

## **Formation: Sécurité des applications Java et Java EE**

Domaine : Base de données

### **DESCRIPTION**

Comme les des réseaux et programmes informatiques, les applications Java et Java EE font face à des enjeux de sécurité. Ainsi, il devient primordial d'appréhender cet aspect sécurité pour garantir la fiabilité des applications. Cette formation vous apportera une compréhension complète des risques liés aux applications et vous formera aux divers outils et techniques pour assurer leur protection.

### **LES OBJECTIFS DE LA FORMATION**

- Comprendre les problématiques de sécurité des applications Web
- Connaître les meilleures pratiques pour écrire un code de qualité intégrant de façon native les fondamentaux de la sécurité
- Connaître les principales attaques Web pour comprendre comment s'en prémunir
- Savoir appliquer les mécanismes techniques de prévention des risques tel que l'authentification forte le cryptage de données ou encore l'utilisation de certificats

### **POUR QUI**

- Développeurs
- Chargés de développement d'applications informatiques

### **PREREQUIS**

- Disposer d'une première expérience de développement
- Maîtriser un langage de programmation (C#, Java ou C++)
- Disposer de notions sur la cryptographie est un plus pour suivre cette formation

## **PROGRAMME**

### **SÉCURITÉ DANS LE FRAMEWORK ET DU CODE**

- Concepts fondamentaux
- Sécurité d'accès du code et des ressources
- Sécurité basée sur les rôles
- Le principe du W^X
- Services de chiffrement
- Validation et contrôle des entrées / sorties
- Gestion et masquage d'erreurs
- Gestion sécurisée de la mémoire
- Contrôle d'authenticité et d'intégrité d'une application/d'un code
- Offuscation du code
- Reverse engineering sur : bundle C#, application Java, binaire Windows
- Contrôle des droits avant exécution du code
- Sécuriser les données sensibles présentes dans un binaire
- Stack/Buffer/Heap overflow

### **LES BASES DE LA CRYPTOGRAPHIE**

- Cryptographie - Les définitions
- Types de chiffrement : chiffrement à clés partagées, chiffrement à clé publique
- Symétrique vs. asymétrique, combinaisons symétrique / asymétrique
- Fonctions de hachage
- Utilisation des sels
- Signatures numériques, processus de signature, processus de vérification

### **CHIFFREMENT, HASH ET SIGNATURE DES DONNÉES**

- Cryptographie Service Providers (CSP)
- System, security, cryptography
- Choix des algorithmes de chiffrement
- Chiffrement symétrique : algorithmes (DES, 3DES, RC2, AES), chiffrement de flux, mode de chiffrement (CBC, ECB, CFB)
- Algorithmes asymétriques
- Algorithme : RSA, DSA, GPG
- Algorithme de hachage : MD5, SHA1 / SHA2 / SH3

### **VUE D'ENSEMBLE D'UNE INFRASTRUCTURE À CLÉ PUBLIQUE (PKI)**

- Certificat numérique : certificat X.509

- PKI - Les définitions
- Les fonctions PKI
- PKI - Les composants
- PKI - Le fonctionnement
- Applications de PKI : SSL, VPN, IPSec
- IPSec et SSL en entreprise
- Smart Cards (cartes intelligentes)
- Autorité de certification

## **SSL ET CERTIFICAT DE SERVEUR**

- Certificat de serveur SSL : présentation, autorité de certification d'entreprise, autorité de certification autonome

## **UTILISATION DE SSL ET DES CERTIFICATS CLIENTS**

- Certificats clients
- Fonctionnement de SSL : phase I, II, III et IV
- Vérification de la couverture d'utilisation d'un certificat (lors du handshake)
- Vérification des dates d'utilisation d'un certificat

## **SÉCURITÉ DES SERVICES WEB**

- Objectifs de la sécurisation des services Web : authentification, autorisation, confidentialité et intégrité
- Limitations liées à SSL
- Sécurité des services Web : WSE 2.0, sécurisation des messages SOAP / REST

## **JETONS DE SÉCURITÉ**

- Jetons de sécurité : User-Name Token, Binary Token, XML Token, JWT (JSON Web Tokens), Session-based Token
- Intégrité d'un jeton (MAC / HMAC)
- Cycle de vie d'un jeton, expiration automatique (ou pas), contexte d'utilisation d'un jeton
- Habilitations suivant le contexte du jeton
- Certificats X.509
- Signature des messages SOAP / REST : création d'un jeton de sécurité, vérification des messages (MAC / HMAC), chiffrement des messages, déchiffrement du message

## **SÉCURITÉ ET DÉVELOPPEMENT WEB**

- Classification des attaques : STRIDE, OWASP
- Les erreurs classiques
- Authentification par jeton et gestion des habilitations
- Les handlers et méthodes HTTP
- Séparation des handlers par contexte de sécurité
- Attaque par injection
- Injection HTML

- Injection CSS
- Injection JS
- Injection SQLXSS (Injection croisée de code) : XSS réfléchi, XSS stocké
- XSS Cookie Stealer
- CSRF : Cross-Site Request Forgery

## **OUTILS DE SÉCURITÉ ET D'AUDIT**

- Outils du SDK liés à la sécurité
- Outils pour mener les tests de sécurité