https://doi.org/10.32815/jitika.v19i1.1070

Volume 19, Issue 1, 2025

Jurnal Ilmiah Teknologi Informasi Asia

Journal Website: https://jurnal.asia.ac.id/index.php/jitika

Article

Analyzing the effectiveness of Cloudflare, Docker and Nginx Proxy Manager in improving web security

Mochamad Yusuf Setiya Putra *, Arif Saivul Affandi

Universitas Merdeka Malang, Malang, 65146, Indonesia

***abstract*—Cybersecurity is becoming an increasingly important matter as technology develops and threats against web-based applications grow. This research aims to examine how well Cloudflare, Docker, and Nginx Proxy Manager work, both alone and together, when used as an extra security measure to improve web application safety against these various threats. The study employed a quantitative approach using a quasi-experimental method with a posttest-only control group design. In this research, the control group consisted of a system without any additional security layers; this served as the starting point for measuring the system's security level. The experimental groups were divided into three types: a system using only Cloudflare, a system using only Docker and Nginx Proxy Manager, and a system using a combination of all three technologies. Testing involved several kinds of attacks, such as DDoS, brute force attacks, XSS, and SQL injections, utilizing tools like Slowhttptest, Burp Suite, XSSer, and SQL Map. The test results were assessed using descriptive analysis for categorical data and statistical methods for numerical data, specifically applying the One Way Anova or Kruskal Wallis tests, along with post-hoc follow-up tests. The findings from the study demonstrate that the system using the combination of Cloudflare, Docker, and Nginx Proxy Manager offered the most effective safety, reducing the number of successful attacks by up to 52% for DDoS, 69% for brute force attacks, 75% for XSS, and 100% for SQL injection. These results show a notable improvement compared to a standard system or systems using these security technologies individually.**

***Keywords*—cloudflare; cybersecurity; docker; nginx proxy manager**

1. Introduction

Cybersecurity remains a critical matter given the rapid advancement of technology today. As internet and web-based technology use grows, criminal actions in the digital realm, commonly known as cybercrime, become more complicated and frequent (Wahib et al., 2022). Data from Indonesia's National Cyber and Crypto Agency (BSSN) indicates that in August 2024 alone, approximately 14,918,178 traffic anomalies occurred, suggesting potential cyberattack activity (Id-SIRTII/CC, 2024). Various cyberattacks that can threaten web applications, such as DDoS, brute force attacks, XSS, and SQL Injection, are increasingly common and can potentially harm many involved parties (Fortinet, 2024).

A Distributed Denial of Service, or DDoS, attack is a type of attack intended to overwhelm a server with numerous requests, possibly causing the server to fail (Firmansyah, 2021). A brute force attack is a cyberattack that attempts to solve a problem by trying many possible password combinations to find the correct one (Rahmah, 2023). Cross-site Scripting, or XSS, is a type of attack that is quite easy to execute because it can be done

* Corresponding author.
E-mail Address: yusufuyaimub87@gmail.com (M. Y. S. Putra)

Author E-mail(s): MYSP (yusufuyaimub87@gmail.com), ASA (fandi@unmer.ac.id),
Digital Object Identifier 10.32815/jitika.v19i1.1070
Manuscript submitted 22 November 2024; revised 11 December 2024; accepted 20 December 2024
ISSN: 2580-8397(O), 0852-730X(P).

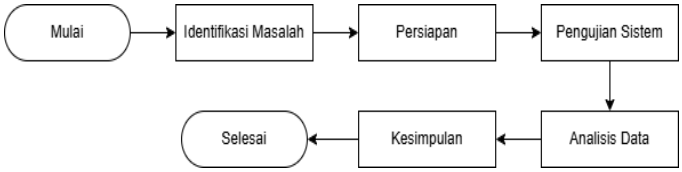

Fig. 1. Research flowchart

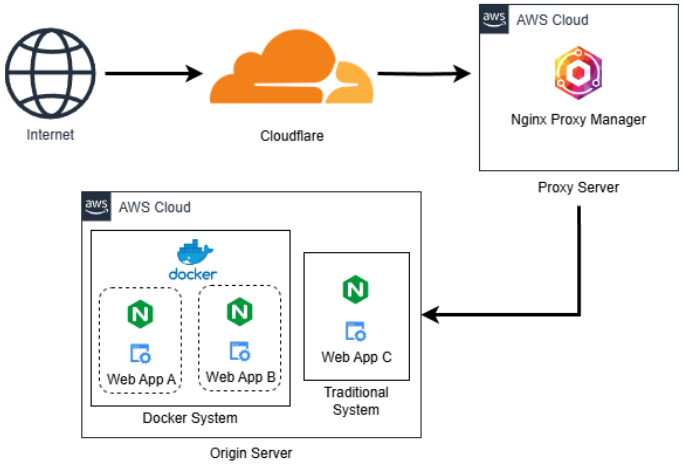

Fig. 2. System architecture topology

without complex tools, simply by entering harmful scripts into a form on a web application (Laleb, 2023). SQL Injection is an attack that exploits website security by sending various harmful SQL queries into the system. This allows attackers to perform actions like modifying, retrieving, or deleting databases without proper authorization (Prasetyo et al., 2024).

To improve the security of web applications against the various types of attacks mentioned above, security efforts must be considered from the application development stage. Developers can apply secure coding practices to enhance application security and prevent SQL Injection attacks by validating URLs, validating data inputs, using PDO to execute queries, and employing session tokenization (Harefa et al., 2021). However, these measures primarily offer protection at the application level and are often insufficient against more sophisticated and network-focused threats. Therefore, additional security strategies are necessary to provide more complete protection against increasingly complex threats, such as using a firewall as a network protection barrier against unauthorized access and guarding the network against suspicious traffic (Satriyawan & Susanto, 2023).

The use of Cloudflare, Docker, and Nginx Proxy Manager can add layers of security to web applications from the network perspective. Research by Kusuma (2022) explains that Cloudflare is a web application security service provider with various features, including a Web Application Firewall (WAF), Content Delivery Network (CDN), and DDoS mitigation, which can be used to improve the security of web applications configured within it. Another study by Ekaputra & Affandi (2023) indicates that using Docker and Nginx Proxy Manager as an additional layer can enhance the flexibility of more secure server settings through reverse proxy and container isolation.

While these studies show that Cloudflare, Docker, and Nginx Proxy Manager are frequently used in security contexts, there is limited research that thoroughly examines the effectiveness of combining these three technologies to address diverse cyber threats like Distributed Denial of Service (DDoS), brute force attempts, Cross-Site Scripting (XSS), and SQL Injection. Most analyses still concentrate on the use of each technology individually. This research offers a novel approach by integrating these three technologies as an additional network-side security layer for web applications. The analysis will not only assess the performance of each technology on its own but will also investigate whether their combined use is more effective than individual use in countering various tested cyber threats.

2. Methods

This research employs a quantitative approach with a quasi-experimental method. A quasi-experiment is a type of experimental study that aims to examine cause-and-effect relationships but does not involve full randomization of the control and experimental groups (Rustamana et al., 2024).. Furthermore, a post-test-only control group experimental design is applied, as it aligns with the research objective of measuring the impact of implementing additional security technology on system security levels after the treatment is administered (Rikatsih et al., 2020).

The study involves two types of groups: a group without intervention (the control group) and a group that receives the treatment (the experimental group). The control group comprises systems without supplementary security technology, serving as the baseline for measuring system security levels. The experimental group is divided into three scenarios: systems with Cloudflare, systems with Docker and Nginx Proxy Manager, and systems with a combination of Cloudflare, Docker, and Nginx Proxy Manager. The procedures carried out in this research encompass several stages, starting with the identification of the problem and progressing through data collection, analysis, and finally, the formulation of conclusions based on the findings. This systematic process allows for a thorough evaluation of the implemented security technologies on the security posture of the systems under investigation.

2.1. *Problem definition*

Fig. 1 illustrates the step-by-step procedure of this research endeavor. At the outset, the research will focus on clearly defining the challenges concerning the necessity for enhanced security in web applications to defend against a range of possible cyber intrusions. This definition will encompass a thorough understanding of the specific threats that can put applications at risk, alongside the various technological tools that will be employed in this study. The chosen technologies are Cloudflare, Docker, and Nginx Proxy Manager. Cloudflare will be utilized for its ability to filter malicious traffic and provide DDoS protection, adding a significant security shield. Docker will offer containerization, creating isolated environments for the application components, which limits the impact of a security breach within one part of the system. Nginx Proxy Manager will be implemented to securely manage incoming requests to the application, providing features such as SSL

Table 1. DDoS test results

Test No.	No Protection	Cloudflare	Docker & Nginx Proxy Manager	Combination
1	786	473	496	439
2	789	501	504	486
3	793	491	504	465
4	790	496	504	491
5	788	497	504	431
...	...	...	...	...
10	792	485	504	489
Attack Mitigation	21%	51%	50%	52%

termination and acting as a reverse proxy to conceal the application's internal structure, thereby adding another layer of defense. These technologies were specifically chosen for their capacity to contribute additional security measures to web applications through attack prevention, system segregation, and the controlled direction of network traffic.

2.2. Preparation

The test environment is set up by establishing the system's structure according to the test needs. This structural preparation occurs using Amazon Web Services' cloud platform, with a general layout shown in Fig. 2.

2.3. System security assessment

To evaluate system security, we conducted simulated cyberattacks, including DDoS, brute force attempts, XSS, and SQL Injection, on each test group. We performed each test ten times to ensure reliable data. For these simulations, we employed specific tools suited to each attack type: slowhttptest for DDoS, Burp Suite for brute force, XSSer for XSS, and SQLMap for SQL Injection. We recorded the number of successful intrusions for DDoS, brute force, and XSS attacks. For SQL Injection attempts, we noted whether the attack succeeded or failed.

2.4. Data anaysis

The data gathered from these tests underwent examination to find meaningful variations among the groups. We will apply statistical analysis to gain a clear and quantifiable understanding of how well Cloudflare, Docker, and Nginx Proxy Manager performed within each test group. By using statistical methods, we can interpret the test outcomes with greater precision, allowing us to judge the degree of notable differences in cyberattack resistance across the test groups.

We will use descriptive analysis for categorical data to summarize the overall attack outcomes. For numerical data from the tests, we will first check for normal distribution. If the data are normally distributed, we will use the One-Way ANOVA parametric test to assess the significance of differences between two or more groups. If the data do not follow a normal distribution, we will use the Kruskal-Wallis non-parametric test (Sugiyono, 2017). Should we find significant differences between groups, we will conduct further post-hoc tests to pinpoint the specific differences and identify which group demonstrates the greatest effectiveness in handling attacks.

2.5. Conclusion

The final part of this research will present conclusions drawn from the testing and analysis regarding the impact of technology on system security levels. This section will detail how effective each technology was, within its respective test group, at resisting and reducing the impact of simulated attacks. Furthermore, we will conclude whether these three technologies are more effective when used separately or together to enhance the security of web applications.

3. Results and discussion

The outcomes of tests conducted on each test group, employing simulated DDoS attacks, brute force attacks, XSS, and SQL Injection, will be presented and examined using both statistical and descriptive methods. This approach aims to provide a clearer understanding of how well the technologies in each test group work. This analysis includes a comparison of the test results from each scenario and an assessment of each technology's capacity to handle security threats, both on its own and when used together.

3.1. DDoS test results

Table 1 shows the number of successful attacks resulting from the DDoS tests performed on each test group. Each test involved an attack frequency of 1000 connections. The DDoS test results varied across the different test groups. A higher percentage of attack mitigation indicates a more secure system. The data collected is numerical and suitable for further statistical analysis. Therefore, a statistical analysis will be performed on the DDoS test results in the next stage to determine the significance of the findings for each group.

3.2. Brute force attack test results

The number of successful attacks from the brute force testing, which aimed to guess login credentials, is shown for each test group in Table 2. Each test group faced 40 password combination payloads per trial. The brute force attack test results indicate that some groups yielded consistent data. For example, the unprotected system and the system with Docker

Table 2. Brute force attack test results

Test No.	No Protection	Cloudflare	Docker & Nginx Proxy Manager	Combination
1	40	13	40	4
2	40	14	40	14
3	40	14	40	13
4	40	13	40	13
5	40	10	40	13
...	...	...	...	...
10	40	14	40	14
Attack Mitigation	0%	67%	0%	69%

Table 3. XSS test results

Test No.	No Protection	Cloudflare	Docker & Nginx Proxy Manager	Combination
1	1094	926	392	392
2	1095	914	392	392
3	897	926	392	282
4	921	924	277	312
5	905	926	318	302
...	...	...	...	...
10	1092	922	319	306
Attack Mitigation	20%	28%	74%	75%

Table 4. SQL injection test results

Test No.	No Protection	Cloudflare	Docker & Nginx Proxy Manager	Combination
1	Access Granted	Blocked Access	Access Granted	Blocked Access
2	Access Granted	Blocked Access	Access Granted	Blocked Access
3	Access Granted	Blocked Access	Access Granted	Blocked Access
4	Access Granted	Blocked Access	Access Granted	Blocked Access
5	Access Granted	Blocked Access	Access Granted	Blocked Access
...	...	...	...	...
10	Access Granted	Blocked Access	Access Granted	Blocked Access

and Nginx Proxy Manager each consistently showed 40 successful attacks. However, the differences among the groups can still be examined using statistical analysis to determine the importance of the variations between each test group. To provide a clearer picture, we can consider the percentage of successful attacks relative to the total number of attempts. Furthermore, analyzing the time taken for successful breaches in each group could offer additional insights into the effectiveness of different security measures.

3.3. XSS test results

Table 3 presents the number of successful attacks in the XSS testing conducted on each group. A total of 1291 malicious scripts were used as payloads. The results from the Cross-site Scripting (XSS) attack testing show varying values across the groups. A higher percentage of attack prevention would indicate a more effective system. Since the XSS test data is numerical, statistical analysis will be employed to assess the importance of the differences observed between the test groups. To add more context, we could examine the specific types of XSS vulnerabilities that were successfully exploited in each group. Moreover, evaluating the impact or severity of these successful attacks could provide a deeper understanding of the security posture of each system.

3.4. SQL injection test results

The success status of the SQL Injection attacks performed on each test group, using the same steps and configuration for each trial, is detailed in Table 4. The data from the SQL Injection attack testing is categorical in nature. Therefore, a descriptive analysis will be used to illustrate the general presentation of the

Table 5. Normality test

Attack	Group	Sig.
DDoS	No Protection	.814
	Cloudflare	.224
	Docker & Nginx Proxy Manager	.000
	Combination	.039
Brute Force Attack	No Protection	.
	Cloudflare	.000
	Docker & Nginx Proxy Manager Combination	. .000
XSS	No Protection	.000
	Cloudflare	.002
	Docker & Nginx Proxy Manager	.045
	Combination	.013
Attack	Group	Sig.
DDoS	No Protection	.814

Table 6. Kruskal-Wallis DDoS test

	Successful Attack
Kruskal-Wallis H	33.270
Df	3
Asymp. Sig	.000

test results. To elaborate, we can present the frequency of successful and unsuccessful attacks for each group. Additionally, detailing the specific SQL injection techniques that proved successful against certain groups could offer valuable information about the vulnerabilities present.

3.5. Normality test results

The security testing results will next undergo analysis to find if notable differences exist among the test groups. To understand the shape of the data distribution for the number of successful attacks in DDoS, brute force, and XSS attack types (which are numerical data), a normality test will first be conducted using the Shapiro-Wilk method. This method is appropriate because the data count for each group is less than 40 (Haryono et al., 2023). The results of this normality test produced significance values as shown in Table 5.

The normality test results indicate that several groups have significance values below 0.05. This value suggests that these groups do not meet the assumption of normality. Furthermore, the brute force attack type shows a significance value represented only by "." because the testing yielded constant data. This indicates that the data had no variation at all and did not meet the normality assumption. Because some groups did not meet the normality assumption for each attack type, a non-parametric Kruskal-Wallis test will be used to maintain the accuracy of the analysis.

3.6. Significance analysis of successful DDoS attack attempts

The DDoS testing results, which consist of the number of successful intrusions into the system, will be examined using the Kruskal-Wallis test to determine the significance of the average values across the groups. This testing produced the Kruskal-Wallis statistical table presented as Table 6.

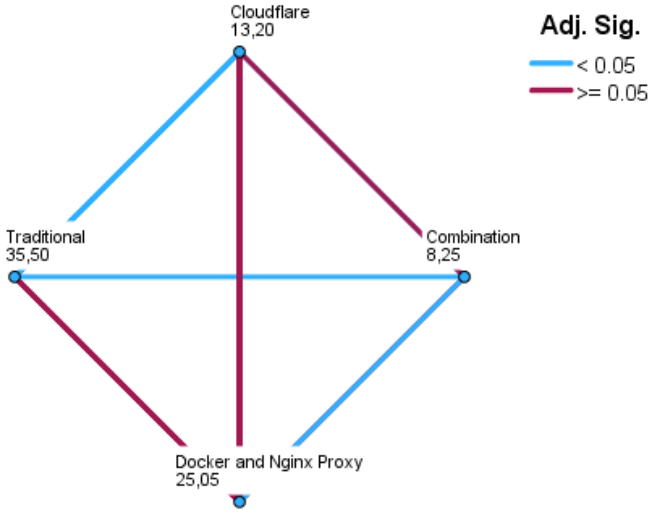

Fig. 3. DDoS pairwise comparison chart

Significance can be observed in the Asymp. Sig. value from the Kruskal-Wallis statistical test, which shows a value of 0.000, lower than 0.05. Therefore, the findings suggest a notable difference in the average number of successful attacks among the four test groups. Given this significant difference between the test groups, a post-hoc test will be performed as the next step to specifically analyze which groups have notable differences from one another. The results of this further analysis are as follows.

Based on the graph in Fig. 3, the combined system group shows the lowest average value compared to the other groups. Although this value is the lowest among all test groups, there was no statistically notable difference compared to the system group using only Cloudflare. This suggests that the system combining Cloudflare, Docker, and Nginx Proxy Manager is the most effective against DDoS attacks, even though its effectiveness is statistically similar to the system group using only Cloudflare individually.

3.7. Significance analysis of successful brute force attack attempts

To understand if the average number of successful brute

Table 7. Kruskal-Wallis test results

	Successful Attack
Kruskal-Wallis H	34.366
Df	3
Asymp. Sig	.000

Table 8. XSS testing results

	Successful Attack
Kruskal-Wallis H	30.224
Df	3
Asymp. Sig	.000

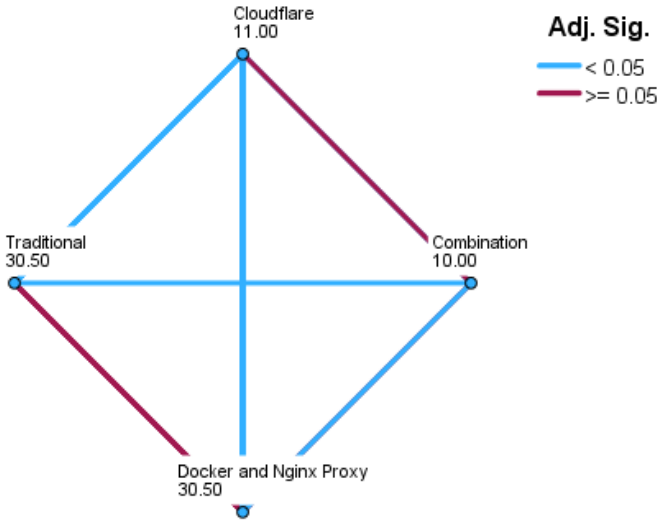

Fig. 4. Brute force attack pairwise comparison chart

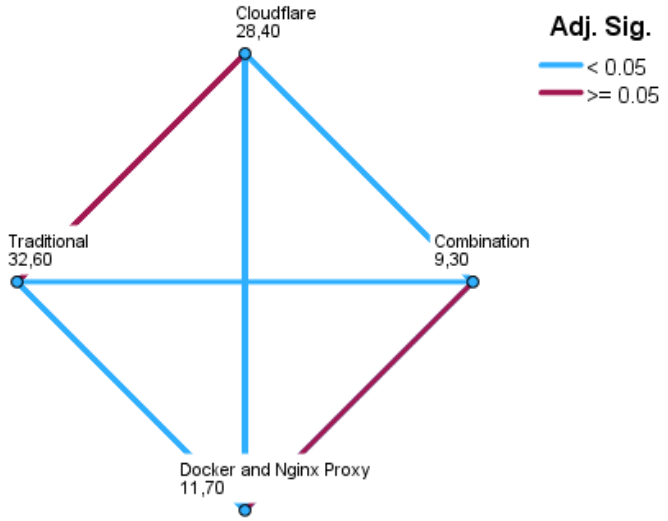

Fig. 5. XSS pairwise comparison chart

force attacks varied significantly across the different test groups, a difference test was conducted. The Kruskal-Wallis test results, presented in Table 7, provide the statistical details.

The results in Table 7 show an Asymp. Sig. value of 0.000, which is less than 0.05. This indicates a significant difference in the average values among the four test groups. To examine these average value differences between each specific pair of test groups more closely, a post-hoc test was performed, and the pairwise comparisons are shown in Fig. 4.

The graph in Fig. 4 reveals that the combined system group had the lowest average value compared to all other groups. However, this result was not statistically different from the group using only Cloudflare. This suggests that while the system combining Cloudflare, Docker, and Nginx Proxy Manager was the most effective against brute force attacks, its effectiveness was statistically similar to using Cloudflare alone.

3.8. Significance analysis of successful XSS attacks attempts

The Kruskal-Wallis test was also used to assess the significance of differences in the average number of successful Cross-site Scripting (XSS) attacks among the test groups. The statistical output of this test is provided in Table 8.

Table 8 shows an Asymp. Sig. value of 0.000, which is below 0.05. This signifies a notable difference in the average values among the tested groups. To further examine these significant differences, a post-hoc test was carried out, and the resulting pairwise comparisons are illustrated in Fig. 5.

Based on the post-hoc test results in Fig. 5, the combined system group exhibited the lowest average value among all test groups. Nevertheless, this outcome did not differ significantly from the groups using only Docker and Nginx Proxy Manager. This implies that the combined system of Cloudflare, Docker, and Nginx Proxy Manager was the most effective in handling Cross-site Scripting (XSS) attacks, although its effectiveness was statistically comparable to systems employing only Docker and Nginx Proxy Manager.

3.9. Significance analysis of successful SQL injection attacks attempts

The data gathered from the SQL Injection tests concerns the success status of attacks and is categorical in nature. Therefore, a descriptive analysis will be performed to illustrate the overall test outcomes. A general overview of these results can be seen in Table 9.

Table 9 indicates that the system group using only Cloudflare and the combined system group were completely secure against all attempted SQL Injection attacks. Conversely, the unprotected system group, as well as the Docker and Nginx Proxy Manager system groups, remained vulnerable in every SQL Injection attempt.

The complete protection offered by Cloudflare alone suggests its strong capabilities in mitigating SQL Injection threats. Similarly, the effectiveness of the combined approach underscores the value of layered security measures. The consistent vulnerability of unprotected systems highlights the critical need for security implementations. Furthermore, the susceptibility of systems utilizing Docker and Nginx Proxy Manager, even with their inherent functionalities, suggests that

Table 9. SQL injection success rate

Group	Successful Attack Attempts	Failed Attack Attempts	Success Rate
No Protection	10	0	100%
Cloudflare	0	10	0%
Docker & Nginx Proxy Manager	10	0	100%
Combination	0	10	0%

additional specific defenses against SQL Injection are necessary in these configurations. This analysis points to the varying degrees of resilience against this type of attack across different system setups.

4. Conclusion

Based on the tests and analysis conducted, the combination of Cloudflare, Docker, and Nginx Proxy Manager offered the most effective defense against the tested attacks when compared to using each technology separately. These technologies together provided optimal layered security. The weaknesses of one technology could be covered by the strengths of the others, and the security level of each technology could be enhanced by the presence of the others.

Cloudflare had a substantial positive effect against almost all types of attacks tested due to its security features. However, for XSS attacks, using Cloudflare alone was not very effective, showing little difference compared to traditional systems. Docker and Nginx Proxy Manager could add extra security layers in a layered security approach. Nevertheless, using these technologies individually was less effective without Cloudflare. In this study, however, Docker and Nginx Proxy Manager significantly improved system security against XSS attacks.

Future research should consider using the paid version of Cloudflare to access more advanced security features. Additionally, it is recommended to perform tests with a wider range of attack types and in environments with higher traffic to understand how well the technologies handle larger attack volumes. Furthermore, it might be beneficial to explore adding other security layer technologies, such as more sophisticated Web Application Firewalls (WAFs) or Intrusion Detection/Prevention Systems (IDS/IPS), to discover more optimal technology combinations for improving the security of web-based applications.

Data availability

All data produced or examined during this study are present in this paper.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Authors' contributions

All authors participated in the study design, writing, and manuscript revision. MYSP drafted and revised the manuscript, and ASA supervised the study. All authors have reviewed and approved the final manuscript.

References

Ekaputra, A. R., & Affandi, A. S. (2023). Pemanfaatan layanan cloud computing dan docker container untuk meningkatkan kinerja aplikasi web. *Journal of Information System and Application Development*, *1*(2), 138–147. https://doi.org/10.26905/jisad.v1i2.11084

Firmansyah, M. D. (2021). Analisa Keamanan Web Server Terhadap Serangan Distributed Denial of Service Menggunakan Modevasive. *Telcomatics*, *6*(1). https://doi.org/10.37253/telcomatics.v6i1.4990

Fortinet. (2024). *What Is A Cyber Attack?* . Fortinet. https://www.fortinet.com/uk/resources/cyberglossary/types-of-cyber-attacks

Harefa, J., Prajena, G., Alexander, A., Muhamad, A., Dewa, E. V. S., & Yuliandry, S. (2021). SEA WAF: The Prevention of SQL Injection Attacks on Web Applications. *Advances in Science, Technology and Engineering Systems Journal*, *6*(2), 405–411. https://doi.org/10.25046/aj060247

Haryono, E., Slamet, M., & Septian, D. (2023). *Statistika SPSS 28* (N. Rismawati, Ed.). Widina Bhakti Persada Bandung.

Id-SIRTII/CC. (2024). *Laporan Hasil Monitoring*. Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center. https://idsirtii.or.id/halaman/tentang/laporan-hasil-monitoring.html

Kusuma, G. H. A. (2022). Sistem Firewall untuk Pencegahan DDOS Attack di Masa Pandemi Covid-19. *Journal of Informatics and Advanced Computing (JIAC)*, *3*(1).

Laleb, I. (2023). Analisis Cross-Site Scripting (XSS) Injection – Reflected XSS And Stored XSS Mengggunakan Framework OWASP 10. *Jurnal Ilmiah Flash*, *8*(1), 36. https://doi.org/10.32511/flash.v8i1.952

Prasetyo, S. E., Haeruddin, H., & Ariesryo, K. (2024). Website Security System from Denial of Service attacks, SQL Injection, Cross Site Scripting using Web Application Firewall. *Antivirus : Jurnal Ilmiah Teknik Informatika*, *18*(1), 27–36. https://doi.org/10.35457/antivirus.v18i1.3339

Rikatsih, N., Andary, R. W., Shaleh, M., Hadiningrum, L. P., Irwandy, I., Prisusanti, R. D., Nggaba, M. E., Hadi, P., Sihombing, B., Setiawan, J., & Saloom, G. (2020). *Metodologi Penelitian di Berbagai Bidang*. Media Sains Indonesia.

Rustamana, A., Wahyuningsih, P., Azka, M. F., & Wahyu, P. (2024). Penelitian Metode Kuantitatif. *Sindoro: Cendikia Pendidikan*, *5*(6).

Rahmah, S. A. (2023). Efektifitas Penerapan Algoritma Brute Force dan Penyalahgunaannya Dalam Sistem Berbasis Web. *Journal of Computers and Digital Business*, *2*(3), 112–119. https://doi.org/10.56427/jcbd.v2i3.235

Satriyawan, H., & Susanto, D. S. (2023). Optimasi Keamanan Smart Grid Melalui Autentikasi Dua Lapis: Meningkatkan Efisiensi dan Privasi dalam Era Digital. *Jurnal RESTIKOM : Riset Teknik Informatika Dan Komputer*, *5*(3), 319–333. https://doi.org/10.52005/restikom.v5i3.254

Sugiyono, S. (2017). *Metode penelitian kuantitatif, kualitatif, dan R&D*. Alfabet.

Wahib, P., Narotama, A. T., Rijki, N. M., Sahrudin, S., Permana, F.,

Sagara, D., Azkhal, D. I., Anwar, M., & Juniawan, M. R. (2022). Sosialisasi Cyber Security Awareness untuk meningkatkan literasi digita. *Abdi Jurnal Publikasi*, *1*(2).

Photograph and biography of the authors (Mochamad Yusuf Setiya Putra and Arif Saivul Affandi) were not available at the time of publication.