

INTISARI

Keamanan aplikasi web menjadi prioritas utama seiring dengan meningkatnya ancaman siber yang semakin kompleks, terutama serangan SQL injection dan Cross-Site Scripting (XSS). Penelitian ini bertujuan untuk membandingkan efektivitas Burp Suite dan OWASP-ZAP dalam mendeteksi kerentanan injeksi dan XSS pada website DVWA. Penelitian dilakukan dengan menguji berbagai tingkat keamanan yang disediakan oleh DVWA menggunakan kedua alat tersebut. Hasil penelitian menunjukkan bahwa OWASP-ZAP lebih efektif dalam mendeteksi kerentanan yang lebih kompleks, terutama pada tingkat yang lebih tinggi, seperti dibandingkan dengan injeksi SQL dan payload berbasis XSS. Sebaliknya, Burp Suite CE cukup efektif dalam mendeteksi kerentanan dasar pada tingkat rendah hingga menengah, namun kurang berhasil pada kerentanan yang lebih kompleks.

Kata Kunci : Keamanan Aplikasi Web, SQL injection, Cross-Site Scripting, Burp Suite CE, OWASP-ZAP, DVWA



ABSTRACT

Web application security has become a top priority as cyber threats are becoming increasingly complex, particularly SQL injection and Cross-Site Scripting attacks. (XSS). This research aims to compare the effectiveness of Burp Suite and OWASP-ZAP in detecting injection vulnerabilities and XSS on the DVWA website. The study was conducted by testing various security levels provided by DVWA using both tools. The research results indicate that OWASP-ZAP is more effective in detecting more complex vulnerabilities, especially at higher levels, compared to SQL injection and XSS-based payloads. In contrast, Burp Suite CE is quite effective in detecting basic vulnerabilities at low to medium levels, but it struggles with more complex vulnerabilities.

Keywords: Web Application Security, SQL Injection, Cross-Site Scripting, Burp Suite CE, OWASP-ZAP, DVWA

