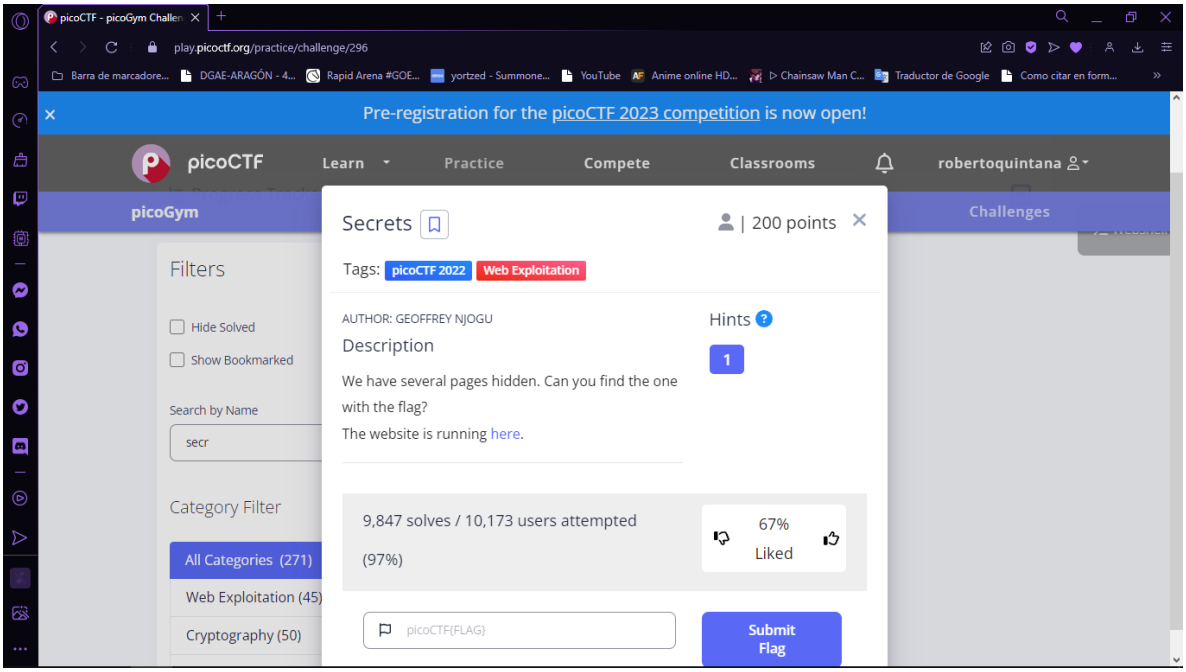
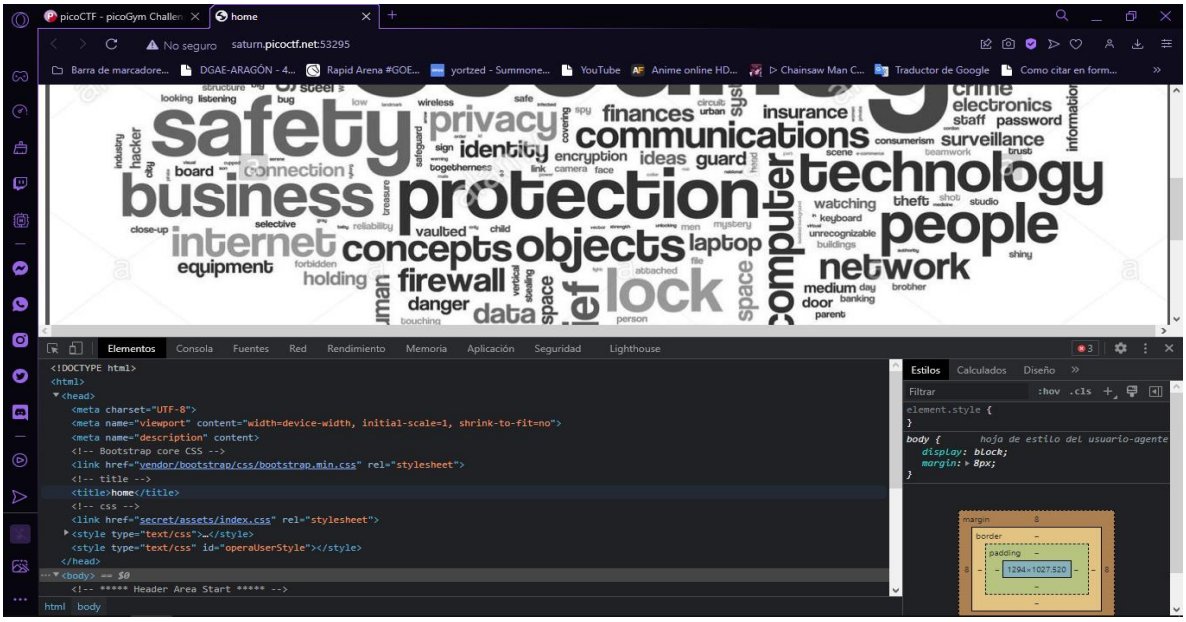
Tarea. Secrets

Alumno. Quintana Escamilla Roberto Carlos

En la instrucción del ejercicio se nos indica que existen varias paginas ocultas donde podría estar la flag.

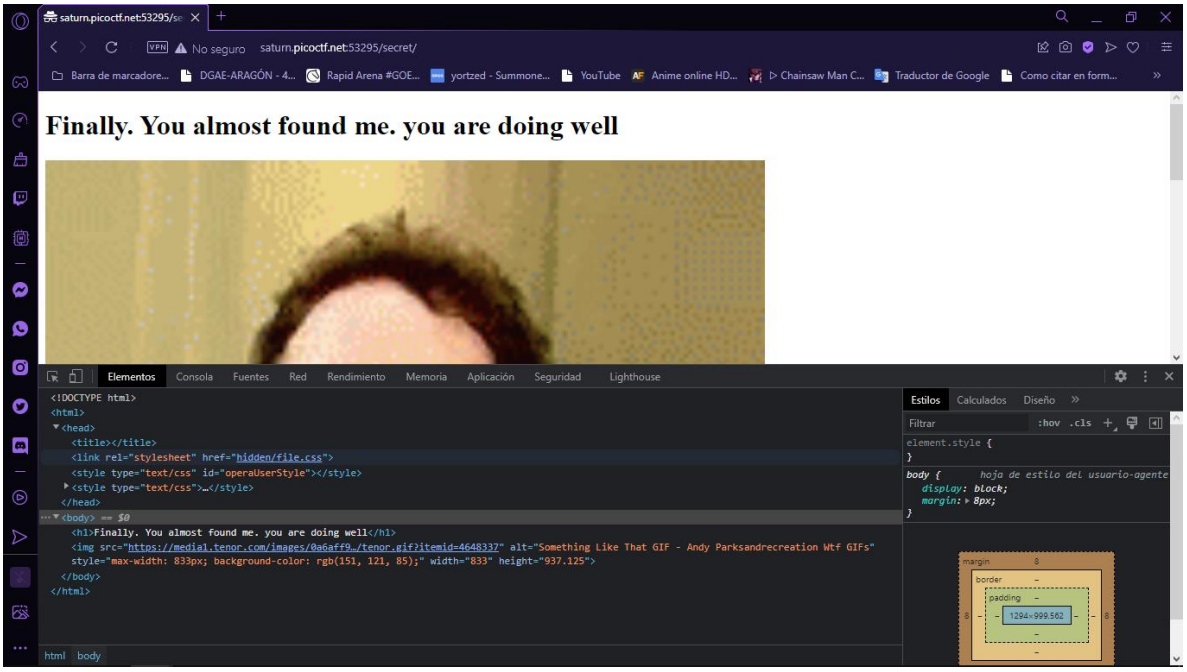


Si abrimos el sitio notaremos una pagina simple con el redireccionamiento a otras paginas almacenadas en el directorio las cuales si hacemos una inspección rápida no encontraremos mas que un par de imágenes. Sin embarco podemos apreciar que para el archivo de estilos se nos desvía a otro directorio completamente distinto.

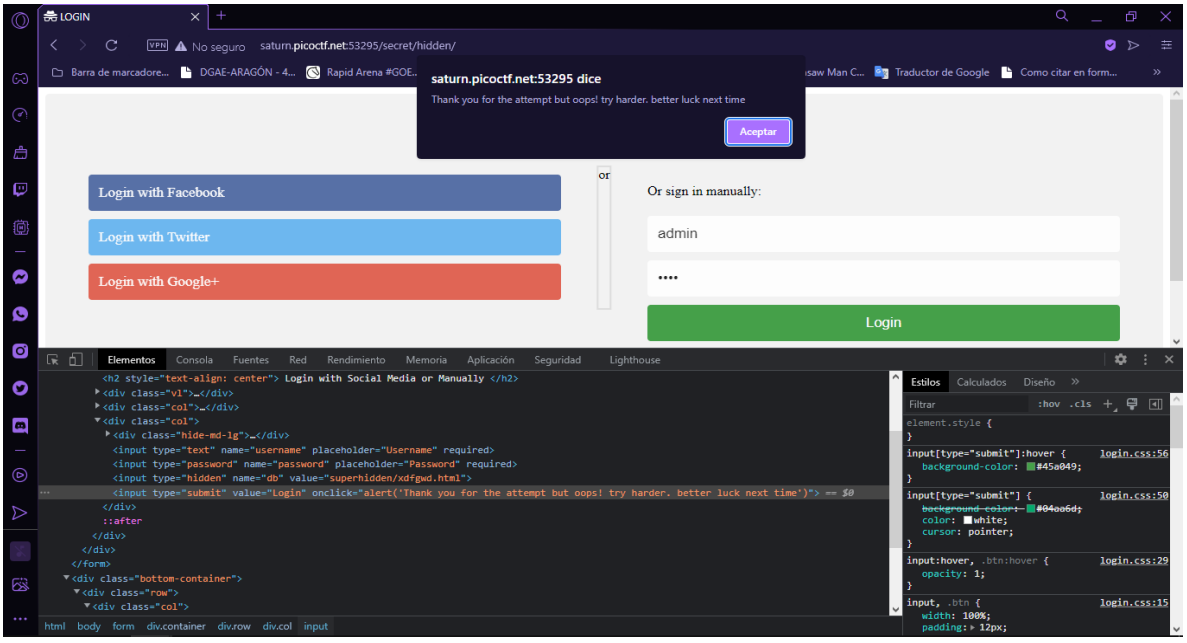


Observamos que el directorio raíz de la ruta tiene un nombre similar que el ejercicio. Si accedemos a este modificando la url del sitio de manera manual para redireccionarnos, nos encontraremos una pagina con el mensaje de que finalmente la hemos encontrado.

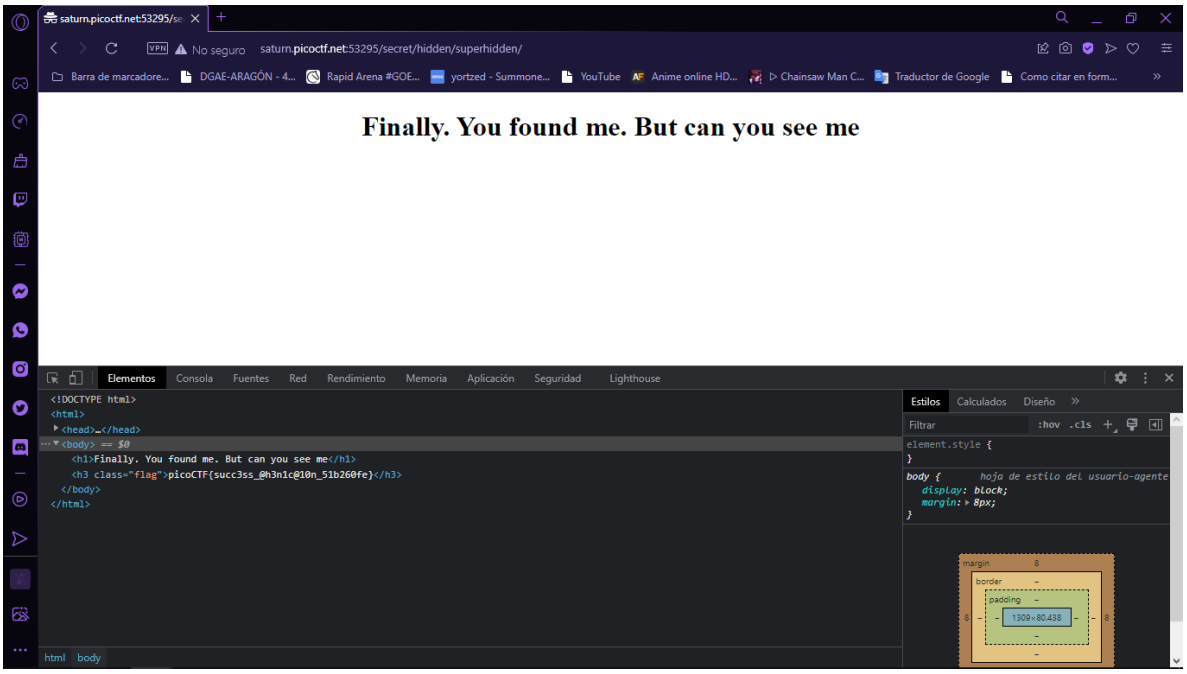
Nota: no la ruta especifica de esta pagina escrita en ninguno de los archivos de la pagina principal.



Notamos que para el archivo de estilos de esta pagina se nos redirige al directorio “hidden” (oculto) en lugar de “assets” (activos). Si revisamos este directorio “oculto” de la misma manera que hemos hecho con secret, Notaremos una nueva pagina que parece ser una pagina de login, sin embargo si inspeccionamos el botón de login notaremos que su única función es mandar un alert con un mensaje. El resto de botones no tienen ninguna función descrita.

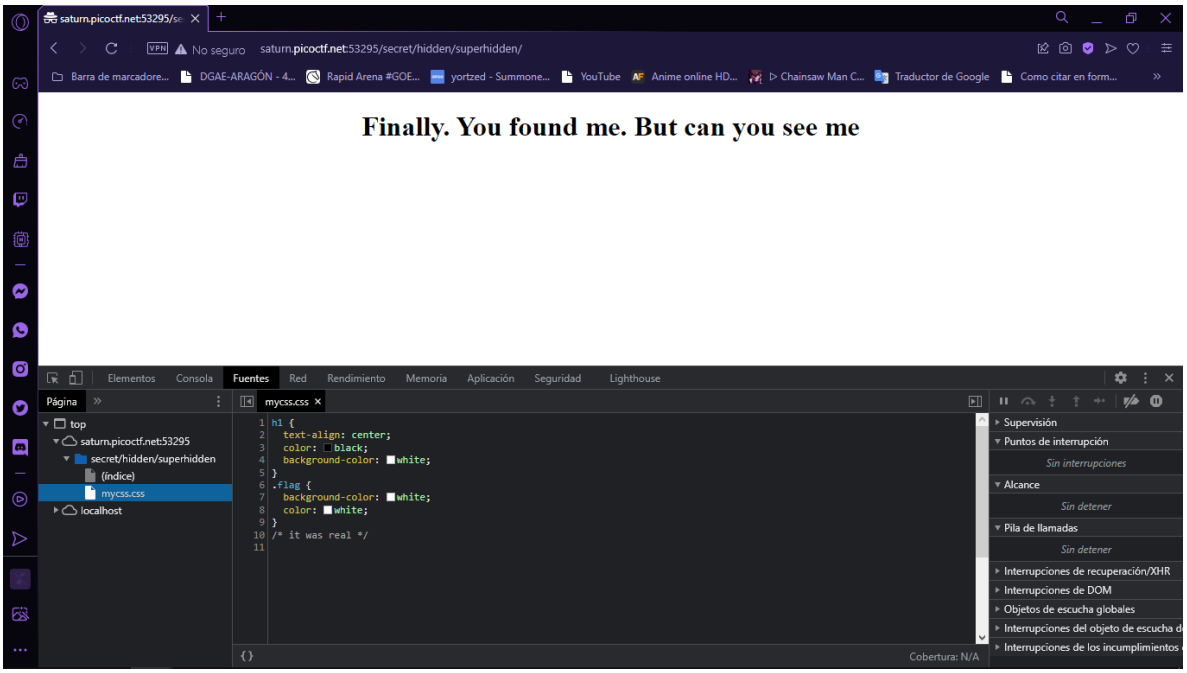


Por lo que probaremos con el mismo método que llevamos haciendo hasta ahorita. Si inspeccionamos el directorio del archivo de estilos de la pagina notaremos el directorio “superhidden”. Si nos redireccionamos a este directorio notaremos una nueva pagina con un particular mensaje, y si revisamos el html e esta encontramos la flag.

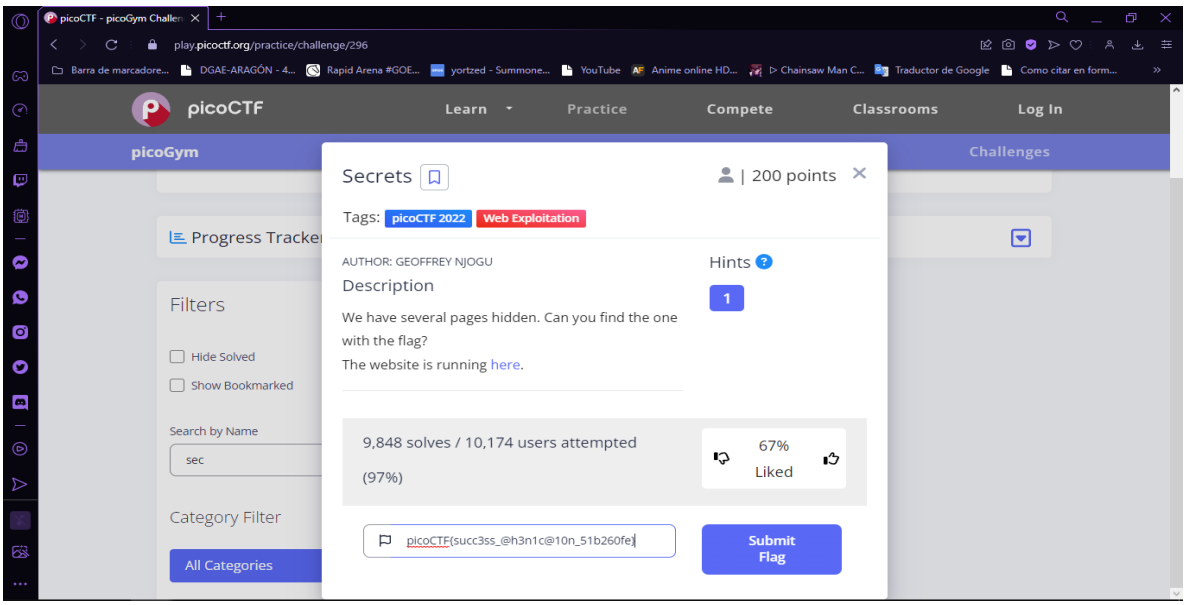


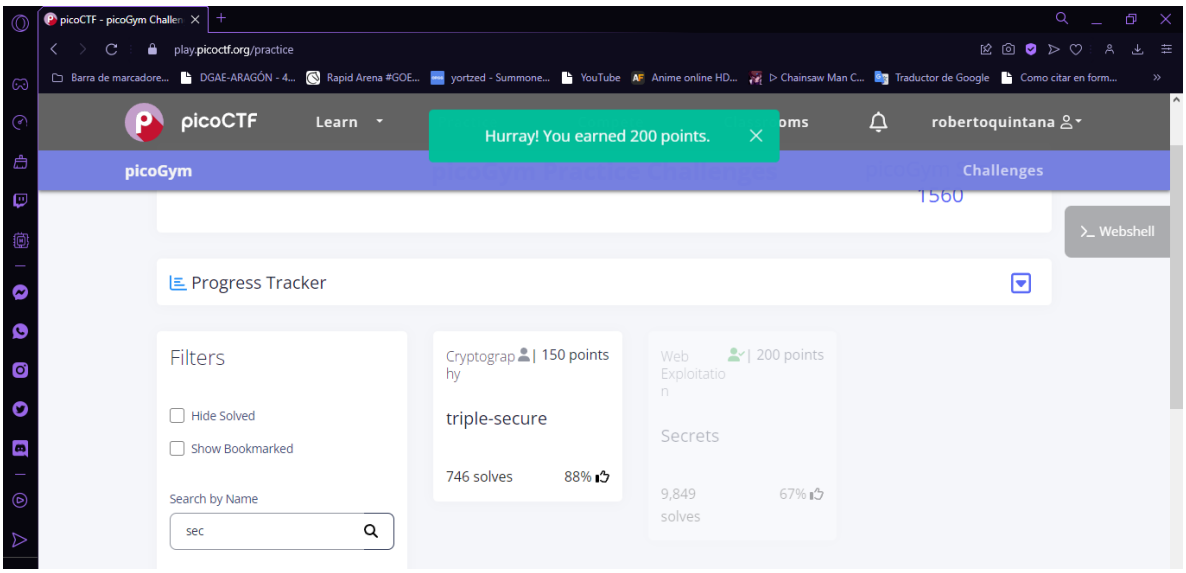
picoCTF{succ3ss_@h3n1c@10n_51b260fe}

Como curiosidad esta flag no es visible debido a que el estilo usado en la etiqueta que almacena el mensaje, indica que los carcteres contenidos se reflejan en color blanco, siendo el mismo color del fondo.



Comprobamos.





Vulnerabilidad

Obviando el echo de que ocultar información mediante la falta de contraste entre la fuente del texto y el fondo que lo contiene, no precisamente la medida de seguridad más efectiva. Con este ejercicio podemos comprobar que el echo de que nuestro sitio no refleje ningún redireccionamiento a los directorios de nuestro servidor, esto no significa que se haya impedido el acceso los mismos.

Solución

Restringir los permisos de acceso a los directorios para cualquier usuario no autorizado.