EduGroupe
Accompagner pour réussir

Sécurité des applications et des services

Référence : **SECAPP** Durée : **6 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Posséder une bonne connaissance de la programmation objet et de la programmation d'application Web.

PROFIL DES STAGIAIRES

• Analystes. • Architectes. • Chefs de projets. • Développeurs.

OBJECTIFS

• Comprendre les problématiques de sécurité des applications. • Connaitre les principales menaces et vulnérabilité. • Appréhender les méthodologies / technologies de protection et de contrôle de la sécurité des applications. • Mettre en place une stratégie de veille.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité défensive

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Introduction à la sécurité informatique

- Le contexte de la sécurité
- Risques encourus et impacts

Principales attaques sur les applications web

- Vulnérabilités techniques (Injection SQL, Cross-Site Scripting, Inclusion de fichier, etc.)
- Vulnérabilités logiques et spécifiques (Conditions de course, Timing Attacks, etc.)
- Contre-mesures et recommandations

Principales attaques sur les applications

- Débordement de tampon
- Problèmes de permissions
- Chiffrement des communications
- Contre-mesures et recommandations

Outils d'analyses

- Analyseurs statiques et dynamiques
- Techniques de 'fuzzing'

Sécuriser les données stockées en base

- Authentification et Autorisation du SGBDr (Système de Gestion de Base de Données relationnelle)
- Rôles serveur et rôles de base de données
- Propriété et séparation utilisateur-schéma
- Chiffrement de données dans la base de données

Sécuriser le système de fichiers

- Crypter les données sensibles dans les fichiers de configuration
- Détecter les tentatives de remplacement des fichiers sources de l'application
- Signer les fichiers

- Protéger les informations des fichiers de log

Sécuriser les échanges de données

- Modèle de chiffrement
- Conception orientée flux
- Configuration du chiffrement
- Choix d'un algorithme
- Mettre en œuvre le chiffrage symétrique
- Mettre en œuvre le chiffrage asymétrique

Mettre en place une veille