Fiche récap : Sécurisez vos applications web avec le Top 10 OWASP

Systèmes & Réseaux

1. Concevoir un cadre d'exigences de sécurité basé sur l'OWASP Top 10 2025.
2. Identifier les vulnérabilités majeures et leurs mécanismes d'exploitation.
3. Définir des garde-fous de sécurité dès la conception de l'application.
4. Automatiser les contrôles de sécurité dans le cycle de développement.
5. Surveiller, détecter et gérer les incidents en production.

Bonnes pratiques 👍

- ✅ Appliquer le principe du blocage par défaut.
- ✅ Vérifier les autorisations côté serveur.
- ✅ Utiliser des requêtes paramétrées.
- ✅ Chiffrer les données sensibles avec des standards modernes.
- ✅ Générer un SBOM pour suivre les dépendances.
- ✅ Activer l'authentification multifacteur.
- ✅ Journaliser les événements critiques sans données sensibles.
- ✅ Centraliser la gestion des exceptions.

Erreurs classiques 👎

- ❌ Faire confiance aux contrôles du frontend.
- ❌ Utiliser des mots de passe par défaut.
- ❌ Concaténer les entrées dans les requêtes SQL.
- ❌ Stocker les secrets dans le code source.
- ❌ Utiliser MD5 ou SHA1 pour les mots de passe.
- ❌ Exposer des traces d'erreur aux utilisateurs.
- ❌ Journaliser des mots de passe ou des jetons.
- ❌ Autoriser un système à échouer en mode ouvert.
- ❌ Nettoyer manuellement les entrées (blacklisting) au lieu de requêtes paramétrées
- ❌ Installer une mise à jour sans vérifier sa signature numérique.

Définitions 🔍

IDOR
accès à une ressource en modifiant son identifiant sans contrôle serveur.

SSRF
faille où un attaquant force le serveur à émettre des requêtes vers une URL du réseau interne.

SBOM
inventaire complet des composants logiciels d'une application.

Prepared Statement
requête SQL séparant les commandes des données utilisateur.

Threat Modeling
analyse des scénarios d'attaque dès la conception.