



Conseil, ingénierie, formations

Formation Sécurité Java/JEE

Durée : 2 jours

Public : Tous

Pré-requis : Connaissance de Java, notions de JEE

Objectifs : Connaître les risques de sécurité d'un site réalisé avec JEE - Savoir mettre en place et maintenir la sécurité d'une application JEE

Introduction

Historique et versions de Java et des outils
Présentation de risques et de catastrophes
Rappels des technologies du domaine : HTML, javascript, CSS, XML
Rappels sur les technologies Java : JSE, JME, Servlets, JSP, Applets, EJBs

Présentation des principes de sécurité

Les enjeux généraux
Méthodes d'évaluation du risque
Exigences et vulnérabilités correspondantes
Types de menaces
Standardisation, méthodes et solutions de test

Disponibilité du service

Les risques courants et les malveillances
Principes de réplication/redondance

Atelier pratique : clusters de serveurs avec Tomcat

La confidentialité

Les systèmes de contrôle d'accès
La cryptographie pour HTTP
Communication interne à Java : résumé des protocoles
La cryptographie pour la communication dans Java
Mise en place et études de cas

L'intégrité du service et l'imputabilité

Possibilités de signature en Java
Les certificats, les applets
Retour sur le contrôle d'accès
Limite de l'imputabilité en Java
Conclusion sur la sécurité

Les avantages

- Un support et les exercices du cours pour chaque stagiaire
- Un formateur expert ayant suivi une formation à la pédagogie
- Le déjeuner compris en inter-entreprises
- Boissons offertes pendant les pauses en inter-entreprises
- Soutien du formateur pendant un mois
- Salles lumineuses et locaux facilement accessibles
- Méthodologie basée sur l'Active Learning : 75% de pratique minimum