
Programme de Formation

Sécurité des applications : Identifier les menaces et appliquer les bonnes pratiques

Description

Formation pratique pour maîtriser la sécurité des applications : identifier les vulnérabilités, comprendre les menaces et appliquer les bonnes pratiques tout au long du cycle de développement.

Points Forts

Approche concrète mêlant théorie, démonstrations et exercices pratiques pour comprendre les vulnérabilités applicatives, appliquer des protections, intégrer des outils de sécurité et anticiper les attaques courantes.



Public visé

- Développeurs
- Architectes logiciels et applications
- Chefs de projet IT



Objectifs pédagogiques

- Comprendre les problématiques de sécurité des applications
- Identifier les principales menaces et vulnérabilités affectation les applications web et mobiles
- Appliquer les bonnes pratiques de sécurité dans le développement d'applications
- Utiliser des outils et techniques pour détecter et corriger les failles de sécurité
- Découvrir les principes de base de la cybersécurité et leur impact sur la sécurité des applications

Organisation

Durée : 21 heures

Mode d'organisation : Mixte

Contenu pédagogique



Description

Jour 1 : Introduction aux menaces et vulnérabilités

Comprendre les problématiques de sécurité 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
- Exemple de travaux pratiques : le formateur interroge les participants concernant les concepts ou problématiques présentés.

Identifier les principales menaces et vulnérabilités affectation les applications web et mobiles



- 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 « command execution »
 - 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
- Exemples de travaux pratiques :
 - Mise en place d'un atelier de pentesting avec des machines et applications vulnérables pour jouer certaines failles de sécurité.
 - Les participants répondent à une série de questions (par exemple via un formulaire en ligne) pour valider la compréhension des définitions abordées. Le formateur peut faire une correction commune en interrogeant les participants.

Jour 2 : Bonnes pratiques et sécurisation des applications

Appliquer les bonnes pratiques de sécurité dans le développement d'applications (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)
- Exemple de travaux pratiques : le formateur crée un certificat SSL pour sécuriser les communications HTTP d'une application web. Les participants reproduisent la démarche.

Appliquer les bonnes pratiques de sécurité dans le développement d'applications (2/2)

- Cryptanalyse et chiffrement
- Bonnes pratiques pour le stockage de données sensibles
- Du choix du protocole de chiffrement pour les mots de passe
- Exemples de travaux pratiques : le formateur crée un certificat SSL pour sécuriser les communications HTTP d'une application web. Les participants reproduisent la démarche.

Jour 3 : Protection et veille

Utiliser des outils et techniques pour détecter et corriger les failles de sécurité

- 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

- Exemples de travaux pratiques : le formateur réalise un audit de sécurité sur un code source et ses dépendances. Les participants reproduisent les opérations sur leur poste de travail.

Découvrir les principes de base de la cybersécurité et leur impact sur la sécurité des applications

A l'issue de cette séquence, vous êtes capable de mettre en place et utiliser des outils et démarches nécessaires pour la veille sécurité.

- La veille sécurité ou risk intelligence
- Identification des risques
- Définition des priorités et planification des actions
- Outils et canaux de veille
- Exemples de travaux pratiques : les participants réalisent un classement des risques et identifie les actions à mener.

Prérequis

- Posséder une bonne connaissance de la programmation objet et de la programmation d'application Web
- Un questionnaire de positionnement sera réalisé au préalable pour adapter la formation à vos besoins

Modalités pédagogiques

- Exercices concrets
- Cas pratiques
- Quiz d'évaluation des connaissances

Moyens et supports pédagogiques

- Mise à disposition de postes de travail
- Vidéoprojecteur, tableau blanc, supports numériques
- Documentation pédagogique numérique

Modalités d'évaluation et de suivi

- Positionnement en amont de la formation :
 - Un quiz de consolidation des pré-requis sera administré en amont de la formation
- Suivi « pendant » :
 - Feuilles de présence
 - Exercices pratiques
 - Évaluation « fin de formation »
 - Évaluation des acquis en fin de formation
 - Formulaires d'évaluation de la formation
- Évaluation à froid :
 - Suivi post-formation : Questionnaire de satisfaction à j+30