**Scientific Journal of Informatics**
Vol. 11, No. 3, Aug 2024
p-ISSN 2407-7658 https://journal.unnes.ac.id/journals/sji/index e-ISSN 2460-0040

# cPanel Server Hosting Security Against Malware and DDoS Attacks on the Open Journal System Platform

**Muhammad Nadzirin Anshari Nur[1*], Hijriani[2]**
[1]Department of Electrical Engineering Faculty of Engineering, Universitas Halu Oleo, Indonesia
[2]Department of Law Unsultra Postgraduate, Universitas Sulawesi Tenggara, Indonesia

**Abstract.**
**Purpose:** This research analyzes the security of cPanel in protecting Open Journal Systems (O.J.S.) from DDoS attacks and malware infections. Since contemporary threats to this environment are continuously evolving, this investigation seeks to offer empirical findings and applicable suggestions for platform managers of academic publishing platforms.
**Methods:** The method applies the scope of the literature study and tests system-specific security using cpanel features to test Imunify360, SSL Manager, IP Blocker, Site Quality Monitoring, Awstats, and Jetbackup. This is then followed by observing the server logs on cPanel, where any suspicious activities or signs of attacks can be identified. It contributes to the detection of attack patterns and weaknesses in a system.
**Result:** This indicates several default settings within cPanel were found to be vulnerable and could allow exploitation for DDoS purposes. Tools available in cPanel helped eliminate malware and strengthen defense against DDoS attacks. This is verified by the AWStats check, which means a quicker and more secure access time from the server.
**Novelty:** This study combines many security features and tools from cPanel to implement a complete manner of detecting and improving its security. This method will not only help find out what the weak points are but also provide actionable solutions that can be employed to secure your application. The research results offer a practical guide for system administrators to enhance cPanel security configurations. This includes applying amended security settings and using more tools to safely sweep O.J.S. from online threats.

**Keywords**: CPanel, DDoS, O.J.S., Malware, Security
**Received** August 2024 / **Revised** September 2024 / **Accepted** September 2024



## INTRODUCTION

Cybersecurity is critical for academic publishing platforms that increasingly rely on digital systems to manage and distribute scientific content. One of the most used systems is Open Journal Systems (O.J.S.), but this also makes it a considerable target for hackers: every day, different botnets scan various addresses to which they can access O.J.S. Two of the lowest hanging yet devastatingly powerful fruit in cyberspace are Distributed Denial-of-Service (DDoS) attacks and web-based malware infections that, together, challenge most online services today [1]–[3] DDoS and malware attacks can cause significant downtime and service disruptions, impacting the reputation of web services, leading to a considerable decrease in web service performance, slowing down response times to user requests, and increasing the risk of system errors [4], [5].

cPanel is a popular hosting control panel with different security measures to protect your website from cyber threats. These features are tools that manage firewalls, monitor sites' performance, and put secure connections between them to improve website security and protect it from all possible attacks [6]. To combat more complex attacks, the default settings of cPanel are not enough, and you will need to update and configure your malware protection. There are clear indicators that cybercriminals now use robots to execute specific attacks and plan to facilitate threats by injecting weaknesses/breaches in software, communication networks, and hardware, among others. These vulnerabilities are taken advantage of by many kinds of cyber threats, including Distributed Denial of Service (DDoS) attacks that illustrate the necessity for more secure measures than those provided by default [3], [7].

*Corresponding author.
Email addresses: nadzirin@uho.ac.id (Nur)*, hijriani@gmail.com (hijriani)
DOI: 10.15294/sji.v11i3.11605

Apart from DDoS and malware hacking, O.J.S. is also at threat of web defacement attacks in which a hacker or Attacker changes or modifications the appearance of the front page area. The goal of this category is not just to break the regular operation of a website but sometimes sinfully publish false or political materials which will destroy further good reputation and credibility for a publisher on such a platform. [8], [9] Attacks on O.J.S. repeatedly affect illegal businesses like online gambling promotions; specifically, this is the case. Network defacement attacks aim to replace or otherwise break their look with unwanted messages and content for O.J.S. These defacement attacks can result in significant financial and data losses and political or economic consequences. Different detection tools and tactics are in place to detect these web defacement attacks to minimize their impact while ensuring the website's overall security. [10], It may not be evident that such breaches have occurred until a journal site is compromised. Indicators of tampering on O.J.S. landing pages are broken or missing content, strange characters, and empty page PHP errors. Disruptions or attacks in an online journal by visitors may be the reason for a negative impression of the site's security and emergence if this method is used to identify publisher possibilities. This perception can mirror the credibility and reputation of the publications hosted on the platform. [11], These attacks are generally performed by actors trying to distribute propaganda or illegal advertisements, which will degrade the reputation and credibility of academic sites. The attacks observed on O.J.S. platforms further show that more security solutions related to content monitoring and system hardening are needed to prevent such attempts. Such a defense combines the reactive approach of detecting and responding to attacks while being proactive by increasing system configurations so that possible hacks do not occur again, thus keeping any academic content material intact.

Open Journal System (O.J.S.) is used globally to simplify the process of scholarly publishing. Hackers can attack unattended O.J.S. installations, thus affecting performance. When we examine the O.J.S. system, we look for weak points where hackers can sneak in through SQL attacks or by obtaining passwords. The main factors to consider in this evaluation are I.P. addresses and open ports. Fixing these weak points requires a complete security plan to keep O.J.S. safe from online dangers [12]. When someone messes up with an online gaming website, it can mess things up by introducing bad stuff or changes that shouldn't be there. These attacks often exploit vulnerabilities in web systems to embed harmful scripts that redirect visitors to illegal gambling sites. Such breaches can lead to data loss or corruption within the O.J.S. system and frequently result in complaints from authors to journal administrators regarding the compromised platform. Addressing these threats requires robust security measures and proactive monitoring to protect the integrity of the system and the data it manages [13]. Addressing these attacks requires careful user activity monitoring and additional safeguards to prevent compromise and unauthorized modification of O.J.S. systems.

Previous studies on network security issues examined vulnerabilities, port scanning, and system audit captures on the O.J.S. system [13]. For example, a survey conducted by many studies successfully found several SQL injections and password leaks through firewalls, also emphasizing the need to conduct security audits to protect the integrity of O.J.S. data [12]. However, no study has specifically analyzed the security mechanisms implemented on cPanel used in O.J.S. management. Therefore, this investigation aims to determine how attacks on cPanel affect O.J.S. and create a way that allows proactive monitoring techniques using the features available in cPanel to protect the O.J.S. system from various advanced cyber threats.

Analyzing cPanel server logs is also performed to detect suspicious activity and attack patterns. Log analysis involves gathering information from log files containing records of events within a computer system. A primary application of log analysis is collecting crucial information regarding system security issues, which can help identify and potentially stop intruders targeting the system. However, many systems generate extensive log data at high frequencies, making the analysis challenging. Effective log management and advanced analytical tools are essential for parsing this data to identify potential threats and enhance overall system security [14], log analysis can identify attack patterns undetected by automated tools and provide insight into protecting systems from more sophisticated threats.

## METHODS

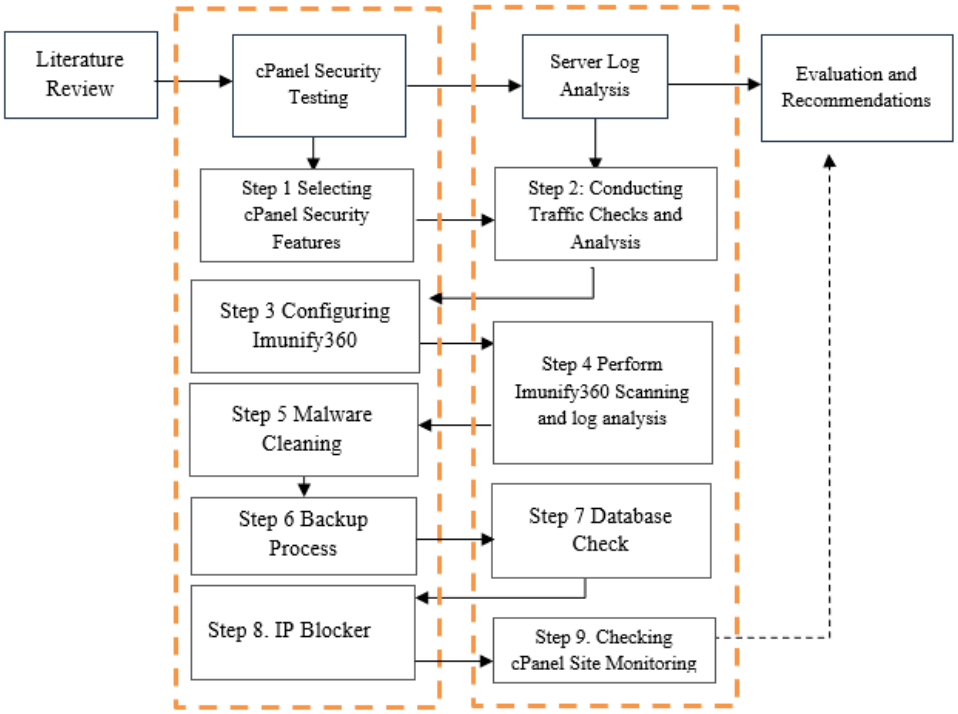


Figure 1. Stages of cPanel security system research

As shown in Figure 1, the research stage starts from a literature study to find out some of the problems of the O.J.S. security system and the vulnerability of DDoS and Malware attacks, then conducting security system testing by selecting security features and tools that are in accordance with the needs, for example, the selection of Imunify360 is done because of the importance of conducting automatic scans periodically, followed by analyzing and checking traffic to find out if there are any unusual visits if found, Imunfi360 scanning and malware cleaning are carried out, the next stage is to back up the system in real-time by cPanel tools, to ensure that there is no infiltration of the database, it is necessary to check the database and if an intruder is found, the IP Blocker process will be carried out, and the final stage is checking through Site Monitoring cPanel to find out the stability of the O.J.S. server, from the entire process, the final stage provides an evaluation and recommendations for the testing process and analysis of the security system that has been carried out.

### Literature review

This research method begins with a literature review to understand the security vulnerabilities faced by platforms like Open Journal Systems (O.J.S.) and the available protection tools and techniques. This phase includes references from previous studies, such as the work by Guntoro et al., which assessed the Open Journal Systems (O.J.S.) security at Universitas Lancang Kuning using I.S.S.A.F. and O.W.A.S.P. methods [13]. The I.S.S.A.F. and O.W.A.S.P. testing results indicate that the O.J.S. system at Universitas Lancang Kuning is secure and not vulnerable to external breaches. However, despite the O.J.S. at Universitas Lancang Kuning being deemed safe, there remains the possibility of attacks originating from within the system [13]. Additionally, research by Riadi et al. analyzed the security of Open Journal Systems websites and recommended updating to the latest version released by O.J.S. Public Knowledge [12]. This literature review provides a theoretical foundation and understanding of the specific security challenges faced by O.J.S. and hosting systems such as cPanel [12]. The literature review focuses on the security of cPanel, Open Journal Systems (O.J.S.), DDoS attacks, malware, web defacement, and online gambling slot attacks. This literature review aims to understand existing vulnerabilities and the mitigation efforts undertaken in similar contexts.

In cPanel, there are many security features. Still, in this study, there are several features used that are adjusted to the needs, such as Imunify360, which is a server security package consisting of several main

security components, such as antivirus, firewall, and PHP Security Layer, IP Blocker feature: preventing access to the website via I.P. address [15], then the Traffic Check feature to find out unusual visits, the JetBackup feature to perform the backup process in real-time [5]. HTTPS with SSL is used for protocol security and as a secure connection [16], and the Site Monitoring feature cPanel is a feature that allows cPanel users to monitor the website automatically and optimize the process to prevent malware attacks [17].

**cPanel security testing**

After the literature review, we begin particularly with some aspects of security testing-cPanel studies in this study. Several cPanel features and tools like Imunify360, SSL, IP Blocker Site Quality Monitoring, and Awstats JetBackup are tried out at this stage to examine how well they secure O.J.S. against threats such as malware DDoS attacks. Each one of those tests may also be hand-done, looking at each web file to ensure full security coverage (15); with Imunify360's protection technology, spam, and viruses are kept under control over data privacy [18]. This process involves setting up and observing assigned security tools and tracking the record of each test to determine if cPanel can manage an eventual attack. This data allows us to see the types of protection cPanel does well and where some areas could use improvement. It can be one of the standalone processes followed by other steps that have to be undergone, including (1) Configuring and monitoring cPanel's security features. (2) Tools used, evaluation of the effectiveness of offenses (3) Overseeing the results of tests

**Analysis log server**

The final stage includes analysis of Server Logs (for detection of unusual activity), Attack Patterns, Measurement & Checking Testing Log Analysis results, and Data Anomaly Detection based on the server [19]. The log data is tracked from the cPanel server to discover an attack pattern and vulnerabilities. Combining both firewall and server log analysis can increase the security of web networks against distributed denial-of-service attacks [20]; hence, vulnerabilities frequently compromised by hackers include brute force attempts or hacking into the system as a quick way out of attacking every administrator username/passwords one after another (much-known method); please refer to [17]. Each of them will be analyzed in great detail, and all test results will be taken into account before system administrators can improve the security around it, including mitigation steps and suggested configuration. The recommendations are intended to help protect existing O.J.S. installations by offering specific guidance for administrators who wish to secure their academic publishing platform. Collect log data from the server, Analyze trends and suspicious activity, and prepare findings and recommendations.

**Evaluation and recommendations**

Based on the testing and log analysis results, practical recommendations are being developed for system administrators. Recommendations will cover security settings, including reports and mitigation steps to improve the O.J.S. The key takeaways are restricting access grants, implementing security tools like Imunify360, and applying updates for both software & configurations. Administrators are also highly encouraged to deploy stringent and ongoing log analysis protocols to monitor and identify unusual behavior. This is to secure the O.J.S. platform from possible attacks and ensure that the scientific publications hosted will retain their importance.

Table 1. Types of research data

| Data Type | Description | Data Source |
|---|---|---|
| Literature Data | Security study references, DDoS threats, malware, defacement | Journal articles, study reports |
| Testing Data | Results of cPanel security feature testing | Configuration results and tools |
| Server Log Data | Server activity, attack patterns | cPanel server logs |
| Evaluation Data | Security effectiveness assessment and recommendations | Testing and analysis results |
| Recommendation Data | Guidelines and mitigation steps | Recommendation documents |

Table 1, organized by type, explicitly states the types of data being controlled in this study. Literature Data & References: These were collected from security studies and included references on DDoS threats, malware, defacement, etc., extracted from academic research articles or study reports. "Testing Data:" Testing data contains results of tests on cPanel security features undertaken with various configurations and tools. Via server log data (Entries for all activity on the cPanel servers, utilizing software security tools to monitor attacks). Evaluation Data: Represents a synthesis of evaluations about the operationalization of security and associated recommendations, as determined from testing and analysis. Recommendation Data: Document the recommended steps to ensure better system security.

## RESULTS AND DISCUSSIONS

Literature analysis shows Open Journal Systems (O.J.S.) software is vulnerable to cyber threats. The O.J.S. security evaluation at Lancang Kuning University was conducted by Guntoro et al. based on I.S.S.A.F. and O.W.A.S.P. entered into the system, which showed that this system has a high level of security, impossible to be penetrated by external attackers. However, this study also indicates that security risks can be internal, such as unauthorized access by a group of people in their system. This underlines that knowing a system is safe from external threats but monitoring internal access reduces violations or abuse [13].

In addition, the research of Riadi et al. O.J.S. recommends constantly updating to the most recent version released by the O.J.S. Public Knowledge Project so it is not vulnerable to new security bugs. This literature review thus once again emphasizes that while in some cases O.J.S. has been declared as secure, the real-world challenges of security remain and need continuous monitoring. This demonstrates the need for strict and immediate O.J.S. monitoring and regular updating of this software in an environment suitably endowed with discrete security features to supervise its operation-all so that data handled by the system remains secure. In addition, automated and real-time searches through search engines (e.g., Google) need to be conducted to identify DDoS attack vulnerabilities, malware/virus-related issues, as well as web defacement detections. A similar threat to O.J.S. sites is that online gambling slots being injected (a growing menace) into the sites poses a critical security issue [13].

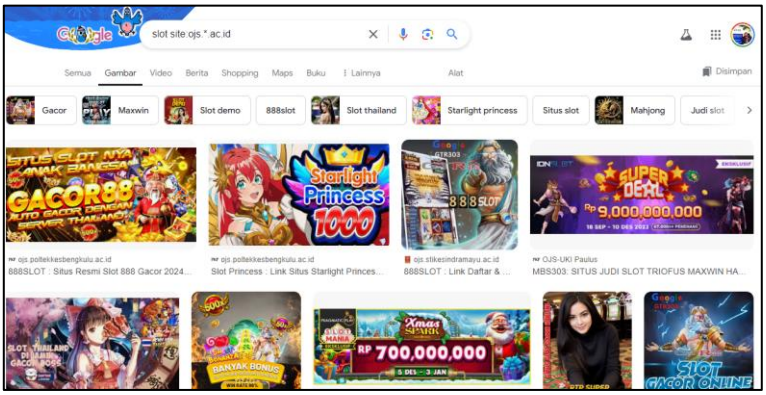


Figure 2. O.J.S. defacement web search results

Figure 2 shows the results of a search related to web defacement on the Open Journal Systems (O.J.S.) platform, showing a large number of O.J.S. sites that have been infiltrated with unauthorized content, such as online gambling promotions using the keyword "slot" in a search with the format "slot site:ojs.*.ac.id". This incident indicates that many O.J.S. sites in academic environments have experienced defacement attacks, where attackers have succeeded in replacing or inserting pages that promote illegal activities. This incident highlights weaknesses in the security configuration of several O.J.S. sites that allow infiltration by irresponsible parties. There needs to be increased monitoring and implementation of stricter security measures to prevent similar attacks in the future. This shows that the O.J.S. sites in the academic world are very susceptible to malware attacks.

### cPanel security testing results

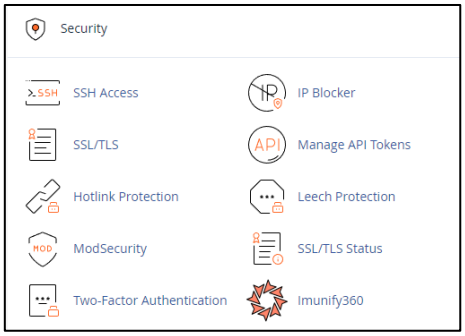


Figure 3. Security features in cPanel

***Step 1 selecting cPanel security features***

Figure 3 shows cPanel security features, including an IP blocker, preventing website access via an IP address. Leech Protection: detects unusual activity in directories that can only be accessed with a password, such as content hijacking or repeated login attempts. Hotlink Protection: prevents website content from being embedded in other websites S.S.H. Access: allows you to connect to the server securely via the command line SSL/TLS: Allows you to manage keys, certificates, and requests cPanel also has the ModSecurity feature, which can be enabled or disabled for all domains or subdomains.

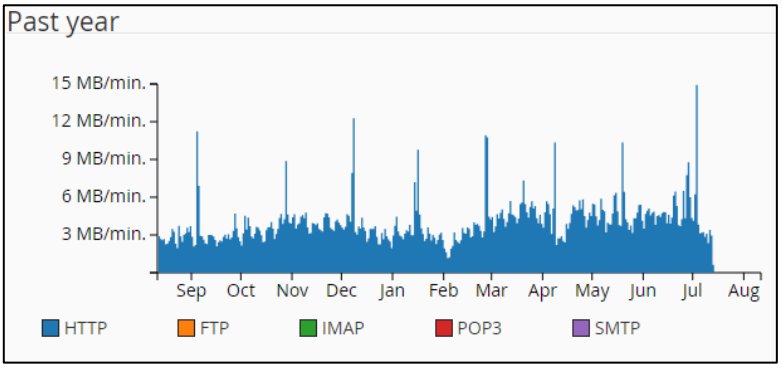


Figure 4. Suspicious bandwidth traffic is attacked by DDoS every month

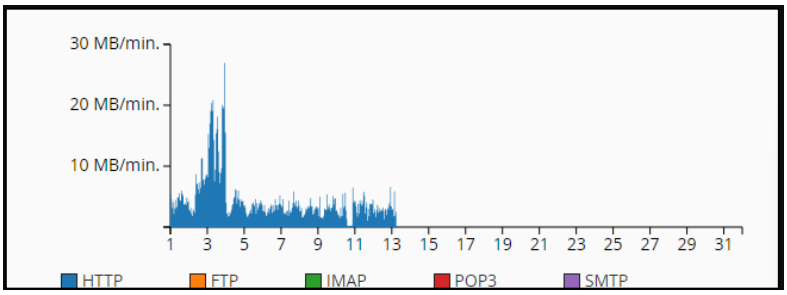


Figure 5. Traffic suddenly increases due to DDoS attacks

***Step 2 performing a traffic check***

DDoS attacks with a rapid increase in visits to the O.J.S. website are shown in Figures 4 and 5 of the site visit pattern [21]. The decisions made by this analysis will help further efforts to build the website. Distributed Denial of Service (DDoS) attacks on the Open Journal Systems (O.J.S.) site can be identified through a sudden and unusual increase in website visits. This suspicious visit pattern was discovered through analysis of server log data; this pattern shows a significant increase in traffic to the O.J.S. site for no apparent reason. This analysis must allow administrators to identify DDoS attack patterns early and take necessary precautions. This analysis not only helps to deal with attacks taken based on this analysis not only helps in mitigating ongoing attacks but also provides useful insights for future efforts to develop and improve the security of the O.J.S. site; this is to ensure resilience and security against similar threats.

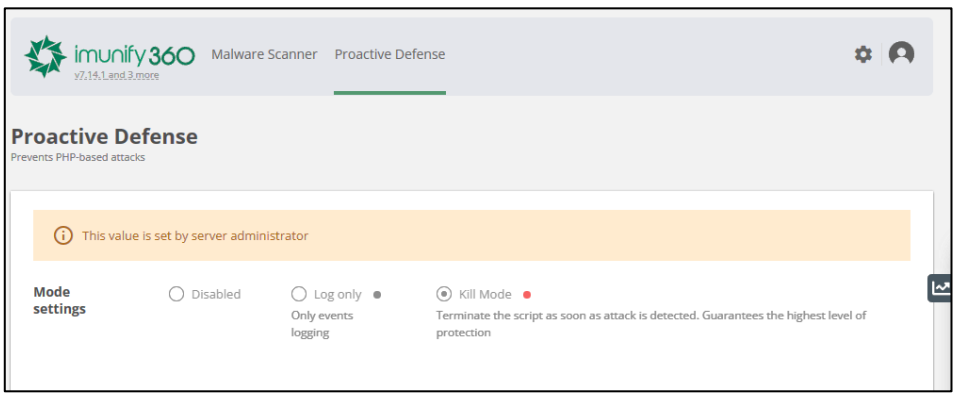


Figure 5. Configuration settings in Imunify360

***Step 3 configuring Imunify360***

In the testing phase, adjustments were made to the default settings on Open Journal Systems (O.J.S.), as shown in Figure 5, to enhance system security and ensure that protective mechanisms operate proactively. These changes included configuring cPanel settings, such as strengthening the firewall, updating SSL certificates to secure connections with web browsers [22], [23], and enabling additional security features like Imunify360 and IP Blocker. By implementing proactive defense in cPanel, the system becomes more resilient in detecting and preventing threats before they can cause harm, thus improving overall protection against cyberattacks and preserving the integrity and availability of data in O.J.S.

The results of these studies illustrate several weaknesses in default settings. For example, cPanel can be used by attackers, as seen in Figure 5. Those defaults need to be reset to ensure a better security system; vulnerabilities on the hosting platform have integrated with its operation, so specific cyber attacks will be exploited for malicious purposes. The use of security tools on cpanel has found quite reasonable results in malware removal and minimizing the impact of DDoS, with insight through Awstats data along with alleviated server speed access.

The research also indicated that obfuscating these methods through using security features in cPanel has helped reduce malware and mitigate some DDoS attacks. Interestingly, the information extracted by Awstats proves that these technologies effectively improve security per server request and site speed.

***Step 4 perform Imunify360 scanning and log analysis.***

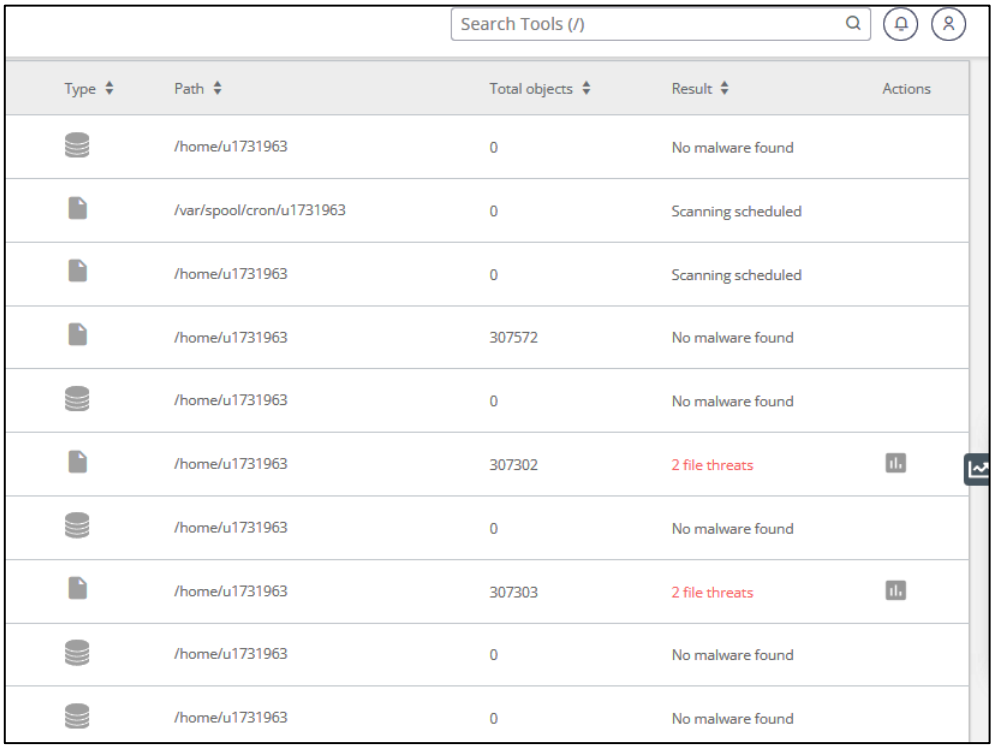


Figure 6. Checking results via Imunify360

From the scan conducted using Imunify360, Figures 6 and 7 show two examples of threats detected in files related to Open Journal Systems (O.J.S.). These threats were identified as potential malware or malicious scripts to infiltrate the system. After these threats were detected, cleaning was performed on the affected files to ensure that the malicious code was removed entirely. This step is essential to prevent further damage and ensure that the O.J.S. system remains secure and functioning correctly without disruption from cyber attacks.

***Step 5 malware cleaning***


Figure 7. Malware cleanup successful

This indicates that threats such as DDoS attacks and malware can be effectively mitigated by maximizing the use of Imunify360 on cPanel. Imunify360 antivirus is designed to enhance web server security by preventing harmful malware and providing comprehensive protection for the web server. The antivirus operates from all server aspects, including cPanel/W.H.M., and integrates with ModSecurity, which is typically available in cPanel.

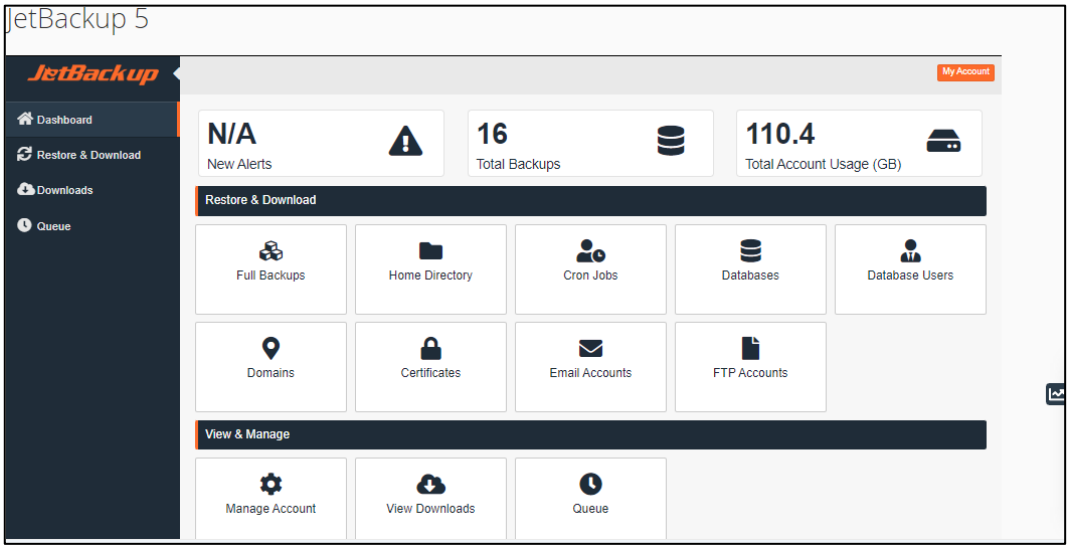


Figure 8. Jetbackup feature in cPanel

***Step 6 backup process***

In Figure 8, Perform regular backups for your important data to prevent damage [23]; system failures or user errors can significantly affect the integrity of files. Regular backups are essential to ensure data security and snapback if an incident occurs, so be careful. This ensures no mission-critical information is lost and avoids prolonged downtime. It is also an extra security net that enables a site to continue work as usual, even when some issues occur.

| ser_id | poster_ip | poster_name | poster_email | title | body |
|---|---|---|---|---|---|
| 833742 | 103.112.0.128 | Bernd Duarte | bernddduarte@hotmail.com | Titre : Naturopathe Ã  Laval : Guide par une Appro... | La dÃ©sintoxication naturelle du nos corps est une... |
| 832926 | 170.83.178.214 | Lashonda Bird | lashondabird@gmail.com | Soutien Aux Entreprises, Commerces Et Industries | Surtout, grÃ¢ce aux plugins, PolyWorks est adaptÃ©... |
| 827829 | 196.242.115.228 | Lina Lundy | linalundy@msn.com | Items De Scooter Pgo Big Max T | Le Yamaha Bws Sports activity possÃ¨de deux cÃ¢ble... |
| 828040 | 95.181.219.83 | Beth Kawamoto | bethkawamoto@gmail.com | Your Article Title | <img src="http://a.rgbimg.com/cache1ldsbr/users/s/... |
| 833278 | 196.18.225.186 | Muriel Driscoll | murieldriscoll@yahoo.com | Titre: Conseils pour un bon dÃ©mÃ©nagement et une ... | trois. Assurance Lorsque vous choisissez un dÃ©mÃ... |
| 834539 | 173.44.155.216 | Ian Sigmon | iansigmon@gmail.com | Bila Video Dewasa Nyasar di Grup | <p><span style="display:block;text-align:center;cl... |
| 833877 | 191.102.156.119 | Keenan Biaggini | keenan.biaggini@sbcglobal.net | Titre : MassothÃ©rapie Ã  Laval : DÃ©tendez-vous e... | Une des principales forces de la naturopathie est ... |
| Consol 42 | 45.12.113.5 | Jewell Cockle | jewellcockle@yahoo.com | Stunning Girls Filipino Site Philippines: The | <img src="https://res.cloudinary.com/ph-160/image/ |

Figure 9. Security flaw in the database in the comment feature in O.J.S.

***Step 7 database check***

Figure 9 shows the results of checking the database hackers managed to enter the server through the comment feature on Open Journal Systems (O.J.S.). This feature, which allows users to leave comments on journal articles, was found to have a security hole that hackers exploited to insert malicious code into the system. This access allowed them to gain further control over the server, potentially causing data corruption, service disruption, and increased risk of malware infection. This finding emphasizes the importance of strict supervision and increased security on interactive features on the O.J.S. platform.

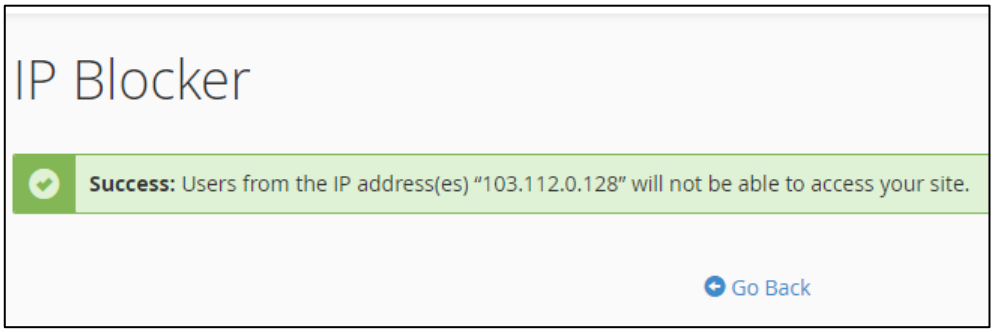


Figure 10. IP blocker in cPanel

***Step 8. IP blocker***

Cloud-based cPanel by feature: if you apply I.P. blocking via the so-called Cpanel based on cloud service Figure 10, your website will block their visitor‟s real or exact I.P. address, which will harm it [22]. Data backup is an essential part of keeping a balance between delivering services and maintainable system continuity, in this case, through backup stores that can restore data at any time when cyber attack damage occurs until during routine operations such as operating failures concerning websites which we turn off hosting intentionally access if maybe because there was human fault.

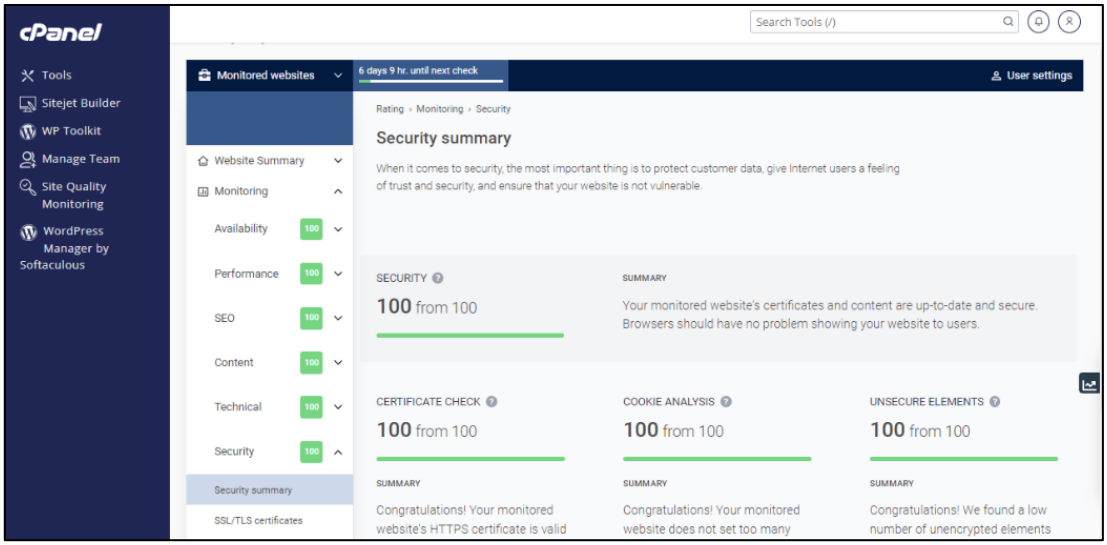

Figure 11. Site quality monitoring feature in cPanel

***Step 9. checking cPanel site monitoring***

From Figure 11, The Site Quality Monitoring feature in cPanel is crucial in overseeing the security of Open Journal Systems (O.J.S.) websites. By monitoring site activity in real time, this feature can detect suspicious changes, such as defacement attempts or other unauthorized activities that could threaten the site's integrity. Site Quality Monitoring provides detailed reports on the site's condition and performance, allowing administrators to address potential threats before they escalate into serious issues promptly. Thus, this feature is an essential tool in maintaining the security and stability of O.J.S.

**Evaluation and recommendations**

This is the final stage of research by analyzing all tests and results and providing conclusions through the following research results table:

Table 2. Recapitulation of security analysis results

| Type of Data | Description | Source | Results |
|---|---|---|---|
| Literature Data | References on security studies, DDoS threats, malware, defacement | Journal articles, research reports | Confirmed from research findings |
| Testing Data | Results of security feature testing on cPanel | Configuration results | Successfully conducted tests with cPanel security tools |
| Server Log Data | Server activity, attack patterns | cPanel server logs | Log data shows DDoS and malware attacked the O.J.S. system |
| Evaluation Data | Assessment of security effectiveness and recommendations | Testing and analysis results | Successfully cleaned malware by deleting it and monitoring site quality |
| Recommendation Data | Guidelines and mitigation steps | Recommendation documents | Implemented configuration changes, periodic traffic checks, and data backups |

Table 2 is the result of research based on the security analysis conducted, where from the literature data collected, it was confirmed that there have been many security threats in the publication of scientific journals through the O.J.S. system. Furthermore, the results of testing the cPanel security features have successfully conducted log data testing, showing that DDoS and malware attacked the O.J.S. system. Thus, malware cleaning is carried out by deleting malware and monitoring site quality, and finally, by periodically changing the configuration and web traffic and performing data backups; the steps above are essential to avoiding attacks and securing the O.J.S. system.

This study combines cPanel's various security features and tools into an in-depth approach to analyze and improve its protection. The study provides practical guidance to help system administrators strengthen security configurations and implement effective solutions to protect O.J.S. from cyberattacks. This exercise advances cPanel security knowledge and offers essential and practical steps to improve server security with O.J.S. publishing. Additionally, in the case of the web, HTTPS and SSL ensure that client-server communications are not only protected from man-in-the-middle attacks but also impenetrable. Addressing

SQL injection attacks has proven to reduce vulnerability levels [16], The author recommends that when choosing a hosting provider, attention should be paid to the security features offered and ensure that the server uses the latest technology [24], it is also advisable to incorporate an intermediary service, such as Cloudflare [25], [26] o further enhance the security between users and the server. Given technological advancements, web security, especially for O.J.S., has become increasingly critical. As cyber threats become more complex and sophisticated, attackers can exploit various system vulnerabilities to gain unauthorized access. Additionally, cyber attackers often operate internationally, making legal action challenging due to the global nature of cyber threats [27].

## CONCLUSION

The conclusions of this study indicate that enhancing security for Open Journal Systems (O.J.S.) hosted on cPanel is crucial for mitigating cybersecurity threats such as DDoS attacks and malware. The research reveals that default cPanel settings are insufficient to protect O.J.S.; however, implementing additional security features significantly improves protection. The impact of this study is the provision of practical guidelines for system administrators to implement more effective security measures, ultimately enhancing O.J.S.'s resilience against increasingly sophisticated cyber threats. Furthermore, the study highlights the necessity of regular monitoring and log analysis to detect suspicious activity and potential attacks. These findings offer a comprehensive and integrated approach for improving O.J.S. security on cPanel, identifying vulnerabilities, and providing concrete solutions to safeguard the platform from evolving cyber threats. By applying the recommended measures, administrators can proactively maintain the integrity and availability of data on O.J.S., ensuring the continued operational stability of the Open Journal System platform.

## REFERENCES


[1] A. Singh and B. B. Gupta, "Distributed Denial-of-Service (DDoS) Attacks and Defense Mechanisms in Various Web- Enabled Computing Platforms: Issues, Challenges, and Future Research Directions," *Int. J. Semant. Web Inf. Syst.*, vol. 18, no. 1, pp. 1–43, 2022, doi: 10.4018/IJSWIS.297143.

[2] M. Fadli Mutaqin and D. Ferdiansyah, "Identifikasi Kerentanan Terhadap Serangan Slot Backdoor Pada Website di Indonesia Dengan Menggunakan Metode OSINT," *J. Pas. Inform.*, vol. 1, no. 2, pp. 2986–5360, 2022, doi: 10.29322/IJSRP.X.X.2018.pXXXX.

[3] Y. Yuliadi, F. Hamdani, Y. B. Fitriana, and N. Oper, "Analisis Keamanan Website Terhadap Serangan DDOS Menggunakan Metode National Institute of Standards and Technology (NIST)," KLIK: Kajian Ilmiah Informatika dan Komputer, vol. 3, no. 6, pp.," *KLIK Kaji. Ilm. Inform. dan Komput.*, vol. 3, no. 6, pp. 1296–1302, 2023.

[4] T. Safitrah, A. B. G. Sinaga, M. Alghifari, and S. N. Neyman, "Pengaruh Serangan Slow HTTP DoS terhadap Layanan Web: Studi Eksperimental dengan Slowhttptest," *J. Technol. Syst. Inf.*, vol. 1, no. 4, p. 11, 2024, doi: 10.47134/jtsi.v1i4.2663.

[5] A. Zulfikri, F. P. E. Putra, M. A. Huda, H. Hasbullah, M. Mahendra, and M. Surur, "Analisis Keamanan Jaringan Dari Serangan Malware Menggunakan Filtering Firewall Dengan Port Blocking," *Digit. Transform. Technol.*, vol. 3, no. 2, pp. 857–863, 2023, doi: 10.47709/digitech.v3i2.3379.

[6] M. N. Abdiansyah, *Manajemen Hosting Berbasis WHM/cPanel*. Excellent Publishing, 2018.

[7] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," *Electron.*, vol. 12, no. 6, 2023, doi: 10.3390/electronics12061333.

[8] B. B. Aji, "Tindakan Kejahatan Cyber Crime Dalam Bentuk Deface Website," *Cyber Secur. dan Forensik Digit.*, vol. 6, no. 1, pp. 25–29, 2023, doi: 10.14421/csecurity.2023.6.1.4049.

[9] J. Desmon, S. Hidayatulloh, and Y. Jumaryadi, "Systematic Literature Review: Serangan Deface Website Sebagai Bentuk Kejahatan Siber," *Just IT J. Sist. Informasi, Teknol. Inf. dan Komput.*, vol. 14, no. 2, pp. 80–149, 2024, [Online]. Available: https://jurnal.umj.ac.id/index.php/just-it/index

[10] M. Albalawi, R. Aloufi, N. Alamrani, N. Albalawi, A. Aljaedi, and A. R. Alharbi, "Website Defacement Detection and Monitoring Methods: A Review," *Electron.*, vol. 11, no. 21, 2022, doi: 10.3390/electronics11213573.

[11] L. Verma, "Ojs security analysis: Issues, reasons, and possible solutions," *DESIDOC J. Libr. Inf. Technol.*, vol. 41, no. 5, pp. 391–396, 2021, doi: 10.14429/djlit.41.5.15975.

[12] 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,

2020, doi: 10.25126/jtiik.2020701928.
[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 (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 5, no. 1, p. 45, 2020, doi: 10.29100/jipi.v5i1.1565.
[14] J. Svacina *et al.*, "On Vulnerability and Security Log analysis: A Systematic Literature Review on Recent Trends," *ACM Int. Conf. Proceeding Ser.*, no. January 2021, pp. 175–180, 2020, doi: 10.1145/3400286.3418261.
[15] R. R. Yusuf and T. N. Suharsono, "PENGUJIAN KEAMANAN DENGAN METODE OWASP TOP 10 PADA WEBSITE EFORM HELPDESK," *Pros. Semin. Sos. Polit. Bisnis, Akuntansi, dan Tek.*, pp. 402–413, 2023.
[16] F. Wibowo, H. H. Nuha, and S. Wibowo, "Network Security Analysis Using HTTPS with SSL on General Election Quick Count Website," *2020 IEEE Int. Conf. Commun. Networks Satell. Comnetsat 2020 - Proc.*, pp. 204–207, 2020, doi: 10.1109/Comnetsat50391.2020.9328940.
[17] R. P. Aji, "Analisis Log Serangan BruteForce Terhadap Web Server Nginx Pada Dasbor Sistem Pencatatan Log Teroptimasi Menggunakan Metode Investigasi Forensik," 2022.
[18] P. Memiah *et al.*, "Highlighting a Digital Platform to Assess Young People Needs: Reaching and Engaging Adolescents and Young Adults for Care Continuum in Health Project (REACH)," *Adolescents*, vol. 2, no. 2, pp. 150–163, 2022, doi: 10.3390/adolescents2020014.
[19] A. A. Ma'ali, Girinoto, M. N. Ghiffari, and R. B. Hadiprakoso, "Analisis Log Web Server dengan Pendekatan Algoritme K-Means Clustering dan Feature Importance," *Info Kripto*, vol. 16, no. 3, pp. 119–123, 2022, doi: 10.56706/ik.v16i3.60.
[20] A. Afifah Rodhiyatun Nisa, Ananditto Daffa Wijayanto, Arya Prabudi Jaya Priana, and A. Setiawan, "Analisis Log Server untuk mendeteksi Serang DDoS pada Keamaan Jaringan di Website," *J. Internet Softw. Eng.*, vol. 1, no. 3, p. 17, 2024, doi: 10.47134/pjise.v1i3.2612.
[21] W. Wagito and D. Librado, "Analisis Data Akses Situs Berdasar Teknologi Log Server," *Technol. J. Ilm.*, vol. 13, no. 1, p. 22, 2022, doi: 10.31602/tji.v13i1.6113.
[22] A. Sirait and M. Siddik, "Implementation of Dynamic IP Blocking Techniques on the Tanungbalai City Library Website," *IJICS (International J. Informatics Comput. Sci.*, vol. 5, no. 3, p. 344, 2021, doi: 10.30865/ijics.v5i3.3452.
[23] A. M. Ujung, M. Irwan, and P. Nasution, "Pentingnya Sistem Keamanan Database untuk melindungi data pribadi," *JISKA J. Sist. Inf. Dan Inform.*, vol. 1, no. 2, p. 44, 2023, [Online]. Available: http://jurnal.unidha.ac.id/index.php/jteksis
[24] M. Huda, *Bisnis Web Hosting: Teknologi Pendukung Untuk Menjalankan Usaha Web Hosting" dan diterbitkan oleh bisakimia pada tahun 2021*. bisakimia, 2021. [Online]. Available: https://books.google.co.id/books?id=-nslEAAAQBAJ
[25] S. E. Prasetyo, H. Haeruddin, and K. Ariesryo, "Website Security System from Denial of Service attacks, SQL Injection, Cross Site Scripting using Web Application Firewall," *Antivirus J. Ilm. Tek. Inform.*, vol. 18, no. 1, pp. 27–36, 2024, doi: 10.35457/antivirus.v18i1.3339.
[26] N. Mamuriyah, S. E. Prasetyo, and A. O. Sijabat, "Rancangan Sistem Keamanan Jaringan dari serangan DDoS Menggunakan Metode Pengujian Penetrasi," *J. Teknol. Dan Sist. Inf. Bisnis*, vol. 6, no. 1, pp. 162–167, 2024, doi: 10.47233/jteksis.v6i1.1124.
[27] E. Susanto, Lady Antira, K. Kevin, E. Stanzah, and A. A. Majid, "Manajemen Keamanan Cyber Di Era Digital," *J. Bus. Entrep.*, vol. 11, no. 1, p. 23, 2023, doi: 10.46273/jobe.v11i1.365.