JAVA

Sécuriser une application Java

Plan de cours N° : 1075

Durée : 3 jours (21h)

PARTICIPANTS / PRE-REQUIS

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

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

OBJECTIFS PEDAGOGIQUES

Déterminer les concepts de sécurité logicielle et les différentes types d'attaques. Employer les API Java en lien avec la sécurité. Apprécier la validation des données entrantes pour protéger contre les attaques courantes. Pratiquer la sécurisation des données stockées dans les bases de données. Protéger les fichiers de configuration et les fichiers de log du système. Implémenter l'architecture Oauth 2.0 pour l'authentification au niveau du navigateur. Mettre en œuvre des techniques de chiffrement pour sécuriser les échanges de données entre les parties.

MOYENS PEDAGOGIQUES

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 exercices de synthèse
Alternance entre apports théoriques et exercices pratiques (en moyenne 30 et 70%)
Remise d'un support de cours.
Assistance post-formation d'une durée de 1 an sur le contenu de la formation via notre adresse mail dédiée formateurs@atp-formation.com

MOYENS PERMETTANT LE SUIVI DE L'EXECUTION ET DES RESULTATS

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 PRESENTIEL

Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs, d'un vidéo projecteur d'un tableau blanc.

MOYENS TECHNIQUES DES CLASSES A 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-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.
Les participants recevront une convocation avec lien de connexion
Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition par mail et par téléphone auprès de notre équipe par téléphone au 04.76.41.14.20 ou par mail à contact@atp-formation.com

ORGANISATION

Les cours ont lieu de 9h00-12h30 13h30-17h00.

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.

ACCESSIBILITE

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.

MISE A JOUR

08/01/2023

31, av. du Granier
38240 Meylan
Tél. 04 76 41 14 20
Fax 04 76 41 38 45

SARL au capital de 120 000€ - 390 032 050 RCS GRENOBLE
SIRET 390 032 050 00010 - APE 8559A - TVA Intracom. FR03390032050

JAVA

Sécuriser une application Java

Plan de cours N° : 1075

Durée : 3 jours (21h)

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 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 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

SARL au capital de 120 000€ - 390 032 050 RCS GRENOBLE
SIRET 390 032 050 00010 - APE 8559A - TVA Intracom. FR03390032050