11 juil.
14 nov.

Nantes / Rennes : 580 € HT
Brest / Le Mans : 580 € HT
Certification : NON

Développements sécurisés

Mise à jour nov. 2023

Durée 1 jour (7 heures)

« Délai d'accès maximum 1 mois »

Prévention / Sécurité

OBJECTIFS PROFESSIONNELS

- 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

PARTICIPANTS

- Développeurs, concepteurs, ingénieurs d'études

PRE-REQUIS

- Connaissance des langages Java et HTML/CSS

MOYENS PEDAGOGIQUES

- Réflexion de groupe et apports théoriques du formateur
- Travail d'échange avec les participants sous forme de
- 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.

MODALITES D'EVALUATION

- Feuille de présence signée en demi-journée,
- Evaluation des acquis tout au long de la formation,
- Questionnaire de satisfaction,
- 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,
- Sanction finale : Certificat de réalisation, certification éligible au RS selon l'obtention du résultat par le stagiaire

MOYENS TECHNIQUES EN PRESENTIEL

- Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs, d'un vidéo projecteur d'un tableau blanc et de paperboard. Nous préconisons 8 personnes maximum par action de formation en présentiel

MOYENS TECHNIQUES DES CLASSES EN CAS DE FORMATION DISTANCIELLE

- A l'aide d'un logiciel comme Teams, Zoom etc... un micro et éventuellement une caméra pour l'apprenant,
- suivez une formation uniquement synchrone en temps réel et entièrement à distance. Lors de la classe en ligne, les apprenants interagissent et comuniquent 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, labs) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré. Nous préconisons 4 personnes maximum par action de formation en classe à distance

ORGANISATION

- Les cours ont lieu de 9h à 12h30 et de 14h à 17h30.

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.

A L'ATTENTION DES PERSONNES EN SITUATION DE HANDICAP

- 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

Sécurité et développement : Introduction (01h00)

- 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 (01h45)

- 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 (03h15)

- 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 (00h45)

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