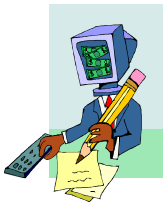
Sécurité JAVA

Ref : PJ-400



PROGRAMMATION

■ OBJECTIF DU STAGE

Comprendre les moyens de sécurisation disponibles

Savoir sécuriser une application Java/JEE de manière efficace

■ PRE-REQUIS

Avoir déjà quelques connaissances sur la programmation Java

■ NIVEAU

Approche pratique

■ DUREE

3 jours

■ PERSONNES CONCERNÉES

Ce cours s'adresse à toute personne désireuse de comprendre les besoins de sécurisation (Architecte, Développeur, Chef de projet, etc)

■ METHODE PEDAGOGIQUE

Le nombre de participants est limité à 6 personnes afin de permettre une progression rapide. La courte durée de ce stage impose un fil conducteur très directif et les stagiaires doivent réaliser les travaux pratiques en temps limité.

Répartition : 50% Théorie, 50% Pratique

■ DOCUMENT REMIS

Un manuel utilisateur.

■ DESCRIPTIF

• *Présentation des concepts liés à la sécurité*

Les différents types d'attaques
Terminologie

• *Sécurité de la machine virtuelle Java*

Historique
Le concept de "bac à sable"
Les mécanismes de protection

• *JCE : Java Cryptography Extension*

Mise en œuvre du chiffrement
Mise en œuvre de la signature
Configuration et choix des Security Provider

• *Le contrôle des Applets*

Les spécificités des applets en matière de sécurité
Le paquetage java.security.acl
Ajout d'une ACL dans le policy tool
Contenu du fichier policy

• *Le contrôle des applications*

Protection des accès sur le disque local
Surcharge des méthodes d'accès: ouverture de socket, autorisation de connexions, ...
Java Secure Socket Extension (JSSE).
L'authentification via certificats X.509, TLS et SSL.
JAAS
Présentation du principe et des acteurs JAAS
Notion de *Principal* et de *Subject*

• *La sécurité d'une application JEE*

Authentification au niveau d'un conteneur Web et d'un conteneur EJB
Rôles applicatifs, permissions et descripteurs de déploiement XML

Prefix Informatique
3, rue des Lavandes
34470 PEROLS (Montpellier)
☎ **04 67 50 09 88**
noirault@prefix-info.fr
www.prefix-info.fr