almond
INSTITUTE

Training sheet
Secure code developments techniques

CONTACT FOR THIS TRAINING

Miora RAHARINIRINA
Almond Institute coordinator
almond.institute@almond.eu
07 64 42 71 56

→ Version 1.0

→ 29/01/2024

Secure code developments techniques

Course overview

This training program is designed to make development teams aware of the security risks associated with web application development. This module presents the attacks commonly used by hackers. The techniques presented are described in detail and put into practice. The module details the best practices to adopt to protect against the attacks presented.

01. Know the **main vulnerabilities** associated with web applications (OWASP Top 10)

02. Know how to detect the **presence of these vulnerabilities**

03. Acquire **good development practices**

Secure code developments techniques

Useful informations

Who should attend?

- Web application developers, whatever the technology used

Entry requirements

Basic knowledge of web environments:

- 1 web language: PHP, JAVA, ASP .NET, Python, etc.
- 1 database language: SQL and/or NoSQL
- 1 operating system: Linux and/or Windows

Method of assessment

- Completion of a final online questionnaire covering all the concepts learned.
- In the case of face-to-face training: practical exercises

How and when to access

The participant is considered registered when:

- The prerequisites and needs are identified and validated
- The training agreement is signed

Registration requests can be sent up to 10 working days before the start of the training.

Accessibility

Whether you are recognized as having a disability or not, making our training accessible to everyone is part of our commitment. If you need compensation or adaptation for the content, the supports, the "venue", the material used, the schedules, the rhythm, **we are at your disposal**.

Secure code developments techniques

Face-to-face and distance learning

Course curriculum

Introduction	Advanced web testing
→ Cybersecurity context (CNIL, threats, attackers, data leaks, the black market in vulnerabilities, etc.). → OWASP → MITRE ATT&CK matrix	→ **The 1st phase covers the essentials of important topics and the OWASP top 10 over 1.5 days:** • Authentification/Password storage/ HTTP (Using Burp Suite) / HTTP field manipulation / Session management / Path Traversal, LFI / Application denial of service / Caching / RCE / XSS / SQL Injections / CSRF / Open Redirect / XXE / SSRF → **The 2nd phase, lasting 0.5 days, covers a number of topics chosen in consultation with the training audience, according to the technologies used and their skills and aptitudes. Possible topics are:** • Insecure deserialization (PHP and/or JAVA) / Type Juggling (PHP) / Log forging / Security headers / Dependency Confusion / OAuth/OpenID / Angular et XSS / SAMLv2 / TLS configuration / NoSQL Injection / API security

Training benefits

- Training delivered by an expert in web application security who has carried out numerous web intrusion tests.
- Face-to-face training includes practical exercises carried out by participants themselves on a test environment

Prices and informations

- **Duration:** 2 days (14 hours)
- **Price:** Contact us
- **Financing:** OPCO support

→ READ MORE