
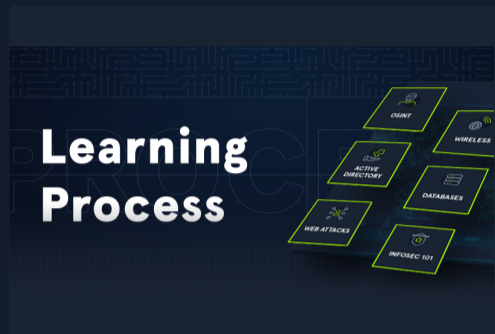




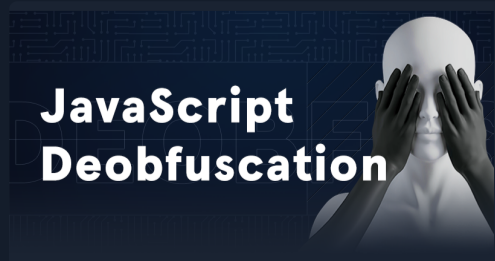


Targets compromised: 62
Ranking: Top 5%

MODULE

PROGRESS

 <h2>Intro to Academy</h2>	<h3>Introduction to Academy</h3> <p>8 Sections Fundamental General</p> <p>This module is recommended for new users. It allows users to become acquainted with the platform and the learning process.</p>	<p>100% Completed</p> <div><div style="width: 100%;"></div></div>
 <h2>Learning Process</h2>	<h3>Learning Process</h3> <p>20 Sections Fundamental General</p> <p>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.</p>	<p>60% Completed</p> <div><div style="width: 60%;"></div></div>
 <h2>Linux Fundamentals</h2>	<h3>Linux Fundamentals</h3> <p>30 Sections Fundamental General</p> <p>This module covers the fundamentals required to work comfortably with the Linux operating system and shell.</p>	<p>60% Completed</p> <div><div style="width: 60%;"></div></div>
 <h2>SQL Injection Fundamentals</h2>	<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>	<p>100% Completed</p> <div><div style="width: 100%;"></div></div>
 <h2>Web Requests</h2>	<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>	<p>100% Completed</p> <div><div style="width: 100%;"></div></div>
 <h2>Introduction to Networking</h2>	<h3>Introduction to Networking</h3> <p>21 Sections Fundamental General</p> <p>As an information security professional, a firm grasp of networking fundamentals and the required components is necessary. Without a strong foundation in networking, it will be tough to progress in any area of information security. Understanding how a network is structured and how the communication between the individual hosts and servers takes place using the various protocols allows us to understand the entire network structure and its network traffic in detail and how different communication standards are handled. This knowledge is essential to create our tools and to interact with the protocols.</p>	<p>100% Completed</p> <div><div style="width: 100%;"></div></div>
 <h2>JavaScript Deobfuscation</h2>	<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>	<p>100% Completed</p> <div><div style="width: 100%;"></div></div>

Windows Fundamentals

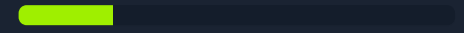


Windows Fundamentals

14 Sections **Fundamental** **General**

This module covers the fundamentals required to work comfortably with the Windows operating system.

21.43% Completed



Attacking Web Applications with Ffuf



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



SQLMap Essentials

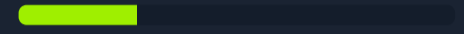


SQLMap Essentials

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.

27.27% Completed



Introduction to Web Applications



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



Cross-Site Scripting (XSS)



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



Using Web Proxies



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



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

