Student Transcript

19-11-2022

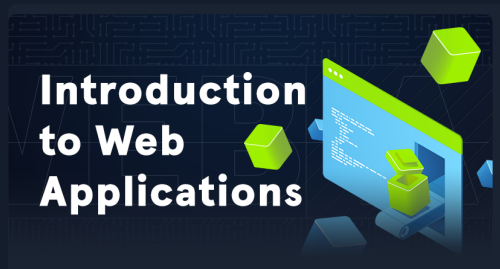
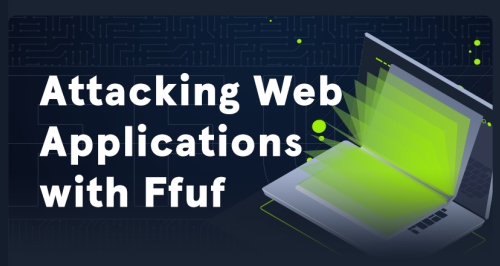
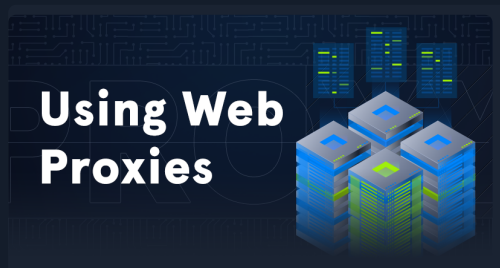
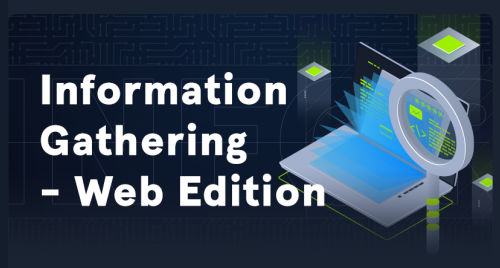
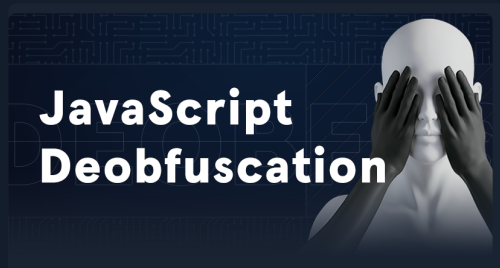
HTB ACADEMY

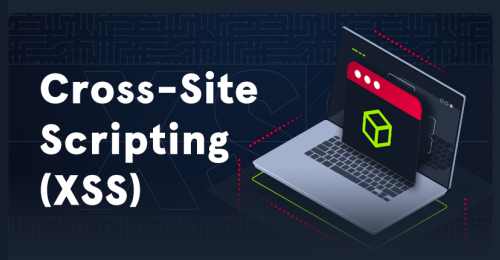
ka3ru

#399320

Targets compromised: 52

Ranking: Top 5%

MODULE		PROGRESS
	Introduction to Academy 8 Sections Fundamental General This module is recommended for new users. It allows users to become acquainted with the platform and the learning process.	100% Completed
	Linux Fundamentals 18 Sections Fundamental General This module covers the fundamentals required to work comfortably with the Linux operating system and shell.	100% Completed
	Web Requests 8 Sections Fundamental General This module introduces the topic of HTTP web requests and how different web applications utilize them to communicate with their backends.	100% 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
	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.	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
	Information Gathering - Web Edition 10 Sections Easy Offensive 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.	100% 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



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.

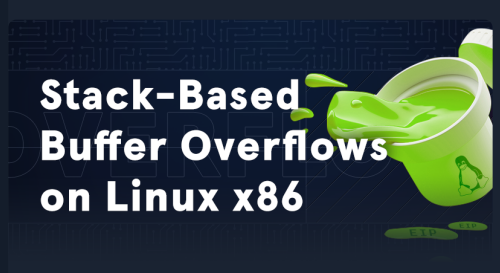
100% Completed

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



Stack-Based Buffer Overflows on Linux x86

13 Sections | Medium | Offensive

Buffer overflows are common vulnerabilities in software applications that can be exploited to achieve remote code execution (RCE) or perform a Denial-of-Service (DoS) attack. These vulnerabilities are caused by insecure coding, resulting in an attacker being able to overrun a program's buffer and overwrite adjacent memory locations, changing the program's execution path and resulting in unintended actions.

38.46% Completed