

Una al Mes (Episodio 2)

@percu

15/06/18

Contenido

MISIÓN	1
RESOLUCIÓN	2
PARTE 1 – WEB Y OFUSCACIÓN	2
PARTE 2 – ESTEGANOGRAFIA	3
REFERENCIAS	6

Challenge

X

EPISODIO 2

200

Mientras estábamos dentro de la caja fuerte, la policía ha podido entrar en el sistema informático de la fábrica. Nos ha abierto un chat "seguro" con el que podemos interactuar con ellos. Pensamos que si se logra explotar de alguna manera, podremos llegar a descomprimir el archivo que tiene la flag.


Chat con la Policía:
<http://34.247.69.86/lacasadepapel/episodio2/index.html>

Info: La flag tiene el formato UAM{md5}

TOP 3: 1. 2. 3.

Unlock Hint for 10 points

Unlock Hint for 20 points

 episodio2.zip

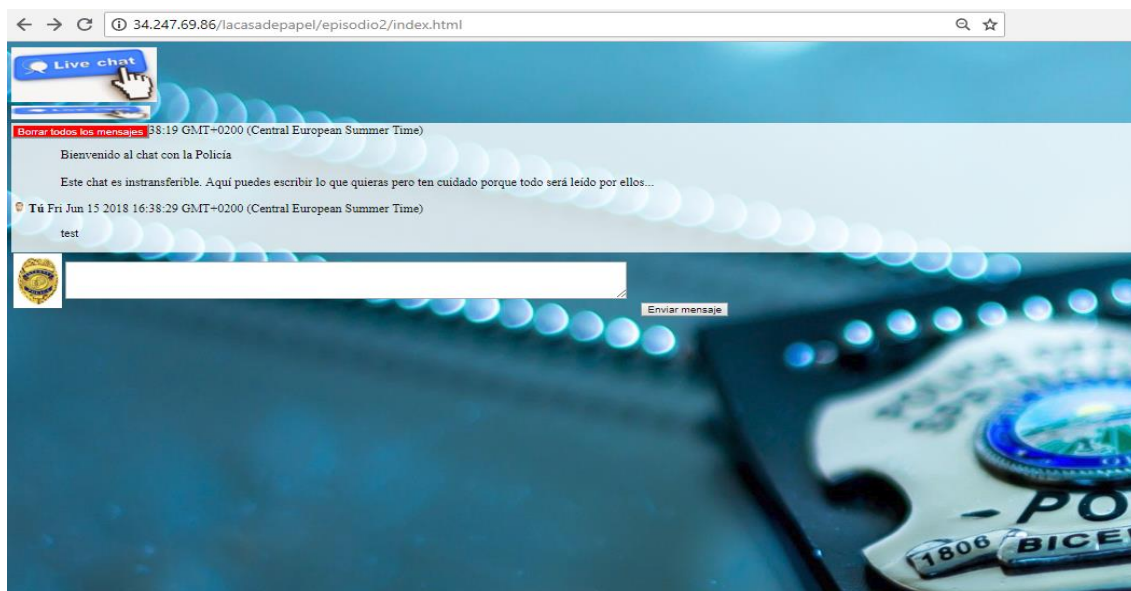
Flag

Submit

RESOLUCIÓN

PARTE 1 – WEB Y OFUSCACIÓN

El primer paso es acceder a la url <http://34.247.69.86/lacasadepapel/episodio2/index.html> donde nos aparece un chat en el que cada vez que escribimos alguna cosa lo muestra por pantalla:

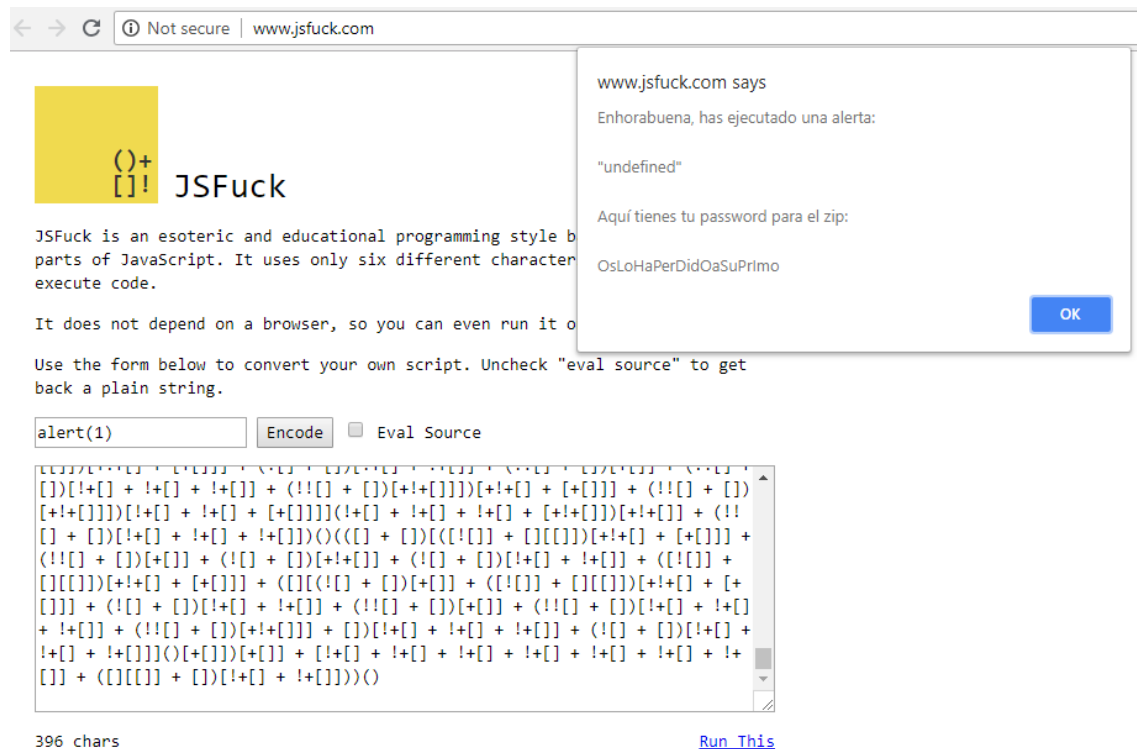


Observando el código fuente vemos que carga un JS de nombre game-frame.js. Vamos a ver qué contiene:



Analizando los caracteres que contiene el fichero JS “`()!+`” llegamos a la conclusión de que es un fichero ofuscado con la técnica JSFuck.

Des de la url <http://www.jsfuck.com/> podemos des ofuscarlo:



Así el password para descomprimir el zip es **OsLoHaPerDidOaSuPrImo**

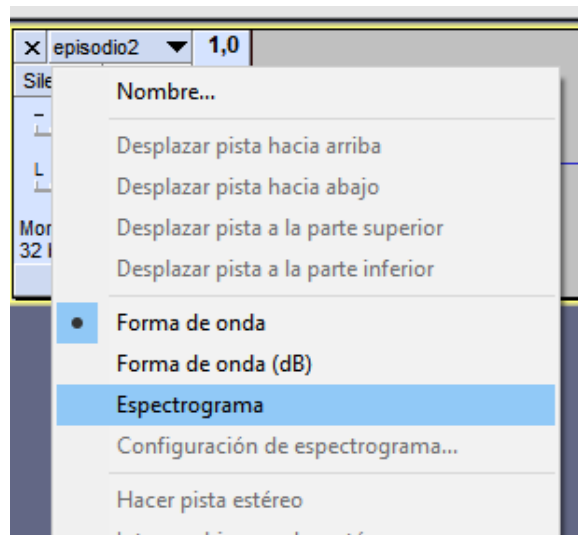
PARTE 2 – ESTEGANOGRAFIA

Al descomprimir el fichero episodio2.zip obtenemos un archivo de audio episodio2.wav

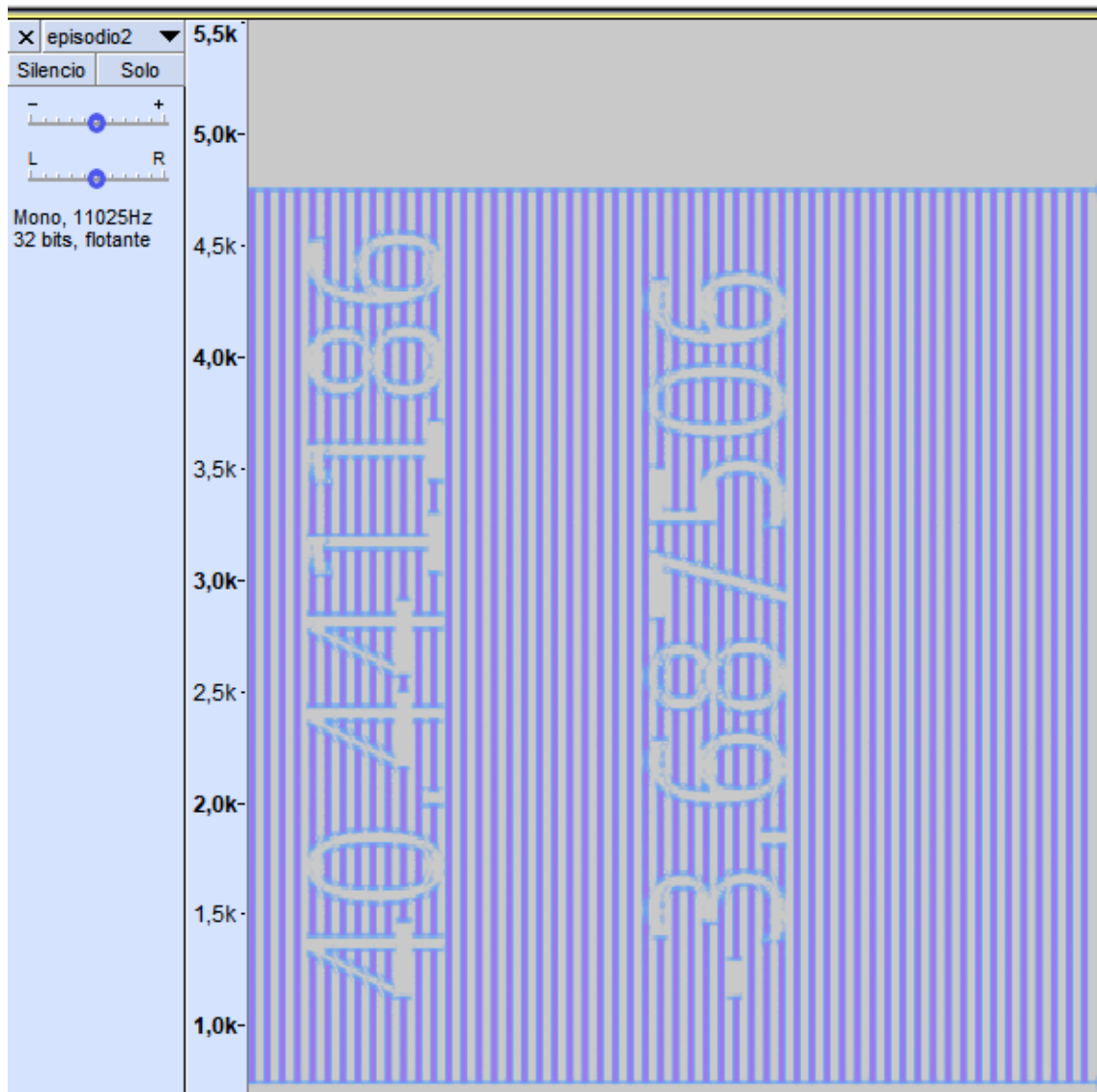
Le pasamos una utilidad para detectar si hay mensaje oculto con la técnica del LSB sin detectar nada.

Probamos con la técnica de espectrograma.

Para esto utilizaremos el programa Audacity y presentaremos el fichero con su espectrograma:



Nos aparece lo que parecen ser unas coordenadas:



40.441186 -3.687506

Son las coordenadas de La Casa de Papel:

← → ↻ ⓘ Not secure | boulter.com/gps/#40.441186%20-3.687506

GPS Coordinate Converter, Maps and Info

Enter coordinates

(like 37 23.516 -122 02.625, but it's flexible)

Decimal Degrees (WGS84)

<u>Latitude</u>	<u>Longitude</u>
40.441186	-3.687506

Degrees, Minutes & Seconds

<u>Latitude</u>	<u>Longitude</u>
N40 26 28	W3 41 15

GPS

<u>Latitude</u>	<u>Longitude</u>
N 40 26.471	W 3 41.250

UTM

<u>X</u>	<u>Y</u>
30N 441694	4476953

Mapa Satélite

La Casa De Papel
Calle de Serrano, 117
28010 Madrid
España
[Ver en Google Maps](#)

La Casa De Papel

Google
Datos de mapas ©2018 Google, Inst. Geogr. Nacional Términos de uso

Clicked At: [40.441169251790946 -3.687506318092346](https://www.google.com/maps/@40.441169251790946,-3.687506318092346)

DETAILED MAPS AT:

Codificamos “La Casa De Papel” a MD5: *UAM{a9f006ec50ac24c766e26be58fab6933}*

La flag nos aparece como incorrecta.

Probamos a codificar directamente a MD5 las coordenadas 40.441186 -3.687506

UAM{9bbf31b30acd21df0d35a4d8333b235e} y esta sí es la solución al reto.

REFERENCIAS

JSFuck:

<https://en.wikipedia.org/wiki/JSFuck>

<http://www.jsfuck.com/>

TÉCNICAS DE ESTEGANOGRAFIA EN FICHEROS DE AUDIO:

<https://iicybersecurity.wordpress.com/2015/08/25/how-to-hide-secret-messages-in-music-files/>

<http://boulter.com/gps/>