

ABSTRAK

Penelitian ini bertujuan untuk menganalisis keamanan aplikasi web menggunakan metode *penetration testing* dengan pendekatan *black-box* berdasarkan standar OWASP Top 10 2021. Objek penelitian yang digunakan adalah OWASP Juice Shop, yaitu aplikasi web yang dirancang secara khusus sebagai media pembelajaran keamanan aplikasi web dalam lingkungan yang aman, legal, dan terkontrol. Tahapan penelitian meliputi instalasi aplikasi, pengumpulan informasi, pemindaian kerentanan, eksploitasi secara terkontrol, analisis hasil pengujian, serta penyusunan rekomendasi perbaikan. Pengujian dilakukan menggunakan beberapa tools, yaitu Burp Suite Community Edition, OWASP ZAP, SQLMap, dan Nmap. Hasil penelitian menunjukkan bahwa metode *penetration testing* berbasis *black-box* mampu mengidentifikasi karakteristik kerentanan keamanan pada aplikasi OWASP Juice Shop sesuai kategori OWASP Top 10 2021. Kerentanan yang berhasil diidentifikasi meliputi *Broken Access Control*, *Cryptographic Failures*, *Injection*, *Insecure Design*, *Security Misconfiguration*, *Vulnerable and Outdated Components*, serta *Identification and Authentication Failures*. Sementara itu, pada kategori *Software and Data Integrity Failures*, *Security Logging and Monitoring Failures*, dan *Server-Side Request Forgery (SSRF)* tidak ditemukan bukti kerentanan yang dapat dikonfirmasi berdasarkan pendekatan *black-box* yang digunakan. Penelitian ini menunjukkan bahwa *penetration testing* dengan pendekatan *black-box* efektif digunakan untuk mengidentifikasi dan menganalisis kerentanan keamanan aplikasi web tanpa memerlukan akses terhadap kode sumber maupun konfigurasi internal aplikasi. Selain itu, penelitian ini menghasilkan rekomendasi perbaikan keamanan yang dapat dijadikan acuan dalam meningkatkan keamanan aplikasi web berdasarkan standar OWASP Top 10 2021.

Kata Kunci: *Penetration testing*, *black-box testing*, OWASP Top 10 2021, OWASP Juice Shop, keamanan aplikasi web.

ABSTRACT

This study aims to analyze the security of a web application using the black-box penetration testing approach based on the OWASP Top 10 2021 standard. The research object is OWASP Juice Shop, a deliberately vulnerable web application designed as a learning platform for web application security in a safe, legal, and controlled environment. The research stages consisted of application installation, information gathering, vulnerability scanning, controlled exploitation, result analysis, and security improvement recommendations. The security assessment was conducted using Burp Suite Community Edition, OWASP ZAP, SQLMap, and Nmap. The results indicate that the black-box penetration testing approach successfully identified security vulnerabilities in OWASP Juice Shop according to the OWASP Top 10 2021 categories. The identified vulnerabilities include Broken Access Control, Cryptographic Failures, Injection, Insecure Design, Security Misconfiguration, Vulnerable and Outdated Components, and Identification and Authentication Failures. Meanwhile, no confirmed vulnerabilities were found in the Software and Data Integrity Failures, Security Logging and Monitoring Failures, and Server-Side Request Forgery (SSRF) categories within the limitations of the black-box testing approach. The findings demonstrate that black-box penetration testing is an effective method for identifying and analyzing web application security vulnerabilities without requiring access to the application's source code or internal configuration. Furthermore, this study provides security improvement recommendations that can serve as references for enhancing web application security in accordance with the OWASP Top 10 2021 standard.

Keywords: penetration testing, black-box testing, OWASP Top 10 2021, OWASP Juice Shop, web application security.