Sécurité web et web mobile selon l'ANSSI

Introduction

L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) est l'autorité française en matière de cybersécurité.
Elle fournit des recommandations essentielles pour sécuriser les systèmes d'information, y compris les applications web et mobiles.

1. Principes fondamentaux de sécurité selon l'ANSSI

- **Confidentialité** : protéger les données sensibles contre tout accès non autorisé.
- **Intégrité** : garantir que les données ne sont pas modifiées de manière non autorisée.
- **Disponibilité** : assurer que les services et données sont accessibles aux utilisateurs légitimes.
- **Traçabilité** : pouvoir suivre les actions effectuées pour détecter et analyser les incidents.
- **Résilience** : capacité à résister et à se remettre rapidement d'une attaque ou d'une panne.

2. Bonnes pratiques pour les développeurs web et mobiles

a) Sécuriser les échanges

- Utiliser **HTTPS/TLS** pour chiffrer les communications.
- Vérifier et renouveler les certificats SSL/TLS régulièrement.

b) Gérer correctement les identités et accès

- Implémenter une **authentification forte** (mot de passe complexe, 2FA).
- Restreindre les droits selon le principe du moindre privilège.
- Protéger les sessions utilisateurs (ex : cookies sécurisés, durée limitée).

c) Protéger les données sensibles

- Chiffrer les données sensibles au repos et en transit.
- Ne jamais stocker les mots de passe en clair (utiliser des fonctions de hachage sécurisées comme bcrypt).
- Valider et filtrer toutes les entrées utilisateur pour éviter les injections (SQL, XSS).

d) Prévenir les vulnérabilités courantes

- Protéger contre les attaques **Injection SQL**, **Cross-Site Scripting (XSS)**, **Cross-Site Request Forgery (CSRF)**.
- Utiliser des frameworks et bibliothèques à jour et reconnues.
- Mettre en place des mécanismes de contrôle d'accès robustes.

e) Assurer la traçabilité et la surveillance

- Logger les actions critiques.
- Mettre en place des alertes en cas d'anomalies.
- Effectuer régulièrement des audits de sécurité et tests d'intrusion.

---

3. Cycle de vie sécurisé du développement (SSDLC)

- Intégrer la sécurité dès la phase de conception.
- Effectuer des revues de code axées sur la sécurité.
- Automatiser les tests de sécurité dans le pipeline CI/CD.
- Assurer la maintenance et les mises à jour régulières.

---

4. Ressources ANSSI utiles pour les développeurs

- Guide d'hygiène informatique
- Recommandations pour le développement sécurisé
- Outils et bonnes pratiques

Conclusion

La sécurité est une responsabilité majeure pour les développeurs web et web mobile.
Appliquer les recommandations de l'ANSSI permet de protéger les utilisateurs, les données et la réputation des entreprises.

> **"La cybersécurité est l'affaire de tous, dès la conception." – ANSSI**