Journal of Informatics and Computer Science Vol. 11, No. 2 Oktober 2026
Universitas Ubudiyah Indonesia
e-ISSN : 2615-5346

ANALISIS KEAMANAN DAN STABILITAS SISTEM WEB JURNAL UNIVERSITAS DEZTRON INDONESIA BERBASIS OJS 3.4.0.10

SECURITY AND STABILITY ANALYSIS OF THE UNIVERSITAS DEZTRON INDONESIA JOURNAL WEB SYSTEM BASED ON OJS 3.4.0.10

Azwar[1], Rizka Albar[2], Mahendar Dwi Payana[3], M. Bayu Wibawa[4]
[1,2,4]Jurusan Sistem Informasi, Informatika[3], Fakultas Sains dan Tekno*log*i, Universitas Ubudiyah Indonesia, Banda Aceh
E-mail : [1]azwar.mhs@uui.ac.id,[2]albar@uui.ac.id, [3]mahendar@uui.com, [4] mbayuw@uui.com

Abstrak - Perkembangan publikasi ilmiah digital menuntut sistem jurnal berbasis web yang tidak hanya fungsional, tetapi juga aman dan stabil. Universitas Deztron Indonesia telah mengimplementasikan *Open Journal Systems (OJS)* versi 3.4.0.10 sebagai platform pengelolaan jurnal elektronik. Namun, dalam proses implementasi dan *upgrade* sistem, ditemukan beberapa permasalahan seperti *error HTTP 500*, konflik *plugin*, kesalahan konfigurasi PHP, serta pengaturan permission direktori yang mempengaruhi stabilitas sistem. Penelitian ini bertujuan untuk menganalisis aspek keamanan server, manajemen *plugin*, konfigurasi sistem, serta stabilitas pasca *upgrade* pada Web Jurnal Universitas Deztron Indonesia. Metode penelitian menggunakan pendekatan studi kasus dengan analisis *log error*, evaluasi konfigurasi server, serta pengujian stabilitas sistem setelah perbaikan dilakukan. Hasil penelitian menunjukkan bahwa stabilitas sistem sangat dipengaruhi oleh konfigurasi *date format*, *permission folder*, kompatibilitas *plugin*, serta penerapan *backup* dan *recovery system*. Evaluasi keamanan dan stabilitas yang sistematis mampu mengembalikan performa sistem menjadi optimal dan mencegah terulangnya kesalahan serupa.

Kata Kunci : OJS 3.4.0.10, keamanan web, *HTTP 500*, manajemen *plugin*, stabilitas sistem

Abstract - The development of digital scientific publications requires journal management systems that are not only functional but also secure and stable. Universitas Deztron Indonesia has implemented Open Journal Systems (OJS) version 3.4.0.10 as its electronic journal platform. However, during system implementation and upgrade processes, several issues were encountered, including HTTP 500 errors, plugin conflicts, PHP configuration errors, and directory permission misconfigurations affecting system stability. This study aims to analyze server security aspects, plugin management, system configuration, and post-upgrade stability of the Universitas Deztron Indonesia Journal Web System. The research employs a case study approach through error log analysis, server configuration evaluation, and system stability testing after corrective actions. The results indicate that system stability is strongly influenced by date format configuration, folder permissions, plugin compatibility, and backup and recovery mechanisms. A systematic evaluation of security and stability successfully restored optimal system performance and prevented recurring errors.

Keywords: *OJS 3.4.0.10, web security, HTTP 500, plugin management, system stability*

I. PENDAHULUAN

Transformasi digital dalam publikasi ilmiah mendorong perguruan tinggi untuk mengimplementasikan sistem jurnal berbasis web yang profesional, aman, dan stabil. *Open Journal Systems (OJS)* menjadi salah satu platform yang banyak digunakan karena mendukung manajemen editorial secara terstruktur. Universitas Deztron Indonesia telah mengadopsi OJS versi 3.4.0.10 untuk mendukung pengelolaan dan publikasi jurnal ilmiah secara digital.

Meskipun sistem telah berjalan, proses *upgrade* dan konfigurasi lanjutan memunculkan beberapa permasalahan teknis, seperti munculnya *HTTP 500* Internal *Server Error*, konflik *plugin*, kesalahan konfigurasi PHP, serta perubahan permission direktori yang mempengaruhi akses sistem. Permasalahan tersebut menunjukkan bahwa keamanan dan stabilitas sistem menjadi faktor kritis dalam keberlanjutan operasional jurnal.

Keamanan sistem web tidak hanya bergantung pada aplikasi, tetapi juga pada konfigurasi server, pengaturan SSL, manajemen file, serta kompatibilitas *plugin*. Kesalahan kecil dalam konfigurasi dapat menyebabkan gangguan sistem secara menyeluruh. Oleh karena itu, diperlukan analisis komprehensif terhadap aspek keamanan dan stabilitas sistem pasca *upgrade*.

Penelitian ini bertujuan untuk menganalisis keamanan server, manajemen *plugin*, konfigurasi sistem, serta stabilitas Web Jurnal Universitas Deztron Indonesia berbasis OJS 3.4.0.10. Analisis dilakukan berdasarkan studi kasus nyata yang terjadi selama proses implementasi dan pemeliharaan sistem.

II. STUDI PUSTAKA

A. Keamanan Sistem Informasi Berbasis Web

Keamanan aplikasi berbasis web menjadi aspek utama dalam pengelolaan sistem informasi modern. Menurut Sugara dan Sriyasa (2024), pendekatan OWASP digunakan sebagai standar dalam

mengidentifikasi risiko keamanan aplikasi web. Kerentanan seperti *SQL Injection* dan *Cross-Site Scripting (XSS)* dapat mengancam integritas sistem apabila tidak dilakukan pengujian keamanan secara berkala.

Guntoro, Costaner, dan Musfawati (2024) menjelaskan bahwa sistem *Open Journal Systems (OJS)* memiliki potensi kerentanan jika tidak dilakukan analisis keamanan menggunakan metode ISSAF dan OWASP. Yunanri (2023) juga menemukan bahwa celah XSS pada OJS dapat dimanfaatkan apabila validasi input tidak diterapkan dengan baik.

Purba, Amandha, dan Purnama (2022) menegaskan bahwa *vulnerability assessment* dan *penetration testing* merupakan metode efektif dalam mengidentifikasi celah keamanan sistem web. Sementara itu, Munawar dan Putri (2020) menyatakan bahwa keamanan jaringan dan server merupakan fondasi utama dalam menjaga keamanan aplikasi berbasis web.

B. Keamanan Server dan Konfigurasi SSL

Konfigurasi server yang tepat sangat menentukan tingkat keamanan sistem. Faatihah, Zulaikha, dan Wicaksono (2024) menyatakan bahwa kesalahan konfigurasi server dapat menyebabkan gangguan akses dan potensi eksploitasi sistem.

Singh dan Chatterjee (2022) menjelaskan bahwa penerapan SSL/TLS mampu melindungi komunikasi data antara pengguna dan server dari serangan penyadapan. Zein et al. (2023) menekankan pentingnya hardening server melalui pengaturan *permission folder* yang tepat, terutama pada sistem berbasis PHP seperti OJS.

Rahman dan Putri (2024) menjelaskan bahwa pemisahan direktori file upload dari direktori publik menjadi strategi penting dalam meningkatkan keamanan sistem.

C. Analisis *Error HTTP 500* dan Konfigurasi PHP

HTTP 500 Internal *Server Error* sering terjadi pada aplikasi berbasis PHP akibat konfigurasi yang tidak tepat. Kumar dan Patel (2021) menyatakan bahwa *error* ini dapat disebabkan oleh konflik *plugin*, *variabel null*, atau kesalahan konfigurasi sistem.

Widodo (2022) menjelaskan bahwa kesalahan konfigurasi pada framework PHP dapat menyebabkan fungsi sistem gagal dijalankan. Bangkit Wiguna et al. (2020) menegaskan bahwa analisis file *log* menjadi langkah utama dalam proses *troubleshooting* sistem web.

Kasus *error convertStrftimeFormat()* pada OJS menunjukkan bahwa konfigurasi *date format* yang tidak terbaca sistem dapat menyebabkan kegagalan inisialisasi template.

D. Manajemen *Plugin* dan Risiko Sistem

Plugin memberikan fleksibilitas dalam pengembangan sistem OJS, namun juga berpotensi menimbulkan risiko. Hassan dan Malik (2022) menyatakan bahwa *plugin* yang tidak kompatibel dapat menyebabkan konflik dan crash sistem.

Chen, Zhang, dan Li (2023) menjelaskan bahwa evaluasi risiko *plugin* perlu dilakukan secara berkala untuk menjaga stabilitas sistem. Ginting et al. (2025) menekankan bahwa manajemen *plugin* pada OJS 3 memerlukan perhatian khusus pasca *upgrade* versi.

E. *Backup* dan *Recovery system*

Backup sistem merupakan bagian dari manajemen risiko keamanan informasi. ISO/IEC 27001 (2022) menegaskan pentingnya kebijakan *backup* berkala. Fahmi (2022) menyatakan bahwa *backup* database dan direktori sistem wajib dilakukan untuk mencegah kehilangan data permanen.

Setiawan dan Nugroho (2024) menjelaskan bahwa *disaster recovery plan* membantu mempercepat pemulihan sistem saat terjadi kegagalan.

F. Stabilitas Sistem Pasca *Upgrade*

Upgrade sistem bertujuan meningkatkan keamanan dan performa. García dan López (2023) menjelaskan bahwa evaluasi stabilitas pasca *upgrade* harus mencakup pengujian kompatibilitas sistem dan monitoring *error*.

Andriani dan Mahendra (2025) menyatakan bahwa stabilitas sistem diukur dari minimnya *error* server dan kelancaran Workflow pengguna.

III. METODE PENELITIAN

A. Jenis Penelitian

Penelitian ini menggunakan metode studi kasus *(case study)* terhadap Web Jurnal Universitas Deztron Indonesia yang menggunakan *Open Journal Systems (OJS)* versi 3.4.0.10.

Pendekatan ini dipilih karena penelitian berfokus pada permasalahan nyata yang terjadi selama:

1. Proses *upgrade* dari versi sebelumnya ke OJS 3.4.0.10
2. Munculnya *error submission* pada akun penulis
3. *Error* SLIM akibat konfigurasi *permission folder*
4. *HTTP 500* Internal *Server Error* pasca perubahan konfigurasi
5. Konflik *plugin* dan kesalahan konfigurasi *date format*

Metode analisis bersifat deskriptif teknis, dengan evaluasi konfigurasi server dan pengujian stabilitas sistem setelah perbaikan dilakukan.

B. Pengumpulan Data

1. Observasi Langsung Sistem

    a. Observasi dilakukan pada:
    b. Proses *submission* naskah oleh penulis
    c. Dashboard admin jurnal
    d. Aktivasi dan deaktivasi *plugin*
    e. Tampilan halaman publik

Kasus utama yang diamati adalah:

a. Popup kosong saat klik —Serahkan‖
b. *HTTP 500* setelah perubahan konfigurasi session
c. *Error* fatal pada fungsi *convertStrftimeFormat()*

2. Analisis *Log* Server
Analisis dilakukan pada file:
/home/siakadud/jurnal.udi.ac.id/error_log

Ditemukan pesan *error*:
PKPString::convertStrftimeFormat():
Argument must be of type string, null given

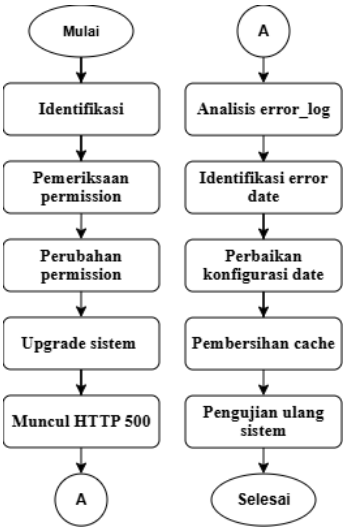
Analisis *log* digunakan untuk:
a. Mengidentifikasi penyebab *HTTP 500*
b. Menentukan konfigurasi yang bermasalah
c. Menentukan *plugin* yang menyebabkan crash

3. Analisis Konfigurasi Sistem
Pemeriksaan dilakukan pada file:
config.inc.php

Bagian yang dianalisis meliputi:
a. [files] → files_dir
b. *Permission folder* (755 dan 775)
c. [session] configuration
d. date_format_short
e. datetime_format_long
f. base_url
g. SSL (HTTPS)

C. Alur Penyelesaian Masalah Sistem

Penelitian ini mengikuti alur penyelesaian masalah berdasarkan kasus nyata yang terjadi.
Tahapan:
a. Identifikasi *error submission* (popup kosong pada akun author)
b. Pemeriksaan *permission folder* files dan Cache
c. Perubahan permission dari 755 menjadi 775
d. *Upgrade* sistem ke OJS 3.4.0.10
e. Muncul *HTTP 500*
f. Analisis *error_log*
g. Identifikasi *error date format* bernilai *null*
h. Perbaikan konfigurasi *date format* di *config.inc.php*
i. Pembersihan *Cache* dan folder *t_compile*
j. Pengujian ulang sistem



Gambar 1. Alur Penyelesaian *Error* Web Jurnal UDI

Diagram menunjukkan tahapan penyelesaian masalah mulai dari *error submission*, analisis *permission folder*, *upgrade* sistem, munculnya *HTTP 500*, analisis *log error*, perbaikan konfigurasi *date format*, hingga sistem kembali stabil.

D. Analisis Permission dan Struktur Direktori

Pada kasus awal, *error* SLIM dan *error submission* terjadi akibat konfigurasi permission yang tidak sesuai.

Direktori yang dianalisis:
/home/siakadud/files
/home/siakadud/jurnaldata
/home/siakadud/jurnal.udi.ac.id/ Cache

Langkah yang dilakukan:
a. Mengubah *permission folder* menjadi 775
b. Memastikan *files_dir* berada di luar direktori publik
c. Membuat *folder sessions* jika diperlukan

Evaluasi dilakukan dengan menguji kembali proses upload file *submission*.

E. Analisis *Error HTTP 500*

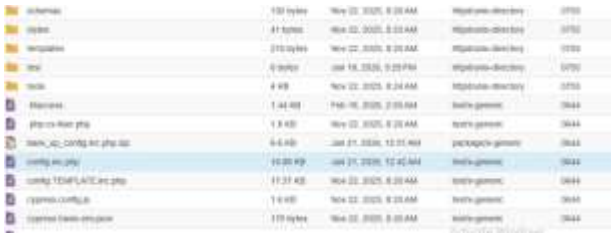
Error HTTP 500 muncul setelah perubahan konfigurasi session dan *upgrade* sistem.

Dari *log* ditemukan *error*:
convertStrftimeFormat(): null given

Penyebab:
Format tanggal tidak terbaca oleh sistem
Nilai date_format_short kosong di konfigurasi

Perbaikan dilakukan dengan menambahkan konfigurasi berikut pada file *config.inc.php:*
date_format_short = "%d-%m-%Y"
date_format_long = "%d %B %Y"

datetime_format_short = "%d-%m-%Y %H:%M"
datetime_format_long = "%d %B %Y %H:%M"



Gambar 2. Struktur Konfigurasi *Date format* pada config.inc.php

Menampilkan bagian konfigurasi *date format* yang ditambahkan untuk mengatasi *error null* pada fungsi convertStrftimeFormat().

F. Analisis Konflik *Plugin*

Plugin yang dianalisis:

a. PDF Viewer *Plugin*
b. *Citation Style Language Plugin*

Langkah yang dilakukan:

a. Menonaktifkan *plugin* bermasalah
b. Menguji sistem tanpa *plugin*
c. Mengaktifkan kembali secara selektif

Hasil menunjukkan bahwa konflik *plugin* dapat memicu *error* fatal saat inisialisasi template manager.



Gambar 3. Pengujian Aktivasi dan Deaktivasi *Plugin*

Menampilkan proses pengujian *plugin* untuk menentukan sumber konflik sistem pasca *upgrade*.

G. Evaluasi Stabilitas Sistem Pasca Perbaikan

Setelah seluruh konfigurasi diperbaiki, dilakukan pengujian:

a. *Log*in multi-role (admin, editor, author)
b. *Submission* naskah
c. Upload file
d. Akses halaman publik
e. Monitoring *error_log* selama 48 jam

Sistem dinyatakan stabil apabila:

a. Tidak muncul *HTTP 500*
b. Tidak ada *error* fatal pada *log*
c. *Workflow editorial* berjalan normal
d. *Plugin* aktif tanpa konflik

IV. HASIL PENELITIAN DAN PEMBAHASAN

A. Hasil Identifikasi Permasalahan Sistem

Berdasarkan observasi langsung terhadap Web Jurnal Universitas Deztron Indonesia berbasis OJS 3.4.0.10, ditemukan beberapa permasalahan utama pasca *upgrade* sistem dan perubahan konfigurasi server. Permasalahan tersebut antara lain:

1. Munculnya popup kosong saat penulis menekan tombol ―Serahkan‖ pada proses *submission.*
2. *Error* SLIM yang menghambat proses unggah file.
3. *HTTP 500* Internal *Server Error* yang menyebabkan website tidak dapat diakses.
4. *Error* fatal pada fungsi convertStrftimeFormat() akibat konfigurasi *date format* yang tidak terbaca sistem.
5. Konflik *plugin* pasca *upgrade* OJS.

Permasalahan tersebut menunjukkan bahwa aspek keamanan dan stabilitas sistem belum sepenuhnya optimal setelah proses *upgrade* dan perubahan konfigurasi dilakukan.

B. Hasil Analisis Permission dan Struktur Direktori

Analisis dilakukan terhadap direktori utama sistem, yaitu:

/home/siakadud/files
/home/siakadud/jurnaldata
/home/siakadud/jurnal.udi.ac.id/ Cache

Pada tahap awal ditemukan bahwa beberapa direktori menggunakan permission 755. Kondisi tersebut membatasi hak akses tulis pada kondisi tertentu, sehingga memicu *error* saat proses upload *submission*.

Setelah dilakukan perubahan permission menjadi 775 pada direktori yang memerlukan akses tulis, proses upload file kembali berjalan normal dan *error* SLIM tidak muncul kembali.

Hasil ini menunjukkan bahwa *konfigurasi permission* direktori memiliki pengaruh langsung terhadap stabilitas sistem OJS.



Gambar 4. Konfigurasi *Permission folder* Sistem

Menampilkan perubahan permission direktori dari 755 menjadi 775 pada folder files dan Cache yang berdampak pada keberhasilan proses *submission* naskah.

C. Hasil Analisis *Error HTTP 500*

Setelah proses *upgrade* ke OJS 3.4.0.10, sistem mengalami *HTTP 500* Internal *Server Error*. Website tidak dapat diakses dan hanya menampilkan pesan kesalahan server.

Berdasarkan analisis file *log* pada:
/home/siakadud/jurnal.udi.ac.id/error_log

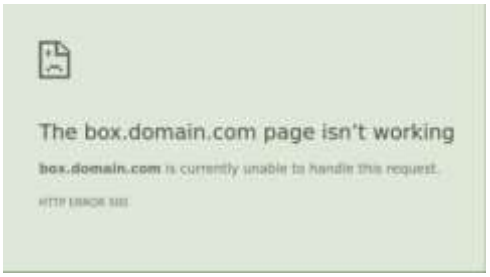
ditemukan *error* sebagai berikut:
PKPString::convertStrftimeFormat():
Argument must be of type string, null given

Error tersebut menunjukkan bahwa sistem menerima nilai *null* pada parameter format tanggal. Investigasi lebih lanjut menemukan bahwa konfigurasi:

date_format_short
date_format_long
datetime_format_short
datetime_format_long

tidak terdefinisi secara eksplisit atau tidak terbaca oleh sistem setelah *upgrade*.

Setelah konfigurasi format tanggal ditambahkan pada file *config.inc.php*, sistem kembali dapat diakses dan *HTTP 500* tidak muncul kembali.



Gambar 5. Potongan *Log Error HTTP 500*

Menampilkan pesan *error convertStrftimeFormat()* pada file *log* server yang menjadi penyebab utama *HTTP 500* Internal *Server Error*.

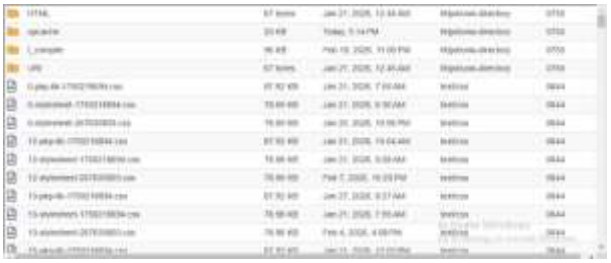
D. Hasil Evaluasi Konfigurasi Session dan *Cache*

Perubahan konfigurasi pada bagian [session] sempat menyebabkan sistem tidak dapat diakses. Hal ini terjadi karena penambahan parameter *session_path* yang tidak sesuai dengan struktur direktori server.

Evaluasi menunjukkan bahwa konfigurasi *session* harus mengikuti standar default OJS apabila tidak diperlukan modifikasi khusus.

Selain itu, dilakukan pembersihan pada direktori:
/ Cache
/ Cache/t_compile

Pembersihan *Cache* berhasil menghilangkan konflik template yang tersimpan dari konfigurasi sebelumnya. Setelah Cache dibersihkan, sistem dapat melakukan inisialisasi ulang template tanpa *error*.



Gambar 6. Direktori *Cache* Sebelum

Menampilkan proses penghapusan isi folder *Cache* dan *t_compile* untuk menghilangkan konflik template lama.

E. Hasil Analisis Konflik *Plugin*

Pasca *upgrade* sistem, ditemukan indikasi konflik *plugin* yang mempengaruhi stabilitas sistem. *Plugin* yang dianalisis meliputi:

1. PDF Viewer *Plugin*
2. *Citation Style Language Plugin*

Pengujian dilakukan dengan metode deaktivasi sementara *plugin* dan pengujian ulang sistem.

Hasil pengujian menunjukkan bahwa pada kondisi *plugin* tertentu aktif, sistem mengalami gangguan inisialisasi template. Setelah *plugin* yang tidak kompatibel dinonaktifkan sementara, sistem berjalan normal tanpa *error* fatal.

Hal ini menunjukkan bahwa kompatibilitas *plugin* terhadap versi OJS terbaru menjadi faktor penting dalam menjaga stabilitas sistem.



Gambar 7. Proses Pengujian Aktivasi dan Deaktivasi *Plugin*

Menampilkan pengujian *plugin* untuk mengidentifikasi *plugin* yang menyebabkan konflik sistem setelah *upgrade* OJS 3.4.0.10.

F. Evaluasi Stabilitas Sistem Pasca Perbaikan

Setelah seluruh perbaikan dilakukan, sistem diuji kembali melalui beberapa skenario:

1. *Log*in menggunakan akun Admin, Editor, dan Author.
2. Proses *submission* naskah oleh Author.
3. Upload dan download file artikel.
4. Akses halaman publik melalui protokol HTTPS.
5. Monitoring *error log* selama 48 jam.
6. Hasil evaluasi menunjukkan bahwa:
7. Tidak ditemukan *HTTP 500.*
8. Tidak terdapat *error* fatal pada *log* server.
9. Workflow editorial berjalan normal.
10. *Plugin* aktif tanpa konflik.
11. Proses *submission* berjalan tanpa *popup error.*

Berdasarkan hasil pengujian tersebut, sistem Web Jurnal Universitas Deztron Indonesia berbasis OJS 3.4.0.10 dinyatakan stabil dan aman untuk digunakan dalam pengelolaan publikasi ilmiah digital.

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan terhadap sistem Web Jurnal Universitas Deztron Indonesia berbasis *Open Journal Systems (OJS)* 3.4.0.10, dapat disimpulkan bahwa:

1. Permasalahan utama yang terjadi pasca *upgrade* sistem meliputi *error submission*, *error* SLIM akibat konfigurasi *permission folder*, serta *HTTP 500* Internal *Server Error* yang disebabkan oleh kesalahan konfiguraisi *date format* dan konflik *plugin*.
2. Konfigurasi *permission* direktori memiliki pengaruh signifikan terhadap keberhasilan proses upload dan *submission* naskah. Perubahan permission dari 755 menjadi 775 pada direktori tertentu terbukti mampu mengatasi *error* akses tulis sistem.
3. *Error HTTP 500* yang muncul setelah *upgrade* disebabkan oleh nilai *null* pada konfigurasi format tanggal, yang memicu kegagalan fungsi *convertStrftimeFormat().* Penambahan konfigurasi *date format* secara eksplisit pada file berhasil mengembalikan akses sistem.
4. Manajemen *plugin* menjadi faktor penting dalam menjaga stabilitas sistem. *Plugin* yang tidak kompatibel dengan versi OJS terbaru dapat menyebabkan konflik sistem dan *error* fatal.
5. Pembersihan *Cache* dan evaluasi konfigurasi session berperan dalam menghilangkan konflik template lama yang tersimpan pada sistem.
6. Setelah seluruh tahapan perbaikan dilakukan, sistem Web Jurnal Universitas Deztron Indonesia dinyatakan stabil, aman, dan mampu menjalankan *Workflow* editorial tanpa gangguan.

Dengan demikian, keamanan dan stabilitas sistem OJS sangat dipengaruhi oleh konfigurasi server, pengelolaan permission, kompatibilitas *plugin*, serta monitoring *log error* secara berkala.

B. Saran

Berdasarkan hasil penelitian, beberapa saran yang dapat diberikan adalah:

1. Administrator sistem perlu melakukan *backup* rutin terhadap database dan direktori sistem sebelum melakukan *upgrade* versi OJS.
2. Setiap proses *upgrade* harus diikuti dengan pengujian kompatibilitas *plugin* untuk mencegah konflik sistem.
3. Monitoring file *log* server perlu dilakukan secara berkala untuk mendeteksi potensi *error* sejak dini.
4. Konfigurasi *permission folder* dan file harus disesuaikan dengan kebutuhan sistem tanpa membuka celah keamanan.

5. Dokumentasi teknis terkait perubahan konfigurasi sistem perlu disusun secara sistematis sebagai panduan pemeliharaan jangka panjang.

Dengan penerapan manajemen keamanan dan stabilitas yang terstruktur, Web Jurnal Universitas Deztron Indonesia dapat beroperasi secara optimal dan berkelanjutan dalam mendukung publikasi ilmiah digital.

REFERENSI

[1] OWASP. (2021). OWASP Top 10: The Ten Most Critical Web Application Security Risks. Open Web Application Security Project.
[2] Singh, J., & Chatterjee, K. (2022). SSL/TLS Implementation for Securing Web-Based Systems. International Journal of Network Security, 24(4), 512–520.
[3] Purba, R., Amandha, D., & Purnama, B. (2022). Vulnerability Assessment dan Penetration Testing pada Sistem Informasi Akademik. Jurnal Tekno*log*i Informasi dan Komunikasi, 11(3), 210–219.
[4] Sugara, A., & Sriyasa, I. (2024). Implementasi OWASP Top 10 pada Pengujian Keamanan Aplikasi Web. Jurnal Tekno*log*i Informasi dan Terapan, 11(2), 95–104.
[5] García, P., & López, M. (2023). Software *Upgrade* Impact on Web-Based Information Systems Stability. International Journal of Advanced Computer Science and Applications, 14(3), 233–241.
[6] Kumar, A., & Patel, S. (2021). Diagnosing Internal *Server Error*s in PHP-Based Web Applications. International Journal of Computer Applications, 183(20), 15–22.
[7] Widodo, E. (2022). Analisis *Error* Konfigurasi Framework Berbasis PHP terhadap Kinerja Sistem Informasi. Jurnal Ilmiah Komputer dan Informatika, 11(2), 145–153.
[8] Hassan, R., & Malik, K. (2022). *Plugin* Security Vulnerabilities in Content Management Systems. Computers & Security, 114, 102603.
[9] Chen, L., Zhang, Y., & Li, H. (2023). Risk Assessment of Third-Party *Plugin*s in Web Applications. Journal of Information Security and Applications, 72, 103457.
[10] Guntoro, M., Costaner, L., & Musfawati. (2024). Analisis Keamanan Open Journal Systems Menggunakan Metode ISSAF dan OWASP. Jurnal Nasional Tekno*log*i dan Sistem Informasi, 10(1), 55–64.
[11] Zein, A., Pradana, R., & Hakim, L. (2023). Evaluasi Konfigurasi Permission Direktori pada Server Linux untuk Aplikasi Web. Jurnal Sistem Komputer, 13(2), 201–209.
[12] Rahman, F., & Putri, L. (2024). Hardening Server untuk Meningkatkan Keamanan Aplikasi Web. Jurnal Keamanan Informasi, 8(1), 33–42.
[13] Munawar, Z., & Putri, A. (2020). Keamanan Jaringan dan Server pada Sistem Informasi Berbasis Web. Jurnal Informatika, 7(2), 89–97.
[14] Fahmi, R. (2022). Implementasi *Backup* dan Recovery Data pada Sistem Informasi Berbasis Web. Jurnal Ilmiah Informatika, 9(2), 120–128.
[15] Setiawan, D., & Nugroho, A. (2024). Disaster Recovery Planning pada Sistem Informasi Berbasis Web. Jurnal Sistem dan Informatika, 18(1), 67–75.
[16] ISO/IEC. (2022). ISO/IEC 27001:2022 Information Security Management Systems — Requirements. International Organization for Standardization.
[17] Andriani, D., & Mahendra, R. (2025). Evaluasi Stabilitas Sistem Informasi Berbasis Web Pasca *Upgrade* Versi Perangkat Lunak. Jurnal Tekno*log*i Informasi dan Ilmu Komputer, 12(1), 45–54.
[18] Bangkit Wiguna, A., Raharjo, S., & Prasetyo, B. (2020). Analisis *Log* Server untuk Identifikasi *Error* pada Aplikasi Berbasis PHP. Jurnal RESTI (Rekayasa Sistem dan Tekno*log*i Informasi), 4(5), 889–897.
[19] Yunanri. (2023). Analisis Kerentanan Cross-Site Scripting (XSS) pada Open Journal Systems. Jurnal Cyber Security, 5(1), 12–20.
[20] Ginting, R., Simatupang, J., & Hutagalung, E. (2025). Implementasi Open Journal Systems Versi 3 pada Pengelolaan Jurnal Ilmiah. Jurnal Tekno*log*i dan Sistem Informasi, 13(1), 15–24.