

Sécurité des applications

Présentation

A l'issue de la formation, le stagiaire sera capable de mettre en oeuvre les règles et bonnes pratiques liées au développement sécurisé d'applications.

Durée : 21,00 heures (3 jours)

Tarif INTRA : [Nous consulter](#)

Objectifs de la formation

- Comprendre les problématiques de sécurité des applications.
- Connaître les principales menaces et vulnérabilité.
- Appréhender les méthodologies / technologies de protection et de contrôle de la sécurité des applications.
- Mettre en place une stratégie de veille

Prérequis

- Posséder une bonne connaissance de la programmation objet et de la programmation d'application Web.

Public

- Architectes,
- Développeurs,
- Analystes,
- Chefs de projets...

Programme de la formation

1. Sécurité du code

- Concepts fondamentaux
- Sécurité d'accès du code et des ressources
- Sécurité basée sur les rôles
- Le principe du W^X
- Services de chiffrement



- Validation et contrôle des entrées / sorties
- Gestion et masquage d'erreurs
- Gestion sécurisée de la mémoire
- Contrôle d'authenticité et d'intégrité d'une application/d'un code
- Obfuscation du code
- Reverse engineering sur : bundle C#, application Java, binaire Windows
- Contrôle des droits avant exécution du code
- Sécuriser les données sensibles présentes dans un binaire
- Stack / Buffer / Heap overflow

2. Les bases de la cryptographie

- Cryptographie – Les définitions
- Types de chiffrement : chiffrement à clés partagées, chiffrement à clé publique
- Symétrique vs. Asymétrique, combinaisons symétrique / asymétrique
- Fonctions de hachage
- Utilisation des sels
- Signatures numériques, processus de signature, processus de vérification

3. Chiffrement, hash et signature des données

- Cryptographie Service Providers (CSP)
- System, security, cryptography
- Choix des algorithmes de chiffrement
- Chiffrement symétrique : algorithme (DES, 3DES, RC2, AES), chiffrement de flux, mode de chiffrement (CBC, ECB, CFB)
- Algorithmes asymétriques
- Algorithme : RSA, DSA, GPG
- Algorithme de hachage : MD5, SHA1 / SHA2 / SH3

4. Vue d'ensemble d'une infrastructure à clé publique (PKI)

- Certificat numérique : certificat X.509
- PKI – Les définitions
- Les fonctions PKI
- PKI – Les composants
- PKI – Le fonctionnement
- Applications de PKI : SSL, VPN, IPSec
- IPSec et SSL en entreprise
- Smart Cards (cartes intelligentes)
- Autorité de certification

5. SSL et certificat de serveur

- Certificat de serveur SSL : présentation, autorité de certification d'entreprise, autorité de certification autonome

6. Utilisation de SSL et des certificats clients

- Certificats clients
- Fonctionnement de SSL : phase I, II, III et IV
- Vérification de la couverture d'utilisation d'un certificat (lors du handshake)
- Vérification des dates d'utilisation d'un certificat

7. Sécurité des webservices

- Objectifs de la sécurisation des services Web : authentification, autorisation, confidentialité et intégrité
- Limitations liées à SSL
- Sécurité des services Web : WSE 2.0, sécurisation des messages SOAP / REST

8. Jetons de sécurité

- Jetons de sécurité : User-Name Token, Binary Token, XML Token, JWT (JSON Web Tokens), Session-based Token
- Intégrité d'un jeton (MAC / HMAC)
- Cycle de vie d'un jeton, expiration automatique (ou pas), contexte d'utilisation d'un jeton
- Habilitations suivant le contexte du jeton
- Certificats X.509
- Signature des messages SOAP / REST : création d'un jeton de sécurité, vérification des messages (MAC / HMAC), chiffrement des messages, déchiffrement du message

9. Sécurité et développement web

- Classification des attaques : STRIDE, Top 10 OWASP
- Les erreurs classiques
- Authentification par jeton et gestion des habilitations
- Les handlers et méthodes HTTP
- Séparation des handlers par contexte de sécurité
- Injection SQL
- Failles XSS (cross-site scripting)
- XSS Cookie Stealer

- CSRF : Cross-Site Request Forgery

10. Outils de sécurité et d'audit

- Outils du SDK liés à la sécurité
- Outils pour mener les tests de sécurité

Organisation

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes.

Moyens pédagogiques et techniques

- Apports didactiques pour apporter des connaissances communes.
- Mises en situation de réflexion sur le thème du stage et des cas concrets.
- Méthodologie d'apprentissage attractive, interactive et participative.
- Equilibre théorie / pratique : 60 % / 40 %.
- Supports de cours fournis au format papier et/ou numérique.
- Ressources documentaires en ligne et références mises à disposition par le formateur.
- Pour les formations en présentiel dans les locaux de Softeam, les stagiaires sont accueillis dans une salle de cours équipée d'un réseau Wi-Fi, d'un tableau blanc ou paperboard. Un carnet de notes est offert. Un ordinateur avec les logiciels appropriés est mis à disposition (le cas échéant).

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation :

- Recueil des besoins : permet de récolter des informations sur le stagiaire (profil, formation, attentes particulières, ...).
- Auto-positionnement des stagiaires afin de mesurer le niveau de départ.

Tout au long de la formation :

- Évaluation continue des acquis via des questions orales, exercices / projet fil rouge, des QCM, des cas pratiques et mises en situation.

A la fin de la formation :

- Auto-positionnement des stagiaires afin de mesurer l'acquisition des compétences.
- Evaluation du formateur des compétences acquises par les stagiaires.
- Questionnaire de satisfaction à chaud : permet de connaître le ressenti des stagiaires à l'issue de la formation.
- Questionnaire de satisfaction à froid : permet d'évaluer les apports réels de la formation et leurs mises en application au quotidien.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.