INTISARI

Perkembangan teknologi informasi yang semakin pesat telah memberikan dampak signifikan pada berbagai aspek kehidupan. Keamanan siber menjadi isu penting dalam era digital ini, mengingat meningkatnya ancaman terhadap sistem digital seperti situs *web* dan aplikasi *web*. Penelitian ini bertujuan untuk mengembangkan sebuah *platform* pengujian penetrasi berbasis *web* yang menggunakan integrasi Burp Suite API, dengan fokus pada deteksi dan mitigasi kerentanan keamanan. Penelitian ini menggunakan teknik *Automated Scaning* dengan metode *Dynamic Application Security Testing* (DAST), untuk mengidentifikasi dan menganalisis kerentanan pada *website*. *Platform* yang dikembangkan memungkinkan pengguna untuk memasukkan URL atau file JSON, yang kemudian akan dipindai secara otomatis oleh sistem. Penelitian ini menguji dua *website*, yaitu Acunetix dan Adaptach. Untuk situs *web* Acunetix, Burp Suite menemukan 1 kerentanan dengan tingkat keparahan *High*, 0 kerentanan *Medium*, 1 kerentanan *Low*, dan 3 kerentanan *Informational*. OWASP ZAP menemukan 0 kerentanan dengan tingkat keparahan *High*, 3 kerentanan *Medium*, 3 kerentanan *Low*, dan 5 kerentanan *Informational*. Untuk situs *web* Adaptach, Burp Suite menemukan 2 kerentanan dengan tingkat keparahan *High*, 0 kerentanan *Medium*, 7 kerentanan *Low*, dan 10 kerentanan *Informational*. OWASP ZAP menemukan 0 kerentanan dengan tingkat keparahan High, 4 kerentanan *Medium*, 7 kerentanan *Low*, dan 6 kerentanan *Informational*. Dibandingkan dengan OWASP ZAP yang hanya menghasilkan kerentanan *medium*, Burp Suite cenderung melakukan eksplorasi lebih mendalam dengan menghasilkan lebih banyak request, meskipun memerlukan waktu pemindaian yang lebih lama. Hasil penelitian menunjukkan bahwa integrasi Burp Suite API dalam *platform* ini efektif dalam mengidentifikasi berbagai jenis kerentanan dengan akurasi tinggi. *Platform* ini juga dirancang dengan antarmuka pengguna yang intuitif dan mendukung pemindaian paralel. *Platform* ini tidak hanya mempermudah proses pemindaian dan pelaporan, tetapi juga membantu tim keamanan untuk lebih responsif dalam menangani ancaman.

Kata Kunci: Keamanan Siber, Pengujian Penetrasi, Burp Suite API, OWASP ZAP, Platform web

ABSTRACT

The rapid advancement of information technology has significantly impacted various aspects of life. In this digital era, cybersecurity has become a crucial issue, given the increasing threats to digital systems such as websites and web applications. This research aims to develop a web-based penetration testing platform integrating the Burp Suite API, focusing on the detection and mitigation of security vulnerabilities. The study employs Automated Scanning techniques using the Dynamic Application Security Testing (DAST) method to identify and analyze website vulnerabilities. The developed platform allows users to input URLs or JSON files, which are then automatically scanned by the system. The research tested two websites, Acunetix and Adaptach. For the Acunetix website, Burp Suite identified 1 High severity vulnerability, 0 Medium, 1 Low, and 3 Informational. In contrast, OWASP ZAP found 0 High severity vulnerabilities, 3 Medium, 7 Low, and 5 Informational. For the Adaptach website, Burp Suite discovered 2 High severity vulnerabilities, 0 Medium, 7 Low, and 10 Informational, while OWASP ZAP found 0 High severity vulnerabilities, 4 Medium, 7 Low, and 6 Informational. Compared to OWASP ZAP, which mostly identified medium severity vulnerabilities, Burp Suite tends to conduct a more in-depth exploration, generating more requests albeit requiring longer scan times. The results indicate that integrating the Burp Suite API into this platform is effective in identifying various types of vulnerabilities with high accuracy. Additionally, the platform is designed with an intuitive user interface and supports parallel scanning, making the scanning and reporting process easier and helping security teams respond more promptly to threats.

***Keywords**: Cybersecurity, Penetration Testing, Burp Suite API, OWASP ZAP, Web Platform*