Jurnal Informatika dan Rekayasa Perangkat Lunak ISSN 2656-2855
Vol. 8, No. 1, March 2026, Page. 176-184 e-ISSN 2685-5518

Analysis of False Positives in an OWASP-Based Web Application Firewall and their Impact on the Performance and Availability of Open Journal Systems (OJS)

Riki Agus Prastyo[1*], **Awang Andhyka[2], Achmad Mufliq**[3]
[1,2,3] Department of Information Systems, Nahdlatul Ulama Sidoarjo University
Email: [1]rikiagus382@email.com , [2]awang85.si@unusida.ac.id,
[3]Achmadmufliq.it@unusida.ac.id

Abstract

The implementation of a Web Application Firewall (WAF) based on the OWASP Core Rule Set (CRS) aims to enhance web application security; however, improper configuration may lead to false positives that adversely affect system performance and service availability. This study analyzes the impact of WAF false positives on Open Journal Systems (OJS) services deployed in a cloud environment using a server log analysis approach. The data were collected from web server error logs and ModSecurity audit logs that recorded the blocking of legitimate requests during the manuscript submission process due to inbound anomaly scores exceeding predefined security thresholds. The results indicate that WAF false positives caused service failures characterized by HTTP 403 responses, increased submission errors, and a measurable reduction in OJS service availability during the observation period. These findings demonstrate that anomaly-based detection mechanisms in OWASP CRS may misclassify normal application behavior as malicious activity. This study provides empirical evidence based on server logs regarding the impact of WAF false positives on cloud service reliability and offers insights for WAF policy tuning to achieve a balance between security and service availability.

Keywords*: Web Application Firewall, False Positive Detection, Server Log Analysis, Cloud Service Availability, Open Journal Systems*

INTRODUCTION

Technological developments *Cloud Computing* has driven digital transformation in various academic services, including the scientific journal management system. Service-based utilization *cloud* enable educational institutions to provide more flexible, scalable, and easily accessible services to users from a variety of locations (Reyes Narváez et al., 2025). One of the most widely used platforms in the management of scientific journals is *Open Journal Systems* (OJS), which supports the process of submitting manuscripts, reviewing, editorial management, and publishing articles online. However, the openness of access to OJS services through public networks also increases the risk of various cybersecurity threats("OWASP CRS | OWASP Foundation," n.d.).

Problems *False positive* WAF not only has an impact on security, but also affects the performance and availability of services (*Availability*) (Siwach and Mann, 2022). Service interruptions that occur due to blocking legitimate requests can lead to system malfunctions, increasing error rates (*Error Rate*), as well as lowering the reliability of service-based *cloud* (MajedA.Alowaidi and Sunil Kumar Sharma, 2025). This creates a dilemma between implementing strict security policies and the need for a stable and always available service to users

A number of previous studies have examined the effectiveness of WAF in detecting and preventing web application attacks. Other research shows that the analysis *Log server* can be leveraged to identify anomalous patterns and evaluate security incidents in the environment *cloud* (MajedA.Alowaidi and Sunil Kumar Sharma, 2025). In addition, several studies have also discussed the relationship between security mechanisms and service reliability, emphasizing that improper security policies can have an impact on declining *Availability* Information

Systems (Ank Shah et al., 2025). Research related to OJS generally focuses more on aspects of journal management, system adoption, and ease of use, while studies on the impact of security mechanisms on OJS operations are still relatively limited.

In recent years, analysis-based research *Log* is increasingly developing as an empirical approach to understanding the behavior of the system in real terms. Analysis *Log server* allows researchers to trace blocking events, service errors, and interactions between users and security systems chronologically. Nonetheless, the integration between the analysis *Log server*, evaluation *False positive* WAF, and its influence on the performance and availability of academic application services are still rarely studied comprehensively (Ott et al., 2021). This indicates the existence of *Research gap* relevant to further research.

Based on the research gap, this study focuses on the analysis of the impact of *false positive Web Application Firewall* on the performance and availability of *Open Journal Systems* services in the *cloud* environment. The approach used is *server log* analysis, which includes web server error logs and *WAF log audits*, to identify legitimate request blocking events as well as their implications for service reliability. This research is expected to be able to provide an empirical picture of how anomaly-based security policies affect the operational processes of scientific journal systems.

The purpose of this study is to identify false *positive patterns* that occur in WAF, analyze their impact on the performance and availability of OJS services, and provide recommendations for improving security policies. Thus, this research is expected to contribute to the development of more balanced information system security practices, which are able to maintain the level of security of web applications without sacrificing the reliability and availability of services in cloud-based scientific journal systems.

LITERATURE REVIEW

The use of cloud-based web applications in the management of scientific journals is driving adoption *Open Journal Systems* (OJS) as the main platform for academic publications. OJS supports the process of submitting manuscripts, managing editorials, and publishing online, but the open access of this system increases the risk of web application attacks (Riadi et al., 2020). Recent research shows that academic web applications are highly vulnerable to parameter exploitation, input injection, and abuse of the HTTP protocol if they are not equipped with adequate security mechanisms (Utama and Nurhadi, 2024).

One of the commonly applied security solutions is *Web Application Firewall* (WAF), which monitors and filters HTTP traffic before it reaches the application (Dawadi et al., 2023). Modern WAF generally adopts *OWASP Core Rule Set* (CRS) with the *anomaly-based detection*, i.e. a risk assessment mechanism based on the accumulation of anomalous scores from detected demand patterns (Scano et al., 2025). This approach has proven to be effective in detecting common attacks such as SQL Injection and Cross-Site Scripting, but highly dependent on the rule configuration and the score threshold applied (Floris et al., 2025)

Although it improves security, the anomaly-based approach has a drawback in the form of potential occurrence *False positive*, which is a condition when a user's legitimate request is blocked by the security system (Ravindran et al., 2025). Several studies in the last five years have shown that false positives can lead to service failures, increased *Error Rate*, as well as decreased availability (*Availability*) Web application (Díaz-Verdejo et al., 2022). In cloud-based services, this has a direct impact on system reliability and user experience, especially on applications that support key business processes such as OJS (Viradia et al., 2025).

To empirically evaluate the impact of false positives, server log analysis has become a widely used approach in recent research. The correlation between *the web server error log* and *the WAF audit log* allows for the identification of legitimate request blocking patterns as well as their association with service interruptions.

However, studies that specifically discuss the impact of false positive WAF on the performance and availability of OJS services are still limited. Therefore, log analysis-based research on cloud-based OJS environments is relevant to fill the research gap (Zhou et al., 2021).

METHOD

2.1 Research Stages

This study uses a log server-based descriptive-analytical approach to evaluate the impact of *false positive Web Application Firewall* on the performance and availability of *Open Journal Systems* (OJS) services in the *cloud environment*. The methodology is developed in stages and systematically so that the analysis process can describe the relationship between security policies, the occurrence of blocking legitimate requests, and their implications for service reliability.

Overall, the research stages consist of five main stages that are in succession, starting from problem identification to the preparation of recommendations. The flow of the research stages is shown in Figure 1.

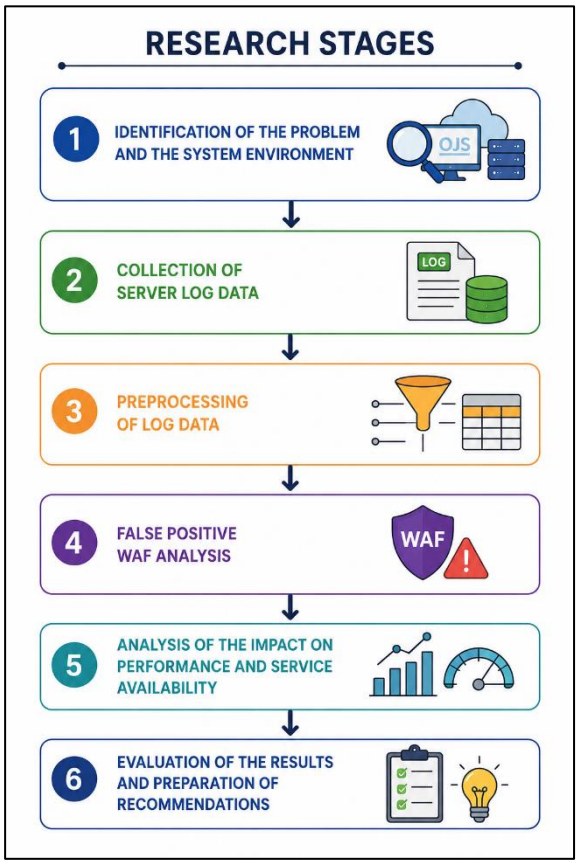

Figure 1. Research Stages

The first stage is the identification of the problem and the system environment. At this stage, observations were made of OJS services running on *cloud* infrastructure, including security mechanisms implemented using WAF based on *the OWASP Core Rule Set*. This stage aims to understand the context of the system, key service flows, as well as early indications of service outages experienced by users during the operational process.

The second stage is the collection of *server log data*. The research data was obtained from *web server error logs* and WAF *log audits* that recorded actual system activity. This log data includes information about the time of the event, the type of system response, and the blocking decisions made by the WAF. Data collection was carried out passively so that it did not affect the performance of OJS services during the observation period.

The third stage is the preprocessing of log data. At this stage, data filtering is carried out to eliminate irrelevant entries, data duplication, and uniformity of time formats. Furthermore, log data is classified based on the type of event, such as blocked legitimate requests and service error events. This pre-process aims to improve the quality of the data and facilitate the analysis process at the next stage.

The fourth stage is the false *positive* WAF analysis. The analysis is performed by identifying legitimate request blocking events triggered by anomaly-based detection mechanisms. The incident was then correlated with the normal activities of the OJS service to ensure that the blocking that occurred did not come from an actual attack, but rather a misclassification by the WAF.

The fifth stage is an analysis of the impact on performance and service availability. At this stage, *false positive events* are analyzed in relation to service interruptions, such as increased access errors and system malfunctions. The analysis focused on the frequency of events, system response, as well as indications of decreased service availability during the observation period.

The last stage is the evaluation of the results and the preparation of recommendations. The results of the analysis were evaluated to draw conclusions regarding the impact of *false positive* WAF on the reliability of OJS services. Based on these findings, recommendations for adjusting WAF policies and configurations are prepared to improve the balance between security and service availability in cloud-based scientific journal systems.

2.2 Data Collection Sources and Techniques

The data source in this study comes from secondary data in the form of *Log server* generated by the system during service operation *Open Journal Systems* (OJS) in the environment *cloud*. Log data was chosen because it represents the actual activity of the system and security mechanisms, thus allowing for empirical analysis of events *false positive Web Application Firewall*.

The type of log data used in this study consists of two main sources, namely *web server error logs* and *Web Application Firewall (WAF) log audits*. *Web server error logs* are used to identify service error events and system responses to user requests, while WAF *log audits* are used to analyze blocking decisions generated by *OWASP Core Rule Set-based security* mechanisms.

Data collection is carried out passively without intervening in the running system. This technique was chosen to ensure that the data obtained reflects the actual operational conditions and does not affect the performance of OJS services. Log data is collected over a specific observation time span that includes the normal activity of the user, specifically during the manuscript submission process.

To maintain the relevance of the data, only log entries related to request blocking events and service errors are further analyzed. The data collection process is carried out by copying and storing log files from the server to a separate storage media for analysis purposes.

Table 1. Research Data Sources

Data Log	Source	Main Information
Web Server Error Log	Server OJS	Time of occurrence, response code, service error
WAF Audit Log	Mod Security	Blocking decisions, anomaly scores, violation types

2.3 Log and Parameter Analysis Techniques

The data analysis technique in this study was carried out with a descriptive analysis approach to *Log server*. Analysis is focused on event identification *False positive* WAF and its relationship with OJS service disruptions. The analysis process is carried out in stages following the methodological flow described in Subchapter 2.1. The initial stage of analysis is the filtering and normalization of log data. The log data that has been collected is selected to eliminate irrelevant entries and is timed standardized to facilitate the correlation process between logs. Furthermore, the data is classified based on the type of event, such as legitimate requests blocked by WAF and service error events on the web side of the server.

Table 2. Service Availability Parameters

Yes	Parameters	Description
1	False Positive *Frequency*	Number of legitimate requests blocked
2	Error Response Codes	System response due to blocking
3	Error Rate	Service error rate
4	Availability Indication	Service interruptions during the observation period

The next stage is the identification of false *positive* events. The analysis parameters used are shown in Table 2. An event is categorized as *a false positive* if a legitimate user request is blocked by the WAF and is not indicated as a web application attack. This identification is done by comparing the user's activity pattern with the security rules that triggered the block.

After *false* positives are identified, an analysis of their impact on service performance and availability is carried out. Service availability parameters are used to assess the reliability level of the system during the observation period. The parameters analyzed in this study include the frequency of legitimate request blocking events, the number of service errors, and indications of decreased service availability. The results of the analysis of these parameters were used to evaluate the impact of *false positive* WAF on the reliability of OJS services. These findings are the basis for the preparation of recommendations for security policy adjustments to improve service availability without reducing the level of system protection.

RESULTS AND DISCUSSION

3.1 Analysis of the Scoring Mechanism

Based on the results of the log audit analysis shown in Figure 2, it is known that the rule protocol enforcement with 920451 ID is active in the initial phase of request processing (phase:1). This rule serves to detect the use of HTTP headers that are restricted by the OWASP

Core Rule Set (CRS) based WAF security policy. Rule 920451 has a critical severity, which indicates that violations of these rules are considered high risk by the security system. Although rule 920451 does not explicitly display numerical score values on individual log rows, the OWASP CRS internal mechanism still performs a risk assessment of detected requests.

This assessment is carried out through the mechanism of adding anomaly scores (anomaly scoring) by utilizing internal system variables. In rule 920451, the process is executed through the setvar command which adds the critical anomaly score value to the inbound anomaly score variable according to the system configuration. This setvar process does not print the score directly on the individual rule log, but rather accumulates the score values into a global score variable that will be evaluated in the next stage. The accumulation of global scores is the main component in the process of evaluating security decisions on WAF. After all the rules in the inspection phase are executed, the system will correlate the *collected inbound anomaly score* values . This value is then compared to the threshold that has been set in the *OWASP Core Rule Set* configuration. If the accumulated score reaches or exceeds that threshold, the blocking mechanism will be executed automatically. Thus, the blocking decision is not determined by a single rule separately, but by the result of the aggregation of scores from the previous inspection process. This mechanism is designed to increase the accuracy of detection, but under certain conditions it can trigger the occurrence of *false positives*.

Figure 2. WAF Score Assessment Mechanism

These findings suggest that the increase in anomaly scores on the system does not come from web application attacks such as SQL Injection or Cross-Site Scripting, but rather from *protocol enforcement* policies implemented by WAF.

Table 3. Summary of Anomaly Score Trigger Rule Characteristics

Parameters	Remarks
Rule ID	920451
Categories	Protocol Enforcement
Execution Phase	Phase 1 (Request Header Inspection)
Paranoia Level	Level 2
Severity	Critical
Evaluation Mechanism	Adding scores via *setvar*
Score Variables	Inbound Anomaly Score
Impact	Contribution to the accumulation of anomalous scores
Classification	False positive *triggers*

Therefore, rule 920451 can be categorized as the main trigger for false positives in the case of sending OJS manuscripts analyzed in this study. The trigger comes from a protocol enforcement mechanism that classifies legitimate request patterns as policy violations, triggering an increase in anomalous scores and leading to service blocks.

3.2 Score Evaluation and Blocking

After the detection process in the initial phase of request processing, the WAF system evaluates the anomalous scores that have been collected. This process aims to determine whether the received request can still be tolerated or should be blocked based on a predetermined threshold. The evaluation of the anomaly score is carried out in the correlation phase, which is represented in the audit log by rule ID 980170.

Based on the score correlation results shown in Figure 3, the system records the combined anomaly score value derived from the inbound component. The correlation results show that all parameters of web application attacks, such as SQL Injection (SQLi), Cross-Site Scripting (XSS), Local File Inclusion (LFI), and Remote Code Execution (RCE), are zero. This condition confirms that there is no indication of a web application attack on the analyzed request.

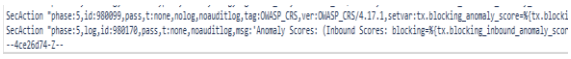

Figure 3. WAF Score Assessment Mechanism

The accumulated recorded anomaly scores are entirely due to the score contribution of the rule *Protocol Enforcement* in the previous phase. In other words, the resulting anomaly score is not the result of a combination of different types of attacks, but rather comes from one type of protocol policy violation. This reinforces the classification of events as *False positive*, where legitimate user activity is classified as a security breach.

This anomalous score correlation process is the basis for the WAF system in making blocking decisions. When the *combined anomaly score* reaches or exceeds the set threshold value, the system automatically executes a blocking mechanism on that request. Therefore, the score correlation stage has an important role in determining the impact of security policies on the performance and availability of OJS services.

Table 4. Correlation Results of Anomalous Scores Based on Log Audit

Parameters	Value
Blocking Inbound Score	5
Detection Inbound Score	5
SQL Injection Score	0
XSS Score	0
LFI Score	0
RFI Score	0
RCE Score	0
HTTP Violation Score	0
Combined Anomaly Score	5
Threshold	5
Evaluation Results	Request blocked (*denied*)
Classification of Occurrences	False Positive

These findings show that the scoring mechanism in WAF is highly dependent on the sensitivity of the rules applied, especially in the protocol enforcement category. This dependency has the potential to cause misclassification if the rules are not adjusted to the characteristics of the protected application. In the context of OJS, complex communication and data transmission patterns can trigger violations of protocol policies even though the activities carried out are normal. Therefore, the correlation results of this score indicate the need to evaluate the configuration of security rules in order to not only focus on the detection aspect, but also consider the context of application use. The policy adjustment is expected to be able to reduce the occurrence of false positives without reducing the effectiveness of the overall system protection.

3.3 The Impact of False Positives on OJS Services

The impact of implementing *Web Application Firewall* (WAF) with *an anomaly-based detection* mechanism is not only visible on the server side, but can also be observed directly at the application layer. In this study, the impact *of* false *positives was identified on the submission process* in the *Open Journal Systems* (OJS) system. When the user fills in the metadata and uploads the script, the system fails to process the request and cannot proceed to the next stage. This condition occurs because any HTTP request sent from the OJS interface must pass an inspection process by the WAF before being forwarded to the application. At this stage, WAF evaluates the headers, request methods, and data content submitted by the user. Although the activity performed is legitimate and compliant with the OJS workflow, certain request patterns are identified as anomalies by active security rules. As a result, the request is blocked and never reaches the application layer, so OJS is unable to process the data submitted by the user.

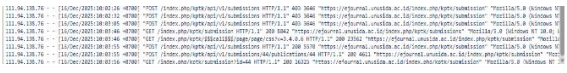

Figure 4. The Impact of HTTP 403 False Positive on OJS Services.

As shown in Figure 4, the OJS application displays error messages to the user in the form of a process failure notification and instructions to reload the page. This message appears in response to an HTTP request that was rejected by a server with an HTTP status code of 403 (Forbidden). From the user interface side, this error appears to be an application glitch, as OJS does not provide technical information regarding the cause of the blocking.

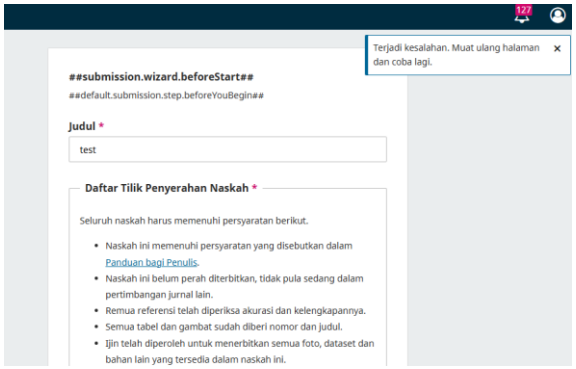

Figure 5. The Impact of False Positive Manuscript Submission on OJS Services.

This condition suggests that security mechanisms at the server layer can affect the app's business processes without providing clear feedback to users. As shown in Figure 5, the OJS application displays error messages to the user in the form of a process failure notification and instructions to reload the page. This message is general and does not provide technical information about the cause of the failure, so from the user's point of view the error appears to be an application system glitch.

Based on the correlation results with *Audit log* and *Error log* server, this process failure occurs due to the blocking of HTTP requests by the WAF that results in an HTTP 403 response. Blocking is done after *Inbound Anomaly Score* Reach a system-defined threshold, even if the request sent is a legitimate user activity. Thus, this occurrence is classified as *False positive*, as there is no indication of a web application attack such as SQL Injection or Cross-Site Scripting.

Table 5. The Impact of False Positives on OJS Services

Aspects	Observation Results
Affected features	Submission
Types of errors	OJS application error
Server response	HTTP 403 (Forbidden)
Source of error	Request blocking by WAF
Type of occurrence	False Positive
Impact on users	Failed to upload and submit manuscript
Impact on services	Decrease in OJS availability

The impact of this condition is the disruption of the main function of OJS as a scientific journal management system. Users are unable to complete the manuscript submission process, which directly lowers the service availability. If this kind of *false positive* occurs repeatedly, the reliability of OJS services in *the cloud environment* will decrease and potentially hinder the process of managing and publishing scientific articles.

Based on the results of server log analysis, this study succeeded in identifying *false positive patterns* that appeared in the implementation *of Web Application Firewall* based on *OWASP Core Rule Set*. This pattern is characterized by triggering protocol enforcement rules that are active in the request inspection phase on HTTP and resulting in an increase in the inbound anomaly score to exceed the system threshold. Furthermore, the impact analysis shows that the *false positive event causes the* submission *process to fail* in OJS and results in an HTTP 403 response, which directly affects the performance and availability of the service. These findings are the basis for formulating recommendations for security policy improvements so that the system protection mechanism can continue to run without interfering with legitimate user activities.

CONCLUSION

This study successfully identified patterns *False positive* that happens in the application *Web Application Firewall* (WAF) based *OWASP Core Rule Set* on the system *Open Journal Systems* (OJS). This pattern is indicated by the triggers of security rules that cause an increase in *Inbound Anomaly Score* to exceed the system threshold, even though the request sent is a legitimate user activity. These findings confirm that the *anomaly-based detection* in WAF has the potential to result in misclassification if not configured correctly.

The results of the analysis further show that the *false positive incident* has a direct impact on the performance and availability of OJS services. The blocking of the request by the WAF resulted in an HTTP 403 response that caused the manuscript submission process to fail, thus disrupting the main function of OJS as a scientific journal management system. This impact also affects the user experience because

the errors displayed on the application side do not provide clear technical information regarding the cause of the glitch.

Based on these findings, this study recommends the need for evaluation and adjustment of security policies in WAF based on OWASP CRS, especially in the management of *anomaly score* thresholds and *protocol enforcement* rules. This policy adjustment is expected to minimize false *positives* without reducing the level of system security, so that the balance between application protection and the availability of OJS services can be maintained.

REFERENCES

Ank Shah, J.K., D Janani, E.A., Rajashree Sutrawe, 2025. CYBER THREAT DETECTION AND PROFILING USING AI. ResearchGate. https://doi.org/10.55041/IJSREM.NCFT025

Dawadi, B.R., Adhikari, B., Srivastava, D.K., Dawadi, B.R., Adhikari, B., Srivastava, D.K., 2023. Deep Learning Technique-Enabled Web Application Firewall for the Detection of Web Attacks. Sensors 23. https://doi.org/10.3390/s23042073

Díaz-Verdejo, J., Muñoz-Calle, J., Alonso, A.E., Alonso, R.E., Madinabeitia, G., Díaz-Verdejo, J., Muñoz-Calle, J., Alonso, A.E., Alonso, R.E., Madinabeitia, G., 2022. On the Detection Capabilities of Signature-Based Intrusion Detection Systems in the Context of Web Attacks. Appl. Sci. 12. https://doi.org/10.3390/app12020852

Floris, G., Scano, C., Montaruli, B., Demetrio, L., Valenza, A., Compagna, L., Ariu, D., Piras, L., Balzarotti, D., Biggio, B., 2025. ModSec-AdvLearn: Countering Adversarial SQL Injections With Robust Machine Learning. IEEE Trans. Inf. Forensics Secur. 20, 6693–6705. https://doi.org/10.1109/TIFS.2025.3583234

MajedA.Alowaidi, S., Sunil Kumar Sharma, 2025. Impact of security standards and policies on the credibility of e-government | Request PDF. ResearchGate. https://doi.org/10.1007/s12652-020-02767-5

Ott, H., Bogatinovski, J., Acker, A., Nedelkoski, S., Kao, O., 2021. Robust and Transferable Anomaly Detection in Log Data using Pre-Trained Language Models. https://doi.org/10.48550/arXiv.2102.11570

OWASP CRS | OWASP Foundation [WWW Document], n.d. URL https://owasp.org/www-project-modsecurity-core-rule-set/ (accessed 12.17.25).

Ravindran, V.K., Ojha, S.S., Cambodia, A., 2025. A Comparative Analysis of Signature-Based and Anomaly-Based Intrusion Detection Systems. Int. J. Latest Technol. Eng. Manag. Appl. Sci. 14, 209–214. https://doi.org/10.51583/IJLTEMAS.2025.140500026

Reyes Narváez, A., Curipallo Martínez, M., Reyes Narváez, E., Lara, F., Reyes Narváez, E.P., Barba Molina, H., 2025. Evaluation Framework for False Positives in Open-Source WAFs Based on OWASP CRS Paranoia Levels: A Systematic Approach for Comparative Measurement. Eng. Proc. 115, 1. https://doi.org/10.3390/engproc2025115001

Riadi, I., Yudhana, A., W, Y., 2020. The security analysis of the Open Journal System website uses the vulnerability assessment method. J. Techno. Inf. and Computing Science. 7, 853–860. https://doi.org/10.25126/jtiik.2020701928

Scano, C., Floris, G., Montaruli, B., Demetrio, L., Valenza, A., Compagna, L., Ariu, D., Piras, L., Balzarotti, D., Biggio, B., 2025. ModSec-Learn: Boosting ModSecurity with Machine Learning, in: Mehmood, R., Hernández, G., Praça, I., Wikarek, J., Loukanova, R., Monteiro dos Reis, A., Skarmeta, A., Lombardi, E. (Eds.), Distributed Computing and Artificial Intelligence, Special Sessions I, 21st International Conference. Springer Nature Switzerland, Cham, pp. 23–33.

Siwach, M., Mann, D.S., 2022. Anomaly Detection for Web Log Data Analysis: A Review. J. Algebr. Stat. 13.

Utama, F.P., Nurhadi, R.M.H., 2024. Uncovering the Risk of Academic Information System Vulnerability through PTES and OWASP Method. Common CommIT. Inf. Technol. J. 18, 39–51. https://doi.org/10.21512/commit.v18i1.9384

Viradia, V., Jain, A., Ogety, S.S., Donvir, A., 2025. Resilient Cloud Computing Systems for Mission-Critical Applications, in: 2025 IEEE International Conference on Electro Information Technology (eIT). Presented at the 2025 IEEE International Conference on Electro Information Technology (eIT), pp. 311–315. https://doi.org/10.1109/eIT64391.2025.11103702

Zhou, Y., Zhang, S., Cui, X., Zhang, C., Li, X., 2021. An Accurate Torque Output Method for Open-End Winding Permanent Magnet Synchronous Motors Drives. IEEE Trans. Energy Converse. 36, 3470–3480. https://doi.org/10.1109/TEC.2021.3083958