

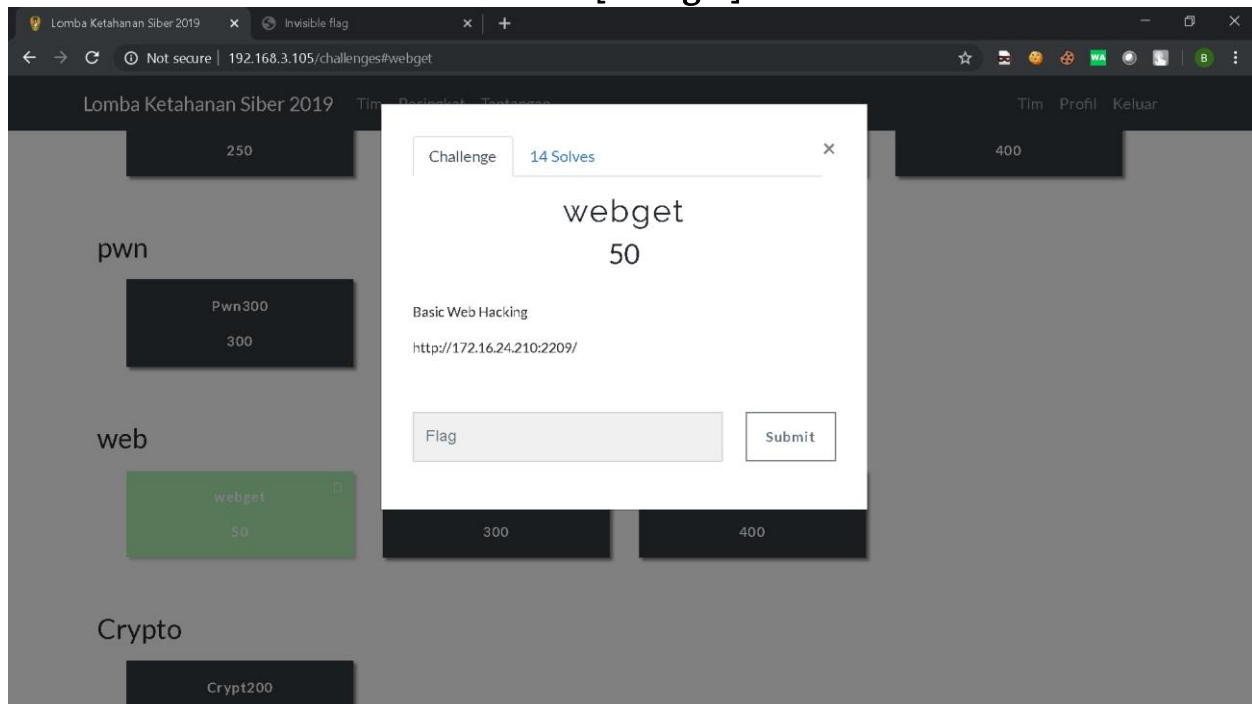


**NAMA TIM :[P.i.n.G]**

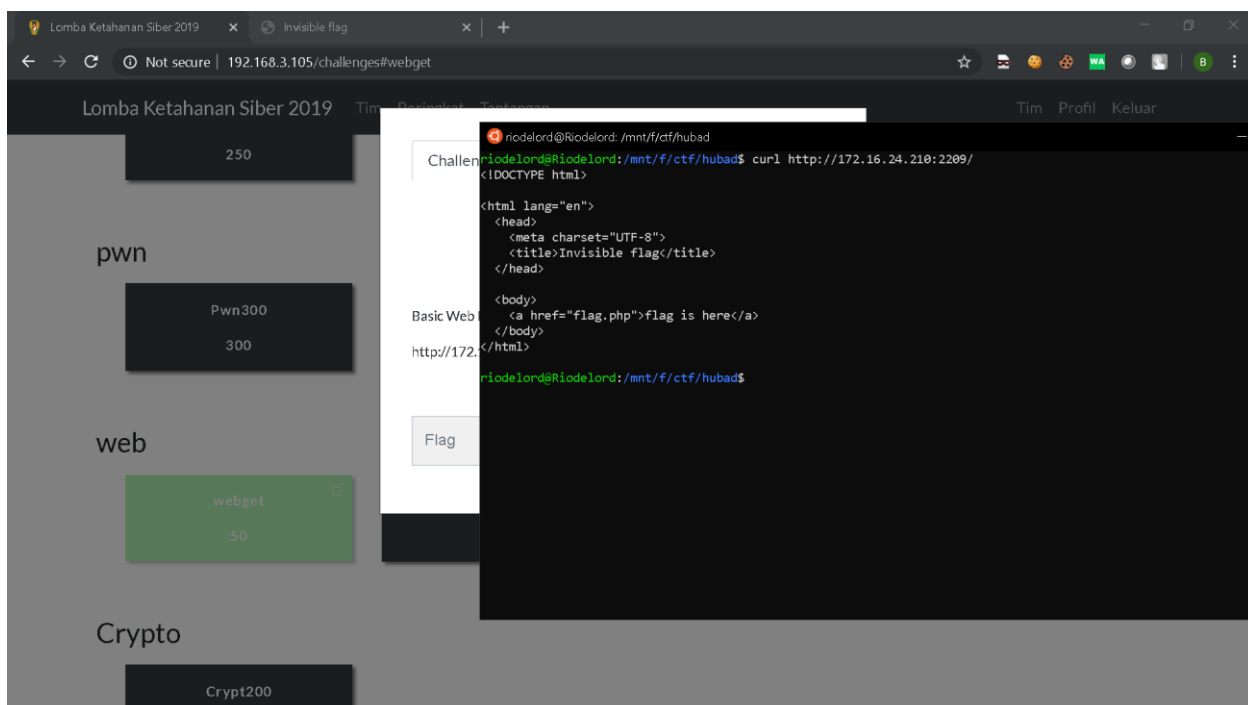
Ketua Tim	
1.	Rio Darmawan
Member	
1.	Fariq Fadillah Gusti Insani
2.	Ahmad Fauzzan Maghribi
3.	
4.	



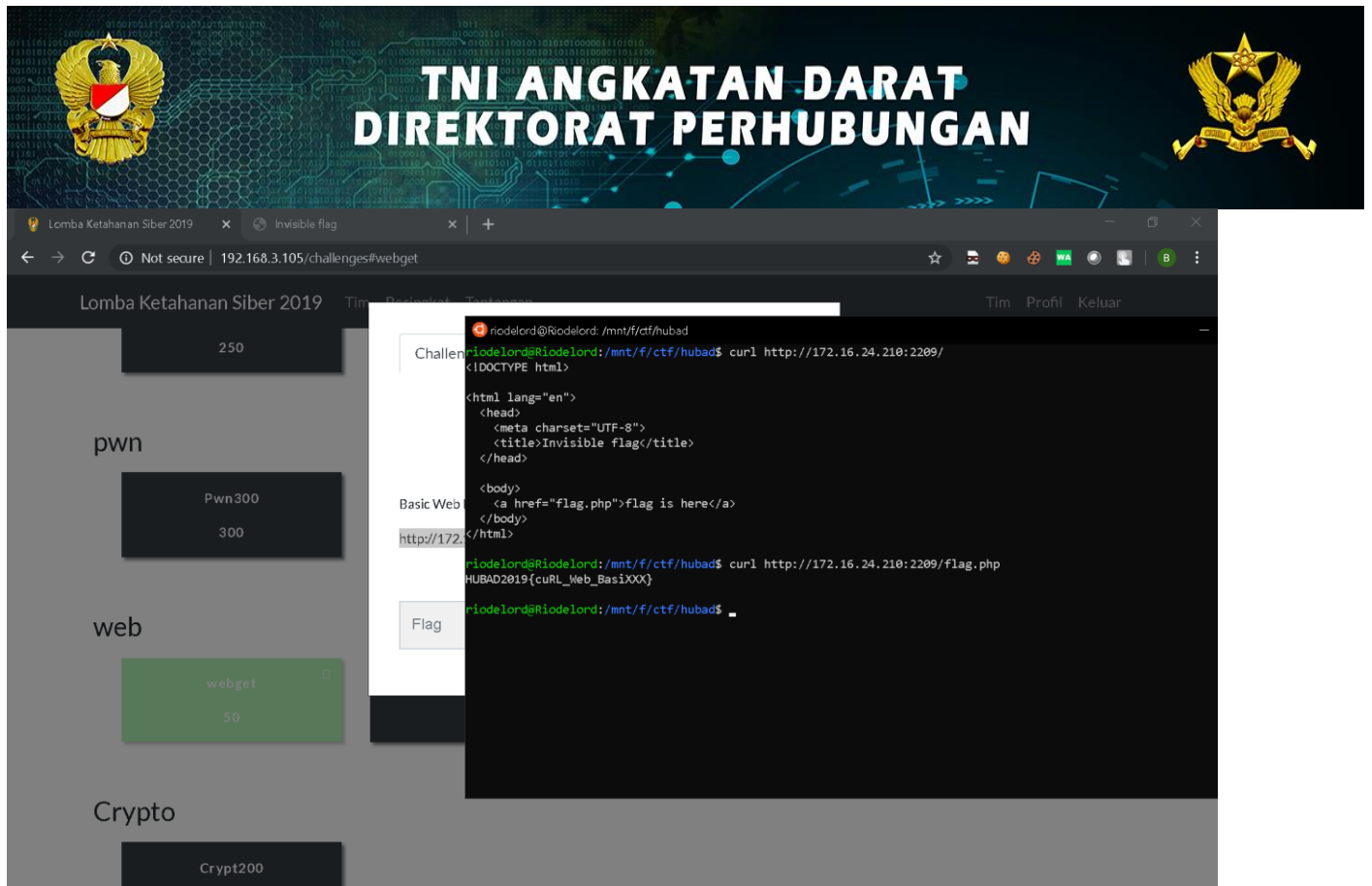
## [Webget]



Diberikan sebuah url yang bila mana dibuka di browser tidak muncul tampilan apapun.. lalu dicoba menggunakan curl munculah source code web tersebut



Lalu curl <http://172.16.24.210:2209/flag.php> dan munculah flagnya

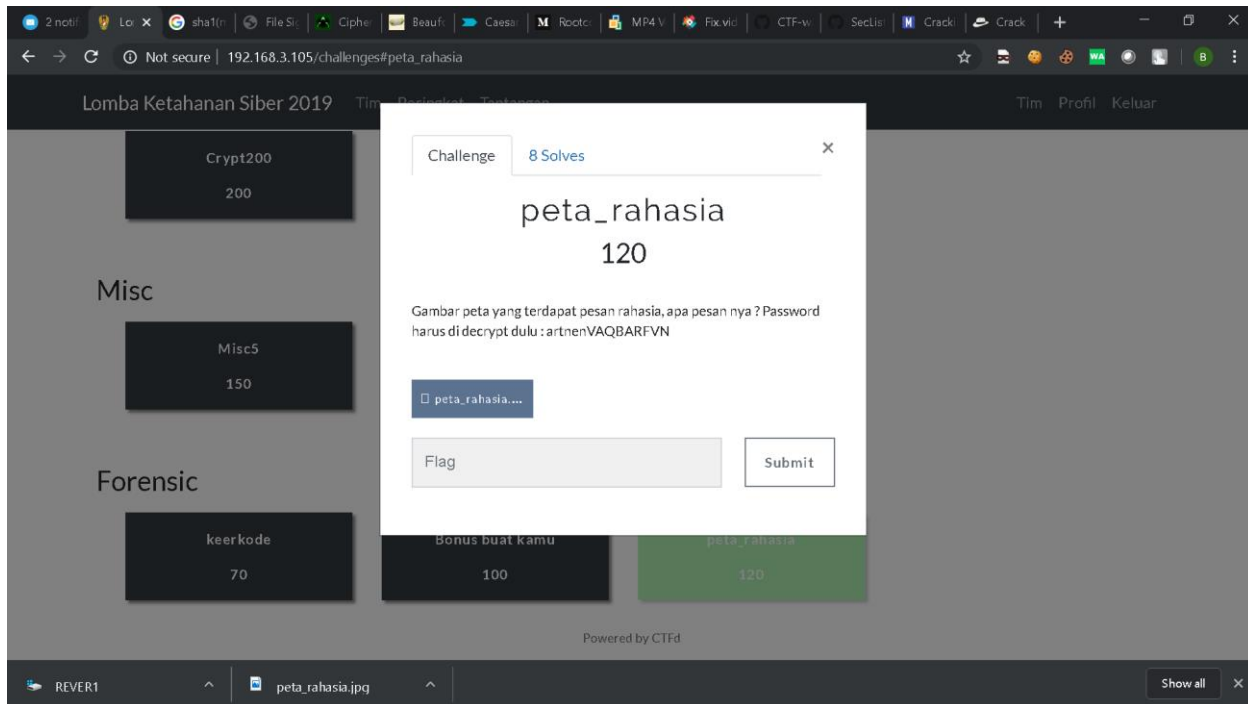


Flag: **HUBAD2019{cuRL\_Web\_BasiXXX}**

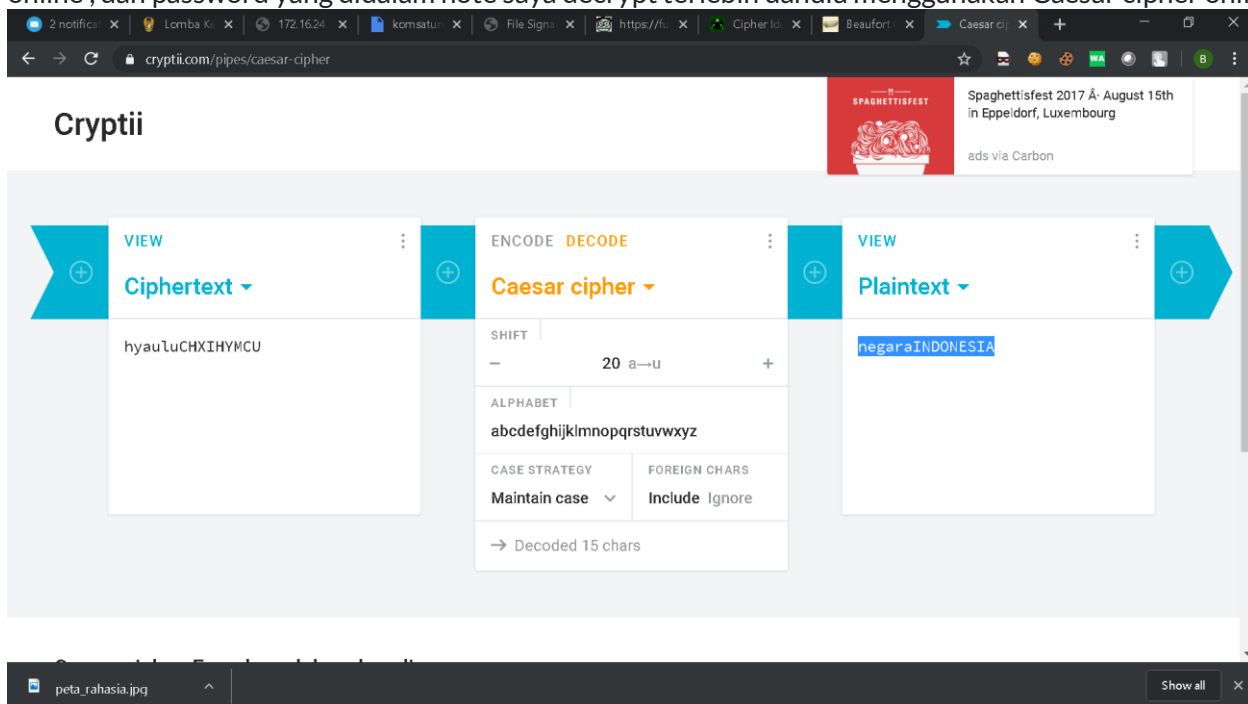


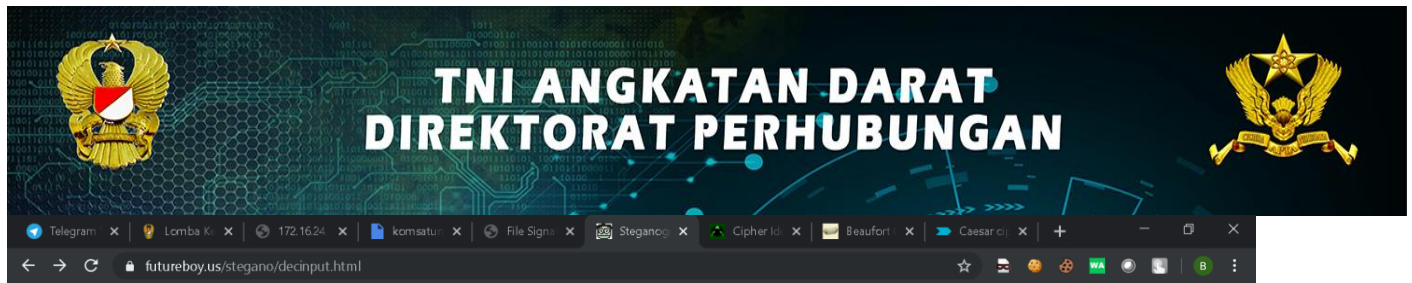
## [Peta Rahasia]

Note : Gambar peta yang terdapat pesan rahasia, apa pesan nya ? Password harus di decrypt dulu : artnenVAQBARFVN



Pertama saya bisa langsung menebak ini adalah stegano , langsung saja saya menggunakan tools steghide online , dan password yang didalam note saya decrypt terlebih dahulu menggunakan Caesar cipher online





## Steganographic Decoder

This form decodes the payload that was hidden in a JPEG image or a WAV or AU audio file using the [encoder form](#). When you submit, you will be asked to save the resulting payload file to disk. This form may also help you guess at what the payload is and its file type...

Select a JPEG, WAV, or AU file to decode:

Choose File | peta\_rahasia.jpg

Password (may be blank):

negaraINDONESIA

- ☒ View raw output as MIME-type   
☐ Guess the payload  
☐ Prompt to save (you must guess the file type yourself.)

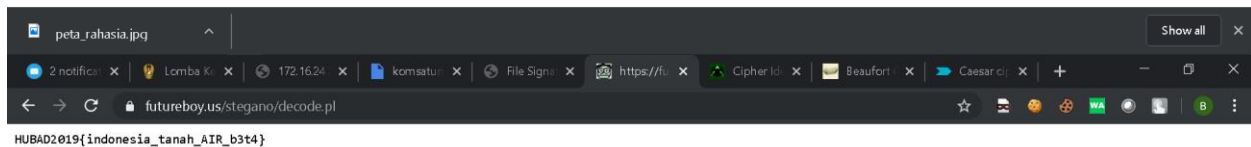
Submit

To use this form, you must first [encode a file](#).

These pages use the [steghide](#) program to perform steganography, and the files generated are fully compatible with steghide.

Please send comments or questions to [Alan Eliassen](#).

[Back to Alan's Home Server](#)

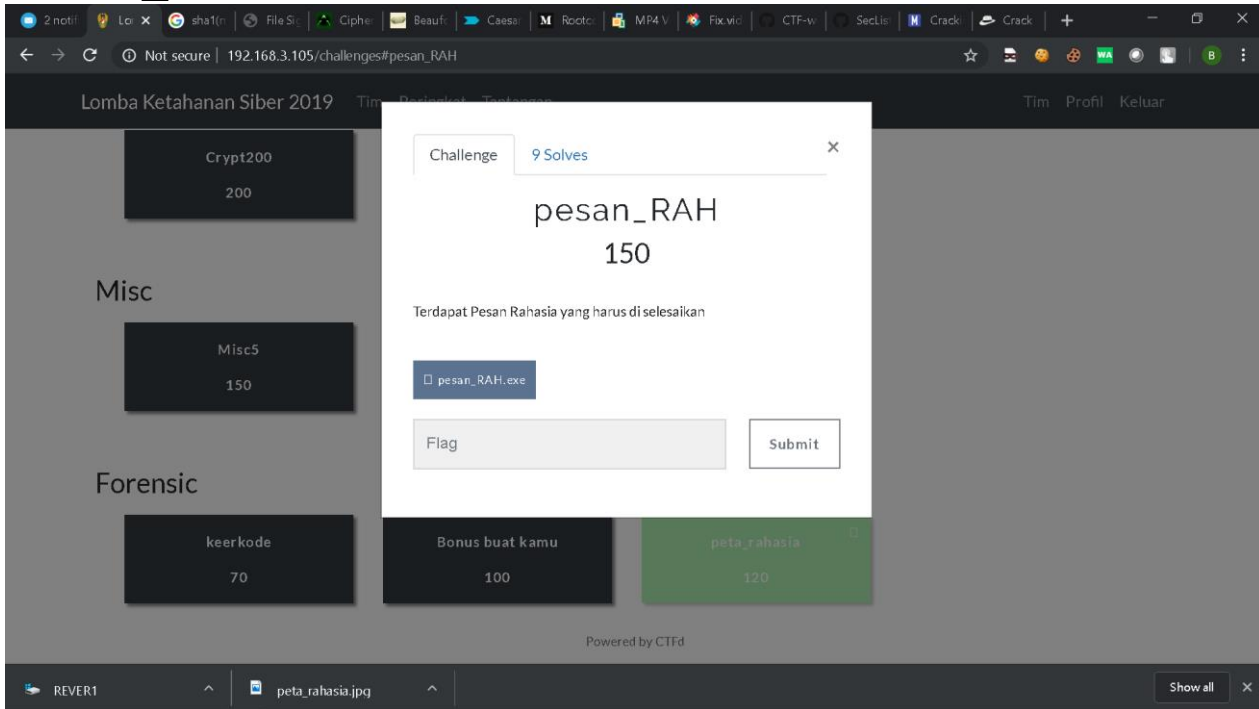


Flag : HUBAD2019{indonesia\_tanah\_AIR\_b3t4}

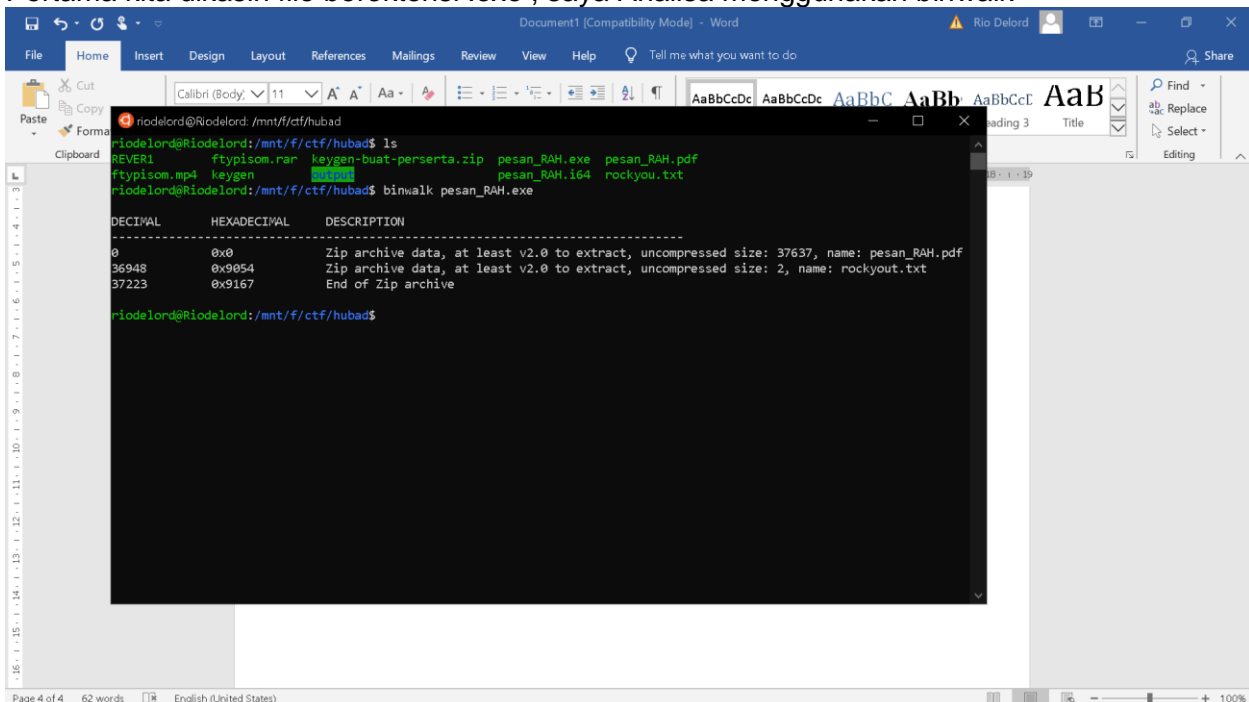


[pesan\_RAHAH]

## Pesan\_RAHAH




Pertama kita dikasih file berektensi .exe , saya Analisa menggunakan binwalk





[illegible]

file:///F:/CTF/HUBAD/pesan\_RAHA.pdf

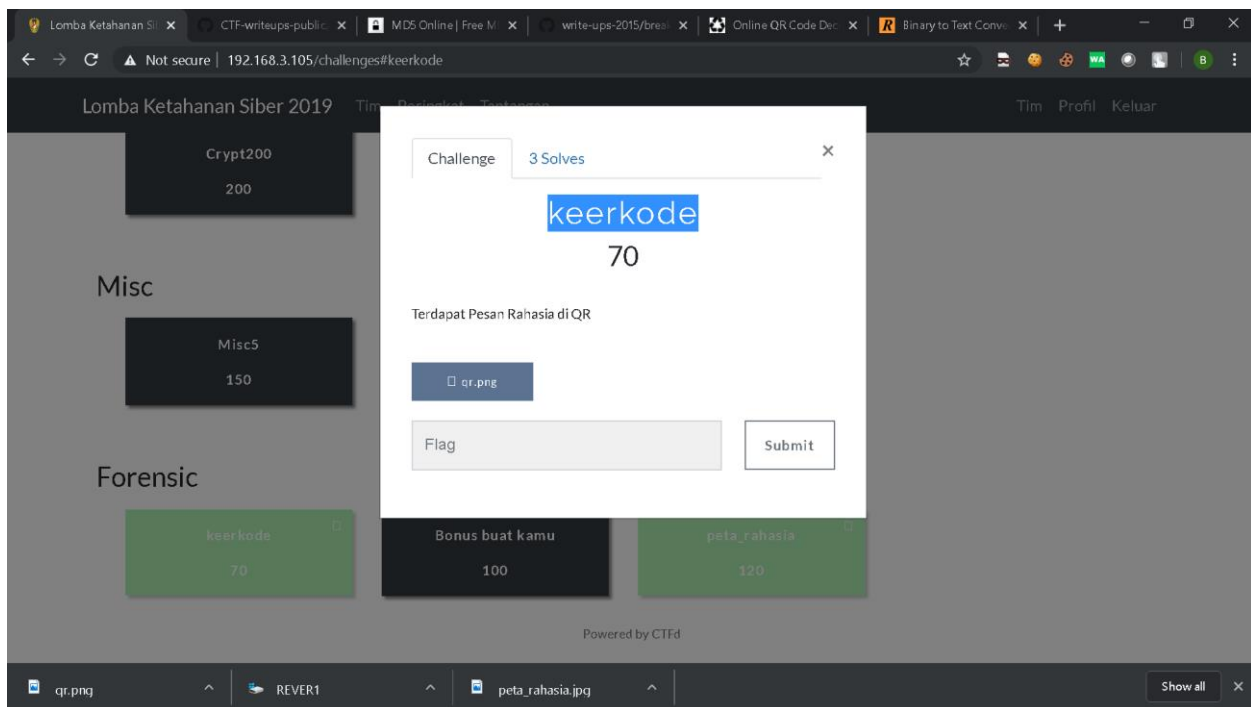


HUBAD2019{BENDERA\_MERAH\_PUTIH!!!!}

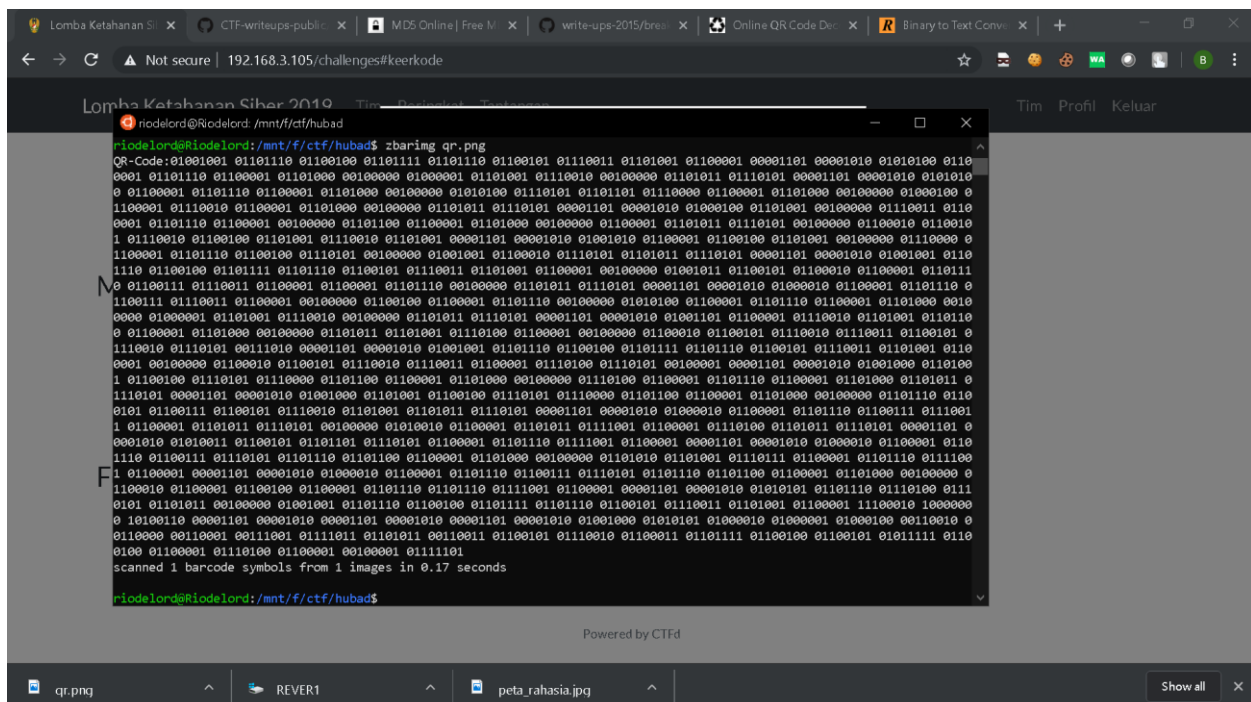
Flag: HUBAD2019{BENDERA\_MERAH\_PUTIH!!!!}



[keer\_Kode]



Kita diberikan file qr.png yang rusak dan tidak bisa di scan. Saya sudah bisa menebak ini bisa diselesaikan menggunakan zbarimg .. langsung saja saya decrypt menggunakan zbarimg



Dan didapatkan sebuah binary code .. langsung saya convert binary ke text .. dan didapatkan hasilnya





berserta flag

rapidtables.com/convert/number/binary-to-ascii.html

Paste binary numbers (e.g. 01000101 01111000 ...) or drop file:

```
01110011 01101001 01100001 11100010 10000000 10100110 00001101
00001010 00001101 00001010 00001101 00001010 01001000 01010101
01000010 01000001 01000100 00110010 00110000 00110001 00111001
01111011 01101011 00110011 01100101 01110010 01100011 01101111
01100100 01100101 01011111 01100100 01100001 01110100 01100001
00100001 01111101
```

Character encoding: ASCII

Convert Reset Swap

BangunLah jiwaanya  
BangunLah badannya  
Untuk Indonesia!}

HUBAD2019{k3rcode\_data!}

Copy Save

Text to binary converter

City Index 70  
Plus500 45  
IG 38  
CMC 37  
FXCM 30

PAY LOWER BITCOIN SPREADS

Spread as of May 27, 2019  
Losses can exceed your deposited funds.

FXCM

NUMBER CONVERSION

- ASCII,Hex,Binary,Decimal converter
- ASCII text to binary converter
- ASCII text to hex converter

This website uses cookies to improve your experience, analyze traffic and display ads. [Learn more](#)

OK

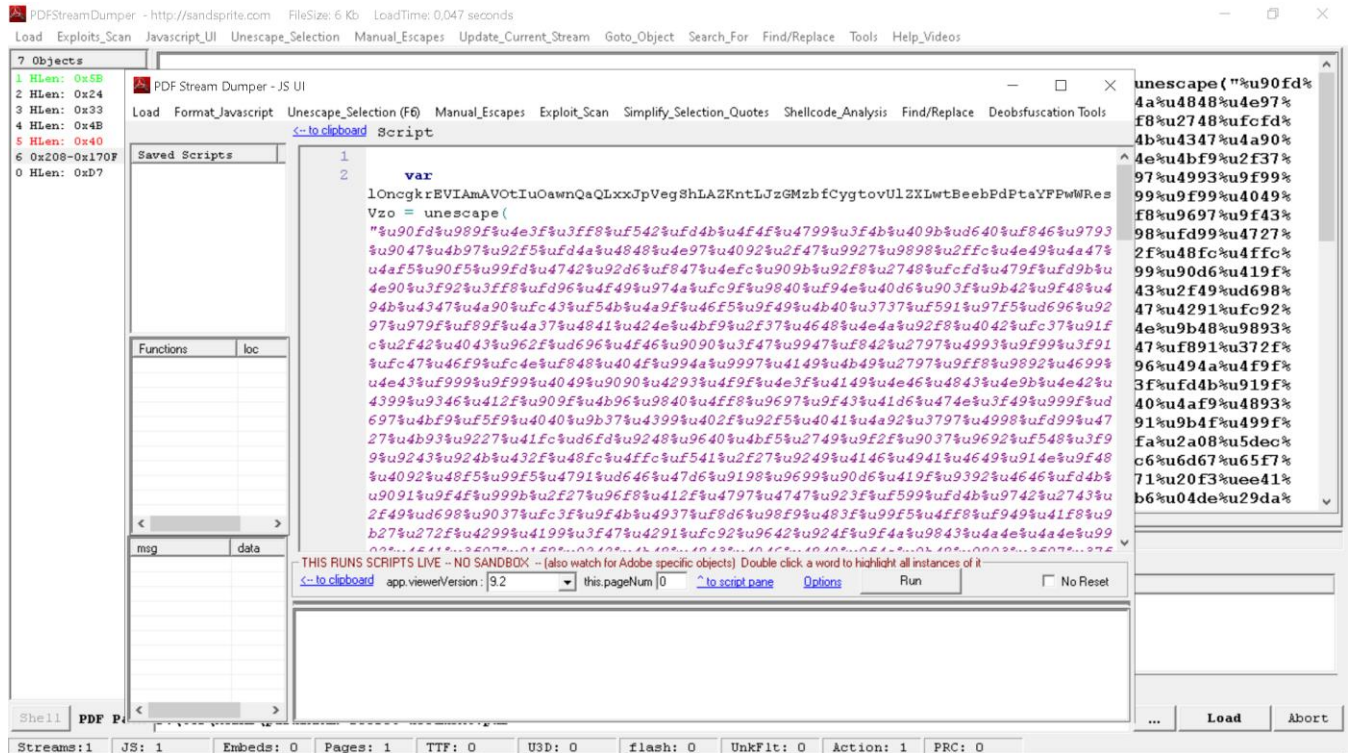
qr.png REVER1 peta\_rahasia.jpg Show all

Flag : HUBAD2019{k3rcode\_data!}

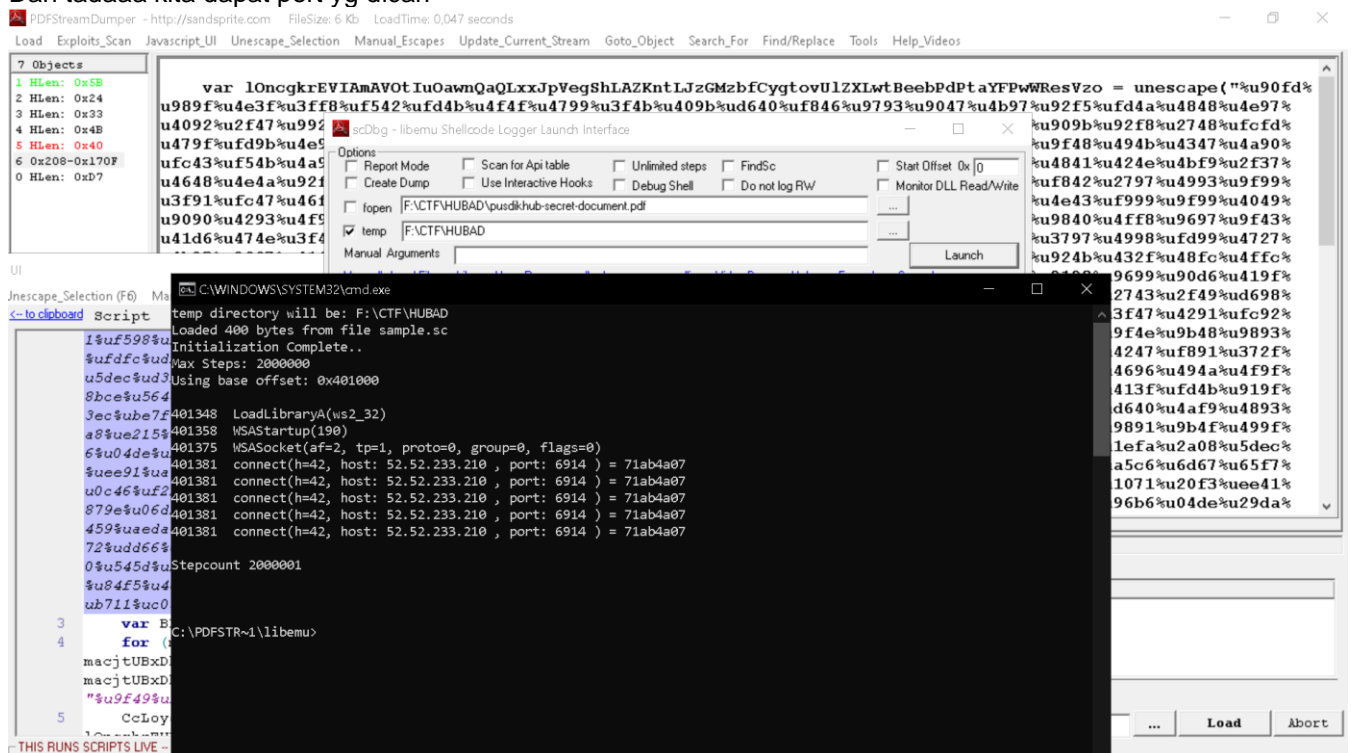




Kita bisa mulai dengan memeriksa apakah ada exploit yang terdeteksi oleh alat menggunakan menu "Exploit Scan"



Lalu lanjut ke menu shellcode\_analysis > scDbg (libemu-emulation) > lalu muncul popup baru > click launch Dan tadaaa kita dapat port yg dicari



Flag : HUBAD2019{52.52.233.210:6914}