

## Una-al-mes: La Casa de Papel (Episodio 1 - 2ª Parte)

Una vez dentro de la caja fuerte, mientras guardamos 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](http://34.247.69.86/lacasadepapel/episodio1/2da_parte.php)

Info: La flag tiene el formato UAM{md5}

### Resolución

Accedemos a la página, donde se nos solicita el MD5 de la flag de la primera parte. Una vez introducida, se nos muestra el mensaje “*Acceso no autorizado a la información clasificada*”. Comprobamos con el complemento “EditThisCookie” que se ha generado una cookie “**acceso**” con el valor “**4a7g%3F%5B%5D%40r%25y**”

Decodificamos, acceso = “**4a7g?[]@r%y**”

Contiene caracteres un poco “fuera” de lo común, junto con el el Hint, “una base más alta de lo normal”, probamos con base91 en <https://www.dcode.fr/base-91-encoding> y obtenemos “**visitante**”.

Probamos a modificar la cookie con la palabra “admin” en base91.  
admin = “**dMLg7=A**” y codificando => “**dMLg7%3DA**”

Sustituimos con el mismo complemento por ese valor, refrescamos la página y pasamos a la siguiente prueba. Se nos muestra el texto:

“*El código para descomprimir el zip está claro... ApdnioimcuFqoftnpSBLLeugbu*”

“*ApdnioimcuFqoftnpSBLLeugbu*” 26 caracteres, 208 bits.....

Tras probar con distintas codificaciones (base58, base 91...) y cifrados clásicos (César, Rot47, Vigenere,...) con bastante suerte probamos el de Playfair en:  
<http://rumkin.com/tools/cipher/playfair.php>

y obtenemos “**ElcodigoesAllisonUAMParker**”

Descargamos el zip, ponemos contraseña “**AllisonUAMParker**” y obtenemos la flag.

**UAM{c9beec67d71c56a0f9b683fe5232e76e}**