Formation Sécurité des applications Web Java EE

Identifier les risques et savoir choisir les solutions de sécurisation

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Avec le développement de services en ligne BtoB et BtoC (consultation d'historiques de consommation par exemple), les entreprises sont de plus en plus nombreuses à exposer des données sur la toile par le biais de serveurs Web. Si certaines de ces données ne revêtent pas une dimension stratégique, il apparait néanmoins indispensable d'en assurer la sécurité, ne serait-ce qu'au regard de la loi. Aussi, sécuriser une application web ainsi que les données auxquelles elle donne accès doit-il devenir un réflexe. Les participants à cette formation de 3 jours découvriront les techniques et bonnes pratiques pour assurer la sécurité des applications développées en Java et hébergées sur des serveurs Web, mais également la sécurité liée à la JVM et proche du coeur des systèmes.

Référence	OBJ394
Durée	3 jours (21h)
Tarif	1 950 €HT

Objectifs

| connaître les risques potentiels dans l'utilisation de Java
| identifier les parades à mettre en oeuvre, les moyens de sécuriser les applications JEE
| sécuriser les différents aspects techniques d'une application
| tester la sécurité des applications Java

Public

| Développeurs et analystes programmeurs anciennes technologies
| Chefs de projets

Prérequis

| Connaître les notions de base du langage Java est nécessaire pour suivre cette formation dans de bonnes conditions

Programme de la formation

Introduction
| Les risques
| Politique de sécurité
| Évaluation des risques en fonction des différents modes d'utilisation de Java (applets, application, servlets)

Sécurisation de la JVM
| Limites naturelles imposées par Java
| Gestion mémoire
| Contrôle du bytecode par la machine virtuelle

Protection de l'exécution
| Exécution protégée
| Security Manager, ClassLoader
| Surcharge des méthodes d'accès
| Lecture, écriture, exécution, ouverture de socket
| Autorisation de connexions...

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
du 7 au 9 juillet 2025
du 1er au 3 septembre 2025

PARIS
du 7 au 9 juillet 2025
du 1er au 3 septembre 2025

AIX-EN-PROVENCE
du 7 au 9 juillet 2025
du 1er au 3 septembre 2025

BORDEAUX
du 7 au 9 juillet 2025
du 1er au 3 septembre 2025

GRENOBLE
du 7 au 9 juillet 2025
du 1er au 3 septembre 2025

LILLE
du 7 au 9 juillet 2025
du 1er au 3 septembre 2025

LYON
du 7 au 9 juillet 2025
du 1er au 3 septembre 2025

NANTES
du 7 au 9 juillet 2025
du 1er au 3 septembre 2025

VOIR TOUTES LES DATES

Chiffrement
| Les mécanismes de signature
| Création de clés publiques et privées
| Les clés RSA, DSA
| Signature d'un document
| Les algorithmes SHA1withDSA, MD5withRSA
| Les MessageDigest
| Les algorithmes MD2, MD5, SHA-1, SHA-512

Certificats
| Cycle de vie d'un certificat
| La fabrique de certificats Java
| Les certificats de modification X509

Contrôle
| Rappel sur les ACL
| Le paquetage java.security.acl
| Ajout d'entrée, vérification d'accès

Obfuscation
| Principe
| Techniques d'obfuscation
| Solutions commerciales

JAAS et sécurité JEE
| Présentation
| Fonctionnement et mise en oeuvre
| Le service de sécurité
| Sécurité Web et EJB
| Autorisations EJB V3
| Accès applicatifs et lien avec un annuaire LDAP

Méthode pédagogique

Une vision objective des risques liés à Java. Un panorama détaillé des solutions en local (JVM) et en mode Web. La mise en oeuvre très technique et pratique des solutions à travers une série d'ateliers.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.

| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.