Sécurité des applications Java, .NET et PHP

Cours Pratique de 3 jours - 21h
Réf : ANP - Prix 2024 : 2 380€ HT

Cette formation très pratique, vous permettra d'appréhender les mécanismes de gestion de la sécurité proposés par Java, .NET et PHP. Vous verrez comment mettre en œuvre la sécurité au niveau de la machine virtuelle Java et maîtriser les mécanismes de sécurité des plateformes .NET et PHP.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Intégrer la sécurité dans les développements dès la conception

Identifier les failles possibles au niveau des développements

Développer des applications plus sécurisées

Mettre en œuvre la sécurité au niveau de la machine virtuelle Java

Maîtriser les mécanismes de sécurité de la plateforme .NET et PHP

LE PROGRAMME

dernière mise à jour : 10/2018

1) 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.

2) Java Authentication and Authorization 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.

3) Problématique de sécurité en .NET

- Définition de sécurité.
- Authentification, Protection, Cryptage.
- Outils de sécurité .NET.
- Sécurité d'exécution, authentification, protection des données et des accès.
- Types de menaces, validation des données saisies.

4) Sécurité du Framework .NET

- Protection du contenu des assembly.
- Protection de l'exécution des programmes.
- Déploiement d'une stratégie de sécurité du CLR.

PARTICIPANTS

Développeurs, architectes applicatifs, chefs de projets amenés à sécuriser des applications.

PRÉREQUIS

Avoir suivi la formation "Développer des applications sécurisées".

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Stratégie de sécurité et déploiement des applications. Principe d'utilisation des "preuves".
- Règles d'exécution selon la provenance des applications.
- Nouveautés de .NET4.
- Confiance totale/Partielle.

Travaux pratiques : Récupérer les preuves présentées par un assembly. Signer/modifier un assembly.

5) Sécurité du code .NET

- Code transparent de sécurité, critique de sécurité et critique sécurisée.
- Quelles sont les autorisations d'accès du code ?
- Comment procéder à l'obfuscation du code. Chiffrement des informations de configuration.
- Mettre en place la gestion déclarative/impérative des mécanismes de sécurité.
- Effectuer la restriction/vérification des droits de l'exécution du programme.
- Comment mettre en œuvre la gestion de la sécurité à partir des rôles.

Travaux pratiques : Autorisation d'accès du code.

6) Les bons réglages pour sécuriser PHP

- Le fichier de configuration PHP.ini. Identifier les directives sensibles, les sessions et les erreurs.
- Comment mettre en place une protection des scripts. Protection physique. Exécution de scripts distants ou à la volée.
- Les cookies et les sessions.

7) La sécurité des bases de données

- Quelles sont les failles potentielles qui peuvent impacter les bases de données. Administration. Stockage.
- Les attaques de type "Injections SQL". Principe et contre-mesure. Procédures stockées et requêtes paramétrées. Limites.
- Quels sont les fichiers d'accès. Organisation et valeurs par défaut. Accès anonymes et protocoles.

8) Sécuriser l'emploi des extensions en PHP

- Email. Spam via un formulaire de contact : injections et contre-mesures.
- Comment réaliser les accès réseau par PHP. Les appels séquentiels et récursifs. Les attaques furtives.

9) Les vulnérabilités des applications Web

- Pourquoi les applications Web sont-elles plus exposées ? Les risques majeurs des applications Web selon l'OWASP.
- Les attaques "Cross Site Scripting" ou XSS. Pourquoi sont-elles en pleine expansion ? Comment les éviter ?
- Les attaques en injection (commandes injection, SQL Injection, LDAP injection...). Les attaques sur les sessions.
- Exploitation de vulnérabilités sur le frontal HTTP (ver Nimda, faille Unicode). Attaques sur les configurations standard
- Comment effectuer la recherche des vulnérabilités.
- Rechercher les vulnérabilités les plus répandues. Le Cross-Site Scripting. L'injection SQL.
- Les erreurs de logique applicative. Le buffer overflow (débordement de tampon). L'exécution de commandes arbitraires.

10) Les bonnes pratiques

- Quels sont les différents types d'entrées ? Comment effectuer la validation des entrées ?
- Quels sont les types d'opérations qui peuvent être effectuées sur les types numériques ?
- Les classes et les exceptions.
- Multi-threading et synchronisation.
- Les entrées-sorties, la sérialisation.

- Savoir effectuer la gestion des permissions.

Travaux pratiques : Les exercices pratiques ont été conçus pour illustrer tous les éléments du langage et pour systématiquement mettre en œuvre les concepts afin de bien maîtriser les mécanismes de sécurité.

LES DATES

CLASSE À DISTANCE
2024 : 26 juin, 25 sept., 09 déc.

PARIS
2024 : 19 juin, 18 sept., 02 déc., 16 déc.