Sécurité applicative Java

Référence SEC-JAV
Durée 3 jours (21 heures)
Certification Aucune
Appréciation des résultats Évaluation qualitative de fin de stage
Modalité et moyens pédagogique Démonstrations – Cas pratiques – Synthèse et évaluation des acquis

À l'issue de ce stage vous serez capable de :

- Connaître les mécanismes de sécurité du JDK
- Comprendre les principales failles de sécurité applicative
- Distinguer sécurité applicative et sécurité réseau
- Mettre en oeuvre les principales stratégies de sécurité en Java
- Utiliser Java Cryptography Extension (JCE)
- Authentifier et autoriser l'accès aux composants Java EE.

Niveau requis

Avoir des connaissances en développement d'application en langage Java ou langage assimilé.

Public concerné

Pentesters et développeurs.

Cette formation :

- est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation ;
- bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Jour 1

La sécurité sous Java

- Sécurité Java SE
- Vérification et Class Loader
- Security Manager
- Access Controller

- Sandbox
- Fichier Java policy
- Package security

Le chiffrement avec Java

- Chiffrement en Java
- Bases du chiffrement
- Librairie JCE
- Classe Cipher
- Algorithmes symétriques type AES
- Algorithme asymétrique RSA
- Fonctions à sens unique type SHA
- Génération de clés
- Génération de certificats

Exemple de travaux pratiques (à titre indicatif)

- **Challenge de cryptographie**

Jour 2

La sécurité avec Java EE

- Sécurité Java EE
- Authentification Web
- HTTP basic et form
- HTTPS et JSSE
- Modules JAAS
- LoginModule
- Rôles et domaines
- Protection des URL
- Protection des méthodes
- Annotations de sécurité
- Sécurité programmatique
- Sécurité réseau et sécurité applicative
- Firewall, proxy et DMZ

Exemple de travaux pratiques (à titre indicatif)

- **Mise en place d'une PKI**

Tester les failles d'une application

- Anatomie d'une faille applicative
- Open Web Application Security Project
- Le Top 10 OWASP
- CVE (Common Vulnerabilities and Exposures)
- CWE (Common Weakness Enumeration)
- CVSS (Common Vulnerability Scoring System)

Exemple de travaux pratiques (à titre indicatif)

- **Installation de Web Goat et ESAPI**

Jour 3

- Failles et remèdes
- Injections SQL
- Cross Site Scripting
- Détournement de sessions
- Référence directe par URL
- Cross Site Request Forgery
- La faille sur les API
- IDOR
- SSRF

Exemple de travaux pratiques (à titre indicatif)

- **Challenge Client et Serveur**

Mettre en place du secure code

- Créer une checklist des bonnes pratiques pour son application
- Ajouter un analyse des risques
- Durcir son application avec OWASP ASVS
- Utiliser les bons outils
  - DAST (Dynamic Application Security Testing)
  - SAST (Static Application Security Testing)
  - WAF (Web Application Firewall)