OWASP Top 10, les vulnérabilités d'une application web
tutorat en option

Cours Pratique de 1 jour
Réf : 4OW - Prix 2022 : 30€ HT

Cette formation digitale a pour objectif de vous faire découvrir les six dernières vulnérabilités du top 10 OWASP. Elle 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

Connaître les vulnérabilités liées au manque de contrôle d'accès

Connaître les vulnérabilités liées à la mauvaise configuration de la sécurité

Connaître les vulnérabilités liées aux failles de type XSS (cross-site scripting)

Connaître les vulnérabilités liées à la désérialisation non sécurisée

Connaître les vulnérabilités liées à l'utilisation de composants avec des vulnérabilités connues

Connaître les vulnérabilités liées au manque de log et de monitoring

PÉDAGOGIE ET PRATIQUES

Formation digitale basée sur une pédagogie active avec une combinaison de théorie, de démonstrations, de partages d'expérience et de bonnes pratiques. Pour renforcer l'apprentissage, les séquences pédagogiques sont de courte durée et un tutorat est proposé en option.

ACTIVITÉS DIGITALES

Exercice, quiz, fiche de synthèse, cours enregistrés et option de tutorat (débriefing, échanges par e-mail avec un expert, social learning, classe à distance sur mesure).

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

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 compétence acquises.

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 pshaccueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

LE PROGRAMME

dernière mise à jour : 08/2021

1) Appréhender les vulnérabilités d'une application web

- Introduction.
- Environnement utilisé.

2) Les vulnérabilités liées au manque de contrôle d'accès

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

3) Les vulnérabilités liées à la mauvaise configuration de sécurité

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

4) Les vulnérabilités liées au 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.
Reproduire avec son logiciel ce qui est montré dans chaque séquence et

5) Les vulnérabilités liées à la désérialisation non sécurisée
- Principe de base.
- Exploitation d'une faille de désérialisation.
- Mise en place de protections.

6) Les vulnérabilités d'utilisation de composants avec vulnérabilités connues
- Principe de base.
- Mise en place de protections.

7) Les vulnérabilités liées au manque de log et de monitoring
- Principe de base.
- Mise en place de protections.

NOS POINTS FORTS

- Séquences de courte durée
- Exercices et fiches téléchargeables
- Activités digitales illimitées pendant 1 an
- Tutorat personnalisé en option
- Accès multi-device (smartphone, tablette ou ordinateur) via une simple connexion internet