SKRIPSI

MONITORING KEAMANAN WEBSITE TERHADAP SERANGAN SQL INJECTION

JONATHAN SURYA

NPM: 2013730065

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI DAN SAINS
UNIVERSITAS KATOLIK PARAHYANGAN

2017

UNDERGRADUATE THESIS

MONITORING WEBSITE SECURITY AGAINST SQL INJECTION ATTACKS

JONATHAN SURYA

NPM: 2013730065

DEPARTMENT OF INFORMATICS
FACULTY OF INFORMATION TECHNOLOGY AND SCIENCES
PARAHYANGAN CATHOLIC UNIVERSITY
2017

LEMBAR PENGESAHAN

MONITORING KEAMANAN WEBSITE TERHADAP SERANGAN SQL INJECTION

JONATHAN SURYA

NPM: 2013730065

Bandung, 18 Mei 2017

Menyetujui,

Pembimbing

Dr. Veronica Sri Moertini

Ketua Tim Penguji	Anggota Tim Penguji
Pascal Alfadian, M.Comp.	Mariskha Tri Adithia, P.D.Eng

Mengetahui,

Ketua Program Studi

Mariskha Tri Adithia, P.D.Eng

PERNYATAAN

Dengan ini saya yang bertandatangan di bawah ini menyatakan bahwa skripsi dengan judul:

MONITORING KEAMANAN WEBSITE TERHADAP SERANGAN SQL INJECTION

adalah benar-benar karya saya sendiri, dan saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika keilmuan yang berlaku dalam masyarakat keilmuan.

Atas pernyataan ini, saya siap menanggung segala risiko dan sanksi yang dijatuhkan kepada saya, apabila di kemudian hari ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya, atau jika ada tuntutan formal atau non-formal dari pihak lain berkaitan dengan keaslian karya saya ini.

Dinyatakan di Bandung,
Tanggal 18 Mei 2017

Jonathan Surya
NPM: 2013730065

ABSTRAK

Teknologi yang berkembang memiliki kemampuan untuk mengolah informasi di dalam dunia dijital. Informasi yang diolah dapat bersifat rahasia sehingga dibutuhkan tempat penyimpanan yang disebut basis data. Basis data akan memanipulasi data yang tersimpan dengan perintah-perintah *structured query language* (SQL). Ancaman serangan *SQL Injection* terhadap aplikasi yang menggunakan perintah SQL untuk memanipulasi data masih sangat banyak. *Server* aplikasi tersebut tidak menangani adanya *query* yang bersifat sensitif terhadap sistem basis datanya. Banyak *server* aplikasi yang memblokir secara manual terhadap pengguna yang melakukan *SQL Injection*.

Dengan ancaman dan kondisi tersebut maka penulis membangun sebuah sistem perangkat lunak yang dapat secara otomatis melakukan pemblokiran terhadap serangan *SQL Injection*. Sistem perangkat lunak juga memiliki fitur untuk memantau adanya serangan atau tidak pada *server*. Sistem perangkat lunak dibangun menggunakan bahasa *Java* dengan *jnetpcap library* sebagai pemeran yang membaca setiap paket jaringan yang melewati *server*. Sistem perangkat lunak akan menggunakan *firewall* sebagai metode yang digunakan untuk memblokir pengguna dengan identitas alamat IP. Pembangunan sistem perangkat lunak ini menggunakan sistem operasi Linux Ubuntu. Pengguna yang akan terdeteksi merupakan pengguna yang melakukan pengiriman paket jaringan melewati atau ke *server*.

Hasil sistem perangkat lunak ini dianggap berhasil membuktikan bahwa pembangunan sistem perangkat lunak monitoring keamanan website terhadap serangan *SQL Injection* berhasil dilakukan. Sistem operasi akan menggunakan *iptables* sebagai pengaturan *firewall* pada Linux. Dengan terbentuknya sistem perangkat lunak monitoring keamanan website terhadap serangan *SQL Injection* maka sistem perangkat lunak ini dapat dijadikan sebuah perangkat lunak untuk meminimalisir serangan *SQL Injection* yang diterima oleh aplikasi *server*, tentunya aplikasi *server* yang menggunakan basis data SQL sebagai media penyimpanan data.

Kata-kata kunci: Keamanan jaringan, SQL Injection, *Java*, *firewall*, Linux

ABSTRACT

Emerging technologies have the ability to process information in the digital world. The information processed can be confidential so it takes a storage place called the database. The database will manipulate the stored data with structured query language (SQL) commands. The threat of SQL Injection attacks against applications that use SQL commands to manipulate data is still very much. The application server does not handle queries that are sensitive to its database system. Many application servers block manually against users who perform SQL Injection.

With these threats and conditions the author built a software system that can automatically block the SQL Injection attack. The software system also has features to monitor the presence of attacks or not on the server. The software system is built using Java language with *jnetpcap library* as the actor who reads every network packets that pass through the server. The software system will use the *firewall* as the method used to block users with IP address identity. The construction of this software system uses the Ubuntu Linux operating system. The user to be detected is a user who sends network packets across or to the server.

The results of this software system is considered successful to prove that the development of website security monitoring software system against SQL Injection attacks successfully done. The operating system will use *iptables* as a firewall setting under Linux. With the establishment of a website security monitoring software system against SQL Injection attacks, this software system can be used as a software to minimize SQL Injection attacks received by the application server, of course, server applications that use SQL databases as data storage media.

Keywords: Network security, SQL Injection, Java, firewall, Linux

Dipersembahkan untuk orang tua, saudara, diri sendiri, pembimbing, dan semua orang yang telah membantu dalam proses penyusunan skripsi ini

KATA PENGANTAR

Puji dan Syukur penulis panjatkan kepada Tuhan Yang Maha Esa atas berkat dan rahmat-Nya sehingga penulis dapat menyelesaikan skripsi ini. Pada kesempatan ini, penulis ingin menyampaikan rasa ucapan syukur dan terima kasih kepada:

1. Orang tua penulis yang selalu memberikan dukungan kepada penulis untuk menyelesaikan skripsi ini.
2. Bapak Chandra Wijaya selaku dosen pembimbing yang telah memberikan bimbingan selama proses pembuatan skripsi ini sehingga dapat diselesaikan dengan baik. Terima kasih atas bimbingan dan pengarahan yang telah diberikan kepada penulis sehingga dapat menyelesaikan skripsi ini dengan baik.
3. Bapak Pascal Alfadian dan Ibu Mariskha Tri Adithia selaku penguji yang telah meluangkan waktu untuk memberikan kritik dan saran dalam penulisan skripsi ini.
4. Devina Emily Hariono yang selalu mendukung dan membantu penulis dalam mengerjakan skripsi ini. Terima kasih untuk waktu dan tenaga yang diluangkan kepada penulis sehingga skripsi ini dapat diselesaikan dengan baik.
5. Rekan kerja Administrator Lab FTIS yang telah memberikan banyak dukungan dan semangat serta bantuan sehingga penulis dapat termotivasi dalam mengerjakan skripsi.
6. Teman-teman mahasiswa UNPAR, GCB Bandung, Rancu, serta teman-teman lainnya yang selalu mengingatkan dan menyemangati penulis untuk menyelesaikan penulisan skripsi ini.

Semoga semua pihak yang telah membantu dalam penyusunan skripsi ini mendapat berkah dan rahmat dari Tuhan Yang Maha Esa. Akhir kata, penulis memohon maaf bila terdapat kesalahan dan kekurangan dalam penyusunan skripsi ini. Semoga skripsi ini berguna bagi semua pihak yang membutuhkan.

Bandung, Mei 2017

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Informasi adalah hasil dari pengolahan data dalam suatu bentuk yang lebih berguna dan lebih berarti bagi penerimanya yang menggambarkan suatu kejadian-kejadian yang nyata yang digunakan untuk pengambilan keputusan. Istilah data itu sendiri adalah representasi dari suatu fakta, yang dimodifikasi dalam bentuk gambar, kata, dan/atau angka. Dengan adanya tatacara penggunaan dan tujuan tertentu, data menjadi sangat sensitif ketika bersifat rahasia karena ditujukan untuk penerima tertentu.

Teknologi sangat membantu pertukaran data antar penggunanya melalui jaringan. Dalam dunia komputer, data dapat bertukar menggunakan jaringan secara *Peer-to-Peer* atau secara *Client-Server*. *Peer-to-peer* adalah koneksi antara 1 entitas (komputer) ke 1 entitas lain. *Client-Server* adalah koneksi antara 1 entitas yang melayani banyak entitas lainnya. Ketika pertukaran data menggunakan sistem *Client-Server*, *server* membutuhkan tempat penyimpanan data agar data *client* yang dikirim ke *server* dapat tersimpan dan terjaga dengan baik. *Server* adalah suatu entitas yang melayani permintaan *client*. Seiring berkembangnya teknologi, basis aplikasi yang berkomunikasi secara *Client-Server* pun turut berkembang.

Web-based application adalah sebuah aplikasi yang memanfaatkan protokol HTTP (*HyperText Transfer Protocol*) untuk menyampaikan suatu informasi yang menggunakan server disebut *web server*. *Web server* adalah server yang melayani permintaan *client* terdapat halaman web dan berkomunikasi dengan *middleware* untuk menterjemahkan kode-kode tertentu, menjalankan kode-kode tersebut dan memungkinkan berinteraksi dengan basis data. Adapun arsitektur aplikasi *web server* adalah sebagai berikut :

- *Browser* atau *client* berinteraksi dengan *web server*.
- Secara internal *web server* berinteraksi dengan *middleware*.
- *Middleware* yang berhubungan dengan basis data.

Contoh web server adalah sebagai berikut:

- Apache
- IIS (*Internet Information Server*)

Sesuai dengan definisinya, sebuah web server menggunakan basis data untuk mengelola informasi yang tersimpan. Server yang melayani basis data dinamakan *Structured Query Language* (SQL) Server. SQL Server menggunakan bahasa pemrograman SQL. SQL adalah bahasa pemrograman khusus yang digunakan untuk berinteraksi dengan basis data. Saat ini aplikasi berbasis *website* sangat marak digunakan sehingga mengakibatkan tindakan penyerangan terhadap suatu *server* yang mempunyai sistem basis data SQL semakin tinggi. Tindakan penyerangan yang memanfaatkan SQL statement untuk dieksekusi oleh *server* disebut *SQL Injection*. Untuk mencegah tindakan tersebut dapat dianalisa segala bentuk penyerangan yang dilakukan terhadap *server*.

Kerentanan *SQL Injection* telah digambarkan sebagai salah satu dari ancaman paling serius terhadap aplikasi web. Aplikasi web yang rentan terhadap *SQL Injection* memungkinkan penyerang untuk mendapatkan hak akses lengkap ke basis data yang digunakan. Karena basis data ini sering mengandung informasi konsumen atau pengguna yang sensitif, pelanggaran keamanan yang dihasilkan dapat mencakup pencurian identitas, kehilangan informasi rahasia, dan kecurangan. Dalam beberapa kasus, penyerang bahkan dapat menggunakan kerentanan *SQL Injection* untuk mengendalikan dan merusak sistem yang menghosting aplikasi web tersebut. [1]

SQL Injection mengacu pada kelas serangan kode injeksi dimana data yang diberikan oleh pengguna disertakan dalam *SQL query* sedemikian rupa sehingga bagian dari masukan pengguna diperlakukan sebagai kode SQL. Dengan memanfaatkan kerentanan ini, penyerang dapat mengirimkan perintah SQL secara langsung ke basis data. Serangan ini merupakan ancaman serius terhadap aplikasi web yang menerima masukan dari pengguna dan menggabungkannya dengan *SQL query* ke basis data yang digunakan. Kebanyakan aplikasi web yang digunakan di internet atau dalam sistem perusahaan bekerja dengan cara ini dan karena itu rentan terhadap *SQL Injection*. [1]

Setiap teknik penyerangan *SQL Injection* mempunyai pola yang unik sehingga dapat dilakukan penangkalan terhadap serangan tersebut. Apabila website tidak mencegah terjadinya serangan *SQL Injection*, *website* tersebut mungkin akan sering mendapat serangan dengan konsekuensi data sudah tidak aman lagi atau bahkan sewaktu-waktu basis data ataupun *server* dapat dihancurkan oleh pihak yang tidak bertanggung jawab. Serangan *SQL Injection* terdiri dari berbagai teknik sehingga perlu dilakukan deteksi teknik yang digunakan oleh pihak penyerang. Jika teknik yang digunakan dapat terdeteksi, maka sistem dapat mencegah agar serangan yang serupa tidak akan terjadi lagi terhadap *server* atau *website*. Beberapa teknik *SQL Injection* yang sering digunakan antara lain: *Line Comments*, *Inline Comments*, *Stacking Queries*, *If Statements*, *Using Integers*, *String Operations*, *String without Quotes*, *String Modification and Related*, dan *Union Injections*

Pada skripsi ini dibangun sebuah sistem perangkat lunak yang dapat menganalisa hingga mencegah serangan berjenis *SQL Injection*. Dengan adanya aplikasi ini, para *developer* aplikasi *web* terutama yang menggunakan sistem SQL database dapat menggunakannya untuk menangkal serangan *SQL Injection* terhadap aplikasi mereka. Perangkat lunak dibuat dengan bantuan JNetPCap sebagai library pemrograman berbahasa Java untuk menangkap paket yang melewati sebuah interface jaringan.

1.2 Rumusan Masalah

SQL Injection sudah menjadi serangan yang marak digunakan oleh para peretas untuk mendapatkan informasi dari sistem database. Dengan memonitor seluruh kejadian yang terkait dengan SQL Injection, website dapat mencegah terjadinya serangan tersebut terhadapnya. Beberapa rumusan masalah sebagai berikut:

- Bagaimana mendeteksi serangan *SQL Injection* ?
- Bagaimana cara memblokir serangan *SQL Injection* ?
- Bagaimana cara membangun sistem perangkat lunak yang dapat mendeteksi dan memblokir serangan *SQL Injection* yang terjadi ?

1.3 Tujuan

Memblokir serangan-serangan SQL Injection adalah tujuan utama dari penelitian ini. Tujuan lainnya tercakup sebagai berikut:

- Mempelajari cara untuk mendeteksi serangan SQL Injection pada *website*.
- Mempelajari cara untuk memblokir serangan SQL Injection.

- Membangun sistem perangkat lunak yang dapat mendeteksi dan memblokir serangan *SQL Injection*.

1.4 Batasan Masalah

Batasan masalah pada penelitian ini adalah :

- Basis data yang digunakan adalah *MySQL* karena dianggap sering digunakan oleh berbagai sistem perangkat lunak lain.
- Teknik yang dapat terdeteksi hanya beberapa teknik yang biasanya digunakan yaitu *Line Comments, Inline Comments, Stacking Queries, Using Integers, String Operations,* dan *Union Injections*.
- Pendeteksian *query* pada paket berkas hanya berlaku pada paket yang memiliki protokol HTTP. Data yang dikirim melalui protokol HTTPS dienkripsi sehingga tidak dapat dilakukan pendeteksian terhadap data tersebut.

1.5 Metodologi Penelitian

Langkah-langkah yang ditempuh untuk melakukan penelitian ini adalah :

1. Melakukan studi literatur terkait model *Client/Server* dan sistem operasi Linux.
2. Melakukan studi literatur mengenai *SQL database programming*.
3. Melakukan studi literatur mengenai beragam teknik *SQL Injection*.
4. Mempelajari bahasa pemrograman Java dengan menggunakan JNetPCap.
5. Menguji apakah JNetPCap dapat digunakan pada sistem operasi Linux.
6. Melakukan analisis terhadap serangan *SQL Injection* yang biasa digunakan oleh penyerang terhadap *dummy web*.
7. Melakukan perancangan aplikasi dengan menggunakan bahasa pemrograman Java.
8. Mengimplementasikan hasil analisis teknik *SQL Injection* untuk memblokir penyerang dengan menggunakan bahasa pemrograman Java.
9. Melakukan pengujian terhadap website yang telah menggunakan aplikasi ini.
10. Menulis dokumen skripsi.

1.6 Sistematika Pembahasan

Sistematika pembasahan penilitian ini sebagai berikut :

1. Bab 1 Pendahuluan.
   Bab ini membahas mengenai latar belakang, rumusan masalah, tujuan, batasan masalah, metodologi penelitian, dan sistematika pembahasan untuk penelitian ini.
2. Bab 2 Dasar Teori.
   Bab ini membahas mengenai pengertian dan penjelasan dari *Client/Server*, dasar-dasar *SQL database*, *SQL Injection*, *jNetPcap*, *web*, *firewall*, dan metode pencegahan.

3. Bab 3 Analisis.
   Bab ini membahas mengenai analisis yang terdiri dari penggunaan *iptables*, skenario teknik-teknik serangan *SQL Injection*, diagram *use-case*, skenario *use-case*, diagram kelas, dan diagram hubungan antar entitas (*ERD*) untuk perangkat lunak yang dibangun.

4. Bab 4 Perancangan Sistem.
   Bab ini membahas mengenai perancangan sistem yang terdiri dari perancangan tabel basis data, diagram alur, diagram kelas rinci dengan penjelasan yang mendalam untuk tiap kelas dan fungsi yang dimiliki, dan perancangan antarmuka yang digunakan.

5. Bab 5 Implementasi dan Pengujian.
   Bab ini membahas mengenai implementasi dan pengujian sistem perangkat lunak yang dibangun. Terdiri dari 2 bagian yaitu bagian implementasi yang membahas tentang lingkungan dari sistem perangkat lunak yang dibangun saat proses implementasi beserta hasilnya dan bagian pengujian membahas tentang lingkungan dari sistem perangkat lunak saat dilakukan proses pengujian beserta hasil pengujian yang telah dilakukan. Bagian pengujian dibagi menjadi dua, pengujian fungsional dan pengujian eksperimental.

6. Bab 6 Kesimpulan dan Saran.
   Bab ini membahas mengenai kesimpulan dari penelitian yang sudah dilakukan dan saran untuk pengembangan lebih lanjut.