Skills Assessment - File Upload Attacks

You are contracted to perform a penetration test for a company's e-commerce web application. The web application is in its early stages, so you will only be testing any file upload forms you can find.

Try to utilize what you learned in this module to understand how the upload form works and how to bypass various validations in place (if any) to gain remote code execution on the back-end server.

Extra Exercise

Try to note down the main security issues found with the web application and the necessary security measures to mitigate these issues and prevent further exploitation.

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

Pwnbox Location

UK 139ms

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!

+7 Try to exploit the upload form to read the flag found at the root directory "/".

HTB{m4573r1ng_upl04d_3xpl0174710n}

Submit Hint

Previous Finish

Cheat Sheet

Go to Questions

Table of Contents

Intro to File Upload Attacks

Basic Exploitation

Absent Validation

Upload Exploitation

Bypassing Filters

Client-Side Validation

Blacklist Filters

Whitelist Filters

Type Filters

Other Upload Attacks

Limited File Uploads

Other Upload Attacks

Prevention

Preventing File Upload Vulnerabilities

Skills Assessment

Skills Assessment - File Upload Attacks

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left