BUFNETS
BULLETIN OF NETWORK ENGINEERING AND INFORMATICS
https://bufnets.tech

BULLETIN OF NETWORK ENGINEERING AND INFORMATICS
Vol. 1 No 2 – October 2023

VULNERABILITY ASSESSMENT PADA WEBSITE PORTAL MANAJEMEN INFORMATIKA POLITEKNIK LP3I

VULNERABILITY ASSESSMENT ON THE PORTAL WEBSITE MANAJEMEN INFORMATIKA POLITEKNIK LP3I

DESFITA EKA PUTRI
Manajemen Informatika, Politeknik Lembaga Pendidikan dan Pengembangan Profesi Indonesia
Kota Pekanbaru, Provinsi Riau, Indonesia

e-mail: desfitaekaputri@plb.ac.id

Received : 10 Mei 2023	Accepted : 05 Juni 2023	Published : 1 October 2023

Abstract

A research on vulnerability assessment of the website portal of Manajemen Informatika Politeknik LP3I was conducted to identify weaknesses or vulnerabilities that could be exploited by malicious parties to launch cyber attacks. The study was conducted using a testing methodology that examined various aspects that affect website security, such as identification of the platform and applications used, risk analysis, identification of potential attack vectors, and technical testing. The results of this research are expected to assist authorized parties in improving website security and preventing attacks that may harm users and the institution. In the digital era, cybersecurity awareness is crucial, especially for websites that contain sensitive information such as the university's portal website. This research is expected to raise awareness of cybersecurity and help develop better security systems in the future, ensuring that the Manajemen Informatika Politeknik LP3I portal website remains safe and protected from cyberattacks that could harm the institution and its users.

Keywords: *Vulnerability Assessment, Website Portal, Cybersecurity, Cyber Attacks, Penetration Testing.*

Abstrak

Penelitian tentang vulnerability assessment pada website portal Manajemen Informatika Politeknik LP3I dilakukan untuk mengidentifikasi kelemahan atau kerentanan pada website yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk melakukan serangan cyber. Penelitian ini dilakukan dengan metode pengujian pada berbagai aspek yang mempengaruhi keamanan website seperti identifikasi platform dan aplikasi, analisis risiko, identifikasi serangan yang mungkin terjadi, dan pengujian teknis. Hasil dari penelitian ini diharapkan dapat membantu pihak yang berwenang dalam meningkatkan keamanan website dan mencegah serangan yang merugikan pengguna dan institusi. Dalam era digital seperti sekarang, kesadaran akan pentingnya keamanan siber sangatlah penting, khususnya pada website yang berisi informasi sensitif seperti website portal universitas. Dengan adanya penelitian ini diharapkan dapat meningkatkan kesadaran akan keamanan siber dan membantu dalam pengembangan sistem keamanan yang lebih baik di masa depan, sehingga website portal Manajemen Informatika Politeknik LP3I dapat tetap aman dan terhindar dari serangan cyber yang dapat merugikan institusi maupun pengguna.

Kata Kunci: *Vulnerability Assessment, Website Portal, Keamanan Siber, Serangan Cyber, Penetrasi Testing.*

1. PENDAHULUAN

Pada era digital saat ini, penggunaan teknologi informasi menjadi hal yang semakin penting dan tak terhindarkan [1]. Hal ini berlaku pula pada sistem informasi yang digunakan oleh Manajemen Informatika Politeknik LP3I untuk menjalankan kegiatan akademik dan administratif. Dalam kaitannya dengan hal ini,

keamanan siber atau cybersecurity menjadi salah satu aspek yang sangat penting untuk diperhatikan dan dijaga [2]. Manajemen Informatika Politeknik LP3I memiliki sebuah website portal yang berisi informasi penting dan rahasia yang hanya boleh diakses oleh pihak yang berwenang. Namun, website portal tersebut rentan terhadap serangan siber apabila tidak memiliki sistem keamanan yang memadai [3].

Untuk memastikan keamanan website portal tersebut, diperlukan sebuah penelitian yang memfokuskan pada identifikasi kelemahan atau kerentanan pada sistem keamanan website portal tersebut [4]. Penelitian ini berjudul Vulnerability Assessment pada Website Portal Manajemen Informatika Politeknik LP3I. Penelitian ini dilakukan untuk mengidentifikasi kelemahan atau kerentanan pada website yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk melakukan serangan cyber. Penelitian ini menggunakan metode pengujian pada berbagai aspek yang mempengaruhi keamanan website seperti identifikasi platform dan aplikasi, analisis risiko, identifikasi serangan yang mungkin terjadi, dan pengujian teknis.

Dalam penelitian ini, pentingnya keamanan siber pada website portal Manajemen Informatika Politeknik LP3I menjadi fokus utama. Penelitian ini diharapkan dapat membantu pihak yang berwenang dalam meningkatkan keamanan website dan mencegah serangan yang merugikan pengguna dan institusi. Keamanan siber menjadi sangat penting karena dapat memengaruhi kredibilitas dan reputasi dari Manajemen Informatika Politeknik LP3I [5]. Oleh karena itu, dengan adanya penelitian ini diharapkan dapat meningkatkan kesadaran akan keamanan siber dan membantu dalam pengembangan sistem keamanan yang lebih baik di masa depan, sehingga website portal Manajemen Informatika Politeknik LP3I dapat tetap aman dan terhindar dari serangan cyber yang dapat merugikan institusi maupun pengguna.

Dalam menjalankan kegiatan akademik dan administratif, Manajemen Informatika Politeknik LP3I sangat bergantung pada sistem informasi yang dimilikinya, termasuk di dalamnya website portal. Oleh karena itu, keamanan siber menjadi faktor penting yang harus diperhatikan. Dalam penelitian ini, diharapkan dapat ditemukan kelemahan atau kerentanan pada website portal yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab, sehingga dapat diambil langkah-langkah yang tepat untuk meningkatkan keamanan siber dari website portal tersebut [6].

2. METODE PENELITIAN

Penelitian Vulnerability Assessment pada Website Portal Manajemen Informatika Politeknik LP3I membutuhkan pendekatan holistik dan sistematis untuk mengidentifikasi dan menilai risiko keamanan. Oleh karena itu, metode penelitian yang digunakan harus memperhatikan berbagai aspek yang mempengaruhi keamanan website, mulai dari identifikasi platform dan aplikasi hingga pengujian teknis dan penyusunan rekomendasi. Berikut ini langkah-langkah yang dilakukan dalam melaksanakan Vulnerability Assessment Pada Website Portal Manajemen Informatika Politeknik LP3I .

a). Identifikasi platform dan aplikasi: Langkah awal adalah mengidentifikasi platform dan aplikasi yang digunakan pada website portal Manajemen Informatika Politeknik LP3I. Hal ini dilakukan dengan memeriksa sumber daya website seperti file HTML, JavaScript, dan CSS, serta memeriksa informasi pada server seperti header HTTP dan informasi server [7].

b). Analisis risiko: Setelah mengidentifikasi platform dan aplikasi, tahap selanjutnya adalah melakukan analisis risiko terhadap website portal Manajemen Informatika Politeknik LP3I [8]. Analisis risiko meliputi identifikasi ancaman yang mungkin terjadi, evaluasi kerentanan yang ada pada website, dan menentukan tingkat risiko yang mungkin timbul akibat kerentanan tersebut, proses analisis dilakukan menggunakan software wp-scan yaitu aplikasi scanner vulnerability khusus untuk platform wordpress [9].

c). Identifikasi serangan yang mungkin terjadi: Langkah selanjutnya adalah mengidentifikasi jenis serangan yang mungkin terjadi pada website portal Manajemen Informatika Politeknik LP3I, seperti serangan SQL Injection, Cross-Site Scripting (XSS), dan lain-lain. Hal ini dilakukan dengan memeriksa kerentanan yang ada pada website dan mengidentifikasi teknik yang mungkin digunakan oleh

penyerang untuk mengeksploitasi kerentanan tersebut [10].

d). Pengujian teknis: Setelah dilakukan identifikasi kerentanan dan serangan yang mungkin terjadi, tahap selanjutnya adalah melakukan pengujian teknis pada website portal Manajemen Informatika Politeknik LP3I [11]. Pengujian teknis dapat dilakukan dengan menggunakan berbagai alat pemindaian kerentanan seperti Nmap dan WPScan [12].

e). Analisis hasil dan rekomendasi: Setelah melakukan pengujian teknis, langkah terakhir adalah melakukan analisis hasil dan menyusun rekomendasi untuk meningkatkan keamanan website portal Manajemen Informatika Politeknik LP3I. Rekomendasi dapat berupa tindakan perbaikan kerentanan, memperbarui sistem keamanan, meningkatkan pengawasan dan monitoring, serta pelatihan dan kesadaran pengguna tentang keamanan siber [13].

Metode Penelitian ini diharapkan dapat memberikan gambaran yang komprehensif tentang keamanan website portal Manajemen Informatika Politeknik LP3I , serta memberikan rekomendasi untuk meningkatkan keamanan website dan mencegah serangan yang merugikan pengguna dan institusi.

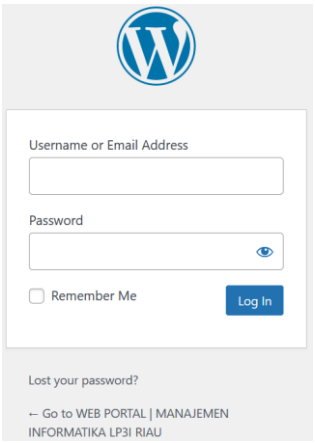
3. HASIL DAN PEMBAHASAN

3.1 Identifikasi platform dan aplikasi

Proses identifikasi platform dan aplikasi dapat menggunakan metode blackbox test, metode ini diasumsikan bahwa serangan dilakukan dari pihak eksternal yang tidak mengetahui spesifikasi dari platform dan aplikasi yang digunakan [14]. Proses identifikasi pada kasus ini dapat dilakukan dengan browser Mozilla firefox yang memiliki fitur inspect element yang dapat digunakan untuk melihat script yang digunakan dalam pembuatan website [15]. Berikut ini Gambar 1 yang berisi hasil identifikasi dari platform dan aplikasi yang digunakan.

Gambar 1. Hasil identifikasi platform dan aplikasi dari WEB Portal MIK LP3I
[Sumber: Penulis, 2023]

Dari proses identifikasi, ditemukan bahwa *source code* website mengandung beberapa *folder* yang identik dengan *folder* yang dimiliki website CMS Wordpress, seperti pada Gambar 1 yang ditunjukan kotak merah (wp-includes, wp-content, themes) yang sering digunakan pada CMS Wordpress [6]. Untuk lebih meyakinkan bahwa website tersebut menggunakan CMS Wordpress maka proses selanjutnya adalah dengan mengakses *URL* administrator CMS Wordpress yang ada pada alamat wp-admin. Berikut ini gambar 2 yang menunjukan halaman login website.



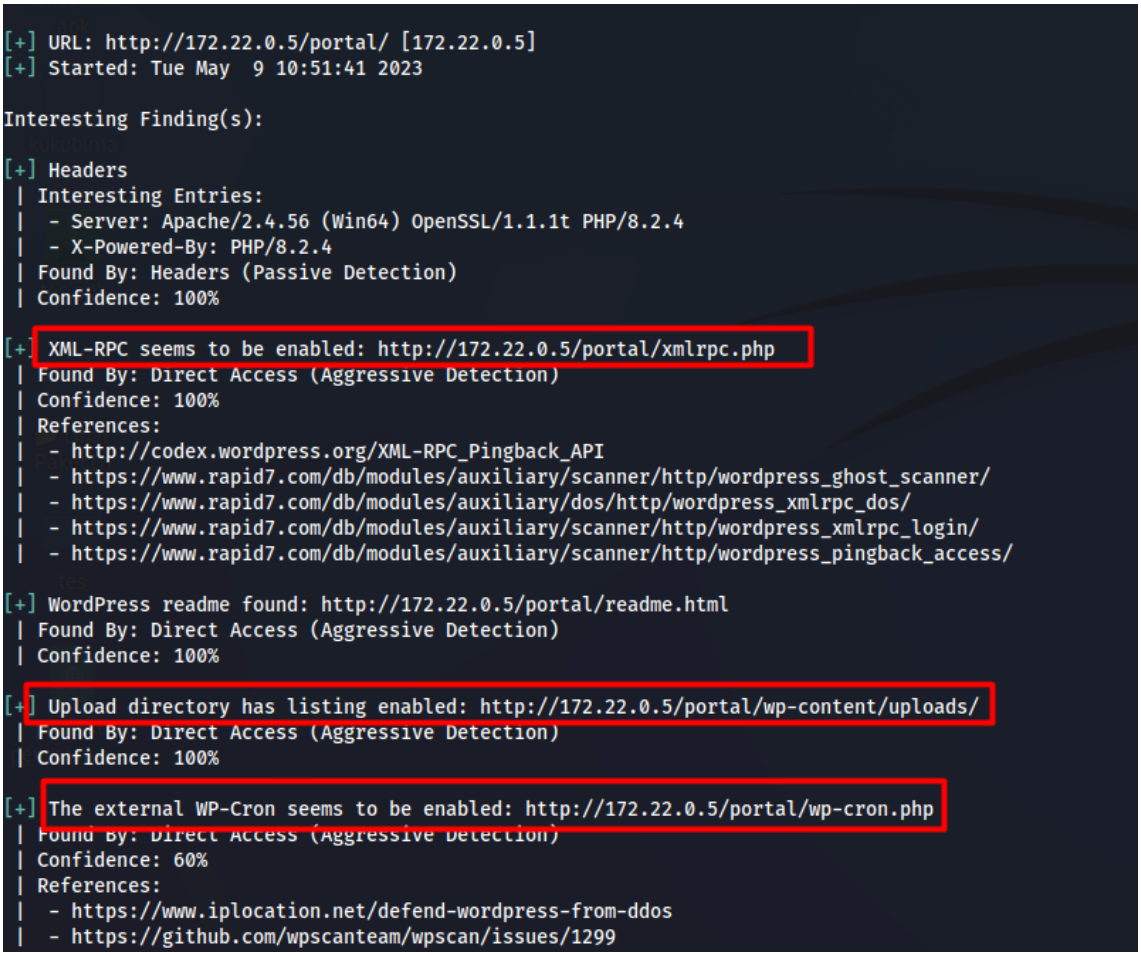
Gambar 2. Halaman wp-login.php dari website portal
[Sumber: Penulis, 2023]

Halaman wp-admin di redirect ke halaman wp-login.php hal ini menunjukan bahwa proses identifikasi menggunakan browser Mozilla firefox dengan fitur inspect element telah berhasil mengidentifikasi platform dari website, website portal tersebut menggunakan CMS Wordpress.

Maka proses selanjutnya yaitu proses analisis resiko dapat dilakukan menggunakan software WPScan yang dapat menemukan vulnerability pada website yang menggunakan CMS Wordpress [17].

3.2 Analisis risiko

Analisis hasil pemindaian. WPScan akan menampilkan daftar kerentanan yang ditemukan pada situs web. Evaluasi setiap kerentanan dan analisis risiko yang mungkin timbul dari kerentanan tersebut. Berikut ini Gambar 3 yang menunjukan vulnerability yang ditemukan oleh software WPScan.



Gambar 3. Hasil WPScan dalam melakukan scanning web portal
[Sumber: Penulis, 2023]

WPScan akan memindai situs web dan menampilkan hasilnya pada terminal. WPScan akan mencari kerentanan keamanan, versi WordPress yang digunakan, dan plugin atau tema yang digunakan pada situs web.

3.3 Identifikasi serangan yang mungkin terjadi

Pada tahap analisis resiko, telah ditemukan beberapa vulnerability yang ada pada website portal, vulnerability ini perlu di identifikasi untuk melihat resiko serangan yang akan terjadi di kemudian hari apabila vulnerability yang ditemukan tidak di tangani dengan serius [18]. Beberapa vulnerability yang ditemukan dari

proses scanning oleh software WPScan dapat dilihat pada Tabel 1 dibawah ini.

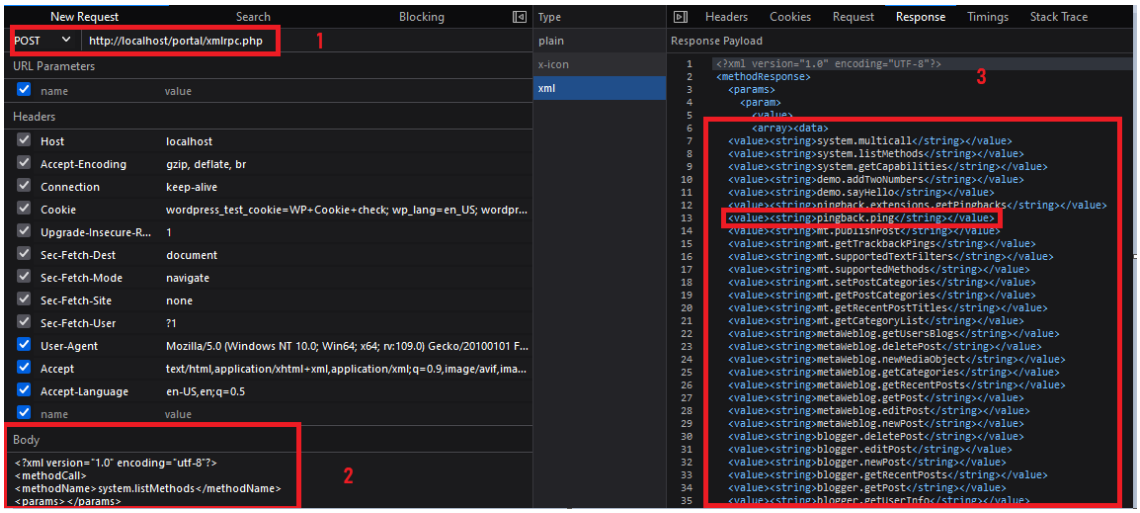
Tabel 1: vulnerability yang ditemukan dan kemungkinan serangan yang akan terjadi

No	Vulnerability	Keterangan
1	XML-RPC ENABLED	Kerentanan ini terjadi ketika protokol XML-RPC diaktifkan pada sistem. Kemungkinan serangan yang dapat terjadi akibat kerentanan ini antara lain adalah serangan brute-force password dan serangan DoS (Denial of Service) [19].
2	UPLOAD DIRECTORY LISTING ENABLED	Kerentanan ini terjadi ketika opsi untuk melihat daftar direktori pada folder upload diaktifkan pada sistem. Kemungkinan serangan yang dapat terjadi akibat kerentanan ini antara lain adalah akses ke file sensitif, perusakan sistem, atau pengungkapan informasi sensitif [20].
3	WP-CRON ENABLED	Kerentanan ini terjadi ketika fitur WP-Cron diaktifkan pada sistem. Kemungkinan serangan yang dapat terjadi akibat kerentanan ini antara lain adalah penyerangan spam, perusakan sistem, atau akses ke data sensitif [21].

3.4 Pengujian teknis

Terdapat empat vulnerability yang ditemukan dan dapat dilakukan pada tahap analisis resiko dan dari tabel 1 beberapa vulnerability telah diberika keterangan tentang serangan yang mungkin akan terjadi apabila vulnerability yang ditemukan tidak segera dilakukan.

Proses uji teknis pertama yang dilakukan adalah melakukan penetrasi testing untuk melakukan serangan pada vulnerability XML-RPC ENABLED, berikut ini gambar 4 yang merupakan proses melihat list fitur yang ada pada xmlrpc-php.



Gambar 4. Ujicoba exploitasi xmlrpc.php
[Sumber: Penulis, 2023]

Pada Gambar 4 menunjukan proses manipulasi request menggunakan fitur inspect element mozilla firefox dengan request yang di tunjukan angka 1 pada Gambar 4 dan payload yang di tunjukan angka 2 pada gambar 4, menunjukan bahwa fitur xmlrpc.php yang dapat di eksploitasi di tunjukan pada angka 3 pada Gambar 4, salah satunya adalah fitur pingback yang dapat dieksploitasi untuk melakukan DDoS [22]. Selain xml-rpc terdapat kelemahan yang cukup serius apabila tidak ditangani dengan baik yaitu upload directory yang terlihat oleh publik yang dapat mengakibatkan file-file sensitif dapat terlihat oleh publik.

Berikut ini Gambar 5 yang menunjukan apabila list file pada direktori tidak disembunyikan, maka file yang diupload akan terlihat orang lain, dan akan berbahaya apabila file yang diupload adalah file sensitif.

Gambar 5. Sensitif direktori listing
[Sumber: Penulis, 2023]

Seorang administrator terkadang lupa untuk menghapus file sensitif yang di upload ke dalam website, sehingga file terlihat orang lain, hal ini akan berbahaya apabila file berisi konfigurasi database maupun konfigurasi lainya.

Ujicoba selanjutnya adalah ujicoba serangan pada vulnerability wp-cron, beberapa sumber [23],[24] menjelaskan bahwa wp-cron digunakan untuk menjalankan cronjob pada situs wordpress, fitur cronjob di perlukan untuk menjadwalkan beberapa tugas yang dapat dilakukan secara terjadwal, namun beberapa kerugian apabila wp-cron dilakukan tidak pada semestinya. Berikut ini ancaman yang akan terjadi jika situs mengaktifkan fitur wp-cron:

a). DDoS Attack: Seperti yang telah disebutkan sebelumnya, wp-cron.php berfungsi dengan membuat permintaan HTTP tambahan untuk dirinya sendiri setiap kali ada permintaan masuk ke situs WordPress. Jika situs tersebut mengalami lalu lintas yang tinggi, penggunaan wp-cron.php dapat membebani server dan mengganggu kinerjanya. Serangan DDoS yang dilakukan dengan cara ini dapat merusak situs dan membuatnya tidak dapat diakses.

b). Remote Code Execution: Jika situs WordPress rentan terhadap serangan Remote Code Execution (RCE), penyerang dapat mengirimkan permintaan palsu ke wp-cron.php untuk mengeksekusi kode berbahaya pada situs tersebut.

c). Timing Attack: Penyerang dapat memanfaatkan wp-cron.php untuk meluncurkan serangan timing attack. Dalam serangan ini, penyerang menggunakan wp-cron.php untuk menghitung waktu yang diperlukan oleh situs WordPress untuk mengeksekusi tugas terjadwal tertentu. Dengan mengeksploitasi informasi ini, penyerang dapat mencoba mengidentifikasi kerentanan pada situs WordPress.

d). Pengungkapan Informasi Sensitif: Jika pengaturan wp-cron.php tidak dikonfigurasi dengan benar, informasi sensitif seperti nama pengguna dan kata sandi dapat diungkapkan secara tidak sengaja melalui wp-cron.php.

Untuk mencegah kerentanan keamanan ini, penting untuk mengkonfigurasi wp-cron.php dengan benar dan melindungi situs WordPress dari serangan yang mungkin terjadi. Ini dapat dilakukan dengan menggunakan plugin keamanan WordPress yang andal, memperbarui WordPress ke versi terbaru, dan mengoptimalkan pengaturan server untuk memastikan kinerja yang optimal.

3.5 Analisis hasil dan rekomendasi

Berdasarkan hasil analisis kerentanan yang ditemukan pada website WordPress, terdapat beberapa rekomendasi yang dapat dilakukan untuk meningkatkan keamanan website, antara lain:

a). Menonaktifkan protokol XML-RPC: Dalam hal ini, direkomendasikan untuk menonaktifkan protokol XML-RPC jika tidak diperlukan pada website, karena kerentanan ini dapat memberikan celah bagi penyerang untuk melakukan serangan brute-force password dan DoS.

b). Menonaktifkan opsi directory listing pada folder upload: Jika opsi directory listing diaktifkan pada folder upload, maka rekomendasi adalah untuk

menonaktifkannya, karena dapat memberikan akses bagi penyerang untuk melihat file sensitif dan memperoleh informasi penting pada website.

c). Menonaktifkan fitur WP-Cron: WP-Cron adalah fitur WordPress yang berguna untuk mengatur tugas yang dijalankan pada waktu yang ditentukan. Jika tidak diperlukan, disarankan untuk menonaktifkan fitur ini untuk menghindari serangan spam, perusakan sistem, atau akses ke data sensitif.

d). Memperbarui sistem WordPress, plugin, dan tema secara berkala: Dalam hal ini, disarankan untuk selalu memperbarui sistem WordPress, plugin, dan tema yang digunakan pada website secara berkala, karena seringkali pembaruan ini dilakukan untuk memperbaiki kerentanan keamanan pada sistem.

e). Menggunakan plugin keamanan: Dalam upaya meningkatkan keamanan website, direkomendasikan untuk menggunakan plugin keamanan yang dapat membantu mendeteksi dan mencegah serangan pada website.

Dengan melakukan tindakan-tindakan pencegahan tersebut, diharapkan dapat membantu meningkatkan keamanan website WordPress dan mengurangi risiko terjadinya serangan atau pelanggaran keamanan pada website [25].

4. KESIMPULAN

Berdasarkan temuan yang ada pada penelitian yang berjudul "Vulnerability Assessment pada Website Portal Manajemen Informatika Politeknik LP3I", dapat disimpulkan bahwa website tersebut memiliki beberapa kerentanan yang dapat memungkinkan terjadinya serangan atau pelanggaran keamanan pada sistem. Kerentanan tersebut antara lain terdapatnya celah pada sistem autentikasi, masalah keamanan pada plugin dan tema yang digunakan, serta adanya informasi sensitif yang dapat diakses oleh pengguna yang tidak berwenang.

Dari hasil analisis risiko dengan menggunakan tools seperti WPScan dan Nmap, ditemukan beberapa serangan yang mungkin terjadi sebagai akibat dari kerentanan yang ada pada sistem, seperti serangan brute-force password, injeksi SQL, cross-site scripting (XSS), serta akses ke informasi sensitif.

Untuk mengatasi kerentanan dan meminimalkan risiko terjadinya serangan, beberapa tindakan pencegahan direkomendasikan, antara lain memperbarui sistem WordPress, plugin, dan tema secara berkala, memperkuat sistem autentikasi dengan menggunakan password yang kompleks dan menerapkan teknik keamanan lainnya, serta membatasi akses terhadap informasi sensitif hanya kepada pengguna yang berwenang.

Dengan menerapkan tindakan pencegahan tersebut, diharapkan dapat meningkatkan keamanan pada website portal manajemen informatika Politeknik LP3I dan mengurangi risiko terjadinya serangan atau pelanggaran keamanan pada sistem..

PERNYATAAN PENGHARGAAN

Ucapan terima kasih yang sebesar-besarnya kepada pengelola website dan tim IT yang telah memberikan akses dan dukungan dalam penelitian kami. Tanpa kerjasama dan partisipasi dari pihak-pihak tersebut, penelitian ini tidak mungkin terlaksana.

Terima kasih juga kepada rekan-rekan yang telah memberikan dukungan, motivasi, dan saran yang sangat berharga dalam proses penelitian ini. Tanpa bantuan dan dukungan dari rekan-rekan, penelitian ini tidak akan mencapai hasil yang memuaskan.

Semoga hasil dari penelitian ini dapat memberikan manfaat yang baik bagi pengembangan sistem informasi dan keamanan informasi di lingkungan kampus maupun organisasi lainnya. Terima kasih atas kerjasama dan partisipasi yang telah diberikan.

DAFTAR PUSTAKA

[1] Kurniawan, M. F., & Wanto, D. (2023). TEKNOLOGI PENDIDIKAN PASCA COVID-19. Jurnal Tunas Pendidikan, 5(2), 439-459.

[2] Saputra, M. F., & Wibawa, A. (2022). Peran dan Tantangan Cyber Security di Era Society 5.0. Jurnal Inovasi Teknologi dan Edukasi Teknik (JITET), 2(7).

[3] Simanjuntak, C. R., Pratama, S. A., & Barovih, G. (2023). Remanajemen Jaringan Menggunakan Framework NIST Pada Perpustakaan Daerah Provinsi Sumatera Selatan. Jurnal Teknologi Sistem Informasi, 4(1), 152-163.

[4] KUNCORO, A. W. (2022). Pengujian Autentikasi Dan Otorisasi Web Mi-

Gateway Uii Berdasarkan Dokumen Owasp Wstg V4. 2.

[5] Utari, S. A., Ardia, V., Jamiati, J., & Fitria, D. (2023). How an Organization Should Implement Risk Communication in Response to Cyber Attack in Indonesia. Journal on Education, 5(4), 14314-14328.

[6] Saputra, I. P., Utami, E., & Muhammad, A. H. (2022, October). Comparison of anomaly based and signature based methods in detection of scanning vulnerability. In 2022 9th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI) (pp. 221-225). IEEE.

[7] Firmansyah, M., & Yuswanto, A. (2022). Knowledge management for information security incident handling at Security Operation Center of Jakarta Provincial Government. Monas: Jurnal Inovasi Aparatur, 4(2), 441-452.

[8] Nurdiansyah, T., & Hendayun, M. (2022). ANALISIS DAN PENERAPAN MANAJEMEN RISIKO APLIKASI PEMANTAUAN SERTA SISTEM MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN. Scientia Regendi, 3(2), 48-67.

[9] Marczak, G. (2022). Security analysis of WordPress platform (Doctoral dissertation, Instytut Elektrotechniki Teoretycznej i Systemów Informacyjno-Pomiarowych).

[10] Gupta, D. (2023). A Critical Review of WordPress Security Scanning Tools and the Development of a Next-Generation Solution.

[11] Jagamogan, R. S., Ismail, S. A., Hassan, N. H., & Abas, H. (2022, July). Penetration Testing Procedure using Machine Learning. In 2022 4th International Conference on Smart Sensors and Application (ICSSA) (pp. 58-63). IEEE.

[12] Reti, D., Elzer, K., & Schotten, H. D. (2023). SCANTRAP: Protecting Content Management Systems from Vulnerability Scanners with Cyber Deception and Obfuscation. arXiv preprint arXiv:2301.10502.

[13] Witsenboer, J. W. A., Sijtsma, K., & Scheele, F. (2022). Measuring cyber secure behavior of elementary and high school students in the Netherlands. Computers & Education, 186, 104536.

[14] MEHARU, M. (2022). WEB SECURITY VULNERABILITY ANALYSIS IN SELECTED ETHIOPIAN GOVERNMENTAL OFFICES (USING WHITE BOX AND BLACK BOX TESTING) (Doctoral dissertation, St. Mary's University).

[15] Priambodo, D. F., Rifansyah, A. D., & Hasbi, M. (2023). Penetration Testing Web XYZ Berdasarkan OWASP Risk Rating. Teknika, 12(1), 33-46.

[16] Landauer, M., Wurzenberger, M., Skopik, F., Hotwagner, W., & Höld, G. (2023). Aminer: A modular log data analysis pipeline for anomaly-based intrusion detection. Digital Threats: Research and Practice, 4(1), 1-16.

[17] Shah, P. G., & Ayoade, J. (2023, January). An Empricial Study of Brute Force Attack on Wordpress Website. In 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 659-662). IEEE.

[18] Ponta, S. E., Plate, H., & Sabetta, A. (2020). Detection, assessment and mitigation of vulnerabilities in open source dependencies. Empirical Software Engineering, 25(5), 3175-3215.

[19] Exploiting the xmlrpc.php on all WordPress versions. (n.d.). Nitesculucian.github.io. https://nitesculucian.github.io/2019/07/01/exploiting-the-xmlrpc-php-on-all-wordpress-versions/

[20] John. (2018, December 24). Upload directory has directory listing enabled. WPMU DEV - Your All-In-One WordPress Platform. https://wpmudev.com/forums/topic/upload-directory-has-directory-listing-enabled/

[21] WordPress Plugin WP-Cron Dashboard Cross-Site Scripting (1.1.5) - Vulnerabilities. (n.d.). Acunetix. Retrieved May 10, 2023, from https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-wp-cron-dashboard-cross-site-scripting-1-1-5/

[22] Rizwan, B. (2020, November 5). Wordpress xmlrpc.php -common vulnerabilites & how to exploit them. Medium. https://the-bilal-rizwan.medium.com/wordpress-xmlrpc-php-common-vulnerabilites-how-to-exploit-them-d8d3c8600b32

[23] Guy, T. cPanel. (2018, October 4). The nightmare that is wp-cron.php. Medium.

https://medium.com/@thecpanelguy/the-nightmare-that-is-wpcron-php-ae31c1d3ae30
[24] WordPress Cron Enabled. (n.d.). Www.tenable.com. Retrieved May 13, 2023, from https://www.tenable.com/plugins/was/113449
[25] Herdianti, H., & Umar, F. (2020). Analisis keamanan website menggunakan teknik footprinting dan vulnerability scanning. INFORMAL: Informatics Journal, 5(2), 43-48.