BAB I PENDAHULUAN

I.1 Latar Belakang

Seiring perkembangan teknologi yang semakin pesat, maka perkembangan sistem informasi pun semakin berkembang. Berbagai entitas sudah melakukan digitalisasi, termasuk berbagai entitas yang menyimpan berbagai data-data pribadi dari pelanggan atau pengguna. Namun, banyak entitas yang masih kurang memperhatikan keamanan sistem informasi ini. Karena kurangnya perhatian dari entitas ini, banyak sekali potensi *vulnerability* yang dapat dengan mudah dimasuki oleh *attacker.* Dengan mudahnya *attacker* masuk ke dalam sistem, maka berbagai data yang terdapat di dalam sistem akan dengan mudah dicuri untuk keuntungan pribadi *attacker.*

Dengan adanya sistem perkuliahan daring yang dijalani saat ini, maka kebutuhan akan aplikasi yang mendukung perkuliahan semakin meningkat. Segala aktivitas perkuliahan yang tadinya dilakukan secara tatap muka, dengan adanya sistem perkuliahan daring ini, dilakukan secara daring dengan dukungan berbagai aplikasi. Aplikasi yang dibuat oleh Fakultas Rekayasa Industri (FRI) Universitas Telkom ini berbasis situs web, untuk memudahkan mahasiswa mengakses aplikasi dari berbagai perangkat, seperti telepon genggam, PC (*Personal Computer*) *tablet, laptop,* ataupun komputer *desktop*.

Kerja Praktek merupakan sebuah kegiatan yang dilakukan oleh mahasiswa untuk mendapatkan pengetahuan dan pengalaman praktis di dunia kerja berdasarkan dasar keilmuan yang telah dicapai. Dalam pelaksanaannya, kerja praktek dilakukan di industri selama minimal 30 (tiga puluh) hari kerja, dan dilakukan pada saat libur antar semester sehingga tidak mengganggu jadwal perkuliahan. Setelah melakukan kerja praktek, mahasiswa diwajibkan untuk menyusun laporan hasil kerja praktek dan dipresentasikan di hadapan dosen pembimbing dalam sidang kerja praktek. Mahasiswa disarankan untuk mengambil kerja praktek sesuai dengan program studi dan kelompok keahlian yang dipilih, supaya memudahkan mahasiswa untuk lebih mendalami kelompok keahlian yang dipilih sebelum mengerjakan Tugas Akhir.

Untuk memudahkan pelaksanaan Kerja Praktek, maka Fakultas Rekayasa Industri (FRI) membuat sebuah aplikasi dalam bentuk situs web. Aplikasi ini bernama KPPM (Kerja Praktek dan Pengabdian Masyarakat) Virtual FRI, dalam domain kppm.virtualfri.id. Aplikasi ini disusun menggunakan *framework* Sails.js yang berbasis pada bahasa pemrograman JavaScript dan berjalan di dalam *Virtual Private Server* (VPS) milik FRI. Aplikasi ini dapat digunakan oleh mahasiswa untuk memilih topik KPPM, mengunggah laporan, logbook, dan file presentasi yang diperlukan untuk presentasi sidang laporan akhir KPPM, dan memantau *progress* penilaian laporan akhir KPPM.

Situs web KPPM ini perlu diuji keamanannya karena dalam situs KPPM ini banyak menyimpan data yang *confidental*, seperti data Nomor Induk Mahasiswa (NIM), data Nomor Induk Pegawai (NIP) dari dosen pembimbing dan pembimbing lapangan mahasiswa tersebut yang dapat digunakan untuk mengambil berbagai data yang tersambung dengan mahasiswa dan dosen tersebut oleh pihak yang tidak bertanggung jawab, dan digunakan secara tidak bertanggung jawab untuk kepentingan pribadi *attacker* tersebut.

Kasus pencurian data *confidental* sudah banyak terjadi di Indonesia. Pada bulan Mei 2021, terjadi kebocoran data dari situs BPJS (Badan Penyelenggara Jaminan Sosial) sebanyak 279 juta data yang mengandung berbagai informasi pribadi dari pengguna BPJS, dan 20 juta data diantaranya mengandung foto personal. Dan pada bulan Mei 2020, terjadi pembobolan data oleh peretas yang telah mendapatkan data sebanyak 2,3 juta warga Indonesia yang mengandung berbagai informasi pribadi, seperti NIK (Nomor Induk Kependudukan), nama lengkap, alamat, dan tanggal lahir.

Berbagai langkah dan mitigasi yang telah dilakukan sebelumnya hanya dapat meningkatkan keamanan dan mengurangi resiko, tidak menjadikan situs web KPPM ini sepenuhnya terbebas dari ancaman kebocoran data. Untuk memastikan bahwa sistem sepenuhnya aman, maka diperlukan kegiatan VA (*Vulnerability Assessment*) untuk menganalisis keamanan sistem dan mencoba keamanan sistem, apakah terdapat *exploit* di dalam sistem ataupun kemungkinan *exploit* yang memungkinkan *attacker* untuk masuk ke dalam sistem.

Untuk melakukan kegiatan VA, banyak *tools* dan *software* yang tersedia, dengan berbagai fitur dan keunggulannya masing-masing, dan harga yang ditawarkan pun beragam. Ada *tools* dan *software* yang dapat digunakan secara gratis (*freeware*), dan ada tools yang berbayar, baik secara sekali pembelian menggunakan lisensi (*licensed*) atau harus berlangganan (*subscribe*).

Terdapat 11 aplikasi berbasis web yang berjalan pada VPS FRI, yaitu sebagai berikut.

No	Nama	Jenis	Fungsi
1	assessment2020	Aplikasi Web Berjalan pada PHP 7.4 Laravel	Aplikasi Assessment dan team building mata kuliah RPL Prodi. SI FRI
2	rpl	Embed Web Slack Bot	Slack Bot untuk perkuliahan RPL Prodi. SI FRI
3	ta1	Aplikasi Web Berjalan pada Sails JS	Aplikasi Dashboard untuk proposal TA1 FRI
4	kppm	Aplikasi Web Berjalan pada Sails JS	Aplikasi Dashboard untuk Kerja Praktek FRI
5	oss	Aplikasi Web Berjalan pada PHP Laravel	Aplikasi One Stop Service Telkom University
6	pipe	Aplikasi Web Berjalan pada Python	Aplikasi Pemilihan Peminatan Prodi SI FRI
7	sofi	Aplikasi Web Berjalan pada PHP Laravel	Aplikasi Dashboard dan Pendaftaran Sidang FRI
8	mentawai	Aplikasi Web Berjalan pada CodeIgniter	Aplikasi Manajemen Pegawai FRI

9	administrasi	Aplikasi Web Berjalan pada CodeIgniter Custom	Aplikasi Administrasi Mahasiswa FRI
10	iris	Aplikasi Web Berjalan pada CodeIgniter	Aplikasi rekruitasi asisten praktikum/laboratorium FRI
11	SAP FRI	Aplikasi Web Berjalan pada CodeIgniter	Aplikasi Administrasi Sertifikasi SAP FRI

Tabel I.1 Aplikasi yang berjalan pada VPS FRI

Dari 11 aplikasi diatas, peneliti memilih untuk melakukan pengujian VA pada situs web aplikasi KPPM FRI (Kerja Praktek dan Pengabdian Masyarakat), karena data yang ada pada situs web tersebut merupakan data yang bersifat *confidental,* seperti NIM (Nomor Induk Mahasiswa), NIP (Nomor Induk Pegawai) dari dosen pembimbing mahasiswa dan pembimbing lapangan tempat mahasiswa melaksanakan program KP (Kerja Praktek) ataupun PM (Pengabdian Masyarakat). Situs web KPPM FRI ini juga dapat diakses oleh pihak eksternal, yaitu pembimbing lapangan mahasiswa, yang meningkatkan resiko dari adanya akses yang tidak diinginkan oleh pihak yang tidak bertanggung jawab.

Penulis menggunakan *tools* Burp Suite dan Intruder untuk melakukan pengujian pada situs web KPPM FRI ini. Burp Suite merupakan *tools* yang sudah jamak digunakan untuk melakukan kegiatan VA pada situs web. Burp Suite banyak digunakan oleh berbagai kalangan dari IT *Security*, baik dari mahasiswa hingga praktisi senior. Intruder merupakan *tools* khusus *corporate* yang juga berfungsi untuk melakukan kegiatan VA. Penulis memilih 2 *tools* tersebut untuk membandingkan performa dari masing-masing *tools*, dan juga untuk membuktikan klaim dari masing-masing pengembang *tools*¸ apakah *tools* yang ditawarkan benar-benar bekerja lebih baik dengan harus membayar lisensi yang lebih besar.

I.2 Perumusan Masalah

Rumusan masalah yang mendasari penelitian ini adalah:

a. Bagaimana struktur dan spesifikasi dari situs web KPPM FRI yang disimpan pada VPS FRI?
b. Bagaimana tingkat potensi kerentanan dari situs web KPPM FRI yang digunakan oleh FRI Universitas Telkom?
c. Bagaimana efektivitas dari tools Burp Suite dan Intruder yang digunakan untuk kegiatan VA pada VPS FRI Universitas Telkom?

I.3 Tujuan Penelitian

Penelitian ini bertujuan untuk mengetahui:

a. Struktur dan spesifikasi detail dari situs web KPPM FRI yang digunakan oleh FRI Universitas Telkom.
b. Ukuran potensi kerentanan dari situs web KPPM FRI yang digunakan oleh FRI Universitas Telkom dengan tools Burp Suite dan Intruder.
c. Ukuran efektivitas dari tools Burp Suite dan Intruder untuk kegiatan VA.

I.4 Batasan Penelitian

Batasan dari penelitian ini adalah sebagai berikut:

1. Penelitian ini merupakan kajian dari analisis kerentanan yang ditemui pada situs web KPPM FRI.
2. Analisis hanya dilakukan pada situs web KPPM FRI dengan alamat *Uniform Resource Locator* (URL) https://kppm.virtualfri.id.
3. Penggunaan metode VA *automated testing* dan tipe VA kombinasi dalam melakukan pemindaian kerentanan pada situs KPPM FRI.
4. Pengujian terhadap situs web KPPM FRI menggunakan *tools* Burp Suite dengan sistem operasi Kali Linux di dalam *Virtual Machine*, dan Intruder dengan sistem operasi Windows 11.
5. Parameter yang diukur merupakan tingkat kerentanan yang ditemukan berdasarkan penggunaan masing-masing *tools*.
6. Hasil analisis dari penelitian ini dapat menjadi acuan untuk melakukan perbaikan terhadap situs web tersebut.

I.5 Manfaat Penelitian

Manfaat penelitian ini adalah sebagai berikut:

1. Penelitian ini bermanfaat bagi Fakultas Rekayasa Industri Universitas Telkom dalam mengetahui tingkat keamanan pada situs web dan *platform* yang digunakan, yang nantinya dapat digunakan untuk melakukan perbaikan dan peningkatan keamanan situs web dan pemilihan *platform* yang digunakan.
2. Penelitian ini bermanfaat bagi peneliti lain yang bergerak dalam keamanan infrastruktur jaringan dalam memilih *tools* dan alat bantu yang tepat untuk melakukan kegiatan VA.