

Sensibilisation au développement sécurisé d'applications WEB

Durée 1 journée

Description A travers des exemples concrets (types de menaces, types d'attaques, démonstrations), sensibiliser les décideurs et les développeurs au développement sécurisé d'applications WEB et transmettre les bonnes pratiques.
Connaissance des pratiques de développement

Pré-requis Sensibilisation à la sécurité des systèmes d'information

Objectifs Acquérir des bonnes pratiques de développement pour sécuriser des applications WEB.

Programme *Rappel sur la sécurité des systèmes d'information*



- Introduction à la sécurité
- Analyse de risques
- Faire des tests de sécurité

Les failles les plus courantes dans les applications WEB

- Paramètre non validé
- Violation de contrôle d'accès
- Violation de gestion d'authentification et de session
- Cross Site Scripting
- Débordement de tampon
- Failles d'injection
- Mauvaise gestion des erreurs
- Stockage non sécurisé
- Déni de service
- Gestion insécurisée de la configuration

Bonnes pratiques de développement sécurisé des applications WEB

- Paramètres non validés
- Cross Site Scripting
- Injection SQL
- Injection de code
- Injection de commandes
- Gestion sécurisée de la session
- Les accès fichiers
- Sécurité à travers l'obscurité
- php.ini / httpd.conf