L'entrée A05:2021 dans le OWASP Top 10 est **Mauvaise configuration de sécurité**. Cette catégorie englobe toutes les vulnérabilités résultant de configurations incorrectes ou non sécurisées des applications, des serveurs et des bases de données.

Points Clés sur A05:2021 Mauvaise Configuration de Sécurité :

- **Exemples de Mauvaise Configuration** :
  - **Configurations Par Défaut** : Utilisation de paramètres par défaut qui peuvent être facilement devinés ou exploités.
  - **Messages d'Erreur Verbeux** : Messages d'erreur détaillés qui divulguent des informations sensibles.
  - **Serveurs Non Sécurisés** : Serveurs avec des ports ouverts ou des services non nécessaires activés.
  - **Permissions Excessives** : Comptes et services disposant de permissions plus élevées que nécessaire.
- **Risques** :
  - **Exposition de Données Sensibles** : Informations sensibles accessibles à des utilisateurs non autorisés.
  - **Compromission de Systèmes** : Les systèmes peuvent être compromis en raison de paramètres non sécurisés.
  - **Exploitation des Failles** : Les configurations incorrectes peuvent être exploitées pour lancer des attaques plus complexes.
- **Mesures Préventives** :
  - **Revue de Sécurité** : Effectuer des revues régulières des configurations de sécurité.
  - **Automatisation** : Utiliser des outils d'automatisation pour gérer et vérifier les configurations.
  - **Principes du Moindre Privilège** : Limiter les permissions des comptes et des services.
  - **Hardening** : Renforcer les serveurs et les applications en désactivant les fonctionnalités inutiles et en appliquant des configurations sécurisées.
- **Scénario d'Exemple** :
  - **Exemple de Base de Données** : Une base de données pourrait être laissée avec son mot de passe administrateur par défaut, tel que "admin" ou "password". Un attaquant pourrait facilement deviner ce mot de passe et accéder à la base de données, volant ainsi des informations sensibles ou modifiant des données critiques.
- **Bonnes Pratiques** :
  - **Gestion des Patches** : Maintenir tous les systèmes à jour avec les dernières mises à jour de sécurité.
  - **Tests de Pénétration** : Effectuer des tests de pénétration pour identifier et corriger les configurations non sécurisées.
  - **Surveillance** : Mettre en place une surveillance continue pour détecter les configurations vulnérables et les corriger rapidement.

Référence :

- OWASP Top 10 - 2021 : OWASP Top 10