Una-al-mes: Episodio#1 – Parte II - Hispasec

Enunciado CTF:

Una vez dentro de la caja fuerte, mientras guardábamos el dinero en las bolsas, la puerta se ha cerrado con nosotros dentro. Debéis interaccionar con la consola de la caja fuerte para poder salir de allí.

Consola de la caja fuerte: http://34.247.69.86/lacasadepapel/episodio1/2da_parte.php

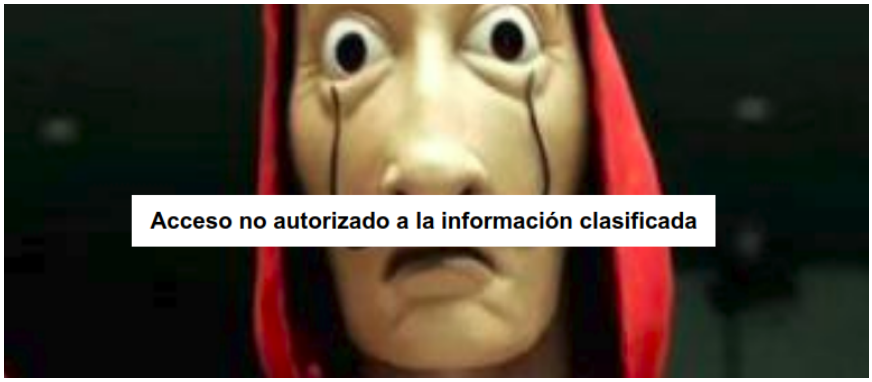
Info: La flag tiene el formato UAM{md5}

También hay un archivo flag.zip que podemos descargar.

Resolución:

Accedemos a la URL que nos facilita el reto:
http://34.247.69.86/lacasadepapel/episodio1/2da_parte.php

Tenemos un formulario en el que nos pide el flag de la parte I. Una vez que lo introducimos, nos aparece el siguiente mensaje en pantalla:



En el código fuente de la página no aparece nada que nos pueda servir de ayuda, pero tenemos una cookie almacenada en nuestro navegador.

Con la extensión para Chrome "Cookie Inspector" vemos el valor de la cookie recibida:

```
acceso=4a7g%3F%5B%5D%40r%25y
```

Con esta cookie, no tenemos acceso autorizado, debemos de averiguar cómo "cocinar" una cookie que nos de acceso a la web con un usuario autorizado.

Los "%" nos dan la pista de que se trata de una codificación URL, por tanto con un URL decode online tenemos lo siguiente:

```
4a7g?[]@r%y
```

Tras probar con algún tipo de cifrado por desplazamiento o también llamado código de César, no tenemos resultados positivos.

Tampoco se trata de un base64, ya que hay caracteres que no se encuentran en su alfabeto.

Probamos con una base superior de las que aparecen en este listado.

Con **base91** obtenemos el valor del flag usando este decodificador online:
https://www.dcode.fr/base-91-encoding
Obteniendo el valor en claro de la cookie: `visitante`

Por tanto, ya sabemos el procedimiento que se ha seguido para crear la cookie:
"visitante" → base91 encode → URL encode → 4a7g%3F%5B%5D%40r%25y

Así que podemos crearnos una cookie para el usuario admin:
"admin" → base91 encode → URL encode → dMLg7%3DA

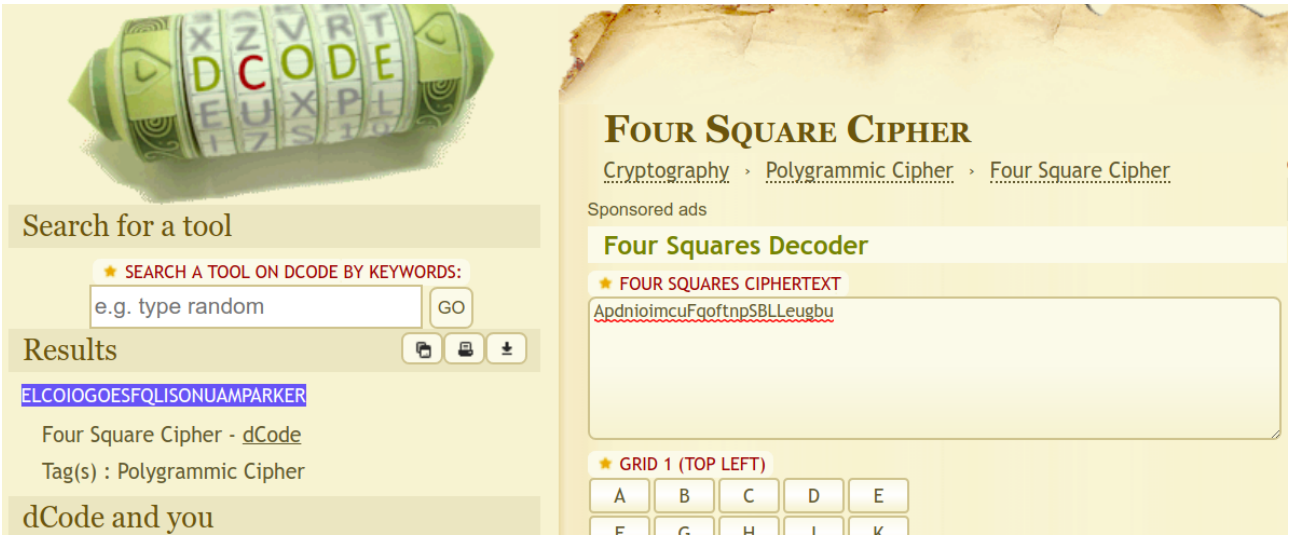
Fijando el valor de la cookie a **acceso=dMLg7%3DA** con la extensión de Chrome "Cookie Inspector", volvemos a hacer la petición a http://34.247.69.86/lacasadepapel/episodio1/2da_parte.php y tenemos el siguiente mensaje por pantalla:

Si probamos ese código para descomprimir el archivo flag.zip vemos que la contraseña es incorrecta, por tanto no está tan "claro".

Se trata de una cadena de 26 letras, con mayúsculas y minúsculas. Son 104 bits. Si miramos un listado de longitud de hash, podemos ver que no corresponde con ninguno.

Probamos con alguno de los cifrados clásicos que aparece en este listado.

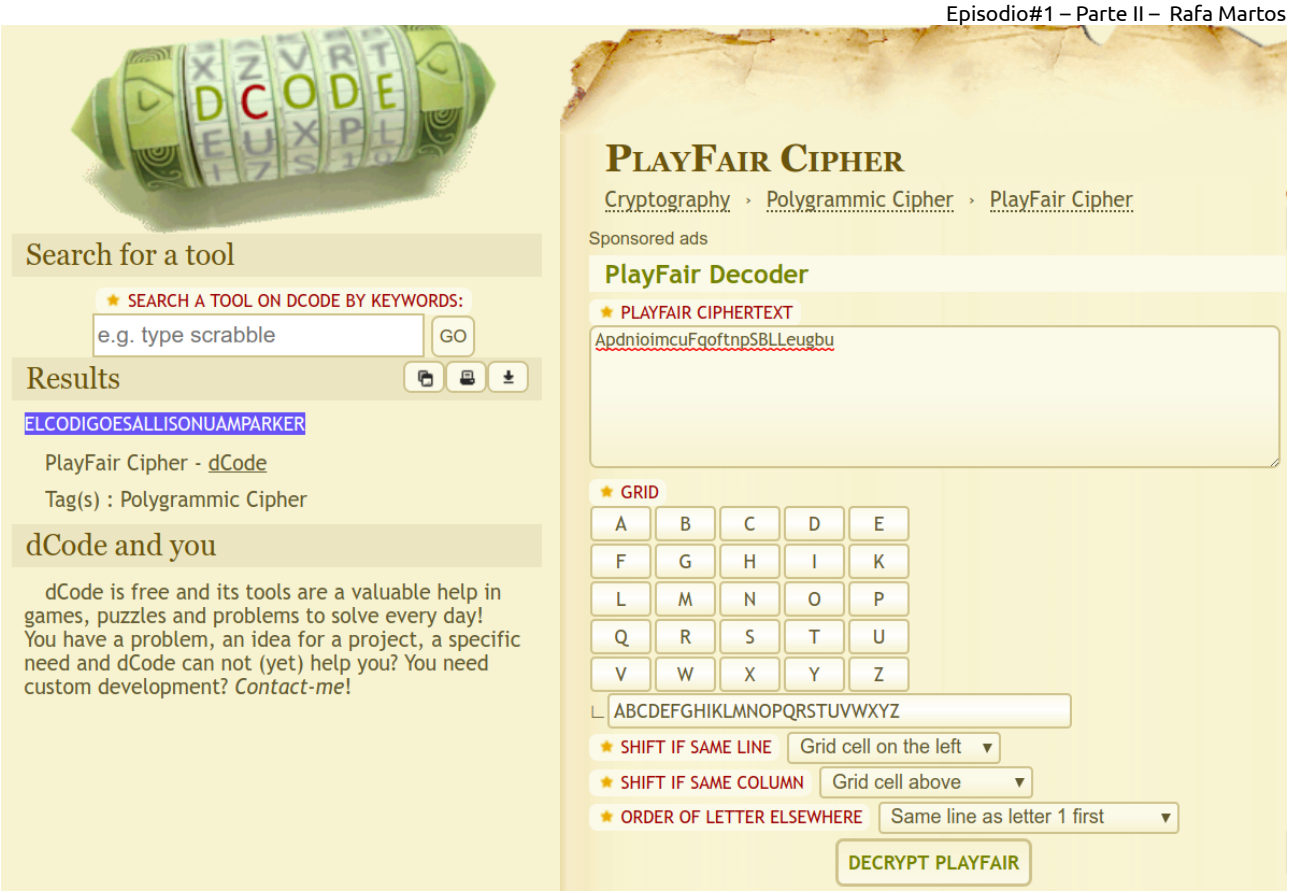
Con el cifrado "Four Square Cipher" obtenemos "casi" el valor del flag: **ELCOIOGOESFQLISONUAMPARKER**



Pero no es correcta. Investigando vemos que el cifrado "Four Square Cipher" es una mejora del cifrado "PlayFair Cipher". Probando con este último, nos da una pista de la posible contraseña del archivo flag.zip.

ELCODIGOESALLISONUAMPARKER

Esta es la web utilizada para realizar la decodificación:
https://www.dcode.fr/playfair-cipher



Probando diferentes combinaciones, obtenemos la contraseña válida para descomprimir el archivo:

```
ELCODIGOESALLISONUAMPARKER  (INCORRECTO)
elcodigoesallisonuamparker  (INCORRECTO)
ALLISONUAMPARKER            (INCORRECTO)
AllisonUAMParker            (CORRECTO)
```

Al descomprimir el archivo, obtenemos un archivo de texto “flag.txt” que contiene el flag:

UAM{c9beec67d71c56a0f9b683fe5232e76e}

Rafa Martos
@elbuenodefali