

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


Mirando el código del html lo primero que me llama la atención es:

```
<!doctype html>
<html>
  <head>
    <meta charset="UTF-8">
    <script src="game-frame.js"></script>
    <link rel="stylesheet" href="styles.css" />

    <script src="post-store.js"></script>
```

Podemos mirar el contenido de game-frame.js .. pero en este caso solo me ha servido para enfocar el tipo de ataque a explotar.

Una simple búsqueda en google de "game-frame.js" y tenemos:



Totes Imatges Shopping Vídeos Més Configuració Eines

Aproximadament 132 resultats (0,38 segons)


javascript - How is this XSS attack working? - Information ...
<https://security.stackexchange.com/.../how-is-this-xss-attack-w...> ▼ Tradueix aquesta pàgina
9 de juny 2014 - What happens is that the HTML output is: ``. `{{ timer }}` is a variable which gets ...
Heu visitat aquesta pàgina el dia 15/06/18.

level.py ? 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 ...
<https://xss-game.appspot.com/level1/source> ▼ Tradueix aquesta pàgina
Internal game scripts/styles, mostly boring stuff -->. `<script src="/static/game-frame.js"></script>`. `<link rel="stylesheet" href="/static/game-frame-styles.css" />`.
Heu visitat aquesta pàgina 2 vegades. Darrera visita: 15/06/18

GitHub - arnoldmyint/COMP2910: COMP 2910 Project for CST.
<https://github.com/arnoldmyint/COMP2910> ▼ Tradueix aquesta pàgina
... and start of game.js\Panel.js Selector tray and shaps at the bottom of the game frame.js\Points.js
Calculations for points, shapes, polygons specifically.

Interesting game: Google XSS Game - Programering
<https://www.programering.com/a/MzM0YzNwATE.html> ▼ Tradueix aquesta pàgina
9 de nov. 2014 - <https://xss-game.appspot.com/static/game-frame.js>. /* If we're being iframed, let the
parent know our URL */ /* Kids: don't do this at home!
Heu visitat aquesta pàgina 2 vegades. Darrera visita: 15/06/18

Imatges sobre "game-frame.js"

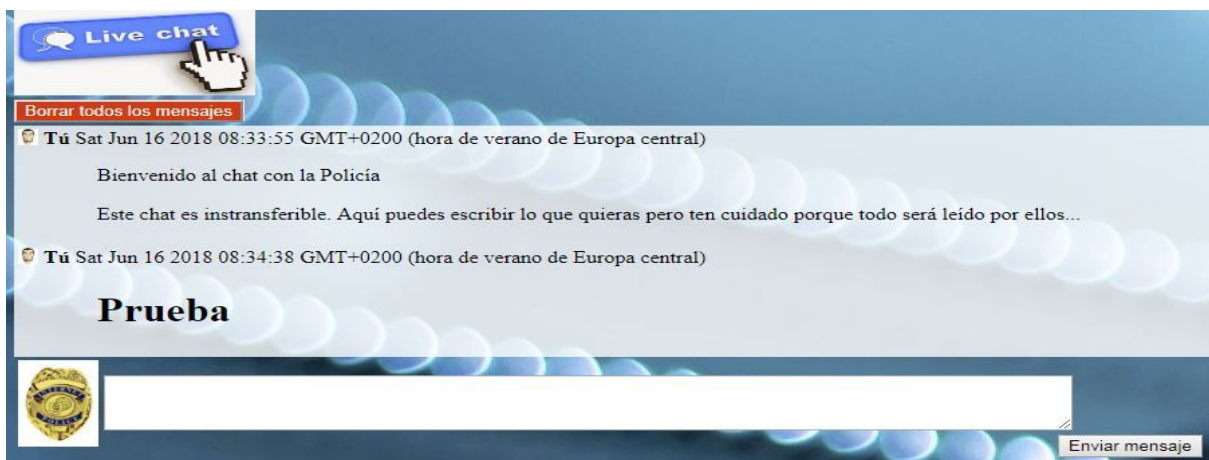
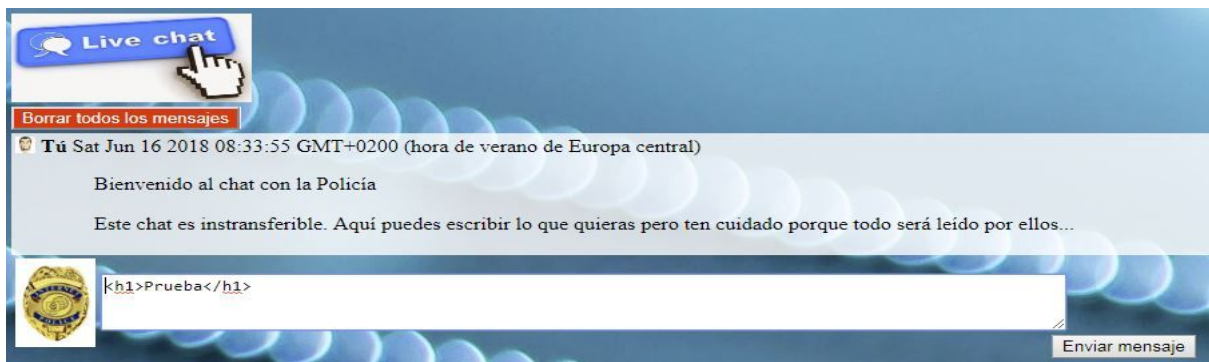


→ Més imatges per a "game-frame.js" Informeu de les imatges

XSS Game Question - Hack Forums

<https://hackforums.net/showthread.php?tid=5724705> - Tradueix aquesta pàgina
(less than)script src="/static/game-frame.js"(greater than)(less than)/script(greater than) Thanks. Reply
- ROOTED Offline Lurking * HF Ub3r. Prestige: 136

Bien, vamos a inyectar código html a ver si lo reconoce:

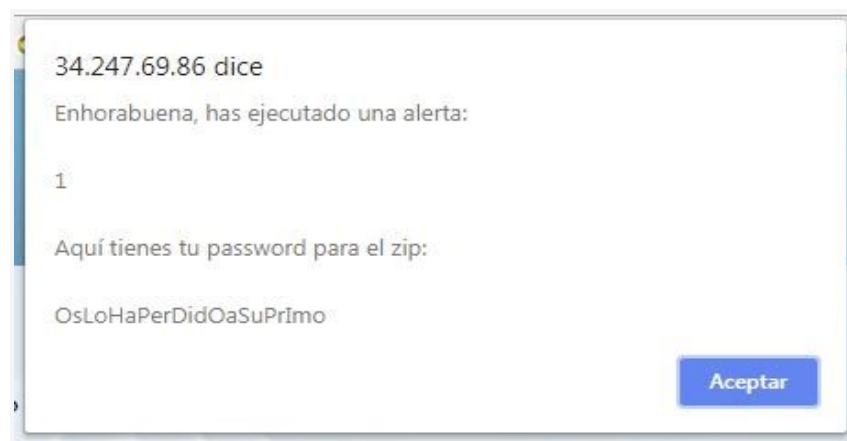


Vamos bien ... mirando ataques de XSS llego a esta web:

<https://www.malc0de.org/complete-solution-to-xss-game-by-google-to-practice-xss/2/>

Allí vemos cómo podemos generar una alerta, así que probamos con el payload:

```
<img src=x onerror=alert(1)>
```



Bien .. ya tenemos el password del .zip que nos hemos descargado, lo descomprimos y tenemos un .wav

Vamos a sacar un poco de información básica:

```
# file episodio2.wav
```

```
episodio2.wav: RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, mono 11025 Hz
```

```
# strings episodio2.wav
```

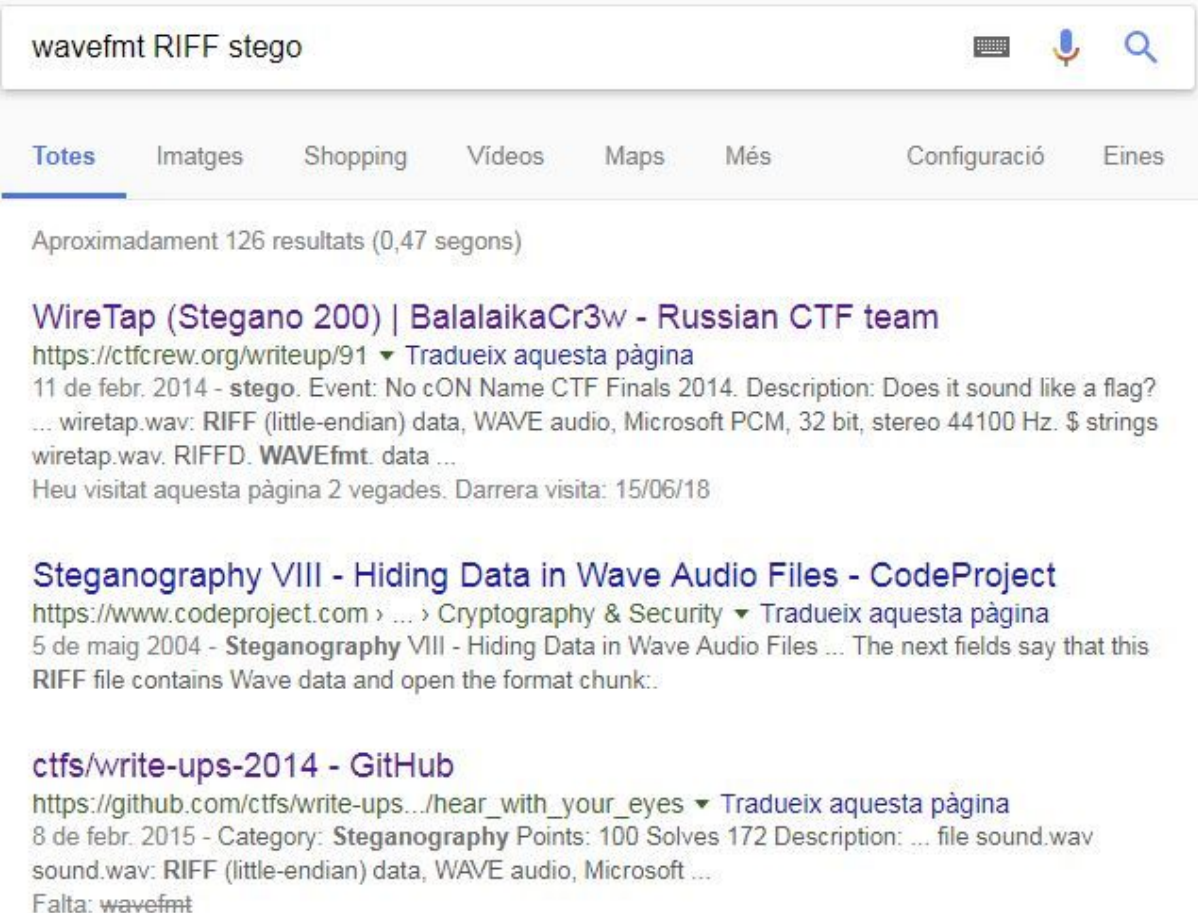
```
RIFF
```

```
WAVEfmt
```

```
data
```

Lo escuchamos .. y claramente hay un tipo de código ... vamos a ver como sacarlo:

Una búsqueda rapida en google:



The screenshot shows a Google search interface with the query 'wavefmt RIFF stego' in the search bar. Below the search bar, there are tabs for 'Totes', 'Imatges', 'Shopping', 'Vídeos', 'Maps', 'Més', 'Configuració', and 'Eines'. The search results are displayed below the tabs, showing approximately 126 results in 0.47 seconds. The first result is titled 'WireTap (Stegano 200) | BalalaikaCr3w - Russian CTF team' and includes a link to 'https://ctfcrew.org/writeup/91'. The second result is titled 'Steganography VIII - Hiding Data in Wave Audio Files - CodeProject' and includes a link to 'https://www.codeproject.com'. The third result is titled 'ctfs/write-ups-2014 - GitHub' and includes a link to 'https://github.com/ctfs/write-ups.../hear_with_your_eyes'.

Search query: wavefmt RIFF stego

Results: Aproximadament 126 resultats (0,47 segons)

WireTap (Stegano 200) | BalalaikaCr3w - Russian CTF team
<https://ctfcrew.org/writeup/91> ▾ Tradueix aquesta pàgina
11 de febr. 2014 - **stego**. Event: No cON Name CTF Finals 2014. Description: Does it sound like a flag?
... wiretap.wav: RIFF (little-endian) data, WAVE audio, Microsoft PCM, 32 bit, stereo 44100 Hz. \$ strings
wiretap.wav. RIFFD. **WAVEfmt**. data ...
Heu visitat aquesta pàgina 2 vegades. Darrera visita: 15/06/18

Steganography VIII - Hiding Data in Wave Audio Files - CodeProject
<https://www.codeproject.com> > ... > Cryptography & Security ▾ Tradueix aquesta pàgina
5 de maig 2004 - **Steganography VIII - Hiding Data in Wave Audio Files** ... The next fields say that this
RIFF file contains Wave data and open the format chunk:..

ctfs/write-ups-2014 - GitHub
https://github.com/ctfs/write-ups.../hear_with_your_eyes ▾ Tradueix aquesta pàgina
8 de febr. 2015 - Category: **Steganography** Points: 100 Solves 172 Description: ... file sound.wav
sound.wav: RIFF (little-endian) data, WAVE audio, Microsoft ...
Falta: wavefmt

Vemos que en

https://github.com/ctfs/write-ups-2014/tree/master/su-ctf-quals-2014/hear_with_your_eyes

nos hablan de cómo ver el espectrograma en Audacity, yo no tenía Audacity instalado en ese ordenador, por lo que busco algún servicio online para obtener el espectro del audio.

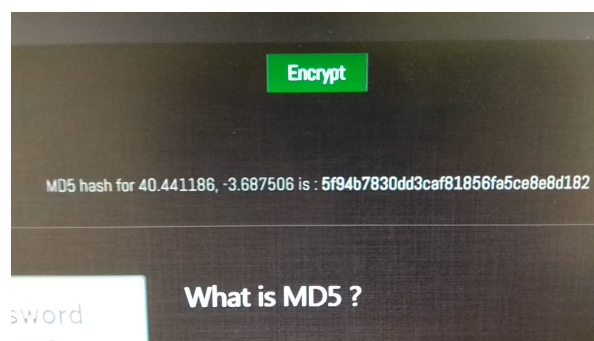
En la web <http://convert.ing-now.com/mp3-audio-waveform-graphic-generator/> encuentro lo que busco y el resultado es:



Unas coordenadas ... busco en google maps y veo que se trata de una supuesta Casa de Papel entiendo que voy bien ... ya que hace referencia a la serie con la que está inspirado el reto ... pero después de mucho buscar por google maps ... reseñas ... etc .. no veo nada que me aporte una pista ... por lo que empiezo a generar md5 de las cosas que tengo .. como “La Casa De Papel” ... etc .. hasta que al final genero el md5 de las coordenadas.

No tengo muy claro cómo generarla .. es decir .. si con espacio .. sin espacio ... voy probando hasta que un hash me da como flag correcto.

En el momento de hacerlo yo era:



Creo que posteriormente se ha cambiado el flag para hacerlo más evidente y directo .. pero al final viene a ser lo mismo.

En este reto parece que ha habido algún tipo de problema con lo de Google Maps... donde seguramente tenía que aparecernos alguna pista para saber que teníamos que hashear las coordenadas, de no ser así no tenía mucho sentido que se hayan tomado la molestia de crear la ubicación en google maps ...

DarkEagle

Challenge		1 Solves	×
Name		Date	
DarkEagle		2 minutes ago	