**Nom de l'application : VulnScan AI**

**Objectif principal :**

Prédire la probabilité qu'un système informatique soit vulnérable à une cyberattaque, en se basant sur des caractéristiques du système et des indicateurs de sécurité.

**Description :**

**VulnScan AI** analyse les données d'un système informatique et prédit sa vulnérabilité en fonction de plusieurs facteurs, comme la configuration du système, l'historique des mises à jour, et les types de logiciels installés. La régression logistique est utilisée pour calculer une probabilité de vulnérabilité (entre 0 et 1), permettant aux administrateurs système de prioriser les actions correctives.

**Caractéristiques du système (Features) :**

1. **Version du système d'exploitation** (obsolète ou récente).
2. **Nombre de ports ouverts** (faible ou élevé).
3. **Fréquence des mises à jour logicielles** (régulière ou irrégulière).
4. **Type d'antivirus utilisé** (robuste ou basique).
5. **Présence de pare-feu actif** (oui ou non).
6. **Nombre d'utilisateurs ayant des privilèges administratifs**.
7. **Historique des attaques précédentes** (aucune, faible, ou élevée).
8. **Complexité des mots de passe** (faible ou élevée).
9. **Nombre de vulnérabilités connues non corrigées**.

**Fonctionnement :**

1. **Collecte des données** :
   * Les informations sont collectées à l'aide d'un agent installé sur les systèmes cibles ou via des scans réseau.
   * Ces données sont ensuite stockées dans une base de données centralisée.
2. **Modèle de régression logistique** :
   * Entraîné sur un ensemble de données contenant des systèmes étiquetés comme vulnérables (1) ou non vulnérables (0).
   * Le modèle apprend les relations entre les caractéristiques du système et sa probabilité de vulnérabilité.
3. **Prédiction** :
   * Pour chaque système scanné, l'application génère une probabilité de vulnérabilité.
   * Par exemple : *"Ce système a une probabilité de 85% d'être vulnérable."*
4. **Interface utilisateur** :
   * Une interface visuelle montre la liste des systèmes avec leur niveau de vulnérabilité.
   * Les systèmes les plus à risque sont mis en évidence pour une action immédiate.

**Cas d'utilisation :**

* **Administrateurs système** : Identifier rapidement les systèmes les plus vulnérables pour appliquer des correctifs.
* **Auditeurs de sécurité** : Évaluer la sécurité globale d'une infrastructure informatique.
* **Développeurs de logiciels** : Tester les vulnérabilités liées à la configuration des applications.

**Fonctionnalités supplémentaires :**

* **Suggestions automatisées** : Fournir des recommandations spécifiques pour réduire la vulnérabilité (par exemple, "fermer les ports inutiles", "mettre à jour l'antivirus").
* **Rapports périodiques** : Générer des rapports hebdomadaires ou mensuels sur l'état de la sécurité.
* **Notifications** : Alertes en temps réel pour les systèmes avec une vulnérabilité critique.

**Exemple d'implémentation technique :**

1. Collecter les données avec des bibliothèques comme **psutil**, **shodan**, ou **osquery**.
2. Construire et entraîner le modèle avec **Scikit-learn** ou **TensorFlow**.
3. Intégrer le modèle dans une application web ou un tableau de bord interactif avec **Flask** ou **Django**.
4. Représenter visuellement les résultats avec **Plotly**, **Dash**, ou **Matplotlib**.

**Impact :**

L'application peut aider les organisations à réduire les risques liés à la cybersécurité en fournissant un outil prédictif simple, basé sur des données réelles et des algorithmes éprouvés.