Session Security - Skills Assessment

You are currently participating in a bug bounty program.

- The only URL in scope is http://minilab.htb.net
- Attacking end-users through client-side attacks is in scope for this particular bug bounty program.
- Test account credentials:
  - Email: heavycat106
  - Password: rocknrol
- Through dirbusting, you identified the following endpoint http://minilab.htb.net/submit-solution

Find a way to hijack an admin's session. Once you do that, answer the two questions below.

VPN Servers

⚠ **Warning:** Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.

All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.

Existing PwnBox instances will automatically switch to the new VPN server.

US Academy 3 Medium Load

PROTOCOL

UDP 1337 TCP 443

DOWNLOAD VPN CONNECTION FILE

Connect to Pwnbox

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

Pwnbox Location

UK 140ms

Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

Enable step-by-step solutions for all questions

? Go to Questions

Table of Contents

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

Questions

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

Download VPN Connection File

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

vHosts needed for these questions:

- `minilab.htb.net`

+ 9 Read the flag residing in the admin's public profile. Answer format: [string]

[YOU_ARE_A_SESSION_WARRIOR]

Submit Hint

+ 1 Go through the PCAP file residing in the admin's public profile and identify the flag. Answer format: FLAG{string}

FLAG{SUCCESS_YOU_PWN3D_US_H0PE_YOU_ENJ0YED}

Submit

Previous Finish

Powered by HACKTHEBOX