

# Web Attacks - Skills Assessment

## Scenario

You are performing a web application penetration test for a software development company, and they task you with testing the latest build of their social networking web application. Try to utilize the various techniques you learned in this module to identify and exploit multiple vulnerabilities found in the web application.

The login details are provided in the question below.

**Start Instance**

∞ / 1 spawns left

Waiting to start...

## Questions

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

Target: [Click here to spawn the target system!](#)

 Authenticate to with user "htb-student" and password "Academy\_student!"

+ 5  Try to escalate your privileges and exploit different vulnerabilities to read the flag at '/flag.php'.

Submit your answer here...

 Submit

 No Hint

 Previous

OFFLINE

 Start Instance

∞ / 1 spawns left

## Table of Contents

Introduction to Web Attacks

### HTTP Verb Tampering

Intro to HTTP Verb Tampering

 Bypassing Basic Authentication

 Bypassing Security Filters

Verb Tampering Prevention

### Insecure Direct Object References (IDOR)

Intro to IDOR

 Identifying IDORs

 Mass IDOR Enumeration

 Bypassing Encoded References

 IDOR in Insecure APIs

 Chaining IDOR Vulnerabilities

IDOR Prevention

### XML External Entity (XXE) Injection

Intro to XXE

 Local File Disclosure

 Advanced File Disclosure

 Blind Data Exfiltration

XXE Prevention

### Skills Assessment

 Web Attacks - Skills Assessment

## My Workstation

OFFLINE

 Start Instance

∞ / 1 spawns left