INTISARI

EVALUASI PERFORMA *WEB APPLICATION FIREWALL OPEN-SOURCE* DALAM PERLINDUNGAN APLIKASI WEB RENTAN TERHADAP SERANGAN OTOMATIS

Eko Bagas Cahyoto

21/474531/SV/18962

Ancaman yang dihadapi aplikasi web terus berkembang dalam skala dan kecanggihan membuatnya semakin sulit dideteksi. Hal ini mendorong kebutuhan solusi keamanan yang dapat diandalkan, seperti *Web Application Firewall* (WAF) yang dirancang khusus untuk melindungi aplikasi web. Penelitian ini mengevaluasi efektivitas WAF *open-source* dalam melindungi aplikasi web yang rentan dari serangan otomatis dengan arsitektur *reverse proxy* berbasis Docker. WAF yang diuji mencakup model berbasis aturan (ModSecurity dan Coraza) serta model berbasis *machine learning* (open-appsec dan SafeLine). Pengujian dilakukan menggunakan alat *penetration testing* otomatis yang menyimulasikan berbagai jenis serangan. Hasil menunjukkan bahwa seluruh WAF mencapai efektivitas 100% terhadap serangan XSS (Dalfox) dan cukup efektif terhadap serangan SQL *Injection* (SQLMap) dengan efektivitas berkisar antara 72,73% hingga 100%. open-appsec secara konsisten menunjukkan performa terbaik, terutama dalam skenario SQLMap dan Dirsearch. Namun, efektivitasnya menurun signifikan dalam skenario pemindaian celah keamanan tidak sah (ZAP), dengan efektivitas serendah 19,74%. Dalam skenario *Denial of Service* (DoS), tingkat mitigasi bervariasi, dengan SafeLine menunjukkan efektivitas tertinggi sebesar 94,29%.

Kata kunci: *Web Application Firewall* (WAF), Kerentanan Web, Pengujian Penetrasi, Serangan Otomatis, *Reverse Proxy*, Docker

ABSTRACT

EVALUATION OF THE PERFORMANCE OF OPEN-SOURCE WEB APPLICATION FIREWALLS IN PROTECTING VULNERABLE WEB APPLICATIONS AGAINST AUTOMATED ATTACKS

Eko Bagas Cahyoto

21/474531/SV/18962

Threats facing web applications continue to grow in scale and sophistication, making them increasingly difficult to detect. This drives the need for reliable security solutions, such as Web Application Firewalls (WAFs) that are specifically designed to protect web applications. This study evaluates the effectiveness of open-source WAFs in protecting vulnerable applications from automated attacks using a Docker-based reverse proxy architecture. The tested WAFs include rule-based models (ModSecurity and Coraza) and machine learning-based models (open-appsec and SafeLine). Automated penetration testing tools were employed to simulate various attack scenarios. Results show that all WAFs achieved 100% effectiveness against XSS attacks (Dalfox) and performed well against SQL injection (SQLMap), with effectiveness ranging from 72.73% to 100%. open-appsec consistently outperformed others, particularly in SQLMap and Dirsearch scenarios. However, performance dropped significantly in unauthorized vulnerability scans (ZAP), with effectiveness as low as 19.74%. In Denial of Service (DoS) scenarios, mitigation effectiveness varied, with SafeLine achieving the highest impact reduction of 94.29%.

Keyword: Web Application Firewall (WAF), Web Vulnerabilities, Penetration Testing, Automated Attacks, Reverse Proxy, Docker