Formation Java Security

Code : DEV-JAVA-300 Durée : 3 jours (21 heures)

Public visé

Pentesters, développeurs impliqués dans des cycles DevSecOps, développeurs déjà formés aux bonnes pratiques du développement sécurisé et souhaitant découvrir les méthodes de protection des contournements potentiels.

{{< formation-prerequis >}}

Objectifs pédagogiques

À l'issue de cette formation, vous serez capable de :

- Reconnaître les mécanismes de sécurité du JDK (Java Development Kit)
- Décrire les principales failles de sécurité applicative
- Distinguer la sécurité applicative de la sécurité système et réseau
- Mettre en oeuvre les principales stratégies de sécurité en Java
- Utiliser JCE (Java Cryptography Extension)
- Authentifier et autoriser l'accès aux composants Java EE
- Créer des tests visant à éprouver la sécurité des applications
- Formuler des exigences de sécurité aux autres corps de métiers

Programme

Jour 1 - Matin

Rappels sur la sécurité applicative

- Fonctionnement de la pile d'exécution
- L'analyse de code
- L'hijacking de ressources
- Les overflows
- Les protections lors de l'exécution

La sécurité des plateformes Java

- La sécurité de Java SE / ME / FX
- Le Java Class Loader
- Le Security Manager

- L'Access Controller
- Le Sandboxing
- Implémentation de la Default Policy
- La Policy File Syntax
- Contenu du Package java.security

Jour 1 - Après-midi

Le chiffrement avec Java

- Rappel des bases du chiffrement
- Les fonctions de hash
- Les algorithmes symétriques type AES
- Les algorithmes asymétriques type RSA
- La librairie JCE (Java Cryptography Extension)
- La classe Cipher
- Générer des clés
- Générer des certificats

Travaux pratiques indicatifs :

- Création d'un outil de chiffrement / déchiffrement symétrique
- Création d'un outil de vérification de l'intégrité de contenu d'un répertoire

Jour 2 - Matin

La sécurité avec Java EE

- La sécurité de Java EE
- L'HTTPS avec JSSE (Java Secure Socket Extension)
- Gestion de l'authentification Web
- Exploitation des HTTP basic et HTTP form
- Utilisation du module JAAS (Java Authentication and Authorization Service)
- Utilisation du module LoginModule
- Définition des rôles et domaines
- Les fichiers .policy
- Créer des permissions avec Java Security Permission
- La protection des URL
- La protection des méthodes
- Les annotations de sécurité
- La sécurité programmatique de Java EE

Travaux pratiques indicatifs :

- Mise en place d'une PKI
- Création d'un formulaire d'authentification

Jour 2 - Après-midi

Tester les failles d'une application

- Anatomie d'une faille applicative
- Présentation de l'OWASP et de ses projets
- Les Security Cheat Sheets
- Le Top 10
- Les guides de l'OWASP (Test Guide, Dev Guide...)
- L'ASVS (Application Security Verification Standard)
- Les grandes familles de vulnérabilités
- Les CVE (Common Vulnerabilities and Exposures)
- Les CWE (Common Weakness Enumerations)
- Le scoring CVSS (Common Vulnerability Scoring System)

Travaux pratiques indicatifs :

- Installation de WebGoat et ESAPI
- Estimation de la vulnérabilité d'un produit commercial
- Exploitation d'une injection d'entête HTTP
- Exploitation d'une injection SQL
- Exploitation d'une Cross-Site Scripting
- Exploitation d'une Cross-Site Request Forgery
- Exploitation d'une Server-Side Request Forgery
- Exploitation d'un vol de session
- Exploitation d'une désérialisation
- Exploitation d'une référence directe à un objet

Jour 3 - Matin

La sécurité du code externe

- Le cas des librairies
- Le cas des API
- La sécurité dans les API JDBC, JNDI, JTA, JMS et JCA

La sécurité des WebServices

- La sécurité des WebServices SOAP
- Utilisation de WS-Security avec WSS4J et XWSS
- Utilisation de WS-Policy
- La sécurité des WebServices REST
- Utilisation de JAX-RS
- Utilisation de OAuth 1.0 et 2.0

Jour 3 - Après-midi

Mettre en place du Secure Code

- Durcir son application avec l'OWASP ASVS et l'OWASP Dev Guide
- Les bonnes pratiques de sécurisation du code

- La protection du bytecode
- Se protéger de la décompilation
- L'obfuscation du code
- Les descripteurs de déploiement XML
- L'authentification des conteneurs Web et EJB
- Les contrôles dynamiques

Faire des tests et des validations

- Les tools des navigateurs
- La capture via proxy
- La capture via tcpdump ou Wireshark
- Les tests avec Postman
- Les vulnerability scanners
- Le DAST (Dynamic Application Security Testing)
- Le SAST (Static Application Security Testing)
- Sonatype Nexus, Acunetix, Contrast Security

Filtrer les échanges

- Les WAF (Web Application Firewalls)
- Les IPS (Intrusion Prevention System) et IDS (Intrusion Detection System)

Limiter l'exposition

- Rôle des firewalls, proxies et DMZ

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode démonstrative, interrogative et active via travaux pratiques et mises en situation.

Moyens pédagogiques :

- Ordinateurs Mac ou PC, connexion internet fibre
- Tableau blanc ou paperboard
- Vidéoprojecteur ou écran tactile interactif (distanciel)
- Environnements de formation installés sur postes ou en ligne
- Supports de cours et exercices

Modalités d'évaluation des acquis

- En cours de formation, par des études de cas ou travaux pratiques
- En fin de formation, par questionnaire d'auto-évaluation

Accessibilité

Le groupe M2I s'engage pour faciliter l'accessibilité de ses formations. Toutes nos formations sont accessibles aux personnes en situation de handicap.

Modalités et délais d'accès

Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.

{{< formation-require >}}

{{< formation-seealso >}}