

Paper Title:

Detecting SQL Injection Attack using Natural Language Processing

Paper Link:

<https://ieeexplore.ieee.org/document/9986458>

1 Summary**1.1 Motivation**

The study was motivated by the increasing severity of web application SQL injection attacks. In order to overcome this problem, the paper uses NLP and BERT to increase feature extraction. It is hypothesized that this strategy will provide more accuracy than conventional techniques.

1.2 Contribution

The contribution is in the form of a new methodology for SQL injection attack detection that combines NLP and BERT. A significant improvement over the shortcomings of previous methods is indicated by the 97% accuracy that was attained.

1.3 Methodology

The methodology involves the use of BERT, a bidirectional contextual learning model, for feature extraction. The authors use a classifier layer for binary classification, preprocess the dataset, and optimize BERT on the given SQL injection dataset. Traditional classifiers such as K-Nearest Neighbors, Support Vector Machine, Gaussian Naive Bayes, Decision Tree, and Logistic Regression are outperformed by the suggested model.

1.4 Conclusion

The study comes to the conclusion that online application security is seriously threatened by SQL injection attacks. With a 97% accuracy rate, the suggested strategy which combines NLP and BERT shows encouraging results, highlighting the superiority of machine learning-based solutions over conventional techniques.

2 Limitations**2.1 First Limitation**

Despite the great accuracy of the suggested model, there may be a diversity issue with the datasets. For the purpose of ensuring the model's robustness, more research should be done on how well it works in different kinds of online applications and SQL injection scenarios.

2.2 Second Limitation

The computational expense of pre-training BERT is another drawback. The feasibility and scalability of applying the suggested approach in actual situations should be covered in the article, particularly for resource-constrained enterprises.

3 Synthesis

The concepts discussed in the study provide directions for future investigation and useful applications. The combination of NLP and BERT for SQL injection detection raises more questions about how to improve online application security in general. Subsequent investigations could investigate merging many NLP models and broadening the scope of the research to encompass query languages other than SQL.