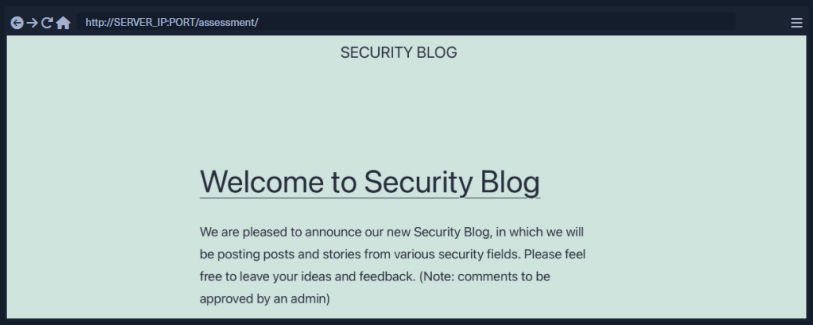
# Skills Assessment

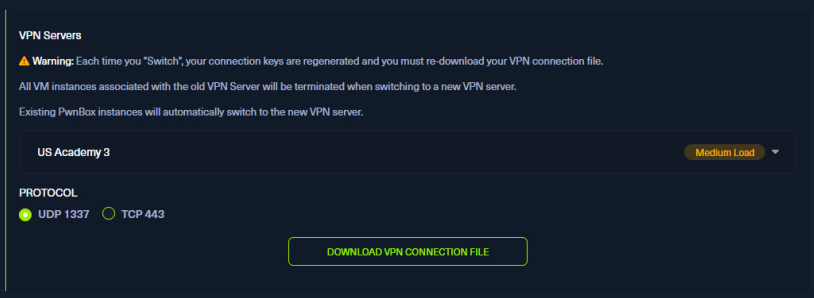
We are performing a Web Application Penetration Testing task for a company that hired you, which just released their new `Security Blog`. In our Web Application Penetration Testing plan, we reached the part where you must test the web application against Cross-Site Scripting vulnerabilities (XSS).

Start the server below, make sure you are connected to the VPN, and access the `/assessment` directory on the server using the browser:

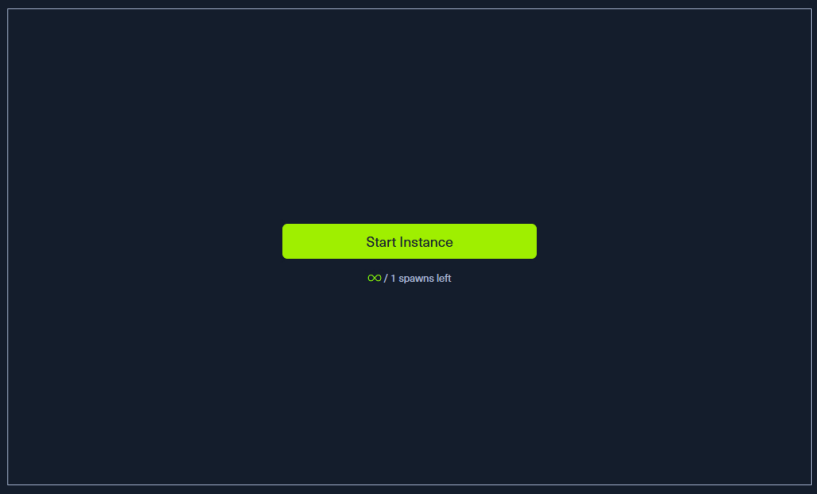



Apply the skills you learned in this module to achieve the following:

1. Identify a user-input field that is vulnerable to an XSS vulnerability
2. Find a working XSS payload that executes JavaScript code on the target's browser
3. Using the `Session Hijacking` techniques, try to steal the victim's cookies, which should contain the flag








Waiting to start...

Enable step-by-step solutions for all questions

## Questions

Answer the question(s) below to complete this Section and earn cubes!

Cheat Sheet

Download VPN Connection File

Cheat Sheet

Go to Questions

Table of Contents

XSS Basics

- Intro to XSS
- Stored XSS
- Reflected XSS
- DOM XSS
- XSS Discovery

XSS Attacks

- Defacing
- Phishing
- Session Hijacking

XSS Prevention

- XSS Prevention

Skills Assessment

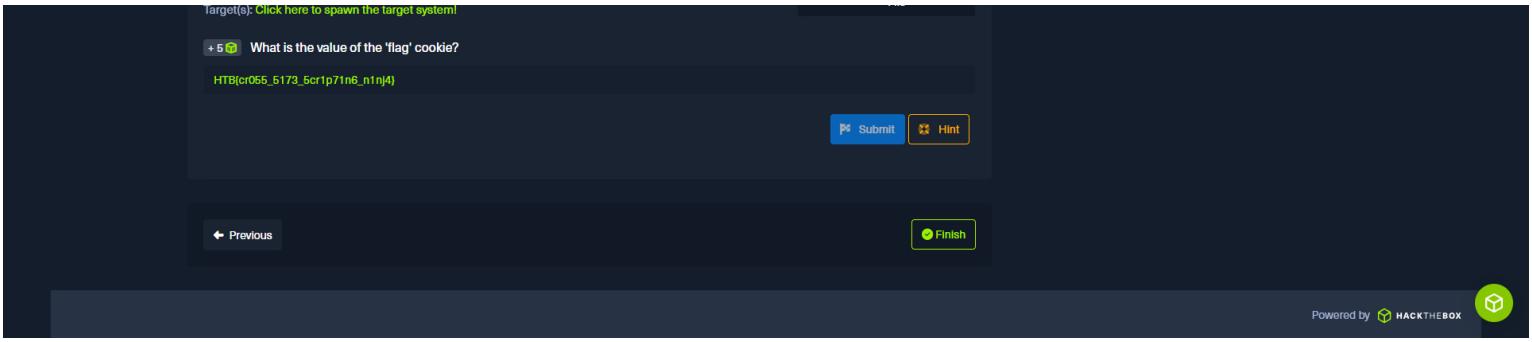
- Skills Assessment

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left


Target(s): Click here to spawn the target system!
+5
What is the value of the 'flag' cookie?
HTB{cr055_5173_5cr1p71n6_n1nj4}
Submit
Hint
Previous
Finish
Powered by HACKTHEBOX