Skills Assessment - Using Web Proxies

We are performing internal penetration testing for a local company. As you come across their internal web applications, you are presented with different situations where Burp/ZAP may be helpful. Read each of the scenarios in the questions below, and determine the features that would be the most useful for each case. Then, use it to help you in reaching the specified goal.

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!

+2 The /lucky.php page has a button that appears to be disabled. Try to enable the button, and then click it to get the flag.

HTB{d154bl3d_bu770n5_w0n7_570p_m3}

Submit Hint

+2 The /admin.php page uses a cookie that has been encoded multiple times. Try to decode the cookie until you get a value with 31-characters. Submit the value as the answer.

3dac93b8cd250aa8c1a36fffc79a17a

Submit Hint

+5 Once you decode the cookie, you will notice that it is only 31 characters long, which appears to be an md5 hash missing its last character. So, try to fuzz the last character of the decoded md5 cookie with all alpha-numeric characters, while encoding each request with the encoding methods you identified above. (You may use the "alphanum-case.txt" wordlist from Seclist for the payload)

HTB{burp_1n7rud3r_n1nj4!}

Submit Hint

+2 You are using the 'auxiliary/scanner/http/coldfusion_locale_traversal' tool within Metasploit, but it is not working properly for you. You decide to capture the request sent by Metasploit so you can manually verify it and repeat it. Once you capture the request, what is the 'XXXXX' directory being called in '/XXXXX/administrator/..'?

CFIDE

Submit Hint

Cheat Sheet

Go to Questions

Table of Contents

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left


Previous
Finish
Powered by HACKTHEBOX