Sécurité des Développements Web Java

Référence : **SECSJWD** Durée : **3 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• 1-Connaissance du langage JAVA. • 2-Connaissance du développement Web en JAVA EE. • 3- Avoir suivi la formation DELJ001 Concepts objets et programmation Java. • 4- Avoir suivi le cours DEAS004 JEE Développement Web.

PROFIL DES STAGIAIRES

• Chefs de projet. • Développeurs.

OBJECTIFS

• Appréhender les différentes attaques existantes. • Comprendre les enjeux de la sécurité des applications web. • Connaître les mécanismes de sécurité spécifiques à JAVA EE. • Mettre en place les bonnes pratiques de sécurité.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité défensive

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Jour 1

Architecture d'un projet JAVA

- Structure d'une webapp JEE
- Configuration et fonctionnement de base
- Top 10 des vulnérabilités/menaces OWASP

Le cross-site scripting (JavaScript)

- Principe du cross scripting
- Vol de session
- Fixement de session
- Comment s'en prémunir ?

Jour 2

Les Injections SQL

- Principe général
- Exécution d'une injection SQL, les différentes étapes
- Comment sécuriser les accès à la base de données ?

Gestion des fichiers

- L'upload de fichiers
- Les fichiers temporaires
- L'accès direct à des fichiers déployés
- Contrôler le contenu des fichiers

Jour 3

Authentification et autorisation

- Bien gérer les mot de passe et les comptes utilisateurs
- Cryptographie et hashage
- Authentification sécurisée
- Gestion des droits au niveau des URL

- Gestion des droits au niveau des méthodes
- Illustration avec spring security

Autres fonctions à risque

- Exécution de commande système
- Librairies tierces

Le déploiement d'un projet JAVA