

Targets compromised: 51
Ranking: Top 5%

MODULE

PROGRESS

	<div>Introduction to Academy</div> <div>8 Sections Fundamental General</div> <div>This module is recommended for new users. It allows users to become acquainted with the platform and the learning process.</div>	<div>100% Completed</div> <div></div>
	<div>Linux Fundamentals</div> <div>18 Sections Fundamental General</div> <div>This module covers the fundamentals required to work comfortably with the Linux operating system and shell.</div>	<div>100% Completed</div> <div></div>
	<div>Web Requests</div> <div>8 Sections Fundamental General</div> <div>This module introduces the topic of HTTP web requests and how different web applications utilize them to communicate with their backends.</div>	<div>100% Completed</div> <div></div>
	<div>Introduction to Web Applications</div> <div>17 Sections Fundamental General</div> <div>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.</div>	<div>100% Completed</div> <div></div>
	<div>Attacking Web Applications with Ffuf</div> <div>13 Sections Easy Offensive</div> <div>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.</div>	<div>100% Completed</div> <div></div>
	<div>Using Web Proxies</div> <div>15 Sections Easy Offensive</div> <div>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.</div>	<div>100% Completed</div> <div></div>
	<div>Information Gathering - Web Edition</div> <div>10 Sections Easy Offensive</div> <div>This module covers techniques for identifying and analyzing an organization's web application-based attack surface and tech stack. Information gathering is an essential part of any web application penetration test, and it can be performed either passively or actively.</div>	<div>100% Completed</div> <div></div>
	<div>JavaScript Deobfuscation</div> <div>11 Sections Easy Defensive</div> <div>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.</div>	<div>100% Completed</div> <div></div>



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



SQL Injection Fundamentals

17 Sections **Medium** **Offensive**

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.

47.06% Completed

