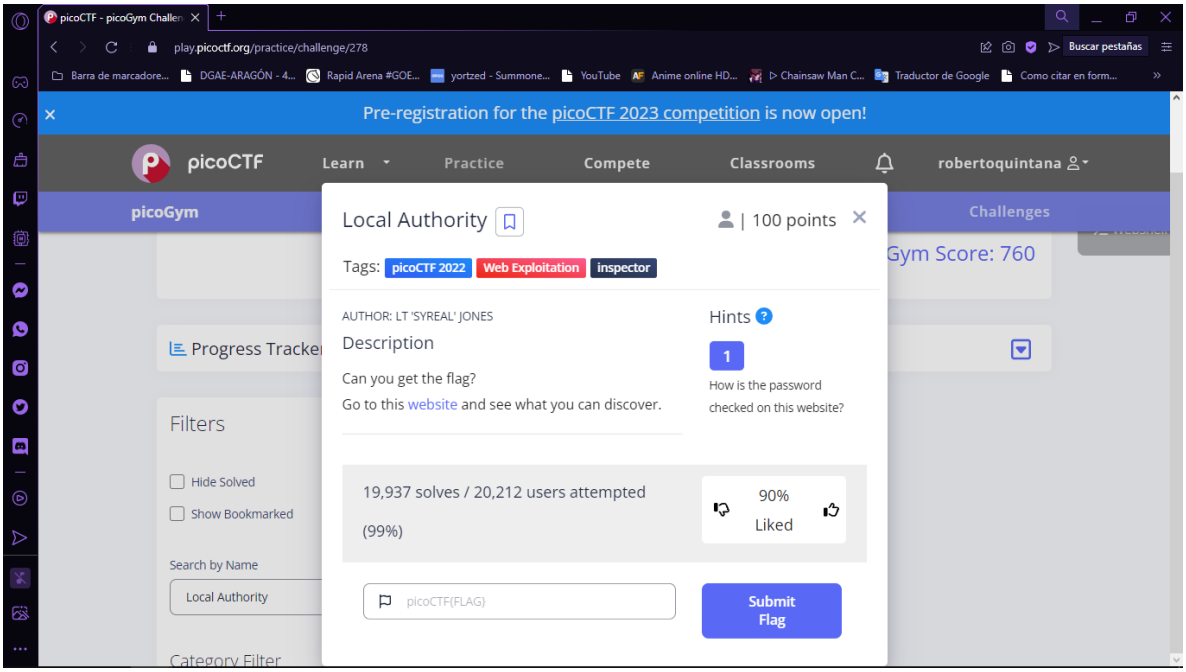
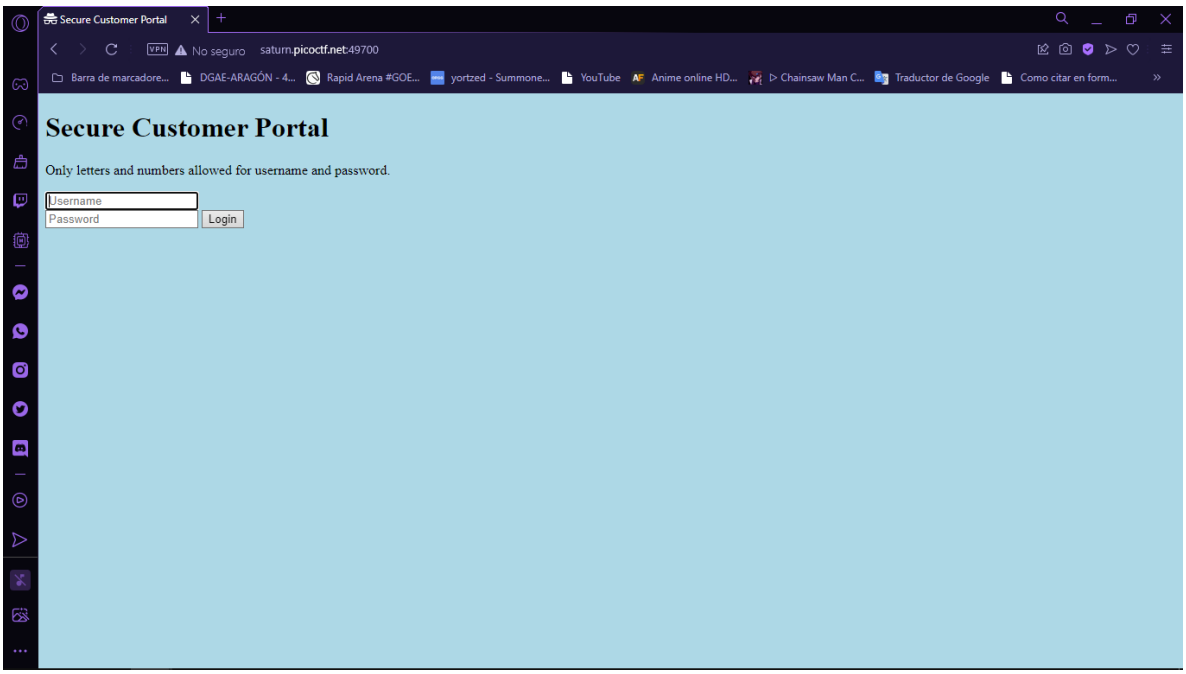
Tarea: Local Authority

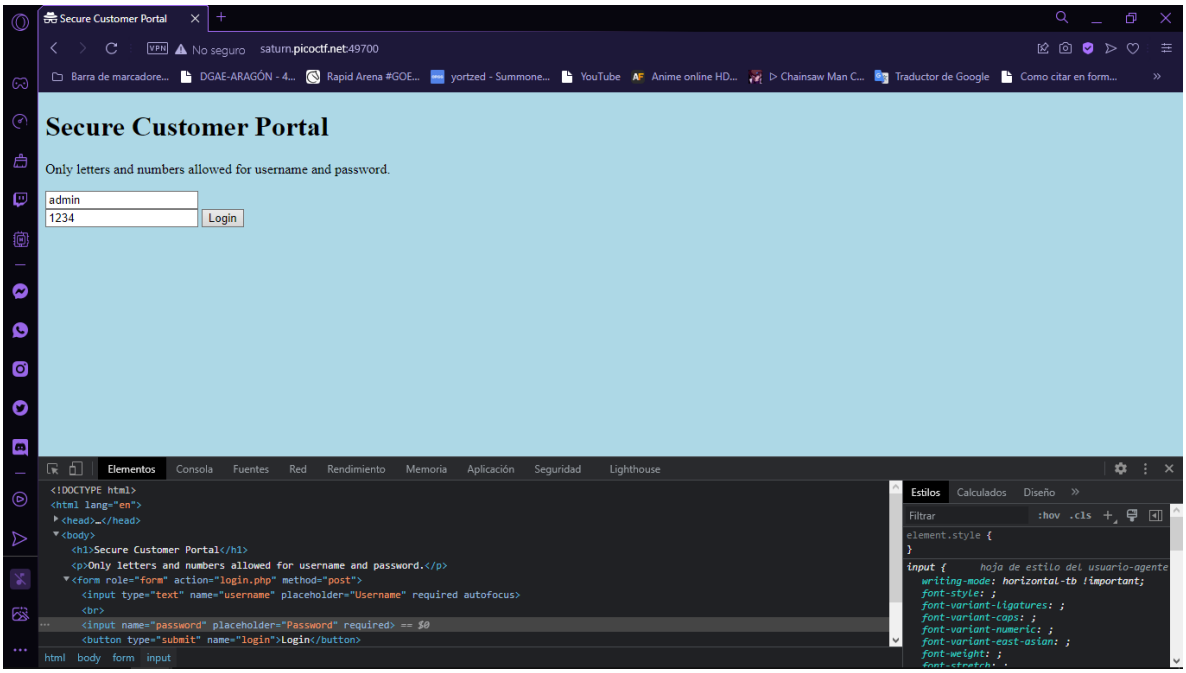
Alumno: Roberto Carlos Quintana Escamilla

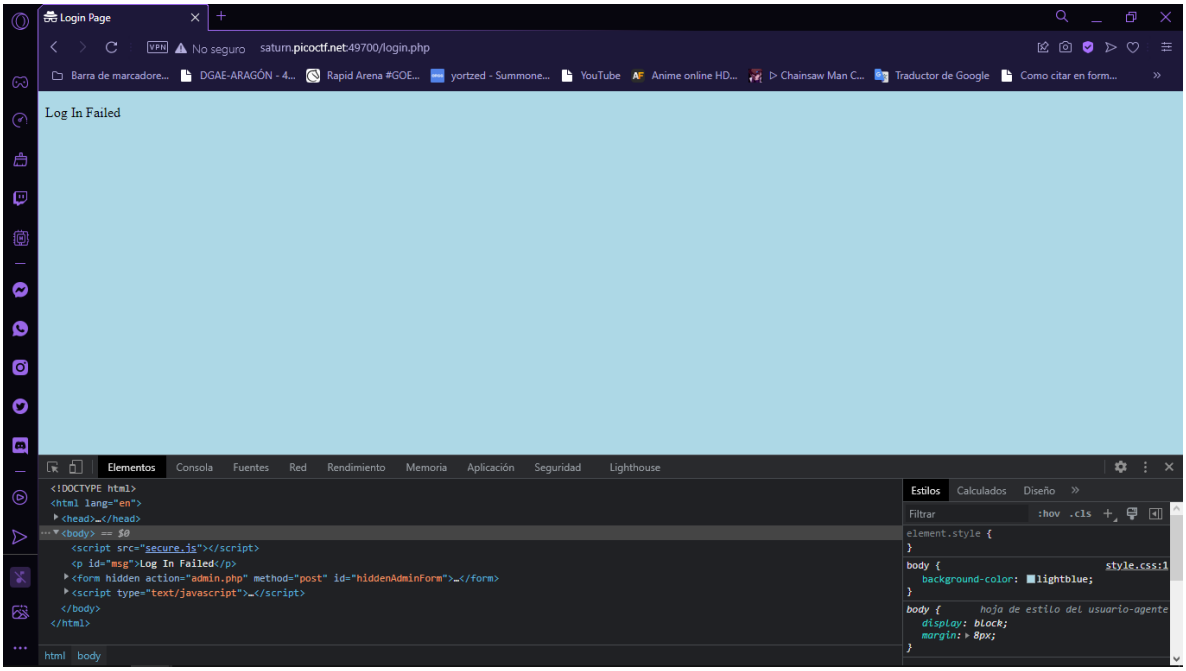


Observamos las indicaciones del ejercicio y observamos que solo nos pregunta sobre que podemos descubrir del sitio web que se nos da. La cual solo es una pagina de logueo

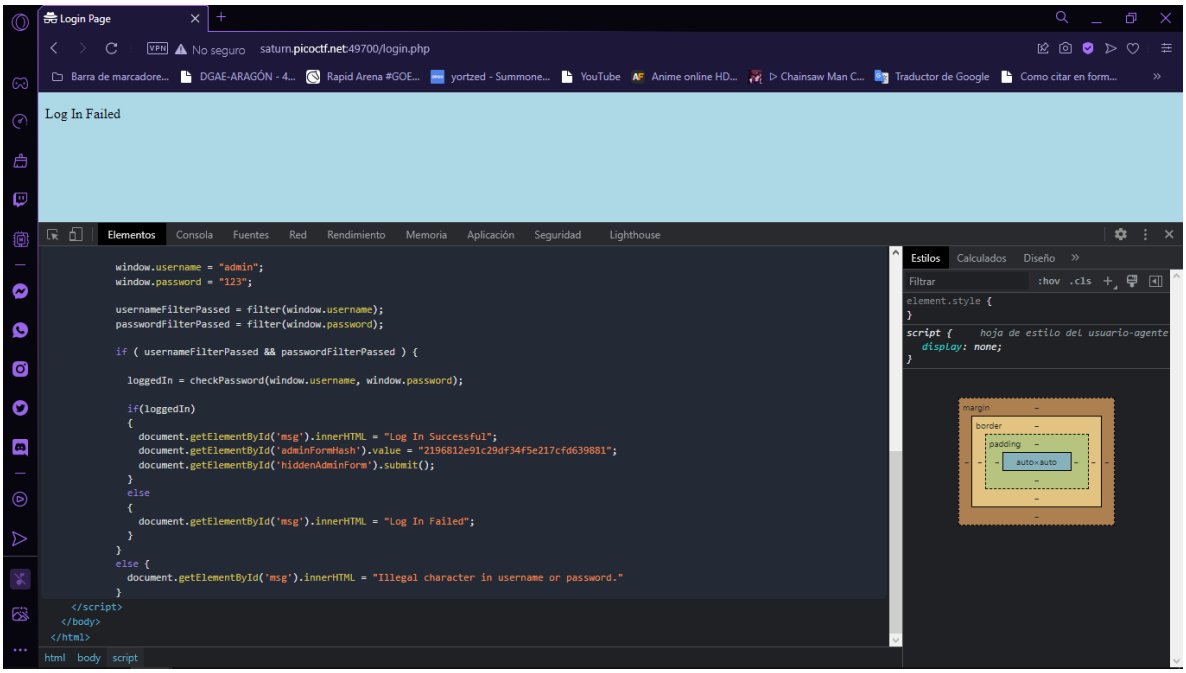


Probemos que ocurre cuando ingresamos unas credenciales cualquiera (usamos el inspector solo para poder ver que escribimos en la contraseña).

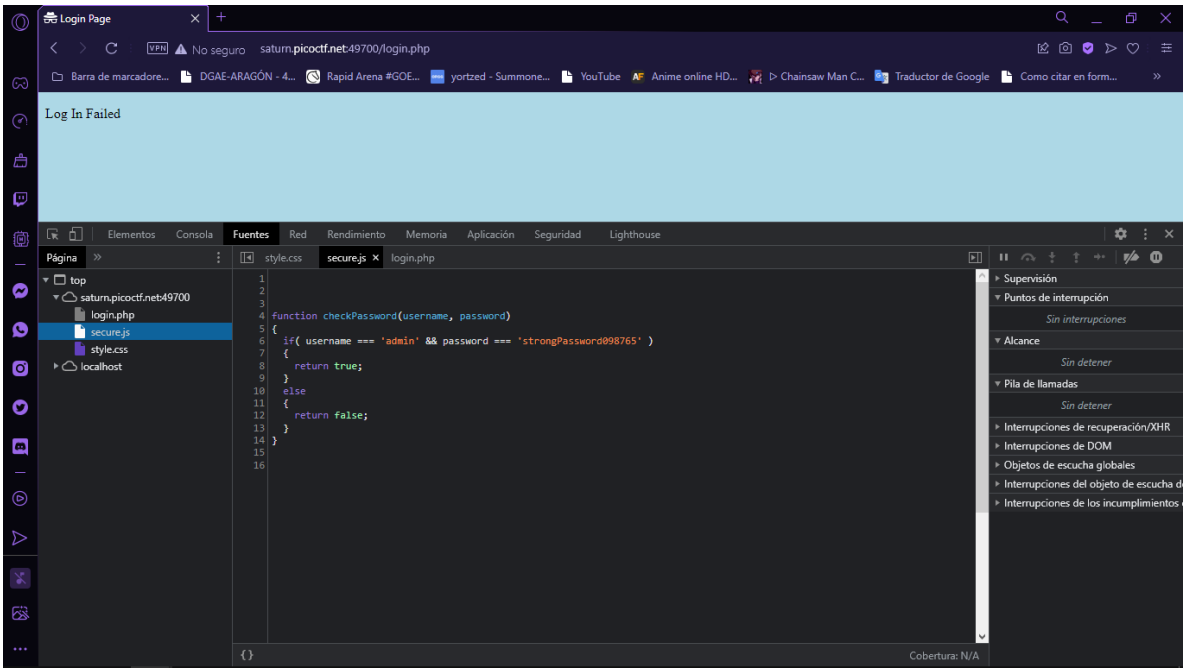




Observamos que el logueo fue fallido. Sin embargo inspeccionando el HTML del sitio podemos encontrar la función que se usa para realizar el logueo



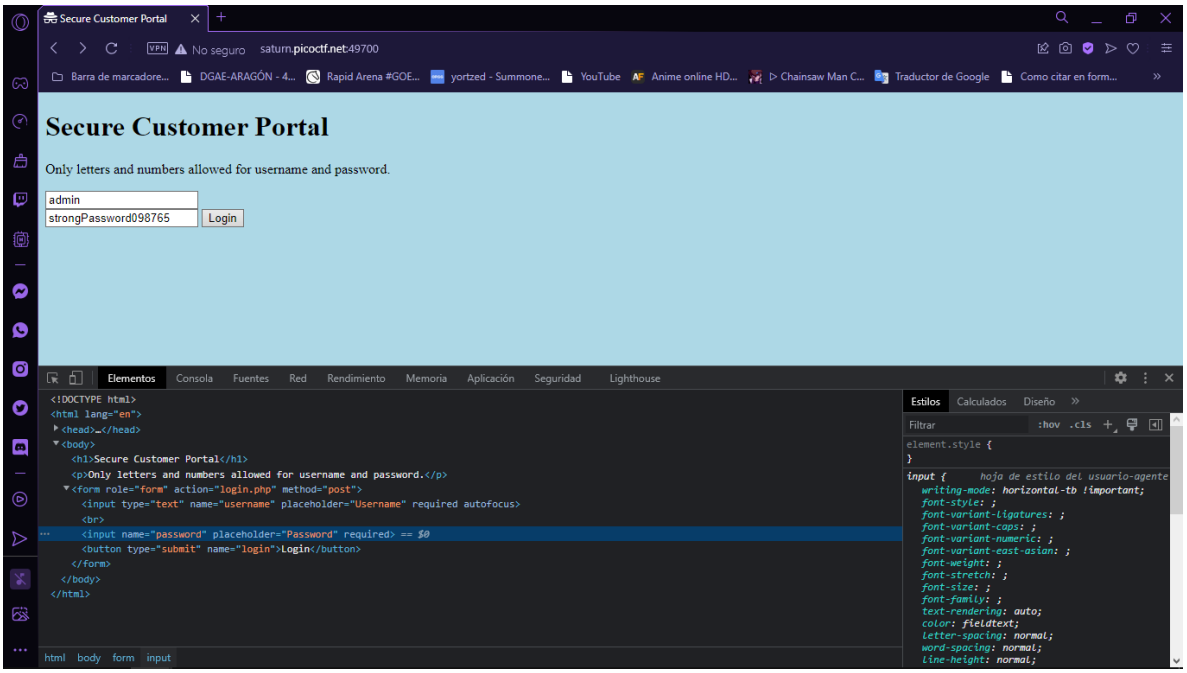
Si observamos los archivos del sitio nos topamos con el archivo securere.js en el cual se encuentra programada la función que buscábamos. Y vemos las credenciales que necesitamos para que la funcion retorne True.

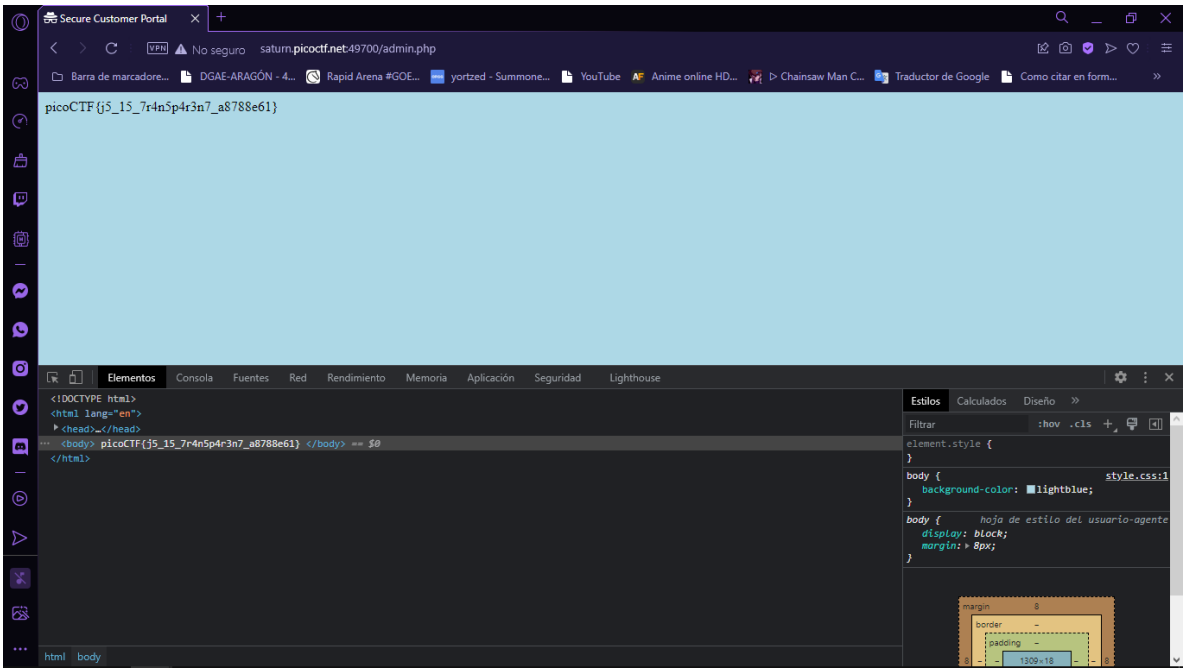


User: admin

Pass: strongPassword098765

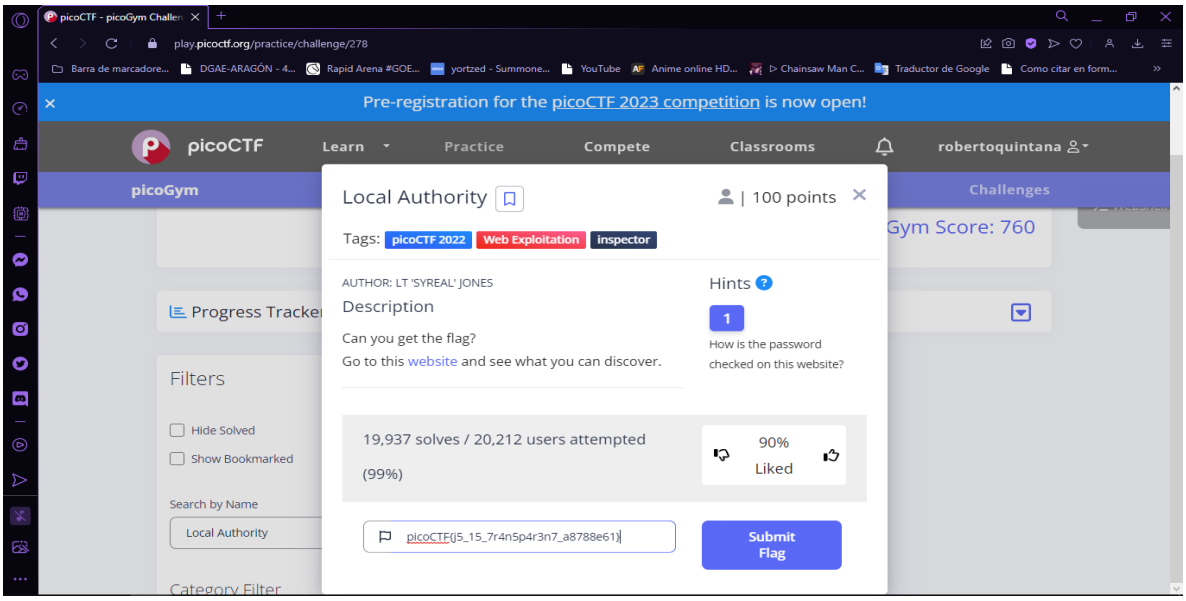
Regresando a la pagina inicial he ingresado estas credenciales. Obtenemos la pagina donde se encuentra la flag del ejercicio.

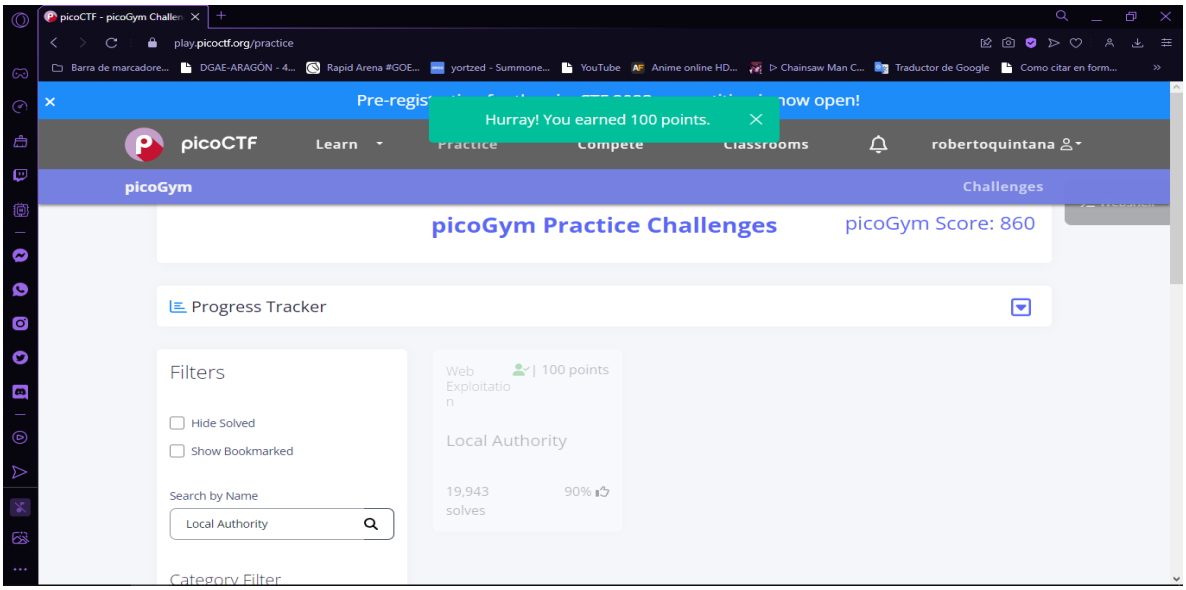




picoCTF{j5_15_7r4n5p4r3n7_a8788e61}

Comprobamos.





Vulnerabilidades

En este ejercicio notamos que se a usado la función de chek de credenciales directamente en el frontend de la pagina, lo cual nos permite saber cual es la protección que tenemos que superar. Pero la vulnerabilidad mas peligrosa del sitio fue programar esta función en un archivo legible desde el frontend.

Posible solución

Para ello hay que mover esta función de chek al backend del sitio para que la autorización se obtenga mediante una petición hacia un endpoint en el servirdor.