Sécurité des applications web – OWASP top 10 2021 (Open Web Application Security Project)

Sécurité des applications web – OWASP top 10 2021 (Open Web Application Security Project)

Formation	2 sessions disponibles	Attestation de présence
Formation en ligne, Formation présentielle	14 heures	Réalisable en ligne

Référence de la formation: FR-CyberWeb-

Version: 10.05.2024. Vous trouverez toutes les informations actuelles sur https://academie-fr.tuv.com/s/FR-CyberWeb-

OWASP (Open Web Application Security Project) est une organisation internationale à but non lucrative. Sa mission : Conseiller sur le développement, l'achat et le maintien d'applications web et d'API fiables et sécurisées. A cet effet, elle partage des publications, des vidéos, des événements, des outils et des méthodes. Elle réunit dans son référentiel OWASP top 10 les dix failles de sécurité des applications web les plus critiques et propose des solutions de remédiation.

Après un panorama de la cybersécurité, ses référentiels et son écosystème, nous verrons ensemble en détail chaque vulnérabilité composant le top 10 OWASP 2021 avec des exemples concrets, des exercices pratiques et les moyens à mettre en oeuvre pour s'en prémunir. Vous serez en mesure d'utiliser cette base de référence pour réduire les risques de sécurité de vos applications web les plus fréquents.

Les objectifs

- Appréhender les problématiques de développement sécurisé et les risques associés aux mauvaises pratiques.
- Idenfier les bonnes pratiques de développement sécurisé.
- Apprendre à sécuriser votre base de code logiciel.

Le public ciblé

Amateurs et professionnels en développement ou sécurité IT, intéressées par la sécurité des applications

web (développeurs, intégrateurs, concepteurs, chefs de projet).

Les prérequis

Des connaissances en développement d'application web ainsi que des notions en informatique et réseau sont souhaitables.

Si formation à distance :

- Un accès internet stable via Ethernet ou Wi-Fi avec un débit correct (1.2 Mb/s en débit descendant minimum est recommandé)
- Un PC / MAC avec l'outil Teams d'installé ainsi qu'un accès non restreint à internet.

Le contenu de la formation

JOUR 1 :

Introduction à la cybersécurité

- Vocabulaire et définition
- Comprendre le besoin et son évolution au fil du temps
- La notion de « surface d'attaque »

Les référentiels

- Présentation de l'OWASP Top 10
- Présentation de CWE Top 25

Ecosystème des vulnérabilités

- CVE : Common Vulnerability Enumeration
- CVSS : Common Vulnerability Scoring System
- Trouver et rapporter une vulnérabilité

A01:2021-Contrôle d'accès défaillant

- Présentation de la catégorie de vulnérabilité
- Exercice/Démo
- Remédiation/Outillage

A02:2021-Défaillances cryptographiques

- Présentation de la catégorie de vulnérabilité
- Exercice/Démo
- Remédiation/Outillage

A03:2021-Injection

- Présentation de la catégorie de vulnérabilité
- Exercice/Démo
- Remédiation/Outillage

A04:2021-Conception non sécurisée

- Présentation de la catégorie de vulnérabilité
- Exercice/Démo
- Remédiation/Outillage

JOUR 2 :

A05:2021-Mauvaise configuration de sécurité

- Présentation de la catégorie de vulnérabilité
- Exercice/Démo
- Remédiation/Outillage

A06:2021-Composants vulnérables et obsolètes

- Présentation de la catégorie de vulnérabilité
- Exercice/Démo
- Remédiation/Outillage

A07:2021-Identification et authentification défaillante

- Présentation de la catégorie de vulnérabilité
- Exercice/Démo

- Remédiation/Outillage

A08:2021-Manque d'intégrité des données et du logiciel

- Présentation de la catégorie de vulnérabilité
- Exercice/Démo
- Remédiation/Outillage

A09:2021-Manque de surveillance et de journalisation

- Présentation de la catégorie de vulnérabilité
- Exercice/Démo
- Remédiation/Outillage

A10:2021-Falsification de requête côté serveur

- Présentation de la catégorie de vulnérabilité
- Exercice/Démo
- Remédiation/Outillage

Méthodes pédagogiques

- Alternance d'exposés théoriques, d'illustrations par des cas concrets, d'exercices individuels ou en groupes de travail et de jeux de rôle.

Modalités d'évaluation :

- Exercices individuels, en binôme, en groupe,
- Débriefing par les groupes,
- Débriefing par le formateur,
- Evaluation des compétences acquises via un questionnaire en fin de formation.

Informations importantes

Ce cours est proposé en partenariat avec SERMA Safety & Security.

Si vous êtes en situation de handicap, nous vous remercions de bien vouloir nous contacter avant de procéder à l'inscription en envoyant un mail à formation@fr.tuv.com. Nous mettrons tout en œuvre pour répondre à votre besoin de formation.

Aperçu des dates et réservation

Réservez dès maintenant la date de votre choix directement en ligne sur https://academie-fr.tuv.com/s/FR-CyberWeb- et profitez de ces avantages :

- Processus de réservation rapide
- Compte client personnel
- Réservation simultanée pour plusieurs participant(e)s.

Vous pouvez également utiliser le formulaire de commande pour commander par e-mail.