

Write up - Reto 9 CTF - Hackers4Fun

Detalles:



Hackers4Fun CTF Team

@Hackers4F

Siguendo

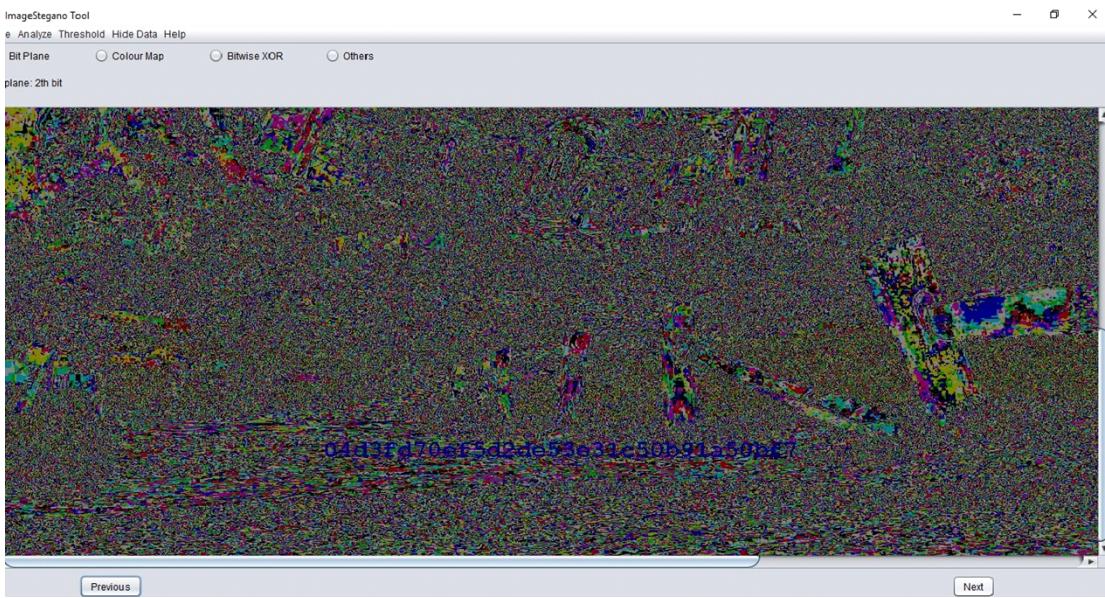
#Reto 9 #H4F Entrenamiento #CTF ... Sure you can! > Categoria > Stegano > La entrada a la taberna del "Patito Modosito" 🐥 esconde un mensaje 🕵️. El #Reto trata de princesas 🧑‍公主 que nos desvelarán un buen consejo 👍
> Download 📁
drive.google.com/file/d/1NTdIOW...



Bien, descargamos la imagen del link que se adjunta a Google Drive:



Abrimos la imagen con stegsolve o ImageStegano y le damos a siguiente hasta que encontremos algo ;



Bien! encontramos lo que parece ser un hash MD5, procedemos a descodificarlo en la siguiente página web ; (www.md5online.es)

Obtenemos el siguiente enlace;

<https://drive.google.com/file/d/1Fg36MgJ5B9FSyClJ56us8XB4wCq3vSUg/view>
en el que se encuentra esta imagen :



Vemos que en herramientas como stegsolve no nos aparece nada, así que procedemos a usar la herramienta online Steganographic Decoder (<https://futureboy.us/stegano/decinput.html>).

Parece que hemos tenido suerte, encontramos el siguiente hash:
867a375cec13208995192cd7b61a183b

Nos vamos a esta página (<https://md5hashing.net/hash/>) y descodificamos el hash y obtenemos lo siguiente ;

Decoded value:

Select Decoded Value

sDRGeyNYMVJlZE1hc1NlZ3vyYV8jww9RdVVUdULyaWF9

Parece que es un Base64, probemos a descodificarlo en esta página: (www.base64decode.org)

```
SDRGeyNYMVJIZE1hc1NlZ3VyYV8jWW9RdVVUdUljaWF9
```

◀ DECODE ▶

UTF-8

You may also select input charset.

Live mode ON

Decodes while you type or paste (strict format).

Note that decoding of binary data (like images, documents, etc.) does not work in live mode.

UPLOAD FILE

Decodes an entire file (max. 10MB).

```
H4F{#X1RedMasSegura_#YoQueTulria}
```

Y efectivamente es un Base64, ya tenemos la flag!!

H4F{#X1RedMasSegura_#YoQueTulria}

@Frantkdz

