L'entrée A03:2021 dans le OWASP Top 10 est **Injection**. Cette catégorie englobe diverses formes d'attaques par injection où des données non fiables sont envoyées à un interpréteur comme partie d'une commande ou d'une requête. Ces injections peuvent se produire dans divers contextes tels que SQL, NoSQL, OS et LDAP.

Points Clés sur A03:2021 Injection :

- **Formes Communes** :
  - **Injection SQL** : Où du code SQL malveillant est inséré dans une requête.
  - **Injection NoSQL** : Similaire à l'injection SQL, mais cible les bases de données NoSQL.
  - **Injection de Commandes OS** : Où un attaquant peut exécuter des commandes arbitraires sur le système d'exploitation hôte.
  - **Injection LDAP** : Implique l'insertion de déclarations LDAP malveillantes.
- **Risques** :
  - **Violation de Données** : Accès non autorisé à des données sensibles.
  - **Perte/Manipulation de Données** : Modification ou suppression de données.
  - **Compromission du Système** : Contrôle potentiel total sur le système.
- **Mesures Préventives** :
  - **Validation des Entrées** : Valider et nettoyer toutes les entrées.
  - **Requêtes Paramétrées/Instructions Préparées** : Utilisez-les pour empêcher l'insertion directe de l'entrée utilisateur dans les requêtes.
  - **Procédures Stockées** : Utilisez-les au lieu des requêtes dynamiques.
  - **Échappement** : Échapper correctement les caractères spéciaux dans les entrées.
  - **Principe du Moindre Privilège** : Assurez-vous que l'application dispose des permissions minimales nécessaires.
- **Scénario d'Exemple** :
  - **Injection SQL** :

```
SELECT * FROM users WHERE username = 'utilisateur' AND password =
'motdepasse';
```

Si l'entrée n'est pas correctement nettoyée, un attaquant pourrait saisir `utilisateur' OR '1'='1`, menant à :

```
SELECT * FROM users WHERE username = 'utilisateur' OR '1'='1' AND
password = 'motdepasse';
```

Cette requête renverra toujours vrai, exposant potentiellement toutes les données utilisateur.

Référence :

- OWASP Top 10 - 2021 : OWASP Top 10