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

Updated on 08/19/2026

Sign Up

INE Security eWPTX© Certification Training

3 days (21 hours)

Overview

Our eWPTX© certification preparation course will enable you to demonstrate your mastery of penetration testing on web applications.

The eWPTX© exam is based solely on advanced practical skills. This allows you to demonstrate your web application hacking skills in real-world scenarios. It is a demanding exam in which only candidates who produce a high-quality audit report pass.

You will need to attack multiple machines in a virtual lab. You will also need to write a penetration testing report that includes professional documentation and security recommendations. The total duration of the exam is 14 days. This includes 7 days of access to the exam labs and 7 days for feedback on your report.

Our eWPTX© certification preparation course will cover everything you need to pass the exam, including advanced web application attacks, advanced SQL injections, and cross-site scripting.

Like all our training courses, this one will cover **the latest stable version** of the technology and its new features.

Objectives

- Strengthen your pentesting skills targeting web applications
- Be prepared to take the eWPTX© certification exam

Target Audience

- Security managers
- Auditors
- Ethical hackers
- Network administrators

Prerequisites

Solid experience in IT security; preferably already hold a certification in the field.

Note: Ambient IT does not own eWPTX©; this certification belongs to INE Security©.

OUR EWPTX TRAINING PROGRAM

INTRODUCTION TO WEB PENETRATION TESTING

- Understanding the basics of web application security and the HTTP protocol
- Overview of common vulnerabilities in web applications
- Introduction to penetration testing tools and techniques
- The importance of ethics in penetration testing
- Setting Up a Secure Testing Environment

ADVANCED ATTACKS ON WEB APPLICATIONS

- Techniques for Exploiting XXE and SSRF Vulnerabilities
- Remote File Inclusion (RFI) Methods and Their Impacts
- Practical Attack and Defense Scenarios
- Log Analysis to Detect Intrusion Attempts
- Using Proxies and Interception Tools to Manipulate Web Requests

ADVANCED SQL INJECTION

- Understanding the different types of SQL injection, including blind and out-of-band injection
- Techniques for identifying SQL injection points in an application
- Exploiting SQL vulnerabilities using automated and manual tools
- Case studies on the impacts of SQL injections
- Mitigation and database security best practices

CROSS-SITE SCRIPTING (XSS) AND FILTER EVASION

- Details on the different types of XSS: Reflected, Stored, and DOM-based
- Advanced techniques for evading XSS filters and bypassing WAFs
- Creating and testing XSS scripts for various scenarios

- Defense against XSS attacks: HTTP headers, content security policies
- Hands-on workshops on XSS exploitation and mitigation

ATTACKS ON BUSINESS LOGIC AND ACCESS CONTROL

- Identifying and exploiting business logic vulnerabilities
- Techniques for testing and securing authentication and access control mechanisms
- Exploiting race conditions and transaction-related vulnerabilities
- Best practices for securing authentication and session management processes
- Simulation of account enumeration and access control bypass attacks

CTF (CAPTURE THE FLAG) CHALLENGES AND REVIEW

- Introduction to Capture The Flag-style competitions to reinforce learning
- Setting up and solving practical challenges covering the vulnerabilities studied
- Techniques for writing clear and detailed penetration testing reports
- Q&A session to address questions and reinforce understanding

Target Audience

This training is intended for both individuals and companies—large or small—seeking to train their teams in new, advanced IT technologies or to acquire specific industry knowledge or modern methodologies.

Pre-training Assessment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency level across various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth operation of the training session.

Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical instruction from the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been properly acquired

of the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.

Training organization registered under number 11 75 54743 75. This registration does not constitute state accreditation.
© Ambient IT 2015-2026. All rights reserved. Paris, France - Switzerland - Belgium - Luxembourg