

# Introduction à la sécurité applicative et de base de données

Durée : 1 jour

Niveau : Débutant - Intermédiaire

## Description

Dans un premier temps, un survol des architectures trois tiers, des composants impliqués et de leur fonctionnement seront réalisés pour mettre les participants au niveau. Les risques et les catégories de vulnérabilités reliés à ces composants seront expliqués aux participants. (30min)

Dans un second temps, ce cours introduit les participants aux concepts de base de la sécurité de l'information et il enseigne les concepts clés ainsi que les différents domaines que couvre cette branche de l'informatique. (1,5 heure)

Dans un troisième temps, les participants apprennent à identifier les points faibles des applications Web et sont familiarisés avec les principales catégories de vulnérabilités associées à ce type d'application. Cette section du cours permet de bien faire comprendre aux participants de quelle manière un attaquant peut se servir d'une vulnérabilité qui semble banale pour compromettre le système informatique interne de l'entreprise. Cette section du cours peut comporter des exercices. (3 heures).

## Objectifs

À la fin du cours, les participants seront capables de:

- Comprendre les risques et les vulnérabilités associés
- Comprendre les principes de base de la sécurité. Tel que l'authentification, la journalisation, le chiffrement, les algorithmes de hachage, etc.
- Comprendre les types de contrôles d'accès.
- Identifier les types de données (catégorisation) et leur associer un niveau de sécurité (classification).
- Connaître les normes fédérales et des méthodologies impliquées (EMR, Chiffrement, Gestion des périmètres et Authentification)
- Identifier les vulnérabilités présentes dans une application Web.
- Comprendre l'impact qu'une vulnérabilité peut avoir sur une entreprise.
- Identifier les moyens techniques afin de mitiger les risques.
- Décrire les considérations essentielles de la conception sécuritaire.
- Bien comprendre les mécanismes en place afin de bien protéger les informations contenues dans une base de données.
- Comprendre les normes de sécurité de développement telles que OWASP, CERT SCS, CSSL

## Contenu

- Architecture logiciel
- Principes de sécurité de base
- Intégrité et disponibilité des données
- Contrôle d'accès aux données
- Sécurité applicative (Web)
- Sécurité opérationnelle
- Sécurité des bases de données

## Auditoire

- Spécialiste de la géomatique développant des logiciels

## Préalable

- Connaissance de l'architecture d'une application Web 3 tiers

