Top 10 OWASP partie 2, connaître les 6 autres vulnérabilités d'une application web

Formation en ligne - 1h
Réf : 4OW - Prix 2024 : 95€ HT

Ce cours en ligne a pour objectif de vous faire découvrir les six dernières vulnérabilités du top 10 OWASP. Il s'adresse à un public de développeurs, architectes et experts techniques possédant des connaissances de base en conception d'applications web (HTML, CSS, JavaScript, PHP, HTTP). La pédagogie s'appuie sur un auto-apprentissage séquencé par actions de l'utilisateur sur l'environnement à maîtriser. Une option de tutorat vient renforcer l'apprentissage.

OBJECTIFS PÉDAGOGIQUES

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

Connaître les six dernières vulnérabilités du top 10 OWASP

Comprendre le principe sous-jacent derrière chaque vulnérabilité

Mettre en place des protections efficaces

Maitriser les bonnes pratiques pour prévenir les vulnérabilités

PÉDAGOGIE ET PRATIQUES

Une évaluation tout au long de la formation grâce à une pédagogie active mixant théorie, exercice, partage de pratique et gamification. Un service technique est dédié au support de l'apprenant. La formation est diffusée au format SCORM (1.2) et accessible en illimité pendant 1 an.

ACTIVITÉS DIGITALES

Démonstrations, cours enregistrés, partages de bonnes pratiques, quiz, fiches de synthèse.

PARTICIPANTS

Développeurs, architectes et experts techniques.

PRÉREQUIS

Des connaissances de base en conception d'applications web sont souhaitables (HTML, CSS, JavaScript, PHP, HTTP).

COMPÉTENCES DU FORMATEUR

Les experts qui ont conçu la formation et qui accompagnent les apprenants dans le cadre d'un tutorat sont des spécialistes des sujets traités. 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. 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

La progression de l'apprenant est évaluée tout au long de sa formation au moyen de QCM, d'exercices pratiques, de tests ou d'échanges pédagogiques.
Sa satisfaction est aussi évaluée à l'issue de sa formation grâce à un questionnaire.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : documentation et support de cours, exercices pratiques d'application et corrigés des exercices, études de cas ou présentation de cas réels.
ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Une attestation de fin de formation est fournie si l'apprenant a bien suivi la totalité de la formation.

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.

LE PROGRAMME

dernière mise à jour : 06/2023

1) Les vulnérabilités d'une application web

- Introduction.
- Environnement utilisé.

2) Le manque de contrôle d'accès

- Principe de base.
- Champs cachés.
- Inclusion de fichier.
- Autres erreurs.
- Mise en place de protections.

3) La mauvaise configuration de sécurité

- Mauvaises pratiques de la configuration de sécurité.
- Mise en place de protections et de bonnes pratiques.

4) Le cross-site scripting (XSS)

- Principe de base.
- Attaque de type XXS Stored.
- Attaque de type XXS Reflected.

- Attaque de type XXS DOM.
- Mise en place de protections.

5) La désérialisation non sécurisée

- Principe de base.
- Exploitation d'une faille de désérialisation.
- Mise en place de protections.

6) L'utilisation de composants avec vulnérabilités connues

- Principe de base.
- Mise en place de protections.

7) Le manque de log et de monitoring

- Principe de base.
- Mise en place de protections.