Sécurité des applications Web, perfectionnement

Cours Pratique de 3 jours - 21h
Réf : SEI - Prix 2024 : 2 380CHF HT

Ce stage de perfectionnement vous permettra d'enrichir vos compétences pour vous protéger et mieux réagir face aux nombreuses menaces du Web. Vous verrez comment auditer la sécurité de vos applications, les tester et mettre en place les contre-mesures les plus adaptées.

OBJECTIFS PÉDAGOGIQUES

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

Mettre en place un serveur Web présentant des vulnérabilités pour en observer le comportement

Connaitre la démarche et mise en place d'un audit d'une application Web

Mettre en place des mesures de sécurisation pour les applications Web

Mettre en oeuvre une autorité de certification privée avec intégration de certificats dans une application

Utiliser un web spider pour détecter les liens brisés, les pages avec ou sans authentification

MÉTHODES PÉDAGOGIQUES

Bases théoriques illustrées par des travaux et exercices permettant de pratiquer.

EXERCICE

De nombreux exercices et études de cas seront proposés tout au long de cette formation.

LE PROGRAMME

dernière mise à jour : 09/2018

1) Rappel sur les principales failles de sécurité

- L'attaque Cross-Site Scripting (XSS).
- L'injection de commandes et injection SQL.
- Les attaques par Deni de Service (DoS).
- Le Deni de Service Distribué (DDoS).
- Le Buffer overflow (Débordement de pile).
- Le projet OWASP (Open Web Application Security Project).

Travaux pratiques : Mise en place d'un serveur Web présentant des vulnérabilités pour en observer le comportement. Démonstration de l'exploitation d'un buffer overflow.

2) La sécurité des applications

- Concept base et importance.
- Les comptes créés pour effectuer les tests.
- Les dossiers fictifs, peut-on s'en passer ?
- Les séquences de tests et de mise au point sont-elles encore présentes en production ?

3) Auditer et sécuriser une application Web

- Démarche et mise en place d'un audit. Bien gérer l'interaction avec la base de données.
- Mettre en place une authentification sécurisée. Exploitation d'une faille d'authentification.
- Gestion des erreurs, des exceptions et des logs.
- Savoir effectuer l'analyse et la corrélation des informations de log.

PARTICIPANTS

Administrateurs réseaux, systèmes, Webmasters.

PRÉREQUIS

Bonnes connaissances systèmes et réseaux, connaissances de base en développement ou connaissances équivalentes à celles apportées par le cours "Sécurité des applications Web" réf. SER.

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.

- Les bonnes pratiques pour avoir des formulaires sécurisés. Exemple d'exploitation d'un formulaire mal développé.
Travaux pratiques : Mise en oeuvre d'une infrastructure trois tiers, client, serveur Web et bases de données. Simulation d'une tentative d'attaque. Analyse et solution.

4) Le chiffrement

- Rappels sur les principes de base.
- Implémenter le chiffrement dans une application. Les exploitations possibles.
- Tester si une application est bien protégée par le chiffrement.
- Les applications de chiffrement du marché.

Travaux pratiques : Mise en oeuvre d'une autorité de certification privée avec intégration de certificats dans une application.

5) Tester les applications

- Comment tester avant la mise en production.
- Le fingerprinting : l'identification des caractéristiques du serveur (moteur web, framework, applications).
- Utiliser un web spider pour détecter les liens brisés, les pages avec ou sans authentification et chiffrement.
- Comment mesurer la disponibilité d'une application avec une simulation.

Travaux pratiques : Exemple de tentative d'attaques et fingerprinting. Comment écrire un web spider pour détecter les liens brisés. Vérifier l'authentification sur les pages.

LES DATES

CLASSE À DISTANCE
2024 : 10 juin, 23 sept., 25 nov.