3A/3B/3C - Qualité et sécurité des applications : Sécuriser une application

Plan de cours N° : 1075

Durée : 3 jours (21h)

Participants

Développeur souhaitant connaître les différentes techniques de sécurisation d'une application.

Pré-Requis

Avoir une bonne connaissance de la programmation orientée objet et de la programmation d'applications Web.

Objectifs

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

Méthode pédagogique

Alternance entre apports théoriques (40%) et exercices pratiques (60%)

Support de cours fourni lors de la formation

Moyens d'encadrement mis en oeuvre

1 à 8 personnes maximum par session
1 poste informatique par personne
Une assistance post-formation, d'une durée d'un an, sur le contenu de la formation

Moyens permettant de suivre son exécution et d'en apprécier les résultats

Emargement par demi-journée
Evaluation des acquis par mise en situation de travail
Evaluation qualitative de fin de stage
Remise d'une attestation individuelle de formation en fin de stage

Assistance

formateurs@atp-formation.com

Concepts de sécurité logicielle

- Outils de détection de faille de sécurité
- 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
- Pourquoi sécuriser une application ?
- 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 "brute-force"
- 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 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 oeuvre de Oauth

Sécuriser les échanges de données

- Modèle de chiffrement
- Conception orientée flux
- Configuration du chiffrement
- Choix d'un algorithme
- Mettre en oeuvre le chiffrage symétrique
- Mettre en oeuvre le chiffrage asymétrique
- Travaux pratiques
  Réaliser une communication sécurisée à l'aide d'un certificat

31, av. du Granier
38240 Meylan
Tél. 04 76 41 14 20
Fax 04 76 41 38 45
contact@atp-formation.com

SAS au Capital de 40.000€ - 390 032 050 RCS GRENOBLE
SIRET 390 032 050 00010 - APE 8559A - TVA Intracom. FR03390032050