Notion de risques : Chap.6 : Sécurité des logiciels

mercredi 11 septembre 2024 17:10

Chapitre 6 : Sécurité des logiciels

Objectifs

- Comprendre l'importance de la sécurité des logiciels dans le développement et l'utilisation des applications.
- Identifier les menaces courantes qui pèsent sur les logiciels et leurs impacts potentiels.
- Appréhender les meilleures pratiques et les mesures de sécurité à mettre en œuvre lors du développement et du déploiement de logiciels.

A. **Introduction**

La sécurité des logiciels est essentielle pour protéger les systèmes d'information et les données contre les attaques. Avec l'augmentation des cybermenaces, il est crucial d'intégrer des pratiques de sécurité tout au long du cycle de vie du développement logiciel (SDLC). Ce chapitre explore les aspects de la sécurité logicielle, y compris les vulnérabilités communes, les menaces potentielles et les stratégies de mitigation.

B. Concepts

B.1 : Menaces à la Sécurité des Logiciels :

- **Vulnérabilités :**
  - Les failles de sécurité dans le code source, comme les injections SQL, les débordements de tampon, et les failles XSS (Cross-Site Scripting), peuvent être exploitées par des attaquants pour compromettre des systèmes.
- **Logiciels Malveillants :**
  - Les logiciels malveillants peuvent être intégrés dans des applications légitimes ou distribués via des canaux non sécurisés, entraînant des compromissions de données.
- **Attaques sur les API :**
  - Les interfaces de programmation d'applications (API) peuvent être ciblées par des attaques, ce qui peut compromettre les systèmes qui s'appuient sur ces API pour l'échange de données.

B.1 : Bonnes Pratiques de Sécurité Logicielle

- **Sécurité dès la Conception :**
  - Intégrer des principes de sécurité dès les phases de conception du logiciel pour identifier et atténuer les risques avant le développement.
- **Tests de Sécurité :**
  - Effectuer des tests de sécurité réguliers, tels que des tests de pénétration et des analyses de vulnérabilités, pour identifier les failles avant le déploiement.
- **Mises à Jour et Correctifs :**
  - Maintenir les logiciels à jour avec les derniers correctifs de sécurité pour se protéger contre les vulnérabilités connues.

C. Référentiel…

- **Normes et Cadres de Référence :**
  - **OWASP (Open Web Application Security Project) :**
    - Un projet qui fournit des ressources et des outils pour améliorer la sécurité des applications web. OWASP a également publié une liste des dix principales vulnérabilités des applications web.
  - **ISO/IEC 27034 :**
    - Norme qui fournit un cadre pour l'intégration de la sécurité dans le développement et l'utilisation des logiciels.
- **Meilleures Pratiques :**
  - **Code Review :**
    - Effectuer des revues de code régulières pour détecter les failles de sécurité potentielles avant la mise en production.
  - **Formation des Développeurs :**
    - Former les équipes de développement sur les pratiques de codage sécurisé et les vulnérabilités courantes pour réduire les risques dès la phase de développement.