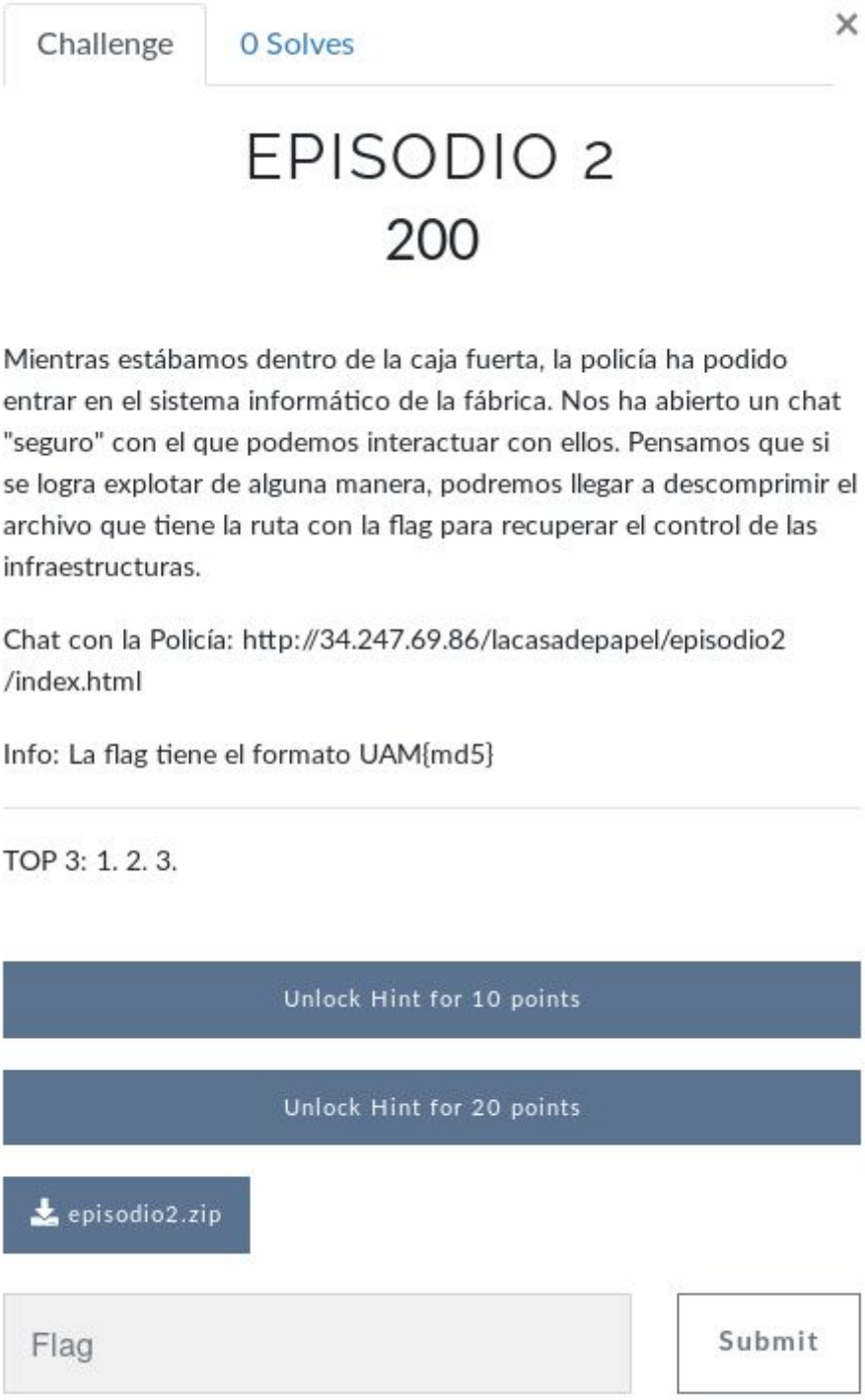
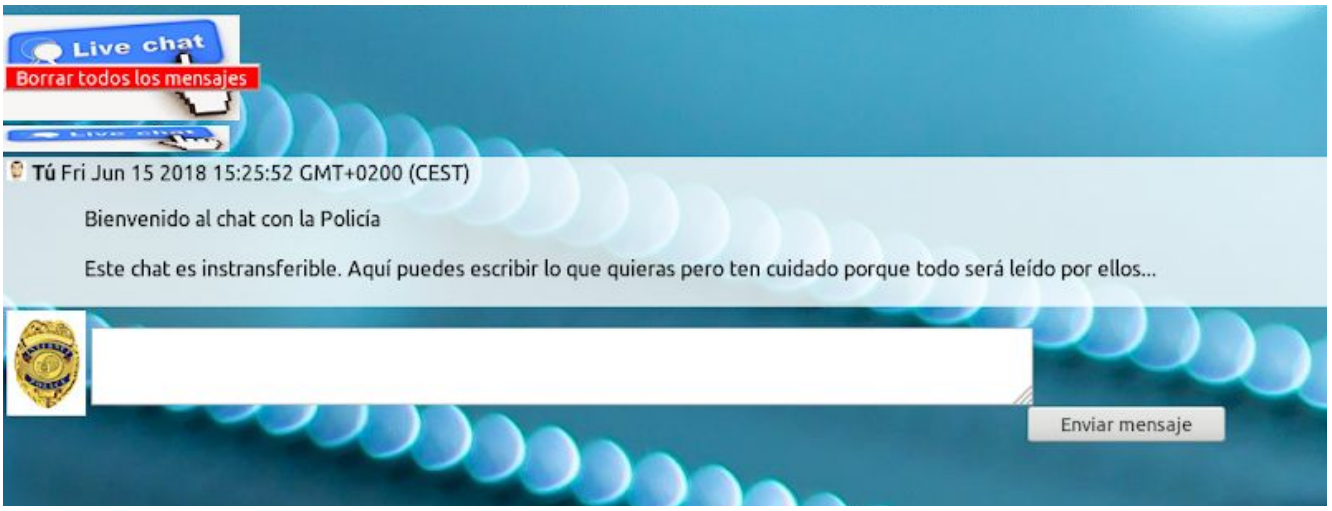
Episodio 2

http://unaalmes.hispasec.com/challenges#EPISODIO%202



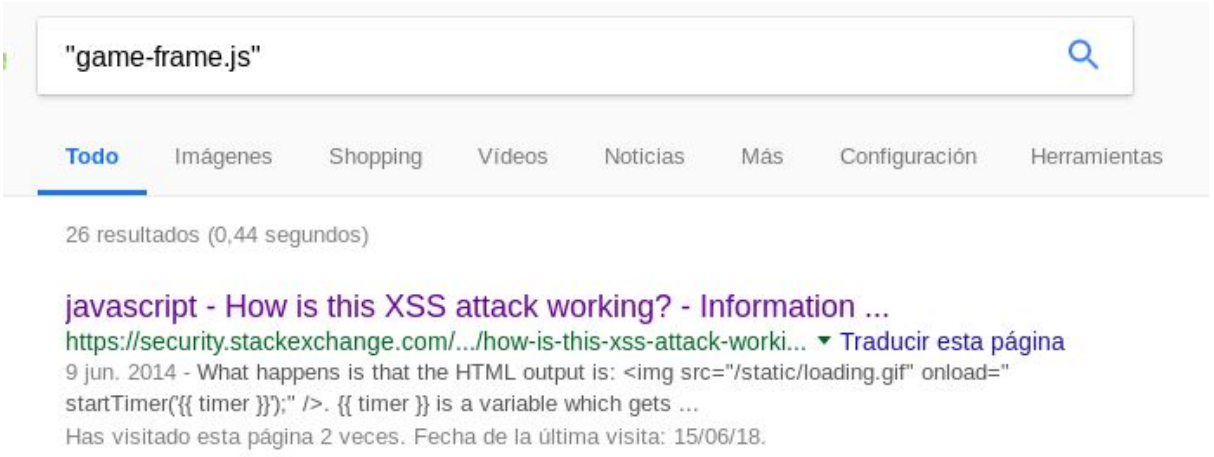
Según nos dice el texto, “buscamos la ruta con la flag” contenido en un archivo de este zip... con password, claro.

Entramos en http://34.247.69.86/lacasadepapel/episodio2 y ncontramos una web con un formulario para enviar mensajes “seguros” a la policía.



Miro los recursos que carga, un poco el javascript, pongo algunos puntos de interrupción en el código… no consigo nada.

Tras revisar un rato el código fuente y perder mucho tiempo tratando de debugar código ofuscado en javascript y mirar las pistas encuentro esto:



Si lo hubiera hecho antes hubiera ido directamente a buscar el xss y no perder puntos por las pistas sin haber buscado un poco más. Aunque, la verdad,tenía ganas de ver cómo eran las pistas :S

Las pistas nos dicen:

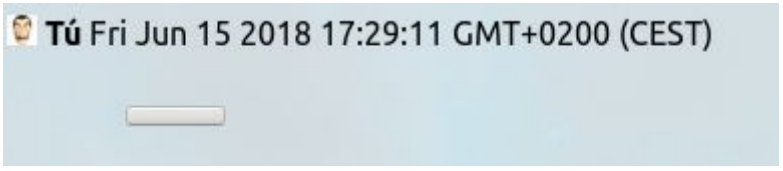
1. que no toquemos código y que interactuemos con el chat (-10 puntos)

2. Es XSS (-20 puntos)

Veo algunas cosas en:
https://github.com/Pgaijin66/XSS-Payloads/blob/master/payload.txt

Meto esto en el mensaje y envío:

<button onClick=”alert(‘’);>



Acabamos de meter un botón que al pulsarlo ejecuta javascript. Cualquiera que lo pulse ejecutará ese javascript. Acabamos de encontrar un XSS.

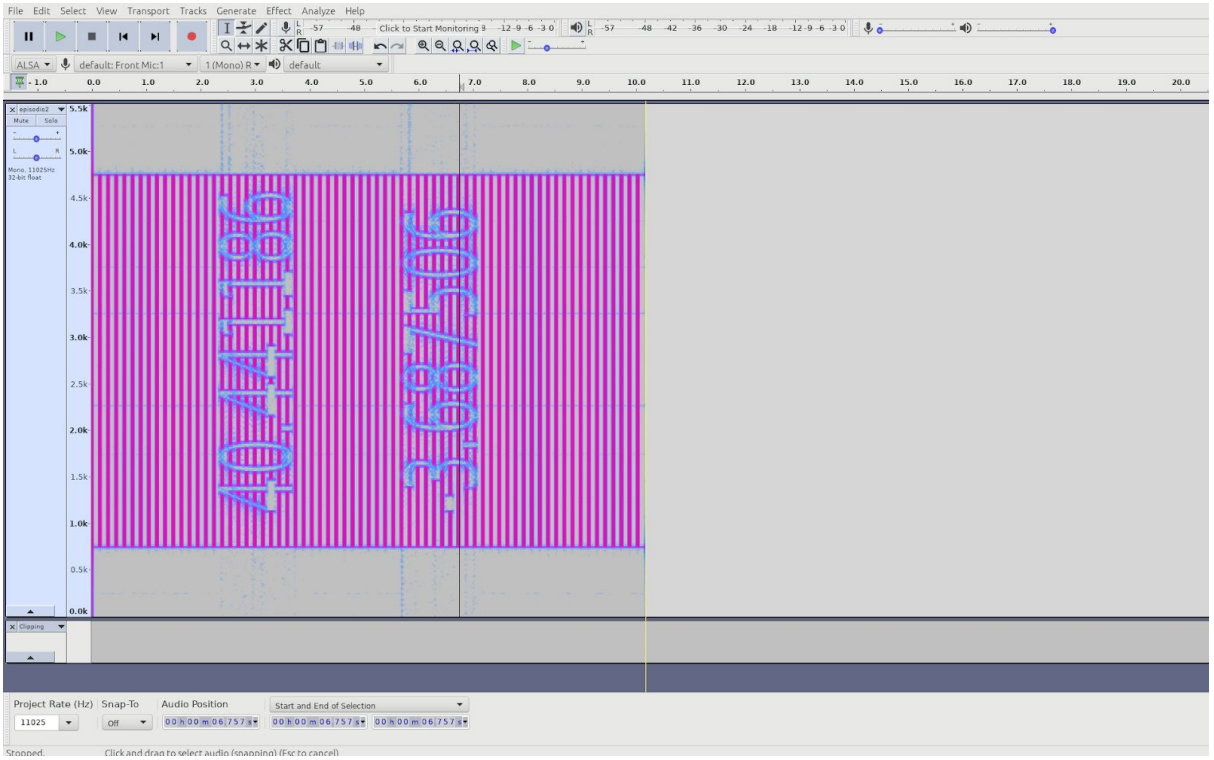
Al pulsar en el botón sale el alert con algo más, que imagino es lo que hace ese javascript ofuscado game-:

Aquí tienes tu password para el zip:

OsLoHaPerDidOaSuPrImo

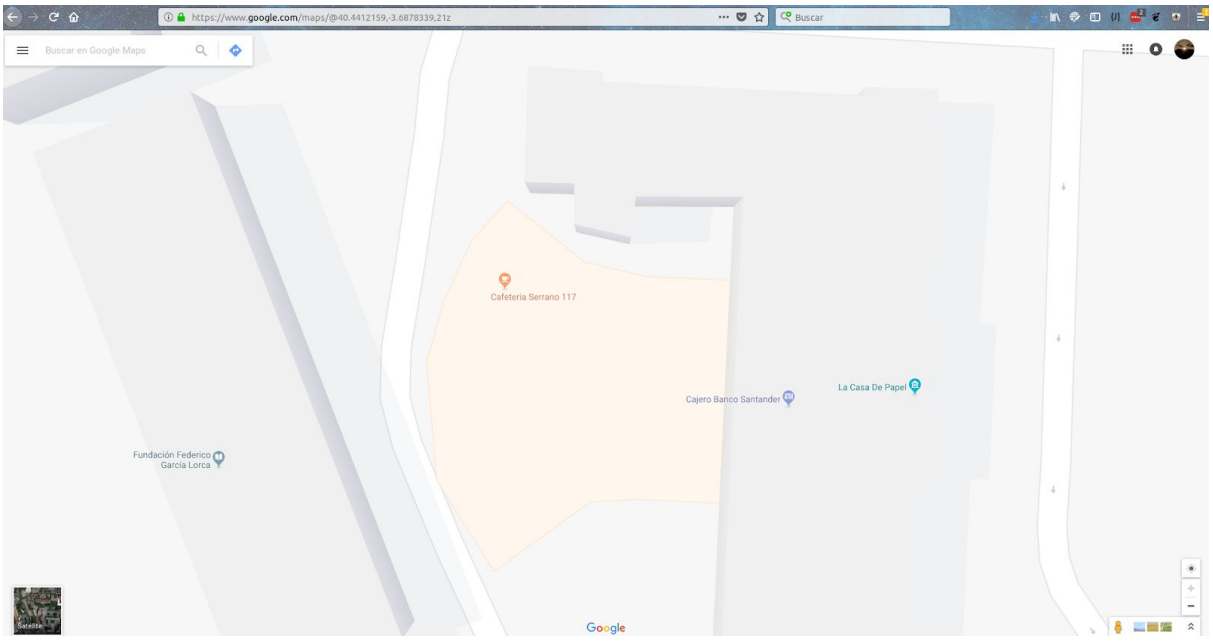
OsLoHaPerDidOaSuPrimo

descomprimios el zip con el password y tenemos un wav con pulsos. Esto me suena. Al ver el espectrograma en audacity vemos esto:


File Edit Select View Transport Tracks Generate Effect Analyze Help
Click to Start Monitoring
ALSA
default: Front Mic:1
1 (Mono) R
default
Project Rate (Hz)
Snap-To
Audio Position
Start and End of Selection
11025
Off
Stopped.
Click and drag to select audio (snapping) (Esc to cancel)

Parecen coordenadas

40.441186
-3.687506



Parece que apunta a la Cafetería Serrano 117

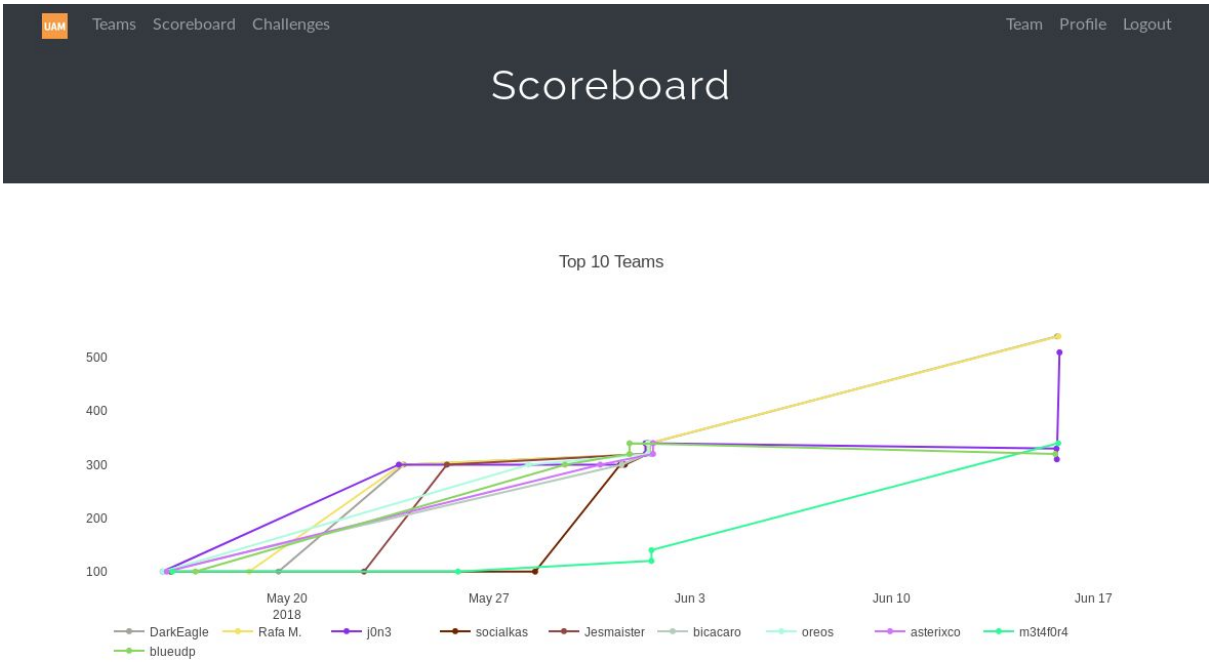
Nos dicen al principio que el archivo contiene la ruta que contiene la flag, y tras probar todo tipo de combinaciones para generar md5 de: Cafeteria Serrano 177,las coordenadas con comas o con puntos, separadas y de todas las formas posibles… consulto con los amos del remo y me confirman que más o menos voy bien peeero… hay que dar un paso atrás… Probaremos con las coordenadas, no con los textos de los lugares adonde apunta.

echo -n 40.441186 -3.687506|md5sum
9bbf31b30acd21df0d35a4d8333b235e

pruebo por enésima vez en la plataforma…

UAM{9bbf31b30acd21df0d35a4d8333b235e}

Correcto!



Place	Team	Score
1	DarkEagle	540
2	Rafa M.	540
3	j0n3	510
4	socialkas	340
5	Jesmaister	340

Un tercer puesto no está mal, aunque debería haber seguido probando cosas de XSS en vez de perder tiempo tratando de entender el código ofuscado en javascript o consumir puntos por las pistas… grr!

De este reto aprendemos lo que es un XSS y por qué debemos evitarlo: Dar la posibilidad a un externo de poner código javascript en nuestras aplicaciones y que cualquier otro usuario pueda ejecutarlo, es un riesgo para todos.

Un saludo!

José Ángel Sánchez
@_j0n3