ANALISIS CELAH KEAMANAN SISTEM INFORMASI RSIA PUTRI SURABAYA MENGGUNAKAN OPEN WEB APPLICATION SECURITY PROJECT (OWASP)

Mahendra Rangga Abimanyu[1], Kharisma Monika Dian Pertiwi[2], Mustafa Kamal[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]mahennnn@students.telkomuniversity.ac.id, [2]kharismamonika@telkomuniversity.ac.id,
[3]mustafakamal@telkomuniversity.ac.id

1. Pendahuluan

Latar Belakang

Perkembangan teknologi saat ini semakin maju dan modern, hal ini membawa perubahan besar dalam kehidupan manusia. Semakin berkembangnya teknologi informasi membuat maraknya kejahatan-kejahatan di internet yang manusia bisa semakin mudah melakukan tindakan kriminal seperti kejahatan siber[1]. Semakin maraknya pengguna internet di kalangan masyarakat luas, semakin tinggi juga peluang kejahatan siber. Peristiwa estonia pada tahun 2007 dan Georgia pada tahun 2008 merupakan contoh serangan siber dengan pemanfaatan *Distributed Denial of Service* (Ddos)[2]. Sistem Informasi Manajemen Rumah Sakit (SIMRS) adalah suatu struktur yang terkait dengan proses pengumpulan, pengolahan, penyajian, analisis, dan penyimpulan informasi, serta penyampaian data yang diperlukan dalam operasional rumah sakit[3]. Hal ini sangat penting untuk dijaga data-data pada sistem informasi rumah sakit, karena data tersebut rentan terhadap kejahatan siber yang dilakukan oleh oknum yang tidak bertanggung jawab. Perlu dilakukannya analisis celah keamanan sistem informasi untuk mengetahui apakah pada sistem informasi pada rumah sakit tersebut rentan terhadap serangan siber. OWASP adalah komunitas profesional keamanan yang mengidentifikasi risiko keamanan aplikasi web paling kritis dalam domain teknologi informasi[4]. Menggunakan metode OWASP bisa mencakup berbagai jenis kerentanan yang dapat mengancam keamanan aplikasi web dan menyediakan langkah-langkah mitigasi yang efektif [5]. Peneliti memilih OWASP karena fokusnya yang spesifik pada sistem informasi, standarnya yang dikenal luas, panduan dan *tools* yang terperinci, pembaruan secara berkala, serta ketersediaan *open source* dan kemudahan implementasi.

Metode ini lebih sesuai dibandingkan dengan ISSAF dan HOTFIT ketika tujuan utama adalah analisis keamanan sistem informasi. *Penetration testing* diperlukan untuk memastikan keamanan sistem informasi dan melindungi data sensitif dari serangan siber, hal ini membuat peneliti menjadi yakin untuk melakukan analisis celah rentan keamanan sistem informasi itu sangat penting untuk dilakukan. Tujuan utama dari OWASP top 10 adalah memberikan pengetahuan kepada IT *Cyber security* dari kesalahan keamanan pada aplikasi web yang memiliki tingkat yang sangat penting[6]. Penelitian ini juga melakukan pembuatan dashboard web yang berisi tentang saat melakukan testing, hasil, rekomendasi perbaikan dan hasil kerentanan yang ditemukan. Studi kasus yang akan menjadi objek penelitian ini adalah website sistem informasi dari RSIA Putri Surabaya. Berdasarkan dari wawancara peneliti, pihak dari Rumah Sakit Putri Surabaya sendiri masih belum pernah melakukan *penetration testing* pada sistem informasi RSIA Putri Surabaya, sedangkan terdapat ribuan data pasien yang harus dijaga privasinya di dalam sistem informasi tersebut. Oleh karena itu, peneliti berniat untuk melakukan analisis celah keamanan sistem informasi RSIA Putri Surabaya ini, guna meminimalisir hal-hal yang tidak diinginkan seperti pencurian data, penyalahgunaan data dan bahkan mengambil ahli sistem oleh pihak penyerang. Untuk itu, dilakukannya *penetration testing* sistem informasi berdasarkan standar keamanan yang ada pada OWASP top 10. Tahapan yang dilakukan peneliti yaitu studi literatur lalu pengumpulan data, melakukan *scanning* sistem informasi pada RSIA Putri Surabaya, *testing*, membuat laporan dan hasil rekomendasi perbaikan berdasarkan standarisasi dari *Common Weakness Enumeration* (CWE). Hasil penelitian ditemukan 3 kerentanan yaitu A02, *Cryptographic Failures,* A04. *Insecure Design* dan A06. *Vulnerable and Outdated Components*.

Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, dapat disimpulkan rumusan masalah pada penelitian ini sebagai berikut:

1. Bagaimana cara melakukan *penetration testing* sistem informasi RSIA Putri Surabaya menggunakan metode OWASP top 10 2021?

2. Bagaimana hasil dari *penetration testing* sistem informasi RSIA Putri Surabaya dengan metode OWASP top 10 2021?
3. Bagaimana rekomendasi perbaikan terhadap hasil pengujian *penetration testing* sistem informasi RSIA Putri Surabaya?
4. Bagaimana cara memantau *penetration testing* RSIA Putri Surabaya pada dashboard website?

Tujuan

Tujuan dari penelitian ini yaitu untuk menganalisis celah kerentanan sistem informasi RSIA Putri Surabaya, dengan melakukan penetration testing dengan menggunakan metode *OWASP Top 10*.

1. Untuk mengetahui cara *penetration testing* pada sistem informasi RSIA Putri Surabaya menggunakan metode OWASP top 10 2021
2. Untuk mendapatkan hasil dari *penetration testing* sistem informasi RSIA Putri Surabaya menggunakan metode OWASP top 10 2021.
3. Dapat merekomendasikan/perbaikan dari hasil *penetration testing* sistem informasi RSIA Putri Surabaya sesuai standarisasi *Common Weakness Enumeration* (CWE).

Dapat melakukan pemantauan SIMRS pada RSIA Putri Surabaya dengan penjelasan setiap celah beserta video dan status celah sudah diselesaikan apa belum.