ABSTRAK

Pada era perkembangan teknologi yang sedang berkembang pesat, pelayanan kesehatan khususnya rumah sakit diminta untuk melakukan pelayanan secara lebih efisien dengan memanfaatkan teknologi informasi. Perlunya implementasi teknologi untuk mempermudah layanan yakni dengan sistem pendaftaran pasien yang memberikan dampak positif akan tetapi juga rentan terhadap ancaman keamanan. Penelitian ini akan berfokus untuk melakukan *vulnerability assessment* dengan mengidentifikasi risiko, menerapkan kontrol keamanan, menemukan masalah keamanan, menanggapi hasil, dan melakukan pelaporan dengan menggunakan OWASP. Metode penelitian dilakukan dari tahapan *footprinting, scanning vulnerability,* hingga penetration testing sehingga menemukan hasil yang dapat dianalisis. Hasil penelitian menunjukan SIMPONI memiliki 26 risiko medium dan 2643 risiko rendah, dengan total sebanyak 2669 kerentanan yang ditemukan. *Penetration testing* menunjukan kerentanan yang berhasil dieksploitasi, seperti adanya *wildcard directive, style-src unsafe*-inline, dan kebocoran informasi sensitif. Penggunaan *Content Security Policy* (CSP), pengamanan cookie, penerapan validasi input, dan melakukan pengaktifan HSTS merupakan rekomendasi perbaikan dari analisis hasil yang ditemukan. Penelitian ini menyimpulkan bahsa sistem SIMPONI masih mempunyai banyak celah keamanan yang harus segera diperbaiki untuk meningkatkan keamanan. Penggunaan alat pentesting yang lebih canggih dan metode yang lebih baik dengan tujuan meningkatkan keakuratan dan efektivitas deteksi kerentanan harus dilakukan merupakan saran untuk penelitian mendatang.

Kata Kunci : *vulnerability assessment,* OWASP, sistem pendaftaran pasien, keamanan sistem, deteksi dini. penetrasi