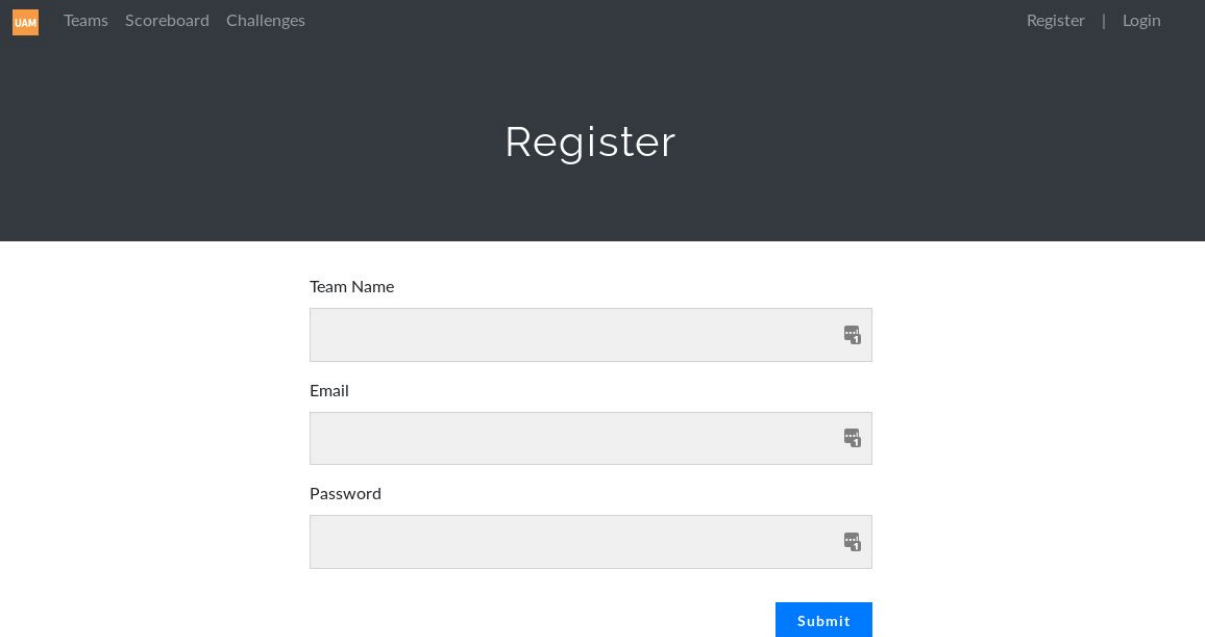


Mission 7 o... Episodio 1 - parte 1

<https://unaaldia.hispasec.com/2018/05/una-al-mes-mayo-lavado-de-cara-y.html>

Esta vez tenemos que registrarnos en la plataforma. ¡Qué buena pinta!



The screenshot shows a web page for registration. At the top, there is a dark header with the UAM logo on the left and navigation links 'Teams', 'Scoreboard', and 'Challenges' in the center. On the right side of the header are links for 'Register' and 'Login'. The main content area has a dark background with the word 'Register' in large white text. Below this, there are three input fields: 'Team Name', 'Email', and 'Password'. Each field has a small icon of a person with a plus sign on the right side. At the bottom right of the form is a blue 'Submit' button.

UAM Teams Scoreboard Challenges Register | Login

Register


Team Name

Email

Password

Submit

Como parece que se podrán hacer equipos lo nombro SPC, y una vez registrados accedemos al reto.

 Teams Scoreboard Challenges

Challenge0 Solved

EPISODIO 1100

Hemos conseguido entrar en la Fábrica Nacional de Moneda y Timbre. Pero una vez dentro, la lanza térmica que usáramos para abrir la caja fuerte se ha roto. Debes descubrir los códigos para abrirla, y con ello conseguirás la contraseña para el zip del programa que genera la flag y el dinero ;).

Caja fuerte: <http://34.253.233.243/lacasadepapel/episodio1/puerta.php>

Info: La flag tiene el formato UAM{md5}

TOP 3:

episodio1.zip

Flag

Submit

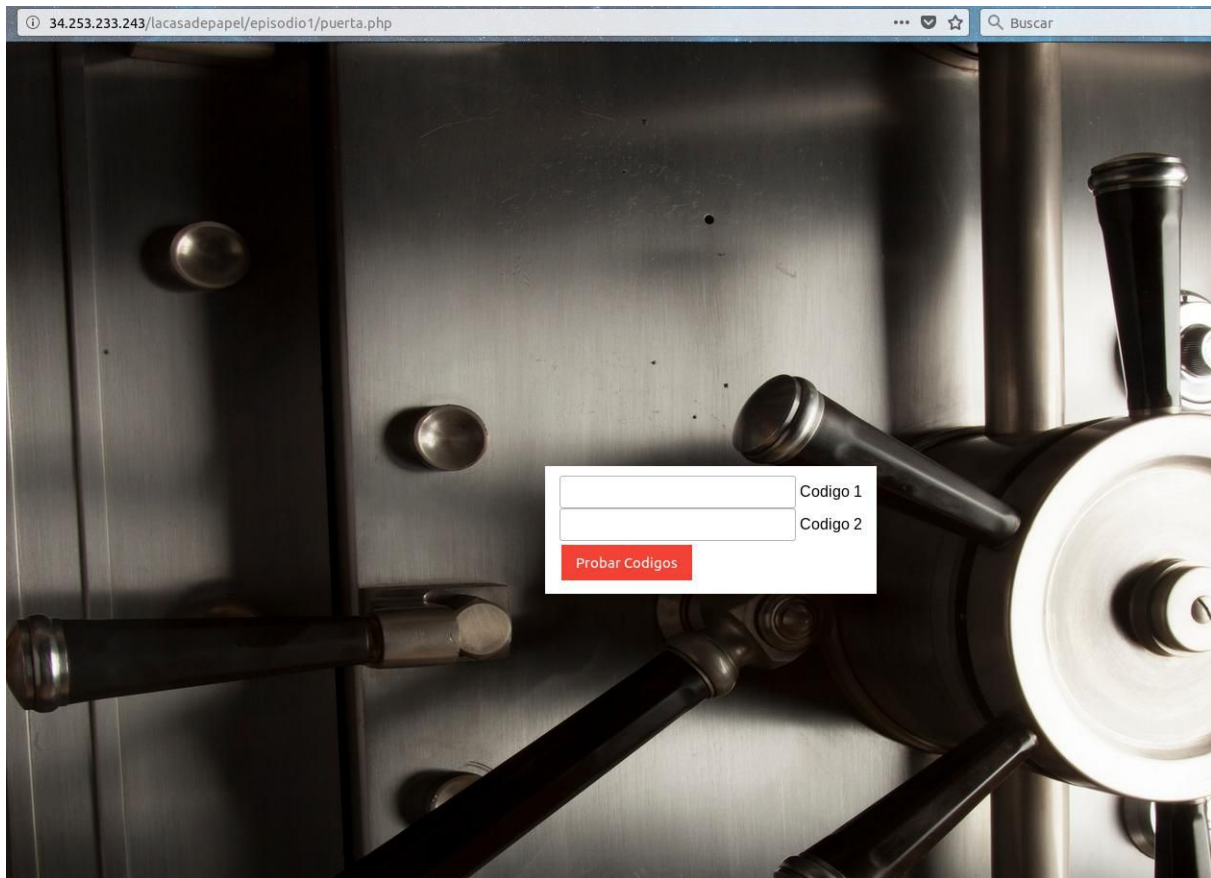
LA CASA DE PAPEL

EPISODIO 1100

Bajamos el zip y está protegido con contraseña.

Vamos a ver qué hay en esa url: <http://34.253.233.243/lacasadepapel/episodio1/puerta.php>

Encontramos un login y password



Vemos en el código fuente de la página que incluye un javascript: login.js

```
1 <html>
2   <head>
3     <title>Apertura con codigo</title>
4     <script language="JavaScript" src="login.js"></script>
5     <style>
6     body {
7       background-image: url("images/background.jpg");
8       background-size: 1920px 1080px;
9     }
10    form {
11      position: absolute;
12      top: 45%;
13      left: 800px;
14      background-color: #FFFFFF;
15      padding: 10px 15px;
```

Ese login.js contiene esto:

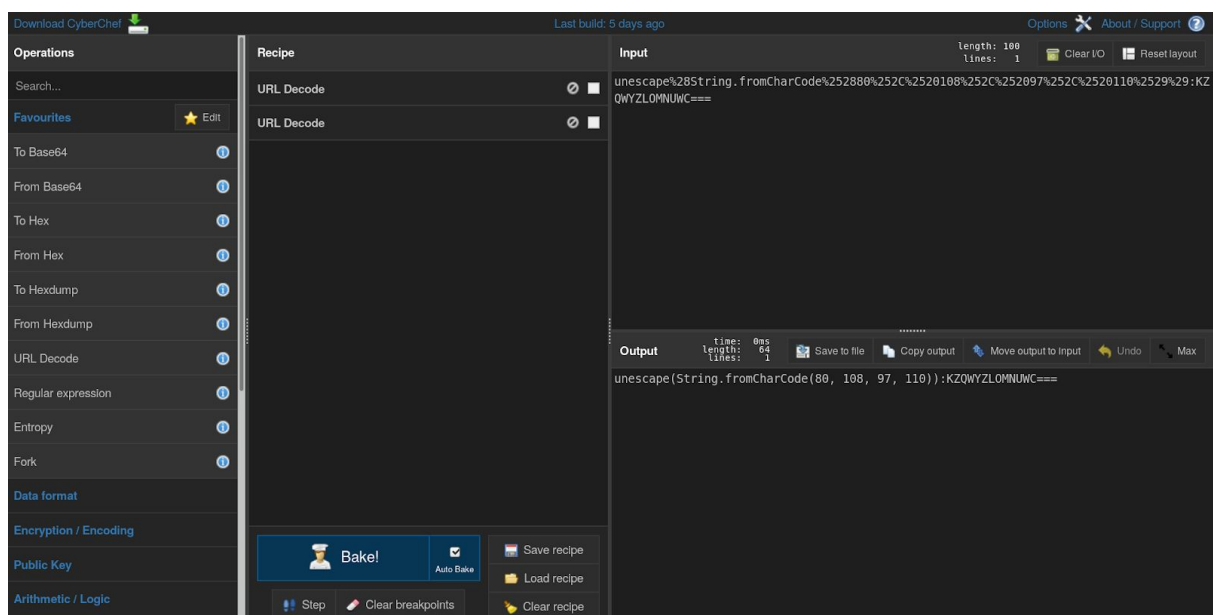
```

/*
function conexion(){
  var Password = "unescape%28String.fromCharCode%252880%252C%2520108%252C%252097%252C%2520110%2529%29:KZQWYZLOMNUWC===";
  for (i = 0; i < Password.length; i++)
  {
    if (Password[i].indexOf(code1) == 0)
    {
      var TheSplit = Password[i].split(":");
      var code1 = TheSplit[0];
      var code2 = TheSplit[1];
    }
  }
}
*/

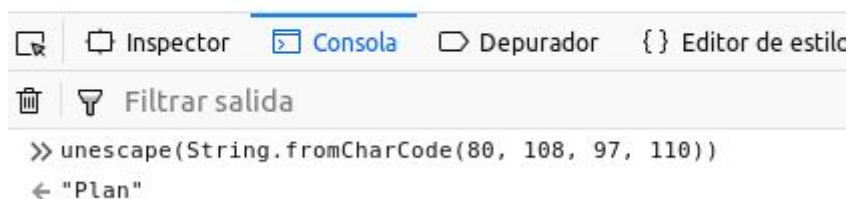
```

Por lo que parece se compone de dos partes separadas por un punto y coma:

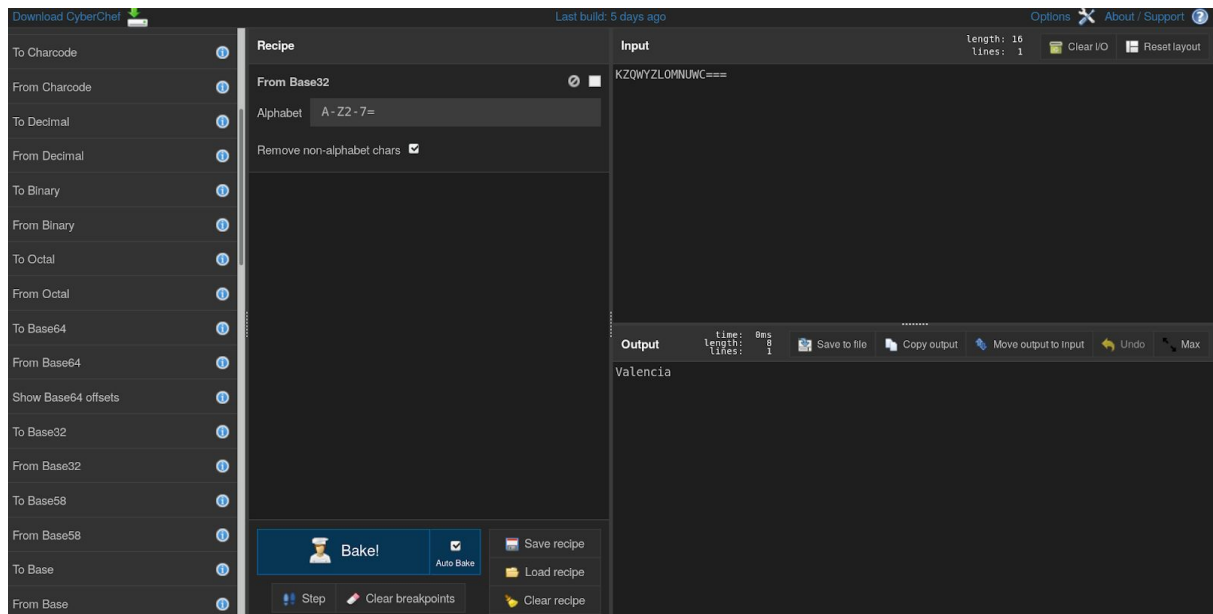
Parecen [URLDecode](#) y [Base32](#). Uso [CyberChef](#) para decodificarlo. Con dos decodificaciones de URL obtenemos la función javascript que oculta el texto:



Ejecutamos la función en la consola del navegador y encontramos la primera clave: Plan



Después de jugar un poco con la otra parte vi que era un base32: Valencia



Introducimos ambas claves en el formulario

Código 1: Plan

Código 2: Valencia



Vamos a usar esta clave para descomprimir el archivo.

Aparece un ejecutable: episodio1.exe

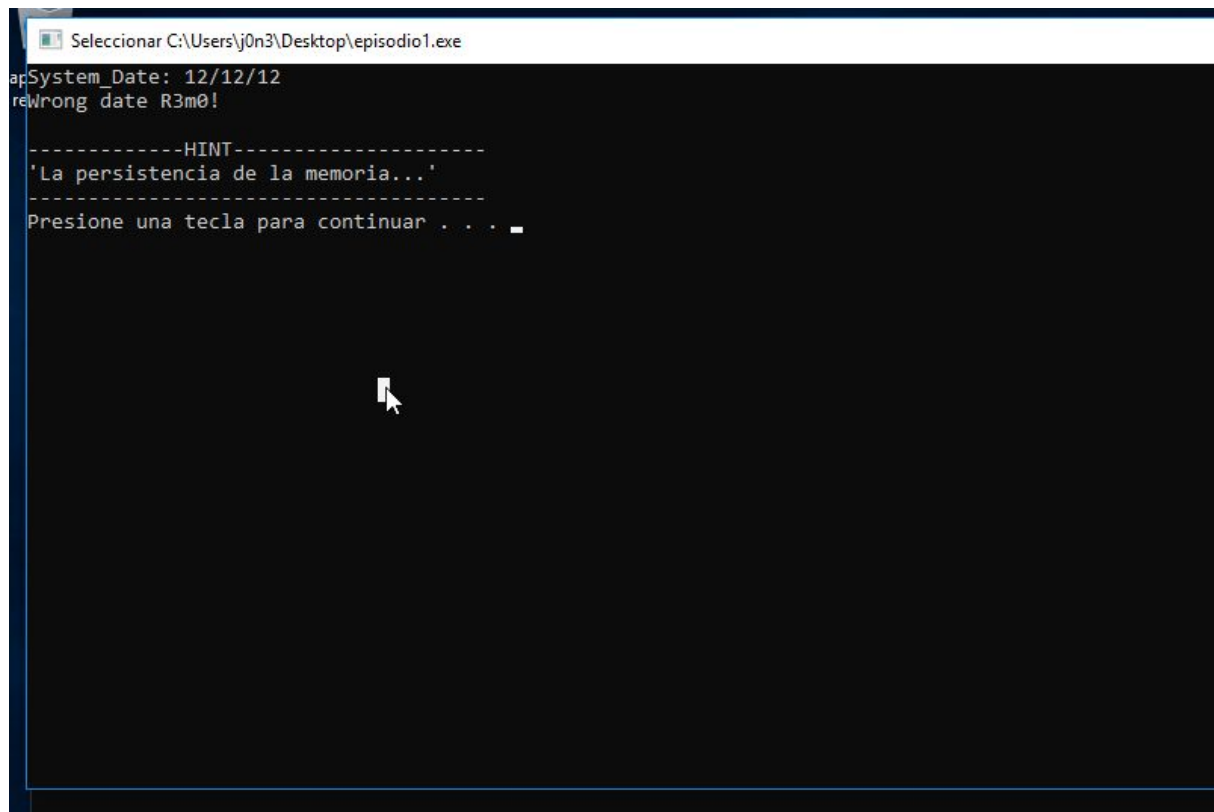
hago un strings a episodio1.exe y en un minuto y con un poco de paciencia encuentro esto:

```
QZ^&
01/23/89
Congratulation!! , Stealing Money $$$...
-----
Stolen: 1.000.000.000 $
Flag:
-----
System_Date:
Wrong date R3m0!
-----HINT-----
'La persistencia de la memoria...'
-----
pause
0123456789abcdef
%s: __pos (which is %zu) > this->size() (which is %zu)
basic_string::at: __n (which is %zu) >= this->size() (which is %zu)
basic_string::copy
basic_string::compare
basic_string::_S_create
basic_string::erase
basic_string::_M_replace_aux
basic_string::insert
basic_string::replace
```

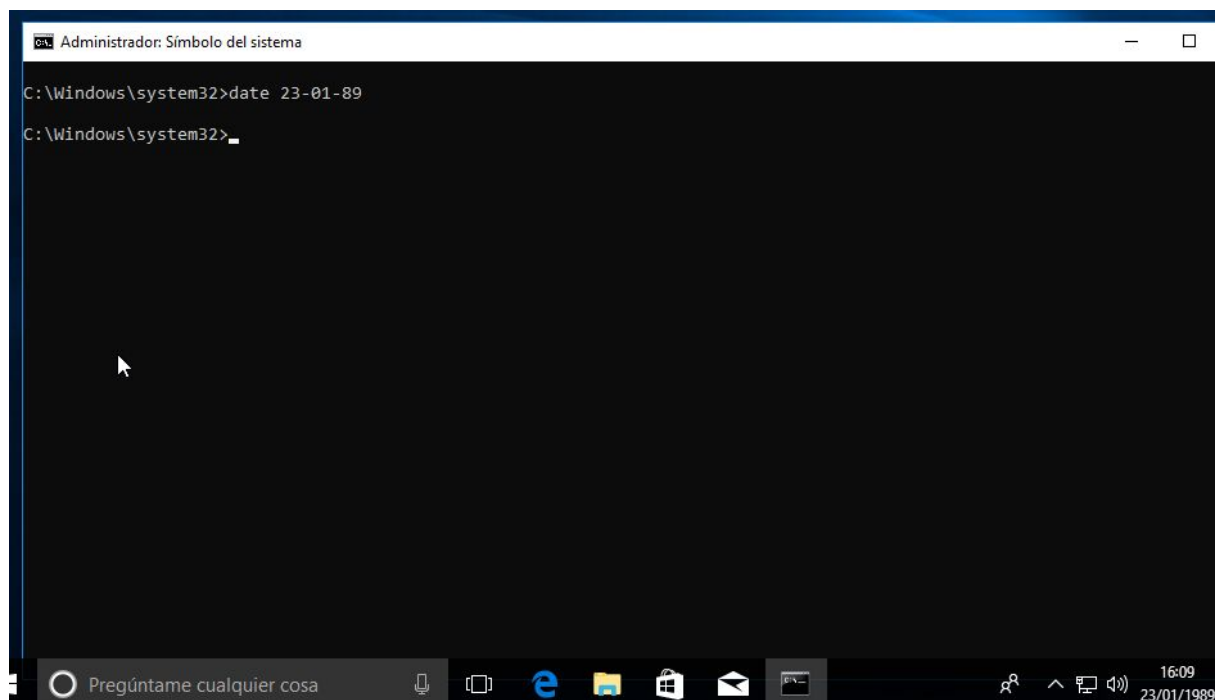
Esa fecha de arriba parece un poco sospechosa, 01/23/89... Además parece que tenemos alguna pista sobre lo que tendremos que hacer, System_Date: Wrong date R3m0!

Con wine no he conseguido hacerlo funcionar así que me he instalado una máquina virtual con un Windows.

al ejecutar episodio1.exe con una fecha cualquiera



Ponemos nuestra sospechosa fecha al sistema y volvemos a ejecutarlo



```
C:\Users\j0n3\Desktop\episodio1.exe

Congratulation!!, Stealing Money $$$...
-----
Stolen: 1.000.000.000 $
-----
Flag: e30f35ad8d9cb6efc0778539a669fa85
.....
Presione una tecla para continuar . . .
```

flag = UAM{e30f35ad8d9cb6efc0778539a669fa85}

Ponemos la flag en la plataforma y...

Challenge 2 Solved

EPISODIO 1

100


Hemos conseguido entrar en la Fábrica Nacional de Moneda y Timbre. Pero una vez dentro, la lanza térmica que usaríamos para abrir la caja fuerte se ha roto. Debes descubrir los códigos para abrirla, y con ello conseguirás la contraseña para el zip del programa que genera la flag y el dinero ;).

Caja fuerte: <http://34.253.233.243/lacasadepapel/episodio1/puerta.php>

Info: La flag tiene el formato UAM{md5}

TOP 3:

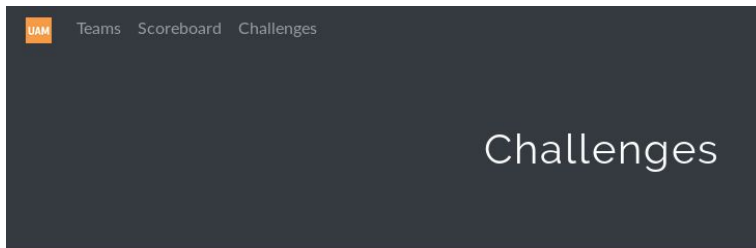
1. SPC
2. cukz

 episodio1.zip

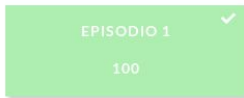
Submit

¡Bingo! ¡y primer puesto!

Ya aparece como resuelto



LA CASA DE PAPEL

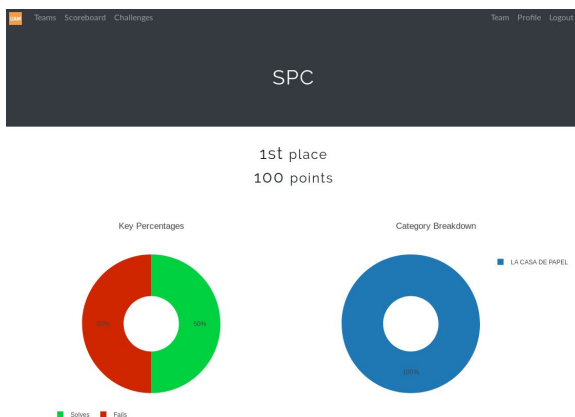


Como extra, si buscamos la flag en crackstation veremos que encuentra un resultado...



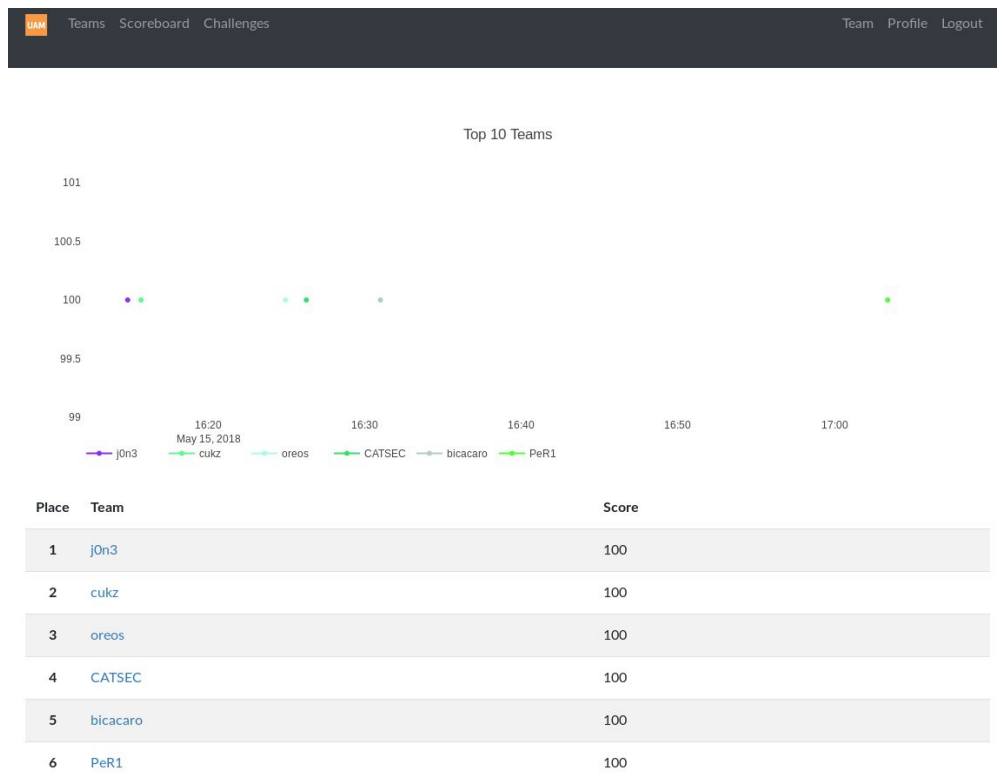
La flag es el md5 de la fecha, que es lo primero que probé UAM{01/23/89} :)

Por eso luego veo en el perfil de la plataforma el intento fallido:



Lástima no haber probado primero la flag en crudo :/ no me fijé bien y el formato era UAM{md5}

Tras un cambio de nombre...



Esperemos que con ayuda de la plataforma haya muchos más retos. Sin duda ha sido una buena idea.

¡Muchas gracias por hacernos pasar tan buen rato y espero que haya más pronto!

José Ángel Sánchez
@_j0n3