INTISARI

Perkembangan teknologi informasi membawa manfaat besar, tetapi juga meningkatkan ancaman keamanan siber seperti serangan *SQL* Injection. Salah satu kasus potensial adalah ancaman pada keamanan data pelanggan Tikako Hotel Banjarnegara, yang menggunakan database terenkripsi untuk mengelola data sensitif. Penelitian ini bertujuan menganalisis kerentanan sistem terhadap serangan *SQL* Injection menggunakan metode *Vulnerability Assessment and Penetration Testing* (VAPT). Metode penelitian melibatkan beberapa tahap yaitu *Planning*, *Information Gathering* dengan Nmap, *Vulnerability Scanning* menggunakan ZAP Proxy, *Penetration Testing* dengan payload *SQL Injection*, serta *tools SQL*Map, dan *Reporting*. Hasil pengujian menunjukkan bahwa serangan berhasil melalui payload pada form login, yang memungkinkan akses tidak sah ke halaman admin. Namun, pengujian dengan *SQL*Map gagal karena perlindungan tambahan seperti validasi input. Penelitian ini menegaskan pentingnya validasi input ketat dan penggunaan teknik keamanan seperti *parameterized query* untuk mencegah serangan *SQL Injection*. Rekomendasi diberikan kepada pengelola sistem untuk memperkuat keamanan dengan enkripsi *end-to-end* pada data sensitif serta melakukan pengujian keamanan secara berkala. Hasil penelitian ini memberikan wawasan praktis dalam menangani ancaman keamanan siber terhadap sistem berbasis *database*.

Kata kunci: *SQL Injection*, *Vulnerability Assessment Penetration Testing*, *Website*, Tikako Hotel, keamanan database.

ABSTRACT

The development of information technology brings great benefits, but also increases cybersecurity threats such as SQL Injection attacks. One potential case is the threat to the security of Tikako Hotel Banjarnegara's customer data, which uses an encrypted database to manage sensitive data. This research aims to analyze system vulnerabilities to SQL Injection attacks using the Vulnerability Assessment and Penetration Testing (VAPT) method. The research method involves several stages, namely Planning, Information Gathering with Nmap, Vulnerability Scanning using ZAP Proxy, Penetration Testing with SQL Injection payload, and SQLMap tools, and Reporting. The test results showed that the attack was successful through the payload on the login form, which allowed unauthorized access to the admin page. However, testing with SQLMap failed due to additional protections such as input validation. This research confirms the importance of strict input validation and the use of security techniques such as parameterized queries to prevent SQL Injection attacks. Recommendations are given to system administrators to strengthen security with end-to-end encryption on sensitive data as well as conduct regular security testing. The results of this research provide practical insights in dealing with cybersecurity threats to database-based systems. Translated with DeepL.com (free version).

Keywords: SQL Injection, Vulnerability Assessment Penetration Testing, Website, Tikako Hotel, security database.