

Skills Assessment

You are contracted to perform a penetration test for a company, and through your pentest, you stumble upon an interesting file manager web application. As file managers tend to execute system commands, you are interested in testing for command injection vulnerabilities.

Use the various techniques presented in this module to detect a command injection vulnerability and then exploit it, evading any filters in place.

Start Instance

0 / 1 spawns left

Waiting to start...

Questions

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

Cheat Sheet

Target: Click here to spawn the target system!

Authenticate to with user "guest" and password "guest"

+ 10 What is the content of '/flag.txt'?

Submit your answer here...

Submit

Hint

Previous

Cheat Sheet

Go to Questions

Table of Contents

Intro to Command Injections



Exploitation

Detection



Injecting Commands



Other Injection Operators



Filter Evasion

Identifying Filters



Bypassing Space Filters



Bypassing Other Blacklisted Characters

Bypassing Blacklisted Commands

Advanced Command Obfuscation

Evasion Tools



Prevention

Command Injection Prevention

Skills Assessment

Skills Assessment

My Workstation

OFFLINE

Start Instance

0 / 1 spawns left