L'entrée A06:2021 dans le OWASP Top 10 est **Composants vulnérables et obsolètes**. Cette catégorie met en lumière les risques liés à l'utilisation de composants logiciels qui présentent des vulnérabilités connues ou qui ne sont plus maintenus par leurs développeurs.

Points Clés sur A06:2021 Composants Vulnérables et Obsolètes :

- **Sources de Vulnérabilités** :
  - **Librairies et Frameworks** : Utilisation de librairies et frameworks contenant des failles de sécurité connues.
  - **Composants Non Mis à Jour** : Composants logiciels qui ne sont pas mis à jour avec les derniers patches de sécurité.
  - **Composants Obsolètes** : Utilisation de composants qui ne sont plus supportés par les développeurs et pour lesquels il n'y a plus de mises à jour de sécurité.
- **Risques** :
  - **Compromission du Système** : Les vulnérabilités dans les composants peuvent être exploitées pour prendre le contrôle du système.
  - **Exposition des Données** : Accès non autorisé à des données sensibles via des composants vulnérables.
  - **Propagation des Vulnérabilités** : Une faille dans un composant peut entraîner une cascade de vulnérabilités dans l'ensemble du système.
- **Mesures Préventives** :
  - **Gestion des Dépendances** : Maintenir une liste à jour de toutes les dépendances et de leurs versions.
  - **Mises à Jour Régulières** : Appliquer régulièrement les mises à jour et patches de sécurité pour tous les composants utilisés.
  - **Scanner de Vulnérabilités** : Utiliser des outils de scan de vulnérabilités pour identifier les composants à risque.
  - **Politique de Sécurité des Composants** : Adopter des politiques strictes pour l'utilisation de composants externes, y compris la vérification de leur sécurité et de leur support.
- **Scénario d'Exemple** :
  - **Exemple de Librairie JavaScript** : Une application web utilise une librairie JavaScript populaire mais obsolète, connue pour avoir une faille de sécurité critique. Un attaquant peut exploiter cette faille pour injecter du code malveillant, compromettant ainsi la sécurité de l'application et de ses utilisateurs.
- **Bonnes Pratiques** :
  - **Inventaire des Composants** : Maintenir un inventaire détaillé de tous les composants et leurs versions.
  - **Surveillance des Annonces de Sécurité** : Suivre les annonces de sécurité des fournisseurs de composants pour être informé des nouvelles vulnérabilités.

    - **Tests de Sécurité** : Intégrer des tests de sécurité dans le cycle de développement pour détecter les composants vulnérables avant le déploiement.

Référence :

- OWASP Top 10 - 2021 : OWASP Top 10