SOURCE CODE VULNERABILITY SCAN USING AI

7COM1039-0509-2022 - Advanced Computer Science Masters Project

Vineeth Gopinadhan

21059965 | University of Hertfordshire

Aim

The aim of this project is to develop an intelligent system that utilizes artificial intelligence (AI) techniques to perform automated vulnerability scans on source code. The system will assist developers and security professionals in identifying potential vulnerabilities in software code, allowing for timely detection and mitigation of security risks.

Research questions/hypothesis

1. Can AI algorithms effectively identify and classify different types of vulnerabilities in source code?
2. How can the performance and accuracy of AI-based vulnerability scanning be optimized?
3. What are the potential challenges and limitations of using AI for source code vulnerability scanning?
4. How does the AI-based vulnerability scanning approach compare to traditional manual code review techniques in terms of effectiveness and efficiency?

Objectives

1. Analyse existing vulnerability scanning techniques and tools to understand their limitations and potential areas of improvement.
2. Develop an AI-based algorithm capable of identifying and classifying different types of vulnerabilities in source code.
3. Design and implement a software system that integrates the AI algorithm for vulnerability scanning.
4. Evaluate the performance and effectiveness of the AI-based vulnerability scanning system through experimentation and comparative analysis.
5. Identify and address the challenges and limitations of the AI approach in source code vulnerability scanning.

Short description

The proposed project aims to leverage the power of AI to automate the process of vulnerability scanning in software source code. By training machine learning models on large datasets of known vulnerabilities, the system will be able to identify patterns and indicators of potential security weaknesses in code. This will provide developers and security professionals with a valuable tool to enhance the security posture of software applications. The AI-based vulnerability scanning system will involve pre-processing and feature extraction steps to analyse the source code. Machine learning algorithms, such as deep learning models or natural language processing techniques, will be employed to learn from labelled datasets of known vulnerabilities and build a predictive model. The system will then use this model to scan new source code and generate reports highlighting potential vulnerabilities.

Research Plan

1. Review existing literature and research papers on vulnerability scanning techniques, AI applications in cybersecurity, and source code analysis.
2. Identify and collect datasets of known vulnerabilities in source code for training and evaluation purposes.
3. Design and implement the AI algorithm for vulnerability scanning, utilizing appropriate machine learning techniques and programming languages.
4. Develop a software system that integrates the AI algorithm and provides a user-friendly interface for code scanning and vulnerability reporting.
5. Conduct experiments and performance evaluations using benchmark datasets and real-world code samples to assess the accuracy, efficiency, and effectiveness of the AI-based vulnerability scanning system.
6. Compare the results of the AI approach with traditional manual code review techniques to determine its advantages and limitations.
7. Analyse and interpret the findings, identifying potential areas for improvement and addressing challenges in the AI-based vulnerability scanning process.
8. Document the research process, results, and conclusions in a comprehensive report, adhering to academic standards and guidelines.