# Article information:

A Deep Learning Approach to Web Application Firewall | by Tarcísio Marinho | Medium
[https://medium.com/@tarcisioma/a-deep-learning-approach-to-web-application-firewall-c6190a9bd31a](https://medium.com/%40tarcisioma/a-deep-learning-approach-to-web-application-firewall-c6190a9bd31a)

# Article summary:

1. Web applications are vulnerable to attacks such as SQL injection, cross-site scripting, path traversal, file inclusion, remote code execution, and XML external entity.

2. Rule-based web application firewalls (WAFs) are not effective in identifying complex payloads used by hackers to exploit vulnerabilities.

3. A deep learning approach using a pre-trained transformer model achieved 96.5% accuracy in classifying malicious payloads and can be used to enhance the effectiveness of WAFs in protecting web applications.

# Article rating:

Appears moderately imbalanced: The article provides some useful information, but is missing several important points or pieces of evidence that would be required to present the discussed topics in a balanced and reliable way. You are encouraged to seek a more balanced perspective on the presented issues by exploring the provided research topics and looking at different information sources.

# Article analysis:

The article "A Deep Learning Approach to Web Application Firewall" by Tarcísio Marinho discusses the use of deep learning and Transformer models in identifying malicious payloads in web applications. The author highlights the vulnerabilities that web applications face, such as SQL injection, cross-site scripting, path traversal, file inclusion, remote code execution, and XML external entity attacks. The article explains how rule-based web application firewalls (WAFs) are not effective in mitigating these attacks due to evasion techniques used by hackers.

The author presents a dataset of 44,299 samples from eight distinct classes, including six malicious payload classes and two non-malicious classes. The training approach involved fine-tuning a pre-trained transformer language model using Tensorflow and Ktrain libraries. The trained model achieved an average accuracy of 0.96 at classification tasks.

While the article provides valuable insights into the use of deep learning for identifying malicious payloads in web applications, it has some limitations. Firstly, the proposed solution only classifies six vulnerability classes among a vast list of web application vulnerabilities. Secondly, the proposed solution was not implemented or evaluated at a commercial or open-source WAF to test its accuracy on a real-world scenario.

The article also lacks evidence for some claims made by the author. For instance, while the author claims that deep learning outperforms classical machine learning approaches such as LSTM and SVMs in classifying text data, no evidence is provided to support this claim.

Moreover, the article does not explore counterarguments or present both sides equally. For example, while the author highlights the limitations of rule-based WAFs in mitigating web application attacks due to evasion techniques used by hackers, no mention is made of any potential risks associated with using deep learning models for identifying malicious payloads.

In conclusion, while "A Deep Learning Approach to Web Application Firewall" provides valuable insights into using deep learning for identifying malicious payloads in web applications, it has some limitations and lacks evidence for some claims made by the author. The article could benefit from exploring counterarguments and presenting both sides equally to provide a more balanced perspective on the topic.

# Topics for further research:

* Risks associated with using deep learning models for web application security
* Comparison of deep learning and classical machine learning approaches for text classification
* Other types of web application vulnerabilities beyond the six identified in the article
* Evaluation of deep learning models for web application security in real-world scenarios
* Limitations of using pre-trained transformer language models for web application security
* Ethical considerations in using deep learning for web application security

# Report location:

<https://www.fullpicture.app/item/24c795608bca57e9f32bc7fcc9d0e9eb>