Sécurité des Applications Java, .NET et PHP

Lien : https://innov-systems.com/formation/securite-des-applications-java-net-et-php

DURÉE
4 jours (28h)

RÉFÉRENCE
SEC118

CATÉGORIE
Sécurité des Applications

OBJECTIFS DE LA FORMATION

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

- Identifier et décrire les enjeux de la sécurité
- Appréhender les mécanismes de gestion de la sécurité proposés par Java, .NET et PHP
- Apprendre à sécuriser vos applications objet

POUR QUI ?

- Développeurs
- Architectes applicatifs
- Chefs de projets

Innov Systems

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 / Sécurité de la machine virtuelle Java

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

3 / 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

4 / Le chiffrement en Java

Innov Systems

- 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

5 / 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

1 / Problématique de sécurité en .NET

- Définition de sécurité
- Authentification, Protection, Cryptage
- Outils de sécurité .NET
- Sécurité d'exécution, authentification, protection des données et des accès
- Types de menaces, validation des données saisies

Innov Systems

2 / Sécurité du Framework .NET

- Protection du contenu des assembly
- Protection de l'exécution des programmes
- Déploiement d'une stratégie de sécurité du CLR
- Stratégie de sécurité et déploiement des applications
- Règles d'exécution selon la provenance des applications
- Nouveautés de .NET4
- Confiance totale/Partielle

3 / Sécurité du code .NET

- Code transparent de sécurité, critique de sécurité et critique sécurisée
- Quelles sont les autorisations d'accès du code ?
- Chiffrement des informations de configuration
- Mettre en place la gestion déclarative/impérative des mécanismes de sécurité
- Effectuer la restriction/vérification des droits de l'exécution du programme
- Comment mettre en œuvre la gestion de la sécurité à partir des rôles

1 / Les bons réglages pour sécuriser PHP

- Le fichier de configuration PHP.ini
- Protection des scripts
- Protection physique
- Exécution de scripts distants ou à la volée
- Les cookies et les sessions

2 / Sécuriser l’accès aux bases de données

- Scénarii d’authentification vers une base de données
- Les attaques par SQL Injection. Principe et contre-mesure
- Procédures stockées et requêtes paramétrées. Limites
- Les fichiers d'accès

Innov Systems

- Organisation et valeurs par défaut
- Accès anonymes et protocoles

3 / Sécuriser l'emploi des extensions en PHP

- Email. Spam via un formulaire de contact : injections et contre-mesures
- Réaliser les accès réseau par PHP
- Les appels séquentiels et récursifs
- Les attaques furtives

4 / Les vulnérabilités des applications Web

- Les risques majeurs des applications Web selon l'OWASP
- Les attaques "Cross Site Scripting" ou XSS
- Les attaques en injection (commandes injection, SQL Injection, LDAP injection...)
- Les attaques sur les sessions
- Exploitation de vulnérabilités sur le frontal HTTP (ver Nimda, faille Unicode)
- Attaques sur les configurations standards
- Comment effectuer la recherche des vulnérabilités
- Rechercher les vulnérabilités les plus répandues
- Le Cross-Site Scripting. L’injection SQL
- Les erreurs de logique applicative

5 / Les bonnes pratiques

- Les différents types d'entrées
- Effectuer la validation des entrées
- Les types d'opérations qui peuvent être effectuées sur les types numériques
- Les classes et les exceptions
- Multi-threading et synchronisation
- Les entrées-sorties, la sérialisation
- Savoir effectuer la gestion des permissions

Inov Systems

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

16 au 19 Fév. 2027	Présentiel - Casablanca
13 au 16 Avr. 2027	Présentiel - Casablanca
08 au 11 Juin 2027	Présentiel - Casablanca
03 au 06 Août 2027	Présentiel - Casablanca
28 Sep. au 01 Oct. 2027	Présentiel - Casablanca

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

Innov Systems — Tous droits réservés