Formation Sécurité des applications Java

Informations

Durée : 3 jours (21h.)

Tarif* : 1790 € HT

Réf : SEJA

Niveau : Difficile

inter intra à distance

*tarif valable jusqu'au 13/07/2024

Prochaines sessions

21 octobre - 23 octobre ()

Pré-requis

- Maîtriser Java

Objectifs

- Identifier le périmètre de la sécurité des applications Java
- Contrôler les actions de tout code java sur votre système (fichier .policy)
- Mettre en oeuvre les API de cryptographie : JCA/JCE
- Sécuriser l'accès à vos écrans web et vos EJB avec JAAS
- Utiliser l'outil keytool pour manipuler des certificats
- Sécuriser via SSL la communication entre client/serveur

Programme

Les concepts clés

L'authentification
L'autorisation
La confidentialité
L'intégrité
L'empreinte
Le chiffrement
La signature

Les failles et les remèdes

Top 10 OWASP
Les injections SQL
Cross Site Scripting (XSS)
Le détournement de sessions
La référence directe par URL
Cross Site Request Forgery (CSRF)

La sécurité Plateforme

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

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

La sécurité conteneur web et EJB

Spécification JAAS
Realm DB, LDAP, LoginModule
HTTP BASIC, FORM, CLIENT-CERT
Spécificités Tomcat / WILDFLY / GLASSFISH
@ServletSecurity, @HttpConstraint

@RunAs,DeclareRoles,@RolesAllowed,
@DenyAll, @PermitAll...
Les limites de JAAS
Les outils : Apache Shiro, Spring Security

L'audit Sécurité

Les scanners réseau / Ports
Les scanners de Vulnérabilité
La base de données d'exploits
Les normes PCI/DSS
Les normes CERT JAVA
Les outils : Nmap, OpenVAS, WebGoat