Fiche récap : Sécurisez vos applications web avec l'OWASP

Le Top 10 de l'OWASP : liste des dix vulnérabilités les plus critiques pour les applications web.

1. **A01:2021-Contrôles d'accès défaillants**
   Les défaillances dans les contrôles d'accès permettent des accès non autorisés aux fonctionnalités et aux données.

2. **A02:2021-Défaillances cryptographiques**
   Met l'accent sur les erreurs dans la mise en œuvre de la cryptographie qui exposent les données sensibles.

3. **A03:2021-Injection**
   Les vulnérabilités d'injection, y compris les XSS, permettent aux attaquants d'envoyer du code malveillant à l'application.

4. **A04:2021-Conception non sécurisée**
   Souligne l'importance de la sécurisation dès la conception avec des modèles et principes de sécurité.

5. **A05:2021-Mauvaise configuration de sécurité**
   Les configurations par défaut ou incorrectes peuvent exposer l'application à des risques.

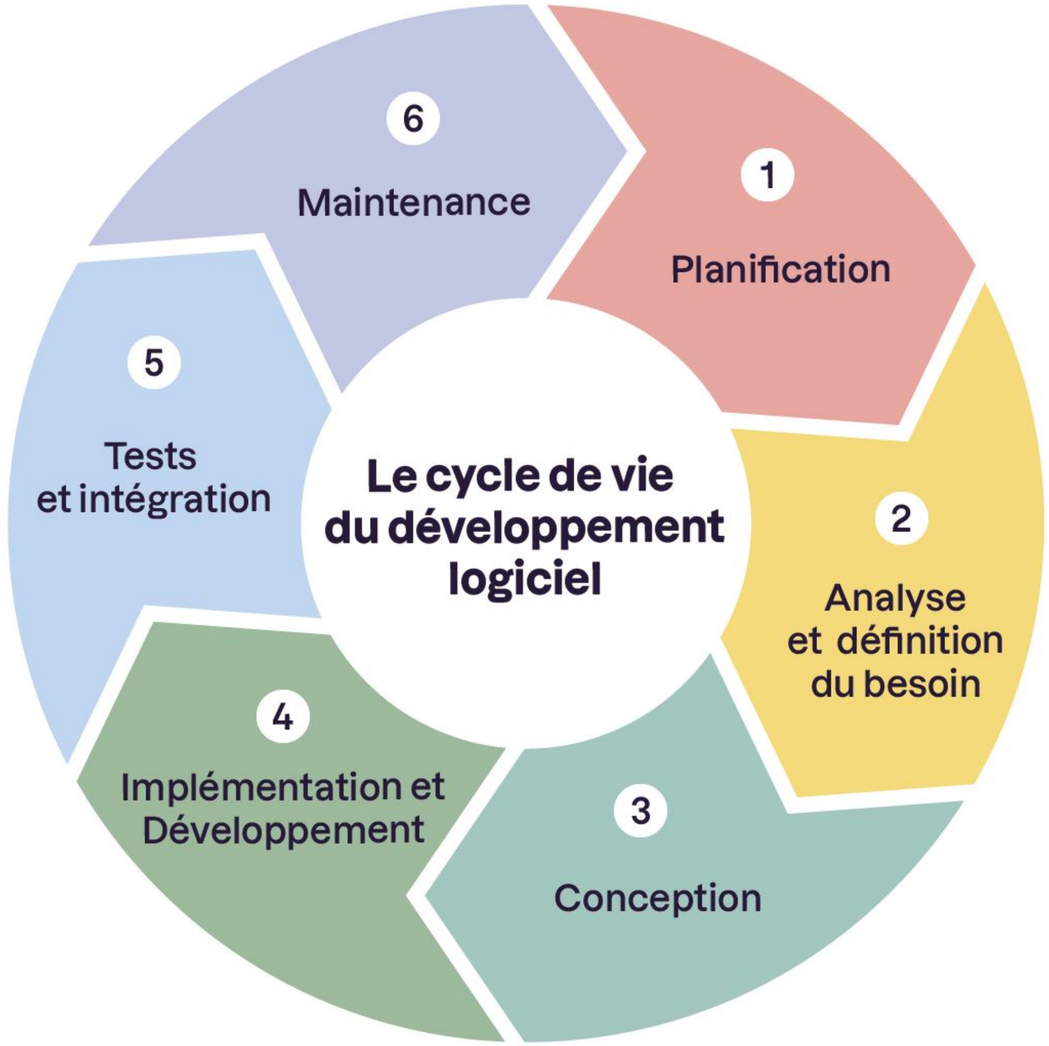
6. **A06:2021-Composants vulnérables et obsolètes**
   L'utilisation de composants avec des vulnérabilités connues met en péril la sécurité de l'application.

7. **A07:2021-Identification et authentification de mauvaise qualité**
   Les faiblesses dans ces processus peuvent permettre aux attaquants d'usurper l'identité d'utilisateurs légitimes.

8. **A08:2021-Manque d'intégrité des données et du logiciel**
   L'absence de vérification de l'intégrité des mises à jour et des données critiques peut entraîner des compromissions.

9. **A09:2021-Carence des systèmes de contrôle et de journalisation**
   Le manque de surveillance et de journalisation adéquates limite la capacité à détecter et à répondre aux incidents de sécurité.

10. **A10:2021-Falsification de requête côté serveur**
    Permet aux attaquants d'induire en erreur l'application pour accéder ou manipuler des informations côté serveur.



Fiche récap : Sécurisez vos applications web avec l'OWASP

Définitions

OWASP (Open Web Application Security Project)
Fondation travaillant à l'amélioration de la sécurité des logiciels.

RGPD (Règlement Général sur la Protection des Données)
Réglementation européenne sur la protection des données personnelles.

HDS (Hébergement de Données de Santé)
Certification française pour la sécurité des données de santé.

PCI-DSS (Payment Card Industry Data Security Standard)
Norme pour sécuriser les transactions par carte bancaire.

ASVS (Application Security Verification Standard)
Cadre de référence pour la sécurité des applications web.

WSTG (Web Security Testing Guide)
Guide pour le test de sécurité des applications web.

ZAP (Zed Attack Proxy)
Outil de test de sécurité pour identifier les vulnérabilités dans les applications web.

Injection SQL
Technique d'attaque exploitant des failles de sécurité dans la gestion des entrées SQL.

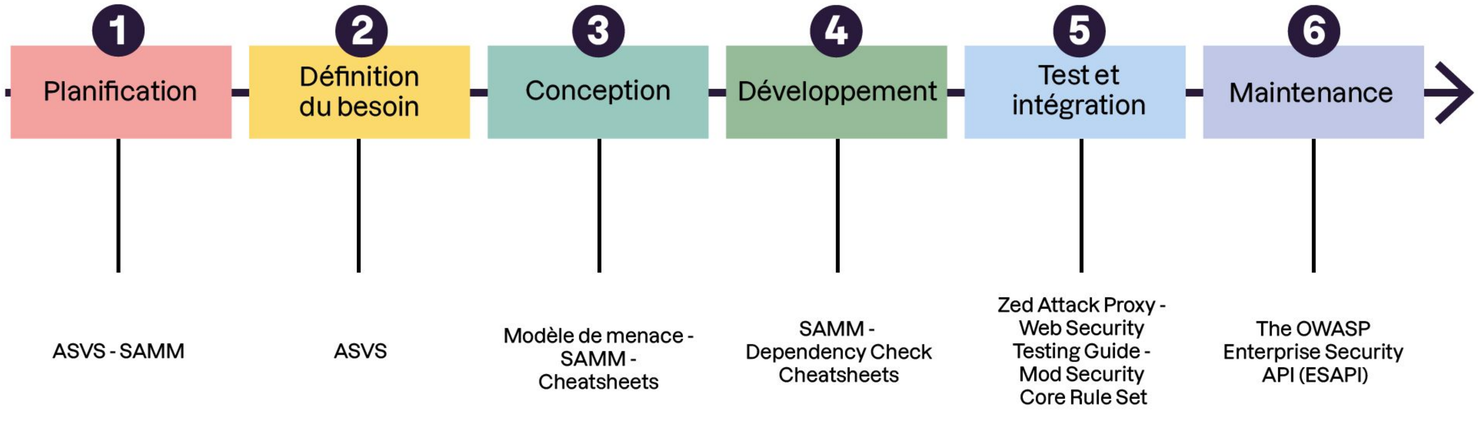
Cross-Site Scripting (XSS)
Type d'attaque qui injecte des scripts malveillants dans des sites web.

Cross-Site Request Forgery (CSRF)
Attaque qui force l'utilisateur à exécuter des actions non souhaitées dans une application web où il est authentifié.

Authentification Forte
Méthode d'authentification nécessitant plusieurs facteurs pour vérifier l'identité d'un utilisateur.

Chiffrement
Processus de conversion des données en un format codé pour prévenir l'accès non autorisé.

Salage
Technique ajoutant une donnée aléatoire au mot de passe avant son hachage pour renforcer la sécurité.



Ressources

- OWASP Top 10
- OWASP Application Security Verification Standard (ASVS)
- OWASP Software Assurance Maturity Model (SAMM)
- OWASP Security Knowledge Framework
- OWASP Cheatsheet Series
- OWASP Dependency Check
- OWASP Dependency Track
- OWASP Zed Attack Proxy (ZAP)
- OWASP Web Security Testing Guide