Web applications became a critical part of our routine, supporting everything from e-commerce via social networks and banking to even healthcare services. Their spread has brought about a revolutionary change in the way we relate to each other, communicate, and do business. At the same time, this growing dependency on web platforms also makes them very attractive targets for cyberattacks. Among these threats, SQL injection remains the highest and most dangerous vulnerability, posing a few severe dangers to data security and user privacy.  
To counter SQL injection attacks, input validation and parameterization of queries have been used as base security measures, in addition to the extra firewalls for protection. While some of these older techniques can protect against risks, many examples of detection have eluded them when it comes to smarter and ever-evolving attacks. Given the very dynamic trends in the cyber world, there lies a need for more advanced and flexible measures for detecting real-time malicious SQL queries.  
Modern breakthroughs in AI and deep learning have created new room for cybersecurity with intelligent models capable of learning and adapting toward highly complex patterns of attack behavior. Among them, transformer architectures, especially BERT (Bidirectional Encoder Representations from Transformers), can truly be said to stand out in their ability to understand textual patterns and contextual relationships. Although intended for NLP tasks, BERT has potential applications in cybersecurity, including intrusion detection and malice query classification.  
This research aims to apply deep learning techniques to establish an intelligent detection system for SQL injection. The focus of training on real-world datasets is to create a highly robust detection framework that distinguishes between legitimate SQL queries and malicious ones with great precision. The principal advantage of our method is its ability to dynamically adapt to new attack patterns, thus adding enhanced security to web applications, unlike the conventional rule-based approach.  
Chapter 1 introduces SQL injection attacks, covering definitions, types, real-world examples, and traditional detection methods.  
  
Chapter 2 explains key concepts in Machine Learning and Deep Learning and presents the neural network architectures used in our experiments.  
  
Chapter 3 describes the dataset, preprocessing steps, and technical details, including model architectures and hyperparameters.  
  
Chapter 4 presents and analyzes the results using various evaluation metrics and discusses model performance.  
  
Through this study, we aim to demonstrate the effectiveness of deep learning techniques in cybersecurity, particularly for the early detection of SQL injection attacks.

**Conclusion chapiter 4**

This chapter presented a detailed evaluation of various models for SQL injection detection. Traditional approaches such as SVM and Logistic Regression achieved strong results. However, deep learning methods, particularly LSTM and BERT, performed even better. BERT achieved outstanding performance, with an accuracy of 99.92 percent and a recall of 100 percent on the test set. It also showed excellent generalization on unseen data. These results confirm that transformer-based architectures are highly effective in accurately and reliably detecting SQL injection attacks

**Conclusion generale**

**General Conclusion**

In this thesis, we studied the problem of SQL Injection attacks, which are among the most common and dangerous threats to web applications. We explored different approaches to detect these attacks using both traditional machine learning models and deep learning techniques.

Our experiments showed that classical models such as Logistic Regression and SVM gave good results when using proper text preprocessing and vectorization. However, deep learning models performed better. Among them, BERT, a pre-trained language model based on the Transformer architecture, achieved the best performance. It reached very high accuracy and recall, even when tested on new and unseen data.

These results confirm the strong potential of deep learning in the field of cybersecurity. BERT’s ability to understand the context and meaning of queries makes it especially suited for detecting malicious SQL statements. Its success in this task shows that language models can play a key role in building more secure web applications.

Even if the results are promising, future work could involve testing the model in real-world environments, increasing the size and diversity of the dataset, and adapting the system to detect other types of attacks. This would make the solution more robust and useful in practice.

To conclude, this work proves that modern deep learning models like BERT are powerful tools for improving web security. They offer a high level of precision and can help in building smarter and more adaptive defense systems against SQL Injection attacks