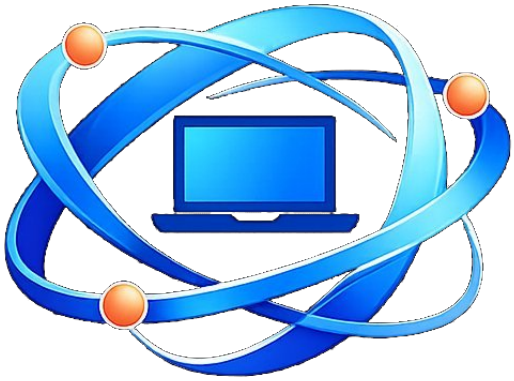

MFE-IT

Reference: PH/EN/SECA

Application Security Training Course

Integrate Protection from Code to Deployment

Duration: 3 Days | Hours: 21 h

Remote · Sessions guaranteed from 1 registrant · 60% hands-on practice

DESCRIPTION

Attacks targeting web and mobile applications are on the rise. XSS, injection, broken access control, unsecured APIs and vulnerable dependencies all expose organisations to data breaches and reputational damage. It is now crucial to integrate security throughout the entire application lifecycle, from design to deployment.

This Application Security training course will enable you to identify common vulnerabilities (OWASP Top 10), avoid them from the design stage onwards, secure your code, APIs and data, and deploy robust, compliant applications. The training combines technical practice with strategic vision, so participants leave with both hands-on remediation skills and a clear DevSecOps roadmap.

LEARNING OBJECTIVES

By the end of this training course, participants will be able to:

- Understand the most common types of attacks on applications
- Integrate security best practices into code (input validation, session management, cryptography)
- Test and fix vulnerabilities with appropriate tools (SAST, DAST, ZAP, Burp)
- Secure communications (HTTPS, TLS, CORS, CSP)
- Apply security to APIs (authentication, authorisation, tokens, rate limiting)
- Integrate security into a DevSecOps CI/CD pipeline
- Understand legal and regulatory aspects (developer responsibility)

PREREQUISITES

- Basic knowledge of web or mobile development (HTML, JS, PHP, Python, Java)
- Comfortable with an IDE and a local or cloud deployment environment
- No cybersecurity knowledge required (beginner to intermediate level)

> *Because each participant is unique, a personalised interview is systematically organised in advance with our expert to design a training programme perfectly aligned with their objectives, level and professional challenges.*

TARGET AUDIENCE

Front-end and back-end developers, DevOps engineers, testers, tech leads and anyone wishing to professionalise their application security practice.

DETAILED PROGRAMME

> The training alternates between theoretical input and hands-on practice (approximately 60% of the time). Modules are built around practical exercises based on real-world business use cases.

Module 1 – Application Threats: Understand to Prevent

- Overview of vulnerabilities (OWASP Top 10)
- Attack vectors and real-world impacts
- Balancing security and user experience

Module 2 – Best Practices for Secure Development

- Input validation and output encoding
- Session management, access control and authentication
- Logging and front-end / back-end security patterns

Module 3 – Securing APIs and Microservices

- Authentication: OAuth 2.0, JWT, OpenID Connect
- Authorisation, API Gateway and rate limiting
- IP filtering, access auditing and zero-trust patterns

Module 4 – Vulnerability Detection Tools and Tests

- SAST vs DAST: which tool for which stage
- OWASP ZAP and Burp Suite in practice
- Automated penetration testing and integration into dev workflows

Module 5 – Security in CI/CD and DevSecOps

- Integrating scanners into GitHub Actions and GitLab CI/CD
- Security rules in builds, alerts and automated fixes
- Secrets management and dependency scanning

Module 6 – Compliance and Responsibilities

- Log management and security data retention
- Developer and publisher responsibility
- Security documentation and audit readiness

TEACHING METHODS

Format and Delivery

The training is delivered remotely via an interactive virtual classroom. It can also be delivered on-site, with content customised to match the needs of your professional project. The theory/practice split is approximately 40%/60%.

MFE-IT Ultra-Personalised Format

Each session accommodates between 1 and 3 participants, ensuring highly individualised support. A preliminary interview allows us to tailor the content to each participant's profile. Inter-company sessions are guaranteed from just 1 registrant (except in cases of force majeure).

Skills Assessment

Throughout the training, the trainer assesses participant progress through multiple-choice questions, role-playing exercises and hands-on work. At the end, a certificate of achievement is issued to each participant.

Post-Training Support

For one month following the training, each participant can contact MFE-IT trainers with questions about implementing acquired knowledge. A response is provided by email or telephone within 48 working hours.

Accessibility

MFE-IT is committed to welcoming people with disabilities. Contact: contact@mfe-it.com.

PRACTICAL INFORMATION

Trainer Resources

- Structured demonstrations aligned with the detailed programme
- Exercise briefs and solutions throughout the training
- A ready-to-use technical environment for practical workshops
- Trainer validation of acquired knowledge at the end of each workshop
- Digital reference documents

Certification and Validation

At the end of the training, a certificate is sent by email specifying the objectives, nature, duration and assessment results. A completion certificate can also be provided on request.

Benefits for Participants

- Train from your workplace or home, with no travel required
- Benefit from an expert trainer-consultant on the subject
- Enjoy an ultra-personalised format (1 to 3 participants)
- Continue training even in the event of unforeseen circumstances

Benefits for the Organisation

- Optimise the training budget by reducing travel and accommodation costs
- Offer quality training to all employees, regardless of location
- Reduce absence time linked to travel
- Support team upskilling in all contexts