PROGRAMME DE FORMATION EN SÉCURITÉ D'APPLICATION WEB et MOBILE

Description

La formation en Sécurité d'Application Web et Mobile est conçue pour offrir une compréhension approfondie des menaces et des vulnérabilités spécifiques aux applications web et mobiles. Elle vise à former des professionnels capables de protéger efficacement les applications contre les cyberattaques. Cette formation commence par une introduction aux principes fondamentaux de la sécurité informatique, couvrant les concepts de base tels que la confidentialité, l'intégrité et la disponibilité des données. Elle explore ensuite les spécificités de la sécurité des applications web et mobiles, en se concentrant sur les vulnérabilités courantes comme les injections SQL, le cross-site scripting (XSS), le cross-site request forgery (CSRF), et les failles de sécurisation des API.

Objectif

Les participants apprendront à identifier et à analyser ces vulnérabilités à l'aide de méthodologies éprouvées telles que les tests de pénétration et les audits de sécurité. La formation inclut des sessions pratiques où les participants mettront en œuvre des outils de sécurité tels que OWASP ZAP, Burp Suite et d'autres scanners de vulnérabilités pour tester et sécuriser des applications.

Objectifs spécifiques

De façon spécifique

- En plus de la détection et de la correction des failles, la formation couvre également les meilleures pratiques de développement sécurisé, en intégrant la sécurité dans le cycle de vie du développement logiciel (SDLC). Cela comprend la rédaction de code sécurisé, la gestion des dépendances tierces, et l'implémentation de mécanismes d'authentification et de cryptographie robustes.
- Un aspect crucial de la formation est la compréhension des standards et des réglementations de sécurité, tels que OWASP Top Ten, GDPR, et PCI-DSS, pour s'assurer que les applications sont conformes aux exigences légales et normatives. À la fin de la formation, les participants auront acquis les compétences nécessaires pour évaluer et améliorer la sécurité des applications web et mobiles, en appliquant une approche proactive et systématique pour prévenir les cybermenaces.

Débouchés

1. Analyste en Sécurité des Applications
2. Ingénieur en Sécurité Logicielle
3. Consultant en Sécurité Informatique
4. Architecte de Sécurité des Applications
5. Responsable de la Sécurité des Systèmes d'Information (RSSI)

Prérequis

Connaissances de Base en Programmation : Les participants doivent avoir une bonne compréhension des langages de programmation couramment utilisés pour le développement web et mobile, tels que HTML, CSS, JavaScript, ainsi que des langages côté serveur comme PHP, Python, Java, ou Node.js. Une expérience pratique en écriture de code est essentielle pour comprendre et corriger les vulnérabilités.

Public cible

Développeurs de Logiciels et d'Applications
Ingénieurs en Sécurité Informatique
Architectes Logiciels
Testeurs et Analystes QA (Assurance Qualité)
Administrateurs Systèmes et Réseaux
Chefs de Projet
Responsables de la Conformité et de la Réglementation
Étudiants en Informatique
Étudiants en sciences
Professionnel IT

Formateurs :

- **Dr ASSOGBA Emery** (+229 69292907)
- **Ing. KASSA Célia**
- **Ing. ODJO Abousidikou**

Méthode de formation : Cours magistraux, TP, TD, étude de cas

Mode d'évaluation : QCM

Critère de validation du certificat : 70% de taux de bonne réponse sur l'ensemble des questions

Nombre total d'heures : 35h

Intitulé	Contenu	Masse horaire
Introduction et Fondamentaux de la Sécurité	Introduction à la Sécurité des Applications Importance de la sécurité des applications web et mobiles Principes de base : confidentialité, intégrité, disponibilité Menaces et Vulnérabilités Types de menaces : injections SQL, XSS, CSRF Vulnérabilités spécifiques aux applications mobiles Cycle de Vie du Développement Sécurisé Intégration de la sécurité dans le SDLC Modèles de menace et analyse des risques	07H
Sécurité des Applications Web	Sécurité des Applications Web - Partie 1 Injections SQL et méthodes de prévention Vulnérabilités liées à l'authentification et à la gestion des sessions Sécurité des Applications Web - Partie 2 Cross-Site Scripting (XSS) : types, impacts, et mesures de protection Cross-Site Request Forgery (CSRF) : détection et prévention	07H
Sécurité des Applications Mobiles	Sécurité des Applications Mobiles - Partie 1 Architecture de sécurité des applications mobiles Gestion des permissions et des autorisations Sécurité des Applications Mobiles - Partie 2 Sécurisation des API pour les applications mobiles Techniques de protection des données locales et de chiffrement	07H
Outils et Techniques de Sécurité	Outils de Sécurité pour Applications Web Introduction à OWASP ZAP et Burp Suite Utilisation des scanners de vulnérabilités Outils de Sécurité pour Applications Mobiles Introduction à MobSF et autres outils de sécurité mobile Analyse de sécurité des applications mobiles avec des outils spécifiques	07H

Conformité, Meilleures Pratiques et Évaluation	Conformité et Réglementations Introduction à OWASP Top Ten, GDPR, PCI-DSS Mise en conformité des applications Meilleures Pratiques et Stratégies de Sécurité Bonnes pratiques de développement sécurisé Stratégies de défense en profondeur Résumé et Évaluation Finale Révision des concepts clés Examen final et certification Conclusion et Suivi Séance de Questions/Réponses et Feedback Réponses aux questions des participants Discussion sur les cas pratiques et les expériences des participants	07H

Références bibliographiques

1- Sécurité informatique: principes et méthode Laurent Bloch, Christophe Wolfhugel, Christian Queinnec, Nat Makarévitch, Hervé Schauer, Éditeur Eyrolles, 2009, ISBN 2212125259, 9782212125252, 292 pages

2- The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, Jason Andress Éditeur Elsevier, 2011 ISBN 1597496545, 9781597496544 208 pages