Sécurité des applications Web,

Durée : 4 jours Référence : SAWEB

Cette formation dresse un panorama complet des menaces du Web. Elle détaille les failles des navigateurs, les attaques sur les réseaux sociaux et le Web2.0, les nouvelles vulnérabilités sur SSL/TLS et les certificats X509, ainsi que les failles des applications J2EE, .NET et PHP. Illustrée par de nombreuses démonstrations, elle présente les solutions les plus efficaces pour protéger et contrôler la sécurité de vos applications : développement sécurisé avec SDL, scanner de vulnérabilités Web, Firewall applicatif et Firewall XML.

Contenu

- Introduction
- Menaces et vulnérabilités des applications Web
- Les protocoles de sécurité SSL et TLS
- Les attaques visant l'utilisateur et le navigateur
- Les attaques visant l'authentification
- La sécurité des Web services
- Comment sécuriser efficacement les applications Web ?
- Contrôler la sécurité des applications Web

Participants

Directeurs et Responsables sécurité, concepteurs, développeurs, chefs de projets et administrateurs réseau / système.

Pré-requis

Connaissances de base en informatique et en réseaux.

Programme

Introduction

- Evolution des attaques protocolaires et applicatives.
- Le monde des hackers : qui sont-ils ?
- Statistiques et évolution des failles liées au Web selon IBM X-Force IBM et OWASP.

- Le protocole HTTP 1.0 et 1.1.
- Redirection HTTP, host virtuel, proxy cache et tunneling.
- Architecture réseau, Firewall, Proxy, Reverse Proxy...

Menaces et vulnérabilités des applications Web

- Les 10 risques majeurs des applications Web selon l'OWASP (2010).
- Les attaques de type " Cross Site Scripting " alias XSS.
- Les attaques en injection et sur les sessions.
- Les nouvelles failles introduites par le Web 2.0.
- Propagation de faille avec un Web Worm.
- Attaques sur les configurations standard.

Les protocoles de sécurité SSL et TLS

- Mise en œuvre des protocoles SSL et TLS
- Les techniques cryptographiques SSL v2/v3 et TLS.
- PKI, certificats X509 et autorité de certification.
- Les nouveaux certificats à validation étendue (X509 EV).
- Quel est l'impact de SSL sur la sécurité des firewalls UTM et des IDS/IPS ?
- Les failles et attaques sur SSL/TLS
- Techniques de capture et d'analyse des flux SSL.
- Attaque de type “ Man In The Middle “ avec sslsniff.
- Attaque " HTTPS stripping " sur les liens sécurisés.
- Attaques sur la cryptographie SSLv2.
- Attaques en renégociation sur SSLv3/TLS.
- Attaques sur les certificats X509.
- Attaques sur le protocole OCSP.
- Optimisation des performances SSL
- SSL et les performances des applications Web.
- Utilisation de carte crypto-hardware SSL/TLS.

Les attaques visant l'utilisateur et le navigateur

- Attaques sur les navigateurs Web
- Le navigateur le plus sûr.
- Rootkit navigateur et poste utilisateur.
- La sécurité des Smartphones pour le surf sur le Net.
- Attaques sur l'utilisateur du Web
- Codes malveillants et réseaux sociaux.
- Les dangers spécifiques du Web 2.0.
- Les techniques de Social engineering.

Les attaques visant l'authentification

- Les mécanismes d'authentification des utilisateurs
- L'authentification via HTTP.
- L'authentification via SSL par certificat X509 client.
- Comment mettre en œuvre une authentification forte.
- Autres techniques d'authentification par logiciel.
- Solution de Web SSO non intrusive (sans agent).
- Les principales attaques sur les authentifications
- Attaque sur les mots de passe.
- Attaque 'Man in the Middle'.
- Attaque sur les authentifications HTTPS.

La sécurité des Web services

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

Comment sécuriser efficacement les applications Web ?

- Etape 1 : durcissement des serveurs
- En quoi consiste le durcissement ou " hardening " ?
- Sécuriser le système et le serveur HTTP.
- Techniques de virtualisation et sécurité des applications Web.
- Etape 2 : intégration de la sécurité dans le cycle de vie du logiciel
- La sécurité des environnements .NET, PHP et Java.
- Les 5 phases du processus SDL.
- Comment utiliser les techniques de " fuzzing " ?
- Comment qualifier son application avec l'ASVS ?
- Etape 3 : ajout d'une protection active de type Firewall applicatif
- Les limites des firewalls réseaux.
- WAF : quelle efficacité, quelles performances ?
- Construire son WAF en Open source avec Apache.
- Les principaux produits sur le marché.
- Les critères d'évaluation d'un WAF selon le WASC.
- Etape 4 : optimisation des performances et haute disponibilité
- Utilisation des solutions de virtualisation.

- L'équilibrage de charges par load et Web balancing.
- L'accélération du protocole HTTP par compression.
- " Benchmarker " son application Web.

Contrôler la sécurité des applications Web

- La supervision de sécurité des applications Web
- Pentest vs audit de sécurité.
- Comment organiser une veille technologique efficace ?
- Scanners de vulnérabilités Web : comment s'en servir ?
- Le contexte juridique
- Les contraintes d'utilisation des outils de surveillance.
- Cryptographie : le point sur la réglementation.
- Que faire en cas d'intrusion sur votre application Web ?
- Obligation de déclaration des incidents de sécurité.