Qualité et sécurité des applications : sécuriser une application

Informatique

Développement Back-End

Référence : 4-JA-SEA
Durée : 3 jours
Présentiel ou en classe à distance

Tarif Inter : 750 € Prix HT jour / personne
Tarif Intra : 1400 € Prix HT jour / groupe

Mise à jour : 27/11/2023

Durée de validité : du 01/01/2026 au 31/12/2026

Objectifs

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

Prérequis

Aucun prérequis obligatoire

Niveau recommandé

Pour suivre ce stage, il est nécessaire d'avoir une bonne connaissance de la programmation orientée objet et de la programmation d'applications Web

Public concerné

Cette formation s'adresse aux développeurs souhaitant connaître les différentes techniques de sécurisation d'une application

Contenu pédagogique

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

---

Moyens pédagogiques

- Réflexion de groupe et apports théoriques du formateur.
- Travail d'échange avec les apprenants 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 sur 30 à 50% du temps)

Modalités pédagogiques : Présentiel, Distanciel et AFEST

Moyens techniques

En formation présentielle

Accueil des apprenants dans une salle dédiée à la formation et équipée avec :

- Ordinateurs
- Vidéo projecteur ou Écran TV interactif
- Tableau blanc ou Paper-Board

En formation distancielle

A l'aide d'un logiciel comme ® Microsoft Teams ou Zoom, un micro et une caméra pour l'apprenant.

- Suivez une formation en temps réel et entièrement à distance. Lors de la session en ligne, les apprenants interagissent et communiquent entre eux et avec le formateur.
- Les formations en distanciel sont organisées en Inter-Entreprise comme en Intra-Entreprise.
- L'accès à l'environnement d'apprentissage (support de cours, ressources formateur, fichiers d'exercices ...) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré.
- Les participants recevront une convocation avec le lien de connexion à la session de formation.
- Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition par téléphone au 02 35 12 25 55 ou par email à commercial@xxlformation.com

Modalités d'évaluation

- Positionnement préalable oral ou écrit.
- 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
- Evaluation formative tout au long de la formation.
- Evaluation sommative faite par le formateur.

Profil du formateur

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

Adaptation pédagogique et matérielle

Si vous avez besoin d'adaptation matérielle ou pédagogique, merci de prendre contact avec notre référent Handicap par téléphone au 02 35 12 25 55 ou par email à handicap@xxlformation.com

Modalités et délais d'accès à la formation

Les formations sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.
Les conditions d'accès à la formation dans le cadre du CPF sont celles implicitement présentées dans les CGU disponibles sur le site Mon Compte Formation en vigueur à date d'inscription.
Voir CG_MCF_V16_VF.pdf Article 5.1.

Nos sessions INTER 2026

Sessions de formation à venir :

- Aucune session à venir pour cette formation.

Nos sessions INTRA 2026

Pour organiser cette formation en intra-entreprise, veuillez nous contacter par mail à commercial@xxlformation.com ou par téléphone au 02 35 12 25 55