

**ANALISIS KERENTANAN WEB API STUDI KASUS : DAMN  
VULNERABLE WEB SERVICES-NODE YANG MENGGUNAKAN WEB  
APPLICATION FIREWALL OPEN-APPSEC**

**MUHAMMAD THORIQ AL-FATIH**

**ABSTRAK**

Penelitian ini membahas analisis kerentanan Web API dengan studi kasus pada Damn Vulnerable Web Services-Node (DVWS-Node) yang menggunakan Web Application Firewall (WAF) open-appsec. Web API, sebagai bagian integral dari pengembangan aplikasi web modern, sering menjadi target serangan karena akses publik dan potensi kelemahan keamanan yang signifikan. Studi ini bertujuan untuk mengidentifikasi dan menganalisis kerentanan pada DVWS-Node serta mengevaluasi efektivitas WAF open-appsec dalam mencegah berbagai jenis serangan web. Metode penelitian meliputi identifikasi masalah, studi literatur, pemasangan dan perancangan DVWS-Node dan open-appsec, serta uji kerentanan dengan menggunakan burpsuite. Hasil penelitian menunjukkan bahwa WAF open-appsec efektif dalam mendeteksi dan mencegah serangan-serangan tersebut tanpa memerlukan perancangan tambahan yang signifikan. Ini menunjukkan bahwa WAF open-appsec dapat meningkatkan keamanan aplikasi web secara substansial, melindungi data sensitif, dan memastikan integritas sistem dari berbagai ancaman keamanan web. Penelitian ini memberikan kontribusi penting dalam bidang keamanan siber dengan menunjukkan pentingnya implementasi WAF dalam melindungi aplikasi web dari serangan yang berpotensi merusak. Selain itu, hasil penelitian ini juga dapat digunakan sebagai referensi bagi pengembang dan profesional keamanan dalam meningkatkan keamanan API mereka.

Kata Kunci: OPEN-APPSEC, WAF, Damn Vulnerable Web Services-Node

**ANALISIS KERENTANAN WEB API STUDI KASUS : DAMN  
VULNERABLE WEB SERVICES-NODE YANG MENGGUNAKAN *WEB  
APPLICATION FIREWALL OPEN-APPSEC***

**MUHAMMAD THORIQ AL-FATIH**

**ABSTRACT**

*This research discusses the analysis of Web API vulnerabilities with a case study on Damn Vulnerable Web Services-Node (DVWS-Node) using the open-appsec Web Application Firewall (WAF). Web APIs, as an integral part of modern web application development, are often targets of attacks due to public access and significant potential security weaknesses. This study aims to identify and analyze vulnerabilities in DVWS-Node and evaluate the effectiveness of the open-appsec WAF in preventing various types of web attacks. The research methodology includes problem identification, literature review, installation and design of DVWS-Node and open-appsec, and vulnerability testing using Burp Suite. The results show that the open-appsec WAF is effective in detecting and preventing these attacks without requiring significant additional design. This indicates that the open-appsec WAF can substantially enhance web application security, protect sensitive data, and ensure system integrity against various web security threats. This research makes an important contribution to the field of cybersecurity by demonstrating the importance of implementing WAF to protect web applications from potentially damaging attacks. Furthermore, the results of this research can be used as a reference for developers and security professionals in improving the security of their APIs.*

*Key Word:* open-appsec, WAF, Damn Vulnerable Web Services-Node