

ABSTRAK

Website layanan e-clinic Klinik Pratama Rawat Jalan Kamandaka berperan penting dalam mendukung layanan dan pengelolaan data klinik. Namun, website tersebut menyimpan data penting dan sensitif sehingga berpotensi menghadapi berbagai ancaman keamanan siber. Selain itu, pengujian keamanan secara menyeluruh perlu dilakukan untuk mengetahui potensi kerentanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Oleh karena itu, penelitian ini bertujuan untuk menganalisis tingkat keamanan website Klinik Kamandaka dengan menggunakan teknik penetration testing yang mengacu pada standar *Penetration Testing Execution Standard (PTES)*. Metode ini terdiri dari beberapa tahapan utama, yaitu *Information Gathering*, *Threat Modelling*, *Vulnerability Analysis*, *Exploitation*, dan *Reporting*. Alat bantu yang digunakan dalam proses pengujian ini meliputi OWASP ZAP, NMAP, dan SQLMap, dengan fokus utama pada identifikasi dan eksploitasi kerentanan seperti SQL Injection dan kelemahan konfigurasi keamanan. Hasil pengujian menunjukkan bahwa website memiliki beberapa kerentanan yang dikategorikan dalam tingkat risiko *medium*, *low*, dan *informational*, dengan total 12 temuan kerentanan berdasarkan hasil *scanning* OWASP ZAP. Pada pengujian eksploitasi, *form login* replika berhasil ditembus menggunakan *payload* SQL Injection, sedangkan *form login* asli berhasil menolak serangan tersebut. Pengujian menggunakan SQLMap juga tidak berhasil karena sistem tidak menyediakan parameter *input* yang dapat diuji secara langsung. Dari keseluruhan proses, dapat disimpulkan bahwa website Klinik Kamandaka sudah memiliki tingkat perlindungan dasar terhadap serangan injeksi, namun masih terdapat beberapa celah keamanan yang perlu diperbaiki.

Kata kunci: Keamanan Website, *Penetration Testing*, PTES, OWASP ZAP, Klinik Kamandaka.

ABSTRACT

The e-clinic service website of the Kamandaka Outpatient Clinic plays a crucial role in supporting clinical services and data management. However, the website stores important and sensitive data, making it vulnerable to various cybersecurity threats. Furthermore, thorough security testing is necessary to identify potential vulnerabilities that could be exploited by malicious parties. Therefore, this study aims to analyze the security level of the Kamandaka Clinic website using penetration testing techniques that adhere to the Penetration Testing Execution Standard (PTES). This method consists of several main stages: Information Gathering, Threat Modelling, Vulnerability Analysis, Exploitation, and Reporting. The tools used in this testing process include OWASP ZAP, NMAP, and SQLMap, with a primary focus on identifying and exploiting vulnerabilities such as SQL Injection and security configuration weaknesses. The test results indicate that the website has several vulnerabilities categorized as medium, low, and informational, with a total of 12 vulnerabilities identified based on the OWASP ZAP scanning results. In the exploitation test, the replica login form was successfully penetrated using a SQL Injection payload, while the original login form successfully resisted the attack. Testing using SQLMap was also unsuccessful because the system did not provide input parameters that could be tested directly. From the overall process, it can be concluded that the Kamandaka Clinic website already has a basic level of protection against injection attacks, but there are still several security vulnerabilities that need to be fixed..

Keywords: Website Security, Penetration Testing, PTES, OWASP ZAP, Kamandaka Clinic.