EVALUASI KEAMANAN OPEN JOURNAL SYSTEMS (OJS) VERSI LAMA MENGGUNAKAN KERANGKA ISSAF

Toto Andri Puspito
Institut Agama Islam Negeri Metro
Jl. Ki Hajar Dewantara No.15A, Iringmulyo, Kec. Metro Timur., Kota Metro
totoandri@metrouniv.ac.id

ABSTRAK

Open Journal Sistem (OJS), yang dikembangkan oleh Public Knowledge Project dan dirilis dengan lisensi public GNU, banyak digunakan oleh lembaga pendidikan dan swasta untuk mempublikasikan hasil penelitian, Lebih dari 44.000 jurnal di 148 negara menggunakan OJS untuk menerbitkan penelitian dalam 60 lebih Bahasa [1] namun, seperti halnya system berbasis website lainnya, OJS memiliki kerentanan system yang memerlukan pemabaruan untuk menutup celah kemanan, meningkatkan kompatibilitas dan meningkatkan fitur kinerja. Berdasarkan survei awal peneliti menemukan bahwa beberapa jurnal di perguruan tinggi masih menggunakan OJS versi lama. Peneliti kemudian meneliti lebih lanjut dengan menggunakan Information System Security Assessment Framework (ISSAF) dan OWASP ZAP untuk mengidentifikasi kerentanan pada OJS versi lama yang masih digunakan oleh perguruan tinggi. Kerentanan yang ditemukan meliputi informasi yang tercatat pada Common Vulnerabilities and Exposures (CVE), seclist.org, exploit-db.com. studi ini menunjukan bahwa beberapa institusi yang menggunakan OJS versi lama menambahkan WAF (Web Aplication Firewall) untuk mengurangi resiko keamanan artikel ini membahas temuan tersebut dan memberikan rekomendasi untuk penelitian lanjutan mengenai peningkatan keamanan OJS.

Kata kunci : Open Journal System, ISSAF, OWASP ZAP

ABSTRACTS

The Open Journal System (OJS), developed by the Public Knowledge Project and released under the GNU public license, is widely used by educational and private institutions to publish research results. More than 44,000 journals in 148 countries use OJS to publish research in more than 60 languages. [1] However, as with other web-based systems, OJS has system vulnerabilities that require updates to close security gaps, improve compatibility, and improve performance features. Based on an initial survey, researchers found that several journals in higher education still use the old version of OJS. Researchers then researched further using the Information System Security Assessment Framework (ISSAF) and OWASP ZAP to identify vulnerabilities in the old version of OJS which universities still use. The vulnerabilities include information recorded in Common Vulnerabilities and Exposures (CVE), seclist.org, and exploit-db.com. This study shows that some institutions that use older versions of OJS add a WAF (Web Application Firewall) to reduce security risks. This article discusses these findings and recommends further research on improving OJS security..

Keywords: Open Journal System, ISSAF, OWASP ZAP

1. PENDAHULUAN

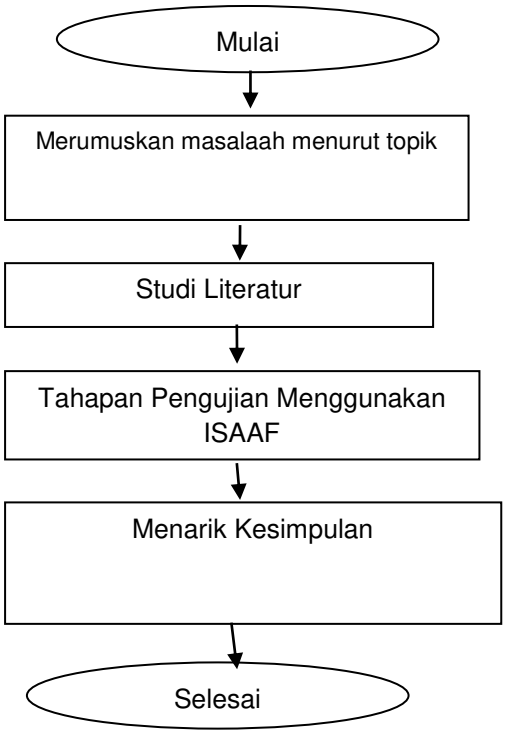
Di Indonesia *Open Journal System* (OJS) banyak di gunakan oleh perguruan tinggi baik negeri maupun swasta. OJS merupakan sebuah software yang digunakan untuk mengelola dan menerbitkan artikel ilmilah, Sebagai software sumber terbuka OJS dapat digunakan secara gratis hal ini yang menjadikan jumlah pengguna OJS diseluruh dunia terus meningkat. Di indonesia hampir seluruh perguruan tinggi negeri dan swasta menggunakan OJS sebagai system publikasi ilmiah. Mesikupn aplikasi sumber terbuka tim *Public Knowledge Project* (PKP) sebagai penmbuat OJS terus menyediakan pembaruan untuk pengguna agar mendapatkan fitur keamanan terbaru, dapat berjalan di lingkungan server terbaru, mendapatkan peningkatan signifikan dalam kegunaan dan kinerja [1] namun, di Indonesia, masih banyak ditemukan pengguna yang menggunakan OJS versi lama, OJS versi lama memiliki tangkat kerentanan serangan cyber, hal ini dibuktikan oleh pengujian yang dilakukkan oleh Imam riadi dkk. [2] analisis kemanan website Open Journal System menggunakan metode vulnerability Asessment dari hasli analisis menemukan bahwa OJS Versi 2.4.7 memiliki banyak celah kerentanan. Untuk meneliti lebih jauh sebab masih banyaknya penggunaan OJS versi lama di Indonesia, Selanjutnya peneliti mencoba untuk menganalisis beberapa journal perguruan tinggi yang ada di provinsi Lampung dan peneliti menemukan beberpa jurnal perguruan tinggi di Lampung masih menggunakan OJS versi lama. Meskipun beberapa website *vulnerabitiy* telah mempublikasikan *vulnerability* XSS database

OWASP yang menunjukan versi OJS lama memiliki kerentanan terhadap XSS (*Cross Site Scripting)*

Dari hasil temuan awal yang peneliti temukan penyebab beberapa perguruan tinggi masih menggunakan OJS versi lama, peneliti menemukan bahwa beberapa OJS versi lama memberikan tambahan *Web Application Firewall* (WAF) untuk mengamankan OJS yang mereka miliki. WAF mampu menanggulangi terjadinya SQL Injection, XSS, file inclusion dengan memeriksa lalu lintas pada HTTP [3] . untuk membandingkan penggunaan WAF dalam menanggulangi kerentanan pada OJS versi lama, peneliti mencoba untuk menguji tingkat kerentanan dengan menggunakan *Information System Security Assessment Framework* (ISSAF) dan Zed Attack Proxy (ZAP), ZAP merupakan sebuah aplikasi Vulnerability Scanner yang banyak digunakan karena kemudahan penggunaannya, dan memiliki tingkat akurasi yang baik [4] .

2. METODE PENELITIAN

Pada tahap ini peneliti mencoba mencari beberapa literatur yang berkaitan dengan pengujian kerentanan sebuah sistem dan referensi lain yang dapat peneliti gunakan untuk melakukan analisis. Selanjutnya menggunakan framework ISSAF (*Information System Security Asessment Framework*) untuk melakukan pengujian kerentanan



Gambar 1 Tahapan Penelitian.

2.1 Tahapan Pengujian ISSAF

a. Tahap *Information Gathering*
Tahapan ini merupakan tahapan pengumulan informasi terhadap target penelitia menggunakan Whois.com untuk mengetahui Name Server, penggunaan WAF atau tidak dan informasi umum yang dibutuhkan.[5]
b. Tahapan *Network Mapping*
Tahapan ini dilakukan untuk mengetahui port yang terbuka dan memperoleh informasi service apa saja yang berajalan pada server [6] peneliti menggunakan software Nmap untuk melihat port apa saja yang terbuka pada server OJS.
c. Tahap *Vulnerability Identification*
Pada tahap ini merupakan tahapan untuk melakukan pemindaian terhadap sistem target untuk mengetahui kerentanan pada sistem [7], peneliti menggunakan ZAP 2.15.0
d. Penetration testing
Merupakan proses menguji keamanan suatu sistem dengan cara melakukan simulasi nyata. Tujuan dari pentest adalah untuk mencari kelemahan-kelemahan dalam sistem untuk mencegah kemungkinan terjadinnya kemungkinan hacking dan mengurangi resiko akses yang tidak sah, pencurian data [8].
e. Gaining Access and Privilege Escalation
Pada tahap ini merupakan sebuah percobaan untuk mendapatkan akses terhadap akun dengan menggunakan blank password maupun default password.
f. Enumerating Further
Tahapan ini merupakan tahapan pengujian dengan melakukan pengambilan,pemecahan informasi password yang didapatkan dari sistem
g. Compromise Remote User/Sites,
Tahap ini merupakan tahapan pengujian dengan melakukan ekspoitasi user root yang biasa digunakan untuk remot/hubungan jarak jauh.
h. Maintaining Access
Tahap ini merupakan tahap managemen akses, maintaining access tahapan pengujian untuk memastikan akses yang sah tetap diberikan kepada yang berhak.
i. Covering Tracks,
Tahapan ini adalah tahapan terakhir dari pengujian penetration testing tahapan ini akan menghapus log serangan yang telah dilakukan pada tahapan – tahapan sebelumnya.

3. HASIL DAN PEMBAHASAN

Pada bagian ini disajikan hasil evaluasi keamanan terhadap sistem Open Journal Systems (OJS) versi lama dengan menggunakan kerangka Information System Security Assessment Framework (ISSAF). Evaluasi dilakukan berdasarkan tahapan-tahapan yang tercantum dalam ISSAF.

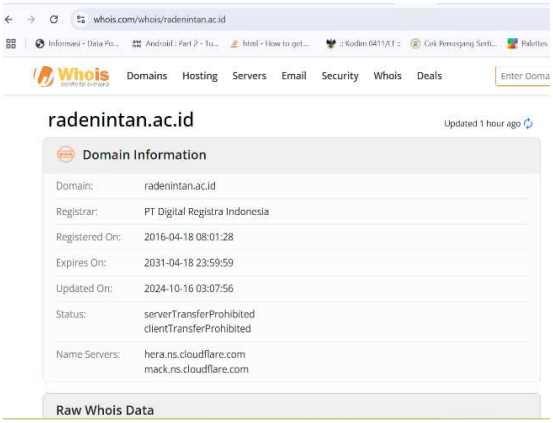
3.1 Proses Pengujian

P-ISSN: 2337-8344
E-ISSN: 2623-1247

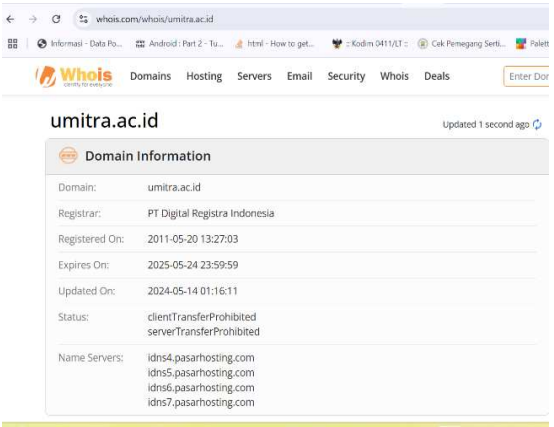
Untuk melakukan pengujian ini peneliti menggunakan mengumpulkan informasi terkait kampus yang masih menggunakan ojs versi *outdated* yang kemudian dilakukan proses analisis menggunakan framework ISSAF.

a. *Information Gathering*

Pada tahap ini peneliti melakukan pengecetak versi ojs yang digunakan dengan melihat page source pada jurnal untuk mengetahui versi OJS yang digunakan, setelah itu peneliti menggunakan https://www.whois.com/ untuk melihat apakah OJS menggunakan WAF atau tidak dan selanjutnya peneliti menggunakan https://www.ssllabs.com/ untuk mengetahui SSL, dan IP publik yang digunakan. SSL (*Secure Sockets Layer*) merupakan teknologi keamanan standar yang digunakan antara server dan klien, dimana semua komunikasi antar klien dan server terenkripsi[9]

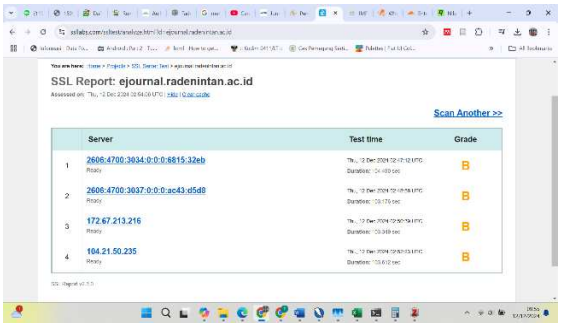


Gambar 2 Hasil lookup domain kampus X

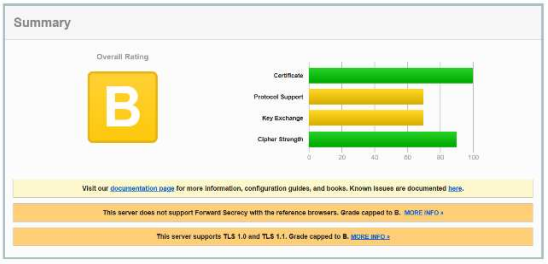


Gambar 3 Hasil Lookup Domain Kampus Y

Dari hasil lookup tersebut didapatkan bahwa kampus X menggunakan WAF, sedangkan kampus Y tidak menggunakan WAF. Selanjutnya pengujian menggunakan SSLLabs



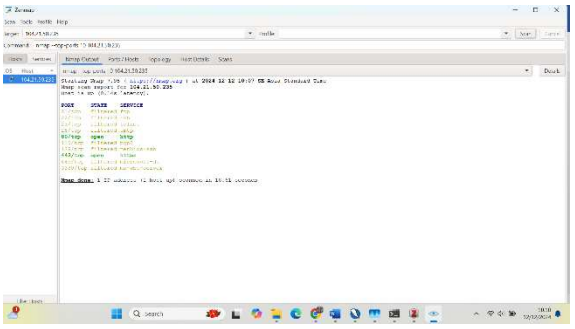
Gambar 4. Hasil pengujian SSL Labs kampus X



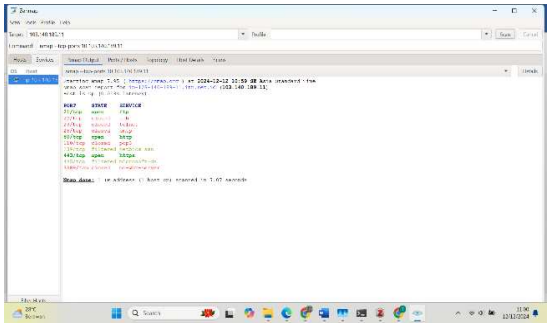
Gambar 5 Hasil Pengujian SSL Labs Kampus Y

b. Tahapan Network Mapping

Dari hasil pengujian menggunakan NMAP dengan kalibrasi pengujian pada 10 top port pada kampus X didapatkan 2 port terbuka yaitu port 80 dan port 443 port ini pada umumnya terbuka karena digunakan untuk keamanan komunikasi HTTP dan HTTPS [10] dan memfilter port - port lain berbeda dengan yang dilakukan oleh kampus X, kampus Y membuka port 80,443,21 dan menutup port lain. Untuk fleksibilitas memfilter port adalah pilihan bagus, namun untuk keamanan menutup port adalah pilihan tepat dengan mengorbankan fleksibilitas website.



Gambar 6. hasil pengujian Nmap Kampus X

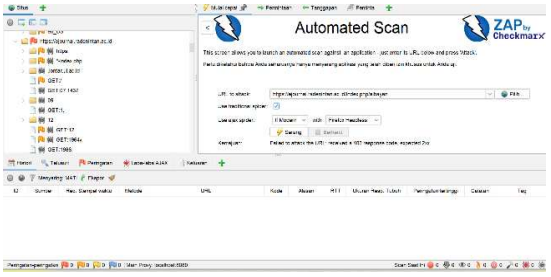


Gambar 7. Hasil Pengujian Nmap Kampus Y

c. Tahap Vulnerability Identification

Pada tahapan ini peneliti menggunakan ZAP 2.15.0 untuk kampus X tidak didapatkan hasil karena WAF memblokir pola trafik yang dianggap mencurigakan Sedangkan pada kampus Y didapatkan 2 alert yang berkaitan dengan big redirect yang berpotensi kebocoran informasi sensitif,kebocoran melalu HTTP.

Gambar 8. Hasil Pengujian ZAP Kampus X



Gambar 9. hasil pengujian ZAP Kampus Y

Alert type	Risk	Count
Big Redirect Detected (Potential Sensitive Information Leak)	Lemah	2 (100,0%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Lemah	43 (2.150,0%)
Total		2

Gambar 10 detail hasil pengujian ZAP

Penggunaan aplikasi ZAP 2.15.0 Pada tahap *Penetration testing, Gaining Access and Privilege Escalation,Enumerating Further, Compromise Remote User/Sites, Maintaining Access, Covering Tracks* dianggap sudah cukup untuk mencakup semua tahap pengujian tersebut diatas [11].

Dari hasil pengujian – pengujian yang telah dilakukan diatas maka dapat disimpulkan bahwa penggunaan WAF mampu melindungi dari serangan jahat oleh permintaan HTTP meskipun memiliki kekurangan karena harga yang mahal, dan WAF tidak dapat memblokir request yang belum dikenali [12].

Rekap Hasil pengujian dapat dilihat pada table dibawah ini :

Tabel 1. Rekap Hasil Pengujian

Parameter	Kampus X	Kampus Y
Pengguna WAF	Ya	Tidak
Kerentanan Yang ditemukan	Tidak	Big Redirect, Kebocoran HTTP
Alat Pengujian	ZAP	ZAP
Metode	WAF	Tidak Ada

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

Beberapa penelitian telah dilakukan terkait dengan pengujian keaman OJS diantaranya Analisis Keamanan Web Server Open Journal System(OJS) Menggunakan Metode ISSAF Dan OWASP (Studi Kasus Ojs Universitas Lancang Kuning) [13], Analisis Keamanan Pada Web Aplikasi Open Journal System Terhadap Serangan Cross Site Scripting (XSS) Menggunakan Metode Vulnerability Assessment [14], dari penelitian yang sudah dilakukan diatas penggunaan ISSAF dan OWASP sebagai framework pengujian umum digunakan untuk pengujian keamanan OJS, namun peran WAF sebagai pengaman yang mampu melindungi OJS dari serangan belum dibahas sehingga peneliti mencoba membandingkan antara OJS yang menggunakan WAF dan yang tidak menggunakan WAF, penelitian ini menguji 2 OJS versi 2 yang memiliki celah keamanan dimana pengguna terdaftar dapat mengunggah file berbahaya, dan file yang diunggah dapat diakses melalui url meskipun file ojs mampu merubah nama namun ekstensi file yang diunggah tetap [15]. dikemudian hari dibutuhkan penelitian yang membandingkan keamanan OJS versi terbaru dengan menggunakan WAF maupun tanpa menggunakan WAF.

4.2 Saran

Beberapa penelitian telah dilakukan terkait dengan pengujian keaman OJS diantaranya Analisis Keamanan Web Server Open Journal System(OJS) Menggunakan Metode ISSAF Dan OWASP (Studi Kasus Ojs Universitas Lancang Kuning) [13], Analisis Keamanan Pada Web Aplikasi Open Journal System Terhadap Serangan Cross Site Scripting (XSS) Menggunakan Metode Vulnerability Assessment [14], dari penelitian yang sudah dilakukan diatas penggunaan ISSAF dan OWASP sebagai framework pengujian umum digunakan untuk pengujian keamanan OJS, namun peran WAF sebagai pengaman yang mampu melindungi OJS dari serangan belum dibahas sehingga peneliti mencoba membandingkan antara OJS yang menggunakan WAF dan yang tidak menggunakan WAF, penelitian ini menguji 2 OJS versi 2 yang memiliki celah keamanan dimana pengguna terdaftar dapat mengunggah file berbahaya, dan file yang diunggah dapat diakses melalui url meskipun file ojs mampu merubah nama namun ekstensi file yang diunggah tetap [15]. dikemudian hari dibutuhkan penelitian yang membandingkan keamanan OJS versi terbaru dengan menggunakan WAF maupun tanpa menggunakan WAF.

OJS Versi lama memiliki tingkat kerentanan keamanan yang signifikan, XSS (Cross Site Scriping) dan kebocoran informasi. Penggunaan *Web Application Firewall* (WAF) mampu mengurangi resiko keamanan, meskipun terbatas pada serangan yang dikenali. Penggunaan OWASP ZAP terbukti efektif untuk menganalisis celah kemanan pada OJS. Pembaruan OJS tetap perlu dilakukan untuk memperbarui tingkat keamanan, perningkatan fitur, menjaga agar tetap kompatibel dengan browser yang digunakan, perbaikan bug pada OJS. Dari penelitian ini dapat dilakukan penelitian lebih lanjut mengenai penerapan WAF pada OJS versi baru.

DAFTAR PUSTAKA

[1] A. C. N. de Rivera, “It’s Time to Upgrade OJS,” Public Knowledge Project. Accessed: Dec. 13, 2024. [Online]. Available: https://pkp.sfu.ca/2022/02/23/its-time-to-upgrade-ojs/

[2] I. Riadi, A. Yudhana, and Y. W, “Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment,” *J. Teknol. Inf. Dan Ilmu Komput.*, vol. 7, no. 4, pp. 853–860, Aug. 2020, doi: 10.25126/jtiik.2020701928.

[3] A. Aryapranata, “Web Application Firewall pada Situs Web Institut Bisnis Nusantara www.ibn.ac.id,” *J. Esensi Infokom J. Esensi Sist. Inf. Dan Sist. Komput.*, vol. 4, no. 1, pp. 55–59, May 2020, doi: 10.55886/infokom.v4i1.321.

[4] M. G. A. Danialdo, F. A. Bakhtiar, and M. Data, “Pengujian Efektivitas OWASP ZAP dalam Menemukan Kerentanan dari Metasploitable”.

[5] I. G. A. S. Sanjaya, G. M. A. Sasmita, and D. M. S. Arsa, “Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF,” *J. Ilm. Merpati Menara Penelit. Akad. Teknol. Inf.*, p. 113, July 2020, doi: 10.24843/JIM.2020.v08.i02.p05.

[6] Z. A. Khan, “Penetration Testing Information System Security Assessment Framework (ISSAF)”.

[7] R. Umar, I. Riadi, and S. A. Wicaksono, “Security Analysis of Learning Management System Using Penetration Testing with ISSAF Framework,” *PIKSEL Penelit. Ilmu Komput. Sist. Embed. Log.*, vol. 12, no. 1, pp. 59–68, Mar. 2024, doi: 10.33558/piksel.v12i1.8331.

[8] Dept of Information Technology, Faculty of Engineering, Udayana University, Bali, Indonesia, I. G. A. S. P. Wijaya, G. M. A. Sasmita, and I. P. A. E. Pratama, “Web Application Penetration Testing on Udayana University’s OASE E-learning Platform Using Information System Security Assessment Framework (ISSAF) and Open Source Security Testing Methodology Manual (OSSTMM),” *Int. J. Inf. Technol. Comput. Sci.*, vol. 16, no. 2, pp. 45–56, Apr. 2024, doi: 10.5815/ijitcs.2024.02.04.

[9] M. Azwan, A. F. Adriansyah, and M. R. A. Fauzan, “PROTOKOL SECURE SOCKET LAYER UNTUK KEAMANAN BERBASIS WEB,” vol. 1.

[10] I. C. Utomo and S. Rokhmah, “Konfigurasi SSL Untuk Meningkatkan Keamanan Web server Pada Program Studi Teknik Informatika Universitas Muhammadiyah Surakarta,” *J. Rekayasa Teknol. Inf. JURTI*, vol. 6, no. 2, p. 143, Dec. 2022, doi: 10.30872/jurti.v6i2.8333.

[11] A. Jakobsson and I. Häggström, "Study of the techniques used by OWASP ZAP for analysis of vul- nerabilities in web applications".

[12] M. Ito and H. Iyatomi, "Web application firewall using character-level convolutional neural network," in *2018 IEEE 14th International Colloquium on Signal Processing & Its Applications (CSPA)*, 2018, pp. 103–106. doi: 10.1109/CSPA.2018.8368694.

[13] G. Guntoro, L. Costaner, and M. Musfawati, "ANALISIS KEAMANAN WEB SERVER OPEN JOURNAL SYSTEM (OJS) MENGGUNAKAN METODE ISSAF DAN OWASP (STUDI KASUS OJS UNIVERSITAS LANCANG KUNING)," *JIPI J. Ilm. Penelit. Dan Pembelajaran Inform.*, vol. 5, no. 1, p. 45, June 2020, doi: 10.29100/jipi.v5i1.1565.

[14] Yunanri.W, "Analisis Keamanan Pada Web Aplikasi Open Journal System Terhadap Serangan Cross Site Scripting (XSS) Menggunakan Metode Vulnerability Assessment," *Digit. Transform. Technol. Digit.*, vol. 3, no. 1, pp. 83–90, Mar. 2023.

[15] H.-T. Bridge, "Open Journal Systems (OJS) 2.3.6 - Multiple Script Arbitrary File Upload," Exploit Database. Accessed: Dec. 12, 2024. [Online]. Available: https://www.exploit-db.com/exploits/37001