Sécurité des applications Web, synthèse
analyser les solutions et leurs mises en œuvre

Séminaire de 2 jours - 14h
Réf : SEW - Prix 2024 : 2 090€ HT

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

OBJECTIFS PÉDAGOGIQUES

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

Identifier les menaces de sécurité sur les applications Web

Connaître les protocoles de sécurité Web

Comprendre les typologies d'attaque

Sécuriser les applications Web

LE PROGRAMME

dernière mise à jour : 12/2019

1) Menaces, vulnérabilités des applications Web

- Risques majeurs des applications Web selon IBM X-Force 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.

2) 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.

3) 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 techniques de Social Engineering.

4) Attaques ciblées sur l'authentification

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

PARTICIPANTS

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

PRÉREQUIS

Connaissances de base en informatique et en réseaux.

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.

5) 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.

6) 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, quelles performances ?

7) 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 œuvre 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.

LES DATES

CLASSE À DISTANCE	PARIS
2024 : 13 juin, 17 oct.	2024 : 06 juin, 10 oct.