SECURE PROGRAMMING

C’est quoi la programmation sécurisée

La programmation sécurisée est une approche de développement de logiciels qui vise à minimiser les risques de vulnérabilités et d'exploits de sécurité dans le code.

Cela implique l'utilisation de techniques et de bonnes pratiques de programmation pour identifier, prévenir et corriger les erreurs de programmation qui peuvent être exploitées par des attaquants pour compromettre la sécurité du système.

Pourquoi la programmation sécurisée

La programmation sécurisée est importante pour plusieurs raisons :

- Protection des données sensibles
- Protection des systèmes : Les vulnérabilités de sécurité peuvent également être exploitées pour compromettre le fonctionnement des systèmes informatiques
- Réputation de l'entreprise : Les violations de sécurité peuvent également nuire à la réputation d'une entreprise

  En adoptant une approche de programmation sécurisée, les développeurs peuvent aider à minimiser les risques de vulnérabilités et d'exploits de sécurité dans le code, ce qui peut protéger les données sensibles, les systèmes et la réputation de l'entreprise.

Meilleures pratiques

Parmi les techniques couramment utilisées en programmation sécurisée, on peut citer :

- La validation et la vérification des entrées utilisateur pour éviter les attaques par injection de code (comme les attaques SQL ou XSS)
- Limiter les droits d'accès : Les utilisateurs et les processus ne doivent avoir accès qu'aux ressources et aux fonctions qui leur sont nécessaires. Les droits d'accès excessifs peuvent rendre les systèmes vulnérables aux attaques.
- Privilégier la simplicité : Garder un code simple et clair est un excellent moyen de garantir sa sécurité. Simplement parce que la complexité augmente la probabilité d apparition de failles au sein du code
- La gestion correcte des erreurs pour éviter les fuites d'informations sensibles
- L'utilisation de bibliothèques de sécurité fiables pour éviter les vulnérabilités connues
- la protection des données avec des procédés cryptographiques pour protéger le secret de l’utilisateur

Les pratiques citées ci-dessous n’ont pas caractère à être exhaustives, il faut noter également que la programmation sécurisée va au-delà du code et que c’est tout ensemble de politique de sécurité bien définie qui doit être mise en place.

Ressources

Voici quelques ressources pour vous aider à mettre en place une bonne programmation sécurisée :

- OWASP : L'Open Web Application Security Project (OWASP) est une communauté mondiale de professionnels de la sécurité qui fournit des ressources pour améliorer la sécurité des applications Web
- SANS Institute : Le SANS Institute est une organisation qui fournit des formations en sécurité informatique. Leur site web propose des cours en ligne et en personne, ainsi que des webinaires et des ressources gratuites pour améliorer la sécurité des logiciels.
- NIST : L'Institut national des normes et de la technologie (NIST) fournit des normes et des lignes directrices pour améliorer la sécurité des systèmes informatiques et des logiciels. Leur site web contient des publications, des outils et des informations sur les dernières vulnérabilités et menaces.

Sources

#OWASP

#NIST