WEB-300: Advanced Web Attacks and Exploitation

Duration: 90 Days

Course Description:

OffSec's Advanced Web Attacks and Exploitation (WEB-300) course dives deep into the latest web application penetration testing methodologies and techniques. Learners gain extensive hands-on experience in a self-paced environment, designed to elevate their skills in ethical hacking, vulnerability discovery, and exploit development.

Successful completion of the online training course and challenging exam earns the OffSec Web Expert (OSWE) certification. This web application security certification validates expertise in advanced web application security testing, including bypassing defenses and crafting custom exploits to address critical vulnerabilities, making certified professionals an asset for securing any organization against web-based threats.

Course Outlines:

JavaScript Prototype Pollution

- Explore how attackers manipulate JavaScript's prototype inheritance model to inject malicious data, compromise application logic, and even achieve remote code execution.

Advanced Server-Side Request Forgery (SSRF)

- Delve into advanced techniques for exploiting SSRF vulnerabilities, including bypassing filters, accessing internal resources, and exploiting complex application architectures.

Web Security Tools and Methodologies

- Master a variety of cutting-edge web security tools and methodologies, including fuzzing, static analysis, dynamic analysis, and manual code review.

Source Code Analysis

Learn how to analyze source code to identify security vulnerabilities, understand the application's logic, and uncover potential attack vectors.

Persistent Cross-Site Scripting

- Discover how attackers store malicious code on a web server to launch persistent XSS attacks, targeting multiple users over time.

Session Hijacking

- Learn how attackers take over user sessions, potentially gaining unauthorized access to sensitive information and functionality.

.NET Deserialization

- Understand the risks associated with deserialization in .NET applications and how attackers can exploit these vulnerabilities to achieve remote code execution.

Remote Code Execution

- Explore various techniques used by attackers to execute arbitrary code on a target web server, often leading to complete compromise of the system.

Blind SQL Injection

- Learn how to exploit SQL injection vulnerabilities even when there is no direct feedback from the application, using various techniques to infer information and compromise the database.

Data Exfiltration

- Understand how attackers extract sensitive data from web applications, including through SQL injection, XXE attacks, and compromised file uploads.