NEWTON: Networking and Information Technology
Vol. 6 No. 1 June 2026, Page. 65 - 68
E-ISSN: 2797-0728

Brute Force Attack Mitigation Using WordPress and MikroTik Firewall

Tholib Hariono[1], Muhammad Ishomuddin[2]
[1,2] Information Syatem, Universitas KH. A. Wahab Hasbullah

Email:muhishomuddi03@gmail.com

ABSTRACT
This study discusses the development and implementation of a brute force attack mitigation system for websites by integrating WordPress-based detection with a MikroTik router firewall. Brute force attacks remain one of the most common threats to web authentication systems, particularly for educational institutions that rely on Content Management Systems such as WordPress. Conventional protection methods often depend solely on application-level mechanisms, which may increase server workload and reduce effectiveness during large-scale attacks. This research employed a Research and Development approach, including system analysis, design, implementation, and testing. The proposed system monitors repeated failed login attempts on the WordPress login page. When a predefined threshold is exceeded, the attacker's IP address is automatically transmitted to the MikroTik router through the RouterOS API and blocked using firewall address-list rules. Functional testing was conducted to ensure system reliability and accuracy. The results indicate that the integrated system successfully detects and blocks brute force attacks in real time, preventing repeated unauthorized access attempts and reducing server processing load. The system provides a practical and cost-effective solution for improving website security, particularly for educational institutions with limited cybersecurity resources.

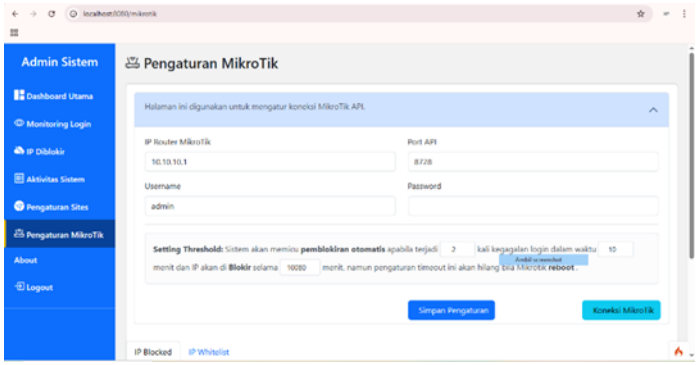
***Keywords**: Brute force attack; Website security; MikroTik router; Firewall integration*

INTRODUCTION
The rapid development of information technology has led to a significant increase in the use of websites for managing academic and administrative information in educational institutions. Along with this development, cyber threats targeting electronic systems have also increased. One of the most common of these threats is the brute-force attack, which targets login mechanisms by repeatedly trying different combinations of usernames and passwords.(Informasi et al., 2022)(Verizon, 2022). Many educational institutions use the WordPress platform due to its flexibility and ease of management. However, its widespread use makes it a frequent target for attackers. Security measures such as CAPTCHA testing, login attempt limits, and security plugins are typically implemented. However, these methods often rely solely on server-side processing and may reduce system performance during intense attacks.(Smith, J., & Kumar, 2021)

Previous studies have demonstrated the effectiveness of MikroTik routers in securing networks through firewall rules and access control mechanisms. However, most applications focus on network security without integrating detection mechanisms from web applications. Consequently, there is a lack of coordination between application monitoring and network-wide response.(Informasi et al., 2022)(Wicahyanto, 2024). This study aims to bridge this gap by developing an integrated system to mitigate random guessing attacks, combining WordPress login detection with the MikroTik router's firewall application. The unique aspect of this research lies in its immediate integration between the web application and the network infrastructure, providing a more efficient and responsive security solution for educational institutions.

METHOD
This study used a descriptive Research and Development method to design and implement a brute force attack mitigation system for websites. The research process followed several stages, including

system analysis, design, implementation, and testing. The system was developed using a WordPress-based website as the application platform and a MikroTik router as the network security device. The detection mechanism records all login attempts and identifies repeated failed logins based on a predefined threshold.



Figur 1. System Architecture of WordPress and MikroTik Integration

When the threshold is exceeded, the system automatically sends the attacker's IP address to the MikroTik router using the RouterOS API. The router then adds the IP address to a firewall address-list and blocks further access attempts. System testing was conducted using functional (black-box) testing to ensure that each feature operated according to the defined requirements.

RESULT AND DISCUSSION

The integrated brute force mitigation system was successfully implemented according to the planned design. The system includes essential features such as login attempt monitoring, IP address logging, automatic firewall synchronization, and dashboard-based monitoring. Testing was conducted using simulated brute force attack scenarios that reflect common attack patterns on WordPress login pages. The results show that the system was able to detect repeated failed login attempts and block malicious IP addresses in real time without affecting legitimate users.

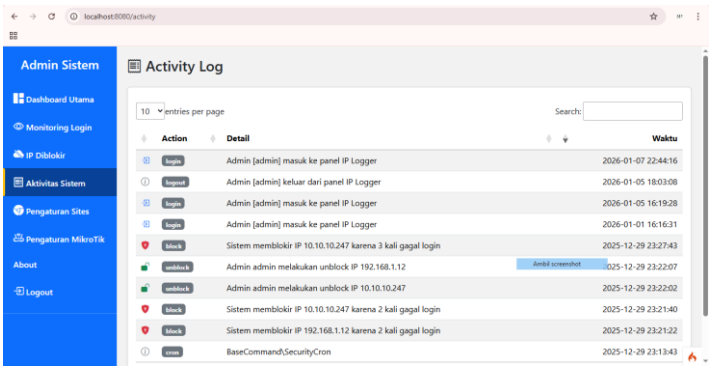


Figure 2. Brute Force Detection and IP Blocking Flow

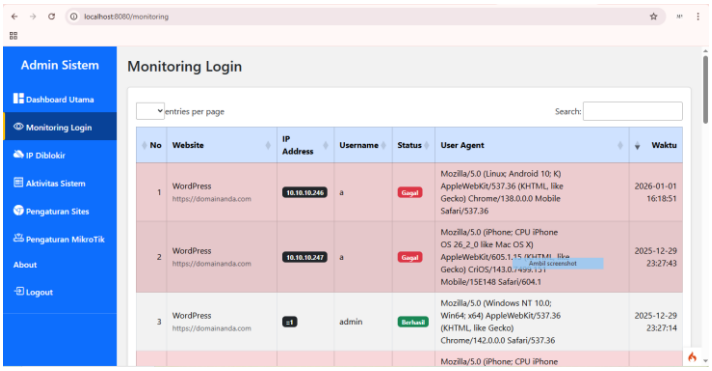


Figure 3. Monitoring Dashboard of Login Attempts and Blocked Ips

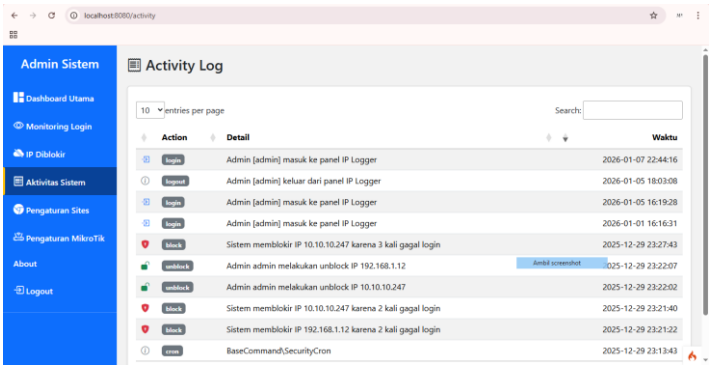


Figure 4. Brute Force Detection and IP Blocking Flow.

The application of the proposed system yielded the following results:

1. The system successfully recorded and analyzed all login attempts to the WordPress site.
2. Malicious IP addresses were automatically blocked after exceeding a predefined limit of failed login attempts.
3. The blocking process was implemented at the router level, preventing further data from reaching the web server.
4. The system performed efficiently during testing without impacting user access.

Tabel 1. Comparison of Server Load Before and After IP Blocking

Aspect	**Before Integration**	**After Integration**
Failed login attempts handled by server	High	Low
Server processing load	High	Reduced
Response time to attacks	Delayed	Real-time
Manual intervention required	Yes	No

Discussion

Font The results of this research indicate that integrating a WordPress-based brute-force attack detection system with a MikroTik router firewall significantly improves the effectiveness of website security mechanisms. By shifting IP address blocking tasks from the application layer to the network layer, the system reduces server load and improves response speed. These findings support information systems theories suggesting that automation and systems integration can enhance efficiency and minimize human error. Compared to previous studies that relied solely on security plugins or static firewall rules, the proposed system offers a more dynamic and responsive approach by enabling real-time coordination between the web application and the network device.

Similar research has indicated improvements in security performance through automated firewall mechanisms; however, the reduced server processing load observed in this study demonstrates the added advantage of enforcing security at the router level. Furthermore, centralized logging and monitoring features address security data fragmentation issues, allowing administrators to analyze security incidents

more effectively. In practice, this system is well-suited for educational institutions with limited infrastructure and technical personnel. Thanks to its simplicity and cost-effectiveness, this system offers a practical solution for improving website security without requiring complex configurations or sophisticated hardware. However, the system is limited to threshold-based detection and focuses exclusively on brute-force attacks. Future research may expand this approach by incorporating behavioral analysis or broader attack detection mechanisms.

CONCLUSIONS

This study concludes that integrating a WordPress-based random access detection system with a MikroTik router firewall is an effective approach to improving website security. The developed system is capable of detecting repeated failed login attempts and automatically blocking malicious IP addresses at the network level. This mechanism prevents unauthorized access attempts before they reach the web server, reducing server load and improving overall system performance. The results demonstrate that migrating security measures from the application layer to the network layer offers significant advantages in terms of response time and efficiency. Automatic firewall synchronization eliminates the need for manual intervention by administrators and ensures consistent enforcement of security policies. These findings support the idea that integrated information systems can enhance operational efficiency and reliability, particularly in environments with limited technical resources.

In practice, the proposed system offers a cost-effective and easily deployable solution for educational institutions that rely on WordPress and MikroTik infrastructure. The system addresses common security challenges without requiring complex configurations or sophisticated hardware. However, this research is limited to detecting threshold-based random intrusion attempts and focuses solely on login-related attacks. Future research may improve this system by incorporating behavioral analysis, machine learning techniques, or by extending protection to other types of cyberattacks. Extensive testing in real-world environments is also recommended to more accurately assess the system's performance and scalability.

REFERENCES

Informasi, J. S., Informasi, T., Gutama, D. H., & Estetikha, A. (2022). *Penanganan Serangan Brute Force dan Port Scanning Pada Router Mikrotik*. *1*, 1–13.

Smith, J., & Kumar, A. (2021). (2021). *Machine Learning based Intrusion Detection System for Web-Based Attacks*. https://www.researchgate.net/publication/342406733_Machine_Learning_based_Intrusion_Detection_System_for_Web-Based_Attacks

Verizon. (2022). DBIR: Data Breach Investigations Report. *The Race for 5G Supremacy*, 145–159. https://www.verizon.com/business/resources/T717/reports/2023-data-breach-investigations-report-dbir.pdf

Wicahyanto, A. (2024). *Rancang Bangun Firewall Router Mikrotik Berbasis Data Plugin Wordfence Mikrotik Router Firewall Design Based on Wordfence Plugin Data*. *12*(3), 3–8. https://doi.org/10.26418/justin.v12i3.80045