800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

OffSec Advanced Web Attacks and Exploitation WEB-300 (OSWE) Training

OffSec Authorized Training · Applied Technology Academy

We are a Premier Provider of WEB-300 OffSec OSWE Training. In Advanced Web Attacks and Exploitation, you will learn white box web app pentesting methods. The bulk of your time will be spent analyzing source code, decompiling Java, debugging DLLs, manipulating requests and more, using tools like Burp Suite, dnSpy, JD-GUI, Visual Studio, and the trusty text editor.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Intermediate	**5 Days**	**2 years: Programming & Security**	**$112,301**	**Yes**

Course Overview

Advanced Web Attacks and Exploitation (WEB-300) is an advanced web application security review course. We teach the skills needed to conduct white box web app penetration tests.

WEB-300 features three new modules, updated existing content, new machines, plus refreshed videos .

Students who complete the course and pass the exam earn the OffSec Web Expert (OSWE) certification, demonstrating mastery in exploiting front-facing web apps. The OSWE is one of three certifications making up the new OSCE 3 certification, along with the OSEP for advanced pentesting and the OSED for exploit development.

Course Outline

- The course covers the following topics.
- Cross-Origin Resource Sharing (CORS) with CSRF and RCE
- JavaScript Prototype Pollution
- Advanced Server-Side Request Forgery (SSRF)
- Web security tools and methodologies
- Source code analysis
- Persistent cross-site scripting
- Session hijacking
- .NET deserialization
- Remote code execution
- Blind SQL injection
- Data exfiltration
- Bypassing file upload restrictions and file extension filters

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

- PHP type juggling with loose comparisons
- PostgreSQL Extension and User Defined Functions
- Bypassing REGEX restrictions
- Magic hashes
- Bypassing character restrictions
- UDF reverse shells
- PostgreSQL large objects
- DOM-based cross site scripting (black box)
- Server-side template injection
- Weak random token generation
- XML external entity injection
- RCE via database functions
- OS command injection via WebSockets (black box)

Intended Audience

All students are required to have:

- Comfort reading and writing at least one coding language (Java, .NET, JavaScript, Python, etc)
- Familiarity with Linux: file permissions, navigation, and editing and running scripts
- Ability to write simple Python / Perl / PHP / Bash scripts
- Experience with web proxies such as Burp Suite and similar tools
- General understanding of web app attack vectors, theory, and practice
- Experienced penetration testers who want to better understand white box web app pentesting
- Web application security specialists
- Web professionals working with the codebase and security infrastructure of a web application

Prerequisites

- Comfort reading and writing at least one coding language
- Familiarity with Linux
- Ability to write simple Python / Perl / PHP / Bash scripts
- Experience with web proxies
- General understanding of web app attack vectors, theory, and practice

Follow-On Courses

- PEN-300: Advanced Evasion Techniques and Breaching Defenses
- EXP-301: Windows User Mode Exploit Development

- EXP-312: Advanced macOS Control Bypasses
- EXP-401: Advanced Windows Exploitation

Features

- Course Materials
- Active Student Forums
- Access to Home Lab Setup
- Instructors with decades of cumulative real world experience</>

This course is also available in On Demand formats:

- Learn One Package – $2,749
- One course
- 365 days of lab access
- Two exam attempts
- Plus exclusive content
- Learn Unlimited Package – $6,099
- All courses
- 365 days of lab access
- Unlimited exam attempts
- Plus exclusive content

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.