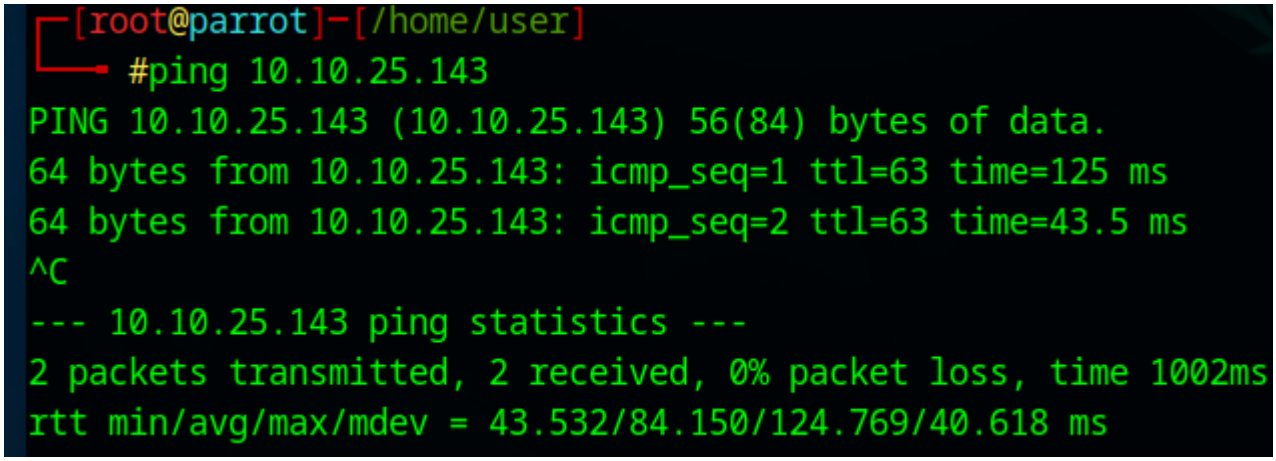
Sticker Shop – TryHackMe

Our objective is to find the flag – flag.txt

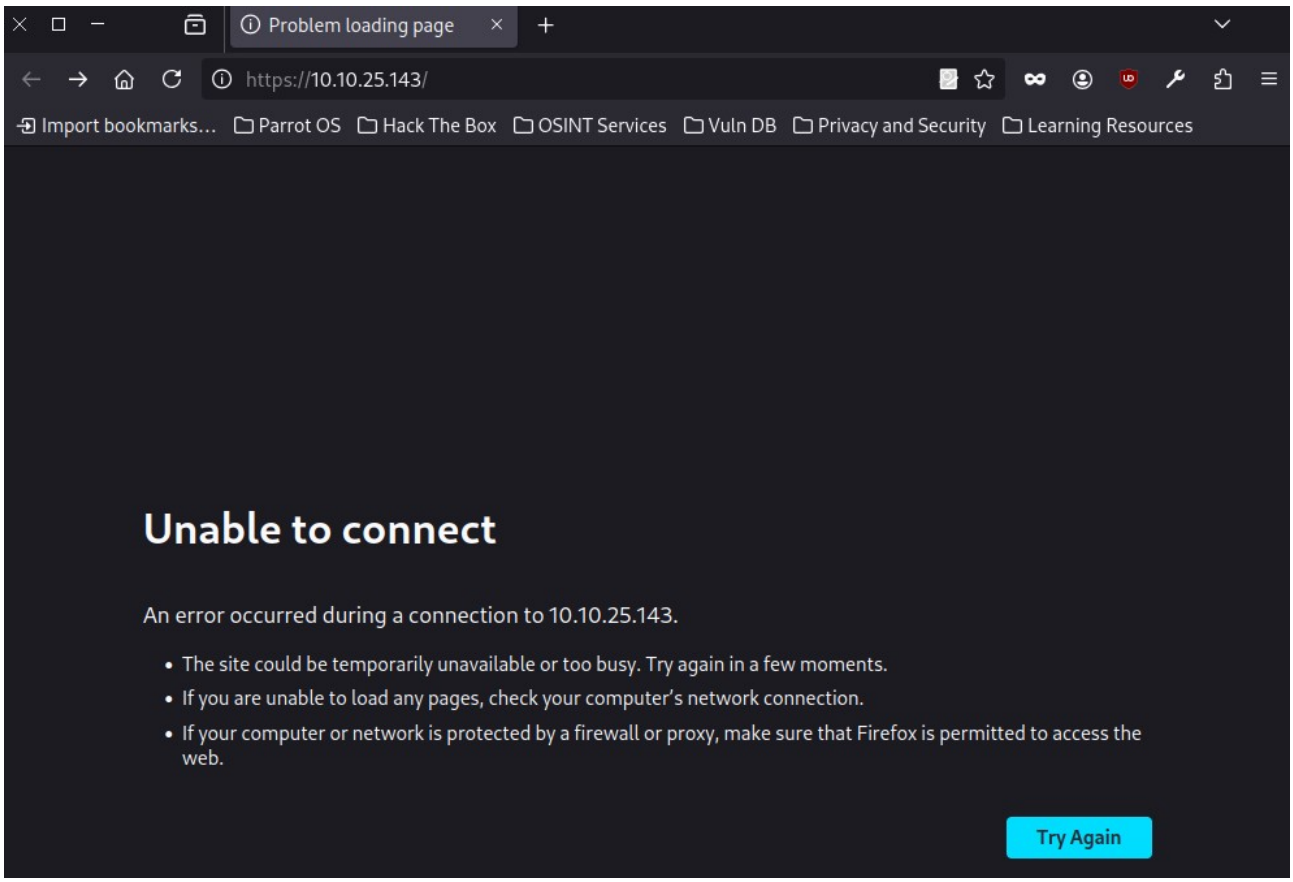
Contents

1.Reconnaissance

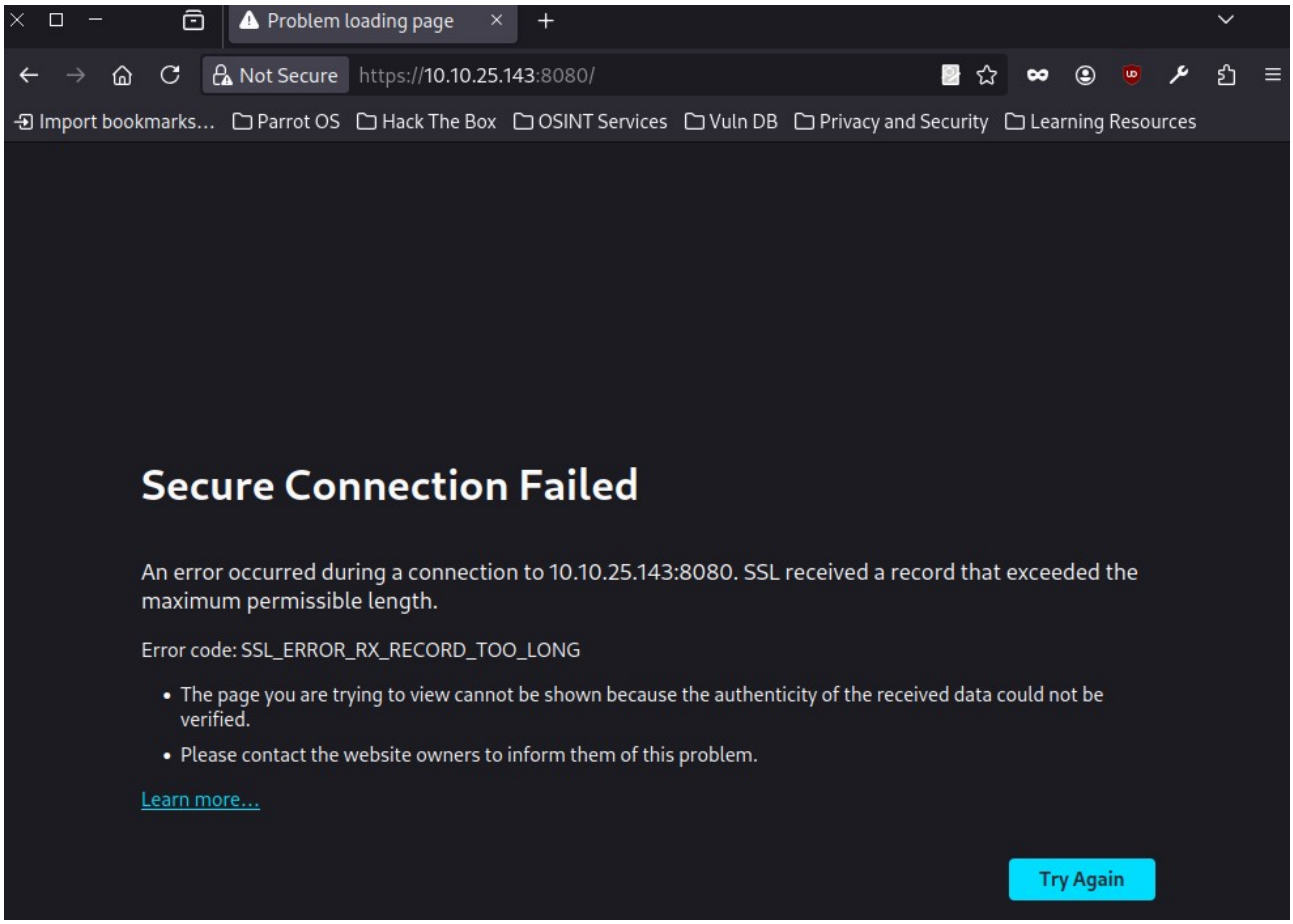
We begin by checking if the host is active.



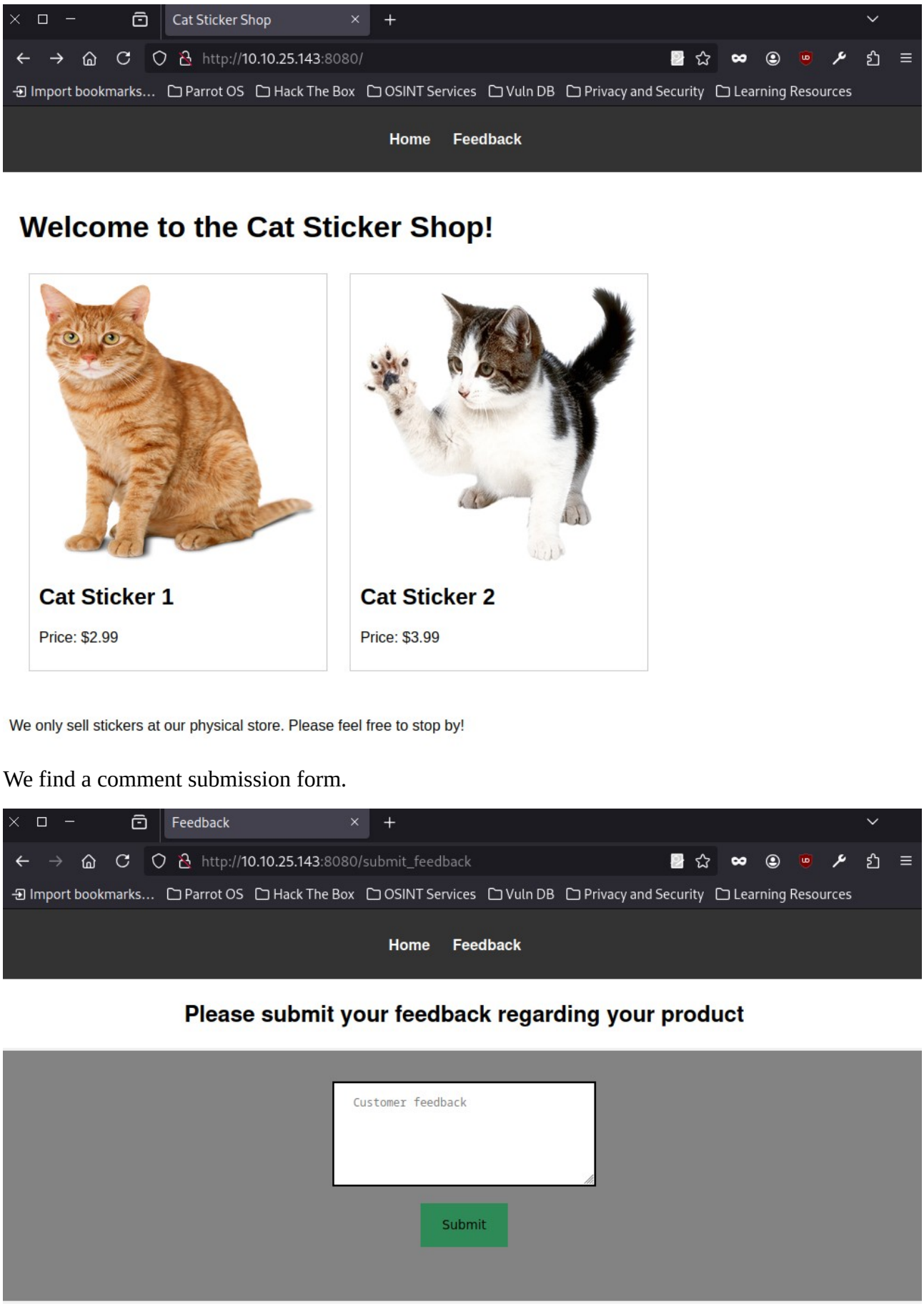
The host responds – let’s explore the website.



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



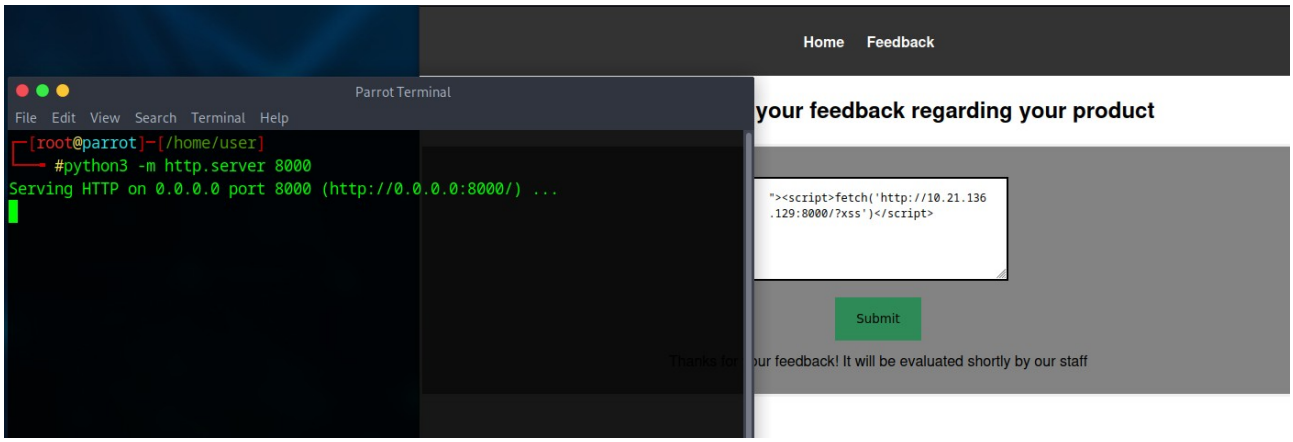
To access it, we simply remove the "s" from "https", leaving just "http".



We find a comment submission form.

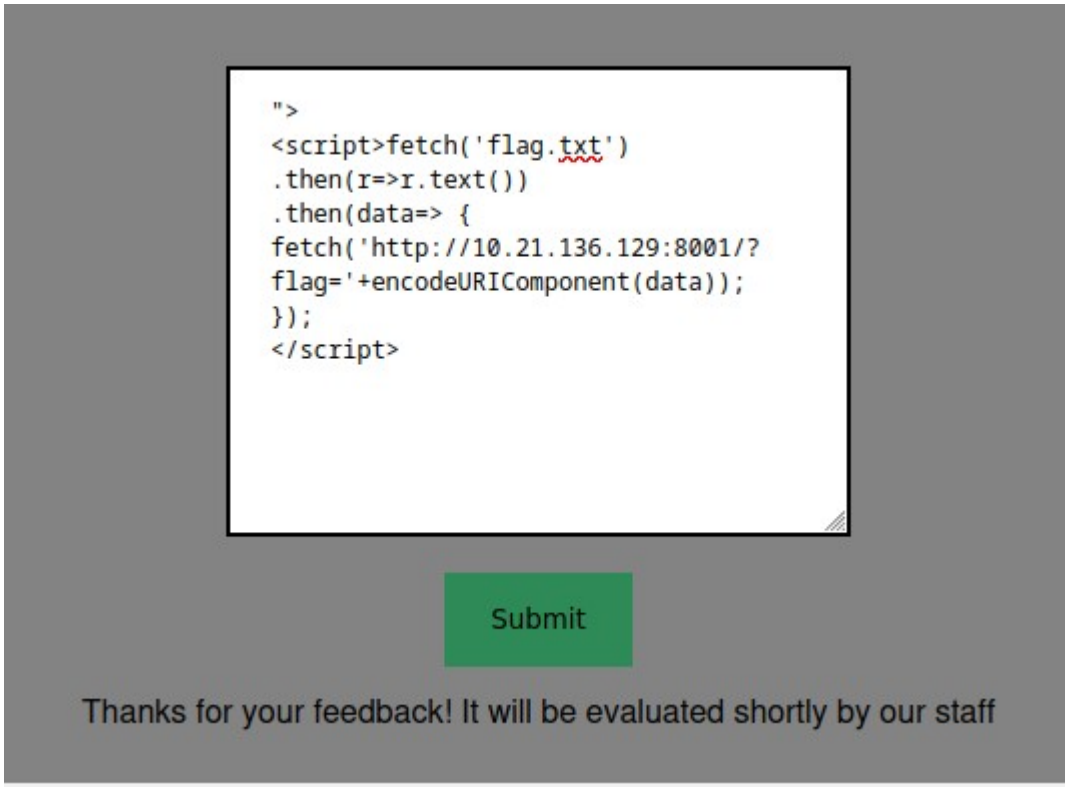
2.Flag

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



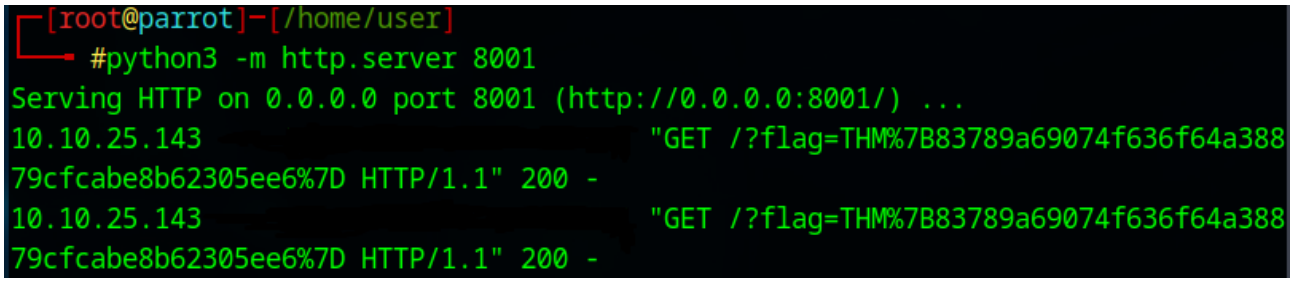
We get confirmation that the XSS attack works.

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!



3.Summary

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