WEB-300 (OSWE)

Advanced Web Attacks and Exploitation

Summary:

Web security experts and pen testers deepen their proficiency in web app security with this course. Within a white-box framework, they analyze decompiled source code, detect logical vulnerabilities, and launch complex attacks. This proactive approach curtails breach risks and helps maintain regulatory compliance. Successful exam-takers earn the OSWE certification.

Great For:

- Exploitation Analysts
- Software Developers
- Secure Software Assessors
- Vulnerability Assessment Analysts
- Cyber Defense Analysts
- Information Systems Security Developers

Learn:

- JavaScript Prototype Pollution
- Advanced XSS
- Advanced SSRF
- Command Injection via WebSockets
- Server-side Template Injection for RCE

Benefits:

- **Risk Mitigation:** Identify and exploit vulnerabilities that many enterprise scanners cannot detect to proactively address potential security threats, thereby reducing the risk of costly breaches.
- **Organizational Efficiency:** The practical experience with private exercise machines and custom web apps translates into more efficient and effective cybersecurity practices within the business.
- **Competitive Advantage:** Ensure the highest level of protection of customer and proprietary data and maintain your competitive advantage while protecting your brand.
- **Investment in Human Capital/Employee Retention:** Invest in your best and brightest with advanced training opportunities. Stronger cybersecurity protections and a happier team is a win/win
- **Regulatory Compliance:** Avoid potential fines and penalties and maintain a positive reputation by exceeding regulatory requirements.

Available On:

Course & Cert Exam Bundle | Learn One | Learn Unlimited | Learn Enterprise

OffSec Partner Program | EXPLOIT LABS www.xplt.com