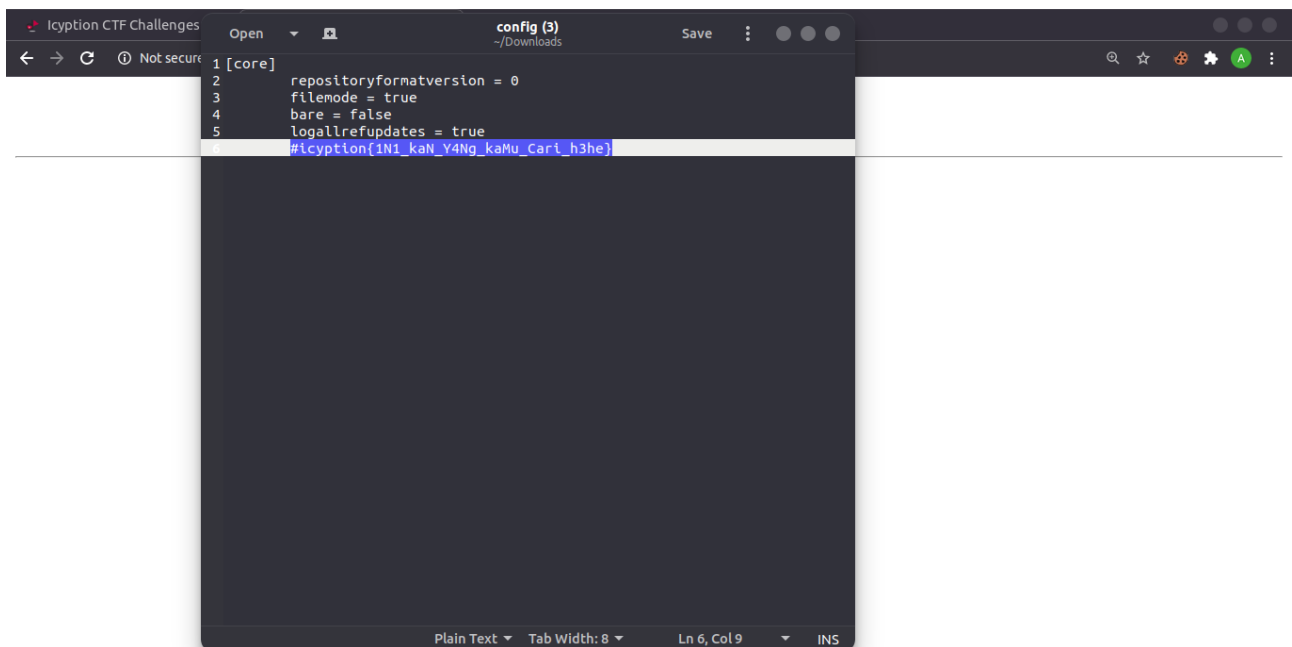
setelah itu saya save dan reload

dan berhasil masuk sebagai administrator



Lalu saya mendapat clue yaitu git saya coba melihat gitnya dengan cara <http://180.250.135.6:8080/src/.git/> lalu forbidden

kemudian saya ingin melihat isi config git nya dengan cara <http://180.250.135.6:8080/src/.git/config> dan terdownload file config nya dan disana ada flagnya yaitu :



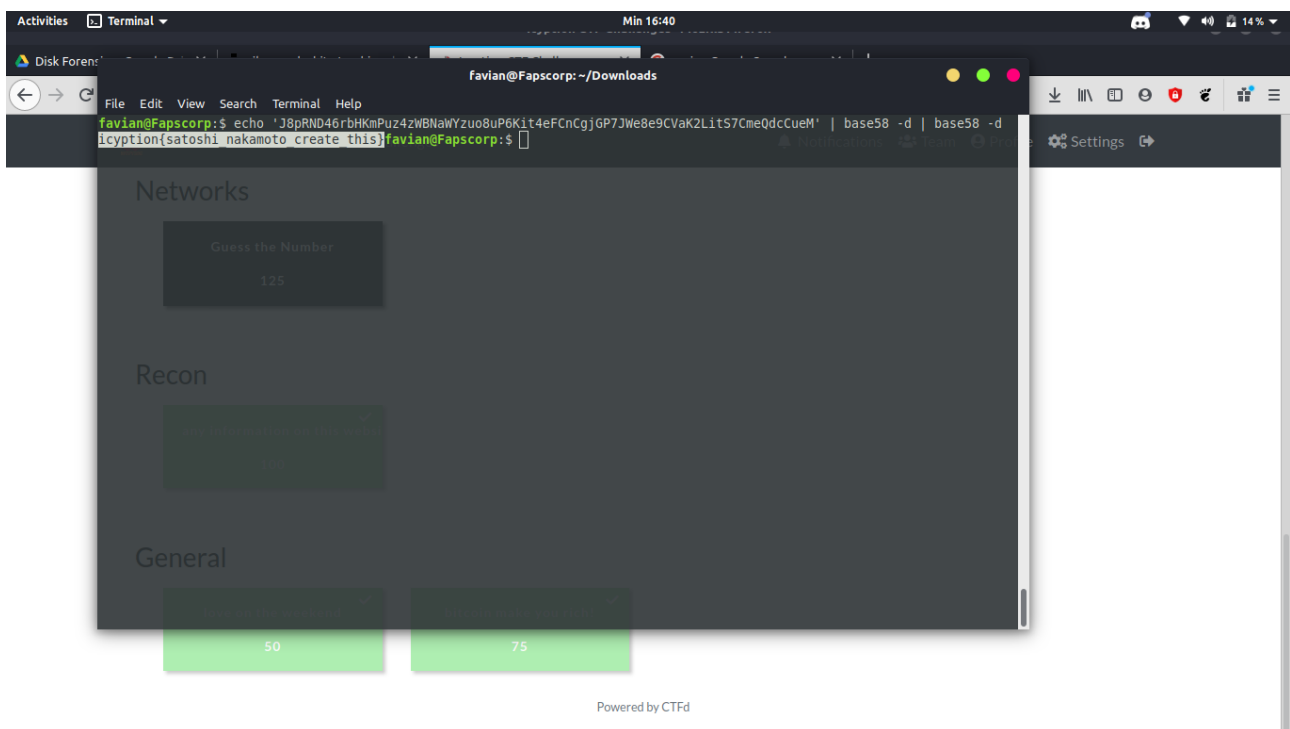
#icryption{1N1_kaN_Y4Ng_kaMu_Cari_h3he}

Bitcoin make you rich!

Menggunakan module **base58** yang diinstall dengan perintah **pip3 install base58**. Setelah itu, mendecrypt cipher text yang ada dengan perintah **base58**.

Perintahnya :

```
echo 'J8pRND46rbHKmPuz4zWBNaWYzuo8uP6Kit4eFCnCgjGP7JWe8e9CVaK2LitS7CmeQdcCueM' |  
base58 -d | base58 -d
```



Flag :

icyption{satoshi_nakamoto_create_this}

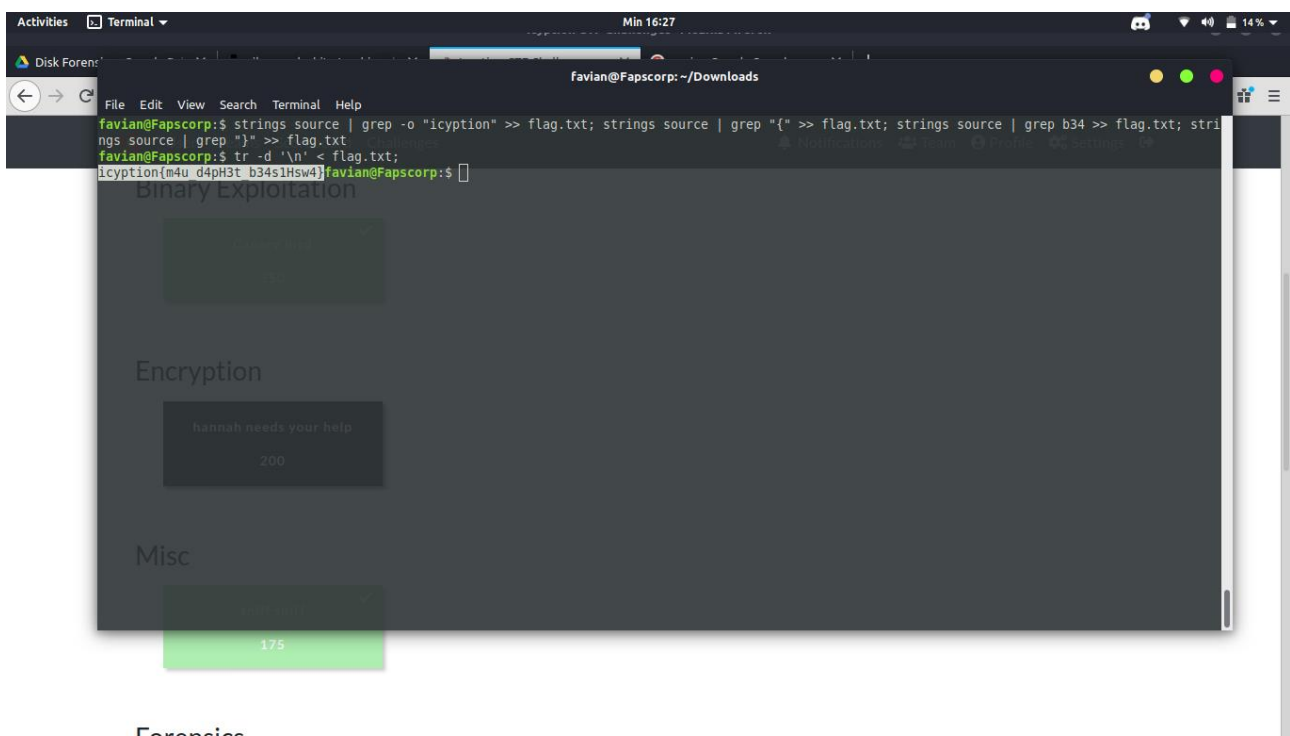
Canary bird

Mendownload filenya, lalu menggunakan perintah **strings** untuk mengambil flag yang ada. Lalu disimpan didalam file **flag.txt**. Dan terakhir kalimat yang ada pada file **flag.txt** dijadikan menjadi satu baris.

Perintahnya :

```
strings source | grep -o "icyption" >> flag.txt; strings source | grep "{" >> flag.txt; strings source |  
grep b34 >> flag.txt; strings source | grep "}" >> flag.txt
```

```
tr -d '\n' < flag.txt;
```



Flag :

icyption{m4u_d4pH3t_b34s1Hsw4}

FORENSICS (WONDERFUL PAINTING)

Download filenya, setelah didownload maka gambarnya seperti ini



Maka saya buka program **Stegsolve** dan memilih menu **Stereogram Solver** untuk mengedit offsetnya. Setelah itu saya XOR kan gambarnya agar terlihat lebih jelas tulisannya. Gambar akhir adalah ini



Tulisannya diatas “Here’s your flags icyption{S3m0g4_K4m1_M3n4ng}”

GENERAL (LOVE OF THE WEEKEND)

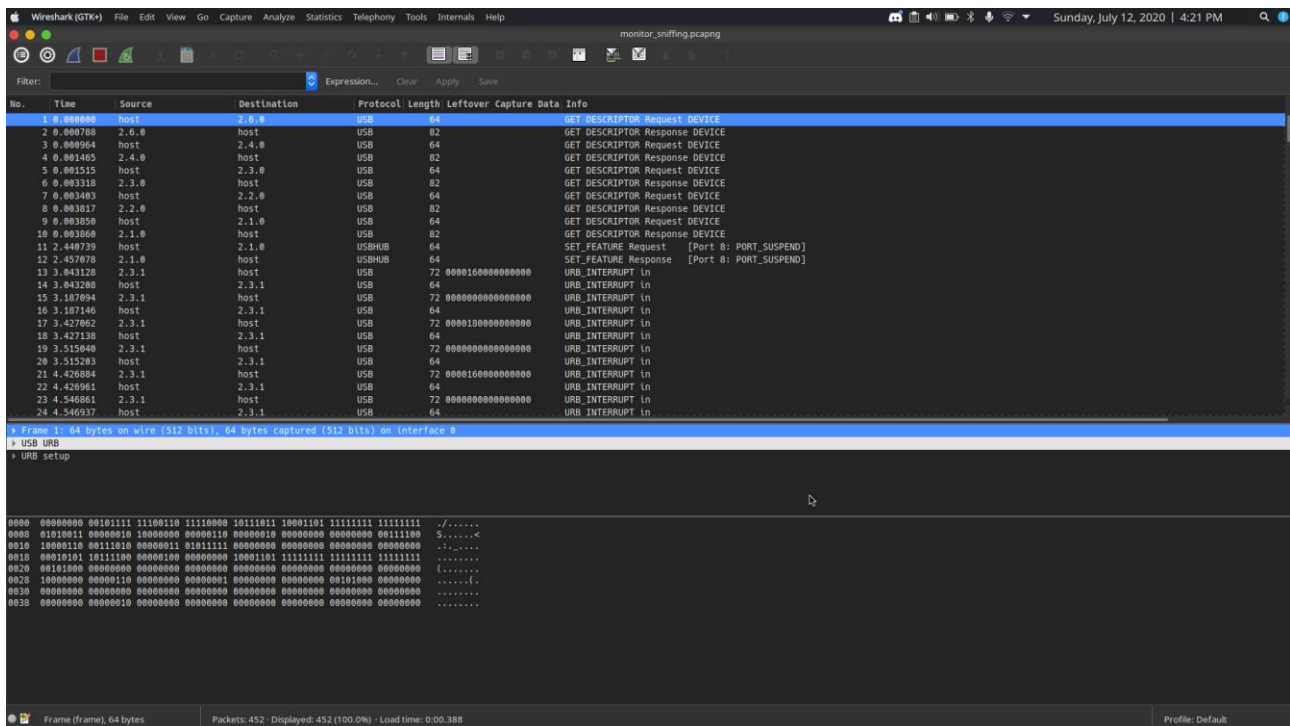
Download filenya, filenya berbentuk mp3. Saya coba exiftool dulu untuk memastikan file tersebut dan muncul seperti ini pada bagian Lyrics

```
CTF: bash — Konsole
Audio Layer      : 3
Audio Bitrate    : 320 kbps
Sample Rate      : 48000
Channel Mode     : Joint Stereo
MS Stereo        : On
Intensity Stereo : Off
Copyright Flag   : False
Original Media   : True
Emphasis         : None
ID3 Size         : 52035
Title            : John Mayer - Love on the Weekend (with)
Album            : John Mayer - Love on the Weekend (with)
Recording Time    : 2016
Encoder Settings : Lavf58.26.101
Lyrics           : It's a Friday, we finally made it.I can't believe I get to see your face.You've been working and I've been waiting.To pick you up and take you from this
                  place.Love on the weekend, love on the weekend.Like only we can, like only we can.Love on the weekend, love on the weekend.I'm coming up and I'm loving every minute of it.You be the DJ,
                  I'll be the driver.You put your feet up in the getaway car.I'm flying fast like a, a wanted man.I want you, baby, like you can't understand.Love on the weekend, love on the weekend.We f
                  ound a message in a bottle we were drinking.Love on the weekend, love on the weekend.I hate your guts 'cause I'm loving every minute of it.Oh oh oh oh-oh.I gotta leave ya, it's gonna hur
                  t me.My clothes are dirty and my friends are getting worried.Down there below us, under the clouds.Baby, take my hand and pull me down, down, down, down.And I'll be dreamin' of the next
                  time we can go.Into another serotonin overflow.Love on the weekend, love on the weekend.I'm busted up but I'm loving every minute of it.Love on the weekend.Love on the weekend.Love on the weekend.icyption[D
                  o_y0u_l1k3_J0hn_May3r}.I'm looking for a little love I'm looking for a little love, oh yeah.Love on the weekend.Love on the weekend.Love on the weekend.
Picture MIME Type : image/jpeg
Picture Type      : Other
Picture Description :
Picture           : (Binary data 39809 bytes, use -b option to extract)
Date/Time Original : 2016
Duration          : 03:34 (approx)
(base) ifzahri@ifzahri-computer:~/Documents/CTF$
```

icyption{Do_y0u_l1k3_J0hn_May3r}

MISC (SNIFF SNIFF)

Download filenya dan buka di wireshark



Setelah itu , saya melihat leftover data pada traffic, maka saya tambahkan filter ((usb.transfer_type == 0x01) && (frame.len == 72)) && !(usb.capdata == 00:00:00:00:00:00:00) pada wireshark, dan saya tambahkan juga pada terminal shark -r ~/Documents/CTF/monitor_sniffing.pcapng -Y "(usb.transfer_type == 0x01) && frame.len == 72)) && !(usb.capdata == 00:00:00:00:00:00:00)" -e "usb.capdata" -Tfields > leftover.txt

```
CTF : bash — Konsole
(base) ifzahri@ifzahri-computer:~$ cd Documents/CTF
(base) ifzahri@ifzahri-computer:~/Documents/CTF$ cat leftover.txt
0000160000000000
0000180000000000
0000160000000000
0000040000000000
00000b0000000000
00002c0000000000
00001c0000000000
0000040000000000
00002c0000000000
0000110000000000
00001c0000000000
0000040000000000
0000150000000000
```

Setelah itu diddecode textnya maka didapatkan `icyption{W1r3sh4k_n0t_only_f0r_n3tw0rks}`