Détection des Injections SQL sur les Plateformes E-commerce avec un Modèle de Machine Learning

Par Malisuku Cecile Dayanah

Université Nouveaux Horizons

September 5, 2024

Sommaire

Introduction

Avec l'évolution rapide des plateformes e-commerce, la sécurité des données devient une priorité absolue. Les attaques d'injection SQL (SQLi) figurent parmi les menaces les plus sérieuses auxquelles ces plateformes doivent faire face.

J'ai développé un modèle de machine learning utilisant l'algorithme de Random Forest pour détecter les tentatives d'injection SQL. Le modèle a été évalué à l'aide de plusieurs indicateurs de performance.

Problèmes posés par les injections SQL

- **Vol de données sensibles :** Les informations bancaires, adresses et autres données personnelles peuvent être volées.
- **Modification ou suppression des données :** Les attaquants peuvent altérer ou supprimer des informations critiques.
- **Conséquences légales et réglementaires :** Les violations peuvent entraîner des amendes importantes, comme celles liées au RGPD.

Modèle de détection basé sur Random Forest

Le modèle de machine learning s'appuie sur l'algorithme Random Forest, capable de traiter des ensembles de données déséquilibrés et d'identifier des patterns complexes.

Métriques de performance analysées :

- Courbe Précision-Rappel
- Courbe ROC et AUC
- Matrice de Confusion
- Accuracy et F1 Score

Courbe Précision-Rappel

- **Équilibre :** La courbe se rapproche du coin supérieur droit, montrant un bon équilibre entre précision et rappel.
- **Précision de 1 :** Le modèle prédit correctement les injections SQL dans la majorité des cas.
- **Chute de précision :** À des seuils de rappel élevés, plus de faux positifs apparaissent.

Courbe ROC et AUC

- La courbe ROC se rapproche du coin supérieur gauche, indiquant une bonne performance.
- L'AUC de 0.97 montre une excellente capacité du modèle à distinguer les requêtes légitimes des injections SQL.

Matrice de Confusion

- **Vrais négatifs (TN) :** 3720 requêtes légitimes correctement classées.
- **Faux positifs (FP) :** 162 requêtes légitimes incorrectement classées comme injections SQL.
- **Faux négatifs (FN) :** 255 injections SQL non détectées.
- **Vrais positifs (VP) :** 1985 injections SQL correctement détectées.

Accuracy et F1 Score

- **Accuracy :** 93% des requêtes ont été correctement classées.
- **F1 Score :** 0.90, indiquant un bon équilibre entre précision et rappel.

Conclusion

Le modèle basé sur Random Forest a montré des performances solides, avec une AUC de 0.97 et un F1 Score de 0.90, démontrant sa capacité à détecter les injections SQL tout en minimisant les faux positifs.

Annexe

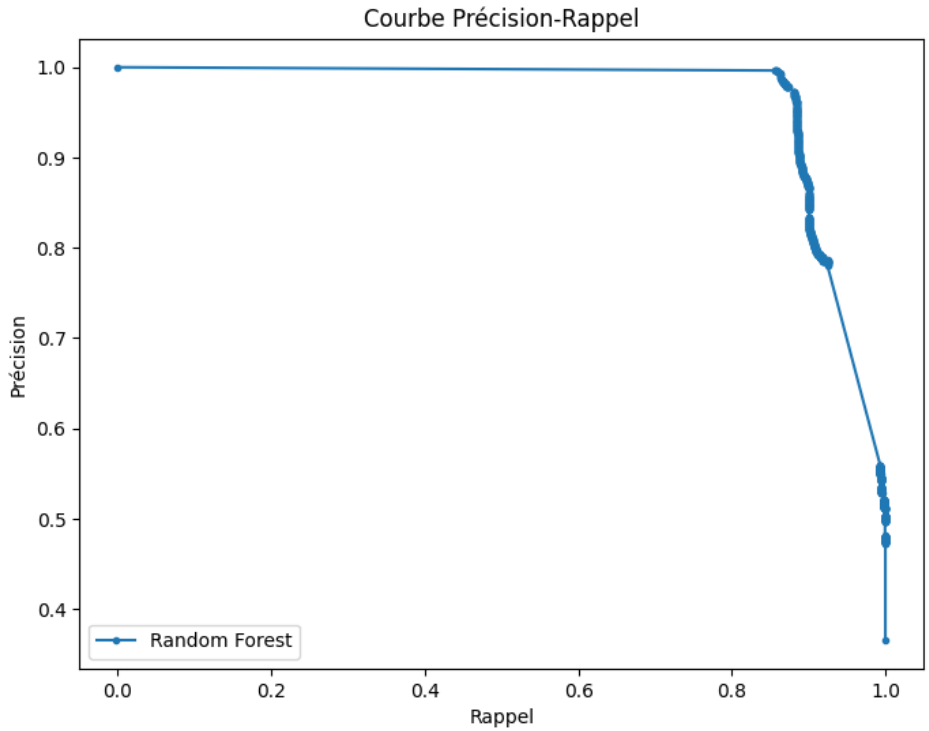

Figure: Courbe Précision-Rappel du modèle Random Forest

Annexe

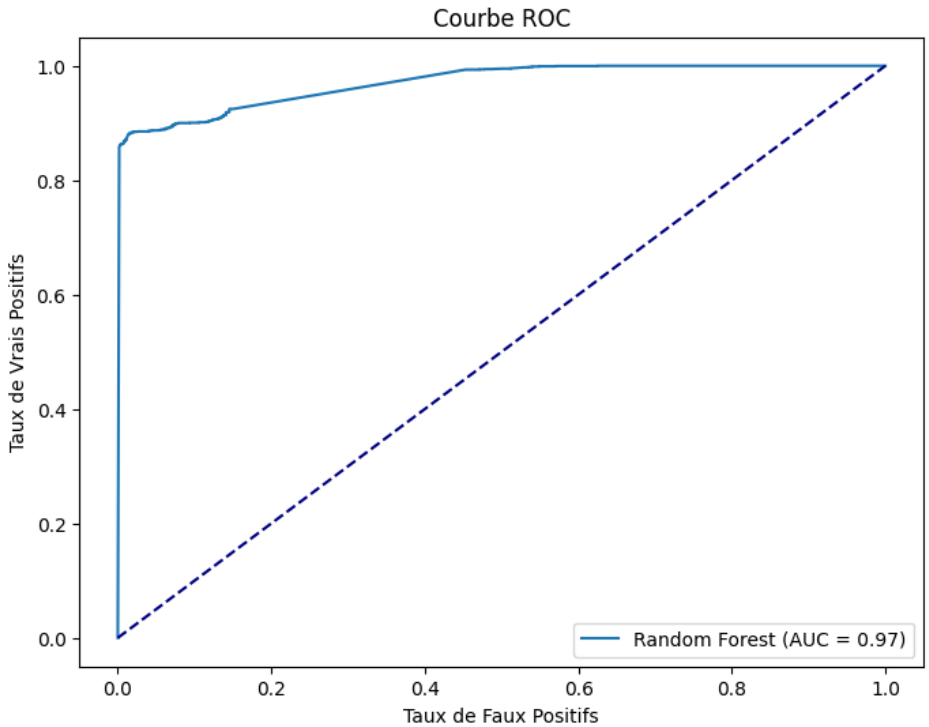

Figure: Courbe ROC du modèle Random Forest

Annexe

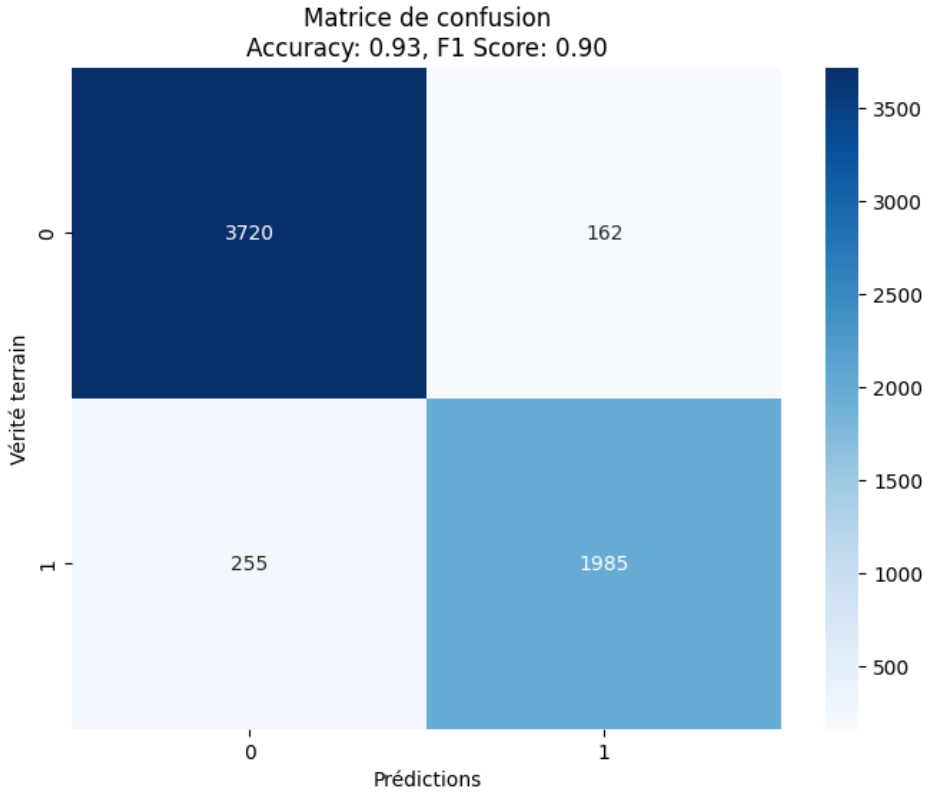

Figure: Matrice de confusion du modèle Random Forest