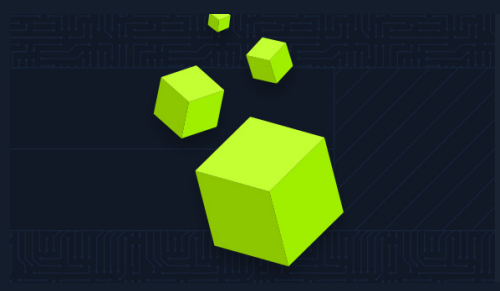
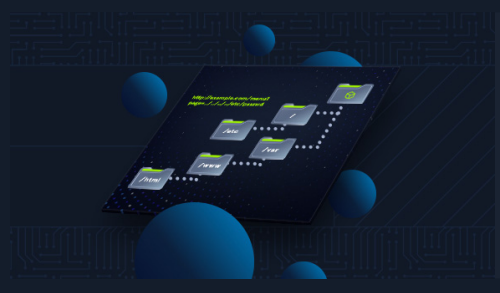
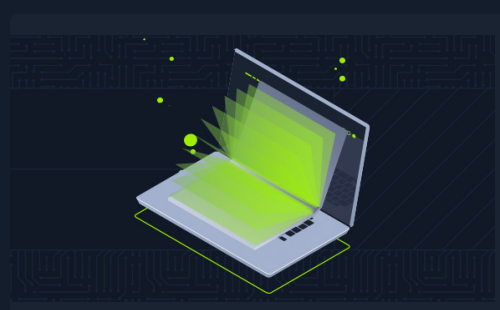
Student Transcript

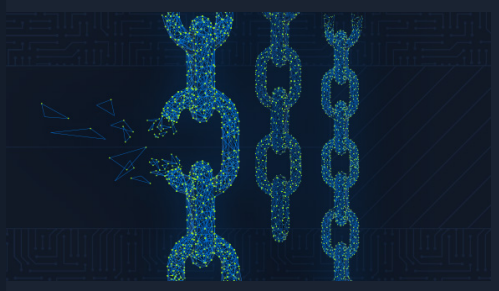
18-04-2026

HTB ACADEMY

Abram Magwai
#635545

Targets compromised: 95
Ranking: Top 10%

MODULE	PROGRESS
 Intro to Academy 8 Sections · Fundamental · General Your first stop in Hack The Box Academy to become acquainted with the platform, its features, and its learning process.	100% Completed
 Learning Process 20 Sections · Fundamental · General The learning process is one of the essential and most important components that is often overlooked. This module does not teach you techniques to learn but describes the process of learning adapted to the field of information security. You will learn to understand how and when we learn best and increase and improve your learning efficiency greatly.	100% Completed
 Cracking Passwords with Hashcat 14 Sections · Medium · Offensive This module covers the fundamentals of password cracking using the Hashcat tool.	71.43% Completed
 File Inclusion 11 Sections · Medium · Offensive File Inclusion is a common web application vulnerability, which can be easily overlooked as part of a web application's functionality.	63.64% Completed
 Using the Metasploit Framework 15 Sections · Easy · Offensive The Metasploit Framework is an open-source set of tools used for network enumeration, attacks, testing security vulnerabilities, evading detection, performing privilege escalation attacks, and performing post-exploitation.	6.67% Completed
 JavaScript Deobfuscation 11 Sections · Easy · Defensive 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.	100% Completed
 Attacking Web Applications with Ffuf 13 Sections · Easy · Offensive 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.	15.38% 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.

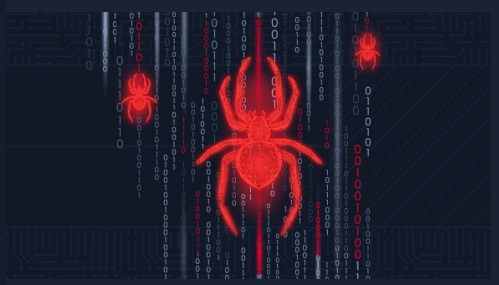
100% Completed

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



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.

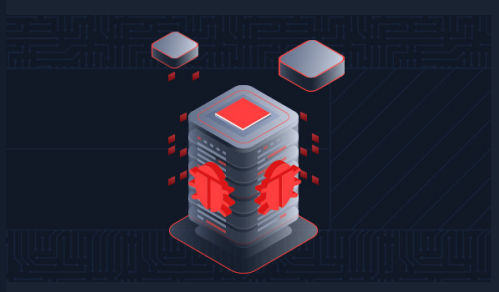
100% Completed

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

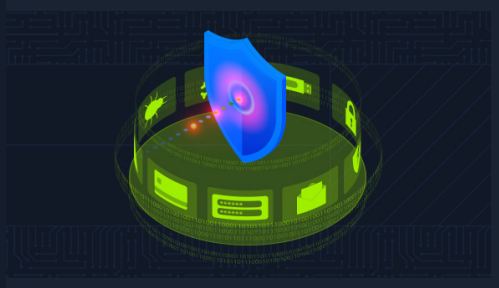


Server-side Attacks

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



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

Modern Web Exploitation Techniques

18 Sections | Hard | Offensive

This module covers advanced web concepts and exploitation techniques, including performing DNS Rebinding to bypass faulty SSRF filters and the Same-Origin Policy, identifying and exploiting Second-Order vulnerabilities, and conducting common web attacks via WebSocket connections.

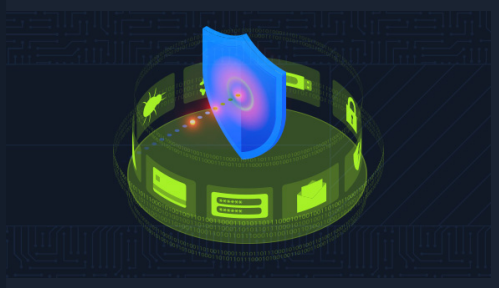
100% Completed

Advanced XSS and CSRF Exploitation

17 Sections | Medium | Offensive

Modern web browsers and applications utilize a variety of security measures to protect against CSRF and XSS vulnerabilities, rendering their exploitation more difficult. This module focuses on exploiting advanced CSRF and XSS vulnerabilities, identifying and bypassing weak and wrongly implemented defensive mechanisms.

100% Completed



API Attacks

13 Sections | Medium | Offensive

Web APIs serve as crucial connectors across diverse entities in the modern digital landscape. However, their extensive functionality also exposes them to a range of potential attacks. This module introduces API Attacks, with a specific focus on the OWASP API Security Top 10 - 2023.

100% Completed