Advanced Web Application Security: OSWE Certification Prep Course

Offensive Security Web 300 (OSWE) Course Introduction:

The Offensive Security Web 300 (OSWE) course is an advanced web application security program designed for individuals looking to develop sophisticated skills in identifying, exploiting, and defending against complex web application vulnerabilities. This course emphasizes hands-on, practical experience, allowing students to transition from foundational knowledge to expert proficiency in web security. Through a series of modules, learners will gain deep insights into web exploitation techniques, advanced vulnerability analysis, and the methodology necessary to conduct detailed security assessments.

Module 1: Introduction to Advanced Web Exploitation

• Overview of Web Application Security: Explore the current landscape of web application security, including prevalent threats and vulnerabilities.

• OSWE Course Methodology: Understand the learning path and methodologies utilized throughout the OSWE course to develop advanced skills.

• Setting Up the Lab Environment: Guidelines for creating a robust lab setup to practice and test web application security techniques.

Module 2: Comprehensive Web Application Reconnaissance

• Advanced Information Gathering Techniques: Master tools and techniques for collecting detailed information about target web applications.

• Understanding Web Technologies: Delve into the intricacies of web technologies that form the backbone of modern web applications.

• Identifying Attack Surfaces: Learn to recognize potential entry points and vulnerabilities within complex web applications.

Module 3: Advanced Vulnerability Analysis

• In-Depth Code Review: Techniques for manually reviewing web application code to identify potential security flaws and weaknesses.

• Automated Vulnerability Scanning: Utilize and interpret results from automated tools to complement manual vulnerability assessments.

• Logic Flaws and Business Logic Vulnerabilities: Discover how to identify and exploit logic flaws that can compromise web application security.

Module 4: Exploitation Techniques and Strategies

• Exploiting Injection Flaws: Explore advanced techniques for exploiting SQL, NoSQL, and other injection vulnerabilities.

• Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF): Advanced methods for detecting and exploiting XSS and CSRF vulnerabilities.

• Remote Code Execution and File Inclusion: Learn how to exploit vulnerable web applications to execute arbitrary code and include malicious files.

Module 5: Advanced Authentication and Session Management Attacks

• Bypassing Authentication Mechanisms: Techniques for bypassing complex authentication mechanisms to gain unauthorized access.

• Session Management Vulnerabilities: Identify and exploit weaknesses in session management to hijack user sessions and escalate privileges.

• Multi-Factor Authentication and Bypasses: Explore methods for circumventing multi-factor authentication implementations.

Module 6: Exploiting Advanced Web Application Frameworks

• Understanding Framework-Specific Vulnerabilities: Analyze and exploit vulnerabilities specific to popular web application frameworks.

• Case Studies in Framework Exploitation: Practical examples and exercises demonstrating real-world exploitation of framework vulnerabilities.

• Custom Frameworks and Proprietary Code: Strategies for assessing and exploiting vulnerabilities in custom-built applications.

Module 7: Defensive Techniques and Mitigation Strategies

• Implementing Secure Coding Practices: Guidelines for writing secure code to prevent common web vulnerabilities.

• Web Application Firewalls and Security Controls: Understand the role and limitations of web application firewalls in defending against attacks.

• Incident Response and Post-Exploitation: Develop skills for effectively responding to security incidents and mitigating the impact of successful exploits.

Module 8: Capstone Project and Practical Assessment

• Capstone Project Introduction: Outline and objectives of the capstone project designed to assess cumulative skills and knowledge.

• Conducting a Comprehensive Security Assessment: Step-by-step guidance for performing a thorough security evaluation of a web application.

• Preparing for the OSWE Certification Exam: Tips and resources for successfully passing the OSWE certification examination.

By the end of this course, students will have developed the skills necessary to conduct detailed web application security assessments, identify and exploit advanced vulnerabilities, and implement effective defensive measures to protect web applications from sophisticated attacks.