Course : Campus Atlas - Application security

Practical course - 3d - 21h00 - Ref. LAN
Price : 1940 CHF E.T.

NEW

À l'issue de la formation, le participant sera capable de développer des applications web et mobiles sécurisées. Tous les points fondamentaux de la sécurité des applications seront abordés, des modèles de maturité aux bonnes pratiques en Java incluant un tour d'horizon des vulnérabilités courantes et spécifiques pour mieux les gérer. Ce programme de formation est destiné aux salariés des branches professionnelles relevant de l'OPCO Atlas.

Teaching objectives

At the end of the training, the participant will be able to:

- Understanding 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

Intended audience

OPCO Atlas members: architects, developers, analysts, project managers...

Prerequisites

Posséder une bonne connaissance de la programmation objet et de la programmation
d'applications web.

PARTICIPANTS

OPCO Atlas members: architects, developers, analysts, project managers...

PREREQUISITES

Posséder une bonne connaissance de la programmation objet et de la programmation
d'applications web.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

Practical details

Hands-on work

Practical exercises and/or case studies.

Teaching methods

60% pratique – 40% théorie. Pour optimiser le parcours d'apprentissage, des modules e-learning peuvent être fournis avant et après la session présentielle ou la classe virtuelle, sur simple demande du participant.

Course schedule

1 OWASP Top 10 - Web application vulnerabilities part 1 - Pre-training digital learning content

- Introduction.
- Lack of access control.
- Incorrect security configuration.
- Cross-site scripting (XSS).
- Insecure deserialization.
- Use of components with known vulnerabilities.
- Lack of logs and monitoring.

Digital activities

In this online training course, you'll learn about the latest 6 vulnerabilities in the OWASP top 10, the security principles you need to know to prevent them, the techniques used by hackers to exploit them, and the best practices and countermeasures you can put in place to protect your web applications.

2 IT security, essential concepts and protection techniques for the user - Digital learning pre-training content

- Safety concepts.
- Malware.
- Network security.
- Secure web use.
- Secure messaging.
- Data security management.

Digital activities

In this online training course, you'll discover the main risks associated with computer security, their causes and consequences, and the best practices for preventing them. After an introduction to fundamental concepts, you'll explore the threats associated with malware, networks, Internet browsing, messaging and the protection of stored data, so you can use your computer with complete confidence.

3 Introduction to application security

- Key definitions: vulnerability, threat, risk, attack.
- Security players: CERT, OWASP, BSIMM.
- Application development risks.
- Traces left by developers: memory, logs...

Demonstration

Analysis of a vulnerable application to identify traces left by developers.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

4 Safety maturity models

- Presentation of the OpenSAMM model.
- The 4 levels of maturity.
- Introduction to BSIMM (Building Security In Maturity Model).

Hands-on work
Calculating an organization's maturity level using OpenSAMM.

5 Common web application vulnerabilities

- Application Security Verification Standard (ASVS).
- An ecosystem of open source tools.
- OWASP Top 10: Broken Access Control, Cryptographic Failures, Injection (e.g. SQL Injection)...

Hands-on work
Simple exploitation of a SQL Injection or XSS vulnerability on a Java mini-application. How could it have been avoided?

6 Vulnerabilities specific to mobile applications

- Unsecured storage.
- Weak authentication.
- API exhibition.

Hands-on work
Analysis of a mobile application to identify specific vulnerabilities.

7 Safety by design

- Security by Design principles.
- Integrating security into the development cycle (DevSecOps).

Demonstration
Case study in secure application design.

8 Best practices in Java

- User input validation.
- Error and exception handling.
- Secure REST APIs with Spring Security or Jakarta Security.

Hands-on work
Use Spring Security or Jakarta Security to secure a REST API.

9 Configuration and dependency security

- Management of sensitive configurations.
- Updating dependencies and managing known vulnerabilities.

Demonstration
Use Dependency-Check to identify vulnerabilities in the dependencies of a Java project.

10 Securing mobile applications

- Best practices for secure mobile development.
- Tools and techniques specific to mobile platforms.

Hands-on work
Applying best security practices to an existing mobile application.

11 Introduction to security testing

- Security testing objectives: proactive detection.
- Static code review (SAST).
- Dynamic testing (DAST).
- Interactive tests (IAST).

Demonstration
Tool-based analysis of an application to identify vulnerabilities.

12 Vulnerability management

- Vulnerability management process.
- Implementation of corrective measures and follow-up.

Hands-on work
Drawing up a vulnerability management plan for an existing application.

13 Final workshop - Putting it into practice

- Apply the knowledge acquired to a complete project.
- Identifying and correcting vulnerabilities.
- Presentation of solutions implemented.

Hands-on work
Project to secure a web or mobile application, from identifying vulnerabilities to correcting them.

14 OWASP Top 10 - Web application vulnerabilities part 2 - Post-training digital learning content

- Introduction.
- Injections.
- Authentication and session management violation.
- Exposure of sensitive data.
- The XXE (XML External Entity) attack.

Digital activities
In this online training course, you'll learn about the top 4 vulnerabilities in the OWASP Top 10, including injections (SQL, XPath, code), authentication and session management flaws, exposure of sensitive data and XXE attacks. You'll learn how hackers exploit them and what best practices to apply to secure your web applications.

Dates and locations

REMOTE CLASS
2026 : 24 Mar., 16 June, 22 Sep., 24 Nov.