

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.

Start Instance

1 / 1 spawns left

Waiting to start...

Questions

Cheat Sheet

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

Target: [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)

Submit your answer here...

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?

Submit your answer here...

Submit


Hint

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

Submit your answer here...

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?

Submit your answer here...

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?

Submit your answer here...

Submit

Hint



← Previous

 Cheat Sheet







? Go to Questions

Table of Contents

Introduction

Introduction	
Web Fuzzing	

Basic Fuzzing

 Directory Fuzzing	
 Page Fuzzing	
 Recursive Fuzzing	

Domain Fuzzing

DNS Records



 Sub-domain Fuzzing



Vhost Fuzzing



 Filtering Results



Parameter Fuzzing

 Parameter Fuzzing - GET



Parameter Fuzzing - POST



 Value Fuzzing




Skills Assessment

 Skills Assessment - Web Fuzzing

My Workstation

O F F L I N E

 Start Instance

1 / 1 spawns left