EVALUASI DAN MITIGASI SERANGAN XSS DAN CSRF PADA *OPEN JOURNAL SYSTEMS* VERSI 3.5 MENGGUNAKAN *HYBRID PENETRATION TESTING* DAN *CVSS SCORING*

SKRIPSI

Program Studi Teknik Elektro
Jurusan Teknik Elektro

Oleh:

DONNY SAPUTRA

NIM. D1021191076

FAKULTAS TEKNIK

JURUSAN TEKNIK ELEKTRO

UNIVERSITAS TANJUNGPURA

PONTIANAK

2026

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama : Donny Saputra

NIM : D1021191076

Menyatakan bahwa dalam SKRIPSI ini yang berjudul "Evaluasi dan Mitigasi Serangan XSS Dan CSRF pada *Open Journal Systems* Versi 3.5 Menggunakan *Hybrid Penetration Testing* dan CVSS *Scoring*" tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu perguruan tinggi manapun. Sepanjang pengetahuan saya, tidak terdapat karya atau pendapat yang pernah ditulis atas diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam Daftar Pustaka.

Demikian pernyataan ini dibuat dengan sebenar-benarnya. Saya sanggup menerima konsekuensi akademis dan hukum di kemudian hari apabila pernyataan yang dibuat ini tidak benar.

Pontianak, 30 Juli 2026

Donny Saputra
NIM D1021191076

KEMENTERIAN PENDIDIKAN TINGGI, SAINS,
DAN TEKNOLOGI
UNIVERSITAS TANJUNGPURA
FAKULTAS TEKNIK
Jalan Prof. Dr. H. Hadari Nawawi Pontianak 78124
Telepon: (0561) 740186, WA: +6282152280907
Email: ft@untan.ac.id Website:http://teknik.untan.ac.id

HALAMAN PENGESAHAN

EVALUASI DAN MITIGASI SERANGAN XSS DAN CSRF PADA *OPEN JOURNAL SYSTEMS* VERSI 3.5 MENGGUNAKAN *HYBRID PENETRATION TESTING* DAN *CVSS SCORING*

Jurusan Teknik Elektro
Program Studi Sarjana Teknik Elektro

Oleh:

Donny Saputra
NIM D1021191076

Telah dipertahankan di depan Penguji Skripsi pada tanggal 30 Juli 2026
dan diterima sebagai salah satu persyaratan untuk memperoleh gelar sarjana.

Susunan Penguji Skripsi

Dosen Pembimbing Utama	: Leonardus Sandy Ade Putra, S.T., M.T., NIP. 199410072020121003
Dosen Pembimbing Kedua	: Ir. H. Fitri Imansyah, S.T., M.T., IPU, ASEAN Eng., ACPE., NIP. 196912271997021001
Dosen Penguji Utama	: Dr. Redi Ratiandi Yacoub, S.T.,M.T., NIP. 197101031997021002
Dosen Penguji Kedua	: Steven Pangestu, S.T., M.T., NIP. 199401122024061001

Pontianak, 30 Juli 2026

Dekan,

Pembimbing Utama

Dr.-Ing. Ir. Slamet Widodo, M.T., IPM
NIP. 196712231992031002

Leonardus Sandy Ade Putra, S.T., M.T.,
NIP. 199410072020121003

KEMENTERIAN PENDIDIKAN TINGGI, SAINS,
DAN TEKNOLOGI
UNIVERSITAS TANJUNGPURA
FAKULTAS TEKNIK
Jalan Prof. Dr. H. Hadari Nawawi Pontianak 78124
Telepon: (0561) 740186, WA: +6282152280907
Email: ft@untan.ac.id Website: http://teknik.untan.ac.id

SURAT KETERANGAN SELESAI PENULISAN SKRIPSI

Yang bertanda tangan di bawah ini Dosen Pembimbing Utama dan Dosen Pembimbing Pendamping pada penulisan skripsi yang berjudul **"Evaluasi dan Mitigasi Serangan XSS Dan CSRF pada Open Journal Systems Versi 3.5 Menggunakan Hybrid Penetration Testing dan CVSS Scoring"** yang ditulis oleh mahasiswa Fakultas Teknik Universitas Tanjungpura.

Nama : Donny Saputra

NIM : D1021191076

Jurusan : Teknik

Prodi : Teknik Elektro

Konsentrasi : Teknik Telekomunikasi

Demikian ini menerangkan bahwa mahasiswa tersebut telah menyelesaikan penulisan skripsinya.

Pontianak, 30 Juli 2026

Pembimbing Utama	Pembimbing Pendamping
Leonardus Sandy Ade Putra, S.T., M.T.,	Ir. H. Fitri Imansyah, S.T., M.T., IPU,
NIP. 199410072020121003	ASEAN Eng., ACPE.,
	NIP. 196912271997021001

ABSTRAK

Open Journal Systems (OJS) merupakan aplikasi pengelolaan jurnal berbasis web yang rentan terhadap serangan *Cross-Site Scripting* (XSS) dan *Cross-Site Request Forgery* (CSRF). Penelitian ini bertujuan mengevaluasi kerentanan keamanan pada OJS versi 3.5, mengukur tingkat risikonya menggunakan *Common Vulnerability Scoring System* (CVSS) v4.0, menerapkan mitigasi pada kode sumber, serta memvalidasi efektivitasnya melalui *retesting*. Metode yang digunakan adalah *Penetration Testing* yang menggunakan *black-box testing* dengan mengacu pada *OWASP Web Security Testing Guide* (WSTG) dan *Penetration Testing Execution Standard* (PTES). Tahapan penelitian meliputi pemindaian kerentanan, pengujian eksploitasi, analisis kode sumber, penilaian risiko menggunakan CVSS, implementasi *secure coding*, dan *retesting*. Hasil penelitian menunjukkan bahwa pendekatan *Penetration Testing* mampu mengidentifikasi kerentanan XSS dan CSRF pada OJS versi 3.5. Mitigasi yang diterapkan berhasil meningkatkan keamanan aplikasi dan mengurangi peluang eksploitasi berdasarkan hasil pengujian ulang. Penelitian ini menunjukkan bahwa kombinasi *Penetration Testing*, CVSS, dan *secure coding* merupakan pendekatan yang efektif untuk mengevaluasi dan meningkatkan keamanan OJS terhadap serangan XSS dan CSRF.

Kata kunci: *Open Journal Systems*, *Penetration Testing*, XSS, CSRF, CVSS.

ABSTRACT

Open Journal Systems (OJS) is a web-based journal management application that is vulnerable to Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF) attacks. This study aims to evaluate security vulnerabilities in OJS version 3.5, assess their risk levels using the Common Vulnerability Scoring System (CVSS) v4.0, implement mitigation measures in the source code, and validate their effectiveness through retesting. The research employs a Penetration Testing approach using black-box testing based on the OWASP Web Security Testing Guide (WSTG) and the Penetration Testing Execution Standard (PTES). The research stages include vulnerability scanning, exploitation testing, source code analysis, risk assessment using CVSS, implementation of secure coding practices, and retesting. The results indicate that the Penetration Testing approach successfully identified XSS and CSRF vulnerabilities in OJS version 3.5. The implemented mitigation measures effectively enhanced the application's security and reduced the likelihood of successful exploitation based on the retesting results. This study demonstrates that the combination of Penetration Testing, CVSS, and secure coding practices is an effective approach for evaluating and improving the security of OJS against XSS and CSRF attacks.

Keywords: *Open Journal Systems, Penetration Testing, XSS, CSRF, CVSS.*

PRAKATA

Puji syukur penulis panjatkan kehadirat Allah Subhanahu Wa Ta'ala atas segala rahmat dan karunia-Nya, penulis diberikan kesanggupan dan kemudahan sehingga mampu menyusun tugas akhir yang berjudul "Evaluasi dan Mitigasi Serangan XSS Dan CSRF pada *Open Journal Systems* Versi 3.5 Menggunakan *Penetration Testing* dan *CVSS Scoring*" ini dapat disusun dengan baik. Shalawat dan salam semoga tercurahkan kepada Nabi Muhammad Shallallahu'Alaihi Wassalam dan kepada keluarganya, Tabi'in, Tabiut Tabi'in serta pengikutnya yang mengikuti beliau hingga akhir zaman.

Tugas akhir ini disusun sebagai salah satu syarat dalam menyelesaikan studi di program sarjana dan dalam penyusunannya penulis mengalami berbagai hambatan. Namun, semua hal itu dapat dilalui dengan pertolongan Allah Subhanahu Wa Ta'ala melalui bantuan dan bimbingan serta pengarahan dari berbagai pihak sehingga penulis dapat menyelesaikan tugas akhir ini. Pada kesempatan ini penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Kedua orang tua dan juga kepada keluarga yang selalu mendoakan. memberi semangat, dan dukungan kepada penulis.
2. Bapak Dr. Ing. Ir. Slamet Widodo, M.T., IPM selaku Dekan Fakultas Teknik Universitas Tanjungpura Pontianak.
3. Bapak Prof. Dr. Ing. Seno Darmawan Panjaitan, S.T., M.T. IPM selaku Ketua Jurusan Teknik Elektro Fakultas Teknik Universitas Tanjungpura.
4. Bapak Jannus Marpaung, S.T., M.T., IPM., selaku Ketua Program Studi Teknik Elektro Fakultas Teknik Universitas Tanjungpura.
5. Ibu Ir. Neilcy Tjahjamooniarsih, S.T., M.T., IPM, selaku kepala Laboratorium Telekomunikasi program studi Teknik Elektro, Fakultas Teknik, Universitas Tanjungpura.
6. Ibu Hilda, S.T., M.T., IPM., ASEAN Eng, selaku Dosen Pembimbing Akademik yang telah mendidik, memberi kritik dan saran selama saya berkuliah.
7. Bapak Leonardus Sandy Ade Putra, S.T., M.T., selaku dosen pembimbing utama yang telah memberikan bantuan, masukan, kritik, serta saran dalam

menyelesaikan tugas akhir.

8. Bapak Ir. H. Fitri Imansyah, S.T., M.T., IPU, ASEAN Eng., ACPE., selaku dosen pembimbing pendamping yang juga memberikan pengarahan dan bimbingan selama penulisan tugas akhir ini.
9. Bapak Dr. Redi Ratiandi Yacoub, S.T.,M.T., Selaku Dosen Penguji Utama yang telah memberi banyak masukan, kritik, dan saran selama proses menyelesaikan tugas akhir ini.
10. Bapak Steven Pangestu, S.T., M.T., Selaku dosen penguji pendamping yang telah memberi banyak masukan, kritik, dan saran selama proses menyelesaikan tugas akhir ini.
11. Comdev & Outreaching Universitas Tanjungpura yang telah membiayai kuliah saya melalui program beasiswa Bidikmisi.
12. Seluruh dosen program studi Teknik Elektro Universitas Tanjungpura yang telah membekali ilmu yang sangat membantu dan bermanfaat bagi penulis.
13. Sahabat, orang terdekat serta teman-teman yang telah memberikan dukungan, masukan, saran, serta solusi dalam penyelesaian tugas akhir ini yang tidak dapat penulis sebutkan satu per satu.

Penulis menyadari bahwa pada penyusunan tugas akhir ini masih jauh dari kesempurnaan karena keterbatasan kemampuan yang penulis miliki, untuk itu penulis masih mengharapkan kritik dan saran demi perbaikan pada masa yang akan datang. Semoga ini dapat memberikan manfaat bagi pengembangan ilmu pengetahuan, khususnya di bidang keamanan siber dan sistem manajemen jurnal berbasis web.

Akhir kata, semoga tugas akhir ini dapat memberikan manfaat dalam menambah wawasan serta pengetahuan.

Pontianak, 27 Juli 2026

Penulis

Donny Saputra

NIM. D1021191076

DAFTAR ISI

ABSTRAK ..... **i**
ABSTRACT ..... **ii**
PRAKATA ..... **iii**
DAFTAR ISI ..... **v**
DAFTAR GAMBAR ..... **viii**
DAFTAR TABEL ..... **x**
DAFTAR LAMPIRAN ..... **xi**
DAFTAR ISTILAH ..... **xii**
DAFTAR SINGKATAN ..... **xiv**
BAB I PENDAHULUAN **1**
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Tujuan Penelitian 3
1.4 Pembatasan Masalah 3
1.5 Sistematika Penulisan 4
BAB II LANDASAN TEORI **2**
2.1 Penelitian Terdahulu **2**
2.2 Landasan Teori **8**
2.2.1 Keamanan Aplikasi Web 8
2.2.2 *Open Journal System* 8
2.2.3 *Penetration Testing* 10
2.2.4 *Kali Linux* 11
2.2.5 OWASP Web Security Testing Guide (WSTG) 12
2.2.6 OWASP Top 10 13
2.2.7 *Cross-Site Scripting* (XSS) 14
2.2.8 *Cross-Site Request Forgery* (CSRF) 15
2.2.9 *Secure Coding* 15
2.2.10 *Common Vulnerability Scoring System* (CVSS) 16
BAB III METODOLOGI PENELITIAN **6**
3.1 Diagram Alir Penelitian **6**

3.2 Alat dan Bahan Penelitian 19
3.2.1 Alat Penelitian 19
3.2.2 Bahan Penelitian 20
3.3 Tempat dan Waktu Penelitian 21
3.4 Metode Penelitian 21
3.5 Variabel atau Data 24
3.5.1 Pemetaan Titik Serangan OJS 24
3.5.2 Parameter Penilaian Risiko 25
3.5.3 Mitigasi dan *Retesting* 26
3.6 Analisa Hasil 26
3.6.1 Analisa Hasil Serangan OJS 26
3.6.2 Analisa Penilaian Risiko 27
3.6.3 Analisa Mitigasi dan Hasil *Retesting* 28
BAB IV HASIL DAN PEMBAHASAN 19
4.1 Deskripsi Umum Hasil Pengujian 19
4.2 Pengujian Kerentanan *Cross-Site Scripting* (XSS) 30
4.2.1 Pengujian Stored XSS pada *Endpoint Title Field* Pengajuan Naskah (*Submission)* 30
4.2.2 Pengujian Stored XSS pada *Endpoint Abstract Field* Pengajuan Naskah (*Submission)* 35
4.2.3 Pengujian Stored XSS pada *Endpoint Keyword Field* Pengajuan Naskah (*Submission)* 38
4.2.4 Pengujian Stored XSS pada *Endpoint References Field* Pengajuan Naskah (*Submission)* 40
4.2.5 Pengujian Stored XSS pada *Endpoint Review Comment* Pengajuan Naskah (*Submission)* 43
4.2.6 Pengujian Reflected XSS pada *Endpoint Search Submission/Metadata* Pengajuan Naskah (*Submission)* 47
4.2.7 Pengujian Stored XSS pada *Endpoint Review Comment* (*Reviewer*) 50
4.3 Pengujian Kerentanan *Cross-Site Request Forgery* (CSRF) 53
4.3.1 Pengujian CSRF pada *Endpoint Save New Submission* Pengajuan Naskah (*Submission)* 54

4.3.2 Pengujian CSRF pada *Endpoint Update Submission Metadata* Pengajuan Naskah (*Submission)* 57
4.3.3 Pengujian CSRF pada *Endpoint Submission Discussion Reply* Pengajuan Naskah (*Submission)* 59
4.3.4 Pengujian CSRF pada *Endpoint Accept Review Assignment* (*Reviewer)* 61
4.3.5 Pengujian CSRF pada *Endpoint Submit Review Recommendation/Decision* (*Reviewer)* 64
4.4 Analisis Hasil Pengujian 66
BAB V PENUTUP 30
5.1 Kesimpulan 30
5.2 Saran 69
DAFTAR PUSTAKA 69

DAFTAR GAMBAR

Gambar 2.1 Logo Open Journal System 9
Gambar 2.2 Alur Penerbitan Open Journal System 10
Gambar 2.3 Tampilan Kali Linux 12
Gambar 2.4 OWASP Top 10 Vulnerabilities 13
Gambar 2.5 Logo CVSS 17
Gambar 3. 1 Diagram Alir Penelitian 6
Gambar 3. 2 Tampilan Website OJS TE Untan Journal 21
Gambar 3. 3 Tahapan Pelaksanaan Metode Penetration Testing 22
Gambar 3. 4 Tes Hasil Capture Penetration Testing OWASP ZAP 27
Gambar 3. 5 Kalkulator CVSS 27
Gambar 4. 1 Tampilan Halaman Submission 30
Gambar 4. 2 Tampilan Automated Scan ZAP pada endpoint 31
Gambar 4. 3 Tampilan kerentanan pada endpoint title[id] 32
Gambar 4. 4 Tampilan hasil Intercept di fitur Repeater untuk endpoint title[id] 32
Gambar 4. 5 Tampilan hasil attack payload pada endpoint pada fitur Intruder ... 33
Gambar 4. 6 Tampilan skrip XSS yang ditampilkan sebagai teks 34
Gambar 4. 7 Tampilan kerentanan pada endpoint abstract[id] 35
Gambar 4. 8 Tampilan simulasi serangan payload pada endpoint abstract[id] ... 36
Gambar 4. 9 Tampilan skrip XSS yang ditampilkan sebagai teks 37
Gambar 4. 10 Tampilan kerentanan pada endpoint keyword[id] 38
Gambar 4. 11 Hasil encoding setelah diberi salah satu skrip 39
Gambar 4. 12 Tampilan skrip XSS yang ditampilkan sebagai teks di metada 40
Gambar 4. 13 Tampilan kerentanan pada endpoint citationsRaw 41
Gambar 4. 14 Tampilan simulasi serangan payload pada endpoint citationsRaw42
Gambar 4. 15 Tampilan skrip XSS yang ditampilkan sebagai teks 42
Gambar 4. 16 Tampilan menu Diskusi Review 43
Gambar 4. 17 Tampilan hasil pemindaian pada fitur Diskusi Review 44
Gambar 4. 18 Daftar kerentanan pada endpoint comment melalui Active Scan . 45
Gambar 4. 19 Response HTML dari URL Alert CSP: script-src unsafe-inline ... 45
Gambar 4. 20 Response serangan salah satu payload pada endpoint comment .. 46

Gambar 4. 21 Pemantauan Source Code setelah penginputan payload XSS pada fitur Comment 46
Gambar 4. 22 Halaman pencarian submission/metadata pada OJS..... 47
Gambar 4. 23 Tampilan kerentanan pada endpoint Search Submission..... 48
Gambar 4. 24 Tampilan simulasi serangan payload pada endpoint abstract[id] . 49
Gambar 4. 25 Tampilan skrip XSS yang ditampilkan sebagai teks di kolom pencarian 50
Gambar 4. 26 Tampilan hasil pemindaian pada fitur Diskusi Review 51
Gambar 4. 27 Daftar kerentanan pada endpoint comment melalui Active Scan . 51
Gambar 4. 28 Response HTML dari URL Alert CSP: script-src unsafe-inline... 52
Gambar 4. 29 Response serangan salah satu payload pada endpoint comment .. 52
Gambar 4. 30 Pemantauan Source Code setelah penginputan payload XSS pada fitur Comment 53
Gambar 4. 31 Tampilan Request dari endpoint save new submission..... 54
Gambar 4. 32 Tampilan pengujian di Burp Suite 55
Gambar 4. 33 Tampilan request pada section detail 57
Gambar 4. 34 Tampilan request pada section unggah file 57
Gambar 4. 35 Tampilan request pada section komentar untuk editor 57
Gambar 4. 36 Tampilan request setelah pesan di kirim..... 60
Gambar 4. 37 Tampilan bahwa terdapat masalah setelah scenario dijalankan.... 61
Gambar 4. 38 Tampilan response dari perekaman aktivitas accept review 62
Gambar 4. 39 Tampilan bahwa terdapat masalah setelah scenario dijalankan.... 63
Gambar 4. 40 Tampilan response dari perekaman aktivitas penyerahan hasil review..... 64

DAFTAR TABEL

Tabel 2.1 Tabel Penelitian Terdahulu 2
Tabel 3.1 Alat Penelitian 19
Tabel 3.2 Bahan Penelitian 20
Tabel 3.3 Penjelasan Tahapan Pelaksanaan Metode Penetration Testing 22
Tabel 3.4 Titik Serangan XSS & CSRF pada OJS 24
Tabel 3.5 Parameter Penilaian Risiko CVSS 25
Tabel 4. 1 Bentuk karakter yang diencoding 33
Tabel 4. 2 Rekap scenario pengujian pada Endpoint Save New Submission 56
Tabel 4. 3 Rekap scenario pengujian pada section detail 58
Tabel 4. 4 Rekap scenario pengujian pada section detail 58
Tabel 4. 5 Rekap scenario pengujian pada section detail 58
Tabel 4. 6 Rekap pengujian pada endpoint submission discussion reply 60
Tabel 4. 7 Rekap pengujian pada endpoint Accept Review Assignment 62
Tabel 4. 8 Rekap pengujian pada endpoint Submit Review Recommendation / Decision 65

DAFTAR LAMPIRAN

LAMPIRAN A PAYLOAD UJI XSS 72

DAFTAR ISTILAH

Open Source	:	Perangkat lunak yang kode sumbernya tersedia untuk dipelajari, dimodifikasi, dan didistribusikan secara bebas.
Penetration Testing	:	Proses pengujian keamanan dengan mensimulasikan serangan untuk menemukan kerentanan pada suatu sistem.
Patch	:	Pembaruan perangkat lunak yang dibuat untuk memperbaiki bug, meningkatkan fitur, atau menutup celah keamanan.
Vulnerability	:	Kelemahan pada sistem yang dapat dimanfaatkan oleh pihak yang tidak berwenang.
Session Hijacking	:	Serangan yang mengambil alih sesi pengguna dengan mencuri atau memanfaatkan informasi sesi yang valid.
Injection	:	Serangan yang memasukkan data atau perintah berbahaya ke dalam aplikasi agar dijalankan oleh sistem.
Filtering	:	Proses menyaring data masukan atau keluaran untuk mencegah konten yang tidak valid atau berbahaya.
Session Management	:	Mekanisme untuk mengelola sesi pengguna selama proses autentikasi dan penggunaan aplikasi.
Input Validation	:	Proses memeriksa dan memastikan bahwa data masukan sesuai dengan aturan yang telah ditentukan.
Security Header	:	Header HTTP yang digunakan untuk meningkatkan keamanan komunikasi antara server dan browser.
Bug	:	Kesalahan atau cacat pada perangkat lunak yang menyebabkan fungsi sistem tidak berjalan sebagaimana mestinya.
Payload	:	Bagian dari serangan yang berisi kode atau data berbahaya yang dieksekusi pada target.

Reconnaissance	:	Tahap awal pengujian keamanan yang bertujuan mengumpulkan informasi mengenai target.
Enumeration	:	Proses memperoleh informasi lebih rinci mengenai layanan, pengguna, atau konfigurasi suatu sistem.
De facto	:	Standar yang diakui dan digunakan secara luas karena praktik umum, meskipun tidak ditetapkan secara resmi.
Encoding	:	Proses mengubah data ke format tertentu agar aman ditampilkan atau diproses oleh sistem.
Cookie	:	Data kecil yang disimpan oleh browser untuk menyimpan informasi sesi atau preferensi pengguna.
Session Cookie	:	Cookie yang menyimpan identitas sesi pengguna selama sesi browser masih aktif.
Flowchart	:	Diagram yang menggambarkan urutan langkah atau alur proses dalam suatu sistem.
Intercepting Proxy	:	Perangkat atau aplikasi yang berada di antara klien dan server untuk menangkap serta memodifikasi lalu lintas HTTP/HTTPS
Broken Access Control	:	Kerentanan yang memungkinkan pengguna mengakses sumber daya atau fungsi di luar hak aksesnya.
Defacement	:	Serangan yang mengubah tampilan atau isi suatu situs web tanpa izin.
Metadata	:	Data yang memberikan informasi atau deskripsi mengenai data lainnya.
Persistent Script Execution	:	Eksekusi skrip berbahaya yang tersimpan di aplikasi sehingga dijalankan berulang kali saat halaman diakses
Stored Payload	:	Muatan serangan yang disimpan pada server atau basis data sebelum dieksekusi kepada pengguna lain
Endpoint	:	Titik akses pada aplikasi atau layanan yang menerima dan memproses permintaan dari pengguna atau sistem lain.

DAFTAR SINGKATAN

OJS (*Open Journal Systems)*	:	Sistem manajemen jurnal ilmiah berbasis web.
CIA (*Confidentiality, Integrity, Availability)*	:	Tiga prinsip utama dalam keamanan informasi.
CSRF (*Cross-Site Request Forgery)*	:	Serangan yang memanfaatkan sesi pengguna yang telah terautentikasi untuk mengirim permintaan tanpa sepengetahuan pengguna.
PKP *(Public Knowledge Project)*		Organisasi pengembang Open Journal Systems (OJS).
XSS (*Cross-Site Scripting)*	:	Kerentanan aplikasi web yang memungkinkan penyisipan dan eksekusi skrip berbahaya pada browser pengguna.
CVSS (Common Vulnerability Scoring System)	:	Standar untuk mengukur tingkat keparahan suatu kerentanan keamanan.
DOM (*Document Object Model)*	:	Representasi struktur dokumen HTML/XML yang digunakan browser.
DoS (Denial of Service)	:	Serangan yang bertujuan membuat layanan tidak dapat diakses oleh pengguna yang sah.
GPL (*General Public License)*	:	Lisensi perangkat lunak bebas yang memungkinkan penggunaan, modifikasi, dan distribusi ulang perangkat lunak.
HTTP *(Hypertext Transfer Protocol)*	:	Protokol komunikasi untuk pertukaran data pada web tanpa enkripsi.
HTTPS (*Hypertext Transfer Protocol Secure)*	:	Protokol komunikasi web yang menggunakan enkripsi TLS/SSL.
HTML (*Hypertext Markup Language)*	:	Bahasa markah yang digunakan untuk menyusun halaman web.

ISSAF *(Information Systems Security Assessment Framework)*	:	Kerangka kerja untuk melakukan penilaian keamanan sistem informasi.
OWASP *(Open Worldwide Application Security Project)*	:	Organisasi yang menyediakan panduan dan standar keamanan aplikasi web.
PoC *(Proof of Concept)*	:	Pembuktian bahwa suatu kerentanan dapat dieksploitasi.
PTES (*Penetration Testing Execution Standard)*	:	Standar pelaksanaan pengujian penetrasi.
SQL (*Structured Query Language)*	:	Bahasa yang digunakan untuk mengelola basis data relasional.
TLS *(Transport Layer Security)*	:	Protokol keamanan yang mengenkripsi komunikasi melalui jaringan.
WTSG *(Web Security Testing Guide)*	:	Panduan pengujian keamanan aplikasi web yang diterbitkan oleh OWASP.
PHP *(PHP: Hypertext Preprocessor)*	:	Bahasa pemrograman sisi server yang banyak digunakan dalam pengembangan aplikasi web
JSON *(JavaScript Object Notation)*	:	Format pertukaran data yang ringan dan umum digunakan pada komunikasi aplikasi web.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi telah membawa perubahan signifikan dalam berbagai bidang, termasuk dunia akademik dan penelitian. Salah satu platform yang banyak digunakan dalam publikasi ilmiah adalah *Open Journal System* (OJS), sebuah sistem manajemen jurnal berbasis sumber terbuka (*open source*) yang digunakan oleh banyak institusi pendidikan dan penerbit jurnal di seluruh dunia. Dikembangkan oleh Public Knowledge Project (PKP), OJS menjadi pilihan utama bagi banyak institusi pendidikan karena selain sifatnya yang *open source*, OJS juga dinilai ringan, dan memiliki komunitas pengguna yang luas. [1] Pada versi terbarunya yaitu OJS versi 3.5., menjadikan platform ini sangat diminati karena popularitasnya dan fiturnya yang terus bertambah. Namun disisi lain, keamanan sistem menjadi aspek yang sangat penting untuk diperhatikan, mengingat potensi ancaman siber yang terus meningkat.

Keamanan web server yang menjalankan OJS menjadi salah satu faktor utama dalam menjaga integritas data dan aksesibilitas informasi. Namun, karena sifatnya yang *open source*, OJS juga menjadi target potensial bagi berbagai jenis serangan. Penelitian terdahulu dan laporan komunitas telah mengindikasikan adanya celah keamanan pada OJS, khususnya pada versi-versi lama. Dua di antara kerentanan yang paling umum dan berdampak tinggi adalah *Cross-Site Scripting* (XSS) dan *Cross-Site Request Forgery* (CSRF). Serangan XSS memungkinkan penyerang untuk menyisipkan skrip berbahaya ke dalam situs web yang dilihat oleh pengguna lain, yang dapat berujung pada pencurian sesi, pengambilhalihan akun, atau perusakan tampilan situs. [2] Sementara itu, serangan CSRF dapat memaksa pengguna yang terautentikasi untuk melakukan tindakan yang tidak diinginkan, seperti mengubah data jurnal atau mengirimkan artikel palsu tanpa diketahui. [3]

Beberapa penelitian sebelumnya telah melakukan analisis keamanan pada OJS menggunakan berbagai metodologi, seperti ISSAF, OWASP, atau pemindaian kerentanan *Black-Box*. [4] Namun, penelitian-penelitian tersebut sering kali berhenti pada tahap deteksi kerentanan. Terdapat kekosongan riset yang signifikan

dalam hal pembuktian eksploitasi secara praktis, pengukuran dampak risiko secara kuantitatif menggunakan standar industri seperti *Common Vulnerability Scoring System* (CVSS) [5] , serta implementasi dan validasi solusi mitigasi teknis. Tanpa siklus pengujian yang lengkap mulai dari deteksi, eksploitasi, mitigasi, hingga pengujian ulang (*retesting*), rekomendasi keamanan yang dihasilkan bersifat teoretis dan belum terbukti efektivitasnya.

Oleh karena itu, penelitian ini diusulkan untuk mengisi kekosongan tersebut. Dengan menggunakan pendekatan *penetration testing* (*black-box*), penelitian ini akan secara komprehensif mengevaluasi kerentanan XSS dan CSRF pada OJS versi 3.5. Pendekatan tersebut memungkinkan pengujian keamanan secara aktif guna menemukan kelemahan sistem sebelum dieksploitasi oleh pihak yang tidak bertanggung jawab. Selanjutnya, tingkat risiko dari setiap kerentanan yang ditemukan akan diukur menggunakan CVSS v4.0, dan solusi mitigasi teknis berupa *patch* pada kode sumber akan diterapkan. Sebagai tahap akhir, pengujian ulang akan dilakukan untuk memverifikasi bahwa mitigasi yang diimplementasikan berhasil menutup celah keamanan yang ada.

Melalui penelitian ini, diharapkan dapat diperoleh wawasan yang lebih dalam mengenai tingkat keamanan OJS serta langkah-langkah mitigasi yang dapat dilakukan untuk mencegah serangan siber. Selain itu, hasil penelitian ini juga diharapkan dapat menjadi referensi bagi administrator sistem dan pengelola jurnal dalam meningkatkan perlindungan terhadap ancaman keamanan yang berpotensi merugikan. Pentingnya penelitian ini juga didasari oleh meningkatnya jumlah insiden keamanan yang menargetkan platform publikasi ilmiah. Banyak jurnal akademik berbasis OJS mengalami kendala teknis akibat serangan siber yang dapat mengganggu ketersediaan layanan dan merusak reputasi institusi yang mengelolanya. [6]

Lebih jauh, hasil penelitian ini diharapkan dapat menjadi rujukan bagi pengembang OJS dalam meningkatkan fitur keamanan di versi-versi mendatang. Dengan adanya pengujian yang lebih komprehensif dan berbasis metode *penetration testing* yang sistematis, diharapkan OJS dapat menjadi platform publikasi yang lebih aman dan andal dalam mendukung perkembangan ilmu pengetahuan di era digital ini.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, penelitian ini akan menginvestigasi bagaimana kerentanan tersebut dapat diidentifikasi dan dibuktikan secara nyata melalui metode *penetration testing*. Selanjutnya, penelitian akan merumuskan bagaimana tingkat risiko dari setiap temuan dapat diukur secara kuantitatif menggunakan standar skor CVSS untuk memberikan gambaran dampak yang jelas. Lebih lanjut, fokus permasalahan bergeser pada perancangan dan implementasi langkah-langkah mitigasi teknis yang efektif dan dapat diterapkan langsung pada kode sumber OJS yang kemudian dapat diverifikasi secara empiris bahwa solusi mitigasi yang diterapkan benar-benar berhasil menutup celah keamanan melalui proses pengujian ulang yang sistematis.

1.3 Tujuan Penelitian

Adapun tujuan penelitian ini untuk melaksanakan siklus pengujian keamanan yang lengkap pada OJS 3.5 dengan mendeteksi dan membuktikan kerentanan XSS dan CSRF, mengukur risikonya dengan skor CVSS, merancang dan menerapkan solusi mitigasi teknis pada kode sumber, serta memvalidasi efektivitas solusi tersebut melalui pengujian ulang untuk memastikan kerentanan telah berhasil ditutup.

1.4 Pembatasan Masalah

Sehubungan dengan keterbatasan yang dimiliki, dari segi waktu, pemikiran serta biaya, maka batasan masalah pada penelitian ini yaitu:

1. Fokus penelitian adalah pada Open Journal Systems versi 3.5 yang di deploy pada server online sehingga dapat diakses melalui jaringan internet dengan lingkungan pengujian yang terkontrol.
2. Jenis serangan yang diuji secara spesifik adalah *Cross-Site Scripting* (*Stored* XSS dan *Reflected* XSS) dan *Cross-Site Request Forgery* (CSRF).
3. Pengujian difokuskan pada modul yang paling sering berinteraksi dengan pengguna, yaitu modul pengiriman naskah (*submission*) dan modul penelaahan (*review*).
4. Solusi mitigasi yang diterapkan terbatas pada level aplikasi (*code-level patching*) dan tidak mencakup konfigurasi keamanan infrastruktur tingkat lanjut.

1.5 Sistematika Penulisan

Agar penulisan tugas akhir ini teratur, maka sistematika penulisan dibagi dalam beberapa bab sebagai berikut:

BAB I PENDAHULUAN

Bab ini membahas tentang latar belakang, perumusan masalah, tujuan penelitian, pembatasan masalah, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini membahas tentang studi kepustakaan dan dasar teori.

BAB III METODOLOGI PENELITIAN

Bab ini terdiri dari alat dan bahan penelitian, metode penelitian, variabel atau data, analisis hasil serta diagram alur penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab yang berisi hasil pengujian dilanjutkan dengan pengaplikasian mitigasi, pengujian ulang serta penyusunan laporan dan kesimpulan.

BAB V PENUTUP

Bab ini berisikan kesimpulan dan saran berdasarkan hasil dan pembahasan yang telah dilakukan penulis.