AMBIENT-IT

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

Updated on 11/10/2024

Sign up

OWASP Training: Web Security

2 days (14 hours)

Presentation

Thanks to our OWASP training, you'll be able to effectively secure your web applications, including specific protection against the 10 most dangerous threats.

Our comprehensive program includes several essential modules including web security fundamentals, application requirements, HTTP operation and security technologies. We'll introduce you to pentesting techniques so you can conduct end-to-end penetration tests.

You'll learn all about common vulnerabilities such as SQL injection, Cross-Site Scripting, Cross-Site Request Forgery and file inclusion. At the end of this course, you'll be able to protect your APIs and carry out security tests.

Our OWASP training for web security will focus on the latest version of the project, OWASP 2021.

Objectives

- Understanding the security needs of web applications
- Acquire a working knowledge of the steps involved in a web penetration test
- Identify and understand common web vulnerabilities
- Understanding the importance of API security

Target audience

- Developers
- Architects
- Safety auditors

Prerequisites

- Web programming experience
- Test My Knowledge

Technical requirements

- Pre-installing Burp Suite Community
- Pre-installing the ZAP proxy
- IDE and Runtime

OWASP Web Security training program

APPROACH AND TOOLS

- Web security fundamentals
  - Application security requirements
  - Overview of how HTTP works
  - Security technologies
- Introduction to Web penetration testing
  - Definition and importance of penetration testing
  - Intrusion test stages (Recognition, Analysis, Exploitation, Post-exploitation)
- Web penetration testing tools
  - Overview of common tools
    - Burp Suite
    - OWASP ZAP
    - OWASP Amass
- Practical demonstration of Burp Suite and OWASP ZAP
- Analysis of tool results

COMMON WEB VULNERABILITIES

- SQL injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- File inclusion (LFI/RFI)
- Broken access control
- Session vulnerabilities
- Practical demonstrations and exercises

BEEKEEPING SAFETY

- Introduction to API Security
  - The importance of API security
  - API types (REST, SOAP, GraphQL) and their specific vulnerabilities
  - OWASP API Security Top 10

- API security testing
  - Testing methodologies for APIs
  - API testing tools (Postman, Insomnia, OWASP ZAP, etc.)
  - Practical examples and demonstrations

EVERYDAY SAFETY AND BEST PRACTICES

- Integrating safety into daily development
  - Secure Coding concepts
  - Secure code review
  - Management of dependencies and regular updates
  - Safety awareness: why and how?
- OWASP Awareness and Resources
  - Presentation of OWASP resources (Top 10, Cheat Sheets, etc.)
  - Using OWASP resources in day-to-day development
  - Importance of continuing education

ADDITIONAL MODULE (+1 day, in-house only)

- PHPStan with CI/CD integration
- Brakeman code analysis tools for Ruby on Rails

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.