Sécurité des Applications et Prévention des Cyberattaques

Lien :
https://innov-systems.com/formation/securite-des-applications-et-prevention-des-cyberattaques

DURÉE
3 jours (21h)

RÉFÉRENCE
DEV355

CATÉGORIE
Développement D'applications (Java, Eclipse, Windows 10, Spring, Jquery, Labview, Testsand)

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Concevoir des applications robustes et sécurisées dès la phase de design
- Identifier, comprendre et prévenir les principales vulnérabilités applicatives
- Mettre en œuvre les bonnes pratiques de sécurité dans le cycle de développement logiciel
- Expérimenter les techniques offensives et défensives pour renforcer la posture de sécurité
- Élaborer une stratégie de sécurité applicative adaptée à son contexte professionnel

POUR QUI ?

- Développeurs
- Architectes logiciels
- Responsables techniques
- Testeurs et QA
- Équipes Ops et DevOps

Programme détaillé

1 / INTRODUCTION À LA SÉCURITÉ LOGICIELLE

- Rappel des enjeux de la sécurité applicative dans un contexte professionnel
- Notion de “Secure by Default” et “Defense in Depth”
- Les coûts de l’insécurité logicielle : exemples concrets d’attaques

2 / SECURE BY DESIGN : CONCEVOIR UNE APPLICATION SÉCURISÉE

- Principes de conception sécurisée (10 règles d’or)
- Études de cas d’architectures applicatives
- Atelier de réflexion : analyse critique d’un design applicatif

3 / MÉCANISMES DE PROTECTION NATIFS

- Fonctionnement de la SOP (Same Origin Policy)
- Gestion sécurisée du CORS
- Rôle et configuration de la CSP
- Démonstration d’erreurs de configuration fréquentes

4 / SIMULATION D’ATTAQUE ET ANALYSE

- Challenge d’équipe : mise en situation d’un scénario d’attaque
- Debrief : identifier les failles exploitées et proposer des contre-mesures

5 / LE TOP 10 OWASP ET SES ENJEUX

- Panorama des vulnérabilités les plus critiques
- Focus sur les menaces émergentes
- Corrélations entre failles techniques et risques métiers

Inov Systems

6 / MISE EN PRATIQUE DES ATTAQUES – PARTIE 1

- Attaque XSS (Cross Site Scripting) : principe, impact, prévention
- Attaque SQL Injection : exploitation et contre-mesures
- Attaque SSTI (Server Side Template Injection)

7 / MISE EN PRATIQUE DES ATTAQUES – PARTIE 2

- Attaque IDOR (Insecure Direct Object Reference)
- Attaque Mass Assignment
- Attaque CSRF (Cross Site Request Forgery)
- Atelier pratique sur application volontairement vulnérable

8 / ANALYSE POST-ATTAQUE ET TRAÇABILITÉ

- Techniques de logging et monitoring
- Comprendre les signaux faibles d’une intrusion
- Bonnes pratiques de gestion d’incident

9 / BONNES PRATIQUES DE SECURE CODING

- Validation stricte des entrées utilisateurs
- Gestion des erreurs et exceptions
- Utilisation sécurisée des dépendances et librairies
- Atelier de refactoring sécurisé

10 / PROTECTION DES SESSIONS ET DES DONNÉES

- Sécurité des cookies et gestion des tokens
- Paramètres TLS et configuration HTTPS avancée
- Entêtes HTTP de sécurité : bonnes pratiques

11 / OUTILS ET CULTURE DE LA SÉCURITÉ DANS LE CYCLE DE DEV

Inov Systems

- Intégration du “Security as Code” dans les pipelines CI/CD
- Analyse statique et dynamique de code
- Automatisation des tests de sécurité

12 / ATELIER DE SYNTHÈSE : CONSTRUCTION D’UN PLAN DE SÉCURITÉ APPLICATIVE

- Définir une stratégie de protection adaptée à son contexte
- Élaboration collective d’un plan d’action post-formation
- Restitution et partage d’expériences

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

27 au 29 Jan. 2027	Présentiel - Casablanca
24 au 26 Mars 2027	Présentiel - Casablanca
19 au 21 Mai 2027	Présentiel - Casablanca
14 au 16 Juil. 2027	Présentiel - Casablanca
15 au 17 Sep. 2027	Présentiel - Casablanca

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

Innov Systems

Réservation & Renseignements

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

Innov Systems — Tous droits réservés

Innov Systems