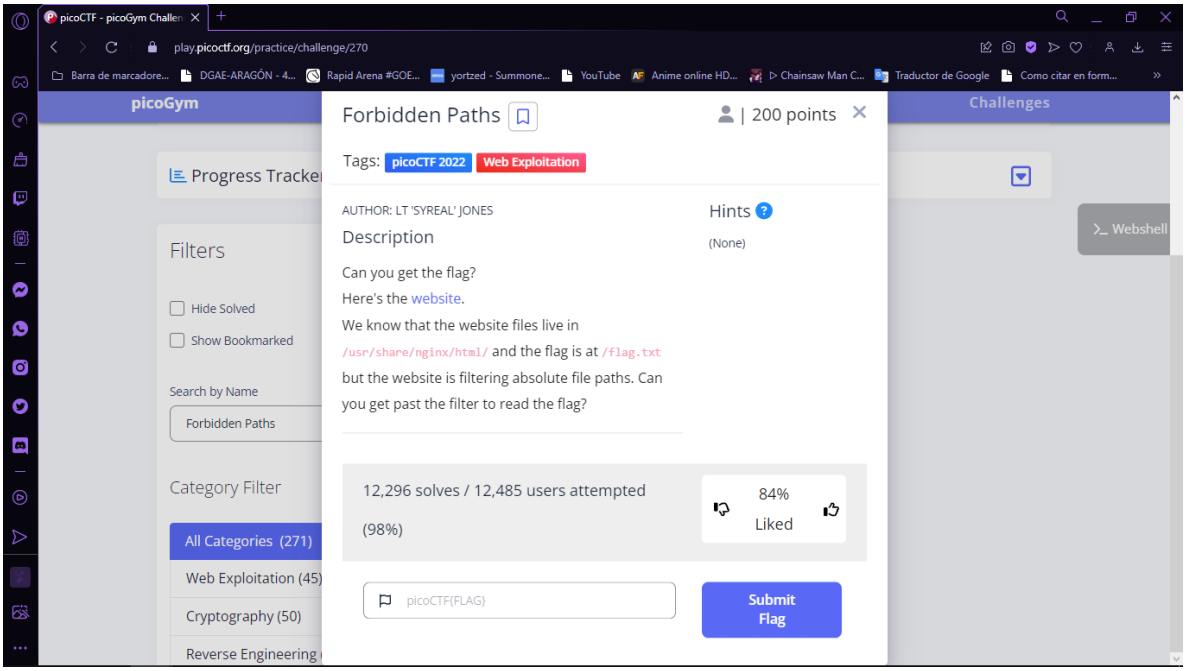
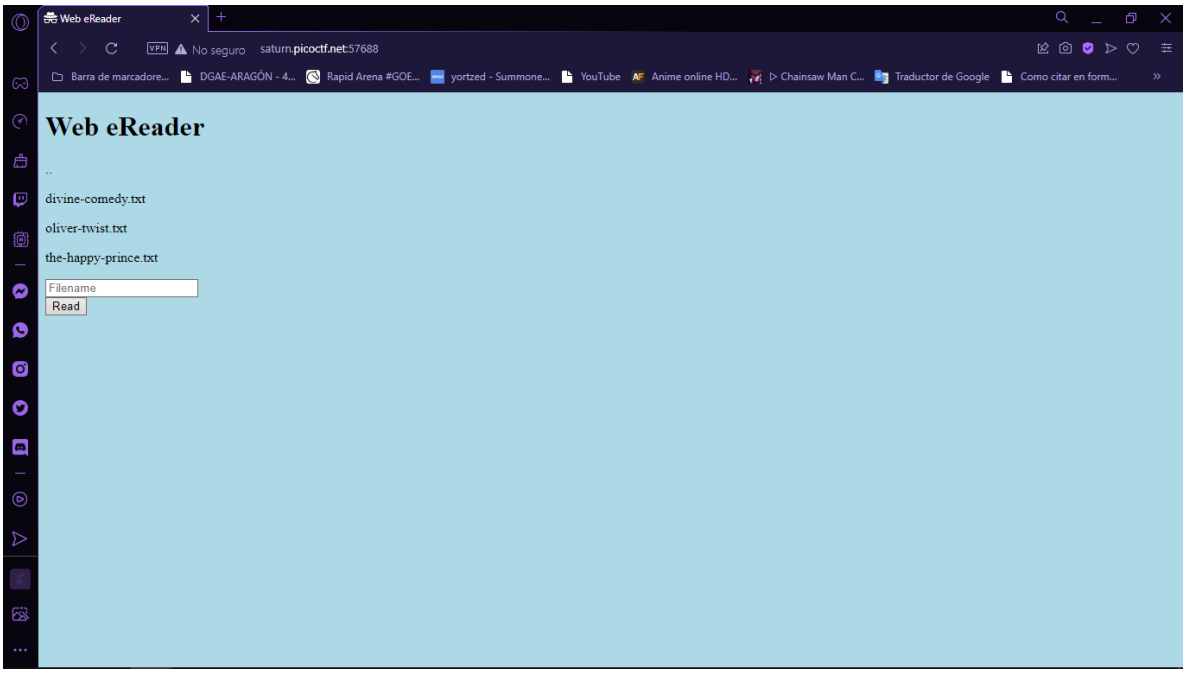
Tarea: Forbidden Paths picoCTF

Alumno: Roberto Carlos Quintana Escamilla

En este ejercicio se nos indica que la flag se encuentra en la dirección /flag.txt, mientras que el sitio que nos proporcionan esta en /usr/share/nginx/html/ , además se nos dice que la pagina filtra las direcciones absolutas.

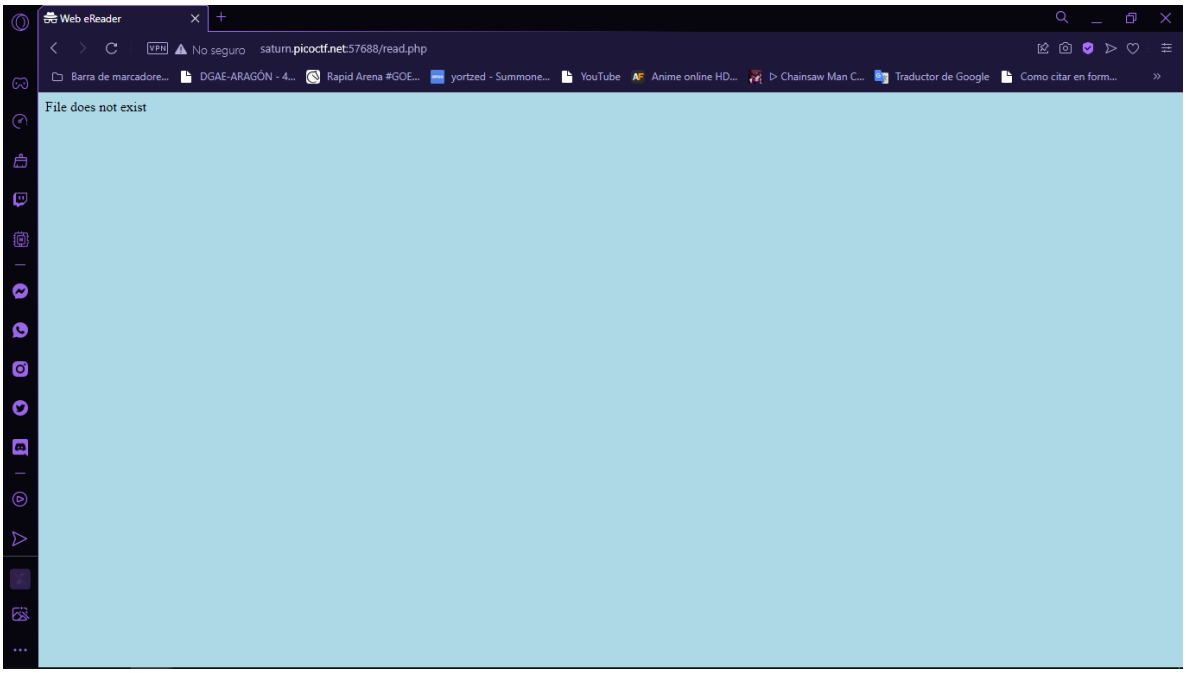


Si vamos al sitio web encontramos una pagina simple que indica ser un lector web, donde podemos ver el nombre de algunos archivos de texto y un tex file donde podremos ingresar información.

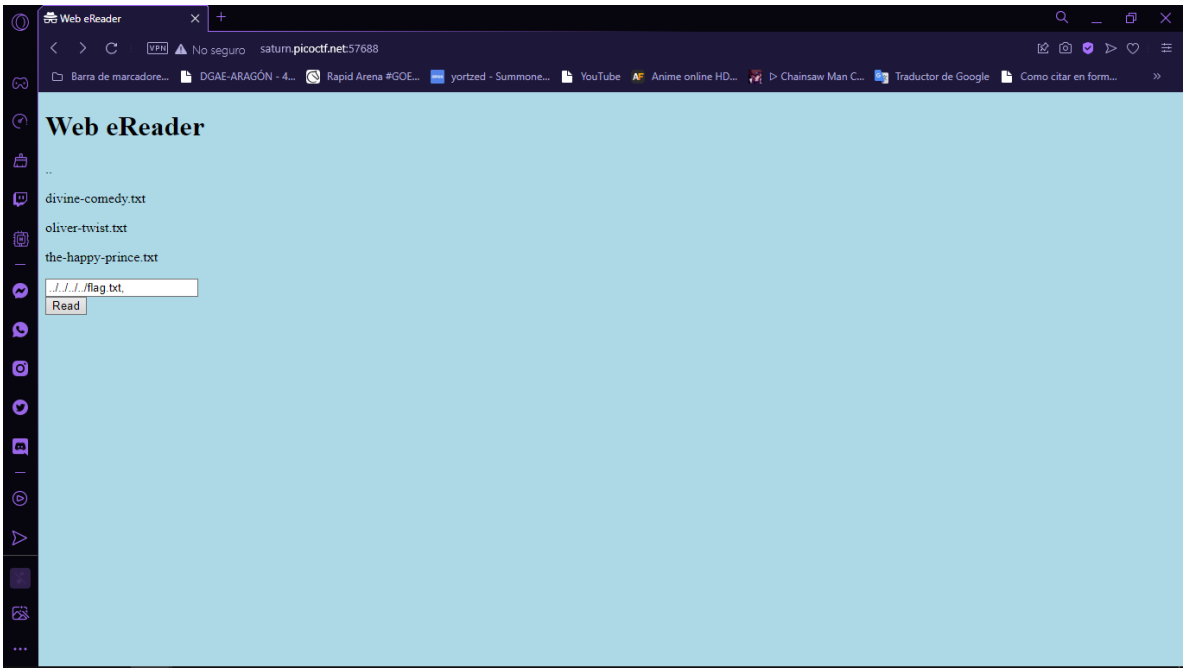


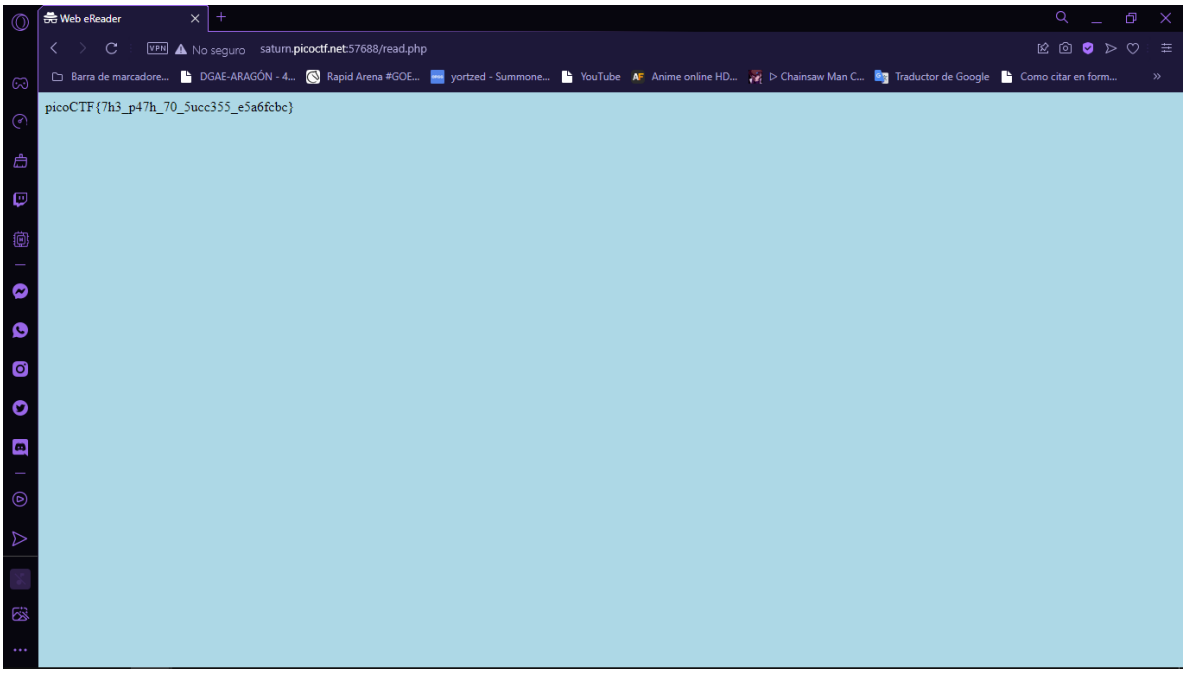
Si ingresamos alguno de estos archivos en el tex file , se nos dará lectura al libro que se menciona. Por lo que suponeos que si ingresamos el archivo flag.txt podremos leerlo.

Sin embargo si hacemos esto se nos indicara que no existe dicho archivo.



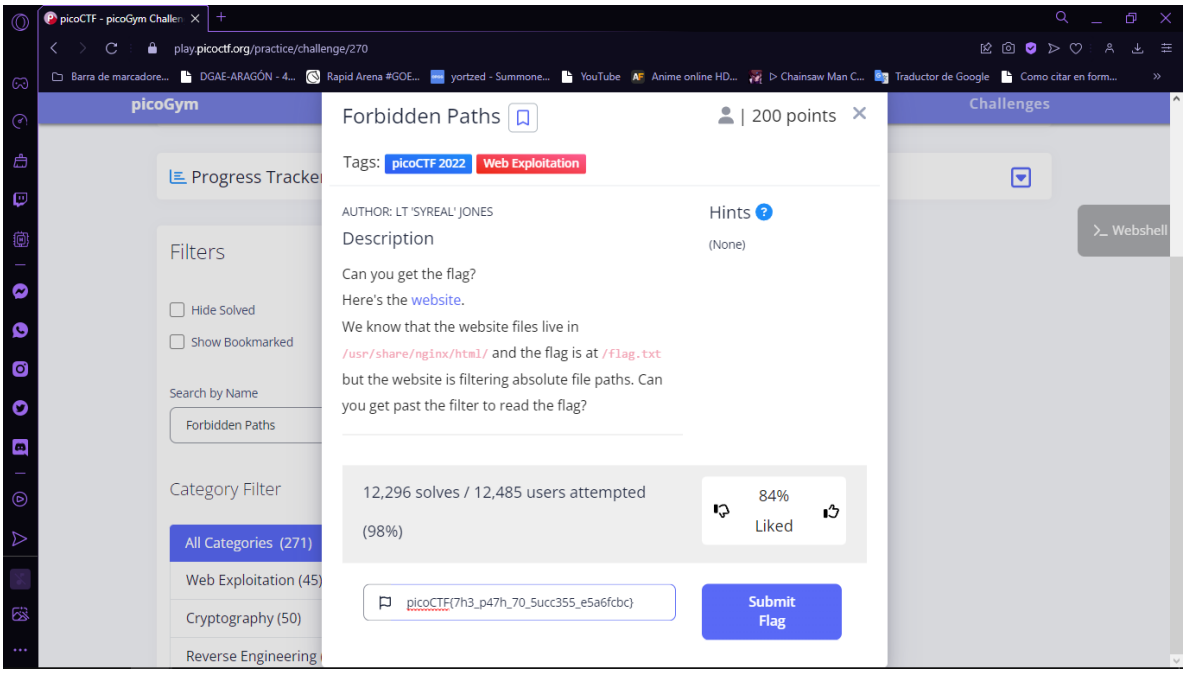
Con la pista que se nos dio en la descripción del ejercicio podemos suponer que es simplemente por que no se encuentra en el directorio donde se manda a llamar la petición echa en el texfile. Por lo que ingresaremos una dirección la cual le indique al programa que nos regrese primero hasta el directorio común de donde nos encontramos y donde se encuentra la flag, luego que lea el archivo deseado. Obtenemos la dirección ../../../../flag.txt si suponemos que el sistema utiliza un direccionamiento tipo Linux.

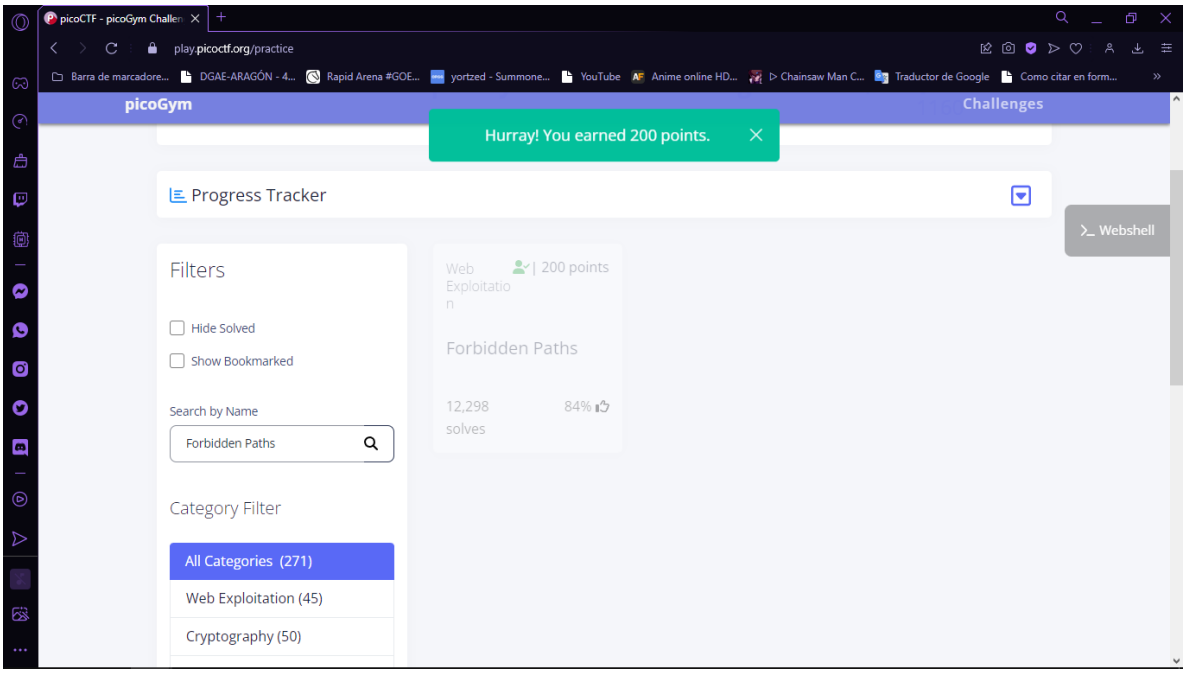




picoCTF{7h3_p47h_70_5ucc355_e5a6fcbc}

comprobamos la flag





Vulnerabilidades

Como pudimos observar el sistema nos permite acceder a archivos en el servidor los cueles deberían permanecer como privados pues no son parte del modelo de negocios de la página y podría dar origen a un robo de información privada.

Solución

Se podría hacer un filtro mejorado donde el sistema rechace cualquier petición que no coincida con el nombre los archivos que queremos que sean accesibles.