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

Updated 06/06/2025

Sign up

Application Security Training

3 days (21 hours)

PRESENTATION

Our application security training course will enable you to develop modern, secure web and mobile applications. At the end of this course, you'll have mastered the best practices needed to effectively protect your code against cyber risks, and be able to keep a continuous and relevant watch on cybersecurity.

Through a comprehensive overview integrating international standards (OWASP, NIST, ANSSI), you will explore the main threats affecting web and mobile applications, such as SQL injections, insufficient access controls or AI-specific vulnerabilities, notably through the various OWASP TOP 10 (Web, Mobile, API).

You'll learn how to integrate security right from the design phase (Secure by Design), adopt secure development best practices and make effective use of modern analysis tools (SAST, DAST, SCA). Practical workshops will enable you to apply these concepts immediately to a realistic application, reinforcing your ability to detect and correct vulnerabilities quickly.

Finally, our training will introduce you to the essential principles of DevSecOps and Cloud security, for continuous and effective protection of your applications, in a proactive and collaborative approach.

As with all our programs, this course places practical exercises at the heart of your learning, enabling you to acquire operational skills that can be put to use immediately.

OBJECTIVES

- Understand application security issues
- Identify the main threats and vulnerabilities affecting web and mobile applications
- Apply best security practices in application development
- Use tools and techniques to detect and correct security vulnerabilities

- Discover the basic principles of cybersecurity and their impact on application security.

TARGET AUDIENCE

- Architects
- Developers
- Analysts
- Project managers

Prerequisites

- Good knowledge of object programming and Web application programming

Our Application Security Training Program

Introduction to application security

- Why is cybersecurity strategic?
- Stakes and consequences of application vulnerabilities
- Average cost of a breach
- Actors and motivations: cyber-crime, hacktivism, espionage, supply-chain
- Legal obligations (RGPD, NIS2)
- Attack surfaces and misuse cases
- Security triangle of the CIA model: Confidentiality, Integrity, Availability
- Role of standards and government agencies (OWASP, ANSSI, NIST, CISA, CERT)
- NIST Cybersecurity Framework 2.0: Governance and Supply Chain
- Principle of the Secure Development Lifecycle (SDLC)
- Common threats and examples of real-life attacks
- Importance of security awareness and culture
- Practical workshop: Collective analysis of a vulnerable application to identify potential risks.

Overview of vulnerability databases

- USA
  - CVE (Common Vulnerabilities and Exposures) by the MITRE Corporation
  - NVD (National Vulnerability Database) CVSS scores, CWE classifications and affected products
  - OffSec's ExploitDB (Exploit Database) containing proofs of concept
  - OSV (Open Source Vulnerabilities) from Google on vulnerabilities affecting open source software
- Europe
  - EUVD (European Vulnerability Database), a new project launched in May 2025 by ENISA
- Others: VulnDB, Vulners, Zero-Day.cz
- Vulnerability prediction and exploitation: EPSS, KEV, LEV

Web vulnerabilities: OWASP Top 10 (2025)

- Presentation OWASP Top 10 web vulnerabilities
- A01 Broken Access Control, A02 Cryptographic Failures, A03 Injection, etc.
- Injection (SQL, LDAP, XML)
- Live examples: SQLi with DVWA, XSS in a microservice
- Faulty access control
- Security misconfigurations
- Cryptographic failures
- Authentication and session management errors
- Practical workshop: Correcting an unfiltered form (Input Validation Cheat Sheet).

Mobile vulnerabilities: OWASP Mobile Top 10 (2025)

- iOS/Android specific: local storage, permissions, reverse engineering
- M1 Improper Credential Usage to M10 Insufficient Cryptography
- Poor credential management
- Insufficient authentication and authorization
- Insecure storage of sensitive data
- Insufficient client-side protection (reverse engineering)
- Insecure communication with backend
- Practical workshop: Examine a vulnerable mobile application to detect the main vulnerabilities. Analyze an APK with MobSF and check MASVS requirements.

Security analysis tests and tools

- SAST: Static analysis techniques, demonstration with SonarQube
- DAST: Dynamic analysis techniques, black-box testing, attack simulation with OWASP ZAP
- SCA: Dependency analysis, OWASP Dependency-Check and CVE flows
- Presentation of tools: OWASP ZAP, Burp Suite
- Simple application pentesting methodology
- Managing and prioritizing discovered vulnerabilities
- Importance of logging and application monitoring
- Practical workshop: Quick scan of the red wire application and interpretation of results.

Security by design

- Principles of secure architecture (Defense-in-depth, principle of least privilege)
- Threat modeling techniques (STRIDE)
- Proactive risk management (identification and prioritization)
- Best practices for partitioning and isolating components
- Securing APIs and microservices
- Use of NIST and ANSSI guidelines on secure design
- Practical workshop: Threat modeling on the "fil rouge" application.

Best practices in secure development

- Principles of defensive coding: input validation, error handling, logging
- Encryption: choice of algorithms, secret management
- Appropriate use of cryptography (encryption, hashing)
- Robust authentication & session management (OAuth 2.1, MFA)
- Secure management of user authentication and sessions
- Secure error and exception handling
- Updating of third-party libraries and components
- Client-side protection (CSP, secure cookie management)
- Practical workshop: Correcting vulnerable code extracts from the fil rouge application.

Modern API security

- OWASP API Security Top 10 presentation
- Access control on API endpoints
- Securing API communications (JWT, OAuth2)
- Strict validation of incoming data
- Secure management of API keys and secrets
- Protection against DoS/API abuse attacks
- Practical workshop: Identifying and correcting a vulnerability in a REST API of the fil rouge application.

Conclusion and opening session: DevSecOps and Cloud Security

- Presentation of DevSecOps principles
- Continuous security integration (SAST/DAST in CI/CD)
- Securing the software supply chain (SBOM, dependency management)
- Infrastructure configuration best practices (secure IaC)
- Continuous monitoring and incident response
- Security culture in development teams
- Image & container hardening: principle of least privilege, signatures
- Securing the CI/CD pipeline: SAST / SCA / IaC scan gates, shift-left
- Zero Trust and identity control in native cloud infrastructures

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced IT 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 forthcoming course, 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 training: 60% hands-on, 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.

Certification

A certificate will be awarded to each trainee who has completed the entire course.