Write up

**Challenge : tiga-step-aja**

Desc :

YjMyIC0+IDN4IA==

JJFEYRKLKZFUQS2OIZKTMU2TLJFUMRCUIVLVGTKLJZEFMTKXJNEESTK2IRDVCU2PJRDESVKPKZNFMSSSJBKTEVCTKZFU4QKUJNKEGUCKGVFEIRKWGJMEURSDIU2FIS2XJM2UYVKLJZFU2SKKJBLEGVKLJBDUUTKVLFKEGTSJLJGUKT2RLJKEWSSBKU2FMU2UJM2DERCFKZBUGSSWJJDEWVJSIJDU4Q2FJVKEWS2LKZGFMQ2TJNCUUNKIIVGVMU2YI5FE2VKZKZFUOTCFGZKDEUCKGVEFKNSRHU6T2PI=

Emuqzcxm kbh xmv? jmur, uvk nynsvai : Sbdmubl2019{Z1oqp\_NbE\_Xghm}

Solusi :

Pada baris pertama kita decode dengan base64 hasilnya “b32 -> 3x”. Mungkin itu sebuah clue untuk mengdecode barus selanjutnya menggunakan base32 sebanyak 3 kali. Setelah melakukan decode menggunakan base32 sebanyak 3 kali kita akan mendapatkan “MICINN merupakan kunci untuk membuat makanan menjadi lebih nikmat.”. Disini kita dapat petunjuk bahwa kata MICINN merupakan salah satu kunci untuk mendecode flagnya. Maka dari itu kami menggunakan vigenere chipher karena pada vinegere chipher memerlukan key untuk menencode atau mendecode sesuatu. Masukan key yang sudah didapat dari clue sebelumnya yaitu MICINN maka hasilnya “Sesimple itu kan? Ini flagnya : Foresty2019{M1cin\_FoR\_Lyfe}.”

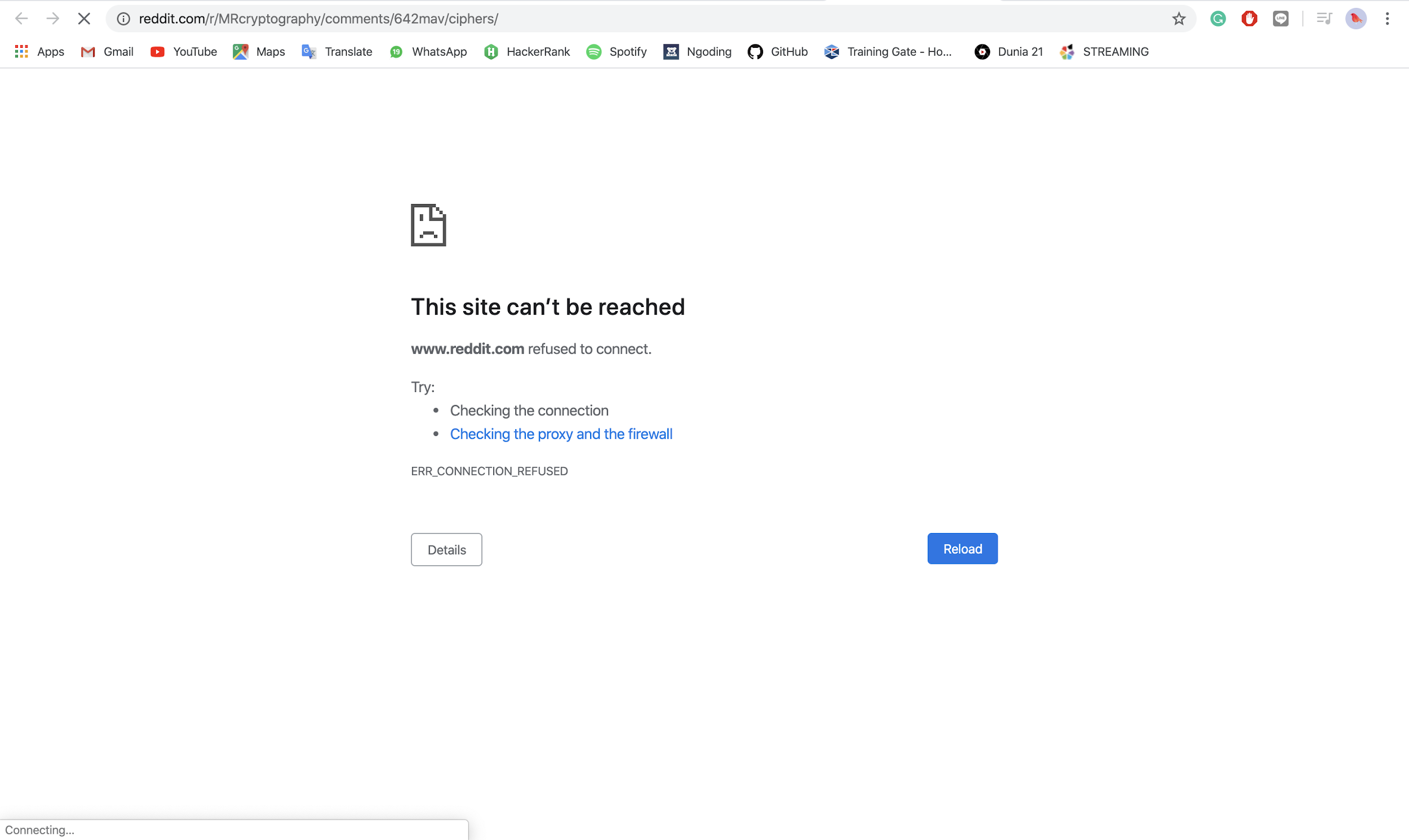
**Challenge: selamat-datang-crypto**

Desc: Saya mendapatkan sebuah cipher dari suatu tempat u@C6DEJa\_`hLrCJ!E\_:$7F?N bisa tolong pecahkan?

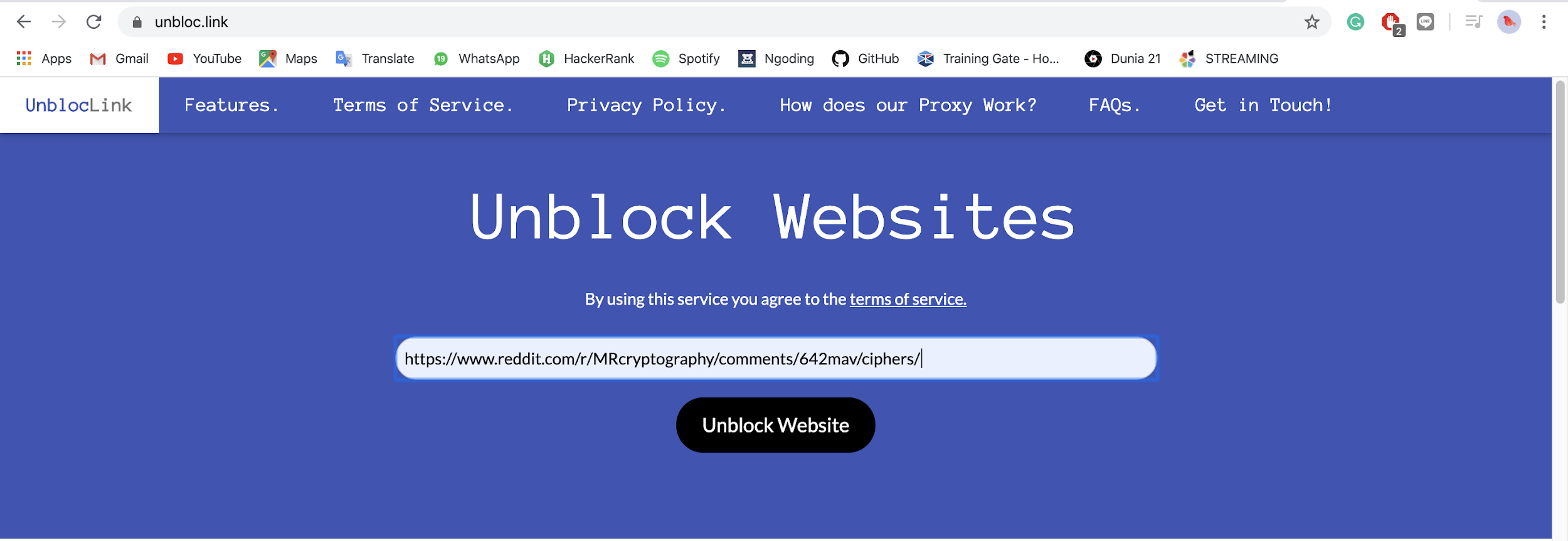
hint: <https://www.reddit.com/r/MRcryptography/comments/642mav/ciphers/>

Solusi:

Link tersebut sudah terblockir di Indonesia.



Untuk masuk kedalam link tersebut kita menggunakan <https://unbloc.link/>.

Setelah masuk kedalam link yang ada di hint, kita akan menjumpai beberapa link web yang bisa decode maupun encode suatu kode. Setelah mencoba beberapa web, akhirnya kami menemukan web yang cocok untuk melakukan decode yaitu [http://www.just-stuart.com/cgi-bin/ur13](https://unbloc.link/index.php?q=ytakoJ-SY9irrl6fqKukYKqlrJKk1l6b06CTxJvMjsbL0F-l15Rn). Setelah melakukan decode diweb tersebut (ROT 47) hasilnya “Foresty2019{CryPt0iSfun}”.

**Challenge: Request Me !!**Description: Web lain ternyata terindikasi mencurigakan, apakah anda dapat mengidentifikasinya ?? 13.76.181.86:9300

Solusi:

Ketika kita buka page tersebut, terdapat sebuah kolom untuk men-submit sebuah kalimat, di kolom tersebut kita harus memasukkan sebuah kalimat yang terdiri dari 17 karakter. Pertama kita coba buka page source web tersebut, kemudian terdapat sebuah potongan kode yang terlihat mencurigakan. Kita coba mengambil setiap karakter yang terdapat di tanda kutip tersebut dan akan membentuk : ??G4lf\_Hal4d2\_In1 , ketika kita balikan kode tersebut dan menjadi 1nI\_@d4laH\_fl4G?? Dan kemudian mensubmit kode tersebut ke halaman tadi, setelah memasukkan kode akan muncul flagnya yaitu Foresty2019{0v33R\_th1nkIng\_m@y\_k1lL\_U}

**Challenge: Chookies choco chips ^\_^**Description: Cookies kue cokelat manis ~~~ 13.76.181.86:9400

Solusi:

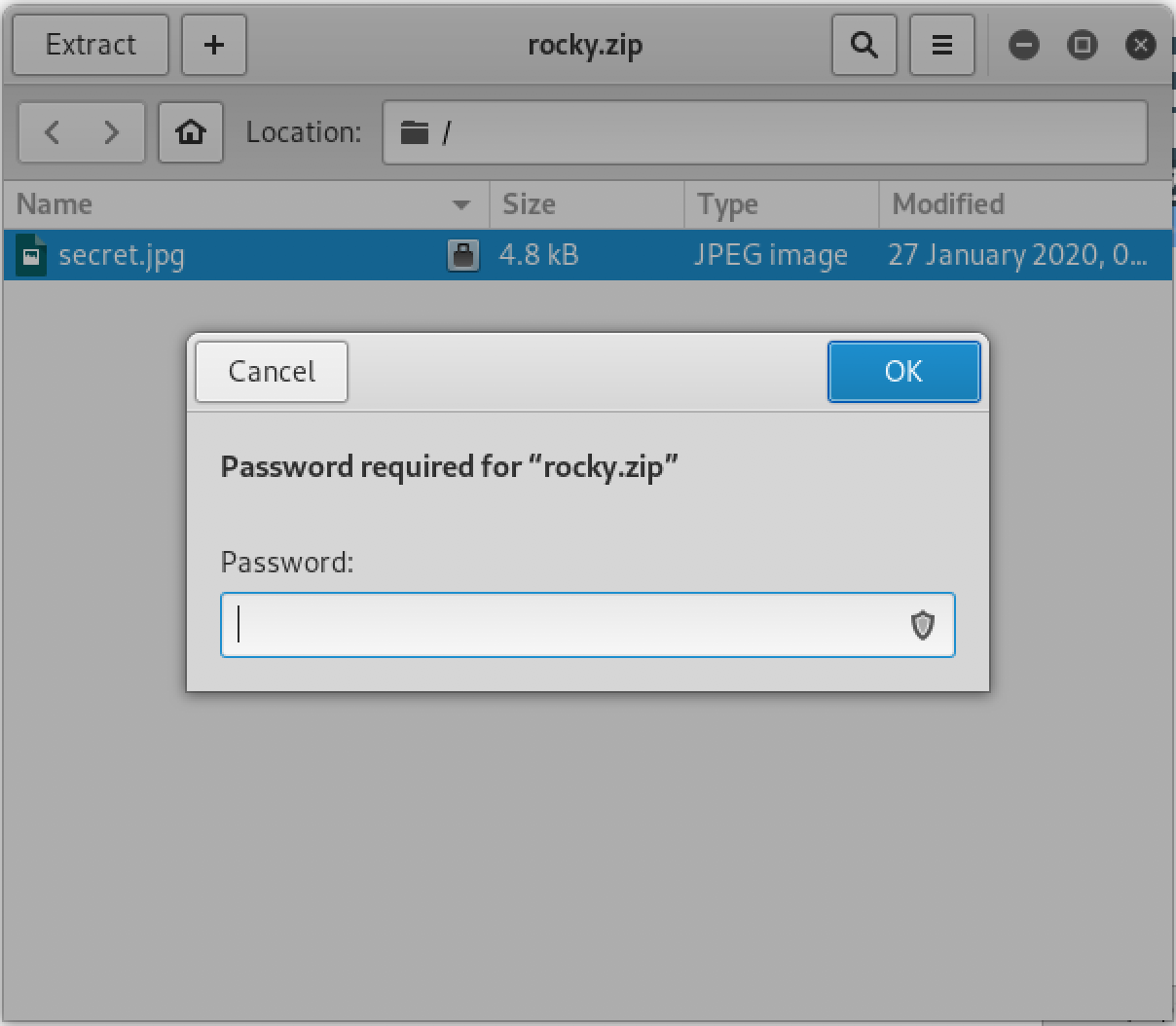
Pada halaman tersebut hanya terdapat gambar, maka kita bisa mengecek page source, setelah dicek source pagenya tidak terdapat sebuah hal yang aneh, kemudian kita bisa menginspect halaman tersebut dan melihat ada sesuatu hal pada cookies tersebut (Storage -> Cookies) terdapat Foresty2019%7Bc00kiEs\_1s\_Imp0rt%40n7%7D dan terdapat juga hal yang bernama path ‘/’ yang menunjukkan kita harus pergi ke path tersebut maka akses  
<http://13.76.181.86:9400/Foresty2019%7Bc00kiEs_1s_Imp0rt%40n7%7D> setelah itu kita inspect elemen lagi dan ke tab Network, kemudian terdapat Flag yaitu Foresty2019{c00kiEs\_1s\_Imp0rt@n7}

**Challenge: John & Rock**Description: John baru saja mengambil file zip rahasia milik temannya yang berasal dari china, akan tetapi terdapat password pada file zip tersebut, sehingga john kesulitan untuk melihat isi dari file tersebut, bisakah kamu membantu john untuk memecahkan masalah tersebut?

File: [rocky.zip](https://foresty.retas.id/files/fce76dec4da8e92c9a1215e2f3f14a5c/rocky.zip?token=eyJ1c2VyX2lkIjoxNCwidGVhbV9pZCI6MTAsImZpbGVfaWQiOjF9.XjLyRg.SSVelpxFv6DDSAqOF7Q3-0XNbhs)

Solusi:

Ketika mencoba untuk mengextract rocky.zip kita membutuhkan password, untuk



membuka zip tersebut kita bisa menggunakan john the ripper, pertama ketik   
zip2john rocky.zip > nama\_file.txt dan kemudian ketik john --format=zip nama\_file.txt

Tunggu hingga selesai, kemudian akan mendapatkan password dari rocky.zip tersebut yaitu “chinese”, kemudian buka file tersebut dan buka gambar, gambar tersebut bisa dipecahkan menggunakan chinese code <https://www.dcode.fr/chinese-code>. Setelah didecode maka flag akan didapat yaitu Foresty2019{JHONYL3BAYY}.

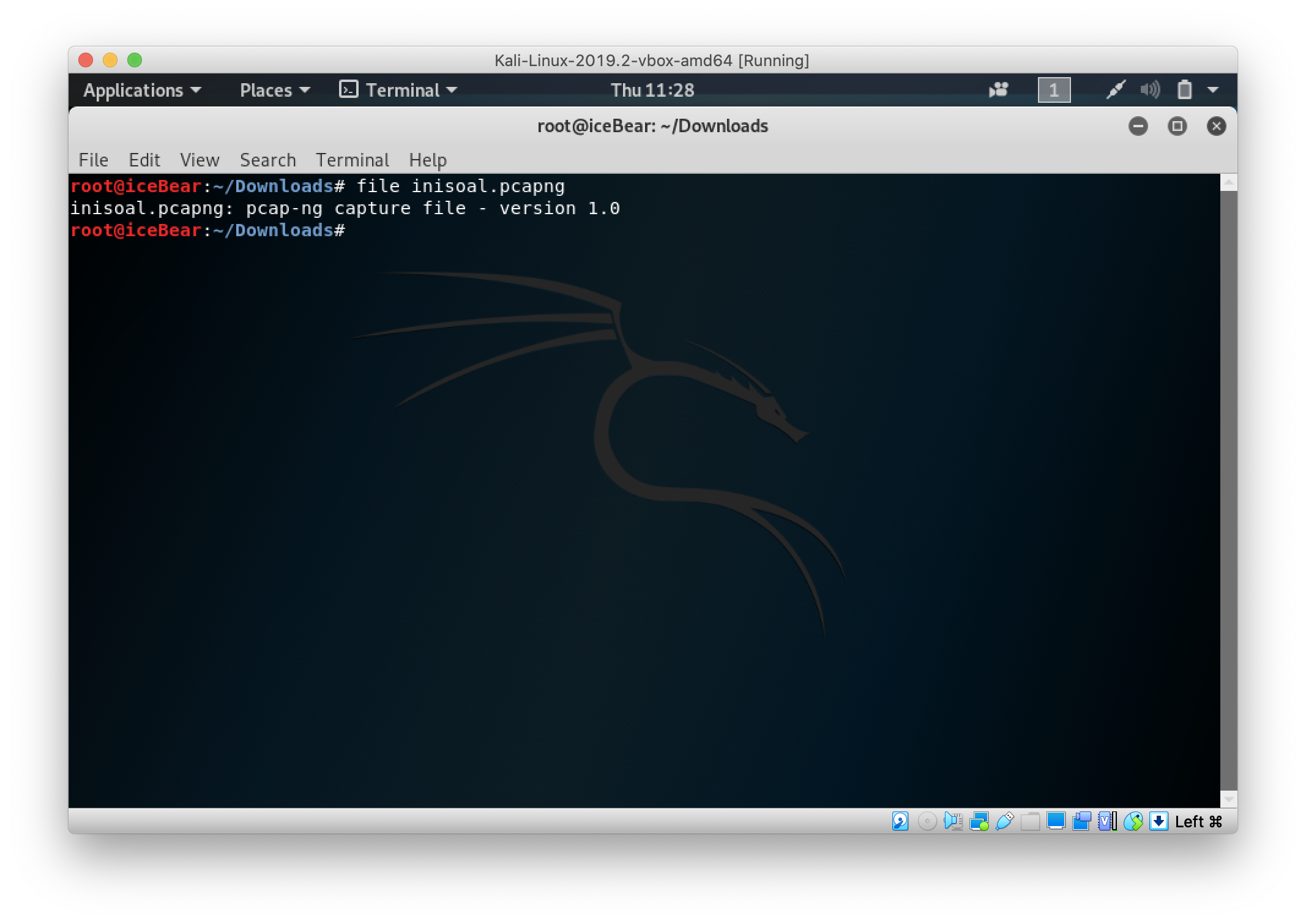
**Challenge : Mamang post**

Desc : Seorang penjaga post melakukan akses ke suatu website.

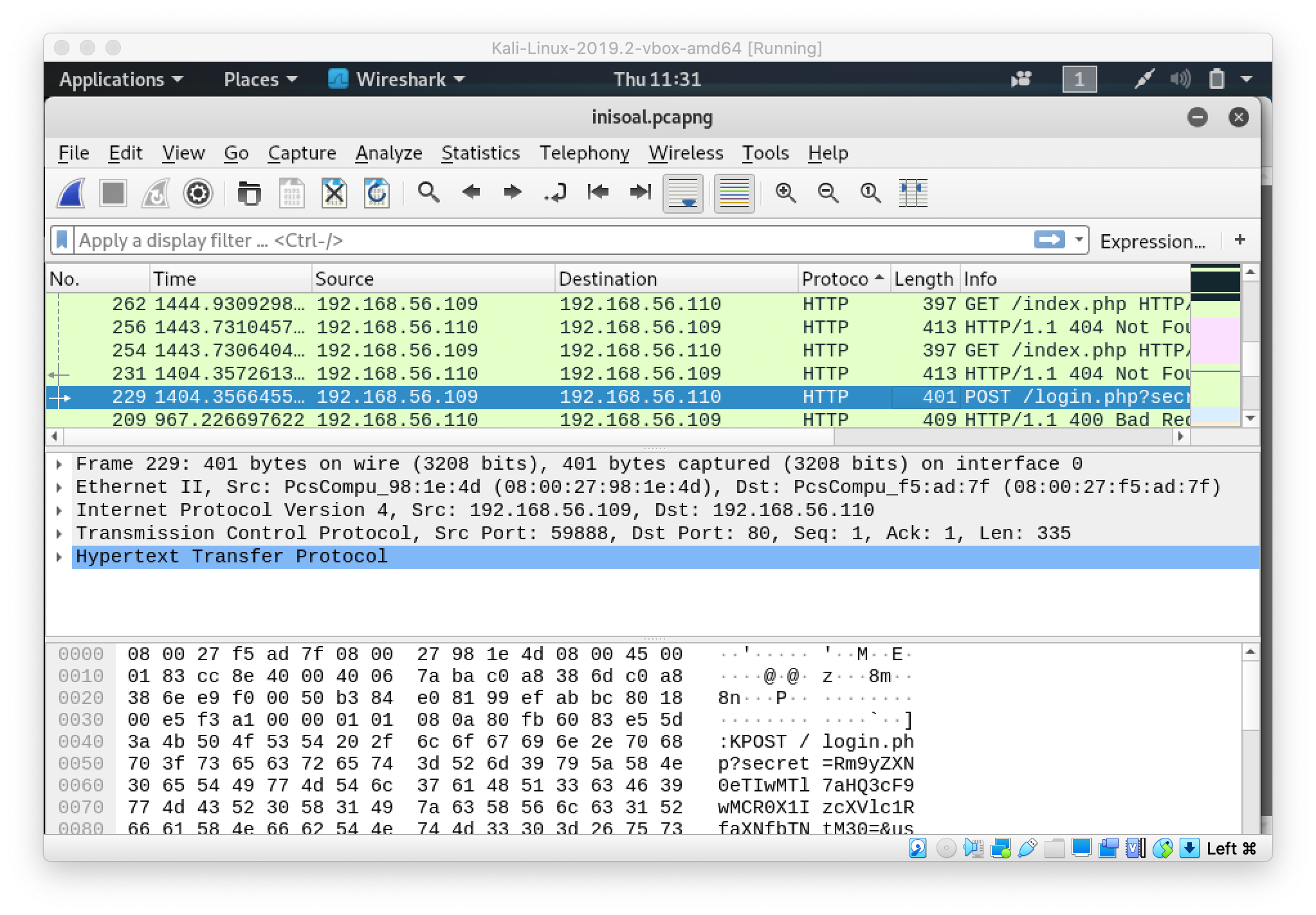
File : [inisoal.pcapng](https://foresty.retas.id/files/4e631693dfad42944bddb5db11012a23/inisoal.pcapng?token=eyJ1c2VyX2lkIjoxNCwidGVhbV9pZCI6MTAsImZpbGVfaWQiOjJ9.XjL1Dg.Cppaj__Lx0nrgmzHIt3MBlVcfC0)

Solusi :

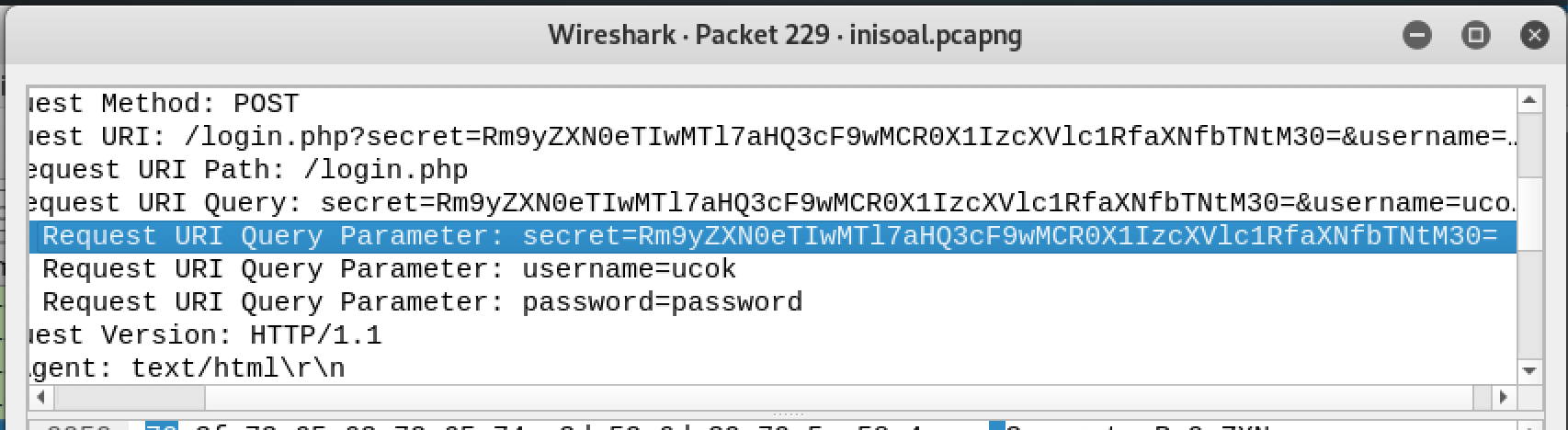
Terdapat file yang harus di download dalam challenge ini hal yang pertama dilakukan adalah mengece file tersebut apakah file tersebut berekstensi .pcapng atau yang lainya. Untuk melakukan pengecekan kita buka terminal lalu kita ketik file inisoal.pcapng.



Setelah di cek ternyata filenya memang berbentuk .pcapng. Lalu saya menggunakan wireshark untuk melihat apa isi dari file dengan cara mengetikan di terminal wireshark inisoal.pcapng. Sesuai dengan desc maka kita membuka Protoco HTTP dan memiliki info POST.



setelah dibuka disana memiliki pesan mencurigakan di variabel secret yaitu Rm9yZXN0eTIwMTl7aHQ3cF9wMCR0X1IzcXVlc1RfaXNfbTNtM30=.



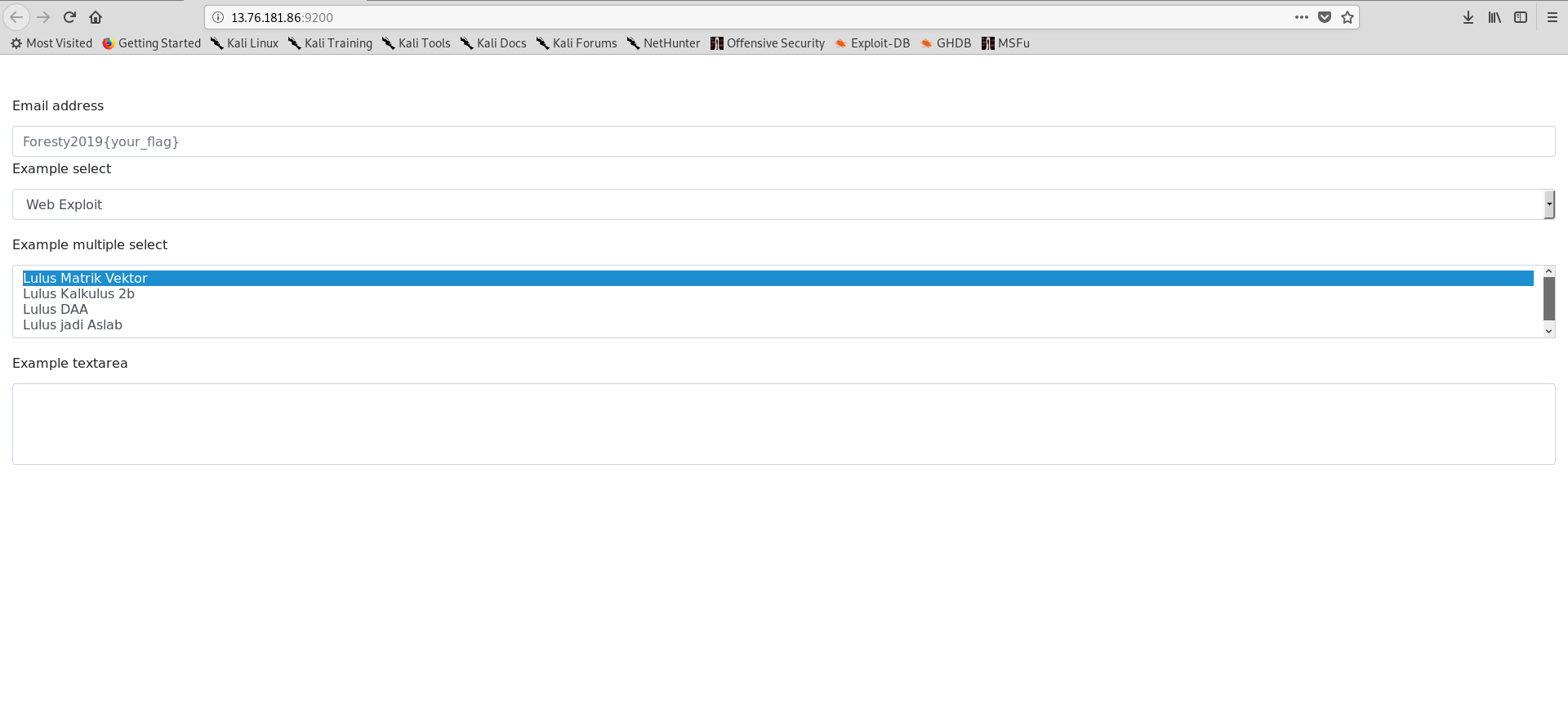
Karena kami mencurigai bahwa pesan tersebut merupakan flag yang di encode maka kami melakukan decode base64 dan didapat Foresty2019{ht7p\_p0$t\_R3quesT\_is\_m3m3}.

**Challenge: Ngoding Web Skuy**

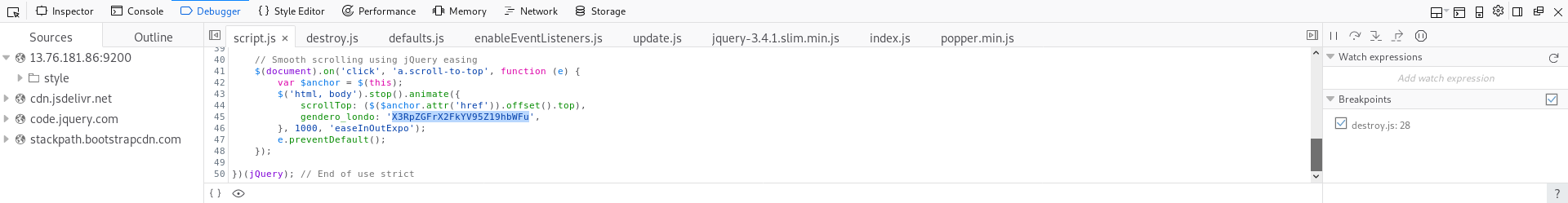
Description : Web ini memiliki beberapa pesan tersembunyi didalamnya, bisakah anda menebaknya ?? 13.76.181.86:9200

Solusi :

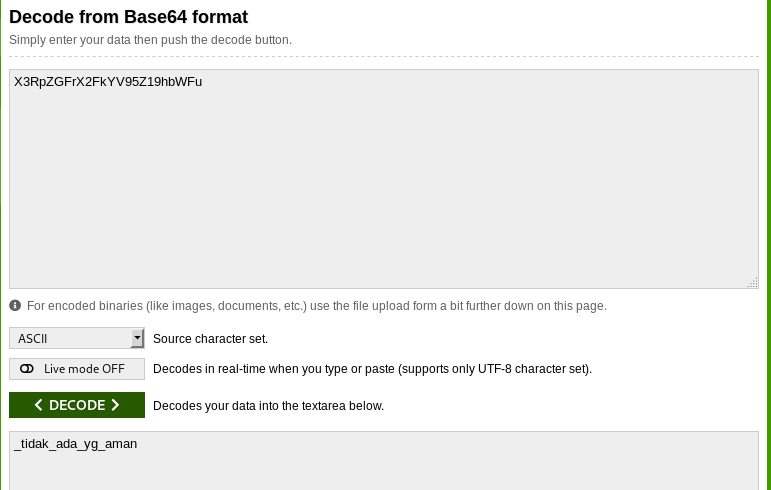
Ketika kita mencoba untuk membuka halaman tersebut, tampilan pertama yang muncul adalah pengisian data “email addres:”, pemilihan “example select” dan “example multiple select”, lalu pengisian “exemple textarea”.



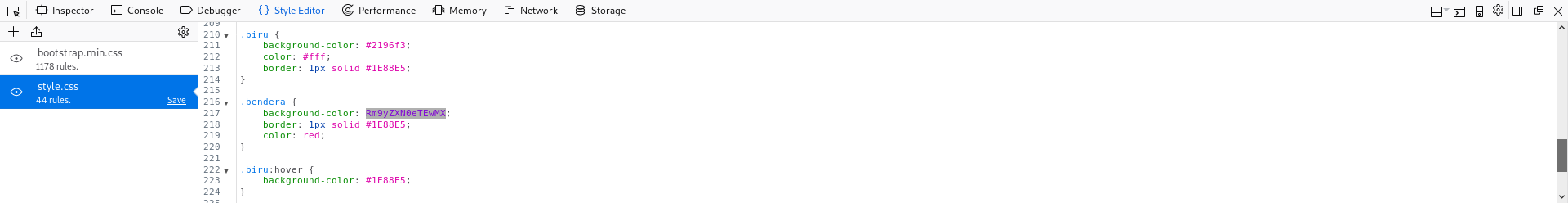
Pada awalnya kita mencoba untuk melihat source page terlebih dahulu, namun tidak ada tanda terdapatnya suatu clue dalam source page tersebut. Karena hal itu, kita melakukan inspect element untuk mencari suatu kejanggalan yang ada disana. Kita membuka satu per satu mulai dari inspector hingga storage. Kejanggalan pertama ditemukan pada Debugger (Style -> Script.js). Ketika kita srolling kebawah, terdapat pesan mencurigakan pada baris ke 45 yaitu gendero\_londo :“X3RpZGFrX2FkYV95Z19hbWFu”.



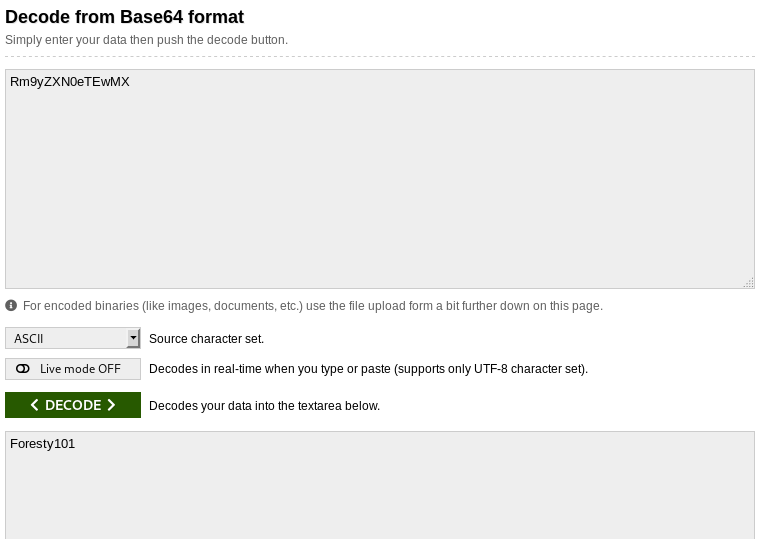
Kita langsung saja mencoba decode dengan menggunakan website <https://www.base64decode.org/> melalui source character set ASCII. Hasil decode nya adalah “\_tidak\_ada\_yg\_aman”.



Kita berpikir bahwa tidak mungkin flagnya hanya seperti itu, kita mulai lagi mencari dimanakah letak dari potongan flag lainnya. Kita menemukan pada Style Editor (style.css) pada baris 216 yaitu background-color :”Rm9yZXN0eTEwMX”.



Kita mencoba sekali lagi untuk mengdecodenya lalu mendapatkan hasil decode berupa “Foresty101”



Dengan demikian. Flag dari Challenge: Ngoding Web Skuy adalah “Foresty101{\_tidak\_ada\_yg\_aman}”.

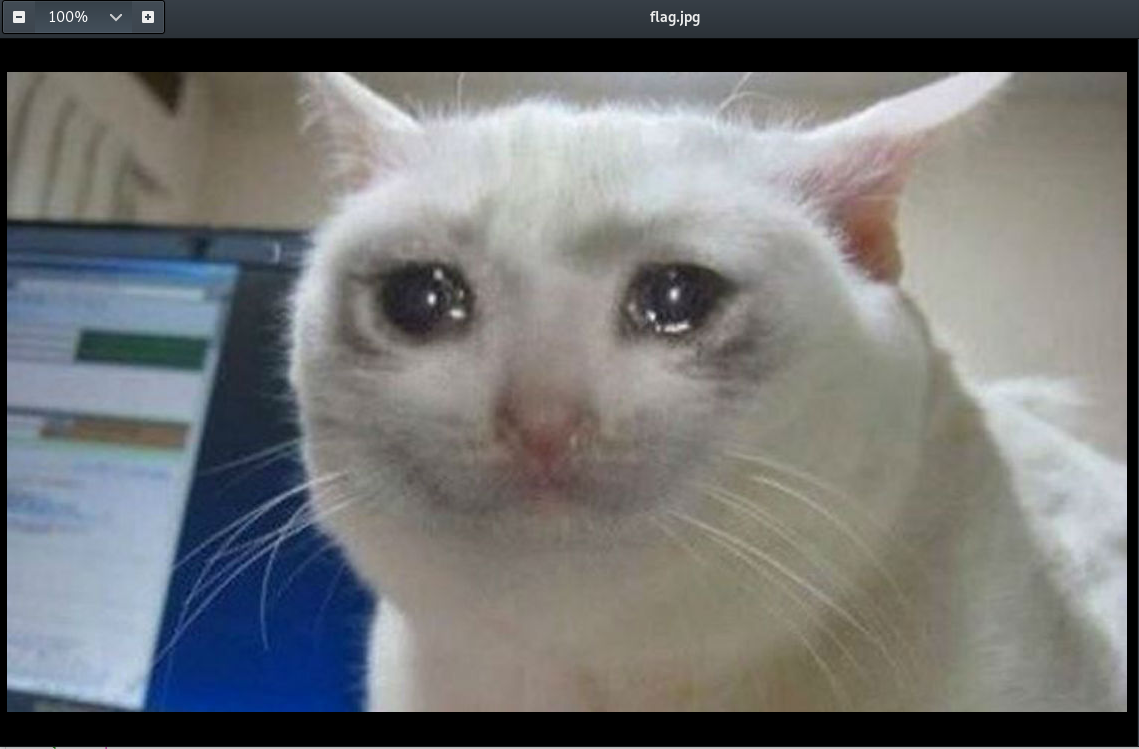
**Challenge : Sisipin 13x**

Description : Suatu file terindikasi mencurigakan, apakah anda dapat mengidentifikasi pesan yang tersembunyi ??

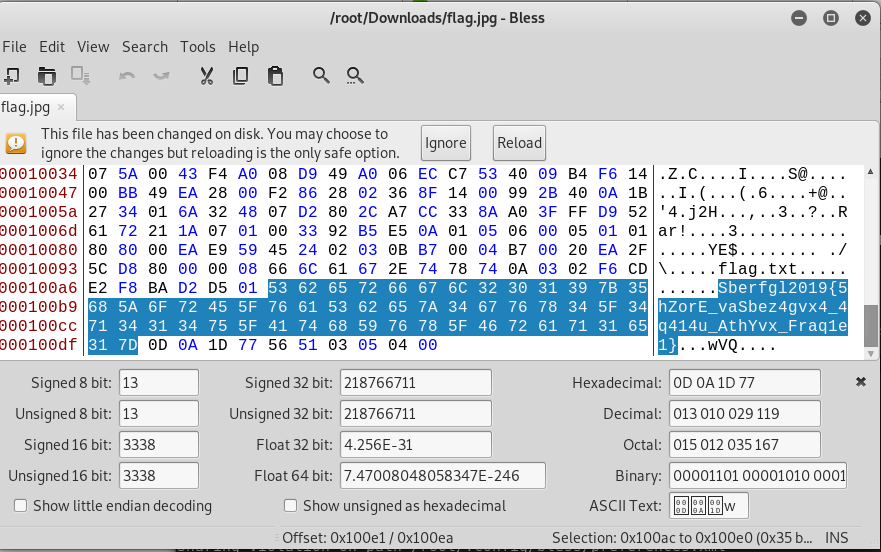
file : sisipin-13x.zip

Solusi:

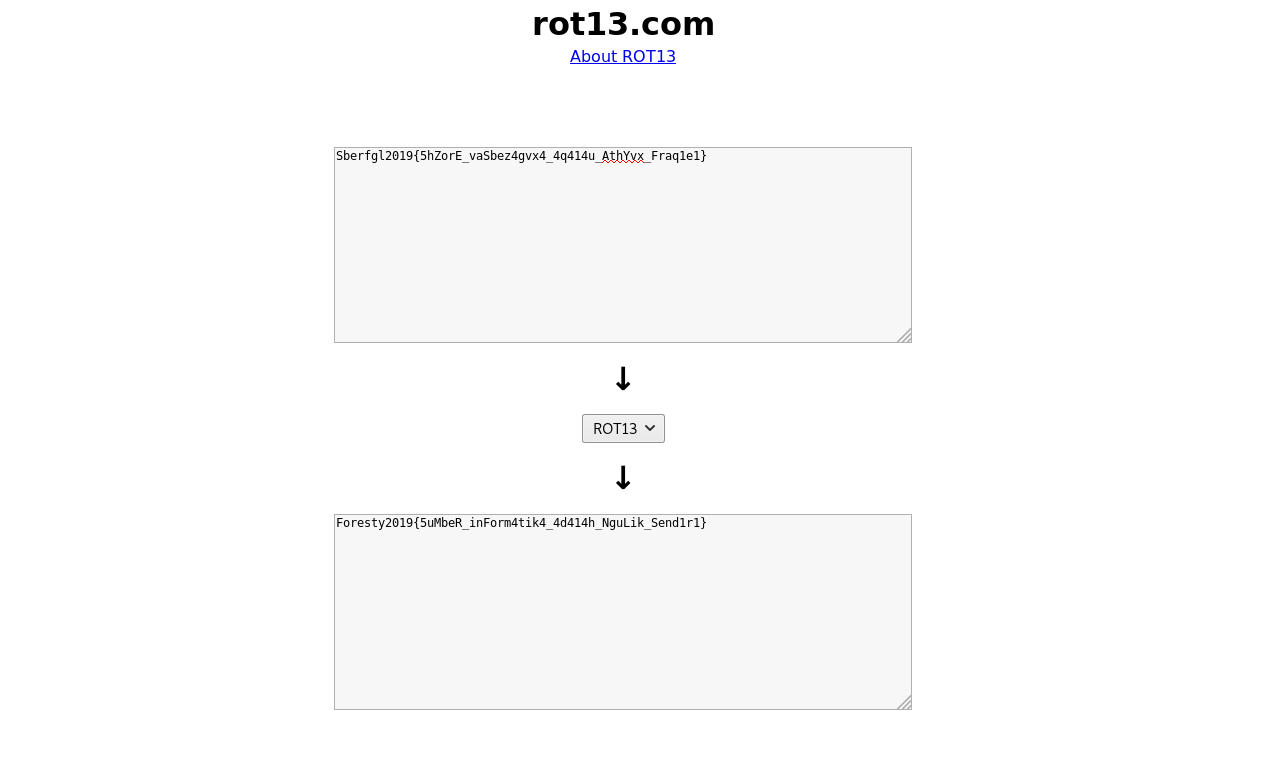
Hal yang pertama kali kita lakukan adalah mendownload file sisipin-13x.zip. Didalam file tersebut terdapat gambar kucing dengan nama flag.jpg.



Karena foto tersebut tidak memberikan clue apa-apa, kita mencoba mengindentifikasinya dengan BlessHexEditor. Kita langsung membuka terminal, membuka BlessHexEditor dengan keyword “bless” pada baris input terminal. Setelah itu kita membuka flag.jpg dengan BlessHexEditor, scrolling terus kebawah hingga mendapatkan sebuah pesan yaitu “Sberfgl2019{5hZorE\_vaSbez4gvx4\_4q414u\_AthYvx\_Fraq1e1}”.



Kita berpikir tidak mungkin flagnya seperti itu, hingga kita mendapatkan sebuah clue dari judul challenge itu sendiri, Sisipin “13x”. Kita langsung mencoba untuk mengdecode nya dengan website <https://rot13.com/>. Hasil decodenya adalah “Foresty2019{5uMbeR\_inForm4tik4\_4d414h\_NguLik\_Send1r1}”.



Setelah itu kita langsung mensubmit flag tersebut dan flagnya ternyata benar.