MFE-IT

Reference: MB/SW/EN

Securing Your Website Training Course

From Known Vulnerabilities to Active Protection

Duration: 3 Days | Hours: 18 h

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

DESCRIPTION

No matter how well a website is designed, it remains vulnerable to numerous threats if security is not built in from the outset. Web attacks target data, reputation and system stability, and the cost of a successful breach far exceeds the cost of preventive hardening.

This training course enables you to understand, detect and correct common security vulnerabilities, while implementing best practices for secure development. You will learn how to secure exchanges, data and sessions, prevent injections and cross-site scripting, and prepare for automated attacks.

LEARNING OBJECTIVES

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

- Understand the most common types of attacks on websites
- Identify the vulnerabilities listed by OWASP Top 10
- Implement secure development practices on the front-end and back-end
- Secure forms, cookies, tokens and user sessions
- Protect exchanged data (HTTPS, encryption, CORS, CSP)
- Respond quickly in the event of an intrusion or suspected exploitation

PREREQUISITES

- Proficiency in website creation or management (HTML, PHP, JS, WordPress)
- Basic knowledge of HTTP, databases and web architecture
- No prerequisites in cybersecurity required

> *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

Web developers, DevOps, security managers and anyone responsible for maintaining or deploying a website or web application.

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 – Introduction to Web Security

- Threat concepts, actors and attackers' objectives
- OWASP Top 10 overview
- Attack surface of a typical website

Module 2 – Common Application Vulnerabilities

- XSS, CSRF and SQL injection
- Header manipulation and clickjacking
- File upload vulnerabilities and remote code execution

Module 3 – Data and Session Security

- HTTPS, TLS configuration and certificate management
- Secure cookies, JWT and token handling
- CORS policies and session lifecycle

Module 4 – Client-Side and Front-End Security

- Preventing malicious code execution
- HTML and JavaScript hardening
- Content Security Policy (CSP) and modern front-end best practices

Module 5 – Monitoring, Auditing and Incident Response

- Vulnerability analysis tools (OWASP ZAP, Burp Suite)
- Injection detection, alerts and log analysis
- Rapid response and incident handling

Module 6 – Best Practices for Secure Deployment

- Server configuration: Apache, Nginx
- Security headers and Web Application Firewall (WAF)
- WordPress and CMS hardening

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