

Sécurité des applications

3 j (21 heures)

Ref : SECW

Public

Architectes, développeurs, analystes, chefs de projets...

Pré-requis

Niveau : Posséder une bonne connaissance de la programmation objet et de la programmation d'application Web

Techniques (formations en classe virtuelle) : Vous devez disposer d'un ordinateur connecté à internet, d'un micro et d'une caméra

Moyens pédagogiques

Modalité : Formation présentielle ou Formation distancielle (classe virtuelle) - Inter / Intra - Groupes de 4 à 12 stagiaires

Méthodes : Présentation des concepts, discussion technique, démonstrations, exercices et TP

Matériel :

Présentiel : Un poste informatique par stagiaire connecté à internet, à une imprimante en réseau et au réseau informatique,

Les salles sont équipées d'un tableau interactif ou d'un vidéoprojecteur et d'un paperboard

Distanciel : Aelion met à disposition de chaque stagiaire

Un PC équipé des outils et logiciels nécessaires à la formation auquel vous accédez via un outil de prise en main à distance

Un accès à un outil de classe virtuelle (Meet)

Support de formation : Un support de formation sera remis à chaque stagiaire en fin de formation : plateforme collaborative intégrant le code source des exercices réalisés en formation, webographie, mémos

Modalités de suivi et d'évaluation

Questionnaire d'évaluation des pré-requis, suivi des connaissances tout au long de la formation, Evaluation des acquis en fin de formation

Questionnaire d'évaluation de la satisfaction en fin de stage, feuille de présence émargée par demi-journée par les stagiaires et le formateur, Attestation de fin de formation

Les applications web sont devenues omniprésentes dans notre environnement. Si elles offrent l'avantage d'être accessibles à l'aide d'un simple navigateur partout et par tous, elles sont particulièrement exposées aux personnes malveillantes. Les effets d'attaques peuvent être catastrophiques pour les sociétés attaquées. La sécurité des applications devient donc un enjeu stratégique dans la conception de nouvelles applications. Cette formation permettra aux développeurs d'intégrer cette dimension dans le cadre de leurs projets à tous les niveaux. A l'issue de la formation, vous serez capable de mettre en œuvre les règles et bonnes pratiques liées au développement sécurisé d'applications.

Action collective OPCO ATLAS - [Inscription CampusAtlas](#)

Objectifs

Identifier les problématiques de sécurité des applications

Définir les principales menaces et vulnérabilité

Identifier les bonnes pratiques permettant de limiter les attaques ou la portée des attaques

Appréhender les technologies de protection et de contrôle de la sécurité des applications

Mettre en place une stratégie de veille

Programme détaillé

IDENTIFIER LES PROBLEMATIQUES DE SECURITE DES APPLICATIONS

Introduction à la sécurité des applications WEB

Positionnement de la sécurité dans le processus de développement

Authentification, identification, habilitation

Sécurité du point de vue du client

Sécurité du point de vue du serveur

Sécurité des supports (https, ssl, analyseur logiciel)

Sécurité des conteneurs et serveurs

Tests d'intrusion : pourquoi ce n'est pas suffisant

CONNAITRE LES PRINCIPALES MENACES ET VULNERABILITE

Classification des attaques selon les référentiels STRIDE et OWASP

Les principales attaques et leur portée :

- Sécurité des supports de communication
- Attaque type « man in the middle »
- Sniffing, Spoofing et packet forging
- Utilité du SSL et du HTTPS
- White et Black listing, monitoring pré-emptif

Déni de service

- Principe de l'attaque DDOS
- Risques sous-jacents et limitations
- Stratégie de déploiement / failover / load-balancing

Exécution malicieuse

- Objectif de l'attaquant
- Attaque type « injection SQL »
- Attaque type « débordement de tampon »
- Risques sous-jacents et limitations
- Les bonnes pratiques pour s'en protéger

Corruption et extorsion de données

- Objectif de l'attaquant
- Attaque type « Hijacking de session »
- Risques sous-jacents et limitations
- Stratégie sans session, OAuth et Oauth 2

IDENTIFIER LES BONNES PRATIQUES PERMETTANT DE LIMITER LES ATTAQUES OU LA PORTEE DES ATTAQUES (1/2)

Sécuriser les communications
Assurances et certificats
Certificat HTTPS avec Let's encrypt
Pare-feu serveur
Pare-feu "proxy" : solutions de Web Application Firewall (WAF)

IDENTIFIER LES BONNES PRATIQUES PERMETTANT DE LIMITER LES ATTAQUES OU LA PORTEE DES ATTAQUES (2/2)

Cryptanalyse et chiffrement
Bonnes pratiques pour le stockage de données sensibles
Du choix du protocole de chiffrement pour les mots de passe

APPREHENDER LES METHODOLOGIES / TECHNOLOGIES DE PROTECTION ET DE CONTROLE DE LA SECURITE DES APPLICATIONS

Introduction à la démarche DEVSECOPS
Outils de sécurité et d'audit
Outils de développement et de test liés à la sécurité
Outils pour mener les tests de sécurité
Audit de code et des dépendances

METTRE EN PLACE UNE STRATEGIE DE VEILLE

Identification des risques
Définition des priorités et planification des actions
Outils et canaux de veille
