Java/JEE, sécurité des applications

-Réference: **SII-196** -Durée: **3 Jours (21 Heures)**

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

A qui s'adesse cette formation ?

POUR QUI :

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

Programme

- **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.

Programme

- **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.

Programme

- 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.

(+212) 5 22 27 99 01

(+212) 6 60 10 42 56

Contact@skills-group.com

Nous sommes à votre disposition :
De Lun - Ven 09h00-18h00 et Sam 09H00 – 13H00

Angle bd Abdelmoumen et rue Soumaya, Résidence Shehrazade 3, 7éme étage N° 30
Casablanca 20340, Maroc