1. Pendahuluan

1.1 Latar Belakang

Serangan SQL Injection, seperti yang didefinisikan oleh OWASP (Open Web Application Security Project), dilakukan dengan menyisipkan atau "menyuntikkan" kueri SQL melalui input data dari klien ke aplikasi. Eksploitasi yang berhasil dari serangan SQL Injection dapat menimbulkan banyak hasil yang merugikan, termasuk pengungkapan data sensitif yang tidak sah yang berada di dalam database, perubahan yang tidak sah dari konten database melalui tindakan seperti penyisipan, pembaruan, atau penghapusan catatan, eksekusi operasi administratif pada database (seperti memulai shutdown DBMS), pengambilan konten file tertentu dari sistem file yang mendasari DBMS, dan, dalam keadaan tertentu, eksekusi perintah yang menargetkan sistem operasi. [1].

Serangan injeksi SQL dapat diklasifikasikan ke dalam kategori yang berbeda berdasarkan beberapa faktor, tetapi faktor yang komprehensif dan umum adalah tujuan penyerang dan mekanisme injeksi yang dilakukan [2]. Oleh karena itu, perlu untuk menentukan tingkat serangan, baik untuk mendeteksi jenis serangan SQL Injection yang berbeda dan untuk pertahanan yang fleksibel terhadapnya [3]. Salah satu metodenya adalah dengan mengklasifikasikan serangan SQL Injection yang teramati menggunakan machine learning khususnya algoritma klasifikasi.

Algoritma Support Vector Machine (SVM) memiliki dasar teori yang kuat dan catatan kinerja empiris yang mengesankan. Mereka tampaknya lebih mudah ditafsirkan daripada jaringan syaraf tiruan dan telah digunakan dalam berbagai masalah klasifikasi, termasuk pengenalan angka tulisan tangan, pengenalan objek, dan klasifikasi teks. Karena kinerjanya yang relatif kuat dalam berbagai domain, mesin vektor pendukung digunakan secara luas [4]. Dengan mengimplementasikan algoritma klasifikasi, diyakini bahwa pencegahan serangan injeksi SQL dapat ditingkatkan ka.

1.2 Topik dan Batasannya

Penelitian ini akan berfokus pada pendeteksian dan pengklasifikasian SQL Injection, sistem yang akan dibangun akan mendeteksi dan mengklasifikasikan SQL injection dalam 5 kelas, yaitu Union based, Error based, Boolean based, Time based dan yang tidak tergolong menjadi SQL Injection menggunakan ensemble learning SVM dan Naïve Bayes.

Batasan dari penelitian ini hanya berfokus pada pendeteksian dan pengklasifikasian menjadi 5 kelas yang telah disebutkan pada paragaf sebelumnya. Dataset yang digunakan berasal dari Kaggle dan payload SQL yang digunakan dalam *Penetration Testing.*

1.3 Tujuan

Penelitian ini bertujuan untuk mendeteksi injeksi SQL menggunakan algoritma machine learning, khususnya Support Vector Machine (SVM) dan Nave Bayes. Pembelajaran mesin yang dievaluasi dimulai dengan SVM dan Naive Bayes yang berdiri sendiri, serta gabungan dari kedua metode tersebut.

1.4 Organisasi Tulisan

Struktur berikut ini merupakan pembahasan dari penelitian yang disajikan pada penelitian berbasis machine learning untuk mendeteksi serangan SQL Injection. Beberapa investigasi penelitian sebelumnya mengenai penggunaan teknik berbasis machine learning untuk mendeteksi SQL injection dijelaskan pada Bab 2. Metodologi dan desain model pembelajaran mesin dibahas pada Bab 3. Hasil dan diskusi dari penelitian ini, serta kesimpulan yang diambil dari seluruh kegiatan penelitian, disajikan pada Bab 4 dan 5.