+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated 04/11/2024

Sign up

OSWE™ Certification Training

ALL-IN-ONE: EXAM INCLUDED IN WEB-300 COURSE FEE

OFFSEC CERTIFICATIONS - BUY YOUR CERTIFICATIONS

4 days (28 hours)

PRESENTATION

Want to be an expert ethical hacker? OSWE™ certification will prove your expertise in evaluating and hacking web applications.

After completing this training course, you'll be able to examine the source code of web applications in depth, and know how to identify and exploit security flaws.

This OSWE™ training will cover all the elements present during the exam such as SQL injections, JavaScript injections, authentication bypassing or deserialization.

After completing our preparation, you'll be able to take the OSWE™ certification included in the fee.

THE PREMIUM PACK

- 90 days' access to self-training Labs
- 8 expert coaching sessions: 8 x Monday mornings (9am-12.30pm) per week (28 hours)
- 1 Passage to certification

OBJECTIVES

- In-depth analysis of web application source code
- Identify vulnerabilities that many enterprise scanners are unable to detect

- Methodically implement chain attacks using different vulnerabilities
- Develop problem-solving and divergent thinking skills

TARGET AUDIENCE

- Ethical hackers
- IT security expert
- Developers
- Technical architects
- Directors
- Project managers

Prerequisites

- A solid understanding of TCP-IP networks
- Experience in Windows and Linux administration
- A good knowledge of Linux
- Ability to write simple scripts in Python / PHP / Perl / Bash
- Good knowledge of at least one coding language (Java, .NET, Python, etc.)
- Knowledge of web proxies
- General knowledge of pentesting, obtaining OSCP™ certification is recommended, but not mandatory

Note: Ambient IT does not own OSWE™, this certification belongs to OffSec ® Services LLC.

OSWE™ CERTIFICATION TRAINING PROGRAM

MASTERY OF TOOLS AND SOURCE CODE ANALYSIS

- Setting up the lab
- Master the Burp Suite (Burp Proxy, Scope, Decoder...)
- Source code recovery
- Source code analysis

FROM XSS TO NCE

- AtMail Email Server Appliance
- Use XSS and CSRF to obtain the RCE
- Hijacking session
- Session Riding
- The various vulnerabilities (atmail, addattachmentAction, globalsaveAction)

BYPASS FILE UPLOAD RESTRICTIONS

- Shell the web
- Unlimited file uploads
- Atlassian Crowd Pre-auth RCE

AUTHENTICATION BYPASS AND RCE

- Vulnerability overview
- Introducing Atutor
- Authentication bypass with Atutor
- Introducing ERPNext
- Authentication bypass with ERPNext
- Introducing openCRX
- Authentication bypass with openCRX

PASSWORD RESET VULNERABILITY

- Test password reset functions
- RCE with SQL injection
- SQL injection at LFI au RCE
- Takeover of OXID online stores prior to announcement of decision
- Using PostgreSQL
- Exploiting H2 SQL injection in RCE

PHP TYPE JUGGLING

- OWASP - PHPMagicTricks TypeJuggling
- The various vulnerabilities
- Type Juggling, PHP Object Injection, SQLi
- Exploits for PHP Type Juggling
- PHP Magic Hashes

JAVASCRIPT INJECTION

- Introducing Bassmaster
- The various vulnerabilities
- Using a Reverse Shell
- Server Side JS Injection
- Remote Code Execution in math.js
- Arbitrary code execution in fast-redact
- SetTimeout and SetInterval use eval therefore are evil
- Pentesting Node.js

DESERIALIZATION

- Deserialization with Java

- Deserialization with .NET
- Deserialization with PHP
- Deserialization with Nodejs

XML (XXE) EXTERNAL ENTITY ATTACK

- Introducing XXE injection
- From XXE to RCE
- Apache Flex BlazeDS XXE vulnerability
- WebLogic EJBTaglibDescriptor XXE

WEBSOCKETS INSECURITY

- Introduction to WebSockets
- Remote control of equipment through hijacking
- Website hijacking
- Source code audit
- Writing static code analyses
- TrendMicro
- Shopify Remote Code Execution
- Find vulnerabilities in source code (APS.NET)
- A deep dive into ASP.NET deserialization

FAQ - QUESTIONS / ANSWERS

WHAT CONTENT WILL I RECEIVE FOR OSWE™ TRAINING?

In addition to the preparation we offer. OSWE™ training includes all training materials issued by OffSec:

- 10 hours of video training
- A 410-page training book in pdf format
- Access to the learners' forum
- 90-day access to the lab

HOW MUCH DOES OSWE™ CERTIFICATION COST?

Certification costs €1,649.

IN WHAT LANGUAGE ARE YOU TAUGHT OSWE™ TRAINING?

Coaching will be in French. However, the additional content offered by OffSec is in English.

IS THE OSWE™ CERTIFICATION EXAM INCLUDED IN THE PRICE OF THE

TRAINING ?

Yes, you can take the exam after completing the training course. HOW

LONG IS THE LAB AVAILABLE FOR?

You have access to the lab for 90 days

HOW DOES THE OSWE™ CERTIFICATION EXAM WORK?

You must read the official guide before taking your exam.

The practical phase of the exam lasts 47 hours and 45 minutes, and consists of hacking as many machines as possible. After this phase, you will again have 24 hours to complete and submit the pentesting report, explaining your approach.

WHAT LANGUAGE IS USED FOR THE EXAM?

The exam is conducted in English.

DO I NEED A GOOD INTERNET CONNECTION?

Yes, because your computer has to support a TeamViewer stream for 24 hours, while constantly attacking other machines.

DO I NEED A WEBCAM?

Yes, your webcam must be active throughout your entire exam, and be able to film your entire room.

What's the difference between Offensive Security and OffSec?

Since March 2023, Offensive Security has been renamed OffSec. It is the same organization.

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.