ABSTRAK

ANALISIS KOMPARATIF TERHADAP ALAT UJI PENETRASI UNTUK MENDETEKSI KERENTANAN APLIKASI WEB BERDASARKAN *OPEN WORLDWIDE APPLICATION SECURITY TOP TEN*

Youvan Alfiz Farandi Putra Hermawan

H1D022087

Penelitian ini bertujuan untuk menganalisis dan membandingkan efektivitas beberapa *Web Vulnerability Scanne*r (WVS) gratis dalam mendeteksi kerentanan aplikasi web berdasarkan *ground truth* yang terverifikasi. Alat yang diuji dalam penelitian ini meliputi OWASP ZAP, Xray, Nikto, dan Nuclei. *Framework* uji yang digunakan adalah *Damn Vulnerable Web Application* (DVWA) yang dikonfigurasi pada tingkat keamanan rendah untuk memastikan seluruh kerentanan dapat terdeteksi. Pengujian dilakukan dalam dua lingkungan berbeda, yaitu *Virtual Private Server* (VPS) dan *localhost*, menggunakan pendekatan *black-box testing* tanpa konfigurasi tambahan di luar pengaturan bawaan masing-masing alat. *Ground truth* dibagi menjadi dua kategori utama, yaitu kerentanan berbasis eksploitasi dan kerentanan berbasis kesalahan konfigurasi (*misconfiguration*). Evaluasi dilakukan menggunakan metrik *precision*, *recall*, dan *F1-score* untuk mengukur akurasi serta cakupan deteksi masing-masing alat. Hasil penelitian menunjukkan bahwa Xray memiliki performa lebih baik dalam mendeteksi kerentanan berbasis eksploitasi seperti *Injection* dan *Cross-Site Scripting* (XSS), sementara ZAP dan Nikto lebih konsisten dalam mendeteksi kerentanan berbasis konfigurasi seperti *missing security headers* dan *directory browsing*. Nuclei menunjukkan keterbatasan pada lingkungan VPS akibat *timeout*, namun performanya meningkat pada lingkungan lokal. Secara umum, tidak terdapat satu alat yang unggul pada seluruh kategori OWASP Top Ten 2025. Hasil penelitian ini menunjukkan bahwa efektivitas WVS sangat bergantung pada kategori kerentanan dan lingkungan pengujian. Oleh karena itu, pemilihan alat pemindaian sebaiknya disesuaikan dengan tujuan pengujian dan karakteristik sistem yang diuji.

Kata Kunci: Black-box Testing, Keamanan Aplikasi Web, OWASP Top Ten 2025, Web Vulnerability Scanner.

ABSTRAK

COMPARATIVE ANALYSIS OF PENETRATION TESTING TOOLS FOR DETECTING WEB APPLICATION VULNERABILITIES BASED ON THE OPEN WORLDWIDE APPLICATION SECURITY TOP TEN

Youvan Alfiz Farandi Putra Hermawan

H1D022087

This study aims to analyze and compare the effectiveness of several free Web Vulnerability Scanners (WVS) in detecting web application vulnerabilities based on a verified ground truth. The tools tested in this research include OWASP ZAP, Xray, Nikto, and Nuclei. The testing framework used is the Damn Vulnerable Web Application (DVWA), configured at a low security level to ensure all vulnerabilities can be detected. Testing was conducted in two different environments, namely a Virtual Private Server (VPS) and localhost, utilizing a black-box testing approach without additional configuration beyond the default settings of each tool. The ground truth is divided into two main categories: exploitation-based vulnerabilities and misconfiguration-based vulnerabilities. The evaluation was performed using precision, recall, and F1-score metrics to measure the accuracy and detection coverage of each tool. The results show that Xray has better performance in detecting exploitation-based vulnerabilities such as Injection and Cross-Site Scripting (XSS), while ZAP and Nikto are more consistent in detecting configuration-based vulnerabilities such as missing security headers and directory browsing. Nuclei demonstrated limitations in the VPS environment due to timeouts, but its performance improved in the local environment. In general, no single tool excels across all OWASP Top Ten 2025 categories. The results of this study indicate that the effectiveness of a WVS is highly dependent on the vulnerability category and the testing environment. Therefore, the selection of a scanning tool should be tailored to the testing objectives and the characteristics of the system being tested.

Keywords: *Black-box Testing, OWASP Top Ten 2025, Web Application Security, Web Vulnerability Scanner.*