Skills Assessment - Web Fuzzing

You are given an online academy's IP address but have no further information about their website. As the first step of conducting a Penetration Test, you are expected to locate all pages and domains linked to their IP to enumerate the IP and domains properly.

Finally, you should do some fuzzing on pages you identify to see if any of them has any parameters that can be interacted with. If you do find active parameters, see if you can retrieve any data from them.

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

Pwnbox Location

UK 137ms

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!

Cheat Sheet

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

+1 Run a sub-domain/vhost fuzzing scan on '*.academy.htb' for the IP shown above. What are all the sub-domains you can identify? (Only write the sub-domain name)

test archive faculty

Submit

+1 Before you run your page fuzzing scan, you should first run an extension fuzzing scan. What are the different extensions accepted by the domains?

.php .php7 .phps

Submit Hint

+2 One of the pages you will identify should say 'You don't have access!'. What is the full page URL?

http://faculty.academy.htb:PORT/courses/linux-security.php7

Submit Hint

+1 In the page from the previous question, you should be able to find multiple parameters that are accepted by the page. What are they?

user username

Submit Hint

+2 Try fuzzing the parameters you identified for working values. One of them should return a flag. What is the content of the flag?

Cheat Sheet

Go to Questions

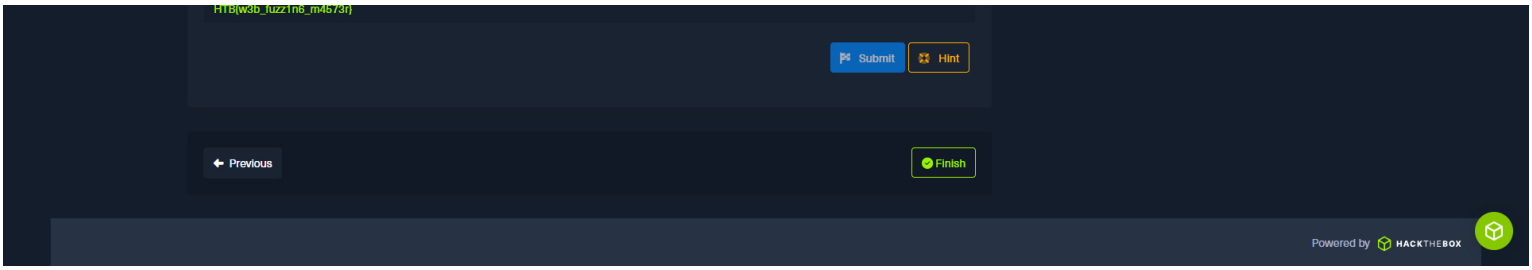
Table of Contents

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left


HTB{w3b_fuzz1n6_m4573r}
Submit
Hint
Previous
Finish
Powered by HACKTHEBOX