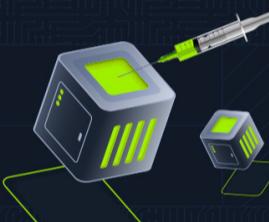


Targets compromised: 141
Ranking: Top 5%

MODULE

PROGRESS

	<h3>Intro to Academy</h3> <p>8 Sections Fundamental General</p> <p>Your first stop in Hack The Box Academy to become acquainted with the platform, its features, and its learning process.</p>	100% Completed
	<h3>Hacking WordPress</h3> <p>16 Sections Easy Offensive</p> <p>WordPress is an open-source Content Management System (CMS) that can be used for multiple purposes.</p>	93.75% Completed
	<h3>SQL Injection Fundamentals</h3> <p>17 Sections Medium Offensive</p> <p>Databases are an important part of web application infrastructure and SQL (Structured Query Language) to store, retrieve, and manipulate information stored in them. SQL injection is a code injection technique used to take advantage of coding vulnerabilities and inject SQL queries via an application to bypass authentication, retrieve data from the back-end database, or achieve code execution on the underlying server.</p>	100% Completed
	<h3>Web Requests</h3> <p>8 Sections Fundamental General</p> <p>This module introduces the topic of HTTP web requests and how different web applications utilize them to communicate with their backends.</p>	100% Completed
	<h3>JavaScript Deobfuscation</h3> <p>11 Sections Easy Defensive</p> <p>This module will take you step-by-step through the fundamentals of JavaScript Deobfuscation until you can deobfuscate basic JavaScript code and understand its purpose.</p>	100% Completed
	<h3>Attacking Web Applications with Ffuf</h3> <p>13 Sections Easy Offensive</p> <p>This module covers the fundamental enumeration skills of web fuzzing and directory brute forcing using the Ffuf tool. The techniques learned in this module will help us in locating hidden pages, directories, and parameters when targeting web applications.</p>	100% Completed
	<h3>Login Brute Forcing</h3> <p>13 Sections Easy Offensive</p> <p>The module contains an exploration of brute-forcing techniques, including the use of tools like Hydra and Medusa, and the importance of strong password practices. It covers various attack scenarios, such as targeting SSH, FTP, and web login forms.</p>	100% Completed

SQLMap Essentials

11 Sections | Easy | Offensive

The SQLMap Essentials module will teach you the basics of using SQLMap to discover various types of SQL Injection vulnerabilities, all the way to the advanced enumeration of databases to retrieve all data of interest.

45.45% Completed

Introduction to Web Applications

17 Sections | Fundamental | General

In the Introduction to Web Applications module, you will learn all of the basics of how web applications work and begin to look at them from an information security perspective.

100% Completed

Broken Authentication

14 Sections | Medium | Offensive

Authentication is probably the most straightforward and prevalent measure used to secure access to resources, and it's the first line of defense against unauthorized access. Broken authentication is listed as #7 on the 2021 OWASP Top 10 Web Application Security Risks, falling under the broader category of Identification and Authentication failures. A vulnerability or misconfiguration at the authentication stage can impact an application's overall security.

100% Completed

Cross-Site Scripting (XSS)

10 Sections | Easy | Offensive

Cross-Site Scripting (XSS) vulnerabilities are among the most common web application vulnerabilities. An XSS vulnerability may allow an attacker to execute arbitrary JavaScript code within the target's browser and result in complete web application compromise if chained together with other vulnerabilities. This module will teach you how to identify XSS vulnerabilities and exploit them.

100% Completed

Command Injections

12 Sections | Medium | Offensive

Command injection vulnerabilities can be leveraged to compromise a hosting server and its entire network. This module will teach you how to identify and exploit command injection vulnerabilities and how to use various filter bypassing techniques to avoid security mitigations.

100% Completed

Using Web Proxies

15 Sections | Easy | Offensive

Web application penetration testing frameworks are an essential part of any web penetration test. This module will teach you two of the best frameworks: Burp Suite and OWASP ZAP.

100% Completed

Web Attacks

18 Sections | Medium | Offensive

This module covers three common web vulnerabilities, HTTP Verb Tampering, IDOR, and XXE, each of which can have a significant impact on a company's systems. We will cover how to identify, exploit, and prevent each of them through various methods.

100% Completed

Information Gathering - Web Edition

19 Sections | Easy | Offensive

This module equips learners with essential web reconnaissance skills, crucial for ethical hacking and penetration testing. It explores both active and passive techniques, including DNS enumeration, web crawling, analysis of web archives and HTTP headers, and fingerprinting web technologies.

100% Completed



File Upload Attacks

11 Sections | Medium | Offensive

Arbitrary file uploads are among the most critical web vulnerabilities. These flaws enable attackers to upload malicious files, execute arbitrary commands on the back-end server, and even take control over the entire server and all web applications hosted on it and potentially gain access to sensitive data or cause a service disruption.

100% Completed



Server-side Attacks

19 Sections | Medium | Offensive

A backend that handles user-supplied input insecurely can lead to devastating security vulnerabilities such as sensitive information disclosure and remote code execution. This module covers how to identify and exploit server-side bugs, including Server-Side Request Forgery (SSRF), Server-Side Template Injection (SSTI), and Server-Side Includes (SSI) injection attacks.

100% Completed

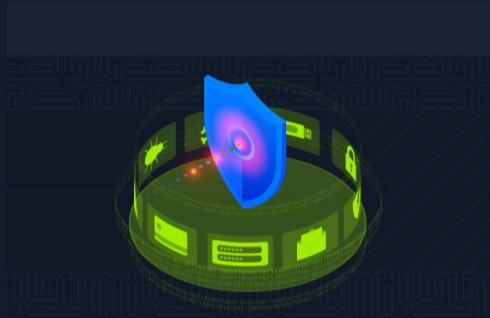


Session Security

14 Sections | Medium | Offensive

Maintaining and keeping track of a user's session is an integral part of web applications. It is an area that requires extensive testing to ensure it is set up robustly and securely. This module covers the most common attacks and vulnerabilities that can affect web application sessions, such as Session Hijacking, Session Fixation, Cross-Site Request Forgery, Cross-Site Scripting, and Open Redirects.

100% Completed



Web Service & API Attacks

13 Sections | Medium | Offensive

Web services and APIs are frequently exposed to provide certain functionalities in a programmatic way between heterogeneous devices and software components. Both web services and APIs can assist in integrating different applications or facilitate separation within a given application. This module covers how to identify the functionality a web service or API offers and exploit any security-related inefficiencies.

100% Completed



Attacking GraphQL

9 Sections | Medium | Offensive

GraphQL is a query language for APIs as an alternative to REST APIs. Clients are able to request data through GraphQL queries. If improperly configured or implemented, common web security vulnerabilities such as Information Disclosure, SQL Injection, and Insecure Direct Object Reference (IDOR) may arise.

100% Completed

