Secure Coding Java

Objectifs :

- sensibiliser les développeurs sur la sécurité du code
- connaître le fonctionnement du chargement des classes
- savoir repérer les erreurs dans le code
- connaître le rôle des acteurs et la classification des risques : CERT, CWE, OWASP
- connaître les bonnes pratiques à appliquer

Durée : 1 journée

Public : développeurs, chefs de projets

Prérequis :

- pratique du langage Java

Démarche pédagogique :

- présentation des concepts, démonstrations et ateliers
    - utilisation de POC (Proof of Concept) et discussion sur les corrections
    - mise en oeuvre des bonnes pratiques

Programme détaillé :

- tIntroduction
    - les risques liés au développement
    - les traces laissés par les développeurs
        - mémoire, journaux, …
    - les attaques
    - les différents acteurs : CERT, PCI, CWE, OWASP, …
    - codage sécurisé d'une application
- Classification des risques CERT
    - domaines
        - validation des entrées, déclaration et initialisation, expressions, ...
    - sévérité, priorité, ...
    - guidelines
- Langage Java et la JVM
    - sécurité intrinsèque du langage
    - modèle mémoire
    - les piles de la JVM
    - le chargement des classes
    - modèle de sécurité : sandbox, fichier policy, ….
- Les bonnes pratiques
    - validation des entrées
    - opérations sur les types numériques
    - les classes

    - les exceptions
    - multi-threading et synchronisation
    - les entrées-sorties
    - la sérialisation
    - gestion des permissions
- Conclusion