Sécurité des Applications Web pour les Développeurs

Lien : https://innov-systems.com/formation/securite-des-applications-web-pour-les-developpeurs

DURÉE
4 jours (28h)

RÉFÉRENCE
SEC132

CATÉGORIE
Sécurité des Applications

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Identifier les vulnérabilités les plus courantes des applications Web
- Comprendre le déroulement d'une attaque
- Connaître les bonnes pratiques pour un développement sécurisé
- Savoir mettre en place une authentification sécurisée des utilisateurs

POUR QUI ?

- Chefs de projets
- Développeurs

Programme détaillé

1 / Introduction

- Les technologies web, les risques
- Mythes et réalités
- Statistiques et évolutions

2 / Vulnérabilités des applications Web

- L'exposition des applications Web
- Classement des risques majeurs selon l'OWASP et le CWE
- Analyse des vulnérabilités et des conséquences de leur exploitation
- Les principales attaques :
- "Cross Site Scripting” (XSS)
- Les attaques en injection
- Les attaques sur les authentifications et sessions
- Attaques de type DDOS
- CSRF...
- Les vulnérabilités des frameworks et CMS
- Les dangers spécifiques du Web 2.0

3 / Technologies liées à la sécurité

- Firewalls, panorama des outils, techniques de base réseaux
- Filtres des requêtes HTTP
- Empreinte de message, les algorithmes SHA-x et MD5
- Signature numérique, Clé publique, clé privée, Coffre à clé et coffre de confiance, Autorités de certification
- Chiffrement de données, les algorithmes AES et RSA
- Protocoles SSL v2/v3 et TLS, PKI, certificats X509

Innov Systems

- Techniques d'authentification HTTP, authentification par certificat

4 / Sécuriser les applications Web

- Protections basiques : Re-post des données, Time-out et déconnexion, Masquer les URL, Validation des données
- Usurpation d'identité : Cookies et certificats numériques, Session ID et jeton de transaction, Détournement
- Se protéger des attaques client :
- XSS ou Cross Site Scripting
- Utilisation des références directes
- CSRF ou Cross Site Request Forgery
- Sécurité d'accès au SGBD
- SQL Injection
- Utilisation du JavaScript
- Échappement des tags HTML
- Protections contre les attaques de Brute-force, Liste de contrôle d'accès

5 / Principe du développement sécurisé

- Les écueils
- La sécurité dans le cycle de développement
- Application à AGILE/SCRUM
- Le budget
- Le rôle du code côté client
- Le contrôle des données envoyées par le client
- Les règles de développement à respecter

6 / Contrôler la sécurité des applications Web

- Test d'intrusion, audit de sécurité, scanners de vulnérabilités
- Organiser une veille technologique efficace
- Déclaration des incidents de sécurité

Innov Systems

7 / Gestion de la sécurité mobile

- Composants d’un système d’exploitation mobile
- Risques auxquels sont exposés les appareils mobiles
- Les principales menaces pesant sur les appareils mobiles
- Étudier les outils de piratage des appareils mobiles
- Méthode pour sécuriser les environnements mobiles

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

05 au 08 Jan. 2027	Présentiel - Casablanca
02 au 05 Mars 2027	Présentiel - Casablanca
27 au 30 Avr. 2027	Présentiel - Casablanca
22 au 25 Juin 2027	Présentiel - Casablanca
24 au 27 Août 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