**Writeup GELATIK 2019**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**bemrdo**

*Note: I’m using Hackintosh Mojave, so there are some different codes with Linux’s terminal*

**LIST OF LYFE**

**JOY 1**

Warm-up 1

**PROGRAMMING 2**

Quiz tebak kata - Reborn 2

**CRYPTOGRAPHY 4**

WannaPIE 4

## JOY

## Warm-up

### 10

Format FLAG adalah: GELATIK${FLAG}

Silakan masukkan flag berikut:

GELATIK{WarmUpChallange}

**POC :**

Tinggal copy paste aja flag nya **GELATIK{WarmUpChallange}**

## PROGRAMMING

## Quiz tebak kata - Reborn

### 75

Akses di link berikut dan jawablah seluruh pertanyaannya

IP: 180.250.7.183 Port: 7007

**Hint :** Serupa tapi tak sama seperti tahun lalu

Transpose mirroring image

**POC :**

Ketika saya coba lakukan netcat muncul text berupa base64 encoded, dan diminta memberikan input dari isi text tersebut dengan batas waktu 8 detik. Setelah saya coba decode, ternyata string tersebut berupa file gambar. Saya write ke file berekstensi .png dan salah satu gambarnya seperti berikut.

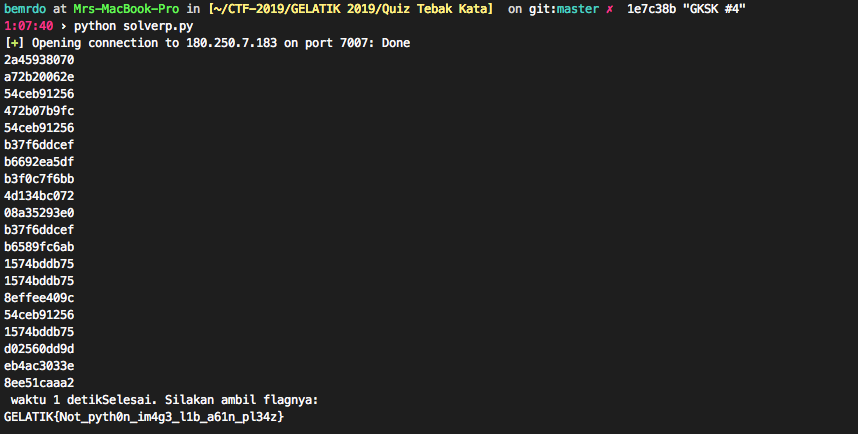


Dari gambar itu saya coba masukkan manual terlebih dahulu dengan batas waktu sebelum 8 detik, ternyata ada gambar lain lagi yang harus dipecahkan (looping). Sehingga saya buat program dalam python untuk menyelesaikan, sekaligus proses flipping image.





Kemudian saya jalankan dan flag bisa didapatkan pada akhir setelah menjawab challenge dengan benar.



Flag pun muncul setelah perjalanan panjang mencari kitab suci ke barat.

**GELATIK{Not\_pyth0n\_im4g3\_l1b\_a61n\_pl34z}**

**CRYPTOGRAPHY**

## WannaPIE

### 100

Someone send me WannaPIE and accidentally run the script and encrypted all my data. Now i can't recover my home files but luckly i have stat.info of the encrypted files, and i think it would be usefull for you as an cyber security researcher.

WARNING! Don't run the script unless you have analyzing it and if you do, be carefull of using it. WannaPIE will encrypt your /home data recursively. If you don't want any harm activity, leave it there and try another challanges. We're not responible for any loss of data. Thankyou :)

URL : https://drive.google.com/open?id=1ZY\_4OLKlbD1zycp0W9x-Q4JnSHHkbmy2

md5sum: 4a255c4d621f37387397f6c20e392a2d MY\_DRIVE.zip 19beb4ca1c4b715d88a2bf0023154c42 wannapie.py

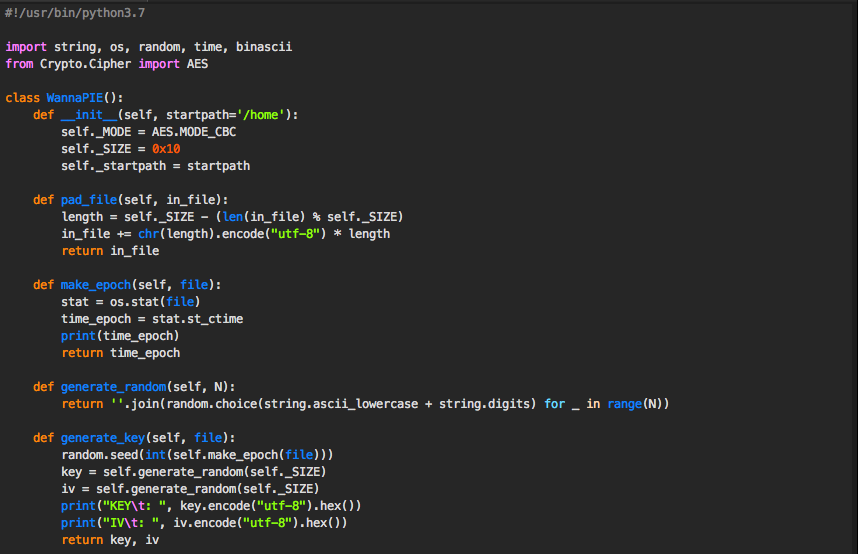
**Hint :** Deja Vu dengan GKSK?

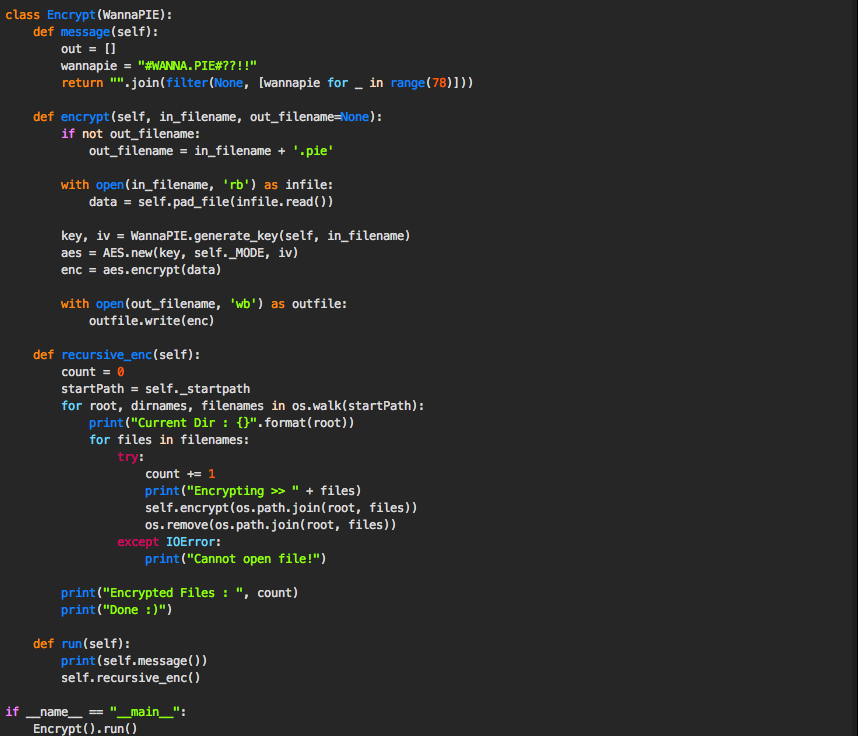
Find the correct seed for the randomization

**Attachment :** <https://drive.google.com/open?id=1ZY_4OLKlbD1zycp0W9x-Q4JnSHHkbmy2>

**POC :**

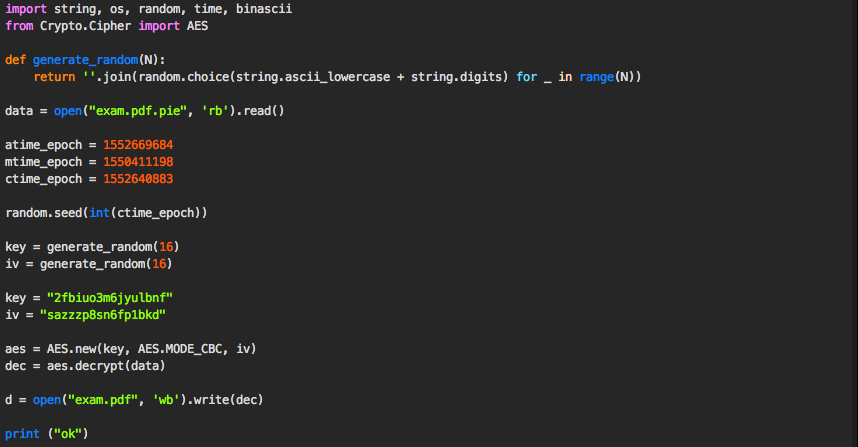
Diberikan sebuah file MY\_DRIVE.zip yang berisi file yang sudah dienkripsi dan sebuah file python wannapie.py yang digunakan untuk mengenkripsi file-file tersebut.

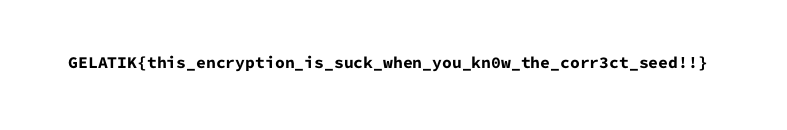




Dari hasil analisa, saya ketahui bahwa program python tersebut melakukan enkripsi file menggunakan AES-CBC pada folder /home. Proses enkripsi menggunakan random key dan random iv, namun memiliki random seed yang diambil dari Change Time (ctime) setiap file. Setelah saya extract file .zip yang diberikan, terdapat file .stat yang merupakan statistik time dari setiap file yang dienkripsi. Selain itu terdapat folder home yang berisi file yang sudah terenkripsi dan folder lainnya yang di dalamnya juga telah terenkripsi. Pertama saya berfokus untuk mendeskripsi file flag?.pdf.pie. Pertama, saya membuat program python untuk mendeskripsi file menggunakan AES-CBC, jadi saya hanya tinggal mencari random seed yang tepat. Saya menggunakan web <https://www.epochconverter.com> untuk mengubah time pada file .stat agar menjadi format yang tepat untuk ctime random seed pada program. Program wannapie.py menggunakan python 3, sehingga untuk proses random juga harus menggunakan python 3 (random pada python 2 dan python 3 berbeda), namun sebuah musibah muncul… python 3 pada laptop saya tidak bisa import Crypto.Cipher.AES, saya mengakalinya dengan menggunakan python 3 hanya untuk mencari random key dan random iv. Sedangkan untuk proses deskripsi saya menggunakan python 2 (untungnya ctime semua file sama).

Ternyata file flag?.pdf.pie setelah di deskripsi merupakan form tugas akhir (maklum authornya udh mau yudisium, mungkin kisah-kasihnya selama kuliah agar dikenang). Setelah menjadi seseorang yang seperti stalkerin mantan :v saya pun menemukan file flag nya yaitu exam.pdf.pie.





Berikut flag dari challenge yang gk bias saya selesaikan ketika GKSK#4

**GELATIK{this\_encryption\_is\_suck\_when\_you\_kn0w\_the\_corr3ct\_seed!!}**