

Les techniques du développement informatique sécurisé

Ce programme de formation présente les techniques du Développement Informatique Sécurisé permettant d'améliorer la résistance des applications aux intrusions malveillantes l'attaquants informatiques. La formation a pour but de former les développeurs aux techniques de codage sécurisées à jour et les façons d'éviter les vulnérabilités de codage communes.



Objectifs

- Faire prendre conscience aux acteurs impliqués sur les projets de développements d'application de la criticité des failles qui peuvent être générées et de l'importance de respecter des bonnes pratiques de sécurisation du code.
- Former les développeurs à des techniques de développement sécurisées à jour, y compris les façons d'éviter les vulnérabilités de développement communes.
- Proposer une formation avec des modules théoriques mais aussi des exercices pratiques et des ateliers techniques.



Jour 1

- Introduction
- Les menaces : exemples d'attaques
- Contraintes réglementaires & normes
- Cycle de développement
- Risque / Vulnérabilité
- Grands principes
- Conception et design sécurisé d'une application
 - Cryptologie
 - Authentification et session
 - Sécurisation des données
 - Audit du comportement de l'application
 - Règles générales d'écritures du code source
- Attaques simples & principales erreurs



Jour 2

- Introduction
- Techniques et utilisation de vulnérabilités
 - Attaques des applications web
 - Authentification
 - Manipulation de champs HTTP
 - Gestion de la session
 - Path Traversal
 - Injection de commandes
 - Commentaires
 - Contrôles côté client
 - Cross-Site Scripting
 - CSRF
 - Injection SQL
 - Encodage
 - Messages d'erreur
 - DoS applicatif
 - Injection CRLF
 - HRS
 - Attaques des webservices
 - Web 2.0

- Attaques des applications non-web



Public concerné

- Développeurs d'applications
- Chefs de projets de développement
- Ingénieurs de tests des applications
- Acteurs en charge de la validation des applications
- Auditeurs de sécurité

Infos pratiques

Durée : 2J