

L'entrée A04:2021 dans le OWASP Top 10 est **Conception sécurisée**. Cette catégorie met l'accent sur l'importance de l'intégration des pratiques de sécurité dès le début du cycle de développement des applications, afin de prévenir les vulnérabilités avant qu'elles ne surviennent.

Points Clés sur A04:2021 Conception Sécurisée :

- **Principes de Conception Sécurisée :**
 - **Sécurité par Conception** : Incorporer des mécanismes de sécurité dès la phase de conception.
 - **Sécurité par Défaut** : Configurer les systèmes pour qu'ils soient sécurisés par défaut, avec des options permettant de renforcer la sécurité.
 - **Modélisation des Menaces** : Identifier et analyser les menaces potentielles dès le début.
 - **Principe du Moindre Privilège** : Restreindre les permissions et l'accès aux ressources au minimum nécessaire.
- **Risques :**
 - **Faillles Architecturales** : Les failles dans la conception peuvent entraîner des vulnérabilités difficiles à corriger après coup.
 - **Complexité de la Sécurité** : Plus la sécurité est ajoutée tardivement, plus elle peut être complexe et coûteuse à implémenter.
 - **Manque de Résilience** : Les systèmes conçus sans une bonne base de sécurité peuvent être moins résilients face aux attaques.
- **Mesures Préventives :**
 - **Revue de la Conception** : Effectuer des revues régulières de la conception pour identifier les failles potentielles.
 - **Tests de Sécurité** : Intégrer des tests de sécurité tout au long du cycle de développement, pas seulement à la fin.
 - **Formation** : Former les développeurs aux pratiques de conception sécurisée.
 - **Outils et Frameworks** : Utiliser des outils et des frameworks qui encouragent les bonnes pratiques de sécurité.
- **Scénario d'Exemple :**
 - Lors de la conception d'une application de gestion financière, une modélisation des menaces peut révéler des scénarios d'attaques potentielles comme l'injection SQL ou les attaques par déni de service. En intégrant des mécanismes tels que des requêtes paramétrées et des contrôles de débit dès la phase de conception, ces menaces peuvent être atténuées avant que l'application ne soit développée.

Référence :

- OWASP Top 10 - 2021 : [OWASP Top 10](#)