

Vamos a resolver el reto de hispasec. Mission 004. Febrero 2018

<http://unaaldia.hispasec.com/2018/02/una-al-mes-mision004.html>

<http://34.253.233.243/mission4.php>



Misión#004

Información personal:

Nombre: Fry
Fecha de nacimiento: 14 de Agosto del 1974
Trabajo: Repartidor
Empresa: Planet Express



Misión:

Nivel: Difícil

Introducción:

Hola Fry, ¿te acuerdas de tu cuenta de usuario de Planet Express?. Necesitas entrar en ella para arreglar el programa de la nave y seguir repartiendo los paquetes. Recuerda que mientras el código del ".exe" sea erróneo, se escuchará la música de un juego clásico. Y cuando sea correcto, escucharás una música característica y te devolverá un string. ¡Date prisa o el profesor Farnsworth te echará la bronca!

Información adicional:

URL del login: <http://34.253.233.243/inicio.php>

Tip: Ejecutad el programa directamente desde consola.

Vamos a la página

<http://34.253.233.243/inicio.php>

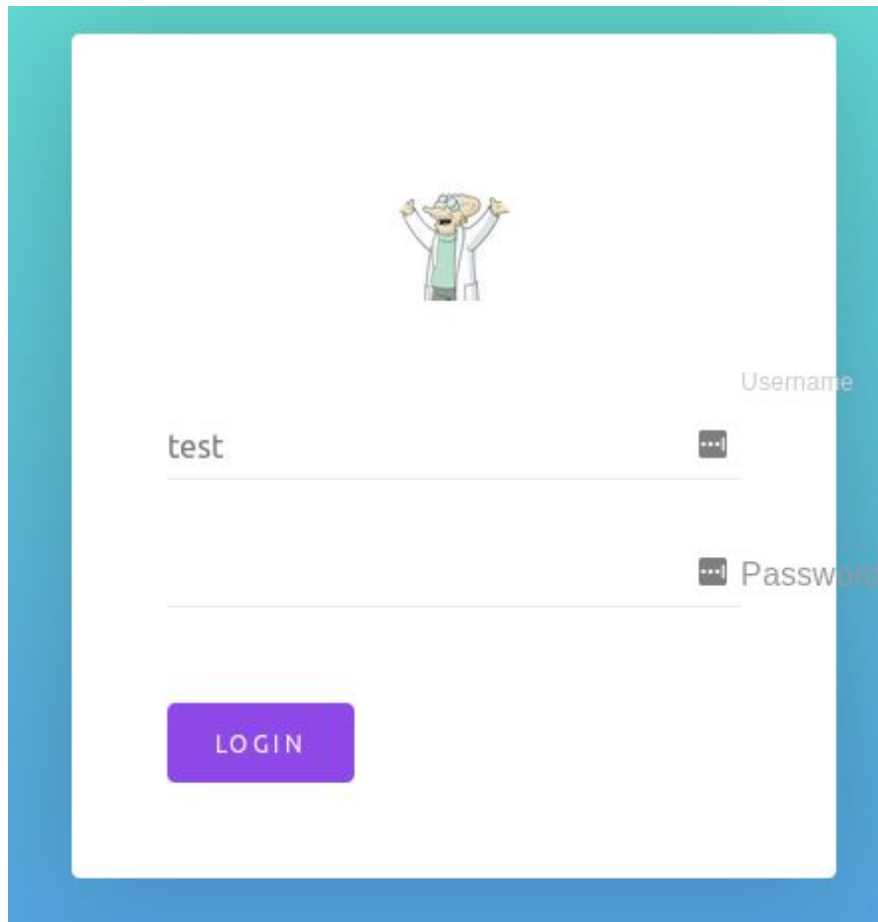


**Este no es el navegador
oficial de Planet
Express**

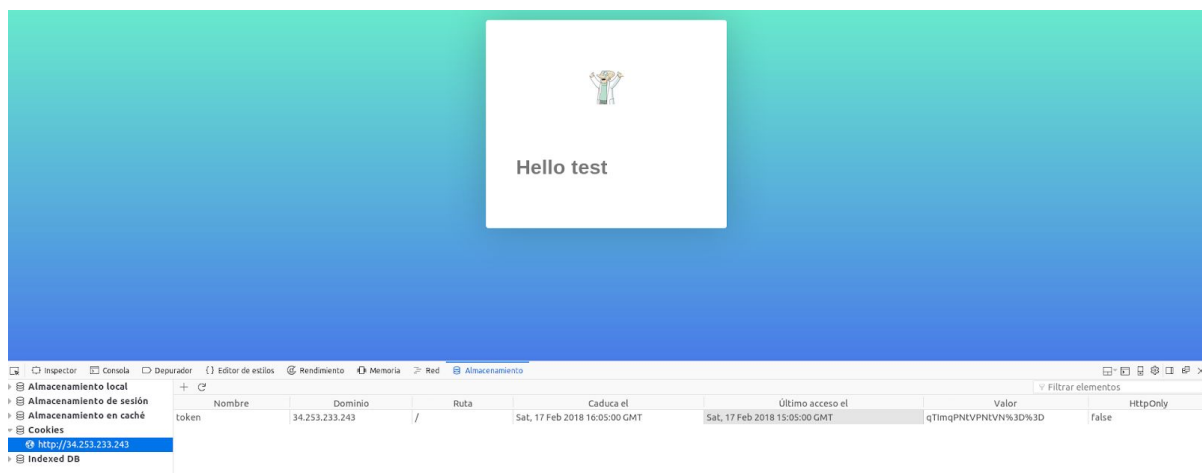
Probando unos cuantos vemos que al menos funciona con este:

TC-8500/1.2 Mozilla/4.0 (compatible; MSIE 5.5; Windows CE; PPC; 240x320)

Nos muestra un formulario con el usuario test ya escrito



Probamos con
username: test
password: test



Vemos que nos genera una cookie:

token value qTImqPNtVPNtVN%3D%3D

Buscando herramientas por ahí encuentro lo que es qTImqPNtVPNtVN==

[https://gchq.github.io/CyberChef/#recipe=From_Base64\('N-ZA-Mn-za-m0-9%2B/%3D',true\)&input=cVRJbXFQTnRWUE50Vk49PQ](https://gchq.github.io/CyberChef/#recipe=From_Base64('N-ZA-Mn-za-m0-9%2B/%3D',true)&input=cVRJbXFQTnRWUE50Vk49PQ)

The screenshot shows the CyberChef web application. The interface is divided into several sections:

- Operations:** A sidebar on the left with a search bar and a list of operations including 'To Base64', 'From Base64', 'To Hex', 'From Hex', 'To Hexdump', 'From Hexdump', 'URL Decode', 'Regular expression', 'Entropy', and 'Fork'. There are also sections for 'Data format', 'Encryption / Encoding', 'Public Key', and 'Arithmetic / Logic'.
- Recipe:** The central panel shows a recipe named 'From Base64'. The 'Alphabet' is set to 'N-ZA-Mn-za-m0-9+/' and 'Remove non-alphabet chars' is checked. At the bottom, there are buttons for 'Bake!', 'Auto Bake', 'Save recipe', 'Load recipe', 'Clear recipe', 'Step', and 'Clear breakpoints'.
- Input:** The top right panel shows the input text 'qTImqPNtVPNtVN=='. It includes statistics: length: 16, lines: 1. Buttons for 'Clear I/O' and 'Reset layout' are present.
- Output:** The bottom right panel shows the output 'test'. It includes statistics: time: 3ms, length: 10, lines: 1. Buttons for 'Save to file', 'Copy output', 'Move output to input', 'Undo', and 'Max' are present.

Base64+ROT13

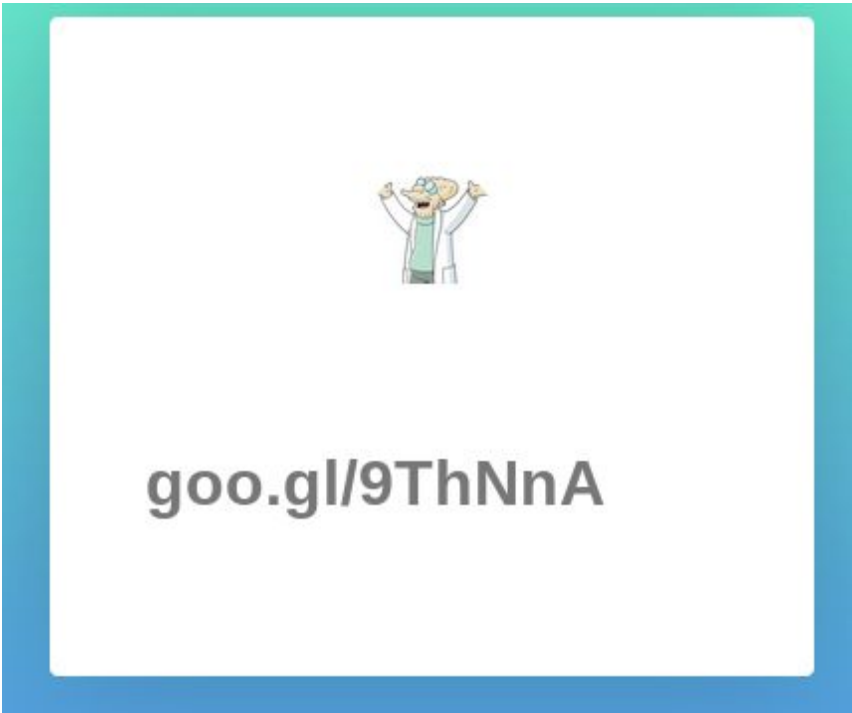
probemos con el usuario fry

This screenshot shows the CyberChef web application with a different recipe and input. The 'Recipe' panel is set to 'To Base64' with the same alphabet 'N-ZA-Mn-za-m0-9+/' and 'Remove non-alphabet chars' checked. The 'Input' panel now contains the text 'fryl'. The 'Output' panel shows the result 'MaW5'. The interface elements and sidebar are consistent with the previous screenshot.

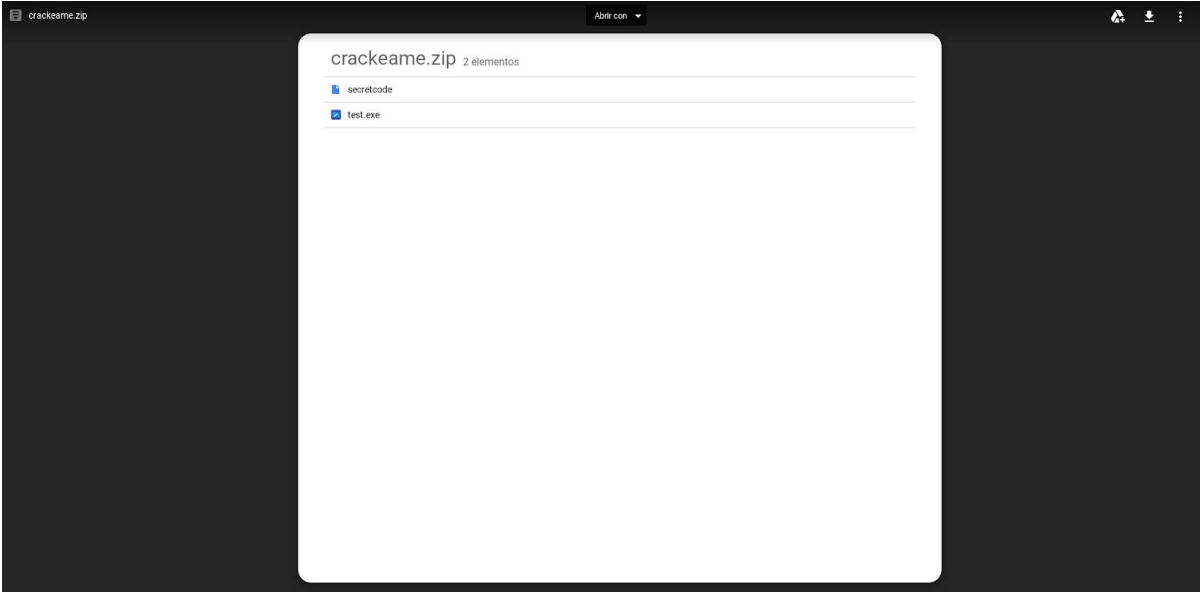
test = "qTImqPNtVPNtVN=="
fry = "MaW5"

cambiando el valor de la cookie token a MaW5

Almacenamiento							
Filtrar elementos							
Nombre	Dominio	Ruta	Caduca el	Último acceso el	Valor	HttpOnly	
token	34.253.233.243	/	Sat, 17 Feb 2018 16:05:00 GMT	Sat, 17 Feb 2018 15:09:23 GMT	MaW5	false	



goo.gl/9ThNnA



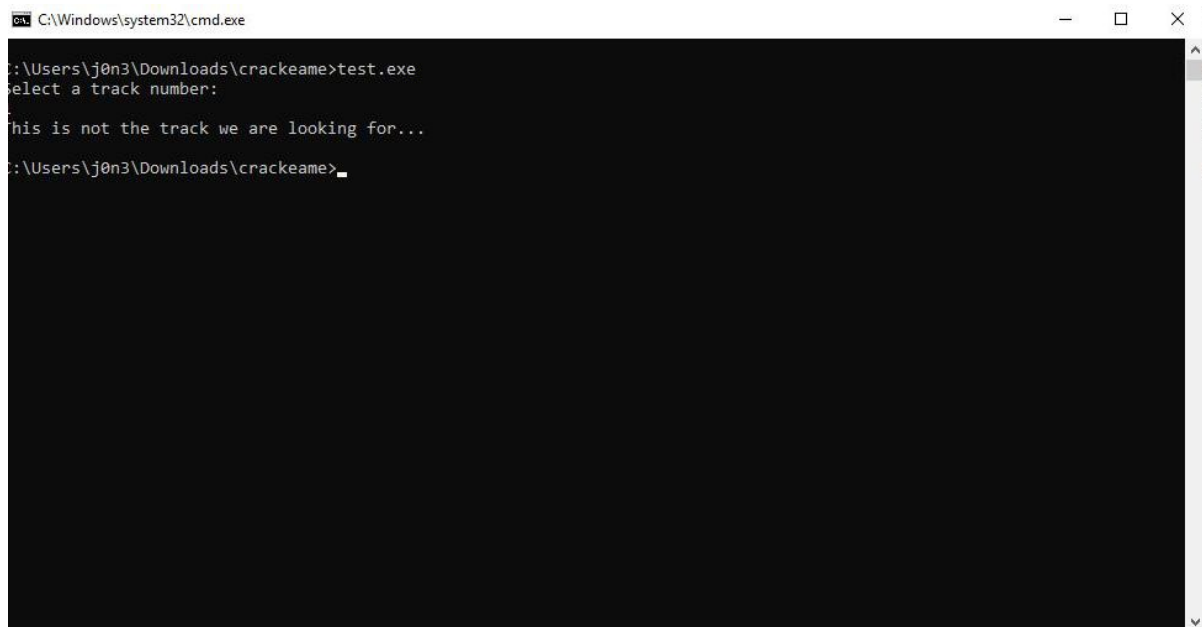
secretcode

!7H.^M6:DkZ?-K7kl3P,)*4wG%

???

datos encriptados?

test.exe

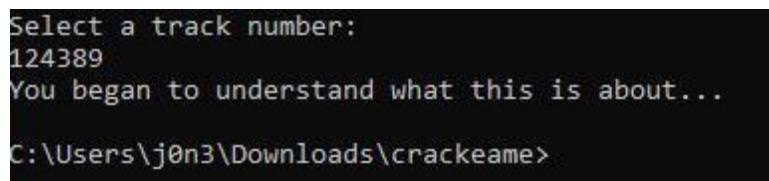


```
C:\Windows\system32\cmd.exe

C:\Users\j0n3\Downloads\crackeame>test.exe
select a track number:
this is not the track we are looking for...
C:\Users\j0n3\Downloads\crackeame>
```

Nos pide una entrada. Con los números del 1 al 9 suena la canción de mario.

Con otros números sale



```
Select a track number:
124389
You began to understand what this is about...
C:\Users\j0n3\Downloads\crackeame>
```

Probando cosas al azar di con 101 y resolví el reto, pero mirando con ida podemos verlo:

Reversing de test.exe (ida)

```

puts("Select a track number:");
scanf("%d", &v4);
v10 = 30;
if ( v4 > 9 )
{
    if ( v4 <= 10 || v4 >= v10 )
    {
        if ( v4 == 101 )
        {
            v3 = 0;
            Str2[0] = 102;
            Str2[1] = 117;
            Str2[2] = 116;
            Str2[3] = 117;
            Str2[4] = 114;
            Str2[5] = 97;
            Str2[6] = 109;
            Str2[7] = 97;
            cool_melody();
            puts("This song is very familiar, where does it come from?");
            scanf("%39s", &Str1);
            result = strcmp(&Str1, Str2);
            v9 = result;
            if ( result <= 0 )
            {
                v8 = "secretcode";
                v7 = readFile("secretcode");
                v6 = "tvB3Cj4iNxxw4rjMNxhmX3DaXAuMG2e";
                v5 = decrypt(v7, "tvB3Cj4iNxxw4rjMNxhmX3DaXAuMG2e");
                printf("%s", v5);
                result = 0;
            }
        }
    }
}

```

Vemos cómo trata la entrada. Espera que sea 101.

```

if ( v4 == 101 )
{
    v3 = 0;
    Str2[0] = 102;
    Str2[1] = 117;
    Str2[2] = 116;
    Str2[3] = 117;
    Str2[4] = 114;
    Str2[5] = 97;
    Str2[6] = 109;
    Str2[7] = 97;
    cool_melody();
    puts("This song is very familiar, where does it come from?");
    scanf("%39s", &Str1);
    result = strcmp(&Str1, Str2);
    v9 = result;
    if ( result <= 0 )
    {
        v8 = "secretcode";
        v7 = readFile("secretcode");
        v6 = "tvB3Cj4iNxxw4rjMNxhmX3DaXAuMG2e";
        v5 = decrypt(v7, "tvB3Cj4iNxxw4rjMNxhmX3DaXAuMG2e");
        printf("%s", v5);
    }
}

```

Cuando metemos 101 en el número de track, suena la música de futurama y nos pregunta.

Si le respondemos 'futurama' descripta el fichero secretcode y ya tenemos el flag :)

```
Select a track number:
101
This song is very familiar, where does it come from?
futurama
UAM{m4y_th3_f0rc3_b3_w1th_y0u}
```

Saludos!

Herramientas usadas:

Firefox y algo de suerte :)

Ida

José Ángel Sánchez.

@_j0n3

