BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan merupakan salah satu aspek yang sangat penting dari sebuah sistem informasi. Keamanan komputer adalah sebuah tindakan pencegahan yang dilakukan untuk melindungi sebuah sistem dari serangan yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab. Tanpa keamanan yang baik, maka data-data pengguna belum dapat dikatakan aman. Hal tersebut pastinya akan mempengaruhi kepercayaan pengguna dalam menggunakan sistem tersebut.

Di era teknologi informasi saat ini, sistem memiliki peran yang besar bagi perusahaan ataupun institusi, baik untuk mendapatkan keuntungan secara finansial maupun untuk memberikan pelayanan yang baik kepada pengguna sistem. Hal tersebut membuat perusahaan-perusahaan maupun instansi bersaing dalam menyediakan layanan terbaik. Namun, seringkali yang menjadi prioritas mereka adalah tampilan sistem dan layanan yang dapat memikat pengguna dengan cepat, sedangkan masalah keamanan berada diurutan bawah atau tidak dianggap begitu penting.

Padahal keamanan data sangat dibutuhkan untuk menjaga dan melindungi privasi pengguna. Ketika data privasi pengguna bocor atau jatuh ke tangan pihak-pihak yang tidak bertanggung jawab, maka rasa kepercayaan pengguna terhadap penyedia layanan pun akan runtuh. Banyak peristiwa yang telah terjadi terkait peretasan atau pembobolan sistem karena minimnya perhatian penyedia layanan terhadap keamanan sistem tersebut, seperti kasus peretasan yang terjadi pada situs Komisi Pemilihan Umum (KPU) Kota Yogyakarta yang terjadi pada bulan Februari 2017 dan kasus peretasan situs Telkomsel yang terjadi beberapa bulan lalu.

Salah satu sistem yang umumnya menjadi sasaran hacker dan cracker adalah aplikasi berbasis website. Hal tersebut dikarenakan pemanfaatan aplikasi mengalami pertumbuhan yang sangat pesat saat ini. Hacker adalah

seseorang yang melakukan peretasan dengan mencari celah keamanan dari sebuah sistem, kemudian memberikan gagasan dan solusi kepada administrator sistem bila terdapat celah keamanan. Sedangkan cracker adalah seseorang yang melakukan peretasan dengan mencari celah keamanan dari sebuah sistem, kemudian menggunakan celah tersebut untuk kepentingan individu seperti mencuri data, menghapus data, merusak data, dan melakukan hal-hal lain yang merugikan pemilik sistem.

Banyak jenis serangan yang umumnya digunakan untuk mencari celah keamanan pada sebuah website. Beberapa jenis serangan tersebut diantaranya SQL Injection, SQL Injection merupakan jenis serangan yang dilakukan dengan cara memodifikasi perintah SQL. Berdasarkan dokumen OWASP (Open Web Application Security Project) tentang 10 risiko keamanan aplikasi website yang paling kritis, serangan SQL Injection berada di posisi teratas. Di Indonesia, teknik ini pun pernah digunakan oleh seorang hacker dengan kode nama "Xnuxer" untuk melakukan peretasan pada hasil Tabulasi Nasional Pemilu (TNP) KPU. Dengan menggunakan teknik SQL Injection, "Xnuxer" berhasil mengubah nama-nama partai peserta Pemilu menjadi Partai Jambu, Partai Nanas, dan nama-nama asal lainnya.

Maka dari itu untuk menjaga keamanan website, perlu dilakukan pengujian aplikasi secara teratur. Ini penting karena jika tidak ada pengujian rutin, tidak ada jaminan bahwa situs tersebut akan aman dan terlindungi dari serangan dalam jangka panjang. Oleh karena itu dengan dilakukan nya penyusunan skripsi ini untuk melakukan perencanaan aplikasi untuk mendeteksi script yang ada terhadap serangan SQL Injection didunia maya.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, perumusan masalah penelitian pada "Aplikasi Deteksi *Cyber Attack* SQL Injection menggunakan Algoritma *Support Vector Machine"* adalah bagaimana membangun system dan mengimplementasikan program atau data dengan algoritma *Support Vector Machine* (SVM)?.

1.3 Batasan Masalah

Agar pengerjaan lebih terarah, dalam penelitian pada "Aplikasi Deteksi *Cyber Attack* SQL Injection menggunakan Algoritma *Support Vector Machine"* terdapat beberapa batasan masalah, diantaranya sebagai berikut:

1. Data masukan yang diterima oleh aplikasi berupa Payloads / Script
2. Proses yang terdapat didalam aplikasi diantaranya jenis virus SQL Injection
3. Hasil keluaran yang akan dihasilkan berupa akurasi dan informasi terkait SQL Injection
4. Target yang dijadikan bahan untuk uji coba telah ditentukan.

Oleh karena itu maka aplikasi yang penulis ajukan adalah sebagai tugas akhir skripsi.

1.4 Tujuan Penelitian

Adapun tujuan yang ingin dicapai pada penelitian ini yaitu membangun aplikasi deteksi serangan cyber SQL Injection menggunakan algoritma Support Vector Machine (SVM) yang dapat mendeteksi data website yang telah dikumpulkan menggunakan *Support Vector Machine Classifier* yang efektif dan efisien serta dapat mengetahui keluaran berupa virus SQL Injection dan dapat membedakannya jika bukan termasuk virus SQL Injection.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah untuk membuat "Aplikasi Deteksi *Cyber Attack SQL Injection* menggunakan *Algoritma Support Vector Machine."* adalah sebagai berikut:

1. Terkumpulnya data - data dari konten website yang mengandung unsur virus cyber attack sql injection yang diterbitkan secara daring untuk dipelajari dan di uji coba
2. Membantu admin dalam mendeteksi dan menganalisa terhadap konten atau kata – kata yang mencurigakan melalui website yang mengandung sql injection dan non-sql injection

3. Tidak perlu mengeluarkan biaya lebih untuk menyewa penyedia jasa keamanan sistem.
4. Menghasilkan informasi mengenai sql injection detection.

1.6 Sistematika Penelitian

Untuk mempermudah melihat dan mengetahui pembahasan yang ada pada skripsi ini secara menyeluruh, maka perlu dikemukakan sistematika pembahasan. Adapun sistematika pembahasannya adalah sebagai berikut:

BAB 1 PENDAHULUAN

Dalam bab ini berisi tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematis penelitian.

BAB II LANDASAN TEORI

Dalam bab ini berisi tentang menjelaskan teori-teori yang terkait dengan permasalahan yang akan diambil sebagai bahan acuan penelitian.

BAB III METODOLOGI PENELITIAN

Dalam bab ini berisi tentang objek penelitian, alat dan bahan, metode pengumpulan data dan menjelaskan mengenai deskripsi sistem kerja dan perancangan software.

BAB IV HASIL DAN PEMBAHASAN

Dalam bab ini berisi tentang pemaparan hasil analisis persoalan yang dibahas dengan berpedoman pada teori-teori yang dikemukakan pada Bab II.

BAB V KESIMPULAN DAN SARAN

Dalam bab ini berisi tentang rangkuman dari pembahasan serta saran hasil penelitian yang dilakukan.