General Conclusion

This project has made significant contributions to the field of web application security by employing BERT for the detection of SQL injections. The primary contribution of our work lies in demonstrating the effectiveness of BERT in accurately identifying SQL injection attempts in real-time. By exploiting the contextual understanding and semantic representation capabilities of BERT, we have achieved superior performance compared to other machine learning models. Our results provide valuable insights into the application of deep learning techniques for mitigating the major risk of SQL injections on web applications.

Despite the promising results obtained, our work has certain limitations that should be admitted. Firstly, the dataset used for training and evaluation, while comprehensive, may not be large enough to fully exploit the potential of BERT. With larger datasets, BERT's ability to capture complex patterns and nuances could be further enhanced. Secondly, we acknowledge that our experiments were conducted in a controlled environment, and the model was not tested or employed in a real-world scenario.

Based on our analysis of the BERT-based model for SQL injection detection, there are several recommendations and future directions to further enhance its capabilities:

- Explore a larger and more diverse dataset. A larger and more diverse dataset will help the model to learn more about different attack scenarios and improve its performance.
- Investigate the model's performance in real-world scenarios. The model's performance in real-world scenarios should be investigated to understand its limitations. This can be done by deploying the model in a production environment and monitoring its performance.
- Continuously update the model with new attack patterns. The model should be continuously updated with new attack patterns to improve its accuracy in detecting new attacks.
- Expand the scope to detect and classify various types of cyber attacks. The scope of the model can be expanded to detect and classify various types of cyber attacks such as Cross-site scripting (XSS) and Cross-Site Request Forgery (CSRF) using a multi-classification model. This will provide a more comprehensive approach to threat detection and mitigation in cybersecurity.

By addressing these recommendations and future directions, we can advance the field of SQL injection detection and contribute to the development of more effective security solutions.