Training: OffSec

OffSec WEB-300 Advanced Web Attacks and Exploitation

OffSec Learning Partner

TRAINING GOALS:

Advanced Web Attacks and exploitation (WEB-300) is an advanced web application security course that teaches the skills needed to conduct white box web app penetration tests. Learners who complete the course and pass the exam earn the OffSec Web Expert (OSWE) certification and will demonstrate mastery in exploiting front-facing web apps. The OSWE is one of three certifications making up the OSCE³ certification along with the OSEP for advanced pentesting and OSED for exploit development.

Benefits

Learners will learn how to:

- Perform a deep analysis on decompiled web app source code
- Identify logical vulnerabilities that many enterprise scanners are unable to detect
- Combine logical vulnerabilities to create a proof of concept on a web app
- Exploit vulnerabilities by chaining them into complex attacks

Who is this course for?

- 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

Exam

- The WEB-300 web application security course and online lab prepares you for the OSWE certification
- 48-hour exam
- Proctored

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Learn more about the exam https://help.offensive-security.com/hc/en-us/articles/360046869951-OSWE-Exam-Guide

What competencies will you gain?

- Performing advanced web app source code auditing
- Analyzing code, writing scripts, and exploiting web vulnerabilities
- Implementing multi-step, chained attacks using multiple vulnerabilities
- Using creative and lateral thinking to determine innovative ways of exploiting web vulnerabilities

CONSPECT:

- Introduction
  - About the AWAE Course
  - Our Approach
  - Obtaining Support
  - Offensive Security AWAE Labs
  - Reporting
  - Backups
  - About the OSWE Exam
  - Wrapping Up
- Tools & Methodologies
  - Web Traffic Inspection
  - Interacting with Web Listeners using Python
  - Source Code Recovery
  - Source Code Analysis Methodology
  - Debugging
  - Wrapping Up
- ATutor Authentication Bypass and RCE
  - Getting Started
  - Initial Vulnerability Discovery
  - A Brief Review of Blind SQL Injections
  - Digging Deeper
  - Data Exfiltration
  - Subverting the ATutor Authentication

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Authentication Gone Bad
- Bypassing File Upload Restrictions
- Gaining Remote Code Execution
- Wrapping Up

- ATutor LMS Type Juggling Vulnerability
  - Getting Started
  - PHP Loose and Strict Comparisons
  - PHP String Conversion to Numbers
  - Vulnerability Discovery
  - Attacking the Loose Comparison
  - Wrapping Up
- ManageEngine Applications Manager AMUserResourcesSyn cServlet SQL Injection RCE
  - Getting Started
  - Vulnerability Discovery
  - How Houdini Escapes
  - Blind Bats
  - Accessing the File System
  - PostgreSQL Extensions
  - UDF Reverse Shell
  - More Shells!!!
  - Summary
- Bassmaster NodeJS Arbitrary JavaScript Injection Vulnerability
  - Getting Started
  - The Bassmaster Plugin
  - Vulnerability Discovery
  - Triggering the Vulnerability
  - Obtaining a Reverse Shell
  - Wrapping Up
- DotNetNuke Cookie Deserialization RCE
  - Serialization Basics
  - DotNetNuke Vulnerability Analysis
  - Payload Options
  - Putting It All Together
  - Wrapping Up
- ERPNext Authentication Bypass and Server Side Template Injection
  - Getting Started

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Introduction to MVC, Metadata-Driven Architecture, and HTTP Routing
- Authentication Bypass Discovery
- Authentication Bypass Exploitation
- SSTI Vulnerability Discovery
- SSTI Vulnerability Exploitation
- Wrapping Up

- openCRX Authentication Bypass and Remote Code Execution
  - Getting Started
  - Password Reset Vulnerability Discovery
  - XML External Entity Vulnerability Discovery
  - Remote Code Execution
- openITCOCKPIT XSS and OS Command Injection - Blackbox
  - Getting Started
  - Black Box Testing in openITCOCKPIT
  - Application Discovery
  - Intro To DOM-based XSS
  - XSS Hunting
  - Advanced XSS Exploitation
  - RCE Hunting
  - Wrapping Up
- Concord Authentication Bypass to RCE
  - Getting Started
  - Authentication Bypass: Round One - CSRF and CORS
  - Authentication Bypass: Round Two - Insecure Defaults
  - Wrapping Up
- Server Side Request Forgery
  - Getting Started
  - Introduction to Microservices
  - API Discovery via Verb Tampering
  - Introduction to Server-Side Request Forgery
  - Render API Auth Bypass
  - Exploiting Headless Chrome
  - Remote Code Execution
  - Wrapping Up
- Guacamole Lite Prototype Pollution
  - Getting Started

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Introduction to JavaScript Prototype
- Prototype Pollution Exploitation
- EJS
- Handlebars
- Wrapping Up

- Conclusion
  - The Journey So Far
  - Exercises and Extra Miles
  - The Road Goes Ever On
  - Wrapping Up

REQUIREMENTS:

All learners are required to have completed or have the equivalent knowledge corresponding to WEB-200 Foundational Web Application Assessments with Kali Linux. Especially:

- 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

Difficulty level

CERTIFICATE:

After passing the OSWE exam, candidates receive a title of OffSec Web Expert (OSWE).

TRAINER:

Authorized OffSec Trainer

ADDITIONAL INFORMATION:

Course is available as the e-learning product, in two subscription's models:

- Course & Cert Exam Bundle

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Learn One

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007