HỆ THỐNG PHÁT HIỆN TẤN CÔNG TIÊM NHIỄM SQL SỬ DỤNG BERT VÀ CÁC KỸ THUẬT MÁY HỌC

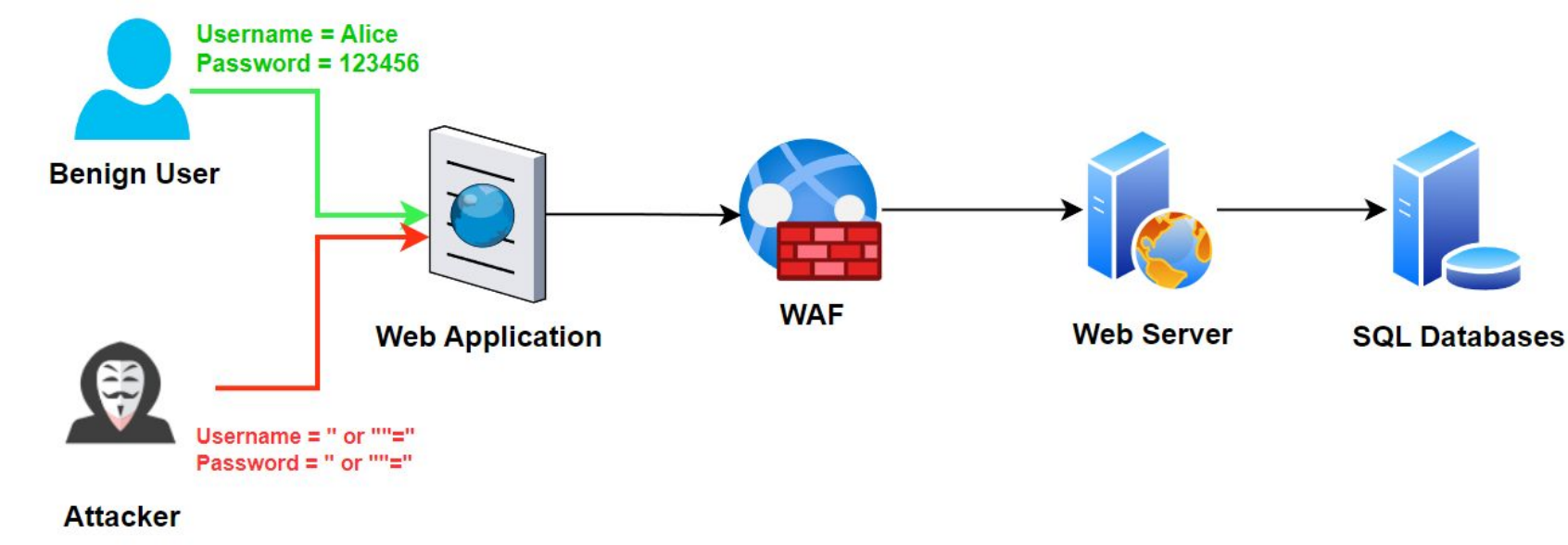
Lê Tuấn Anh - 230202001

Tóm tắt

- Lớp: CS2205.CH181
- Link Github: https://github.com/tuananh8232/CS2205.CH181
- Link YouTube video: https://youtu.be/AmMtdnIGm98
- Họ và Tên: Lê Tuấn Anh - 230202001

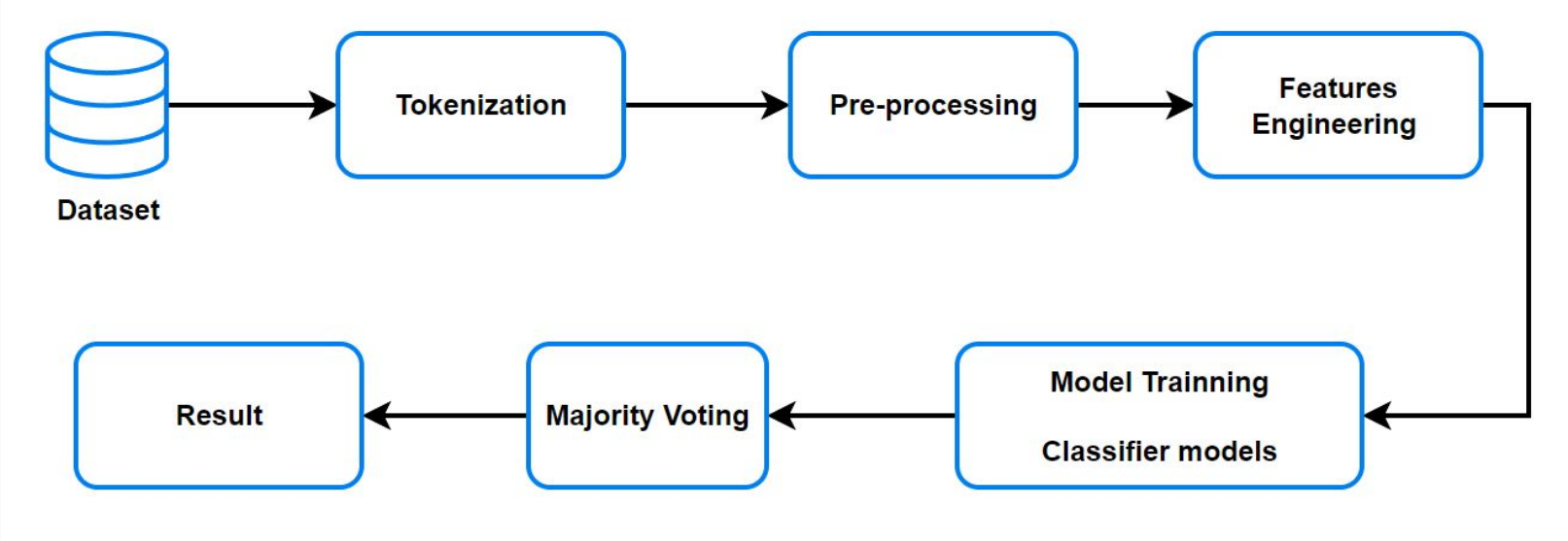
Giới thiệu

- Mô phỏng cuộc tấn công SQLi



Giới thiệu

- Mô hình đề xuất



Mục tiêu

- Nghiên cứu về mô hình BERT và các mô hình phân loại máy học, kết hợp được các mô hình với nhau, áp dụng được vào bài toán phát hiện tấn công SQLi.
- Tạo ra được mô hình phát hiện tấn công SQLi với độ chính xác và hiệu suất tốt, đáp ứng được yêu cầu của bài toán đặt ra nhưng cũng đảm bảo về độ chính xác cũng như hiệu năng của mô hình.
- Đưa ra các so sánh, đánh giá với các phương pháp hiện có.

Nội dung và Phương pháp

Nội dung

- Nghiên cứu về một số hình thức tấn công Web phổ biến, tấn công SQLi.
- Nghiên cứu về mô hình BERT, các mô hình phân loại máy học Naive Bayes, SVM, XGBoost, các kĩ thuật Majority Voting, Random Search.
- Nghiên cứu, tìm ra phương pháp áp dụng, kết hợp các mô hình đã đề xuất áp dụng vào bài toán. Xây dựng được kiến trúc mô hình.
- Thu thập dataset về tấn công SQLi.Huấn luyện mô hình, đánh giá mô hình.
- Xây dựng hệ thống phát hiện tấn công SQLi dựa trên mô hình đã huấn luyện được.

Nội dung và Phương pháp

Phương pháp

- Tìm hiểu cơ chế, kiến trúc của các mô hình BERT, các mô hình phân loại máy học: Naive Bayes, SVM, XGBoost, các kĩ thuật Majority Voting, Random Search.
- Khảo sát tổng luận, tìm hiểu về các nghiên cứu liên quan qua các nguồn tạp chí, hội nghị uy tín.
- Thu thập dữ liệu, tìm hiểu các bộ dữ liệu từ Kaggle, đánh giá, tiền xử lý dữ liệu cho phù hợp với Input của mô hình.

Nội dung và Phương pháp

Phương pháp(tt)

- Thực hiện xây dựng kiến trúc mô hình, huấn luyện mô hình trên tập dữ liệu đã thu thập, thực hiện tinh chỉnh mô hình, tối ưu tham số nhằm cải thiện độ chính xác. Đánh giá mô hình thông qua các thông số như: Accuracy, Precision, Recall, F1 score, Confusion Matrix.
- So sánh tính hiệu quả so với các phương pháp, nghiên cứu liên quan, đưa ra đánh giá, kết luận.
- Phát triển hệ thống thử nghiệm với mô hình đã huấn luyện được.

Kết quả dự kiến

- Báo cáo về kiến trúc, kỹ thuật, và phương pháp áp dụng vào bài toán của các mô hình đã sử như BERT, các mô hình phân loại máy học Naive Bayes, SVM, XGBoost và các kỹ thuật Majority Voting, Random Search.
- Kết quả thực nghiệm, đánh giá, kết luận và so sánh giữa phương pháp đã thực nghiệm với các phương pháp khác.
- Hệ thống phát hiện tấn công SQLi sử dụng mô hình đã thử nghiệm.

Tài liệu tham khảo

[1]. Ignacio Samuel Crespo-Martínez, Adrián Campazas Vega, Ángel Manuel Guerrero-Higueras, Virginia Riego-Del Castillo, Claudia Álvarez-Aparicio, Camino Fernández Llamas: SQL injection attack detection in network flow data. Comput. Secur. 127: 103093 (2023)

[2]. Chen, Yuhong, et al. "Request-Response Network Traffic Packets: Enhancing SQL Injection Attack Detection with a Transformer-Based Model." 2023 9th International Conference on Computer and Communications (ICCC). IEEE, 2023.

[3]. Kasim Tasdemir, Rafiullah Khan, Fahad Siddiqui, Sakir Sezer, Fatih Kurugollu, Sena Busra Yengec-Tasdemir, Alperen Bolat: Advancing SQL Injection Detection for High-Speed Data Centers: A Novel Approach Using Cascaded NLP. CoRR abs/2312.13041 (2023)

[4]. Janet Zulu, Bonian Han, Izzat Alsmadi, Gongbo Liang: Enhancing Machine Learning Based SQL Injection Detection Using Contextualized Word Embedding. ACM Southeast Regional Conference 2024: 211-216