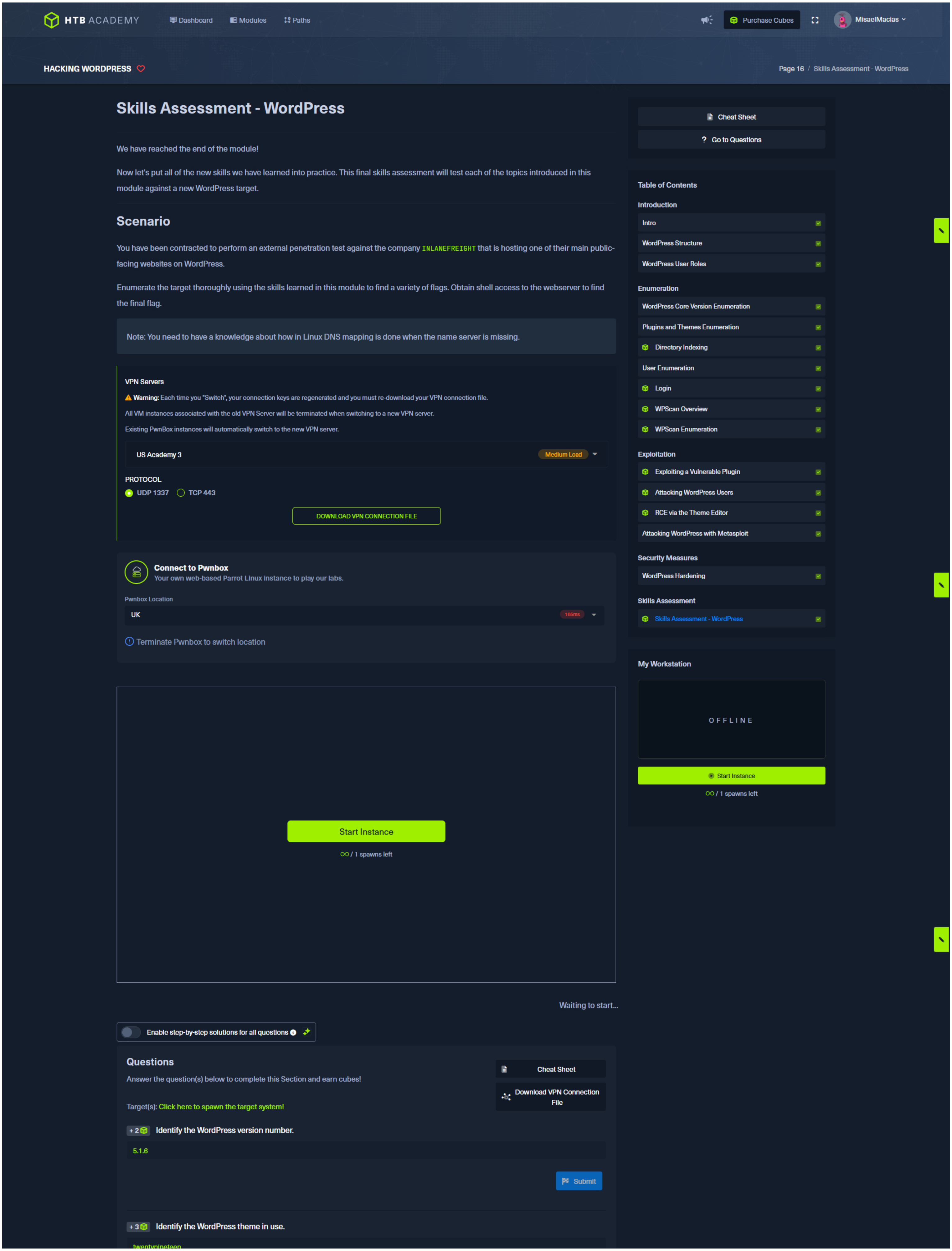


Skills Assessment - WordPress

We have reached the end of the module!

Now let's put all of the new skills we have learned into practice. This final skills assessment will test each of the topics introduced in this module against a new WordPress target.

Scenario

You have been contracted to perform an external penetration test against the company `INLANEFREIGHT` that is hosting one of their main public-facing websites on WordPress.

Enumerate the target thoroughly using the skills learned in this module to find a variety of flags. Obtain shell access to the webserver to find the final flag.

> Note: You need to have a knowledge about how in Linux DNS mapping is done when the name server is missing.

VPN Servers

⚠ **Warning:** Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.

All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.

Existing PwnBox instances will automatically switch to the new VPN server.

US Academy 3 — Medium Load

PROTOCOL

● UDP 1337 ○ TCP 443

DOWNLOAD VPN CONNECTION FILE

Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK — 165ms

Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

Enable step-by-step solutions for all questions

Questions

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

Target(s): Click here to spawn the target system!

Cheat Sheet

Download VPN Connection File

+ 2 Identify the WordPress version number.

5.1.6

Submit

+ 3 Identify the WordPress theme in use.

twentynineteen

Cheat Sheet

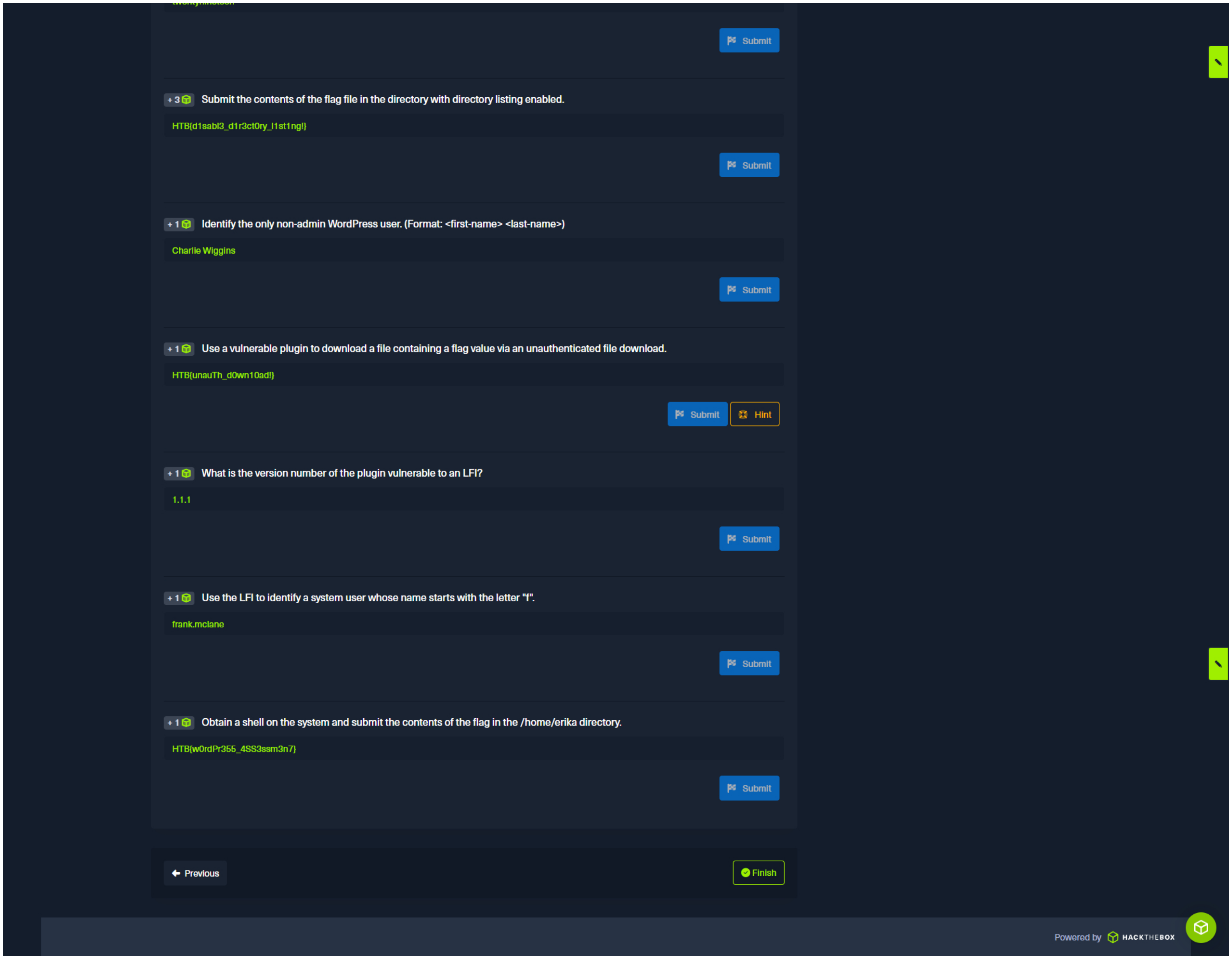
? Go to Questions

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left



twentynineteen

+ 3 Submit the contents of the flag file in the directory with directory listing enabled.

HTB{d1sabl3_d1r3ct0ry_l1st1ng!}

+ 1 Identify the only non-admin WordPress user. (Format: <first-name> <last-name>)

Charlie Wiggins

+ 1 Use a vulnerable plugin to download a file containing a flag value via an unauthenticated file download.

HTB{unauTh_d0wn10ad!}

+ 1 What is the version number of the plugin vulnerable to an LFI?

1.1.1

+ 1 Use the LFI to identify a system user whose name starts with the letter "f".

frank.mclane

+ 1 Obtain a shell on the system and submit the contents of the flag in the /home/erika directory.

HTB{w0rdPr355_4SS3ssm3n7}