Write up La casa de papel

Alejandro Parras

EPISODIO 1 - 1ª PARTE

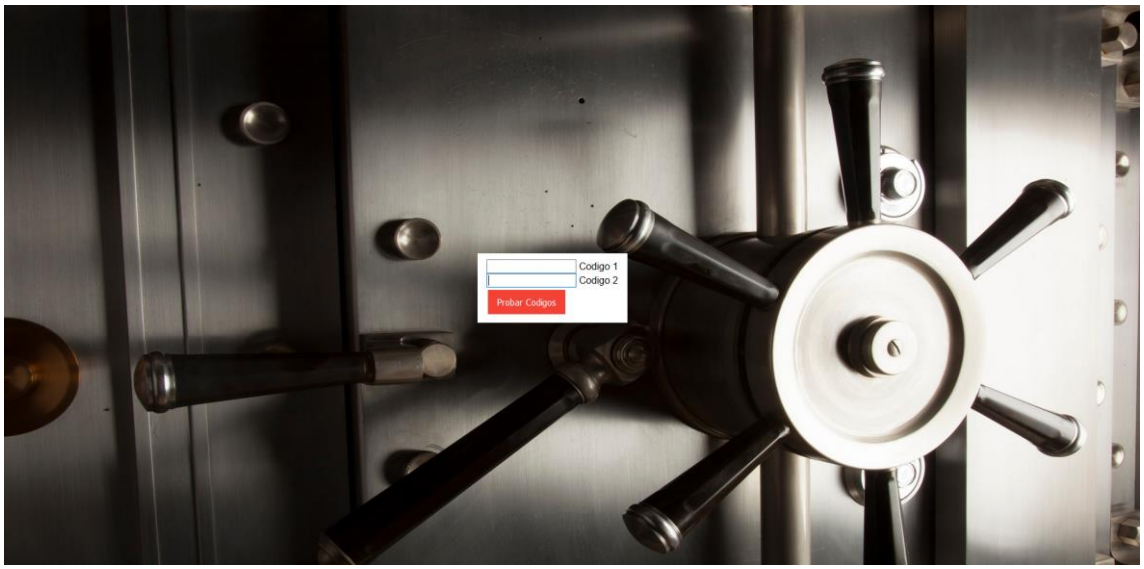
Hemos conseguido entrar en la Fábrica Nacional de Moneda y Timbre. Pero una vez dentro, la lanza térmica que usaríamos para abrir la caja fuerte se ha roto. Debes descubrir los códigos para abrirla, y con ello conseguirás la contraseña para el zip del programa que genera la flag y el dinero ;).

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

Info: La flag tiene el formato UAM{md5}

¡Empezamos!

Accedo a la URL que aparece en la descripción del reto. En ésta encuentro un login que nos devolverá la pass para poder descomprimir la siguiente parte del reto.



Primero echo un vistazo al código usando **Ctrl + u**.

Aparentemente no hay nada, aunque si sigues bajando te encuentras con esto:

```
<! --
Soy mas de 1234/1234 que de admin/admin
-->
</html>
```

Al probar, "*código 1: 1234; código 2: 1234*", no consigo acceder y aparece un mensaje en la parte superior de la web: "*No todo es lo que parece... Hay cosas que pueden llevar a confusion. Debes fijarte en los pequeños detalles*".

Vuelvo a mirar el código y esta vez entro en **login.js**. Me encuentro con 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];
    }
}

*/
```

El código está comentado y en la variable password pueden distinguirse dos posibles pass separadas por ":" por lo que se intuye lo siguiente:

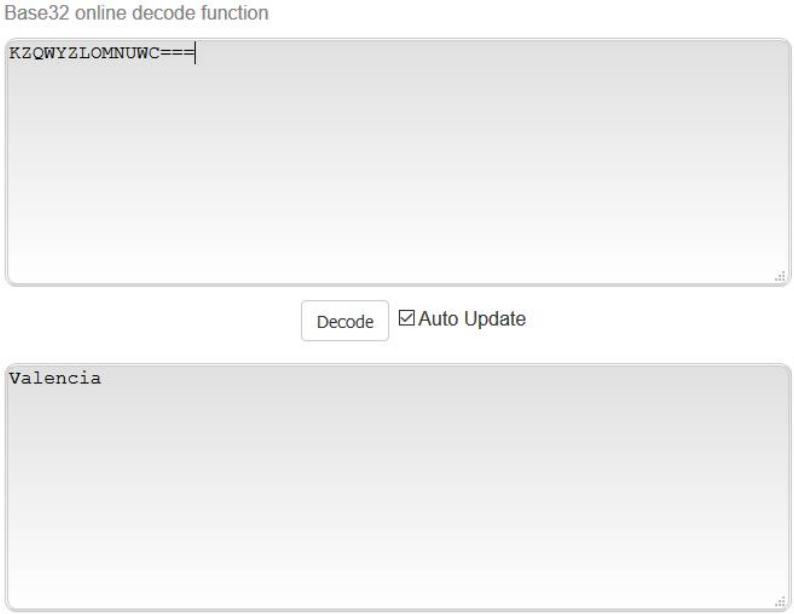
Codigo1:
unescape%28String.fromCharCode%252880%252C%2520108%252C%252097%252C%2520110%2529%29

Codigo2: KZQWYZLOMNUWC===

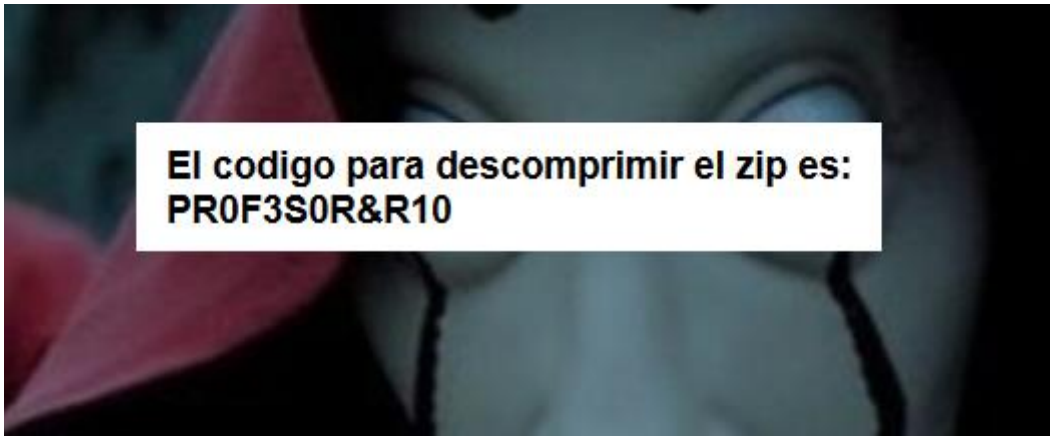
Para descifrar el codigo1 abro la consola web y escribo:

```
» unescape("unescape%28String.fromCharCode%252880%252C%2520108%252C%252097%252C%2520110%2529%29")
← "unescape(String.fromCharCode%2880%2C%20108%2C%2097%2C%20110%29)"
» unescape("String.fromCharCode%2880%2C%20108%2C%2097%2C%20110%29")
← "String.fromCharCode(80, 108, 97, 110)"
» String.fromCharCode(80, 108, 97, 110)
← "Plan"
```

Para descifrar codigo2 me llevó algo más de tiempo, pensé en algún cifrado mixto que incluyese base 64 pero tras herrar varias veces tuve que tirar de otro tipo de cifrado. Investigando un poco encontré algo que se le parecía y probé con base32.



Ya tenía el segundo código. Ahora los introduzco en la web y me devuelve la pass para descomprimir el archivo que se descarga desde la plataforma:



Al descomprimir el archivo lo primero que hago es ejecutarlo. Se muestra de la siguiente manera:

```
System_Date: 05/19/18
Wrong date R3m0!

-------------HINT---------------------
'La persistencia de la memoria...'
--------------------------------------
Presione una tecla para continuar . . .
```

Abro **processHacker** mientras ejecuto el programa para ver las strings. Accedo a memoria, strings… y tras la pista del formato de la flag, UAM{md5}, busco los strings con tamaño mínimo 32 y el resultado es el siguiente:

0x28786c0	190	^gcc-shmem-tdm2-once_obj_shmem-aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaAaAAaAaAAaaaaAaAaaAAaAa
0x28787a0	208	ggcc-shmem-tdm2-_pthread_tls_once_shmem-aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaAaAAaAaAAaaaaAaAaaAAaA
0x2878890	198	bgcc-shmem-tdm2-_pthread_tls_shmem-aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaAaAAaAaAAaaaaAaAaAAA
0x28789c0	212	igcc-shmem-tdm2-mutex_global_static_shmem-aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaAaAAaAaAAaaaaAaAaAAaA
0x2879320	206	fgcc-shmem-tdm2-mxattr_recursive_shmem-aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaAaAAaAaAAaaaaAaAaAa
0x28797d0	204	egcc-shmem-tdm2-mtx_pthr_locked_shmem-aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaAaAAaAaAAaaaaAaAaAa
0x2879f90	192	_gcc-shmem-tdm2-pthr_root_shmem-aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaAaAAaAaAAaaaaAaAaAAaAaa
0x287a140	212	\REGISTRY\USER\S-1-5-21-1647637228-2771519747-2643958445-1001\Software\Microsoft\Windows NT\CurrentVe
0x287a230	198	bgcc-shmem-tdm2-idListNextId_shmem-aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaAaAAaAaAAaaaaAaAaaAAa
0x287a310	192	_gcc-shmem-tdm2-idListCnt_shmem-aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaAaAAaAaAAaaaaAaAaaaAAaaa
0x287a3f0	186	\gcc-shmem-tdm2-idList_shmem-aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaAaAAaAaAAaaaaAaAaaaAaAaaa
0x287a5a0	202	gcc-shmem-tdm2-mxattr_recursive_shmem-aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaAaAAaAaAAaaaaAaAaA
0x287aaf0	192	_gcc-shmem-tdm2-idListMax_shmem-aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaAaAAaAaAAaaaaAaAaaaAaaaa
0x287bf14	78	C:\Users\Overseer\Desktop\episodio1.exe
0x2d61340	39	C:\Users\Overseer\Desktop\episodio1.exe
0x2d61390	39	C:\Users\Overseer\Desktop\episodio1.exe
0x2d618f8	32	e30f35ad8d9cb6efc0778539a669fa85
0x2d6192f	37	C:\WINDOWS\system32\cmd.exe /c pause
0x2d61cf7	41	APPDATA=C:\Users\Overseer\AppData\Roaming
0x2d61d21	48	CommonProgramFiles=C:\Program Files\Common Files
0x2d61d52	59	CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
0x2d61d8e	48	CommonProgramW6432=C:\Program Files\Common Files
0x2d61ddc	35	ComSpec=C:\WINDOWS\system32\cmd.exe
0x2d61e00	48	FPS_BROWSER_APP_PROFILE_STRING=Internet Explorer
0x2d61e31	39	FPS_BROWSER_USER_PROFILE_STRING=Default
0x2d61e8d	44	LOCALAPPDATA=C:\Users\Overseer\AppData\Local
0x2d61eef	35	OneDrive=C:\Users\Overseer\OneDrive
0x2d61f21	427	Path=C:\ProgramData\Oracle\Java\javapath;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wber
0x2d620cd	61	PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC

FLAG: **UAM{e30f35ad8d9cb6efc0778539a669fa85}**

Programas utilizados:

ProcessHacker -> enlace de descarga