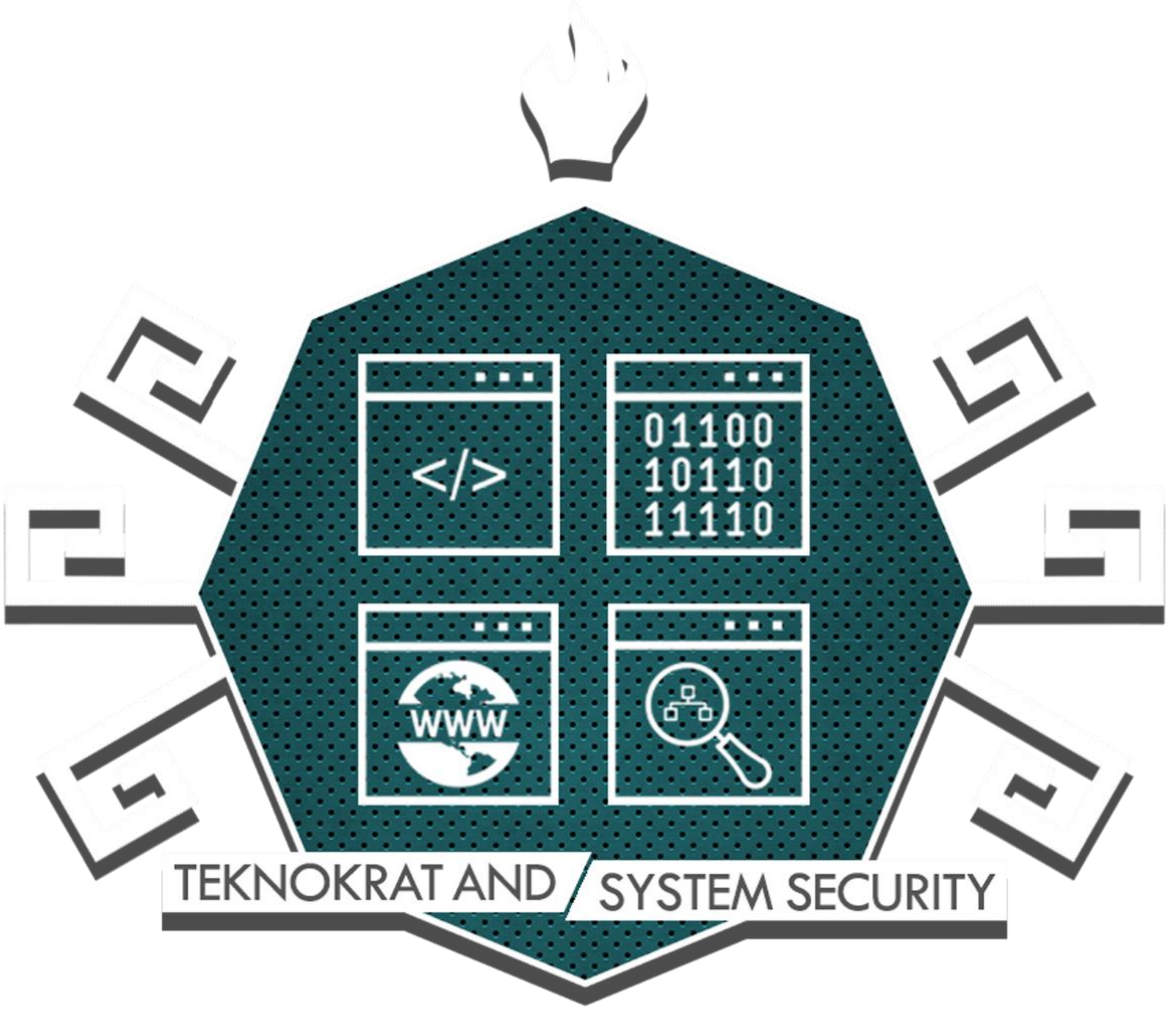


Writeup CTF Compfest 8 by Tenesys

- ***Maze***

Point : 90 pt

Category : Web Hacking (http://musashi.compfest.web.id:11663/)

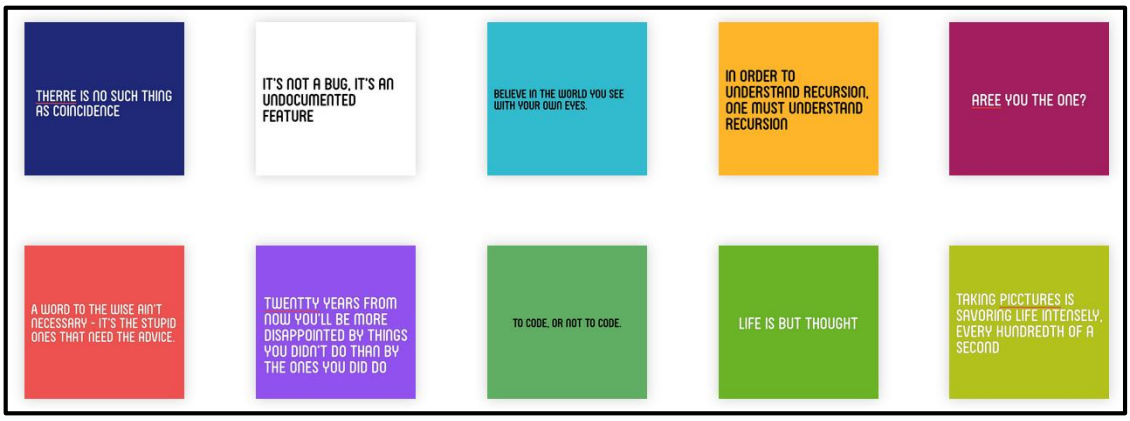
Flag : CFCTF{h0w_d0_y0u_f1nd_th15_fl56}

Description :

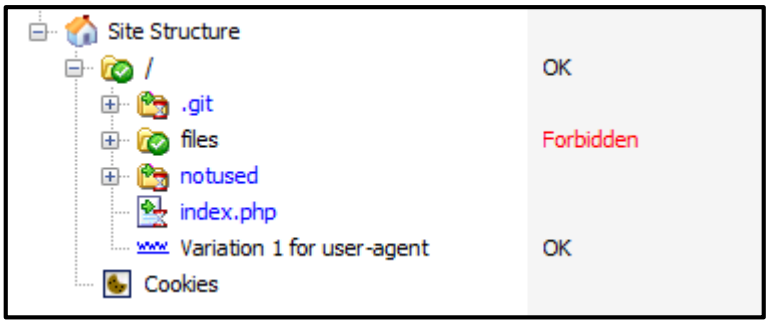
There's a "maze" hidden within this website. Our informants told us that the flag in it has been deleted though. Recovering it would not be a problem for you, would it?

Solution :

Terdapat website dengan tampilan berikut,



Kami coba untuk melakukan scanning direktori/file pada website tersebut menggunakan Acunetix, dan menemukan GIT Repository,



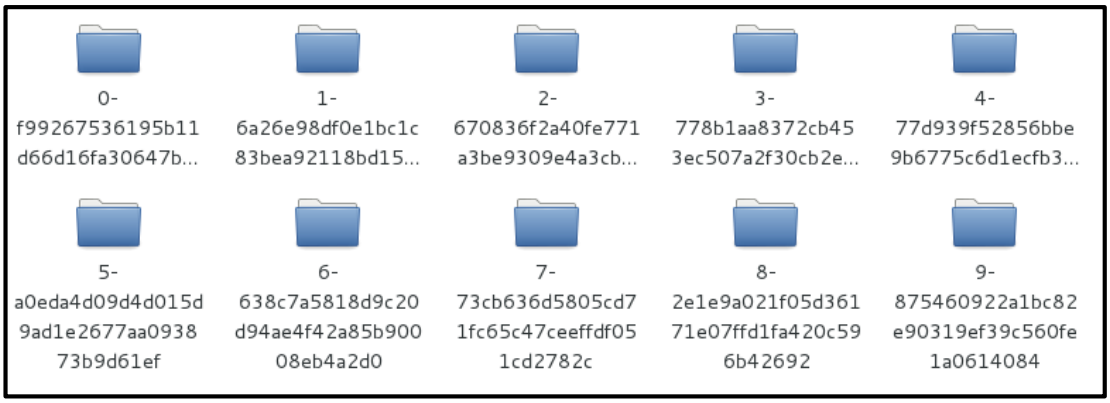
Lalu kami coba dumper GIT tersebut menggunakan GitTools yang kami download dari https://github.com/internetwache/GitTools, dengan perintah :

```
./gitdumper.sh http:// musashi.compfest.web.id:11663/.git/ dump/
```

Lalu kami ekstrak dengan perintah :

```
./extractor.sh /home/jdoor/Download/GitTools/Dumper/dump /f/
```

Sehingga mendapatkan direktori seperti berikut, hingga hardisk kami penuh (13 GB+) haha,



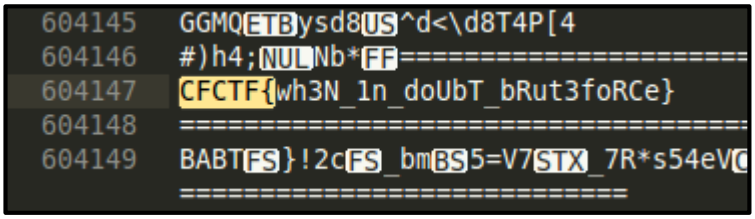
Lalu kami coba mencari string “CFCTF” sesuai dengan format flag,

Dapatlah flag yang kami cari yaitu CFCTF{h0w_d0_y0u_f1nd_th15_fl56}.

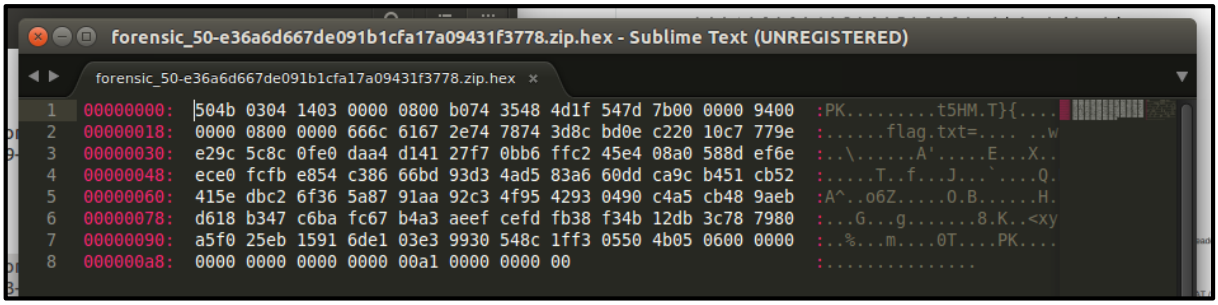
- ***Tambahan***

Sebelumnya kami telah menemukan 2 string yang berformat sama pada direktori hasil dumper GIT tersebut, namun ternyata string tersebut bukan flag yang benar atau pengecoh saja.

String pertama berada pada gambar hasil screenshot pada salah satu direktori,



Sedangkan string kedua didapat dari hasil dari mengubah hex berikut menjadi file .zip dimana setelah dibuka ternyata file corrupt,



Lalu kami coba repair menggunakan winrar sehingga file dapat dibuka, dan mendapat string CFCTF{My_zip_archive_is_broken_as_I_expected}.