BAB 1. PENDAHULUAN

1.1 Latar Belakang Masalah

Universitas Kristen Maranatha adalah perguruan tinggi swasta yang dimana UK. Maranatha menggunakan Sistem Akademik Terpadu atau yang biasa disebut SAT. SAT UK. Maranatha adalah aplikasi yang digunakan oleh mahasiswa untuk melihat data mahasiswa, pengajuan cuti resmi, jadwal kuliah, pengecekan dkbs, melihat nilai ujian, melihat transkrip nilai, perwalian, informasi e-learning, melakukan survey PMB, melihat info tagihan, dan simulasi tagihan untuk mahasiswa.

Selain mahasiswa, aplikasi SAT UK. Maranatha yang berbasis *web* digunakan oleh semua pihak yang terlibat dalam kegiatan akademik untuk beragam kepentingan seperti memperbarui data mahasiswa, mengelola data nilai, jadwal kuliah dan mengelola data lain yang berkaitan dengan kegiatan akademik di UK. Maranatha.

Sistem SAT terdapat halaman yang berisi info tagihan mahasiswa UK. Maranatha. Halaman info tagihan mahasiswa tersebut terbuka tanpa akses *login* dan dapat diakses melalui *URL* tertentu melalui *web browser*. Tujuan awal terbukanya akses info tagihan adalah agar mempermudah dan mempercepat pegawai UK. Maranatha pada saat melakukan pencarian info tagihan mahasiswa dengan cara mengetikkan *URL* tertentu melalui *web browser* dan memasukkan *querystring* berupa NRP mahasiswa.

Halaman info tagihan mahasiswa yang ada di SAT terdapat biodata mahasiswa. Biodata yang ditampilkan pada halaman info tagihan mahasiswa adalah NRP, nama lengkap, alamat lengkap beserta kode pos, nomor telepon, email, status mahasiswa, status keuangan. Selain biodata terdapat rincian tagihan mahasiswa yang sudah dibayar dan yang belum di bayar oleh mahasiswa UK. Maranatha.

Security vulnerability yang ada pada halaman info tagihan mahasiswa UK. Maranatha adalah terbukanya info tagihan mahasiswa tanpa akses *login*. Pengguna dapat memasukkan NRP mahasiswa dari *querystring* juga merupakan *security vulnerability* pada halaman info tagihan mahasiswa.

Security vulnerability yang ada pada info tagihan mahasiswa memungkinkan semua orang dan pihak yang tidak bertanggungjawab dapat mengambil seluruh biodata dan tagihan mahasiswa UK. Maranatha. *Security vulnerability* tersebut dapat dieksploitasi untuk pengambilan biodata dan data tagihan oleh pihak yang tidak bertanggungjawab menggunakan aplikasi yang dibuat sendiri maupun aplikasi yang sudah ada.

Penanggulangan *security vulnerability* info tagihan mahasiswa sangat dibutuhkan. Apabila penanggulangan *security vulnerability* pada halaman info tagihan mahasiswa tidak segera ditangani maka akan terjadi kebocoran data yang bisa dimanfaatkan oleh orang yang tidak bertanggungjawab dan diolah menjadi laporan dan informasi yang dapat merugikan mahasiswa dan pihak UK. Maranatha.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas dan hasil wawancara dan observasi dengan pengelola SAT UK. Maranatha ada beberapa rumusan masalah yang diperoleh yaitu :

1. Bagaimana mengetahui apa saja resiko yang terjadi saat info tagihan terbuka aksesnya?
2. Bagaimana mengetahui langkah-langkah apa saja yang harus dilakukan untuk memperbaiki *security vulnerability* info tagihan?
3. Bagaimana memperbaiki *security vulnerability* info tagihan tetapi tetap mempermudah pegawai UK. Maranatha melihat info tagihan?
4. Bagaimana membatasi hak akses pengguna untuk melihat info tagihan berdasarkan hak akses SAT UK. Maranatha?

1.3 Tujuan Pembahasan

Untuk menjawab rumusan masalah di atas, maka terdapat beberapa tujuan pembahasan sebagai berikut :

1. Menganalisis resiko apa saja yang terjadi saat info tagihan terbuka aksesnya.

2. Membuat langkah-langkah yang harus dilakukan dengan cara melakukan analisa terhadap halaman info tagihan mencari *security vulnerability* dari halaman info tagihan yang harus diperbaiki dan selanjutnya membuat *patch* untuk halaman info tagihan.
3. Memperbaiki *security vulnerability* halaman info tagihan dari sistem yang sebelumnya tetapi tetap mempermudah pegawai UK. Maranatha untuk mengaksesnya.
4. Membuat *role based* untuk mengakses info tagihan berdasarkan hak akses SAT UK. Maranatha.

1.4 Ruang Lingkup Kajian

Agar perancangan aplikasi dan analisis *security vulnerability* dapat dilakukan secara terarah dan mencapai sesuai tujuan maka terdapat beberapa ruang lingkup kajian yaitu :

1. Analisis terhadap *security vulnerability* halaman info tagihan ketika aksesnya terbuka.
2. Analisis resiko jika *security vulnerability* dibiarkan tetap terbuka aksesnya.
3. Analisis resiko dampak yang akan terjadi jika terjadi kebocoran data info tagihan.
4. Analisis solusi apa saja yang memungkinkan untuk memperbaiki halaman info tagihan.
5. Analisis solusi yang tepat untuk memperbaiki halaman info tagihan dan melakukan implementasi.
6. Pembuatan *security patch* untuk halaman info tagihan berupa aplikasi web.
7. Aplikasi menggunakan bahasa pemrograman C# ASP.NET Framework 4.5
8. Aplikasi menggunakan *web service* SAT UK. Maranatha dan *web service* keuangan UK. Maranatha.
9. Aplikasi digunakan untuk memperbaiki halaman info tagihan dari sistem sebelumnya.

10. Aplikasi memberikan tambahan keamanan sesuai dengan hak akses para pengguna (*role based*).

1.5 Sumber Data

Sumber data yang digunakan dalam penulisan laporan tugas akhir ini dibagi menjadi dua kategori. Kategori primer yaitu data dan informasi yang diperoleh dari *web service* SAT UK. Maranatha dan *web service* keuangan UK. Maranatha melalui izin dari pihak terkait. Selain kategori primer terdapat juga kategori sekunder data yang didapat dari referensi lain seperti buku penunjang, sumber informasi tertulis dan situs internet yang bisa dipertanggungjawabkan atas semua datanya.

1.6 Sistematika Penyajian

Sistematika penyajian laporan tugas akhir mengenai pembuatan sistem informasi info tagihan mahasiswa UK. Maranatha dibagi menjadi enam bab yaitu :

BAB I PENDAHULUAN

Bab ini terdiri atas latar belakang masalah, rumusan masalah, tujuan pembahasan, ruang lingkup kajian, sumber data, dan sistematika penyajian.

BAB II LANDASAN TEORI

Bab ini berisi seluruh teori yang dipakai dan relevan dengan penelitian yang dilakukan.

BAB III ANALISIS DAN RANCANGAN SISTEM

Bab ini berisi pembahasan mengenai analisis, gambaran keseluruhan dan desain perangkat lunak yang dirancang.

BAB IV HASIL PENELITIAN

Bab ini berisi pembahasan mengenai perencanaan dari bab 3, perjalanan implementasi aplikasi perangkat lunak, serta fungsionalitas dan ulasan mengenai desain antarmuka pengguna.

BAB V PEMBAHASAN DAN UJI COBA HASIL PENELITIAN

Bab ini berisi pembahasan mengenai jenis-jenis testing yang digunakan terhadap aplikasi perangkat lunak dan hasil yang diperoleh dari testing beserta ulasannya.

BAB VI SIMPULAN DAN SARAN

Bab ini berisi kesimpulan dan saran berdasarkan hasil evaluasi aplikasi perangkat lunak, serta rencana implementasi aplikasi. perangkat lunak.