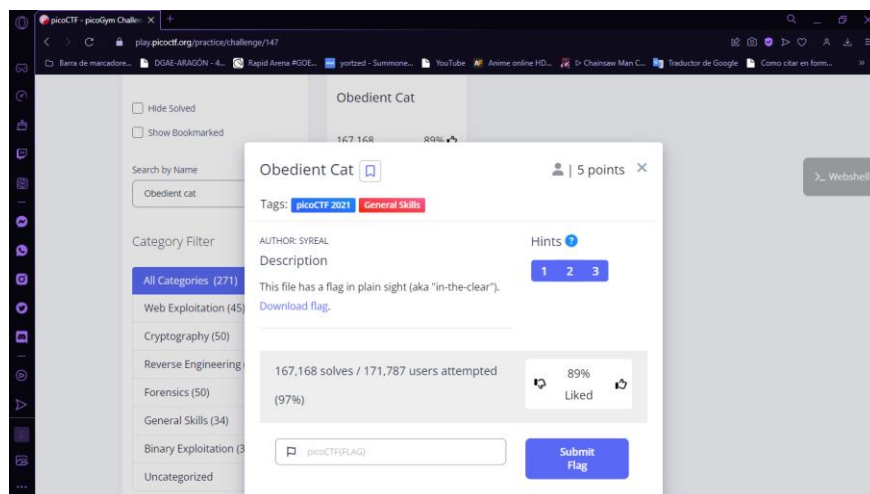


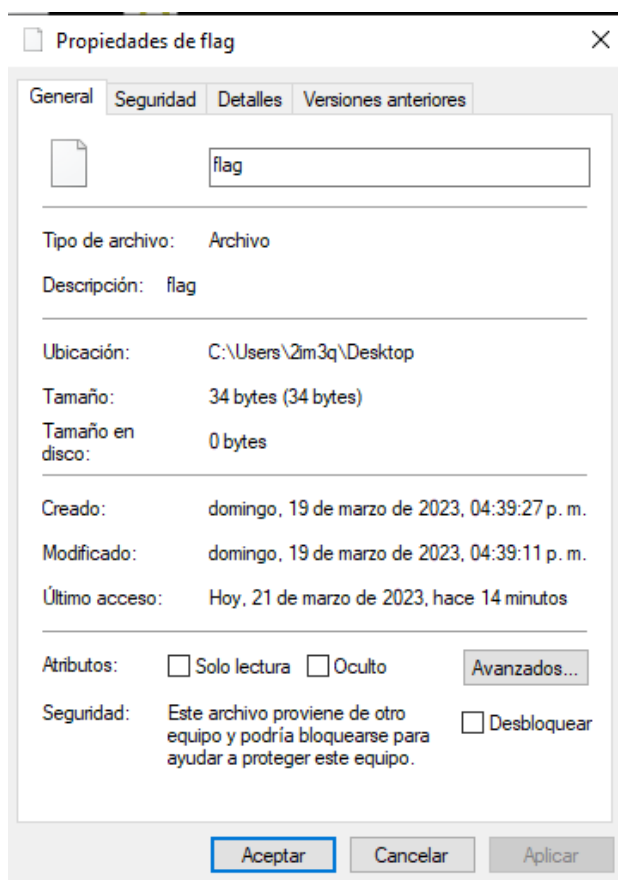
Tarea: Obedient cat

Alumno: Quintana Escamilla Roberto Carlos

En esta ocasión el ejercicio nos indica que la contraseña se encuentra a plena vista y se nos da un archivo.



Si lo descargamos observaremos un archivo de nombre flag sin extensión.



Si utilizamos un comando cat en consola para ver su contenido, encontramos la bandera.

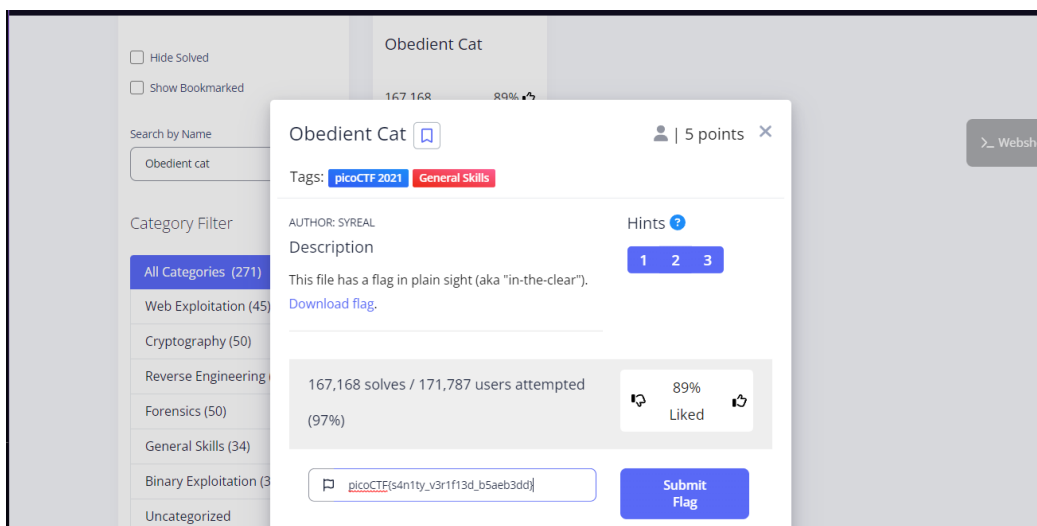
```
MINGW64:/c/Users/2im3q/Desktop

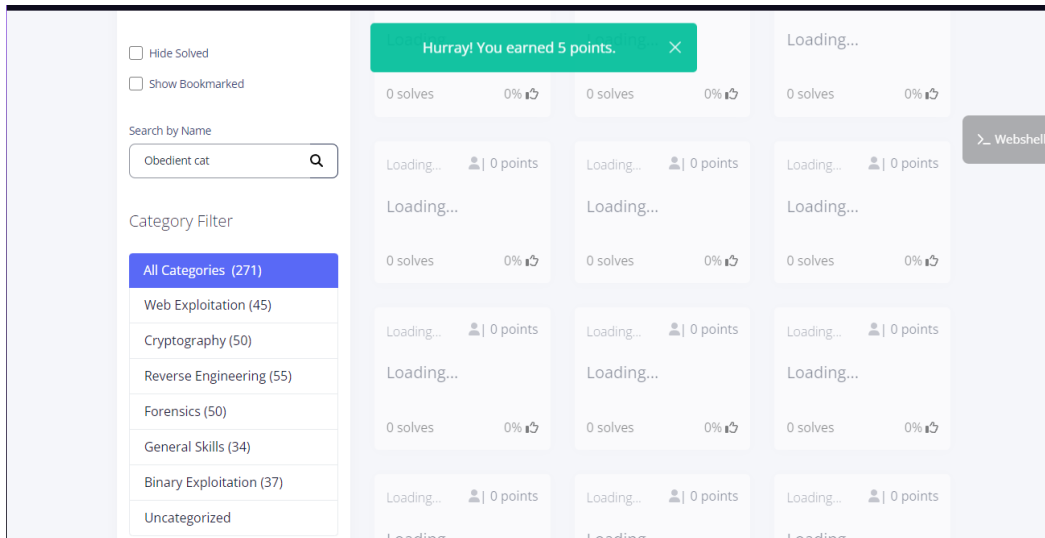
2im3q@DESKTOP-QBL05CF MINGW64 ~/Desktop
$ cat flag
picoCTF{s4n1ty_v3r1f13d_b5aeb3dd}

2im3q@DESKTOP-QBL05CF MINGW64 ~/Desktop
$ |
```

picoCTF{s4n1ty_v3r1f13d_b5aeb3dd}

Comprobamos





Vulnerabilidades

En este caso el ejercicio aclara que la flag se encuentra "in-the-clear", por lo cual es de fácil acceso de manera intencionada. Sin embargo, si consideramos esto como una contraseña esto sería un riesgo pues cualquiera podría acceder a ella por lo cual lo preferible sería encriptarla la información previamente.

Solución.

Para solucionar el problema se debe encriptar el archivo, para ello se debe elegir una contraseña y un algoritmo de encriptación. Hay diversos softwares los cuales nos pueden facilitar el cifrado como podría ser el programa "Encrypto" el cual utiliza el esquema de seguridad AES 256 y únicamente nos requerirá proporcionar el archivo y contraseña para encriptar o desencriptar.

Referencias (pendiente)

BorjaGalisteo. (2019). "🔒🔥 Como ENCRYPTAR | Que es la encriptación de archivos y como se usa". Recuperado de https://www.youtube.com/watch?v=8Ois7NYwf_M