# Web Vulnerability mitigation Using ModSecurity and Reverse Proxy

Vishista Reddy Pandiri
Department of Computer Science
Lowell,Massachusetts
vishistareddy_pandiri@student.uml.edu

***Abstract*— The escalating use of web applications exposes users and organizations to a rising tide of cyber threats. To fortify web application security, this paper proposes the implementation of a Web Application Firewall (WAF) using ModSecurity and the Reverse Proxy method. The WAF, equipped with packet filtering, HTTP request blocking, and logging capabilities, successfully thwarted various tests including cross-site scripting, SQL injection, and unauthorized vulnerability scanning.**

**In the digital era, where businesses heavily rely on web applications, the paper addresses the challenge of securing IT assets through proactive Vulnerability Assessments & Penetration Tests. The research introduces two approaches: (1) leveraging a set of web application vulnerability scanners integrated into a unified framework with Python as the scripting engine, utilizing multi-threading for scan efficiency, and (2) mitigating detected vulnerabilities through the customization of configuration rules with the ModSecurity web application firewall.**

***Keywords -- Web Application Security, Web Application Firewall (WAF), ModSecurity, Vulnerability Assessment, Cyber Threats.***

## I. INTRODUCTION

The ubiquitous use of web applications across diverse sectors has become integral to modern communication and business operations. As a conduit for online banking, shopping, and business activities, web applications serve as a crucial interface for global interactions. However, the surge in web application usage has correspondingly heightened the risk of security threats, particularly at the application layer. Safeguarding web applications and servers against a spectrum of security threats that exploit vulnerabilities has become a paramount concern. Common targets for web application attacks include content management systems such as WordPress and databases.

### *A. Problem Definition:*

Web application security faces persistent challenges due to the evolving landscape of cyber threats. Threats targeting content management systems and databases pose significant risks, necessitating robust security measures. The need to protect against attacks like Cross-Site Scripting (XSS), SQL Injection, and Unauthorized Vulnerability Web Scanning is critical. Traditional vulnerability assessment tools, while valuable, often suffer from time-consuming scans and potential reliability issues. Addressing these challenges requires a comprehensive approach that not only identifies vulnerabilities but also mitigates them effectively.

### *B. Solution Approaches:*

To tackle the identified challenges, this research proposes a multi-faceted solution. The project employs various Vulnerability Assessment Scanners, including Nmap, DIRB, Whatweb, and Nikto, to conduct thorough vulnerability assessments. Importantly, the researchers introduce Multi-Threading to run these scanners concurrently, leveraging the CPU's ability to execute multiple processes simultaneously. This parallel processing significantly reduces scan time, allowing more focus on analyzing results.

The research extends beyond vulnerability identification to encompass mitigation through a Web Application Firewall (WAF) using ModSecurity. The WAF is implemented through the Reverse Proxy method, enhancing its capabilities to filter packets, block HTTP traffic, and provide robust logging. Customizing configuration rules, particularly with the inclusion of the OWASP Core Rule Set, adds complexity to ModSecurity's performance. The integration of ModSecurity as a low-cost, open-source solution strengthens web application security.

In summary, the research aims to address the escalating threats to web applications by proposing an integrated solution. Through efficient vulnerability assessments, facilitated by Multi-Threading, and the implementation of a powerful WAF using ModSecurity, the research seeks to fortify web applications against diverse cyber threats, offering a comprehensive approach to web application security.

## II. THEORETICAL BASIS

### *A. Web Application Security*

Addressing security concerns in web applications is imperative, and various measures can be taken to enhance security services. While acknowledging that perfection is elusive, implementing preventive measures is essential to thwart potential threats. A viable solution is the incorporation of a Web Application Firewall (WAF), which plays a crucial role in scrutinizing packet data traffic within a web application. Additionally, it acts as a deterrent by blocking various attacks targeted at web applications. Referring to the OWASP Top Ten list, the primary focus is on countering the top three attacks: Injection, XSS (Cross-Site Scripting), and Broken Authentication and Session Management. These well-known attacks pose significant risks to web servers, emphasizing the necessity for robust security measures.

### *B. Web Application Firewall*

A Web Application Firewall (WAF) serves as a protective measure for web applications, functioning as a security shield particularly for applications accessed via HTTP. Positioned at the forefront or as a barrier between external and internal networks within a network topology, WAF is strategically placed to mitigate threats from potential attackers.

It operates by filtering incoming and outgoing data, resembling a traditional firewall, and has the capability to halt or block network traffic deemed hazardous based on predefined rules. Noteworthy is that while the implementation of a WAF requires additional configurations to the web server, it does not necessitate modifications to the application builder script. This characteristic allows for the seamless application of WAF to already operational applications without disrupting their functionality.

*C. ModSecurity*

ModSecurity, an open-source module, operates as a Web Application Firewall (WAF) designed for integration with web servers. Its primary function is to identify and thwart attacks targeted at web applications. ModSecurity operates by utilizing configuration rules known as SecRules, enabling real-time monitoring of HTTP traffic. Additionally, it facilitates logging and the filtering of HTTP traffic based on the applied rules [10]. The flexibility of ModSecurity's rules allows for customized configurations aligned with the specific security requirements of the web application.

*D. Reverse Proxy Method*

The Reverse Proxy method is a security approach employed to conceal web servers. In this method, the client is oblivious to the fact that their request does not directly reach the web server; instead, it is routed through a proxy server. As a result, the client is only aware of the proxy server's address. The actual location of the web server, concealed topologically by the Reverse Proxy, remains unknown to the client.

Furthermore, the Reverse Proxy method can serve as a deployment strategy for Web Application Firewall (WAF) implementation in a web application. WAF is applied to web applications on devices with configured Reverse Proxy, expanding the security coverage significantly. This configuration not only shields the web server's actual location but also broadens the protective scope of WAF, making it more challenging for attackers to discern the real server location.

## III. RESEARCH METHODOLOGY

The approach employed in this study is rooted in experimental research methodology, which falls within the realm of quantitative research. Experimental research is conducted in a controlled laboratory setting to investigate the impact of specific treatments on the subject of study. The distinctive feature of this methodology lies in the researchers' ability to deliberately select and manipulate variables, while also maintaining tight control over other factors that could potentially influence the experimental process.

*Preparation Process :*

The preparatory phase serves as the preliminary step preceding the commencement of the research. During this stage, an extensive review of relevant literature and consultations were undertaken to delve into the aspects to be explored in the study. The literature chosen for examination focused on various topics such as Web Application Firewall (WAF), the pivotal role of WAF in enhancing security functionalities within web applications, methodologies for WAF implementation in web applications, the ModSecurity module, the configuration of Reverse Proxies on web servers, prevalent web application attacks, and the tools employed for the experimental implementation and testing.

## V. CONCLUSSIONS AND RECOMMENDATIONS

*A. Discussion:*

The discussion revolves around the multifaceted approach presented in addressing the challenges associated with web application security. By incorporating a set of diverse Vulnerability Assessment Scanners and implementing Multi-Threading, the research aims to enhance the efficiency and coverage of vulnerability detection. The choice of scanners, including Nmap, DIRB, Whatweb, and Nikto, reflects a comprehensive strategy to identify potential vulnerabilities in web applications, ranging from network-level issues to content-specific challenges.

The introduction of Multi-Threading as a methodology for concurrent scanning is a noteworthy innovation. This approach optimizes scanning time and resource utilization, demonstrating a commitment to practicality and effectiveness in addressing the time-consuming nature of traditional vulnerability assessments.

The subsequent discussion explores the significance of the proposed solution's second phase: the implementation of a Web Application Firewall using ModSecurity. By utilizing the Reverse Proxy method and incorporating the OWASP Core Rule Set, the WAF is designed to fortify web applications against specific threats, including XSS, SQL Injection, and unauthorized vulnerability web scanning. The open-source nature of ModSecurity is highlighted as a cost-effective alternative, demonstrating a commitment to accessible and efficient web application security solutions.

*B. Analysis:*

The analysis delves into the implications of the proposed solution in the broader context of web application security. The research acknowledges the dynamic nature of cyber threats and the importance of staying ahead of potential vulnerabilities. The combination of vulnerability assessments and WAF implementation is viewed as a comprehensive strategy, providing a proactive defense against a range of potential attacks.

The Multi-Threading approach is analyzed for its impact on scan efficiency, emphasizing the reduction in scanning time and the potential for more thorough analyses of results. The integration of ModSecurity as a WAF is analyzed for its flexibility, scalability, and ability to cater to the specific security needs of diverse web applications.

Additionally, the analysis considers the practicality of the proposed solution for real-world implementation. Factors such as ease of integration, resource requirements, and scalability are explored to assess the feasibility of adopting this approach across various web application environments.

*C. Conclusion:*

In conclusion, the research introduces a comprehensive strategy to enhance web application security. The combination of advanced vulnerability assessments with Multi-Threading and the implementation of a robust Web Application Firewall using ModSecurity represents a proactive and efficient approach. The proposed solution aims to not only identify vulnerabilities but also mitigate them effectively, addressing the evolving landscape of web application security challenges. The open-source and cost-effective nature of the proposed solution further strengthens its appeal for organizations seeking robust security measures for their web applications.

In this study, a comprehensive approach was undertaken to enhance the security of web applications through effective vulnerability discovery and mitigation. Firstly, the research focused on selecting multiple scanners for web application scanning, leveraging a Python-based scanning engine to run these scanners independently and concurrently using multi-threading. The outcomes revealed a substantial reduction in overall execution time and memory consumption, indicating the efficiency gained by parallelizing the scanning process. Data normalization and parsing, facilitated by configuration rules, were employed to extract meaningful vulnerabilities from the scan results, and these were systematically stored in a database.

Secondly, the analysis shifted towards the mitigation of discovered vulnerabilities using a Web Application Firewall (WAF), specifically ModSecurity. Customized configuration rules were generated for individual vulnerabilities, resulting in a significant reduction and mitigation of the identified threats. The tailored rules within ModSecurity demonstrated their efficacy in fortifying web applications against potential attacks, showcasing the adaptability and precision achievable through this approach.

The primary contribution of this work lies in the demonstrated reduction of execution time for scanners and the utilization of multiple scanners through a Python-based scanning engine. This not only streamlines the vulnerability discovery process but also enhances the scalability and efficiency of web application security measures. Additionally, the research contributes to the field by showcasing the effectiveness of ModSecurity in mitigating discovered vulnerabilities through customized configuration rules, affirming its role as a powerful tool for web application security.

The testing and analysis stages underscored the success of implementing a Web Application Firewall in a web-based application using ModSecurity and the Reverse Proxy method. Through simulated attacks such as Cross-Site Scripting, SQL Injection, and Unauthorized Vulnerability Web Scanning, the combination of ModSecurity and reverse proxy methods within the WAF successfully thwarted all threats, validating the robustness of the proposed security measures.

As a pathway for future research, further development could include the creation of an interface for attack logs, enhancing the efficiency of attack detection. Additionally, the implementation of an alert system could provide real-time notifications to application administrators in the event of an attack attempt, contributing to a more proactive and responsive web application security framework. Overall, this research establishes a foundation for advancing web application security through an integrated and proactive approach.

## REFERENCES


[1] R. A. Muzaki, O. C. Briliyant, M. A. Hasditama and H. Ritchi, "Improving Security of Web-Based Application Using ModSecurity and Reverse Proxy in Web Application Firewall," 2020 International Workshop on Big Data and Information Security (IWBIS), Depok, Indonesia, 2020.

[2] Netcraft, "Netcraft," 28 Februari 2019. [Online]. Available: https://news.netcraft.com/archives/2019/02/28/february-2019-webserver-survey.html.

[3] T. Jain and N. Jain, "Framework for Web Application Vulnerability Discovery and Mitigation by Customizing Rules Through ModSecurity," 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 2019.

[4] V. Clincy and H. Shahriar, "Web Application Firewall: Network Security Models and Configuration," in *42nd IEEE International Conference on Computer Software & Applications*, 2018.

[5] V. Clincy and H. Shahriar, "Web Application Firewall: Network Security Models and Configuration," in *42nd IEEE International Conference on Computer Software & Applications*, 2018.

[6] Positive Technology, "Attacks on web applications: 2018 in review," 26 Juni 2019. [Online]. Available: https://www.ptsecurity.com/wwen/analytics/web-application-attacks-2019/.