Sécurité Applicative Java

Lien : https://innov-systems.com/formation/securite-applicative-java

DURÉE
4 jours (28h)

RÉFÉRENCE
SEC122

CATÉGORIE
Sécurité des Applications

OBJECTIFS DE LA FORMATION

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

- Connaître les mécanismes de sécurité du JDK
- Connaitre et comprendre les principales failles de sécurité applicative
- Apprendre à sécuriser les différents aspects techniques d’une application
- Être capable de tester la sécurité des applications Java

POUR QUI ?

- Développeurs
- Chefs de projets amenés à sécuriser des applications Java et JEE

Programme détaillé

1 / Concepts liés à la sécurité

- L’importance de la sécurité
- Les failles de sécurité classiques
- Identification et méthodes d'authentification
- Autorisations et permissions d’accès
- Confidentialité : les mécanismes de cryptage
- Pare-feu et DMZ, rupture de protocole
- Les types d'attaques
- Le modèle de sécurité de la JVM

2 / Sécurisation de la JVM

- Le bac à sable
- ClassLoader
- SecurityManager
- AccessController
- Le fichier java.policy
- Le fichier security.policy
- L'outil PolicyTool

3 / Le chiffrement en Java

- Les bases du chiffrement
- Classe java.security.Security
- Classe java.security.Provider
- Les services d’un provider
- Les algorithmes de Chiffrement
- Les algorithmes symétriques type AES

- L'algorithme asymétrique RSA
- Les fonctions à sens unique type SHA
- La génération de clés
- La génération de certificats X.509
- Les outils GnuGPG, GPG4Win, Keytool

4 / Java Authentication and Authorization Service

- Architecture de JAAS
- Authentification via le PAM, notion de Subject et de Principal
- Gestion des permissions, les fichiers .policy
- Utiliser JAAS avec Unix ou Windows, JNDI, Kerberos et Keystore. Le support du SSO

5 / SSL avec Java

- HTTP basic et form
- HTTPS et JSSE
- Authentification via certificats X.509. TLS et SSL
- Encryption à base de clés publiques, Java Cryptography Extension (JCE)

6 / La sécurité d'une application JEE

- Sécurité Java EE
- Authentification Web et EJB
- Rôles applicatifs, permissions et descripteurs de déploiement XML
- Contrôles dynamiques via les API Servlets et EJB
- La sécurité dans les API : JDBC, JNDI, JTA, JMS, JCA
- LoginModule
- Rôles et domaines
- Protection des URL
- Protection des méthodes
- Annotations de sécurité

- Sécurité programmatique
- Sécurité réseau et sécurité applicative
- Pare-feu et DMZ

7 / 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)
- 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

8 / 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, SAST, WAF

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

21 au 24 Juil. 2026	Présentiel - Casablanca
15 au 18 Sep. 2026	Distanciel
10 au 13 Nov. 2026	Distanciel

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com