Java/JEE, sécurité des applications

Cours Pratique de 3 jours - 21h
Réf : JAS - Prix 2024 : 1 870CHF HT

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, de serveurs d'applications JEE ainsi que de services Web SOAP et REST.

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 API spécifiques telles que JAAS, JSSE et JCE pour sécuriser vos applications.

Sécuriser vos services Web avec les API WS-Security et oAuth

TRAVAUX PRATIQUES

Mise en œuvre de la sécurité au niveau de la machine virtuelle Java, l'emploi des API spécifiques telles que JAAS, JSSE, JCE, WS-Security et oAuth.

LE PROGRAMME

dernière mise à jour : 06/2021

1) Présentation des concepts liés à la sécurité

- Identification et méthodes d'authentification.
- Autorisations et permissions.
- Confidentialité, non-répudiation, cryptage, clés publiques/privées, autorités de certification.
- Pare-feu et DMZ, rupture de protocole.
- Les types d'attaques.

2) Sécurité de la machine virtuelle Java

- Chargement des classes. Concept de "bac à sable".
- SecurityManager, AccessController et définition des permissions (fichiers .policy).
- Créer ses permissions avec Java Security Permission.
- Mécanismes de protection de l'intégrité du bytecode, la décompilation et l'obfuscation du code.
- Spécificités des Applets en matière de sécurité.

Travaux pratiques : Définition de .policy spécifiques.

3) Java Authentication and Authorization Service

- Architecture de JAAS.
- Authentification via le PAM, notion de Subject et de Principal.
- Gestion des permissions, les fichiers .policy.
- Utiliser JAAS avec Unix ou Windows, JNDI, Kerberos et Keystore. Le support du SSO.

Travaux pratiques : Configurer la politique de contrôle d'accès, mise en œuvre de l'authentification.

4) SSL avec Java

- Fonctions de Java Secure Socket Extension (JSSE).
- Authentification via certificats X.509. TLS et SSL.
- Encryption à base de clés publiques, Java Cryptography Extension (JCE).

PARTICIPANTS

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

PRÉREQUIS

Très bonnes connaissances du langage Java. Bonnes connaissances des concepts JEE. 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

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Utilisation de SSL avec HTTP.
Travaux pratiques : Configurer SSL et mise en œuvre de sockets SSL. Utiliser des outils du JDK (Keystore).

5) La sécurité d'une application JEE
- Authentification au niveau des conteneurs Web et EJB.
- Rôles applicatifs, permissions et descripteurs de déploiement XML.
- Contrôles dynamiques via les API Servlets et EJB.
- La sécurité dans les API : JDBC, JNDI, JTA, JMS, JCA.
Travaux pratiques : Sécurité d'une application déployée dans Tomcat.

6) La sécurité des services Web SOAP
- Sécurité au niveau HTTP.
- Sécurité au niveau SOAP & WSDL avec WS-Security (WSS4J, XWSS...) & WS-Policy.
- Les handlers SOAP WS-Security exploitant JAAS.
Travaux pratiques : Mise en pratique avec une implémentation de WS-Security (XWSS).

7) La sécurité des services Web REST
- Utilisation de SSL avec JAX-RS.
- Les apports de oAuth (authentification sur Internet).
- oAuth 1.0 et 2.0.
Travaux pratiques : Mise en pratique avec une implémentation Apache CXF de JAX-RS.

LES DATES

CLASSE À DISTANCE
2024 : 03 juin, 11 sept., 18 déc.