Publication date : 03/26/2025

Course : Java application security

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

★★★★☆ 4,7 / 5

Nouvelle édition

This course will give you a thorough understanding of the security management mechanisms offered by Java, through a theoretical study of the concepts and their progressive implementation in stand-alone applications and application servers.

Teaching objectives

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

- ✓ Implementing security at the Java virtual machine level
- ✓ Use modern secure infrastructures to safeguard your applications
- ✓ Securing web services with OAuth 2.0

Intended audience

Developers and project managers involved in securing Java applications.

Prerequisites

Very good knowledge of the Java language. Experience in Java programming required.

Practical details

Hands-on work

Implementing security at the Java virtual machine level.

Course schedule

1 Fundamentals of Java application security

- Introduction to the JVM.
- Use of recent Java versions (Java 17+).
- Bytecode and obfuscation.
- Maven dependency management and library vulnerability detection.
- Set up a secure logging system (e.g. SLF4J, Logback or Log4J).

PARTICIPANTS

Developers and project managers involved in securing Java applications.

PREREQUISITES

Very good knowledge of the Java language. Experience in Java programming required.

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.

2 Authentication management

- Various authentication methods (password, biometric, digital key, etc.).
- Use of the OAuth 2.0 standard for modern access management.
- JWT (JSON Web Tokens) for secure session management.
- Multi-factor authentication (MFA).
- Integration of an identity provider.

Hands-on work

Mise en place d'un processus d'identification par mot de passe, d'une clé d'API et d'un token JWT avec Keycloak.

3 Access control and authorization

- Principle of least privilege in applications.
- Use of RBAC (Role-Based Access Control).
- Implementation of access controls in applications. (Spring Security).

Hands-on work

Setting up a secure section based on the principle of least privilege with Spring Security.

4 Using SSL/TLS

- Use SSL/TLS to secure communications.
- Secure configuration of database connections (use of SSL/TLS to connect to MySQL/PostgreSQL).
- Self-signed certificate generation with Java KeyStore.

Hands-on work

Generate a self-signed certificate with KeyStore and host an application with SSL.

5 Data security

- SQL Injection : comment les éviter (utilisation des Prepared Statements, ORMs comme Hibernate).
- Encryption of sensitive data in the database.
- Database access management (separation of roles and privileges).
- Secure password management (storage with algorithms such as MD5, SHA256 or bcrypt).

Hands-on work

Création d'une base de données stockant des mots de passe chiffrés, connexions utilisateurs et utilisation de requêtes préparées.

6 Modern, secure infrastructures

- The different HTTPS certificates.
- Zero trust models.
- Java security in containers.
- SIEMS.
- The CORS protocol.
- Secure architectures by design.

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.

7 Different types of attack

- Never Trust User Input validation.
- Secure RESTful APIs with headers such as Authorization and X-XSS-Protection.
- SQL injections.
- XSS and user input cleaning.
- CSRF (Cross-Site Request Forgery): implementation of anti-CSRF tokens.

Hands-on work

User data cleansing with OWASP.

Dates and locations

REMOTE CLASS

2026 : 18 Mar., 3 June, 14 Sep.