Top 10 OWASP partie 1, connaître les 4 premières vulnérabilités d'une application web

Formation en ligne - 0h45
Réf : 4VM - Prix 2024 : 95€ HT

Ce cours en ligne a pour objectif de vous initier aux quatre premières vulnérabilités d'une application web recensées dans le top 10 OWASP. Il s'adresse à un public de développeurs, architectes et experts techniques possédant des connaissances de base sur la 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 quatre premières 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, fiche(s) de synthèse, composent la formation. Grâce au tutorat, une classe à distance sur mesure, un exercice corrigé, des débriefings et des échanges sont aussi inclus.

PARTICIPANTS

Développeurs, architectes et experts techniques.

PRÉREQUIS

Une connaissance de base sur la conception d'applications web est souhaitable (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) Appréhender les vulnérabilités d'une application web

- Sécurité informatique et le top 10 OWASP web.
- Environnement utilisé.

2) Connaître les injections

- Injection SQL.
- Injection XPath.
- Injection de code.
- Autres injections.
- Mise en place de contre-mesures.

3) Découvrir la violation de gestion d'authentification et de session

- Présentation du vol de session.
- Attaque par brute force.
- Mise en place de contre-mesures.

4) Connaître l'exposition des données sensibles

- Les mauvaises pratiques liées à l'exposition de données sensibles.
- La mise en place de contre-mesures.

5) Découvrir l'attaque XXE (XML Entité Externe)

- L'attaque de type XXE.
- Fonctionnement d'une attaque XXE.
- Mise en place de contre-mesures.