Sécurité des applications Java

Cours Pratique de 3 jours - 21h
Réf : JAS - Prix 2025 : 1 910 HT
Le prix pour les dates de sessions 2026 pourra être révisé

Cette formation vous permettra d'appréhender les mécanismes de gestion de la sécurité proposés par Java, grâce à l'étude théorique des concepts et à leur mise en œuvre progressive, au sein d'applications autonomes et de serveurs d'applications.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Mettre en œuvre la sécurité au niveau de la machine virtuelle Java

Exploiter des infrastructures sécurisées modernes pour sécuriser ses applications

Sécuriser ses services web avec OAuth 2.0

TRAVAUX PRATIQUES

Mise en œuvre de la sécurité au niveau de la machine virtuelle Java.

LE PROGRAMME

dernière mise à jour : 03/2025

1) Principes fondamentaux de la sécurité des applications Java

- Introduction à la JVM.
- Utilisation de versions récentes de Java (Java 17+).
- Bytecode et obfuscation.
- Gestion des dépendances avec Maven et détection des vulnérabilités dans les bibliothèques.
- Mise en place d'un système de logging sécurisé (ex: SLF4J, Logback ou Log4J).

2) Gestion de l'authentification

- Les diverses méthodes d'authentification (mot de passe, biométrique, clé numérique, etc.).
- Utilisation du standard OAuth 2.0 pour une gestion moderne des accès.
- JWT (JSON Web Tokens) pour la gestion des sessions sécurisées.
- L'authentification multifacteurs (MFA).
- Intégration d'un fournisseur d'identité.

Travaux pratiques : 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) Contrôle d'accès et autorisations

- Principe du moindre privilège dans les applications.
- Utilisation de RBAC (Role-Based Access Control).
- Implémentation de contrôles d'accès dans les applications. (Spring Security).

Travaux pratiques : Mise en place d'une section sécurisée basée sur le principe du moindre privilège avec Spring Security.

4) Utilisation de SSL/TLS

- Utilisation de SSL/TLS pour sécuriser les communications.
- Configuration sécurisée des connexions de bases de données (utilisation de SSL/TLS pour la connexion à MySQL/PostgreSQL).

PARTICIPANTS

Développeurs et chefs de projets amenés à sécuriser des applications Java.

PRÉREQUIS

Très bonnes connaissances du langage Java. Expérience requise en programmation Java.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

- Génération d'un certificat autosigné avec Java KeyStore.
Travaux pratiques : Génération d'un certificat autosigné avec KeyStore et hébergement d'une application avec SSL.

5) Sécurisation des données

- SQL Injection : comment les éviter (utilisation des Prepared Statements, ORMs comme Hibernate).
- Chiffrement des données sensibles dans la base de données.
- Gestion des accès à la base de données (séparation des rôles et privilèges).
- Gestion sécurisée des mots de passe (stockage avec des algorithmes comme MD5, SHA256 ou bcrypt).
Travaux pratiques : Création d'une base de données stockant des mots de passe chiffrés, connexions utilisateurs et utilisation de requêtes préparées.

6) Infrastructures sécurisées modernes

- Les différents certificats HTTPS.
- Principe de Zero trust models.
- Sécurité Java au sein des conteneurs.
- Les SIEMS.
- Le protocole CORS.
- Les architectures sécurisées par design.

7) Les différents types d'attaque

- Validation des entrées utilisateur (Never Trust User Input).
- Sécurisation des API RESTful avec des headers comme Authorization et X-XSS-Protection.
- Injections SQL.
- XSS et nettoyage des entrées utilisateurs.
- CSRF (Cross-Site Request Forgery) : mise en place de tokens anti-CSRF.
Travaux pratiques : Nettoyage des données utilisateurs avec OWASP.

LES DATES

CLASSE À DISTANCE	PARIS	STRASBOURG
2025 : 17 déc.	2025 : 17 déc.	2025 : 22 oct.
2026 : 18 mars, 03 juin, 14 sept.	2026 : 18 mars, 03 juin, 14 sept.	