BAB I
PENDAHULUAN

1.1 Latar Belakang

Seiring dengan berkembangnya teknologi dengan pesat di era sekarang menuntut segala pelayanan publik untuk semakin efisien, salah satunya dari sektor kesehatan yakni rumah sakit[1]. Sejalan dengan perkembangan dunia teknologi informasi yang semakin masif, teknologi informasi merupakan hal penting untuk meningkatkan kualitas pelayanan kesehatan kepada pasien agar mendapatkan pelayanan yang baik dan terarah[1]. Sistem pendaftaran pasien telah banyak diterapkan di berbagai wilayah di Indonesia dan penggunaan sistem pendaftaran pasien online ini memberikan dampak positif bagi masyarakat[2]. Dengan adanya sistem pendaftaran pasien dapat memberikan kemudahan kepada pasien tanpa harus menunggu lama untuk mendapatkan pelayanan kesehatan[3].

Saat ini terdapat banyak aplikasi yang sedang dikembangkan, salah satunya aplikasi yang berbasis *Android*. *Android* merupakan sistem operasi *smartphone* yang sangat popular dan membuat *android* menjadi sangat rentan, terdapat celah keamanan sistem aplikasi yang dapat dimanfaatkan oleh banyak peretas[4]. Penyerang berusaha menyusup dan dapat memanfaatkan celah keamanan pada aplikasi untuk mencuri berbagai data penting dari pengguna[4]. Oleh karena itu, sistem *android* harus terjaga dari berbagai ancaman *malware* dengan mengawasi izin akses yang diberikan oleh pengguna. Analisis merupapakn bagian dari implementasi dan alat pengukur keamanan informasi dari serangan siber, analisis terhadap keamanan sistem pada sebuah instansi harus dilakukan secara rutin[5].

Penggunaan *vulnerability assessment* digunakan dalam menguji aplikasi yang memiliki celah kerentanan. Pada saat yang sama dapat digunakan juga untuk mendeteksi masa berlaku dari perangkat lunak, *port* yang terbuka, serta aplikasi yang berjalan. Di samping itu, *vulnerability assessment* juga berguna untuk mendeteksi kelemahan pada jaringan[6]. Metode *vulnerability assessment* dapat digunakan tanpa perlu mengetahui struktur rancang dari target yang dituju, sehingga metode ini cocok untuk digunakan dalam melakukan deteksi dini celah keamanan pada suatu sistem[7]. Dengan melakukan *vulnerability assessment* dapat membantu pihak terkait dalam mengambil tindakan secara dini dalam pencegahan terhadap serangan yang kemungkinkan dapat menyerang sistem[6]. *Vulnerability assessment* menggunakan OWASP atau *Open Web Application Security Procject* sebagai tools dalam mencari celah keamanan pada sistem karena gratis dan *open source*. OWASP Mobile Top Ten merupakan dokumentasi 10 kelemahan terpopuler dalam pengujuan keamanan pada aplikasi[8]. Penggunaan OWASP Mobile Top Ten dalam

metode *vulnerability assessment* cocok digunakan dalam pengujian dan deteksi dini celah keamanan pada suatu sistem, terutama sistem pendaftaran pada rumah sakit.

Dalam penelitian ini berfokus pada deteksi dini keamanan sistem pada SIMPONI dengan menggunakan metode *vulnerability assessment.* Penggunaan metode ini dapat mendukung dalam menemukan celah keamanan pada sistem SIMPONI dan dapat menganalisis bukti-bukti celah keamanan yang ada pada sistem tersebut. Penelitian ini penting dengan melaksanakan *assessment* pada SIMPONI dikarenakan pada sistem ini hendaknya menerapkan keamanan sistem yang lebih baik untuk mengetahui celah keamanan yang ada pada aplikasi dan mengurangi risiko ancaman pada serta mengantisipasi sebelum terjadi serangan terhadap SIMPONI. Hal ini penting dilakukan karena pada masa pandemi *covid-19* terdapat kebocoran data sebanyak 6 juta data pasien yang berisikan data penting pasien dan surat rujukan BPJS Kesehatan[9].

1.2 Perumusan Masalah

Penulis mekaji terkait permasalahan yang ada pada keamanan sistem di SIMPONI RSUD XYZ yang berfokus terhadap *vulnerability* pada aplikasi tersebut. Permasalahan yang akan diuraikan dalam penelitian ini sebagai berikut:

a. Apa metode yang dapat digunakan untuk melakukan *vulnerability assessment* pada SIMPONI?
b. Bagaimana memberikan feedback kepada developer SIMPONI apabila terdapat celah keamanan?

1.3 Tujuan

Adapun tujuan dari penelitian ini adalah:

a. Mengetahui metode yang digunakan dalam melakukan *vulnerability assessment* pada SIMPONI dan mengetahui tingkat keefektifan metode yang digunakan.
b. Dapat memberikan feedback berupa rekomendasi perbaikan terhadap celah keamanan berdasarkan celah keamanan yang ditemukan kepada developer SIMPONI.

1.4 Rencana Kegiatan

Rencana kegiatan yang akan dilakukan memiliki beberapa tahap.

Tahap pertama dalam penelitian adalah melakukan *risk* identification yakni mengidentifikasi masalah dan tujuan dalam melakukan penelitian ini pada SIMPONI. Selanjutnya penulis melakukan tahap kedua yakni melakukan *configuration and* preminary yang bertujuan untuk menyiapkan lingkungan uji, yakni SIMPONI, lalu melakukan konfigurasi alat yang digunakan dalam proses pengujian dan pengambilan data sehinnga penyiapan alat atau *tools* dapat dilakukan. Pada tahap ketiga, penulis akan melakukan detection, pada tahap detection ini melakukan beberapa langkah agar mendapatkan hasil sesuai dengan masalah dan tujuan, langkah yang akan dilakukan yakni melakukan *footprinting*, *scanning vulnerability*, dan *pentesting*. Setelah hasil pada tahap ketiga didapatkan, penulis akan melakukan analisis agar dapat menyimpulkan hasil yang didapatkan. Pada tahap terakhir melakukan rekomendasi perbaikan dari hasil analisis dan membuat laporan yang mencakup Kesimpulan dan temuan pada celah keamanan SIMPONI yang didasarkan dengan standar pada OWASP Top Ten.

1.5 Jadwal Kegiatan

Berdasarkan rencana kegiatan, jadwal pelaksanaan dibuat bulan ke bulan:

Tabel 1. 1 Tabel Jadwal Kegiatan

Kegiatan	**Bulan**					
Risk Identification	1	2	3	4	5	6
Configuration and Preminary						
Detection						
Analisis Hasil						
Maintance						