Qualité et sécurité des applications : sécuriser une application

Informatique

Référence formation : 4-JA-SEA - **Durée : 3 jours**

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

Pré-requis

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

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 »

XXL Formation
34 rue Raymond Aron
76130 Mont Saint Aignan
Tél : 02 35 12 25 55 – **Fax :** 02 35 12 25 56
N° siret : 485 050 611 00014 – N° d'agrément : 23.76.03752.76

- 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

Méthodes pédagogiques	Présentation des concepts, démonstration, exécution, synthèse et exercices pratiques d'assimilation
Modalités pédagogiques	Présentiel - Distanciel - AFEST

Moyens pédagogiques	Formateur expert du domaine - 1 ordinateur, 1 support de cours version papier ou numérique, un bloc-note et un stylo par personne - vidéo projecteur - tableau blanc
Modalités d'évaluation	Positionnement préalable oral ou écrit - Evaluation formative tout au long de la formation - Evaluation sommative faite par le formateur ou à l'aide de la certification **NULL** : https://www.francecompetences.fr/recherche/NULL
Durée journée de formation	7h00
Public concerné	Salariés - Demandeur d'emploi - Reconversion professionnelle - Public en situation de handicap

XXL Formation
34 rue Raymond Aron
76130 Mont Saint Aignan
Tél : 02 35 12 25 55 – **Fax :** 02 35 12 25 56
N° siret : 485 050 611 00014 – N° d'agrément : 23.76.03752.76