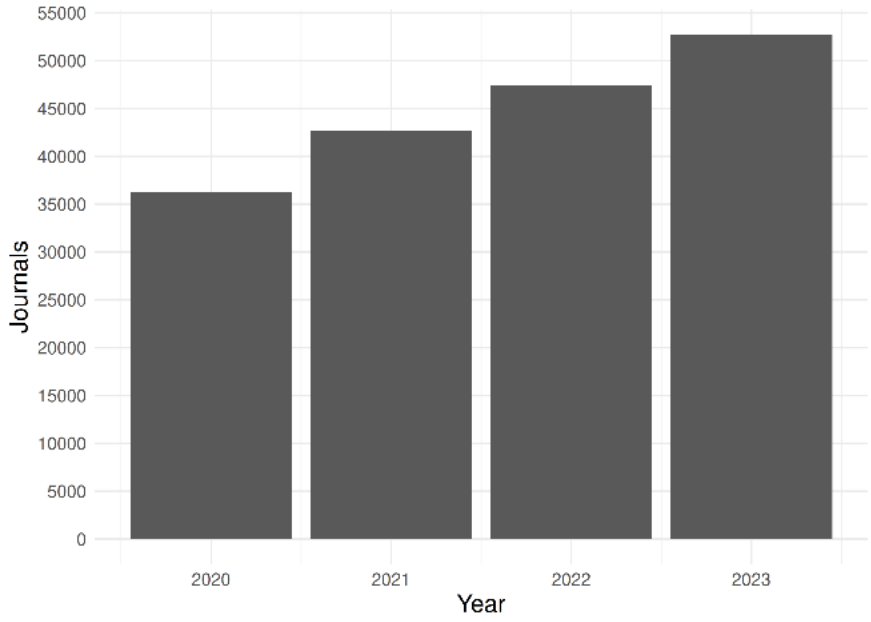
BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dalam bidang publikasi ilmiah mengalami peningkatan yang sangat pesat dalam dua dekade terakhir. Salah satu sistem manajemen jurnal yang paling banyak digunakan secara global adalah *Open Journal Systems* (OJS) yang dikembangkan oleh *Public Knowledge Project* (PKP) sebagai perangkat lunak *open-source* untuk mendukung pengelolaan jurnal ilmiah secara daring. Berdasarkan laporan tahunan PKP tahun 2024 tercatat lebih dari 52.000 jurnal aktif menggunakan OJS di seluruh dunia meningkat sekitar 18% dibandingkan tahun sebelumnya. Tren peningkatan penggunaan platform ini menunjukkan bahwa OJS telah menjadi infrastruktur penting dalam ekosistem publikasi ilmiah global.



Gambar 1. 1 Statistik Pertumbuhan Penggunaan OJS (2020 - 2023)

Sumber**:** PKP Beacon Project (2024)

Gambar 1.1 menunjukkan grafik batang pertumbuhan jumlah jurnal aktif yang menggunakan platform OJS. Berdasarkan grafik tersebut terlihat kenaikan yang konsisten setiap tahunnya. Pada tahun 2023 jumlah jurnal aktif telah mencapai puncaknya melampaui angka 50.000 yang menandakan ketergantungan komunitas ilmiah global terhadap platform ini semakin tinggi. Indonesia sendiri menempati posisi yang sangat

strategis di mana data menunjukkan bahwa Indonesia merupakan negara dengan jumlah pengguna OJS terbanyak di dunia sebagaimana disajikan pada Gambar 1.2. (Public Knowledge Project (PKP), 2024).

	Country	Active OJS Journals in 2023	Percent
1	Indonesia	23486	46.6%
2	Brazil	4032	8%
3	United States	1707	3.39%
4	India	1410	2.8%
5	Spain	1283	2.55%

Gambar 1. 2 Daftar Negara Pengguna OJS Terbesar Tahun 2023

Sumber: PKP Beacon Project (2024)

Gambar 1.2 menyajikan data tabel lima besar negara pengguna OJS di dunia. Berdasarkan tabel tersebut Indonesia menempati urutan pertama dengan total 23.486 jurnal aktif atau setara dengan 46,6% dari total penggunaan global jauh mengungguli negara-negara lain seperti Brazil, Amerika Serikat, India, dan Spanyol. Hal ini menegaskan peran strategis OJS bagi publikasi ilmiah di Indonesia.

Namun peningkatan jumlah pengguna juga diikuti dengan meningkatnya potensi ancaman keamanan siber. Sebagai platform yang bersifat open-source OJS memiliki karakteristik mirip dengan sistem manajemen konten lainnya yang banyak digunakan dan dijalankan di berbagai infrastruktur server yang dikelola secara mandiri dan sangat bergantung pada kepatuhan administrator terhadap praktik keamanan. Menurut OWASP Foundation (2023), serangan *Cross-Site Scripting* (XSS) masih termasuk dalam Top 10 Web *Application Security Risks* global. Serangan XSS memungkinkan penyerang menyisipkan skrip berbahaya ke dalam halaman web sehingga dapat mencuri data pengguna, melakukan session hijacking, atau eskalasi hak akses tanpa sepengetahuan korban.

Urgensi aspek keamanan pada OJS juga ditegaskan oleh Alec Smecher selaku pengembang inti PKP melalui hasil wawancara dengan menggunakan email pada tanggal 2 September 2025. Alec Smecher mengelompokkan beberapa tantangan keamanan yang umum dihadapi pengguna OJS antara lain kerentanan *Remote Code Execution* (RCE),

stored *Cross-Site Scripting* (XSS), supply chain attack melalui dependensi pihak ketiga, kesalahan konfigurasi deployment seperti penempatan files directory di dalam web root, serta penggunaan instalasi yang tidak diperbarui. RCE dipandang sebagai ancaman yang sangat serius karena berpotensi memberikan kendali penuh terhadap server, meskipun kasusnya relatif jarang ditemukan. Sementara itu supply chain attack dinilai sebagai risiko yang semakin meningkat seiring bertambahnya penggunaan komponen pihak ketiga dalam ekosistem OJS. Di antara berbagai ancaman tersebut Alec Smecher menegaskan bahwa stored XSS merupakan kerentanan yang nyata pernah ditemukan pada OJS dan dapat dimanfaatkan penyerang untuk menyisipkan JavaScript berbahaya yang menargetkan pengguna dengan hak akses tinggi seperti Journal Manager atau Site Administrator. Eksploitasi ini berpotensi menyebabkan privilege escalation maupun pencurian kredensial. Dibandingkan dengan RCE yang relatif jarang terjadi serangan XSS memiliki probabilitas kemunculan yang lebih tinggi pada konteks aplikasi web dengan banyak interaksi input seperti OJS sehingga menjadi ancaman yang lebih representatif untuk dikaji dalam lingkungan operasional nyata.

Selain faktor jenis kerentanan penggunaan versi perangkat lunak yang tidak mutakhir juga memperbesar risiko keamanan. Data PKP pada akhir tahun 2024 menunjukkan bahwa sekitar 41% instalasi OJS masih menggunakan versi yang sudah tidak memperoleh dukungan keamanan. Distribusi versi yang beragam termasuk masih banyaknya penggunaan versi legacy menunjukkan adanya kesenjangan antara ketersediaan patch keamanan dan implementasinya di lingkungan produksi. Kondisi ini menjelaskan fakta bahwa banyak institusi cenderung mempertahankan versi tertentu demi stabilitas layanan meskipun pembaruan keamanan telah tersedia. Hasil wawancara ini terlampir pada Lampiran 1.

Di Indonesia implementasi OJS umumnya dilakukan oleh perguruan tinggi dan lembaga penelitian dengan sumber daya yang terbatas. Banyak administrator sistem jurnal tidak memiliki latar belakang khusus di bidang keamanan jaringan maupun keamanan aplikasi web sehingga penerapan hardening sistem sering kali belum optimal. Apabila serangan XSS berhasil dieksploitasi pada sistem jurnal akademik, dampaknya dapat mencakup pencurian kredensial pengguna, manipulasi metadata publikasi, hingga penyalahgunaan hak akses administratif. Dengan meningkatnya ketergantungan institusi

terhadap OJS sebagai tulang punggung publikasi ilmiah, kebutuhan akan mekanisme mitigasi yang efektif menjadi semakin mendesak.

Berdasarkan kondisi tersebut penelitian ini memfokuskan kajian pada mitigasi serangan XSS melalui pendekatan pengamanan berbasis infrastruktur sebagai lapisan pertahanan tambahan (*defense in depth*). Pemilihan fokus pada XSS didasarkan pada bukti bahwa kerentanan ini pernah muncul pada OJS serta memiliki vektor eksploitasi yang realistis pada lingkungan web interaktif. Objek penelitian menggunakan OJS versi 3.3.0-16 dan 3.4.0-5 yang dipilih untuk merepresentasikan dua generasi sistem yang masih banyak digunakan di lingkungan institusi. Lini versi 3.3.x termasuk dalam skema *Long Term Support* (LTS) yang masih luas dioperasikan sedangkan versi 3.4.x merepresentasikan generasi yang lebih baru sehingga memungkinkan evaluasi efektivitas mitigasi pada kondisi yang berbeda.

Berdasarkan dari permasalahan yang dialami tersebut dilakukanlah penelitian ini berjudul **"PERANCANGAN DAN EVALUASI ARSITEKTUR INFRASTRUKTUR KEAMANAN BERBASIS OPEN SOURCE UNTUK MITIGASI SERANGAN CROSS-SITE SCRIPTING (XSS) PADA PLATFORM OPEN JOURNAL SYSTEMS (OJS)"**. Hasil penelitian diharapkan dapat memberikan kontribusi praktis berupa rekomendasi konfigurasi keamanan yang implementatif bagi pengelola jurnal serta kontribusi akademis dalam penguatan kajian keamanan aplikasi web khususnya pada ekosistem OJS melalui penguatan pada sisi infrastruktur.

1.2 Rumusan Masalah

Berdasarkan Latar Belakang yang telah diuraikan terdapat beberapa rumusan masalah dalam penelitian ini sebagai berikut:

1. Apa jenis pola serangan yang umum terjadi pada berbagai OJS?
2. Bagaimana pengaruh konfigurasi infrastruktur berbasis *open source* terhadap tingkat kerentanan OJS terhadap serangan XSS?
3. Bagaimana rancangan konfigurasi infrastruktur yang optimal untuk memitigasi serangan XSS pada OJS?

1.3 Tujuan Masalah

Adapun tujuan dari penelitian ini sebagai berikut:

1. Mengidentifikasi jenis pola serangan pada berbagai versi OJS yang banyak digunakan.
2. Mengidentifikasi kelemahan konfigurasi infrastruktur OJS berbasis *open source* yang berpotensi menjadi celah serangan.
3. Menganalisis pengaruh dari konfigurasi infrastruktur terhadap serangan XSS
4. Merancang konfigurasi infrastruktur keamanan yang tepat untuk meningkatkan ketahanan OJS terhadap serangan XSS.

1.4 Manfaat Penelitian

Berdasarkan tujuan dari penilitian yang ingin dicapai . Adapun manfaat dari penelitian ini sebagai berikut :

1. Manfaat Akademis:

   Penelitian ini diharapkan dapat memperkaya kajian ilmiah di bidang keamanan aplikasi web khususnya terkait kerentanan dan pola serangan XSS pada OJS. Selain itu penelitian ini dapat menjadi referensi bagi mahasiswa dan peneliti yang ingin mengembangkan solusi keamanan berbasis infrastruktur *open source*.
2. Manfaat Praktis:

   Penelitian ini dapat membantu pengelola jurnal dan tim IT perguruan tinggi dalam memahami pola serangan XSS serta menerapkan konfigurasi infrastruktur yang lebih aman. Dengan demikian sistem OJS dapat lebih terlindungi dari ancaman siber dan integritas publikasi ilmiah dapat lebih terjaga.

1.5 Ruang Lingkup Masalah

Agar penelitian lebih fokus dan terarah, ruang lingkup penelitian ini dibatasi pada hal-hal berikut:

1. Objek Penelitian: Platform yang diuji adalah OJS versi 3.3.0-16 LTS dan versi 3.4.0-5. Jenis serangan yang difokuskan adalah XSS.
2. Jenis Kerentanan: Fokus pengujian adalah pada serangan XSS jenis *Stored XSS* yang menargetkan variabel input pada form registrasi bagian givenName, familyName, dan affiliation.
3. Arsitektur Mitigasi: Arsitektur keamanan yang dirancang dan dievaluasi mencakup konfigurasi pada lapisan *Virtual Machine* (VM) menggunakan *Linux*

Container (LXC) pada proxmox VE, penguatan konfigurasi *Web Server*, serta implementasi skrip keamanan sisi server.

4. Teknologi Keamanan: Implementasi pertahanan berfokus pada penggunaan *LightWeight Web Application Firewall* (LWAF) dan *Content Security Policy* (CSP).
5. Lingkungan Pengujian: Eksperimen dilakukan di lingkungan laboratorium komputer yang terisolasi menggunakan jaringan LAN bukan pada sistem jurnal yang sedang berjalan dengan bantuan platform virtualisasi *Proxmox VE* dan menggunakan 4 unit pc dan 1 laptop.
6. Batasan Fokus Pengujian: Penelitian tidak melakukan pengujian terhadap kerentanan pada level infrastruktur sistem operasi (Ubuntu), celah pada *hypervisor* (Proxmox) maupun celah keamanan pada perangkat keras *(hardware)*.
7. Asumsi Penelitian: Seluruh komponen infrastruktur penunjang (OS dan *Hypervisor*) dianggap dalam kondisi terkonfigurasi standar dan aman (*pre-secured*).
8. Vektor Serangan: Pengujian serangan dilakukan secara otomatis menggunakan *tools* XSSer dan divalidasi secara manual melalui browser.
9. Penelitian ini difokuskan pada pengujian serangan dan mitigasi dari sisi infrastruktur tidak mencakupi pengembangan pada OJS.

1.6 Kebaharuan

Penelitian ini menawarkan pendekatan baru dalam mitigasi serangan *Stored* XSS pada platform OJS dengan menitikberatkan pada penguatan arsitektur infrastruktur keamanan berbasis *open source*. Berbeda dengan penelitian sebelumnya yang umumnya berfokus pada perbaikan kode sumber aplikasi atau penggunaan WAF konvensional kebaharuan penelitian ini terletak pada:

1. Pendekatan Arsitektur Agnostik: Mitigasi yang dirancang bersifat agnostik artinya solusi LWAF dan CSP yang diusulkan dievaluasi pada 4 kombinasi teknologi yang berbeda untuk membuktikan efektivitasnya secara universal pada berbagai infrastruktur server.
2. Penerapan *Lightweight Security Middleware*: Penggunaan Lightweight Web Application Firewall (LWAF) dalam bentuk skrip interseptor memberikan solusi

pertahanan aktif yang ringan namun efektif memungkinkan institusi dengan sumber daya *hardware* terbatas melalui LXC untuk memiliki proteksi setingkat *enterprise*.

3. Integrasi Isolasi Container: Penggabungan mekanisme filtrasi paket data dengan isolasi infrastruktur tingkat kontainer menggunakan Proxmox VE yang secara khusus dikonfigurasi untuk memutus rantai serangan lateral (*lateral movement*) antara server aplikasi dan basis data.
4. Solusi *Zero Code Modification*: Penelitian ini memberikan alternatif mitigasi yang dapat diterapkan secara instan tanpa harus mengubah kode inti (*core code*) aplikasi OJS sehingga sangat praktis bagi institusi yang memerlukan perlindungan cepat untuk versi OJS yang belum sempat melakukan pembaruan keamanan.