

# **WRITE UP**

Gemastik 2022 - Divisi II Keamanan Siber

Oleh :

MABANEKAD

Universitas Udayana

Denpasar, 30 Oktober 2022

## Traffic Engayer - Forensic

### Objektif

P balap first blood

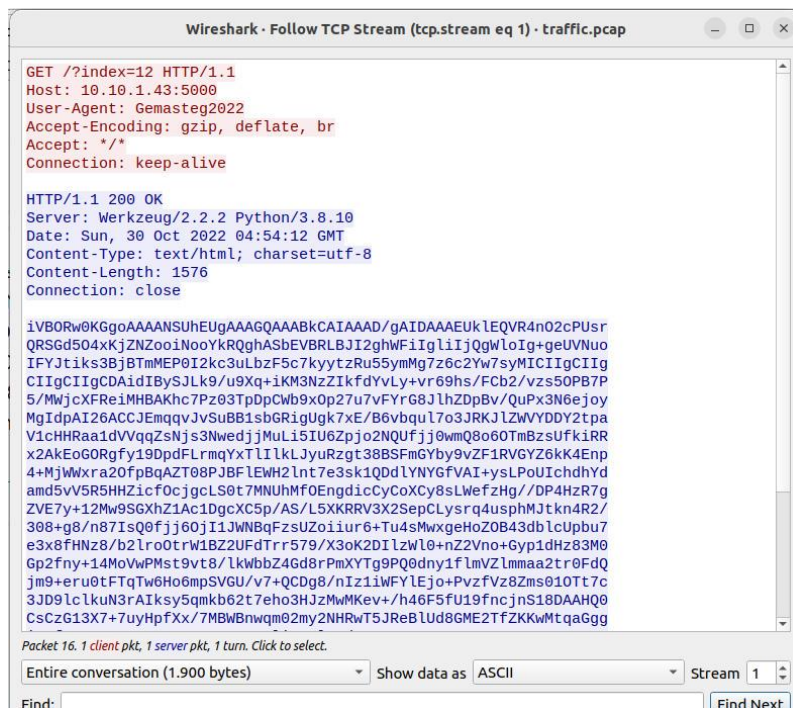
### Lampiran

traffic.pcap

### Kesimpulan

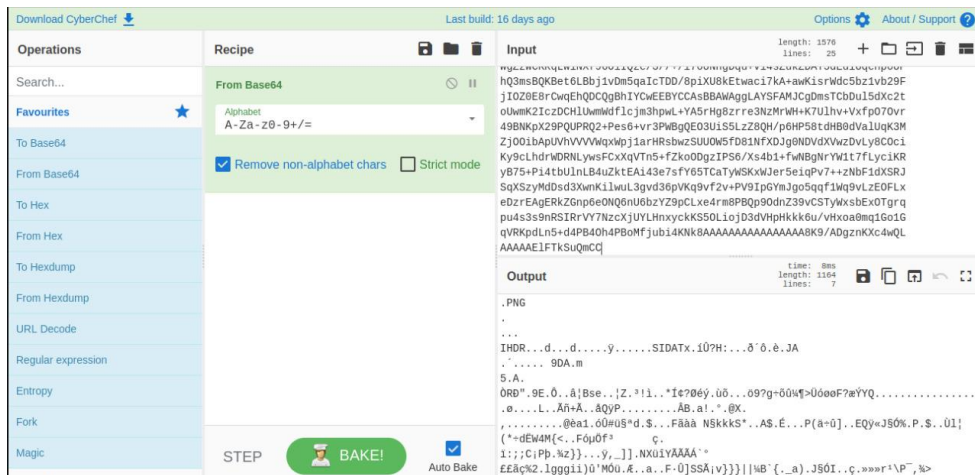
Untuk mendapatkan flag dari challenge ini kami melakukan analisa pada traffic dalam file traffic.pcap menggunakan wireshark lalu menggunakan cyberchef untuk mendecode kode base64 di dalam traffic dan menggunakan online base64 to image converter untuk menemukan bagian dari flag yang akan disusun lagi secara berurutan.

### Hasil Analisa Traffic



Saat menganalisa traffic, kami menyadari bahwa dalam traffic ada pesan yang dienkrpsi dengan base64 pada setiap traffic yang ada.

## Decode Base64



The screenshot shows the CyberChef web application interface. The 'Operations' sidebar on the left lists various tools, with 'From Base64' selected. The 'Recipe' section shows 'From Base64' with the 'Alphabet' set to 'A-Za-z0-9+/' and 'Remove non-alphabet chars' checked. The 'Input' section contains a long Base64 string. The 'Output' section shows the decoded result, which is a PNG image header starting with '.PNG' and 'IHDR'.

Setelah mendecode salah satu traffic, ternyata yang dikirim adalah sebuah file png, ditandai dengan header .png saat di decode.

## Convert base64 to image

### Enter Base64 String



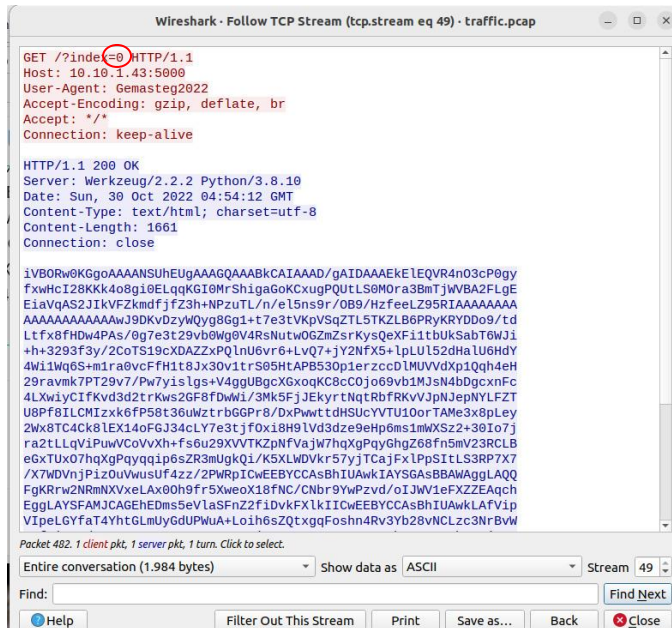
The screenshot shows an online tool for converting Base64 strings to images. The tool has a text input field containing a Base64 string, a 'Generate Image' button, and a 'Download Image' button. The size of the generated image is shown as 1.56 KB, 1576 chars.



Download Image

Setelah tahu jika didalamnya terdapat file png, kami menggunakan online tools untuk convert base64 menjadi gambar, dan ternyata semua gambar yang diberikan berupa angka, huruf atau karakter tertentu. Dimana karakter tersebut merupakan bagian dari flag.

## Merangkai flag



### Enter Base64 String

```
Z2dnGXM3mUw8DS8Cs9nMuMiDg4PiN3hrNBrG0LPZrEaj4XV+QXV2dua7d8dms1VX  
VxfsOnPnp6eGDsch7yvwJhWa1WxqXmcrr7+/uVlRXGfboSiUSlUpEkyXjXTi6X  
S6VSBEElvJYvfn1vqFAoFD7FNx+vEomEO+n0eDyvr68URReE43tjYqNfrv89iY2Nj  
c3OTh3nFNjAwQFFUvtcXC0dHR3/zzfgTExNc5WW320u5wPwz6HS6UchUYUJms5lx  
e/1FCMdx8XC7ncdAoHA5Osk2CsQHEEQJEkyfnRi5Ha7FxyW2F0k8UToX0rAMMxo  
NA4NDfX09KjV6t+/RVNeXh6Px6PRaCgU8vv9FxcXJycngUBA4NkAAAAAAAAAAAAA  
AAD/q8DvrD4r8027AAAAABJRUSErkJggg==
```

Size: 1.65 KB, 1661 chars



Download Image

kami mendapat huruf yang merupakan bagian dari flag yang acak, setelah kami menemukan huruf G besar yang merupakan awal dari format sebuah flag dan pesan tersebut ada di index = 0, maka kami mengurutkan semua karakter yang kami dapat sesuai pada index pesannya masing masing dan menjadi sebuah flag.

## Flag

Gemastik2022{balapan\_first\_blood\_is\_real\_f580c176}

# CodeJuggling - Reverse Engineering

## Objektif

Find the flag!

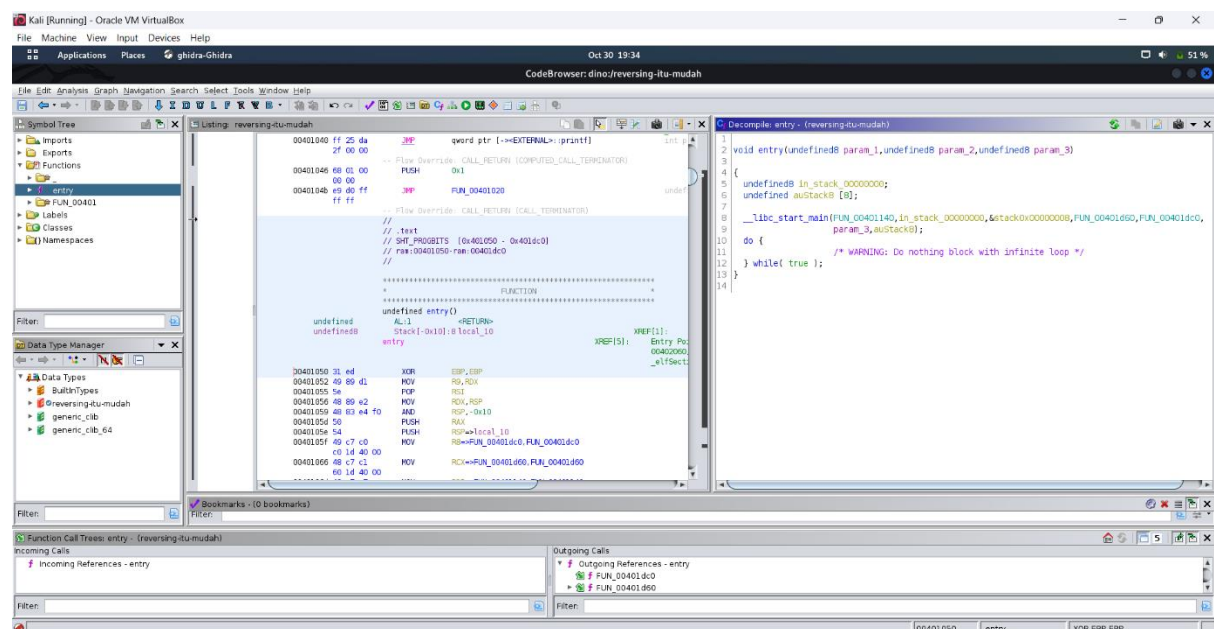
## Lampiran

reversing-itu-mudah

## Kesimpulan

Untuk mendapatkan flag dari challenge ini kami melakukan dekompilasi pada file reversing-itu-mudah dengan menggunakan perangkat lunak Ghidra.

## Hasil Dekompilasi



Gambar diatas adalah hasil dekompilasi dari file reversing-itu-mudah dengan menggunakan perangkat lunak Ghidra. Untuk masuk ke fungsi utama (main) dapat dilakukan dengan klik dua kali pada FUN\_00401140.

## Fungsi Main



dari string flag yang dicari. Untuk mendapatkan karakter penyusun lainnya dapat dilakukan dengan cara yang sama pada fungsi-fungsi lainnya.

### **Flag**

Gemastik2022{st45iUn\_MLG\_k07a\_b4rU}