Développements sécurisés

Mise à jour : Fév. 2024

Durée : 1 jour - 7 heures

OBJECTIFS PÉDAGOGIQUES

- Cette formation est une introduction aux techniques de développement sécurisé
- Elle comprend une introduction aux principes de sécurité ainsi que des cas pratiques illustrant vulnérabilités et solutions techniques à mettre en place pour s'en prémunir
- Ce stage présente un grand nombre de principes permettant d'améliorer la sécurité des développements en se basant sur les « Secure Coding Guidelines » de l'OWASP
- Il permet de comprendre ce qu'est un système vulnérable, les différents concepts, les différentes menaces et la manière de s'en prémunir
- La formation "Développement sécurisé" permet de connaître les bonnes pratiques de développement et de produire du code sécurisé
- Elle apporte une illustration de vulnérabilité et indique les solutions techniques à mettre en place en fonction du langage de programmation ciblé

PRÉREQUIS

- Connaissance des langages Java et HTML/CSS

PARTICIPANTS

- Développeurs, concepteurs, ingénieurs d'études

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
- 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 reçoivent 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. Notre organisme peut vous offrir des possibilités d'adaptation et/ou de compensations spécifiques si elles sont nécessaires à l'amélioration de vos apprentissages

Programme de formation

Sécurité et développement : Introduction

- Qu'est-ce que la sécurité informatique.
- Quelques définitions (faille, menace …)
- La sécurité un état d'esprit
- Qu'est ce que l'OWASP ?

Principes du développement sécurisé

- Minimiser la surface d'attaque
- Réglages sécurisés par défaut
- Principe du moindre privilège
- Principe de la Défense en profondeur
- Échouer en toute sécurité (Fail Securely)
- Séparation des fonctions
- Recommandations de l'OWASP

Bonnes pratiques du développement sécurisé

- Input Validation
- Output Encoding
- Authentication Management
- Session Management
- Access Control
- Cryptographic Practices
- Error Handling and Logging
- Data Protection
- Communication Security
- System Configuration
- Database Security
- File Management
- Memory Management
- General Coding Practices

Le contrôle au quotidien

- Mon application est-elle fiable ?
- Mon code est-il robuste ?
- Les dépendances sont-elles sécurisées ?