Sécurité des applications Java/J2EE

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Domaine : Cybersécurité - sécurité informatique

Filière : Fondamentaux de la cybersécurité

Rubrique : Fondamentaux

Éligible au CPF : Non

Action collective : Non

PRÉSENTATION

Objectifs & compétences

Mettre en œuvre la sécurité au niveau de la machine virtuelle Java
Exploiter des API spécifiques telles que JAAS, JSSE et JCE pour sécuriser vos applications.
Sécuriser vos services Web avec les API WS-Security et oAuth

Public visé

Développeurs et chefs de projets amenés à sécuriser des applications Java et JEE.

Pré-requis

Très bonnes connaissances du langage Java. Bonnes connaissances des concepts JEE.
Expérience requise en programmation Java.

PROGRAMME

Présentation des concepts liés à la sécurité
Identification et méthodes d'authentification.
Autorisations et permissions.
Confidentialité, non-répudiation, cryptage, clés publiques/privées, autorités de certification.
Pare-feu et DMZ, rupture de protocole.
Les types d'attaques.

Sécurité de la machine virtuelle Java
Chargement des classes. Concept de "bac à sable".
SecurityManager, AccessController et définition des permissions (fichiers .policy).
Créer ses permissions avec Java Security Permission.
Mécanismes de protection de l'intégrité du bytecode, la décompilation et l'obfuscation du code.
Spécificités des Applets en matière de sécurité.

Travaux pratiques :
Définition de. policy spécifiques.

Java Authetification et Autorization Service
Architecture de JAAS.
Authentification via le PAM, notion de Subject et de Principal.
Gestion des permissions, les fichiers. policy.
Utiliser JAAS avec Unix ou Windows, JNDI, Kerberos et Keystore. Le support du SSO.

Travaux pratiques :
Configurer la politique de contrôle d'accès, mise en œuvre de l'authentification.

SSL avec Java
Fonctions de Java Secure Socket Extension (JSSE).
Authentification via certificats X.509. TLS et SSL.
Encryption à base de clés publiques, Java Cryptography Extension (JCE).
Utilisation de SSL avec http

Code de formation : JAS-EE

€ Tarifs

Prix public : 1870 €

Tarif & financement :
Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :
Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.
Le dispositif FNE-Formation.
L'OPCO (opérateurs de compétences) de votre entreprise.
France Travail: sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
CPF -MonCompteFormation
Contactez nous pour plus d'information : contact@aston-institut.com

Lieux & Horaires

Durée : 21 heures

Délai d'accès : Jusqu'a 8 jours avant le début de la formation, sous condition d'un dossier d'insciption complet

Prochaines sessions

Consultez-nous pour les prochaines sessions.

Travaux pratiques :
Configurer SSL et mise en œuvre de sockets SSL. Utiliser des outils du JDK (Keystore).

La sécurité d'une application JEE
Authentification au niveau des conteneurs Web et EJB.
Rôles applicatifs, permissions et descripteurs de déploiement XML.
Contrôles dynamiques via les API Servlets et EJB.
La sécurité dans les API : JDBC, JNDI, JTA, JMS, JCA.

Travaux pratiques :
Sécurité d'une application déployée dans Tomcat.

La sécurité des services Web SOAP
Sécurité au niveau HTTP.
Sécurité au niveau SOAP & WSDL avec WS-Security (WSS4J, XWSS...) & WS-Policy.
Les handlers SOAP WS-Security exploitant JAAS.

Travaux pratiques:
Mise en pratique avec une implémentation de WS-Security (XWSS)
La sécurité des services Web REST
Utilisation de SSL avec JAX-RS.
Les apports de oAuth (authentification sur Internet).
oAuth 1.0 et 2.0.

Travaux pratiques :
Mise en pratique avec une implémentation Apache CXF de JAX-RS

MODALITÉS

Modalités

Modalités : en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise.
Pédagogie : essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.
Ressources techniques et pédagogiques : Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom.
Pendant la formation : mises en situation, autodiagnostics, travail individuel ou en sous-groupe sur des cas réels.

Méthode

Fin de formation : entretien individuel.
Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation.
Assiduité : certificat de réalisation.
Validations des acquis : grille d'evalution des acquis établie par le formateur en fin de formation.