

Sécurité PHP et bonnes pratiques

Découvrez la sécurité PHP et les bonnes pratiques pour développer des applications web sécurisées.

Catégorie: Programmation · Durée: 3 jours

POUR QUI ?

- Développeurs PHP
- Ingénieurs sécurité et administrateurs système
- Équipes qui veulent pratiquer sur des cas réels

Cette formation couvre les fondamentaux de la sécurité PHP : bonnes pratiques de codage sécurisé, validation des données, assainissement des entrées, authentification, contrôle d'accès et gestion sécurisée des sessions. Vous découvrirez également les vulnérabilités les plus courantes des applications PHP et les moyens de les corriger. À l'issue de cette formation, vous maîtriserez les principes de la sécurité PHP et serez en mesure de développer des applications web sécurisées.

Prérequis

Connaissances de base en programmation PHP

Programme

- Introduction à la sécurité PHP
- Pratiques de codage sécurisé
- Validation des données et assainissement des entrées
- Authentification et contrôle d'accès
- Gestion sécurisée des sessions
- Vulnérabilités de sécurité courantes
- Prévention des attaques par injection SQL
- Prévention des attaques XSS (Cross-Site Scripting)
- Sécurisation des téléversements de fichiers
- Protection contre les attaques CSRF (Cross-Site Request Forgery)
- Garantir des communications sécurisées
- Bonnes pratiques de sécurité des mots de passe
- Sécurisation de la configuration PHP

- Gestion sécurisée des erreurs
- Mise en place des en-têtes de sécurité
- Accès sécurisé aux bases de données
- Traitement sûr des saisies utilisateur
- Sécurisation des systèmes de fichiers
- Standards de codage sécurisé
- Tests et débogage orientés sécurité