Formation Sécurité applicative – OWASP Top 10

Informations

Durée : 2 jours (14h.)

Tarif* : Nous consulter

Réf : OWAS

Niveau : Moyen

intra

Mise à jour le 30/12/25

*tarif valable jusqu'au 31/12/2026

Prochaines sessions

Contactez-nous pour connaitre nos futures sessions.

Pré-requis

- Connaissances en développement applicatif (web ou API)
- Compréhension générale des architectures applicatives
- Notions de bases en HTTP / API recommandées

Objectifs

Objectifs pédagogiques :

- Comprendre les enjeux de la sécurité applicative
- Connaître le rôle et l'objectif de l'OWASP Top 10
- Identifier les principales vulnérabilités applicatives
- Comprendre les mécanismes d'exploitation des failles
- Connaître les bonnes pratiques de développement sécurisé

Objectifs opérationnels :

- Identifier les vulnérabilités OWASP dans une application
- Comprendre l'impact des failles de sécurité applicative
- Mettre en œuvre des mesures de prévention et de correction
- Appliquer les principes du secure coding
- Contribuer à une démarche DevSecOps

Programme

Jour 1 – Comprendre les vulnérabilités OWASP Top 10

Introduction à la sécurité applicative

Pourquoi la sécurité applicative est critique
Typologie des attaques applicatives
Place de l'OWASP dans l'écosystème sécurité
Présentation de l'OWASP Top 10

Vulnérabilités liées aux accès et à l'authentification

Contrôles d'accès défaillants
Authentification et gestion des sessions
Mauvaises configurations de sécurité
Exemples concrets et impacts

Vulnérabilités liées aux données et aux entrées utilisateur

Injections (SQL, NoSQL, commandes)
Exposition de données sensibles
Validation et filtrage des entrées
Gestion des erreurs et messages

Atelier pratique

Analyse de scénarios applicatifs vulnérables
Identification des failles OWASP
Discussion autour des correctifs possibles

Jour 2 – Secure coding, prévention et intégration DevSecOps

Autres vulnérabilités OWASP Top 10

Désérialisation non sécurisée
Composants vulnérables et dépendances

Journalisation et monitoring insuffisants
Problèmes de conception sécuritaire

Bonnes pratiques de développement sécurisé

Secure coding by design
Principe du moindre privilège
Gestion sécurisée des secrets
Sécurité des API et microservices

Sécurité applicative et DevSecOps

Intégration de la sécurité dans le cycle de développement
Tests de sécurité applicative (SAST, DAST – introduction)
Revue de code et sécurité
Sensibilisation des équipes

Atelier pratique

Analyse d’un extrait de code
Identification et correction de failles
Élaboration d’une checklist de sécurité applicative