Sécurité Java

Durée: 3 Jours Réf de cours: GKJSEC

Résumé:

Le langage Java contient intrinsèquement de nombreux mécanismes permettant l'élaboration de programmes sûrs. Ces mécanismes concernent les différentes facettes de la sécurité comme l'intégrité, la confidentialité, l'identification et la protection contre les malveillances. Cette formation permet de passer en revue ces différents sujets et propose à chaque fois des ateliers pédagogiques permettant de comprendre les mécanismes d'exécution de la JVM.

Public visé:

Cette formation s'adresse à des développeurs, concepteurs, chefs de projets, architectes techniques.

Pré-requis:

Avoir une expérience de programmation en langage JAVA.

Contenu:

Introduction et rappels

Chargement et vérification des cla

sses

- Rôle du compilateur Java
- Rôle des classloader
- Les différentes zones mémoires de la JVM et leur gestion par le garbage collector
- Hiérarchie des différents classloader
- Vérification du byte-code
- Chargement dynamique de classe
- Implémenter un class loader

T.P. : Modification d'un fichier .class et exécution avec l'option -noverify, Implémentation d'un classloader chargeant des classes cryptées

Gestionnaire de sécurité et permissions

- Opérations contrôlables
- Activation du gestionnaire de sécurité
- Domaine de protection, provenance du code et permissions
- Parcours de l'API
- Fichier .policy
- Les classes *Permission*
- Implémentation d'une classe *Permission*

T.P. : Mise au point d'un fichier .policy, implémentation d'une classe Permission

JAAS, Authentification et Autorisations

- Présentation de JAAS
- *LoginContext* et *LoginModule*
- Configuration et empilement des login modules
- LoginModule disponibles
- Implémentation d'un login module spécifique, les *CallbackHandler*
- Packaging d'un login module
- Autorisations, Objet Subject et Principals
- Interface PrivilegedAction
- Configuration des permissions

T.P. : Implémentation d'un LoginModule, Configuration des autorisations à partir de rôles utilisateurs

Signatures numériques et chiffrement

- Empreinte de messsage : SHA1 et MD5
- Signature numérique, clé publiques et clés privées
- L'outil keytool et les keystore
- L'outil jarsigner
- Les autorités de certification
- Déploiement de code signé dans un intranet ou sur internet
- Permissions basées sur des keystore
- Chiffrement de données, les algorithmes AES et RSA

T.P. : Vérification d'une empreinte, Déploiement d'une applet dans un intranet, Chiffrement symétrique et asymétrique

Application de la sécurité dans un environnement Web

- Sécurisation d'un serveur applicatif Java
- Authentification des utilisateurs, descripteur de déploiement d'une application web
- Configuration des logins modules dans les principaux serveurs applicatifs
- Sécurité déclarative des différents tiers de Java EE
- SSL

T.P. : Sécurisation d'une application web

Les attaques WEB

- Les ressources de l'OWASP
- Les dix risques de sécurité applicatifs Web les plus critiques selon l'OWASP
- Identification des principaux risques dans la Cybersécurité
- Configuration d'un scan
- Lancement de l'opération de Scan
- Analyse des résultats

- Les ressources de l'OWASP
- Les dix risques de sécurité applicatifs Web les plus critiques selon l'OWASP
- Identification des principaux risques dans la Cybersécurité
- Configuration d'un scan
- Lancement de l'opération de Scan
- Analyse des résultats

L'audit d'applications en mode dynamique avec APPSCAN Standard

- Les ressources de l'OWASP
- Les dix risques de sécurité applicatifs Web les plus critiques selon l'OWASP
- Identification des principaux risques dans la Cybersécurité
- Configuration d'un scan
- Lancement de l'opération de Scan
- Analyse des résultats

Méthodes pédagogiques :

Les travaux pratiques utilisent l'IDE Eclipse.
Support de cours remis aux participants

Autres moyens pédagogiques et de suivi: