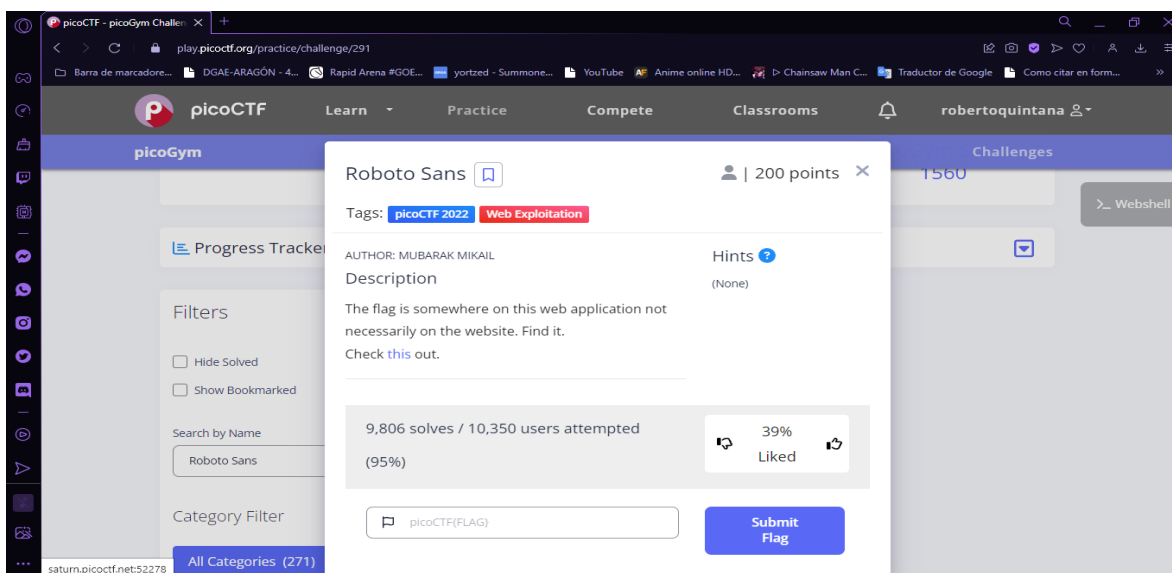


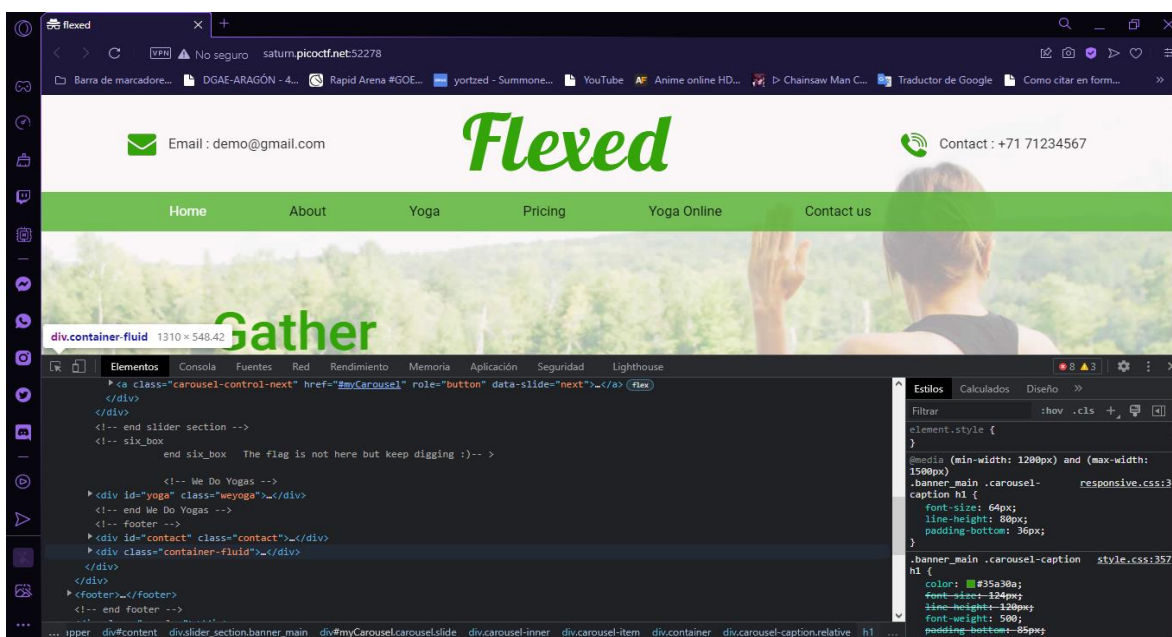
Tarea. Roboto Sans

Alumno. Quintana Escamilla Roberto Carlos

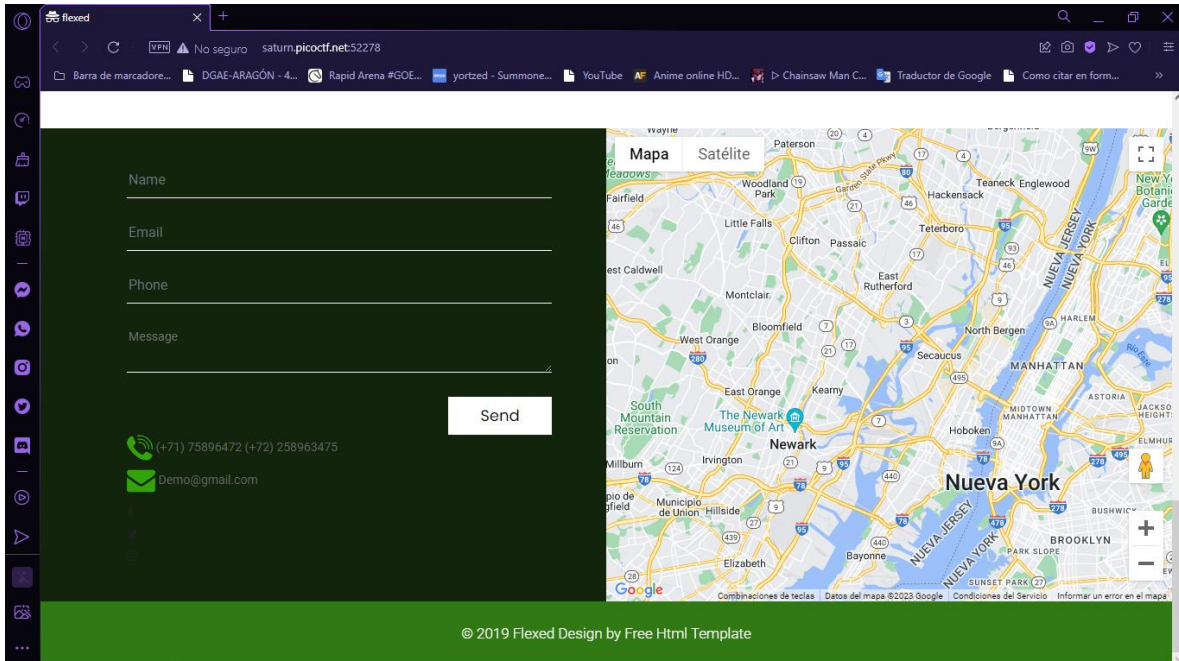
Para este ejercicio se nos indica que la flag se puede encontrar en la aplicación web sin embargo podría no encontrarse en el sitio.



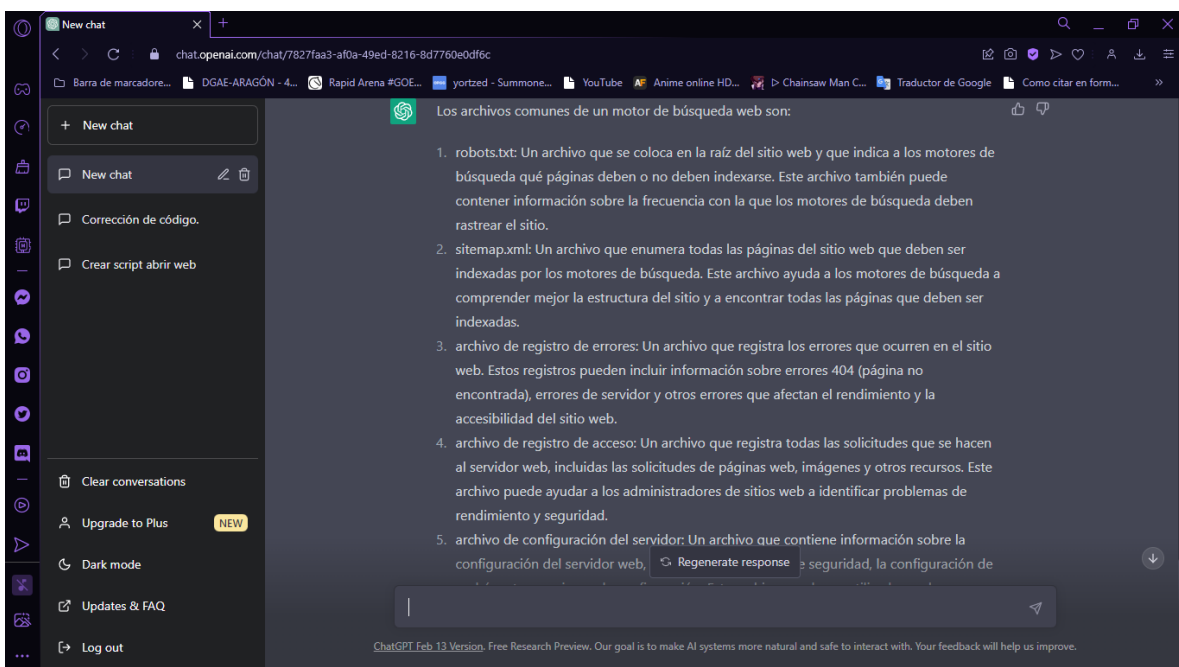
Si accedemos, notaremos un pagina conocida pues es la misma del ejercicio Search Source conteniendo incluso el mismo mensaje en los comentarios del html del index. Sin embargo como podría esperarse por la descripción del ejercicio, la flag ya no se encuentra en el archivo ccs.



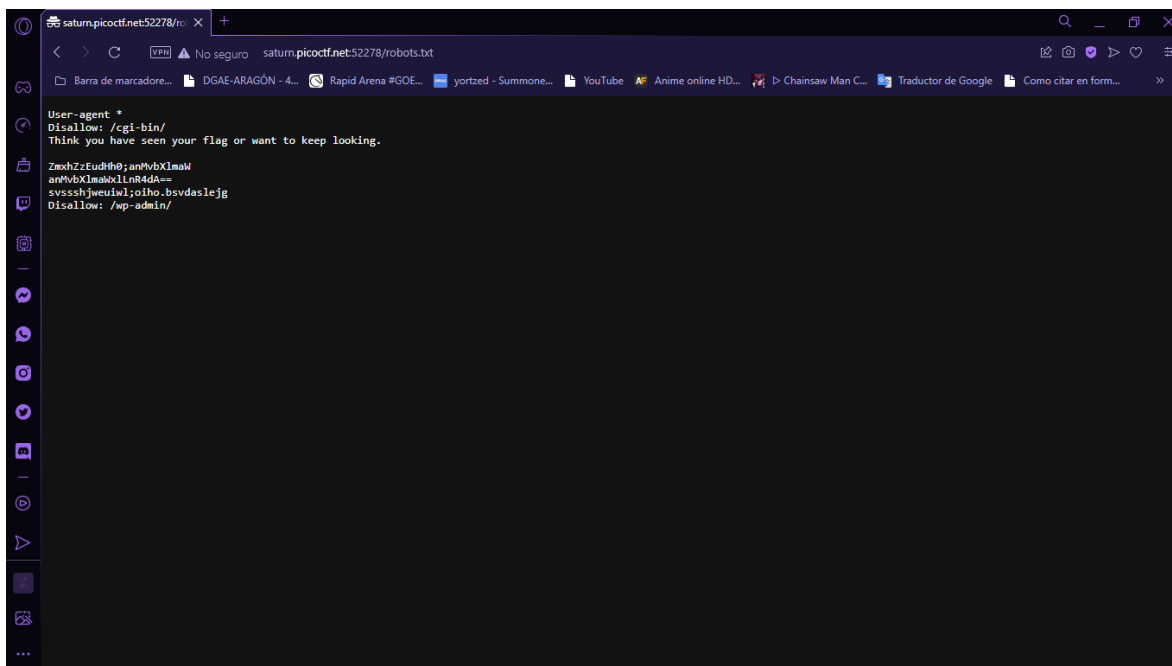
Ahora por las indicaciones, imaginamos que efectivamente la flag no se encuentra en ningún archivo del sitio web por lo que la siguiente pregunta es ¿Qué más hay? Y podemos observar que el sitio tiene redireccionamiento hacia un sitio en Google maps.



Con ayuda de chat gtp preguntamos cuales son los archivos más comunes en un motor de búsqueda web, a lo cual se nos devolverá la siguiente lista. De los cuales el primero se nombra de manera similar a una de las palabras que contiene el titulo del ejercicio.



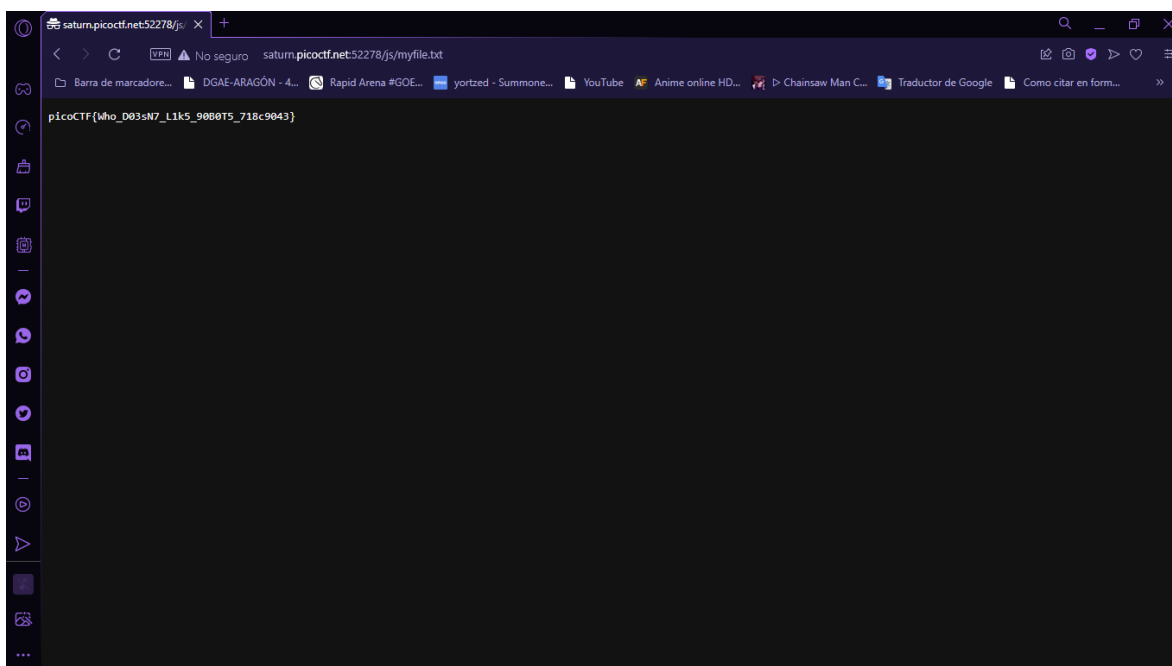
Si nos redireccionamos a este archivo por medio de la url, notaremos un par de líneas de código donde notaremos un en particular, ya que esta encriptada en base 64.



```
User-agent *
Disallow: /cgi-bin/
Think you have seen your flag or want to keep looking.
ZmxhZzEudm90bXlmaWxlnR4dA==
anMvbXlmaWxlnR4dA==
svssshjweuiwl;oiho.bsvdaslejg
Disallow: /wp-admin/
```

anMvbXlmaWxlnR4dA==

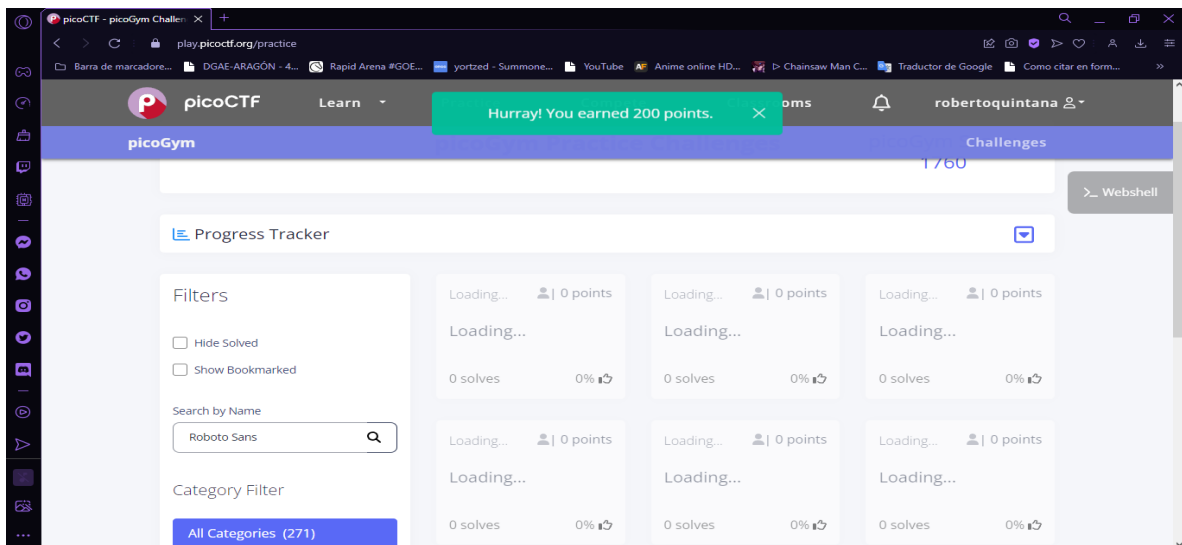
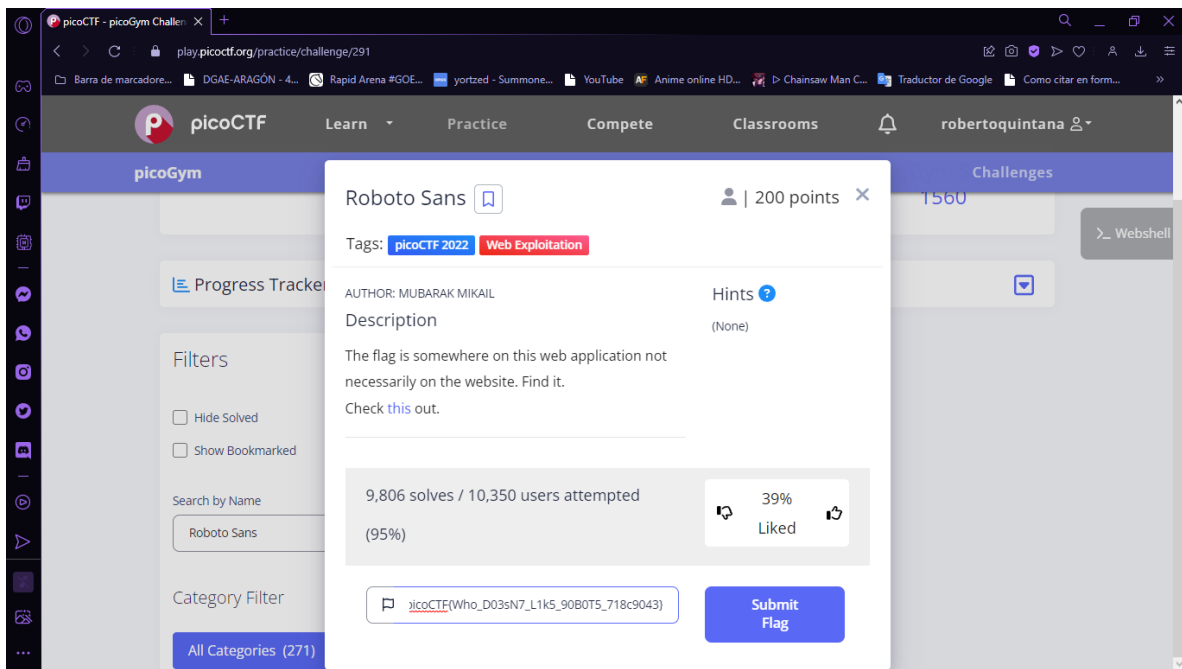
Si decodificamos este mensaje obtenemos el directorio “js/myfile.txt”, Al redireccionarnos a este sitio encontramos la flag .



```
picoCTF{Who_D03sN7_L1k5_90B0T5_718c9043}
```

picoCTF{Who_D03sN7_L1k5_90B0T5_718c9043}

Comprobamos.



Vulnerabilidad

Notamos que aun que no se tenga acceso directo o alguna descripción de todos los archivos de este sitio, notamos que aun así podemos entrar a alguno de ellos mediante la deducción de los archivos comunes que suelen tener aplicaciones similares.

Solución

Restringir el acceso a los usuarios a cualquier directorio que no sea parte del conjunto requerido para el modelo de negocio de nuestro sitio web.