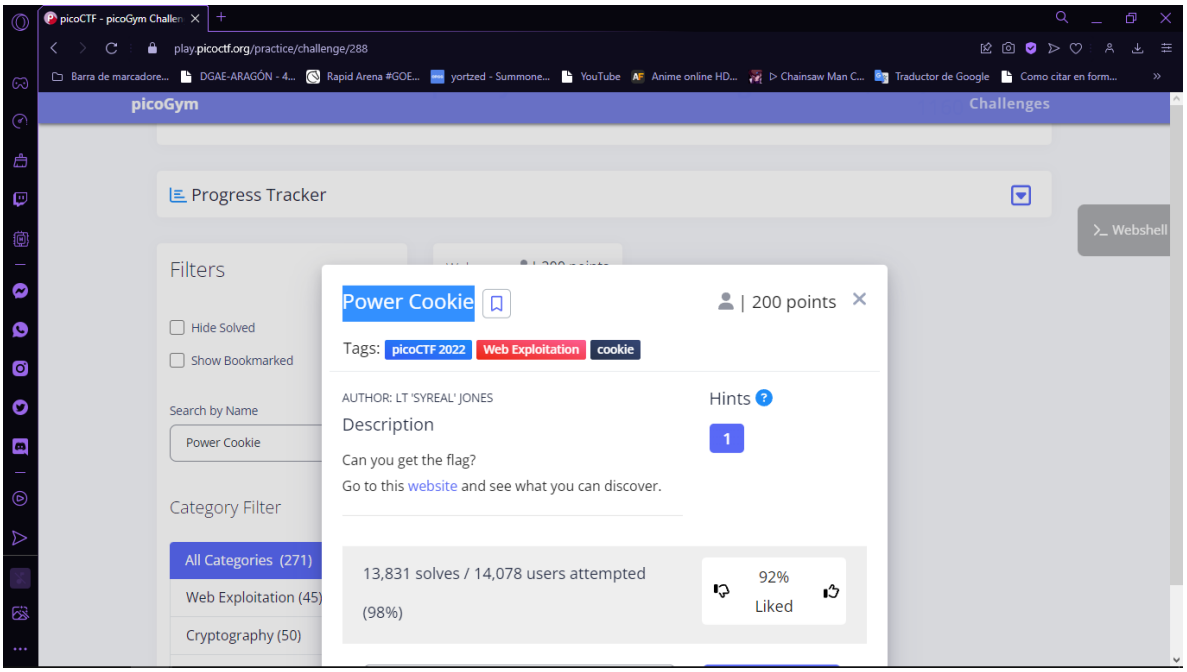
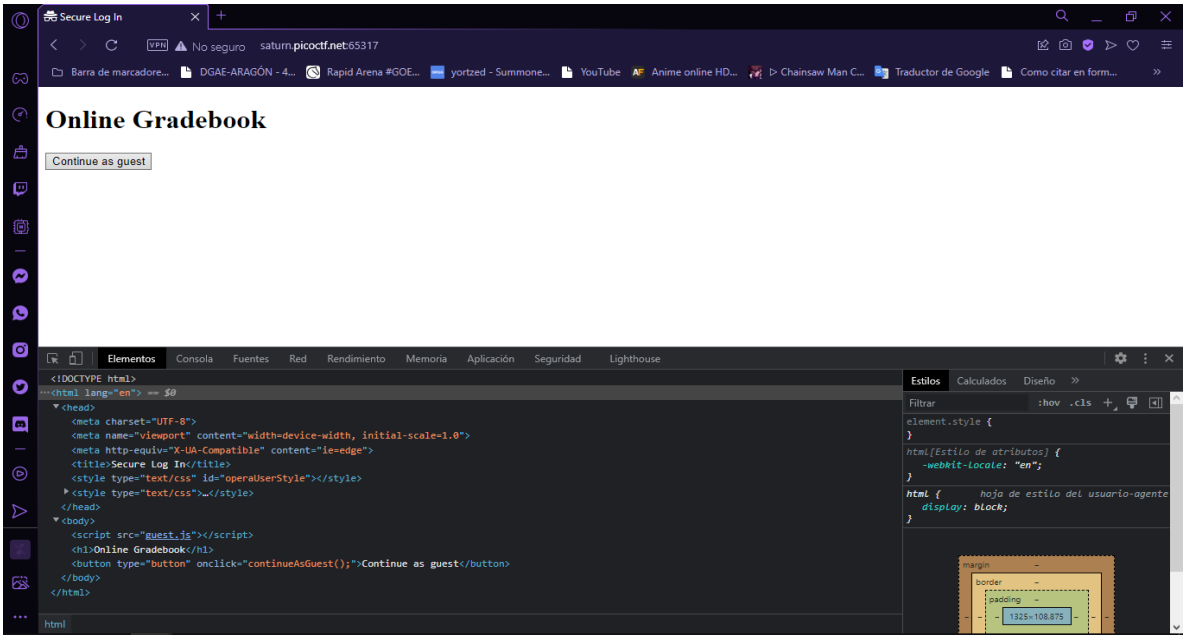
Tarea. Power Cookie

Alumno. Quintana Escamilla Roberto Carlos

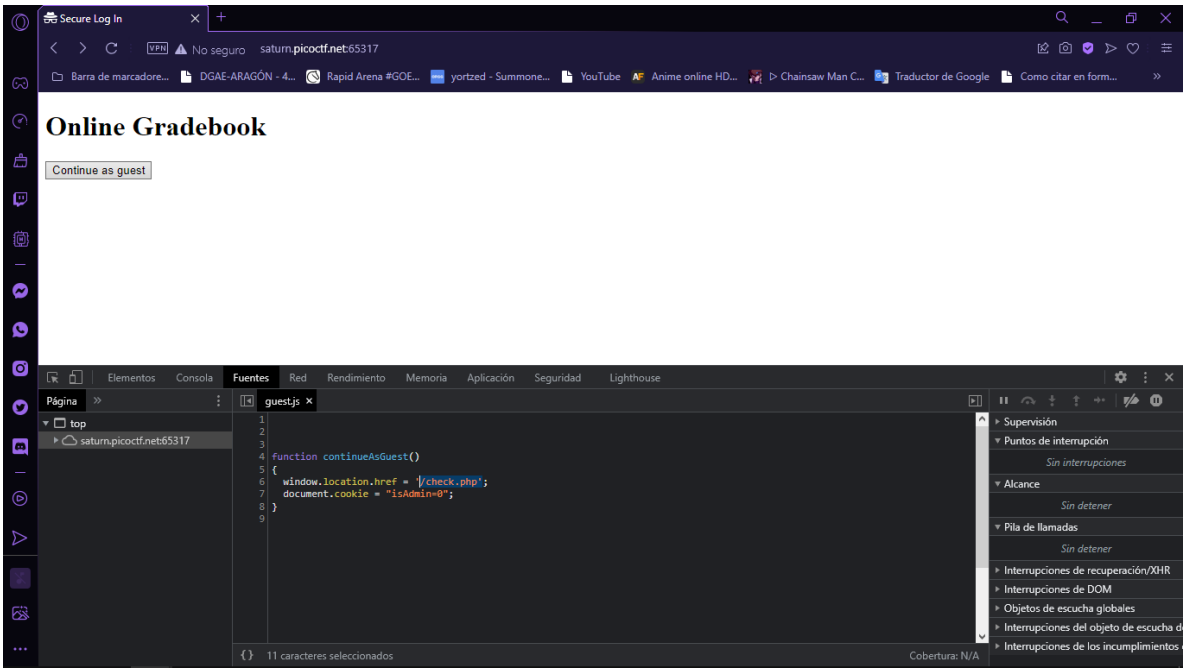
En este ejercicio no nos dan demasiadas pistas en la descripción de este. Sin embargo el titulo nos puede dar la impresión de que la respuesta estará relacionada con las Cookies de sitio web al que se nos redirige.

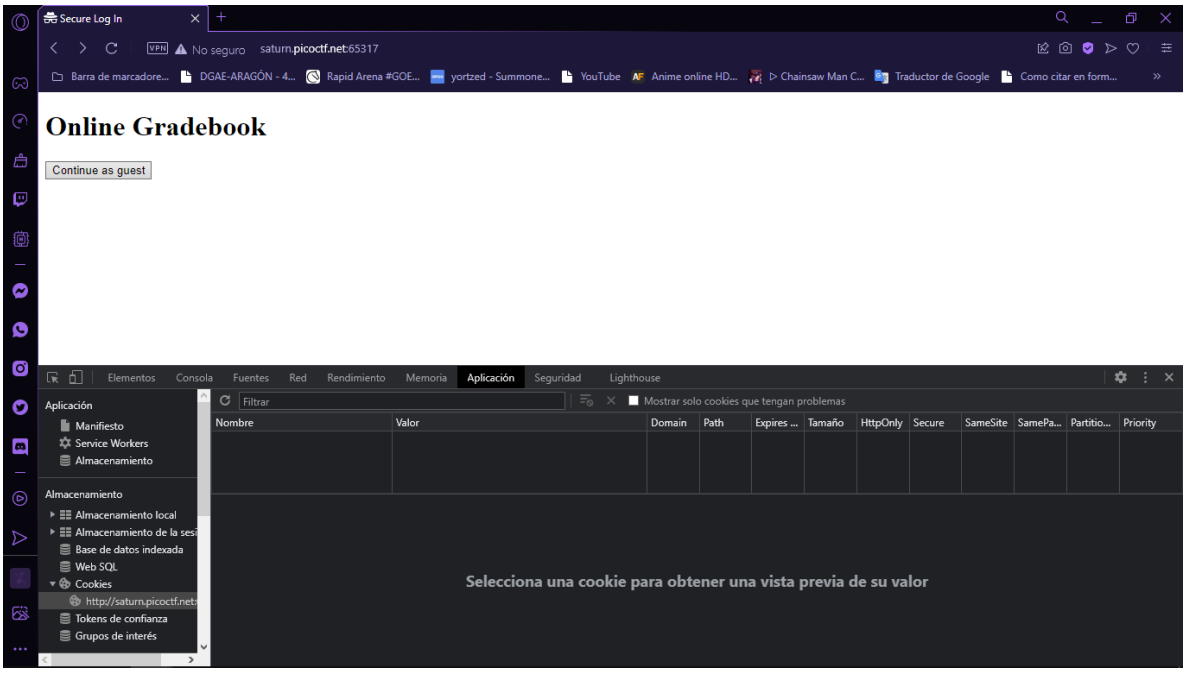


Si entramos al sitio web notamos una pagina simple cuyo titulo no nos indica nada particular. Inspeccionando el código encontramos que se nos indica la función que se ejecuta cuando se oprime el botón.

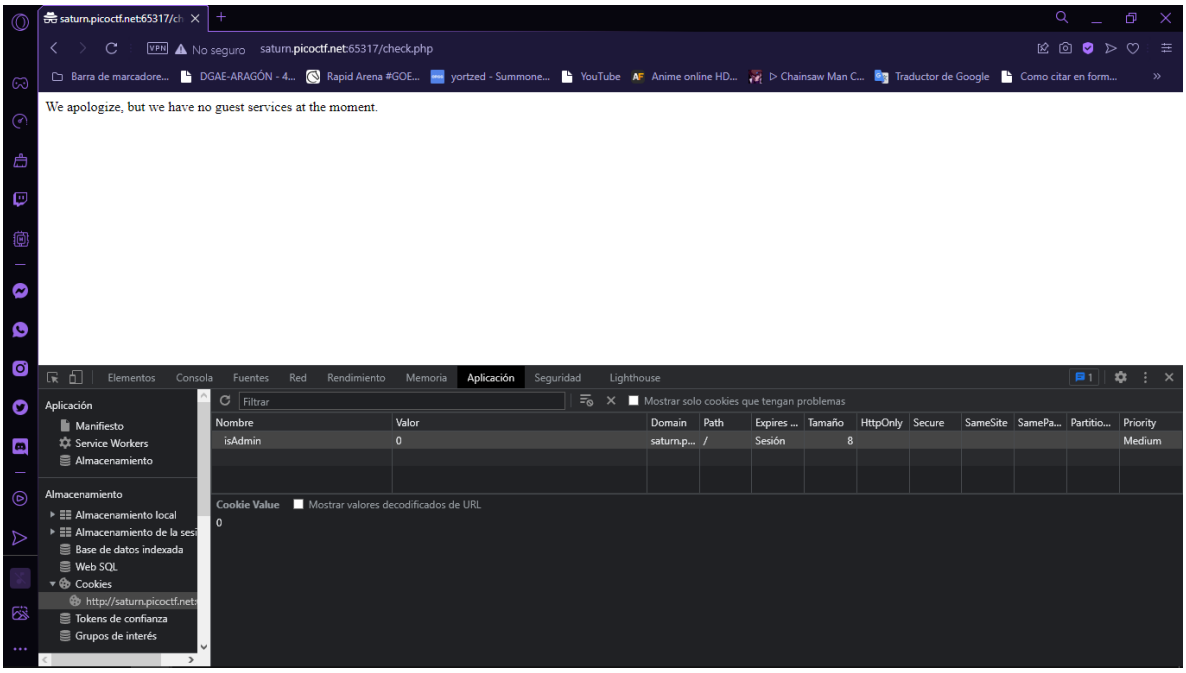


Lleno al archivo js del sitio. Observamos que lee el archivo /check.php y posteriormente hace una comprobación de la cookie isAdmin. Sin embargo, al revisar las cookies del sitio no encontramos dicha cookie activa y solo observaos una cookie con un dominio.

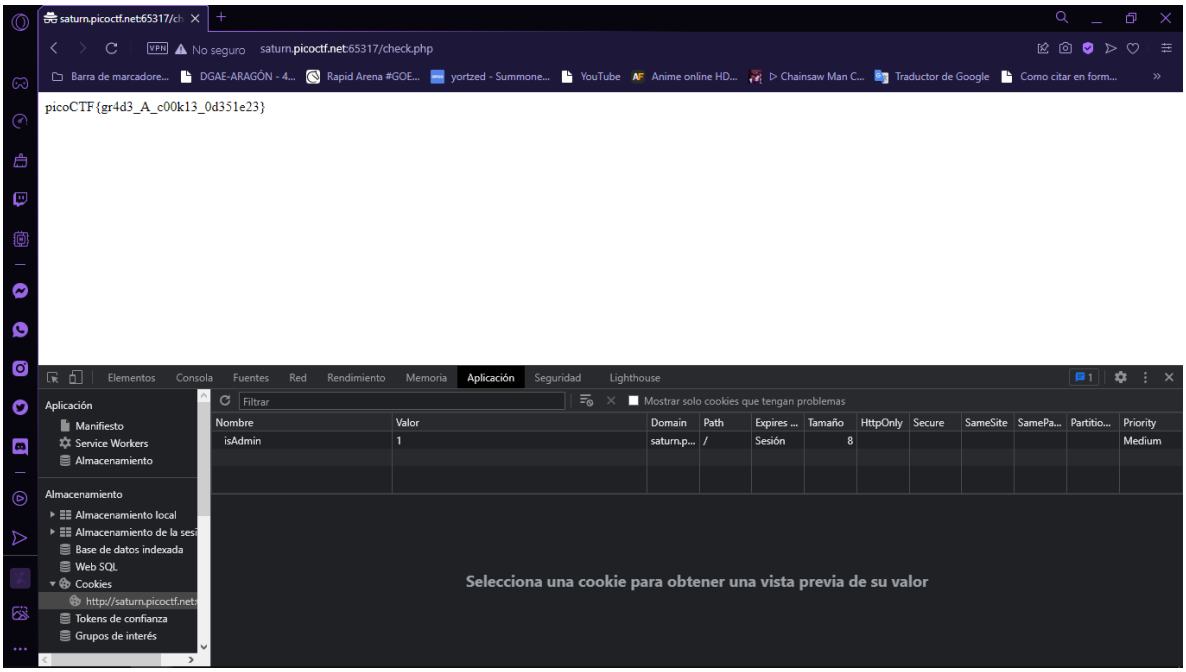




Si oprimimos el botón de continuar como invitado observamos que ahora si aparece la cookie isAdmin con valor 0 .

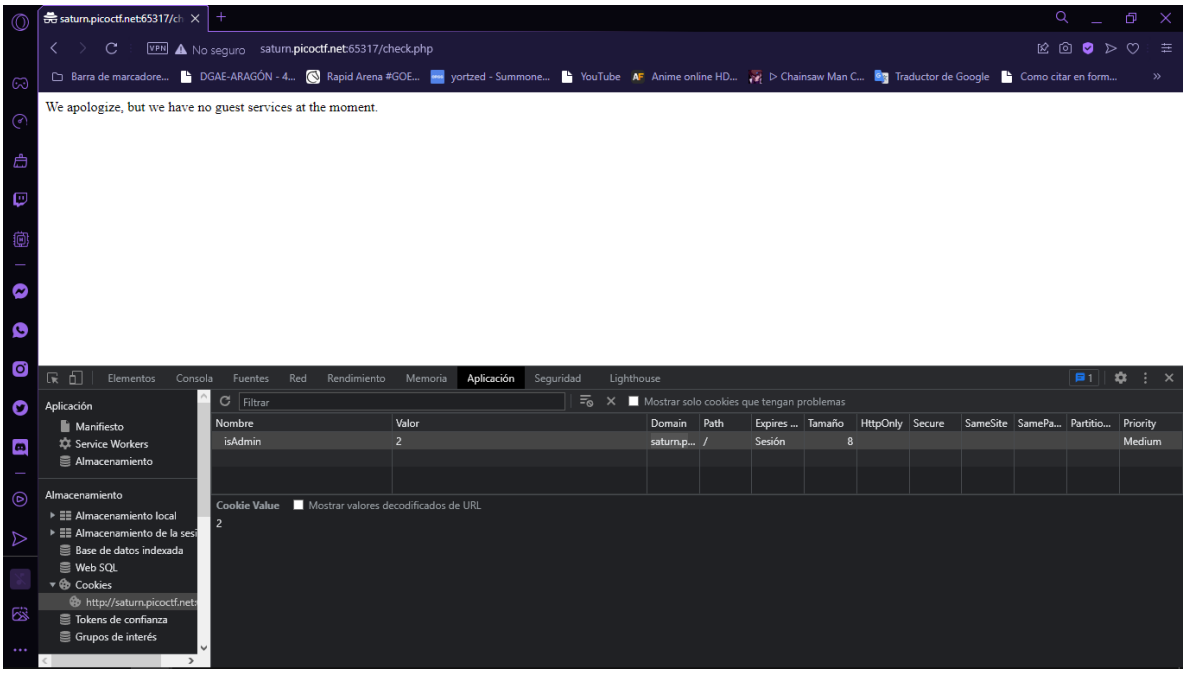


Si cambiamos el valor de esta cookie a 1 y recargamos la pagina encontraremos la flag.

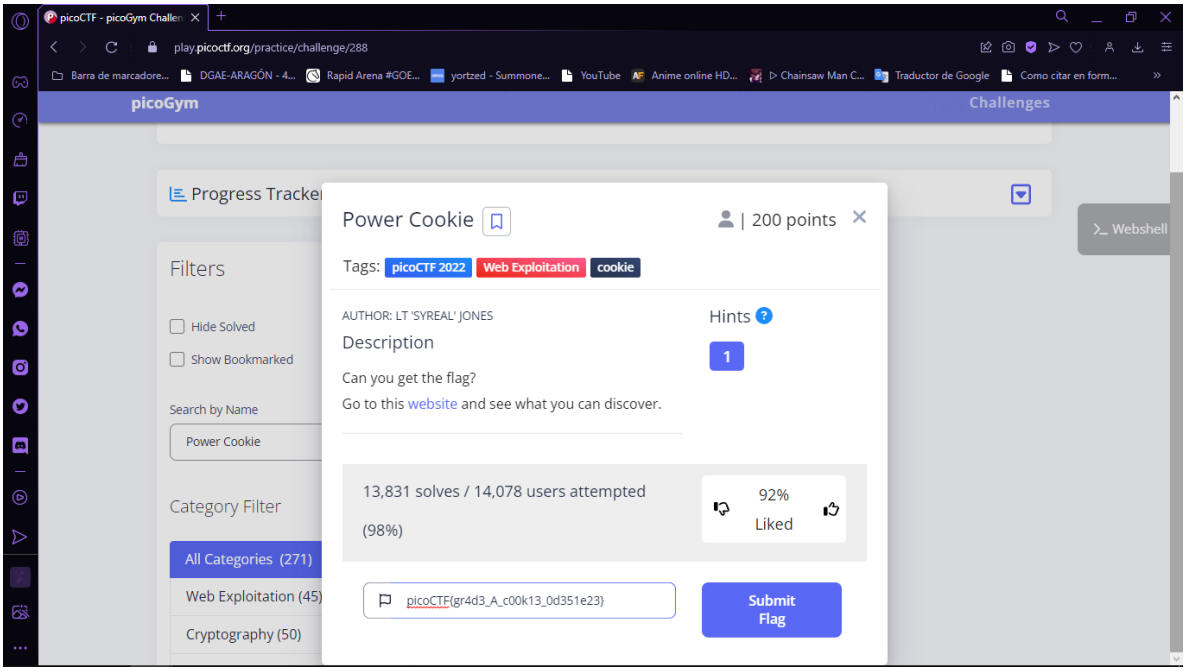


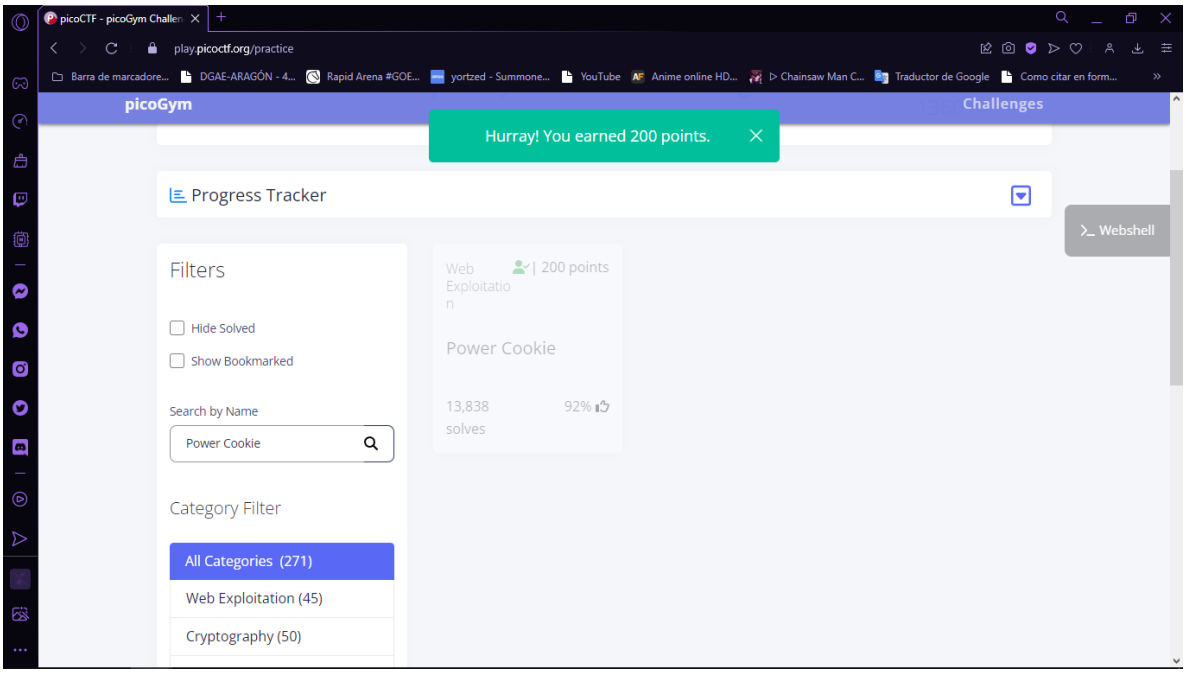
picoCTF{gr4d3_A_c00k13_0d351e23}

Por curiosidad si cambiamos el valor a 2, recibiremos el mismo mensaje inicial.



Comprobamos.





Vulnerabilidad

La vulnerabilidad del sitio se encuentra en el modo en el cual se realiza la validación de credenciales, pues aun que esta se haga desde el bakend utiliza datos fácilmente modificados en el frontend. Y aun que solo se pueda acceder con un valor único de cookie, este podría ser fácilmente encontrado con un ataque de fuerza bruta el cual prueba los diferentes valores uno a uno.

Solución

Para solucionarlo se me ocurre que la comprobación de credenciales debería hacerse por una variable la cual fuera mas complicada de modificar o en su defecto que sea mas complicada de adivinar.