Qualité et sécurité des applications : sécuriser une application

Mise à jour nov. 2020

Durée 3 jours(21 heures)

OBJECTIFS PÉDAGOGIQUES

- Connaitre les différents types d'attaques (attaques par injection SQL, attaques XSS, attaques CSRF, attaques brute force, ...) et les moyens à mettre en œuvre pour s'en prémunir

PARTICIPANTS / PRÉREQUIS

- Cette formation s'adresse aux développeurs souhaitant connaître les différentes techniques de sécurisation d'une application
- Pour suivre ce stage, il est nécessaire d'avoir une bonne connaissance de la programmation orientée objet et de la programmation d'applications Web

MOYENS PÉDAGOGIQUES

- Réflexion de groupe et apports théoriques du formateur
- Travail d'échange avec les participants sous forme de réunion-discussion
- Utilisation de cas concrets issus de l'expérience professionnelle
- Validation des acquis par des questionnaires, des tests d'évaluation, des mises en situation et des jeux pédagogiques
- Alternance entre apports théoriques et exercices pratiques (en moyenne 30 à 50%)
- Remise d'un support de cours

MODALITÉS D'ÉVALUATION

- Feuille de présence signée en demi-journée
- Evaluation des acquis tout au long de la formation
- Questionnaire de satisfaction
- Attestation de stage à chaque apprenant
- Positionnement préalable oral ou écrit
- Evaluation formative tout au long de la formation
- Evaluation sommative faite par le formateur ou à l'aide des certifications disponibles

MOYENS TECHNIQUES EN PRÉSENTIEL

- Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs, d'un vidéo projecteur d'un tableau blanc et de paperboard

MOYENS TECHNIQUES DES CLASSES À DISTANCE

- A l'aide d'un logiciel comme Teams, Zoom etc. un micro et éventuellement une caméra pour l'apprenant, suivez une formation en temps réel et entièrement à distance
- Lors de la classe en ligne, les apprenants interagissent et communiquent entre eux et avec le formateur
- Les formations en distanciel sont organisées en Inter-Entreprises comme en Intra-Entreprise
- L'accès à l'environnement d'apprentissage (support de cours, labs) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré
- Les participants recevront une invitation avec un lien de connexion. Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition auprès de notre équipe par téléphone au 03 25 80 08 64 ou par mail à secretariat@feep-entreprises.fr

ORGANISATION

- Les cours ont lieu de 9h à 12h30 et de 13h30 à 17h

PROFIL FORMATEUR

- Nos formateurs sont des experts dans leurs domaines d'intervention
- Leur expérience de terrain et leurs qualités pédagogiques constituent un gage de qualité

ACCESSIBILITÉ

- Les personnes atteintes de handicap souhaitant suivre cette formation sont invitées à nous contacter directement, afin d'étudier ensemble les possibilités de suivre la formation

Programme de formation

Concepts de sécurité logicielle

- Pourquoi sécuriser une application
- Identifier et comprendre les vulnérabilités de vos applications Attaques « brute-force »
- Attaques par « déni de services » (DOS - Denial Of Service)
- Attaques par analyse de trames IP
- Attaques par « Injection SQL »
- Attaques « XSS » (Cross site scripting)
- Attaques « CSRF » (Cross site request forgery)
- Autres types d'attaques
- Outils de détection de faille de sécurité
- Travaux pratiques : tests de ces différents types de problèmes sur une application mal développée et utilisation des outils de détection de faille de sécurité

Validation des données entrantes

- Protection contre les entrées d'utilisateurs nuisibles
- Utilisation d'expressions régulières
- Détecter et contrer les « injections SQL »
- Détecter et contrer les attaques « XSS »
- Détecter et contrer les attaques « CSRF »
- Détecter et contrer les attaques « bruteforce »
- Sécuriser les données en Cookie
- Protection contre les menaces de déni de service
- Ne pas présenter à l'utilisateur les détails des erreurs techniques
- Travaux pratiques : modification du code de l'application initialement proposée pour interdire ces différents types d'attaques

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
- Travaux pratiques : stocker de manière sécurisée les mots de passe en base de données

Sécuriser le système de fichier

- 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

Oauth 2.0 et l'authentification au niveau du navigateur

- Présentation de l'architecture Oauth 2.0
- Utilisation de l'API Oauth 2.0
- Travaux pratiques : mise en œuvre de Oauth

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
- Travaux pratiques : réaliser une communication sécurisée à l'aide d'un certificat