ENHANCING WEB DEFENSE THROUGH MACHINE LEARNING AND ACTIVE RESPONSE MECHANISM INTEGRATION IN WAF

THESIS

Submitted to Fulfill One of the Requirements in Obtaining a Master of Informatics (S2) Degree

AGUNG PRASETIAWAN
20220130006

MASTER OF COMPUTER SCIENCE PROGRAM
SCHOOL OF COMPUTER SCIENCE

AUGUST 2024

AUTHOR’S STATEMENT

THESIS TITLE : ENHANCING WEB DEFENSE THROUGH MACHINE LEARNING AND ACTIVE RESPONSE MECHANISM INTEGRATION IN WAF

NAME : AGUNG PRASETIAWAN

NIM 20220130006

“I declare that this Thesis is entirely my own work, except for the excerpts and summaries for which I have duly cited the sources. Should another party in the future present sufficient evidence that this thesis is their work, I am prepared to renounce my Master's degree in Computer Science, along with all the associated rights and responsibilities.”

Sukabumi, August 2024

AGUNG PRASETIAWAN

THESIS APPROVAL

THESIS TITLE : ENHANCING WEB DEFENSE THROUGH MACHINE LEARNING AND ACTIVE RESPONSE MECHANISM INTEGRATION IN WAF

NAME : AGUNG PRASETIAWAN
NIM 20220130006

This script has been checked and approved

Sukabumi, August 2024

Head of Study Program,	Supervisor
Prof. Ir. Teddy Mantoro, M.Sc., PhD.	Deshinta Arrova Dewi, S.Kom., M.Si, PhD
NIDN.	NIDN.

THESIS VALIDATION

THESIS TITLE : ENHANCING WEB DEFENSE THROUGH MACHINE LEARNING AND ACTIVE RESPONSE MECHANISM INTEGRATION IN WAF

NAME : AGUNG PRASETIAWAN
NIM 20220130006

This Thesis has been tested and defended in front of the Board of Examiners in Thesis session on July 21, 2024. In our review, this Thesis adequate in terms of quality for the purpose of awarding the Master of Computer Degree (M.SC).

Sukabumi, August 2024

Supervisor I

Prof. Ir. Teddy Mantoro, M.Sc., Ph.D
NIP.

Examiner 1

Umar Aditiawarman, S.T, M.Sc, Ph.D.
NIP.

Supervisor 2

Deshinta Dewi

Deshinta Arrova Dewi, S.Kom.,M.Si, Ph.D
NIP.

Examiner 2

Haris Al Qodri Maarif, S.T., M.Sc., Ph.D.
NIP.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF APPENDIX

DEDICATION

This thesis is lovingly dedicated to my dear parents, my beloved wife Ariestiani, and my wonderful children, Dhiwa Kenshy Aljauzi and Ishana Kanzou Mila. To my late father, whose memory continues to guide and inspire me every day. Your legacy of strength and integrity is a beacon in my life, and your presence remains with me in every decision I make. Though you are no longer with us, your values and teachings continue to influence every aspect of my journey. To my mother, whose constant prayers and unwavering faith in me have been my source of comfort and encouragement. Your love and wisdom are the pillars of my strength, and your sacrifices have not gone unnoticed. Your words of encouragement and belief in my potential have provided me with the courage to overcome countless challenges.

To my beloved wife, Ariestiani, thank you for your endless support, patience, and love throughout this journey. Your unwavering belief in me and every prayer and word of encouragement have been invaluable. You have been my anchor through turbulent times, providing the reassurance and companionship that have been vital to my success. Your understanding and encouragement have fueled my determination and perseverance.

To my wonderful children, Dhiwa Kenshy Aljauzi and Ishana Kanzou Mila, whose joy and laughter inspire me to strive for excellence. Your curiosity and zest for life remind me of the importance of pursuing one’s dreams. You are my pride and joy, and I hope that this work serves as an example of the power of perseverance and dedication. Watching you grow and learn has been a profound joy, and your love and support have been a tremendous source of motivation in completing this thesis. To Dhiwa and Ishana, may you always seek knowledge with passion and curiosity. Remember, learning knows no bounds and is a lifelong journey that enriches both mind and soul.

This journey has been one of learning, growth, and self-discovery. Each of you has played an integral role in helping me reach this milestone, and I am deeply grateful for your unwavering love and support. This accomplishment is as much yours as it is mine, and I dedicate this work to you with all my heart.

FOREWORD

With heartfelt praise and gratitude to God Almighty, for it is solely by His blessings and grace that I have been able to complete this thesis. The writing of this thesis is a necessary step towards fulfilling the requirements for obtaining a Master's degree in Computer Science at Nusa Putra University. I acknowledge that, without the support and guidance from many individuals throughout my academic journey and the thesis-writing process, completing this thesis would have been exceedingly difficult. Therefore, I extend my sincere thanks to :

1. Dr. Kurniawan, ST., M.Sc., MM as Chancellor of Nusa Putra Sukabumi University;
2. Prof. Ir. Teddy Mantoro, M.Sc., PhD as Head of School Computer Science Nusa Putra Sukabumi University and as Supervisors;
3. Deshinta Arrova Dewi, S.Kom.,M.Si, Ph.D as Supervisorss;
4. All Master Of Computer Science Lecturers who have provided very usefull knowledge during lectures;
5. Parents and my family for their supports, patience, prayers and never getting tired of educating and giving, bothmaterial and non-material;
6. Fellow comrades in Master of Computer Science 2022 who always give encouragement and always accompany from the beginning of the lecture until now;
7. All parties who have helped the author in writing this thesis;

For continuous improvement, I welcome any suggestions and constructive criticism with open arms. Ultimately, I submit everything to Allah SWT, hoping that this work will be beneficial, especially for the author, and more broadly, for all of us.

Sukabumi, August 2024

Agung Prasetiawan

ABSTRACT

Today, web applications play an important role in modern digital infrastructure by providing users with public access to services and information quickly and flexibly. Web application security is critical due to the increasing complexity of cyber attacks. This study proposes a new working concept that combines machine learning and active response mechanisms in Web Application Firewalls (WAFs) with the support of the concept of creating libraries that make WAFs more adaptive.

The current state of web application security is defined by the weaknesses of conventional WAFs, which often struggle to withstand changing cyber threats such as zero-day attacks and new attack anomalies due to the static rules and signature bases used in WAFs. On the other hand, dynamic cyber threats are always evolving and can evade conventional WAFs. To stay up to date with the latest cyber dangers, WAF signatures and rules must be updated regularly,

however, this can be a difficult task, time consuming and lacks awareness on the part of various parties.

Using techniques that incorporate machine learning, this paper proposes a WAF concept for identifying and categorizing malicious activities. To ensure robustness and flexibility, the model is trained on a variety of datasets covering various attack scenarios. Developing a library that can also generate future attack patterns is an important step in active response system integration. This concept is intended to better anticipate current and future potential threats or what is known as a zero-day attack. This paper's approach combines supervised and unsupervised learning approaches for initial training and ongoing learning to respond to new threats.

Keyword: Web Application Security, Machine Learning, Web Application Firewall, WAF, Dynamic Security Framework, Zero-day

CHAPTER 1

INTRODUCTION

1.1 Research Background

Web applications are the foundation of digital interactions in a dynamic virtual world, giving users easy access to services, data and connectivity like never before. However, this connectivity comes at a cost, as many cyber threats aim to exploit gaps in this application. Traditional security mechanisms, particularly those related to Web Application Firewalls (WAFs), are finding it increasingly difficult to effectively combat today's cyber adversaries as the digital world becomes more complex. Web applications have been made more resilient against known attacks thanks in large part to the use of traditional WAFs. Unfortunately, today these systems are more vulnerable to dynamic techniques used by cybercriminals, and the online applications they guard perform worse due to their reliance on static rules and signature-based detection. It is becoming increasingly clear that new and flexible defense mechanisms are needed as the complexity and scope of threats increases. This study offers a concept that combines the agility of active response mechanisms with the power of machine learning to redefine web application security through WAF. The core problem is the passive nature of traditional WAFs. While they are adept at recognizing previously known threat patterns, they often struggle to adapt to new attack paths and sophisticated evasion strategies used by cyber adversaries such as zero day attacks. The impact of these obstacles is far-reaching, from false positives that impede legitimate user traffic to an inability to proactively respond to emerging threats. This thesis fills an important gap in web application protection by offering a paradigm shift in which machine learning and active response mechanisms collaborate to build intelligent and dynamic shields. To enhance the capabilities of conventional WAFs, machine learning is becoming a solution due to its ability to evaluate very large data sets and identify complex patterns. Using integrated machine learning models, the proposed concept seeks to provide WAFs with the ability to independently learn predictions and anomalies so as to differentiate between malicious and non-malicious behaviour. Machine learning models evolve into proactive defenders that can recognize and neutralize new and unknown threats through continuous learning and adaptation. In addition to machine learning, the incorporation of active response mechanisms marks an innovative shift from conventional reactive methods. The integration of countermeasures tactics that actively engage attackers to thwart their plans that cannot simply be detected is discussed in this thesis.

The main goal of this project is to create, practice and assess new concepts that allow machine learning and active response mechanisms to be seamlessly integrated into WAF. Therefore, this research aims to:

- Improve Detection Accuracy, reducing false positives and negatives by applying machine learning techniques to improve threat detection recall and precision.
- Adapt to Emerging Threats, create dynamic defenses by giving WAFs the tools they need to continuously learn and adapt to new and changing attack patterns.

The subsequent chapters of this thesis delve into active response mechanisms, machine learning, and online application security. They cover the creation and implementation of the framework and present the research findings, assessing the efficacy of the integrated approach.

1.2 Problem Statement

Traditional WAFs are ineffective against evolving threats due to their static rules, complexity, and lack of awareness of the protected web application.

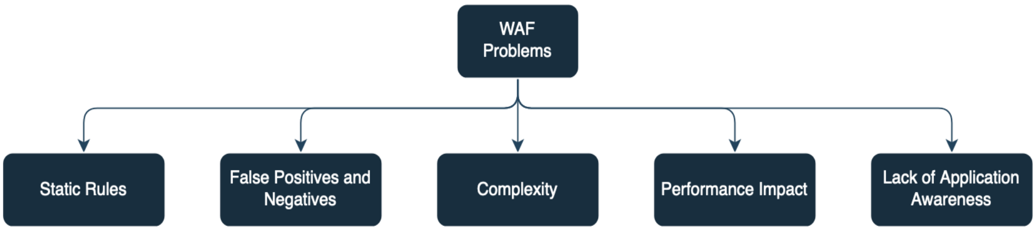

Figure 1: WAF Problems

- Static Rule Sets, because static rule sets and signature-based detection are the main components of conventional WAFs, they are susceptible to evasion tactics employed by skilled adversaries. These systems' incapacity to instantly adjust to new threats renders them less potent in combating dynamic and ever-changing attack vectors.

- False Positives and Negatives, Reliance on predefined patterns often results in false positives, which disrupt the user experience by misclassifying normal traffic as malicious. On the other hand, false negatives pose a significant risk to web application security because they allow some sophisticated attacks to remain undetected.
- Complexity, WAFs can be complex and difficult to configure and manage, which can lead to misconfigurations that can leave web applications vulnerable to attack.
- Performance Impact, WAFs can have a negative impact on the performance of web applications.
- Lack of Application Awareness, The online apps that traditional WAFs safeguard are typically not well-known to them. Improved attack detection and rule execution could reduce performance implications if a greater understanding of the endpoints and structure of the protected application is gained.
- Identifying WAF, Web Application Firewalls (WAFs) face the issue of being identifiable through response patterns, known as WAF Fingerprints. Attackers can discern which WAF is in use by analyzing response behaviors, as different WAFs signal rejections differently. This problem is exacerbated if the WAF is not frequently updated, a common issue with open-source projects. Even proprietary WAFs with automated updates can be identified, providing attackers with insights into their logic and vulnerabilities. This identifiability compromises WAF security, making it easier for attackers to exploit.

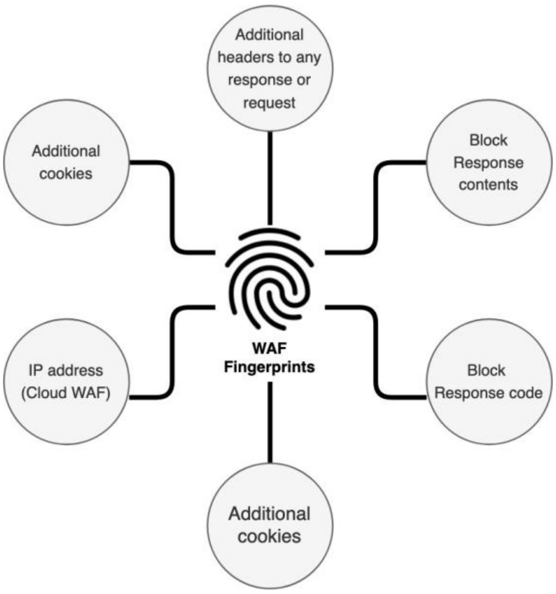

Figure 2: WAF Fingerprint

1.3 Research Objectives

The main goal of this research is to design and evaluate a new architectural concept for Web Application Firewalls (WAFs) that combines machine learning and active response mechanisms. By addressing the shortcomings of conventional and modern WAFs, this concept seeks to offer proactive, proactive and dynamic defense against changing cyber threats. The following are the actual objectives of this research:

1. Enhance Detection Accuracy
   a. Objective: Improve the accuracy of threat detection within WAFs by leveraging advanced machine learning techniques.
   b. Details: Static rule sets are frequently used in traditional WAFs, which can lead to high rates of false positives and false negatives. This research aims to improve threat detection precision by utilizing machine learning methods. This will help to decrease false alarms and make sure that genuine communication is not mistakenly categorized as dangerous. This goal is to create and hone models that, from patterns and behaviors seen in online

traffic, can reliably differentiate between benign and malevolent activity.

2. Adapt to Emerging Threats
   a. Objective: Create a dynamic defense system capable of continuously learning and adapting to new and evolving attack patterns.
   b. Details: Attackers are using ever-more-advanced tactics, and cyber risks are continuously changing. Because traditional WAFs rely on pre-established rules, they find it difficult to keep up with these developments. The goal of this research is to provide WAFs the capacity to continuously learn from fresh data and adjust. The framework will be able to recognize new threats and modify its defensive strategies in response by employing both supervised and unsupervised learning techniques, offering a more reliable and adaptable security solution.
3. Reduce Performance Impact
   a. Objective: Minimize the performance impact of WAFs on web applications while maintaining high levels of security.
   b. Details: The potential for traditional WAFs to impair web application performance is one of major critiques. The goal of this project is to provide a lightweight, effective architecture that guarantees security measures don't negatively impact user experience. The aim is to preserve or even increase application speed while offering enhanced security through the optimization of the implementation of machine learning models and active response mechanism.

The suggested study intends to transform web application security by offering a comprehensive concept that addresses the main weaknesses of WAF. This framework aims to provide robust, flexible, and intelligent security mechanisms for contemporary online applications by improving detection accuracy and adapting to new threats. If this framework is successfully put into practice, it can increase the resilience of web applications against various cyber threats, thereby making the internet a safer and more secure place.

1.4 Research Significance

Because it addresses serious weaknesses in Web Application Firewalls (WAFs), this research has the potential to drastically change the web application security environment. The paradigm shift occurs through the incorporation of machine learning and active response mechanisms into WAF. This study introduces a new concept of threat detection and response, which continues to advance cybersecurity technology. This suggested architecture raises the bar for web application security by using machine learning to dynamically detect and counter new and emerging cyber threats. The unique strategy of combining machine learning with active reaction mechanisms goes beyond the static and reactive characteristics of WAF. This study shows how different technologies can be combined in a way that makes defense systems more adaptable and durable.

The suggested approach can help reduce WAF maintenance costs by minimizing the need for frequent modifications of static rules and signatures. Once trained, machine learning models require less manual intervention to react to new threats. The aim of this research is to offer a new concept for WAFs.

Knowledge in the domains of active defense mechanisms, machine learning, and cybersecurity is expanded through this research. For additional studies and progress in this area, the methods and results may serve as a basis. Cybersecurity professionals can improve their organizations' protective measures by leveraging the knowledge and resources gained from this research.

This research is important for reasons other than only technology. This work has the potential to greatly improve online application security by addressing the flaws in conventional WAFs and offering a dynamic, intelligent, and proactive protection framework. The results of this study should strengthen defenses against cyberattacks and guarantee the dependability and security of vital digital infrastructures. Consequently, this upholds the more general objectives of promoting global user security and preserving confidence in digital systems.

1.5 Research Limitation and Assumptions

There are inherent limits and assumptions that must be addressed, even if the goal of this research is to greatly improve web application security through the integration of machine learning and active response mechanisms in Web Application Firewalls (WAFs). Comprehending these constraints and presumptions is essential for placing the research findings in perspective and directing future investigations in this field.

Limitations

1. Data Quality and Availability
   a. Limitation

      The caliber and volume of training data have a major impact on how well machine learning models perform. The model's performance could be negatively impacted if the dataset is incomplete or biased.

   b. Impact

      A lack of high-quality, diversified datasets to work with could make it more difficult to train models that are broadly applicable to a variety of online application kinds and attack vectors. Moreover, in this study, the focus is primarily on injection attacks such as SQL Injection. This specific focus could limit the model's effectiveness against other types of attacks not covered in the training data.

2. Evolving Threat Landscape
   a. Limitation

      Attackers are always coming up with new ways to get around security systems, which means that cyber risks are always changing. There is always a lag between the appearance of new threats and the model's capacity to identify them, even though machine learning models can adjust to them.

   b. Impact

A window of vulnerability will always exist when new attack types are first introduced, which could jeopardize the suggested framework's efficacy.

3. Resource Constraints
    a. Limitation

       Active response systems and machine learning models can be resource-intensive to implement and maintain. This covers processing power, big dataset storage, and continuous model maintenance and tuning.
    b. Impact

       The deployment and maintenance of such sophisticated security mechanisms may be difficult for resource-constrained organizations, which would restrict the application of the suggested architecture to resource-rich settings.

Assumptions

1. Availability of Sufficient Data
    a. Assumption

       It is anticipated that adequate and pertinent datasets would be available for machine learning model training and validation. These datasets must to include a variety of attack scenarios as well as typical online application behaviors.
    b. Rationale

       Creating reliable and accurate machine learning models requires clean data.
2. Technological Infrastructure
    a. Assumption

       The advanced WAF system can be implemented and managed by organizations utilizing the suggested concepts since they possess the required technological infrastructure, including sufficient processing power and trained staff.

    b. Rationale

       Considerable technological and human resources are needed for the efficient implementation and running of active response mechanisms and machine learning.

3. Continual Learning and Adaptation

    a. Assumption

       The suggested structure will be updated and improved over time in response to fresh information and changing threat environments.

    b. Rationale

       In a dynamic cyber environment, the security measures' continued relevance and efficacy depend on ongoing learning and adaptation.

This section gives a reasonable foundation for interpreting the research findings by highlighting the assumptions and constraints. Although there is much potential for improving web application security through the suggested incorporation of machine learning and active response mechanisms into WAFs, it is crucial to understand the difficulties and limitations associated with this strategy. Reaching the full potential of this novel security architecture will require addressing these constraints and verifying the underlying hypotheses in follow-up studies and real-world applications.

The foundational aspects discussed in this section provide a solid basis for interpreting the research findings by emphasizing the assumptions and limitations inherent in the proposed approach. While the integration of machine learning and active response mechanisms into Web Application Firewalls (WAFs) presents a promising avenue for enhancing web application security, understanding the complexities and challenges associated with this strategy is essential. These constraints may arise from the unpredictability of real-world scenarios, the evolving nature of cyber threats, and the potential limitations of machine learning models themselves.

To fully realize the potential of this innovative security framework, it will be necessary to thoroughly address these challenges. This includes refining the integration process, improving the adaptability of the WAFs, and ensuring that the machine learning models can effectively respond to new and unforeseen threats. Moreover, testing and validation in various environments will be key to confirming the effectiveness and reliability of the proposed solution. Such rigorous evaluation will also help identify areas where further improvements can be made, ensuring that the security architecture remains robust over time. The research also underscores the importance of ongoing studies to refine and validate the underlying hypotheses. These studies should focus on real-world applications and seek to bridge the gap between theoretical models and practical implementations. By doing so, researchers and practitioners can work together to enhance the overall effectiveness of WAFs in defending against increasingly sophisticated attacks. Furthermore, collaboration with industry experts can provide valuable insights into the practical constraints and opportunities that may arise during deployment.

Ultimately, achieving the full potential of this approach will require a multifaceted effort that goes beyond theoretical research. It will involve iterative improvements, continuous monitoring, and adaptation to the ever-changing landscape of cybersecurity. By recognizing and addressing the constraints identified in this study, future research can contribute to the development of more resilient and effective security solutions for web applications.

CHAPTER V

CONCLUSION AND RECOMMENDATION

5.1 Conclusion

This research aimed to enhance the security of web applications by integrating machine learning and active response mechanisms within Web Application Firewalls (WAFs). The primary objectives were to improve detection accuracy, adapt to emerging threats, and proactively disrupt attacks. The following conclusions can be drawn from the research:

Enhanced Detection Accuracy
The implementation of machine learning models, particularly the Random Forest algorithm, significantly improved the accuracy of detecting malicious activities. The Random Forest model achieved an accuracy of 95%, precision of 94%, recall of 95%, and an F1 score of 92%, demonstrating its efficacy in distinguishing between malicious and benign queries. This high level of accuracy ensures that the WAF can reliably identify and block known attack patterns, reducing the risk of successful breaches.
Adaptation to Emerging Threats
The anomaly detection mechanism enabled the system to identify and isolate unknown threats that were not present in the training data. By continuously learning from these anomalies, the system showed an ability to adapt to new attack vectors, enhancing its overall resilience. This adaptive capability is crucial in the ever-evolving landscape of cyber threats, where attackers constantly develop new techniques to bypass traditional security measures.
Proactive Response Mechanisms
The integration of active response mechanisms, such as blocking known attack patterns and isolating suspicious queries, ensured real-time mitigation of threats. This proactive stance is critical in reducing the window of vulnerability and preventing potential damage to web applications. By taking immediate action against identified threats, the system can significantly limit the impact of cyber attacks.

Comprehensive Security Solution
By combining known attack detection, anomaly detection, and active response mechanisms, the proposed system provides a robust and adaptive security solution. The use of stop words and general MySQL patterns further enhanced the system's accuracy and reduced false positives, ensuring legitimate queries were not mistakenly blocked. This comprehensive approach ensures that the system can protect against both known and unknown threats, providing a higher level of security for web applications.

Table 10: Conclusions

Therefore, it can be concluded that the proposed approach to link machine learning to active response mechanisms in WAF systems is efficient for improving web application security. This aspect, which ensures that the system is always learning about various threats, makes it rather effective at combating these threats at any given time. The outcomes obtained reveal that the proposed system can effectively protection web applications in real-time and enhance their security level by a large degree.

5.2 Recommendation

Based on the findings and conclusions of this research, the following recommendations are proposed for further research and practical application:Based on the findings and conclusions of this research, the following recommendations are proposed for further research and practical application.

Firstly, it is probable to permanently enhance the machine learning models applied to the WAF system’s architecture. When new types of attacks are discovered or new techniques are devised, the models become less effective and need to be recalibrated with new sets of data. It is as such recommended that real-time threat intelligence feeds should be incorporated in the system and the models trained at a predefined interval of time.

Secondly, improving the detection of the anomalies in the system is very important. These ideas build upon the current approach in the ways described below: The current approach should include other context-aware features in addition to location; more equipped anomaly detection algorithms have to be used. This will assist in determining the reputation of the IP address and, therefore, distinguish between real zero day threats and other false alarms. Working with the cybersecurity analysts to obtain improved datasets that contain different types of genuine attacks and normal transactions will also strengthen the system's variability and increase its detection capability.

Lastly, for practical application, it is advised to implement a modular and scalable architecture for the WAF system. This will allow for easier integration with existing security infrastructures and the flexibility to adapt to different web application environments. Additionally, providing detailed logging and reporting mechanisms will help security teams understand and respond to detected threats more effectively. Continuous monitoring and feedback loops should be established to refine the system based on operational data and real-world attack scenarios. By following these recommendations, organizations can significantly enhance their web application security posture.

REFERENCES

Chirag Tiwari1, Samaya Pillai1, Ahmed J. Obaid2, Ali Raheem Saear3, Ali Kareem Sabri (2023), *Integration of Artificial Intelligence/Machine Learning in Developing and Defending Web Applications*. http://dx.doi.org/10.1063/5.0171097

Sepczuk Mariusz (2023), *Dynamic Web Application Firewall detection supported by Cyber Mimic Defense approach*. https://doi.org/10.1016/j.jnca.2023.103596

Antonio Coscia, Vincenzo Dentamoro, Stefano Galantucci, Antonio Maci, Giuseppe Pirlo (2023), *An innovative two-stage algorithm to optimize Firewall rule ordering*. http://dx.doi.org/10.1016/j.cose.2023.103423

K Surendhar, Bishwajeet Kumar Pandey, G Geetha, Hardik Gohel (2023), *Detection of payload injection in Firewall Using Machine Learning*. https://doi.org/10.1109/CSNT57126.2023.10134743

Babu Dawadi, Bibek Adhikari, Devesh Srivastava (2023), *Deep Learning Technique-Enabled Web Application Firewall for the Detection of Web Attacks*. http://dx.doi.org/10.3390/s23042073

Shihao Wang, Ruiheng Liu, Xu Guo, Gaoda Wei (2023), *Design of Web Application Firewall System through Convolutional Neural Network and Deep Learning*. https://doi.org/10.1109/CIPAE55637.2022.00101

Chirag Tiwari, Samaya Pillai, Ahmed J. Obaid, Ali Raheem Saear, Ali Kareem Sabri (2023), *Integration of artificial intelligence/machine learning in developing and defending web applications*. http://dx.doi.org/10.1063/5.0171097

Waleed Bin Shahid, Baber Aslam, Haider Abbas, Hamad Afzal,, Saad Bin Khalid (2022), *A deep learning assisted personalized deception system for countering web application attacks*. https://doi.org/10.1016/j.jisa.2022.103169

Tomás Sureda Riera, Juan-Ramón Bermejo Higuera, Javier Bermejo Higuera, José-Javier Martínez Herraiz, Juan-Antonio Sicilia Montalvo (2022), *A new* *multi-label dataset for Web attacks CAPEC classification using machine learning techniques*. https://doi.org/10.1016/j.cose.2022.102788

Andrea Tundis, Samuel Ruppet, Max Mühlhäuser (2022*), A Feature-driven Method for Automating the Assessment of OSINT Cyber Threat Sources*. https://doi.org/10.1016/j.cose.2021.102576

Ines Jemal, Mohamed Amine Haddar, Omar Cheikhrouhou, Adel Mahfoudhi (2022), *SWAF: A Smart Web Application Firewall Based on Convolutional Neural Network*. http://dx.doi.org/10.1109/SIN56466.2022.9970545

Aref Shaheed, David Megias (2022), *Web Application Firewall Using Machine Learning and Features Engineering*. https://doi.org/10.1155/2022/5280158

Waleed Bin Shahid, Baber Aslam, Haider Abbas, Saad Bin (2021), *An enhanced deep learning based framework for web attacks detection, mitigation and attacker profiling*. https://doi.org/10.1016/j.jnca.2021.103270

Applebaum Simon, Gaber Tarek, Ahmed Ali (2021), *Signature-based and Machine-Learning-based Web Application Firewalls: A Short Survey*. https://doi.org/10.1016/j.procs.2021.05.105

Aref Shaheed, M. H. D. Bassam Kurdy (2021), *Web Application Firewall Using Machine Learning and Features Engineering*. https://doi.org/10.1155/2022/5280158

Simon Applebaum, Tarek Gaber, Ali Ahmed (2021), *Signature-based and Machine-Learning-based Web Application Firewalls: A Short Survey*. https://doi.org/10.1016/j.procs.2021.05.105

C. Liu (2020). *An Active Response Mechanism for Web Application Firewalls*. http://dx.doi.org/10.1109/COMPSAC.2018.00144

Cho Do Xuan, Nam Nguyen, Hoa Nguyen Dinha (2020). *An adaptive anomaly request detection framework based on dynamic web application profiles.* http://doi.org/10.11591/ijece.v10i5.pp5335-5346

Davide Chicco, Matthius J. Warrens, and Giusepe Jurman (2020). *The Matthews correlation coefficient (MCC) is more informative than Cohen's Kappa and Brier score in binary classification assessment*. http://dx.doi.org/10.1109/ACCESS.2021.3084050

Xu, G., Wang, Y., & Xu, Y. (2019). Anomaly Detection in Cyber-Physical Systems Using Machine Learning Algorithms.

Saher Manaseer, Ahmad K Al Hwaitat (2018). *Centralized Web Application Firewall Security System*. http://dx.doi.org/10.5539/mas.v12n10p164

Choi, H. J., & Han, D. H. (2018). *A Machine Learning Approach to SQL Injection Detection*. http://dx.doi.org/10.1109/ICECTA48151.2019.8959617

Sun Liangxu (2012). *Improve Aho-Corasick Algorithm for Multiple Patterns Matching Memory Efficiency Optimization*. http://dx.doi.org/10.4156/jcit.vol7.issue19.19

Li, X., Gao, J., & Ji, S. (2016). *SQLi Detecting SQL Injection Attacks Using Graph of Tokens and Random Forests*.