BAB I

PENDAHULUAN

1.1. Latar Belakang

Sistem informasi berbasis *web* pada saat ini sangat berkembang pesat dan memiliki peran besar. Ini terbukti dengan banyaknya yang memanfaatkan sistem informasi berbasis *web* seperti sekolah, universitas, perusahaan atau instansi untuk mendukung tercapainya visi dan misi suatu organisasi. Layanan *web* memiliki kelebihan dapat diakses dari manapun dan kapanpun sehingga dapat memberikan suatu informasi pada saat itu juga. Menurut Direktorat Keamanan Informasi, Direktorat Jendral Aplikasi Informatika dan Kementrian Komunikasi dan Informatika tahun 2011, saat ini *website* merupakan salah satu layanan informasi yang banyak diakses oleh pengguna Internet di dunia. Sebagai salah satu layanan informasi maka perlu dibangun *website* yang mampu menangani permintaan dari banyak pengguna dengan baik.

Berdasarkan data Internet *trafic* Indonesia *Security Incident Response Team on Internet Infrastructure/Coordination Center* (Id-SIRTII/CC) pada bulan Juli tahun 2015 yang dilakukan dari tanggal 01 Juli 2015 sampai dengan 31 Juli 2015. Ancaman keamanan di Internet nasional adalah data *Denial of Service* (DOS) yang memiliki tingkat tertinggi antara tanggal 12 dan 13 dan data *Stuctured Query Language* (SQL) Injeksi yang mendominasi selama satu bulan penuh. Ini menjelaskan bahwa SQL Injeksi sering dilakukan oleh individu atau kelompok tertentu untuk melakukan serangan terhadap target. Celah

keamanan pada suatu aplikasi *web* dapat disalahgunakan oleh individu atau kelompok yang tidak bertanggung jawab seperti melakukan perubahan, mengambil atau bahkan sampai menghapus data sehingga pemilik *website* menjadi sangat dirugikan.

Contoh kasus *web deface* senin 17 Oktober 2016 (https://www.merdeka.com/teknologi/*hacker*-indonesia-sentil-situs-kpu-tuliskritikan-menyentuh.html), salah satu laman *website www.ppid.kpu.go.id/upload/file/*, dari Komisi Pemilihan Umum (KPU) Republik Indonesia kena retas *hacker* lokal. *Hacker* ini mempunyai nama samaran 'M2404', *Hacker* M2404 meretas bagian pengunggahan data dari situs PPID (Pejabat Pengelola Informasi dan Dokumentasi) KPU. Saat tim merdeka.com mencoba mengakses alamat *ppid.kpu.go.id/upload/file/*, terlihat bila laman situs tersebut di-*deface* alias dirubah tampilannya. Menurut Pakar Teknologi Informasi (Ruby Alamsyah,2015), "Selama ini sudah terbukti bahwa : 'Indonesia belum berdaulat di dunia *cyber*'. Sehingga 'penjajahan' jenis baru yaitu di dunia *cyber* masih kerap terjadi dan sangat merugikan Indonesia, di segala bidang terutama politik dan ekonomi.

PT. Andalan Resiko Lestari adalah sebuah perusahaan yang bergerak di bidang pialang reasuransi. Pialang reasuransi adalah perusahaan yang memberikan jasa keperantaraan dalam penempatan reasuransi dan penanganan penyelesaian ganti rugi reasuransi dengan bertindak untuk kepentingan perusahaan asuransi. PT. Andalan Resiko Lestari menyelenggarakan usaha jasa konsultansi dan keperantaraan dalam penempatan reasuransi serta penanganan penyelesaian klaimnya dengan bertindak untuk

dan atas nama perusahaan asuransi dan perusahaan reasuransi. PT. Andalan Resiko Lestari memiliki sebuah *website* yang berfungsi sebagai profil perusahaan, didalam *website* tersebut menjelaskan informasi PT. Andalan Resiko Lestari seperti latar belakang, visi, misi dan struktur organisasi.

Berdasarkan uraian, maka akan dilakukan penelitian dengan mengambil topik Tugas Akhir "**Uji Penetrasi Pada *Web Server* PT. ANDALAN RESIKO LESTARI** ".

1.2. Identifikasi Masalah

Berdasarkan latar belakang di atas, maka identifikasi masalah dalam penyusunan Tugas Akhir ini adalah sebagai berikut :

1. Bagaimana cara menemukan celah keamanan pada *web server*?
2. Bagaimana bentuk temuan celah keamanan?
3. Bagaimana cara melakukan uji penetrasi?
4. Bagaimana cara menutup celah keamanan yang telah ditemukan?

1.3. Batasan Masalah

Agar penelitian tidak menyimpang dan tetap terarah maka ada batasan masalah sebagai berikut:

1. *Web server* yang dilakukan uji penetrasi adalah *web server www.andalanre.co.id*.
2. Melakukan uji penetrasi pada *web server.*
3. Studi kasus ini dilakukan di PT. ANDALAN RESIKO LESTARI.

1.4. Tujuan Penelitian :

1. Mengkaji celah keamanan pada *web server* yang dapat menimbulkan masalah serius terhadap aset organisasi.
2. Diharapkan dapat membantu administrator dalam menemukan celah keamanan.
3. Merekomendasikan cara menutup celah keamanan sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab.

1.5. Manfaat Penelitian

1. Dapat menambah pengetahuan dan pemahaman tentang keamanan pada *web server*.
2. Bagi pihak PT. ANDALAN RESIKO LESTARI dapat terbantu dalam meningkatkan keamanan *web server*.
3. Bagi akademik untuk menjadi salah satu referensi yang sedang melakukan penyusunan Tugas Akhir.

1.6. Metode Penelitian

1. Metode Pengumpulan Data

Dalam menyusun Tugas Akhir ini, data yang diperoleh dari metode pengumpulan data sebagai berikut :

a. Survey

Pada metode ini dilakukan kegiatan survey langsung di PT. ANDALAN RESIKO LESTARI.

Metode survey yang dilakukan adalah :

1. Observasi

Pada proses ini dilakukan pengamatan dan pencatatan secara sistematis mengenai PT. ANDALAN RESIKO LESTARI.

2. Wawancara

Pada proses ini dilakukan wawancara langsung dengan administrator *website* PT. ANDALAN RESIKO LESTARI.

b. Studi Pustaka

Tahap ini melakukan penggalian data dan pengumpulan informasi, melalui buku, jurnal, tugas akhir dan artikel. Yang dapat menjadi bahan referensi dalam pembuatan Tugas Akhir ini.

1.7. Jadwal Perencanaan

Adapun susunan waktu perencanaan dalam penelitian Uji Penetras Pada *Web Server* PT. ANDALAN RESIKO LESTARI adalah sebagai berikut Tabel 1.1, Jadwal Perencanaan :

No	Nama Kegiatan	Tahun 2017 Bulan					
		Maret	April	Mei	Juni	Juli	Agustus
1	Penyusunan Proposal Tugas Akhir.						
2	Observasi,Pengumpulan Data, dan Studi Pustaka.						

3	Persiapan Alat dan Uji Penetrasi.						
4	Mencari Celah Keamanan.						
5	Uji Penetrasi.						
6	Dokumentasi dan Laporan.						

1.8. Sistematika Penulisan

Untuk memberikan gambaran menyeluruh tentang penelitian yang dilakukan, maka tugas akhir ini disusun dengan sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini dijelaskan mengenai latar belakang, identifikasi masalah, batasan masalah, tujuan, manfaat, metode pengumpulan data, jadwal perencanaan dan sistematika penulisan laporan.

BAB II LANDASAN TEORI

Bab ini memuat beberapa referensi dari hasil penelitian yang relevan dengan topik tugas akhir yang disajikan, yang diperoleh dari berbagai sumber.

BAB III GAMBARAN UMUM

Bab ini menjelaskan tentang gambaran umum PT. Andalan Resiko Lestari.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini berisi bahasan mengenai uji penetrasi pada *web server* PT. Andalan Resiko Lestari.

BAB V KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan dan saran untuk meminimalisir celah keamanan yang ada di *web server*.