Sécurité des applications Web, synthèse

★★★★★

PL-45 **2 Jours (14 Heures)**

Description

Ce séminaire dresse un panorama complet des menaces du Web. Il détaille les failles des navigateurs, réseaux sociaux et du Web 2.0, les nouvelles vulnérabilités sur SSL/TLS et certificats X509, ainsi que des applications J2EE, .NET et PHP. Il présente les solutions pour protéger, contrôler la sécurité des applications.

À qui s'adresse cette formation ?

Pour qui

DSI, RSSI, responsables sécurité, développeurs, concepteurs, chefs de projets intégrant des contraintes de sécurité, responsables ou administrateurs réseau, informatique, système.

Prérequis

Aucune

Les objectifs de la formation

- Identifier les menaces de sécurité sur les applications Web
- Connaître les protocoles de sécurité Web
- Comprendre les typologies d'attaque
- Sécuriser les applications Web

Programme de la formation

Menaces, vulnérabilités des applications Web

- Risques majeurs des applications Web selon IBM X-Force IBM et OWASP.
- Attaques de type Cross Site Scripting (XSS), injection et sur sessions.
- Propagation de faille avec un Web Worm.
- Attaques sur les configurations standard.

Protocoles de sécurité SSL, TLS

- SSL v2/v3 et TLS, PKI, certificats X509, autorité de certification.
- Impact de SSL sur la sécurité des firewalls UTM et IDS/IPS.
- Failles et attaques sur SSL/TLS.
- Techniques de capture et d'analyse des flux SSL.
- Attaque HTTPS stripping sur les liens sécurisés.
- Attaques sur les certificats X509, protocole OCSP.
- SSL et les performances des applications Web.

Attaques ciblées sur l'utilisateur et le navigateur

- Attaques sur les navigateurs Web, Rootkit.
- Sécurité des Smartphones pour le surf sur le Net.
- Codes malveillants et réseaux sociaux.
- Les dangers spécifiques du Web 2.
- 0.
- Les techniques de Social engineering.

Attaques ciblées sur l'authentification

- Authentification via HTTP, SSL par certificat X509 client.
- Mettre en oeuvre une authentification forte, par logiciel.
- Solution de Web SSO non intrusive (sans agent).
- Principales attaques sur les authentifications.

Sécurité des Web services

- Protocoles, standards de sécurité XML Encryption, XML Signature, WS-Security/Reliability.
- Attaques d'injection (XML injection.
-), brute force ou par rejeu.
- Firewalls applicatifs pour les Web services.
- Principaux acteurs et produits sur le marché.

Sécuriser efficacement les applications Web

- Durcissement, hardening : sécuriser le système et le serveur HTTP.
- Virtualisation et sécurité des applications Web.
- Environnements .
- NET, PHP et Java.
- Les 5 phases du SDL.
- Techniques de fuzzing.
- Qualifier son application avec l'ASVS.
- WAF : quelle efficacité, performances ?

Contrôler la sécurité des applications Web

- Pentest, audit de sécurité, scanners de vulnérabilités.
- Organiser une veille technologique efficace.
- Déclaration des incidents de sécurité.
- Démonstration Mise en oeuvre d'un serveur Web avec certificat X509 EV : analyse des échanges protocolaires.
- Exploitation d'une faille de sécurité critique sur le frontal HTTP.
- Attaque de type HTTPS Stripping.