BAB I

PENDAHULUAN

1.1. Latar Belakang Penelitian

Perkembangan dalam bidang teknologi semakin pesat. Salah satu perkembangan adalah pemanfaatan terhadap *website*. *Website* tidak hanya terbatas sebagai media informasi sekarang, bahkan *website* sudah digunakan sebagai tempat untuk bertransaksi baik itu dalam bentuk barang maupun jasa. Akan tetapi, perkembangan tersebut secara tidak langsung juga menimbulkan dampak negatif. Salah satu dampak negatif yang dimaksud adalah meningkatkan potensi terjadinya peretasan pada suatu *website*. Dalam jurnalnya (Laksana & Rosyid, 2017: 364) mengungkapkan bahwa Symantec dalam laporan yang dirilis tahun 2016 menyebutkan bahwa serangan yang mengancam *web server* meningkat sebanyak 117% pada tahun 2015 dibandingkan tahun 2014. Oleh sebab itu, pengembang *website* tentunya harus memperhatikan keamanan pada *website* untuk mencegah timbulnya kerugian yang tidak diinginkan.

Peretasan pada *website* dapat dilakukan dengan berbagai teknik. Salah satu teknik yang pada umumnya digunakan oleh peretas dalam melakukan peretasan terhadap suatu *website* adalah teknik SQL Injection. Hal ini diungkapkan oleh (Yulianingsih, 2016: 46) bahwa total serangan terhadap situs-situs yang ada di Indonesia adalah 28.430.843 dan jenis serangan paling besar adalah melalui SQL.

Menurut (Baihaqi, Shiddiqi, & Adi Pratomo, 2013: 2), SQL injection adalah sebuah serangan dengan cara memasukkan sebuah kode ke dalam sebuah string yang akan dieksekusi oleh aplikasi *database server*. Pada umumnya, database akan membaca variabel dan melakukan eksekusi tanpa melakukan *filtering* atau validasi pada variabel tersebut. Teknik SQL Injection mengeksploitasi kelemahan tersebut untuk menyisipkan perintah SQL sehingga *database* membaca nilai pada variabel yang diterima sebagai perintah yang harus dieksekusi. Dengan demikian, secara tidak langsung peretas mendapatkan akses terhadap database dan dapat mencuri informasi.

Tingginya tingkat peretasan pada website yang dilakukan dengan menggunakan SQL Injection mendorong beberapa pihak tertentu untuk mengembangkan cara mencegah teknik tersebut. Salah satu cara yang dikembangkan adalah Honeypot. Menurut (Baihaqi et al., 2013: 1), Honeypot adalah sebuah sistem yang dibuat untuk menyimulasikan layanan yang berjalan di atas sebuah *server* dengan tujuan sebagai umpan untuk mengalihkan atau menarik perhatian peretas untuk menyerang sistem tersebut. Dengan demikian, Honeypot melindungi suatu sistem dengan mengelabui peretas agar menyerang Honeypot itu sendiri. Honeypot juga akan mencatat aktivitas serangan yang dilakukan untuk keperluan penyelidikan.

Berdasarkan penelitian yang dilakukan oleh (Aidin, Nasution, & Azmi, 2016: 2176–2177) dalam jurnal "IMPLEMENTASI HIGH INTERACTION HONEYPOT PADA SERVER", peneliti melakukan instalasi Honeypot pada suatu cubieboard, kemudian peneliti menggunakan beberapa *tools* untuk menguji

kinerja Honeypot tersebut terhadap beberapa teknik peretasan yang pada umumnya digunakan, salah satunya SQL Injection. Dari hasil pengujian, Honeypot berhasil melindungi server dari peretasan dengan teknik SQL Injection. Berdasarkan penelitian tersebut, Honeypot terbukti dapat mencegah peretasan dengan teknik SQL Injection.

PT Duta Computer merupakan salah satu perusahaan yang bergerak dalam bidang IT di Batam. Dalam beroperasi, perusahaan tersebut menggunakan *website* sebagai salah satu sarana informasi untuk menunjang bisnisnya. Namun, baik pada *website* maupun jaringan komputer perusahaan tersebut belum memiliki sistem keamanan yang dapat mencegah teknik SQL Injection. Dengan demikian, *website* perusahaan tersebut berpotensi diretas dengan teknik SQL Injection mengingat banyaknya *website* yang diretas dengan menggunakan teknik ini. Apabila *website* berhasil diretas, hal ini tentu dapat menimbulkan kerugian bagi perusahaan tersebut.

Oleh karena itu pada penelitian ini, peneliti akan menggunakan Honeypot untuk melindungi *website* PT Duta Computer dari peretasan dengan teknik SQL Injection. Kemudian, peneliti akan menganalisis cara kerja teknik SQL Injection dalam peretasan *website* beserta cara pencegahannya dengan menggunakan Honeypot. Peneliti berharap implementasi tersebut dapat mencegah *website* PT Duta Computer dari peretasan dengan teknik SQL Injection. Peneliti juga berharap penelitian ini dapat menambah wawasan masyarakat khususnya pengembang *website* mengenai teknik SQL Injection dan Honeypot serta penelitian ini juga dapat dijadikan referensi untuk penelitian lebih lanjut.

Berdasarkan pembahasan singkat di atas, peneliti akan melakukan penelitian dengan judul "ANALISIS DAN PENCEGAHAN SQL INJECTION DENGAN HONEYPOT".

1.2. Identifikasi Masalah

Berdasarkan latar belakang yang sudah dijelaskan di atas, maka dapat diidentifikasikan permasalahan sebagai berikut:

1. *Website* PT Duta Computer belum memiliki sistem keamanan yang dapat mencegah teknik SQL Injection.
2. Jaringan komputer pada PT Duta Computer belum memiliki sistem keamanan yang dapat mencegah teknik SQL Injection.

1.3. Pembatasan Masalah

Agar penelitian tidak meluas dari pembahasan yang dimaksud, dalam skripsi ini peneliti membatasi pada ruang lingkup sebagai berikut:

1. Analisis yang dilakukan pada teknik SQL Injection, terbatas pada analisis cara kerjanya dalam melakukan peretasan terhadap *website*.
2. Analisis yang dilakukan pada Honeypot, terbatas pada analisis cara Honeypot mendeteksi serangan SQL Injection dan cara Honeypot mencegah SQL Injection pada *website*.

3. Penelitian ini akan menggunakan tool Honeypot yang dimodifikasi oleh peneliti untuk menyesuaikan kebutuhan penelitian. Nama tool tersebut adalah HIHAT *(High Interaction Honeypot Analysis Toolkit*).

1.4. Perumusan Masalah

Berdasarkan latar belakang yang sudah dijelaskan sebelumnya, maka dapat diambil beberapa perumusan masalah adalah sebagai berikut:

1. Bagaimana cara kerja teknik SQL Injection dalam meretas suatu *website*?
2. Bagaimana cara mencegah terjadinya peretasan tersebut dengan Honeypot?

1.5. Tujuan Penelitian

Adapun beberapa tujuan penelitian yang ingin dicapai dalam pembahasan ini adalah sebagai berikut:

1. Mengetahui cara kerja teknik SQL Injection dalam meretas suatu website.
2. Mengetahui cara mencegah terjadinya peretasan tersebut dengan Honeypot.

1.6. Manfaat Penelitian

Manfaat penelitian yang dapat diperoleh dari penelitian ini terbagi menjadi dua aspek, sebagai berikut:

1. Aspek Teoritis

Secara teoritis, penelitian ini diharapkan dapat memperluas pengetahuan pembaca mengenai cara kerja teknik SQL Injection dalam peretasan suatu *website* beserta cara pencegahannya dengan menggunakan Honeypot serta dapat digunakan sebagai referensi untuk penelitian lebih lanjut.

2. Aspek Praktis

Sedangkan dari segi praktis, penelitian ini diharapkan dapat bermanfaat bagi pihak-pihak sebagai berikut:

a. Bagi Mahasiswa

Penelitian ini dapat menambah wawasan mahasiswa dan menjadi referensi untuk penelitian lebih lanjut.

b. Bagi Pengembang Website

Penelitian ini dapat menambah wawasan pengembang *website* dan dapat digunakan sebagai referensi untuk mencegah terjadinya peretasan *website* dengan Honeypot.

c. Bagi Masyarakat

Penelitian ini dapat menambah wawasan masyarakat.