INTISARI

Perkembangan teknologi informasi di sektor kesehatan mendorong pemanfaatan *website* sebagai media pelayanan publik, termasuk pendaftaran pasien secara daring. Namun, penggunaan *website* yang mengelola data sensitif pasien juga berpeluang meningkatkan risiko terjadinya serangan siber. *Website* Rumah Sakit Emanuel Banjarnegara pernah mengalami insiden keamanan berupa spam pendaftaran dan serangan SQL *Injection* yang berdampak pada perubahan data pasien. Kondisi tersebut menunjukkan perlunya evaluasi keamanan sistem secara menyeluruh. Penelitian ini bertujuan untuk menguji tingkat kerentanan keamanan *website* https://eregister.rsemanuel.com/ menggunakan metode *Vulnerability Assessment and Penetration Testing* (VAPT) berdasarkan standar OWASP Top 10. Metode penelitian yang digunakan adalah VAPT dengan pendekatan *black box testing*, yang meliputi tahapan *planning*, *information gathering*, *vulnerability scanning*, *penetration testing*, dan *reporting*. *Tools* yang digunakan antara lain WhatWeb, Nmap, dan OWASP ZAP. Hasil penelitian menunjukkan bahwa website memiliki sejumlah kerentanan keamanan yang termasuk dalam kategori *Security Misconfiguration*, *Injection*, dan *Security Headers Misconfiguration*. Kerentanan tersebut berpotensi dimanfaatkan untuk mengakses informasi sensitif dan mengganggu integritas sistem. Berdasarkan temuan tersebut, penelitian ini memberikan rekomendasi teknis dan non-teknis untuk meningkatkan keamanan *website*. Penelitian ini menunjukkan bahwa penerapan metode VAPT efektif dalam mengidentifikasi dan mengevaluasi kerentanan keamanan website, serta dapat menjadi dasar perbaikan sistem guna melindungi data pasien dan meningkatkan kepercayaan pengguna.

Kata kunci: keamanan *website*, VAPT, OWASP Top 10

ABSTRACT

Advances in information technology in the health sector have encouraged the use of websites as a medium for public services, including online patient registration. However, the use of websites that manage sensitive patient data also increases the risk of cyber attacks. The Emanuel Banjarnegara Hospital website has experienced security incidents in the form of registration spam and SQL injection attacks that have resulted in changes to patient data. This situation highlights the need for a comprehensive evaluation of system security. This study aims to test the security vulnerability level of the website https://eregister.rsemanuel.com/ using the Vulnerability Assessment and Penetration Testing (VAPT) method based on the OWASP Top 10 standard. The research method used is VAPT with a black box testing approach, which includes the stages of planning, information gathering, vulnerability scanning, penetration testing, and reporting. The tools used include WhatWeb, Nmap, and OWASP ZAP. The results show that the website has a number of security vulnerabilities that fall into the categories of Security Misconfiguration, Injection, and Security Headers Misconfiguration. These vulnerabilities have the potential to be exploited to access sensitive information and compromise system integrity. Based on these findings, this study provides technical and non-technical recommendations to improve website security. This study shows that the application of the VAPT method is effective in identifying and evaluating website security vulnerabilities and can serve as a basis for system improvements to protect patient data and increase user trust. Translated with DeepL.com (free version)

Keywords: website security, VAPT, OWASP Top 10, CVSS