Java/JEE, sécurité des applications

★★★★★

SII-196 **3 Jours (21 Heures)**

Description

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 oeuvre progressive, au sein d'applications autonomes, de serveurs d'applications JEE ainsi que de services Web SOAP et REST.

À qui s'adresse cette formation ?

Pour qui

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

Prérequis

Aucune

Les objectifs de la formation

- Mettre en oeuvre de 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

Programme de la formation

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.

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.

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 oeuvre de l'authentification.

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

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.

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).

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.