SÉCURISER UNE APPLICATION AVEC PHP

1200 € HT (tarif inter) | REF : DÉV210
TARIF SPÉCIAL : particuliers et demandeurs d'emploi

Il est primordial de prendre conscience des types d'attaques auxquelles son code sera potentiellement exposé et apprendre les bases de la sécurité en PHP.

3 JOURS | **21** HEURES

CODE CPF : 208979

PROGRAMME

Menaces, vulnérabilités des applications Web

- Risques majeurs des applications Web selon IBM X-Force IBM et OWAS.
- Attaques de type Cross Site Scripting (XSS), injection et sur sessions.
- Propagation de faille avec un Web Worm.
- Attaques sur la configuration standard.

Sécurité des accès avec PHP

- Authentification Web, HTTP basic et form et configuration HTTPS.
- PHP safe mode et configuration PHP renforcée.
- Stratégies de contrôle d'accès.
- Stratégies basées sur les rôles.
- Contrôle d'accès aux fichiers, vérifications et Logging.

Chiffrement en PHP

- Sécurité applicative, sécurité réseau et sécurité applicative.
- Firewall, proxy et DMZ.
- Anatomie d'une faille applicative.
- Open Web Application Security Project.
- Le Top Ten OWASP.

Les failles et les solutions

- Injections SQL.
- Cross Site Scripting et Request Forgery.
- Détournement de sessions.
- Référence directe par URL.
- Exécution à distance.

OBJECTIFS

Identifier les outils de sécurité de PHP Comprendre les principales failles de sécurité applicative Sécuriser une configuration PHP Authentifier et autoriser l'accès aux applications PHP Chiffrer des données avec PHP

PUBLIC | PRÉREQUIS

PUBLIC
Développeurs, auditeurs et responsables en sécurité
PRÉREQUIS
Avoir une pratique du langage PHP et SQL

INFOS PRATIQUES

HORAIRES DE LA FORMATION
de 9 h 00 à 12 h 30 et de 13 h 30 à 17 h 00
MÉTHODOLOGIE PÉDAGOGIQUE
Théorie | Cas pratiques | Synthèse
MODALITÉS D'ÉVALUATION
Évaluation qualitative des acquis tout au long de la formation et appréciation des résultats

DATES ET LIEUX

Aucune session ouverte