Sécurité défensive

Défense des applications Web

3 jours (21h00) | ★★★★☆ 4/5 | SEC-SAW | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Contenu mis à jour le 13/10/2023. Document téléchargé le 23/05/2024.

Objectifs de formation

A l'issue de cette formation, vous serez capable de :

- Intégrer la sécurité dès le début du cycle de développement (DevSecOps)
- Utiliser les techniques de sécurisation des applications Web
- Identifier et mettre en place des contre-mesures contre les vulnérabilités courantes.

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

** nous consulter pour la faisabilité en distanciel*

*** ratio variable selon le cours suivi*

Prérequis

Avoir des connaissances généralistes en programmation Web.

Public concerné

Développeurs, ingénieurs DevOps et professionnels de la sécurité souhaitant intégrer la sécurité dans le processus de développement (DevSecOps).

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Jour 1

Introduction au DevSecOps

- Introduction au DevSecOps
- Rôle de la sécurité dans le cycle de développement
- Méthodologie DevSecOps
- Principes de sécurité dans le développement

Préparation et sécurisation de l'environnement de développement

- Configuration d'un environnement de développement sécurisé
- Utilisation d'outils de sécurité pour l'analyse statique du code
- Intégration de l'authentification forte et de la gestion des accès

Exemples de travaux pratiques (à titre indicatif)

- *Configurer un environnement de développement sécurisé en utilisant des outils tels que Docker avec des images préconfigurées pour la sécurité*
- *Effectuer une analyse statique du code à l'aide d'un outil comme SonarQube*

Jour 2

Détection de vulnérabilités

- Méthodes de détection des vulnérabilités dans le code
- Utilisation d'outils de test d'intrusion automatisés
- Analyses dynamiques de sécurité

Exemples de travaux pratiques (à titre indicatif)

- *Les participants utilisent un outil de test d'intrusion automatisé tel qu'OWASP ZAP pour scanner une application Web factice à la recherche de vulnérabilités*
- *Ils analysent ensuite les résultats et proposent des solutions pour corriger les problèmes identifiés*

Mise en place de contre-mesures

- Sécurisation de l'authentification et de l'autorisation
- Gestion des sessions sécurisées
- Validation et filtrage des données en entrée

Exemples de travaux pratiques (à titre indicatif)

- *Mettre en place une authentification forte (par exemple, l'utilisation de l'authentification à deux facteurs) pour une application Web de démonstration*
- *Discuter des avantages et des inconvénients de différentes méthodes d'authentification*

Jour 3

Mise en place de contre-mesures - Suite

- Protection contre les attaques XSS (Cross-Site Scripting)
- Prévention des attaques CSRF (Cross-Site Request Forgery)
- Utilisation de CSP (Content Security Policy) pour limiter les risques

Exemples de travaux pratiques (à titre indicatif)

- *Travailler une application Web vulnérable aux attaques XSS et CSRF...*
- *Mettre en place des contre-mesures appropriées, telles que l'utilisation de balises de sécurité, de jetons anti-CSRF, et de Content Security Policy (CSP)*

Intégration de la sécurité dans les flux DevOps

- Intégration de la sécurité dans les pipelines DevOps
- Automatisation des tests de sécurité
- Utilisation de ressources et guides de sécurité, y compris l'OWASP Top Ten
- Scénarios pratiques de sécurisation des applications Web dans un environnement DevSecOps

Exemples de travaux pratiques (à titre indicatif)

- *Mettre en place un pipeline DevOps pour une application Web, en intégrant des tests de sécurité automatisés à chaque étape du processus de développement*
- *Utiliser les ressources de l'OWASP Top Ten pour identifier et corriger les vulnérabilités*

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

Modalités d'évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation

Accessibilité de la formation

Le groupe M2i s'engage pour faciliter l'accessibilité de ses formations. Les détails de l'accueil des personnes en situation de handicap sont consultables sur la page Accueil et Handicap.

Modalités et délais d'accès à la formation

Les formations M2i sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.