OffSec

WEB-300

OSWE

Advanced Web Attacks and Exploitation

WEB-300 (Advanced Web Attacks and Exploitation) provides experienced offensive team members with a comprehensive analysis of various vulnerabilities and their exploitation techniques in web applications. Building on the PEN-200 and WEB-200 programs, this program will dig deep into the methodologies and techniques used to analyze the target web applications. This will give learners a complete understanding of the underlying flaws that we are going to exploit. The goal of this course is to expose you to a general and repeatable approach to web application vulnerability discovery and exploitation, while continuing to strengthen the foundational knowledge that is necessary when faced with modern-day web applications.

JavaScript Prototype Pollution	Understand how attackers can manipulate JavaScript's inheritance model to inject malicious data, compromise logic, and execute code remotely in your web applications
Advanced Server-Side Request Forgery (SSRF)	Bypass filters, access internal resources, and exploit complex application architectures through SSRF vulnerabilities
Web Security Tools and Methodologies	Master web security tools and methodologies like: fuzzing, static analysis, dynamic analysis, and manual code review
Source Code Analysis	Analyze source code and parse application logic to identify potential attack vectors and security vulnerabilities
Persistent Cross-Site Scripting	See how attackers store malicious code on web servers to launch persistent XSS attacks on multiple users over time
Session Hijacking	Understand how attackers take over user sessions to gain access to sensitive data and functionality
.NET Deserialization	Identify the ways attackers can exploit vulnerabilities caused by deserialization in .NET applications
Remote Code Execution	Explore the techniques attackers use to execute system-compromising code on targeted web servers
Blind SQL Injection	Use different techniques to exploit SQL injection vulnerabilities to compromise databases without direct application feedback
Data Exfiltration	Understand how attackers use SQL injection, XXE attacks, and compromised file uploads to extract sensitive data from web applications
Bypassing File Upload Restrictions and File Extension Filters	Understand how attackers can bypass security mechanisms designed to prevent malicious files from being uploaded

PHP Type Juggling with Loose Comparisons	Learn how to exploit type juggling and loose comparison behaviors in PHP to bypass authentication to perform malicious actions
PostgreSQL Extension and User-Defined Functions	Learn how attackers can access private data, execute commands, and establish persistent backdoors by leveraging PostgreSQL extensions and user-defined functions
Bypassing REGEX Restrictions	Evade regex-based input validations to inject malicious payloads into web applications
Magic Hashes	Bypass authentication mechanisms and perform unauthorized actions by exploiting “magic hashes” in PHP applications
Bypassing Character Restrictions	Explore the techniques attackers use to bypass character restrictions in web applications in order to inject malicious payloads and manipulate application behavior
UDF Reverse Shells	Learn how attackers can leverage user-defined functions to create reverse shells in order to access underlying operating systems
PostgreSQL Large Objects	Learn how attackers store/execute malicious code and exfiltrate sensitive data by abusing large objects in PostgreSQL databases
DOM-Based Cross-Site Scripting (Black Box)	Learn how the browser’s Document Object Model (DOM) can be manipulated to execute malicious JavaScript code in web applications without direct server-side interaction
Server-Side Template Injection	Identify and exploit vulnerabilities in server-side templates in order to execute remote code, disclose information, or escalate privileges
Weak Random Token Generation	Understand the risks associated with poorly implemented random token generation in web applications and how attackers can exploit them or compromise user sessions
XML External Entity Injection	Discover the ways attackers can exploit XML parser weaknesses to access files, execute commands, or perform DDoS attacks, and how to prevent XXE vulnerabilities in your web applications
RCE via Database Functions	Learn how vulnerabilities in database functions can be exploited to execute arbitrary code on the server to compromise your web applications
OS Command Injection via WebSockets (Black Box)	Identify and mitigate WebSocket vulnerabilities that can be used to inject operating system commands to gain control of underlying servers