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

Updated 06/27/2024

Sign up

# eLearnSecurity eWPTX© certification training

ALL-IN-ONE: EXAMINATION INCLUDED IN PRICE

3 days (21 hours)

## Presentation

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

The eWPTX© exam is based solely on advanced practical skills. So you can prove your web app hacking skills in real-life situations. It's a demanding exam, and only those candidates who write a very good audit report will pass.

You'll need to attack several machines in a virtual lab. You will also have to write a pentesting audit including professional documentation and security recommendations. The total duration of the exam is 14 days. It includes 7 days' access to the exam labs and 7 days' reaction time for your report.

Our eWPTX© certification preparation course will provide you with all the information you need to pass the exam. Advanced attacks on web applications, advanced SQL injections and cross-site scripting.

## Objectives

- Strengthen pentesting skills for web applications
- Be ready for eWPTX© certification

## Target audience

- Safety managers
- Auditors

- Ethical hackers
- Network administrator

## Prerequisites

Good experience in IT security or already have certification in the field.

Note: Ambient IT is not the owner of eWPTX©, this certification belongs to eLearnSecurity©.

# EWPTX TRAINING PROGRAM

### INTRODUCTION TO WEB PENETRATION TESTING

- Understand 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 test environment

### ADVANCED ATTACKS ON WEB APPLICATIONS

- Techniques for exploiting XXE and SSRF vulnerabilities
- Remote file inclusion (RFI) methods and their impact
- Practical attack and defense scenarios
- Log analysis to detect intrusion attempts
- Using proxies and interception tools to manipulate web requests

### ADVANCED SQL INJECTION

- Understand the different types of SQL injection, including blind and out-of-band injection
- Techniques for identifying SQL injection points in an application
- Exploit SQL vulnerabilities with automated and manual tools
- Case studies on the impact of SQL injections
- Database mitigation and security practices

### CROSS-SITE SCRIPTING (XSS) AND FILTER EVASION

- Details of 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 different situations
- Defense against XSS attacks: HTTP headers, content security policies
- Practical 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
- Exploitation of race conditions and transaction vulnerabilities
- Secure authentication and session management processes
- Simulation of account enumeration and access control bypass attacks

### CTF (CAPTURE THE FLAG) CHALLENGES AND REVISION

- Introduction to Capture The Flag competitions to consolidate skills
- Setting up and solving practical challenges covering the vulnerabilities studied
- Techniques for writing clear, detailed penetration testing reports
- Question-and-answer session to clarify doubts and reinforce understanding

## Companies concerned

This 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.