# Episodio 1 - 2ª Parte

Vamos a la URL que nos dan en la prueba:
http://34.247.69.86/lacasadepapel/episodio1/2da_parte.php

Se nos pide que ingresemos en el formulario el md5 de la prueba anterior y aparece esto:
**Acceso no autorizado a la información clasificada**

Antes de todo .. miro el código fuente de la web, y lo único que veo son las imágenes de backround. Hay una que no se muestra, imagino que será para cuando se nos de el password para descomprimir el zip.
Las analizo con técnicas de esteganografía pero no logro encontrar nada, por lo que el siguiente paso (ya que el código de la web es muy simple y no hay nada más fuera de lo normal) es mirar las cookies.

Veo que antes de meter el md5 no hay ninguna cookie y cuando lo metemos se nos crea una cookie de nombre: acceso y valor 4a7g%3F%5B%5D%40r%25y

Para asegurarme, hago un analisis de la primera parte del episodio 1 para ver que tipo de cookie se creaba, y veo que no tiene ningún tipo de cifrado.

Con un URL decoder http://www.utilities-online.info/urlencode/ obtengo el resultado:
4a7g?[]@r%y

Intento decodificar el valor de muchas formas diferentes .. pero no doy con la clave … no se parece a nada que me suene …

Gracias al HINT que se da de que necesitamos una “base” más alta de lo normal .. rapidamente entiendo que tiene que ser una base > 64 por lo que empiezo a buscar codificaciones de este tipo.
El tipo de codificacion utilizada es base91 y utilizo https://www.dcode.fr/code-base-91 para decodificarla. El resultado es: visitante

Con la extensión de google Chrome EditThisCookie y codificando varias palabras que se me ocurren voy cambiando el valor encriptado en base91. Pruebo con administrador, usuario, user, … admin que cifrado queda tal que asi: dMLg7=A
Al recargar la web tenemos el premio:
**El codigo para descomprimir el zip está claro...**
**ApdnioimcuFqoftnpSBLLeugbu**

El problema es que .. no está tan claro … en este punto estoy un poco perdido ya que la cadena ApdnioimcuFqoftnpSBLLeugbu no me dice mucho … busco muchísimas webs con

infinidad de algoritmos de encriptación distintos …  prueba y error, encuentro que en http://rumkin.com/tools/cipher/playfair.php me aparece el mensaje con sentido.

**ElcodigoesAllisonUAMParker**

Descomprimimos con el código: **AllisonUAMParker**
Una vez descomprimido tenemos el fichero flag.txt .. miro que hay en el interior .. y cuando pensaba que habría alguna otra codificación … estaba el md5 en claro:
**UAM{c9beec67d71c56a0f9b683fe5232e76e}**