Perancangan dan Evaluasi Arsitektur Infrastruktur Keamanan Berbasis *OPEN SOURCE* Untuk Mitigasi Serangan *CROSS-SITE SCRIPTING (XSS)* Pada Platform *OPEN JOURNAL SYSTEMS* (OJS)

Muhamad Rafly Deandri, 202231038

Dibawah bimbingan M Yoga Distra Sudirman, S.T., MTI

ABSTRAK

Penelitian ini bertujuan untuk merancang dan mengevaluasi arsitektur infrastruktur keamanan berbasis *open source* untuk memitigasi serangan *Cross-Site Scripting* (XSS) pada platform *Open Journal Systems* (OJS). Fokus utama penelitian adalah mengatasi kerentanan *Stored XSS* melalui penguatan lapisan infrastruktur dengan pendekatan *Zero Code Modification*. Metode penelitian yang digunakan adalah eksperimental dengan teknik *Vulnerability Assessment* (VA) menggunakan *tools* XSSer terhadap empat kombinasi teknologi (Apache/Nginx, MariaDB/PostgreSQL), versi PHP (8.0/7.4) dan versi OJS (3.3.0-16 dan 3.4.0-5). Arsitektur mitigasi dibangun di atas *hypervisor* Proxmox VE dengan isolasi *Linux Container* (LXC) serta integrasi *Lightweight Web Application Firewall* (LWAF) di sisi server dan *Content Security Policy* (CSP) di sisi klien sebagai strategi *Defense in Depth*. Hasil pengujian menunjukkan bahwa pada kondisi *baseline*, tingkat keberhasilan serangan rata-rata mencapai 96%, namun setelah penerapan arsitektur mitigasi, angka tersebut berhasil ditekan hingga di bawah 1% pada mayoritas target. Kesimpulan penelitian menetapkan kombinasi Nginx dan PostgreSQL sebagai konfigurasi paling optimal dalam menjaga integritas data dan ketersediaan layanan publikasi ilmiah.

Kata Kunci: *OJS, XSS, Open Source, Infrastruktur Keamanan, LWAF, CSP.*

Design and Evaluation of Open-Source Security Infrastructure Architecture for Cross-Site Scripting (XSS) Attack Mitigation on the Open Journal Systems (OJS) Platform

Muhamad Rafly Deandri, 202231038

Supervised by M Yoga Distra Sudirman, S.T., MTI

ABSTRACT

This study aims to design and evaluate an open-source security infrastructure architecture to mitigate Cross-Site Scripting (XSS) attacks on the Open Journal Systems (OJS) platform. The primary focus of this research is to address Stored XSS vulnerabilities by strengthening the infrastructure layer through a Zero Code Modification approach. The research method is experimental, employing the Vulnerability Assessment (VA) technique using XSSer tools against four technology combinations (Apache/Nginx, MariaDB/PostgreSQL), PHP versions (8.0/7.4), and OJS versions (3.3.0-16 and 3.4.0-5). The mitigation architecture is built on the Proxmox VE hypervisor with Linux Container (LXC) isolation, integrating a Lightweight Web Application Firewall (LWAF) on the server-side and Content Security Policy (CSP) on the client-side as a Defense in Depth strategy. Testing results show that in baseline conditions, the average attack success rate reached 96%; however, following the implementation of the mitigation architecture, this rate was successfully suppressed to below 1% on the majority of targets. The study concludes that the combination of Nginx and PostgreSQL is the most optimal configuration for maintaining data integrity and the availability of scientific publication services.

Keywords: *OJS, XSS, Open Source, Security Infrastructure, LWAF, CSP.*