**OBJECTIVE OF THE PROJECT**

The prevalence of SQL injection attacks poses a significant threat to the security and integrity of databases, leading to data breaches, financial losses, and reputational damage for organizations. SQL Injection (SQLI) is type of cyber-attack that has been around for a long time. SQLI was considered as the one of the top 10 web application vulnerabilities between 2007 to 2010 by the Open Web Application Security Project.

Traditional methods of detecting SQL injection attacks often rely on various methods like parameterized queries, Input validation, Signature based detection, Syntax based analysis, Anomaly detection which are limited in their ability to detect novel and sophisticated attack variants. Moreover, manual inspection of SQL queries and database logs is labor-intensive, error-prone, and impractical for large-scale systems, leading to delays in incident response and increased exposure to cyber threats. This highlights the pressing need for automated, intelligent solutions that can analyze and interpret the vast amounts of textual data associated with database activities in real-time, enabling early detection and prevention of malicious SQL code.

The emergence of artificial intelligence (AI) and natural language processing (NLP) technologies offers promising avenues for enhancing the detection and prediction of malicious SQL code in databases. By leveraging AI algorithms and machine learning techniques, NLP systems can effectively parse, interpret, and understand the semantics and syntax of SQL queries, enabling them to distinguish between legitimate and potentially harmful database interactions. This presents a compelling research opportunity to explore the application of cutting-edge AI techniques in the domain of cybersecurity, with the aim of developing more robust and adaptive defense mechanisms against SQL injection attack.