AI Security Code Review for CI Pipelines

Jul 19 2023

Executive Summary

This project aims to develop an AI-powered tool that will be integrated into Continuous Integration (CI) pipelines to analyze code for security vulnerabilities. The tool will examine the code changes, identify codebase relevant to the changes and analyze them together for potential security risks. By automating this process, we aim to improve the security minimum in software development, reduce the time and resources spent on manual code reviews, and ultimately contribute to a safer digital environment. CI pipelines are a common practice in software development, and the tool will integrate seamlessly into existing pipelines without disruption to the current workflow, providing real value to our users and acting as a force multiplier to the development teams. We estimate a total budget of $21,420 in API credits and $90,000 in funding for a total of $111,420. We expect to complete the project in 8 months, with an expected completion date of April 1, 2024.

Contents

Executive Summary **1**

Introduction **3**

Objectives **3**

Methodology **4**

Expected Results **4**

Timeline **5**

Budget **5**

API Credits 5

Funding 6

Conclusion **6**

Introduction

In an era where digital threats are increasingly sophisticated, the need for hightened cybersecurity measures is paramount. Our project aims to leverage the power of artificial intelligence to enhance the security of software during development.

Code reviews are an essential part of the software development process, but they are often dreaded by developers. They are time-consuming and can often be the bottleneck in the release cycle. By automating the process of code reviews, we can significantly reduce the time and resources spent on manual reviews and we can guarantee a minimum of security by providing the development team with actionable suggestions.

In this research project we seek to address key questions such as: How can we automate the process of identifying security vulnerabilities in code changes? Can an AI-powered tool effectively and accurately identify potential security risks? How can we integrate this tool into existing CI pipelines with minimal disruption to the current workflow? And, what impact will this tool have on the overall security of the software and the efficiency of the development process? By addressing these questions, we aim to contribute significantly to the field of AI-powered cybersecurity.

Objectives

Our project has several specific objectives. First, we aim to develop an AI-powered tool that can automatically identify security vulnerabilities in code changes and provide actionable recommendations to developers. Second, we strive to ensure that this tool can be effectively and accurately integrated into existing CI pipelines, with several open-source example implementations into popular CI pipelines like Github Actions, GitLab, etc. Third, we aim to measure the impact of this tool on the overall security of the software and the efficiency of the development process. Each of these objectives is designed to be Specific,

Measurable, Achievable, Relevant, and Time-bound (SMART), ensuring that we have clear goals to work towards and can accurately measure our progress.

Methodology

Our methodology involves using Large Language Models (LLMs) to identify security vulnerabilities in code. Because of the importance of context size we have decided to use OpenAI gpt4-32k model. We will collect and label data from various open-source projects and use this data to validate our methods. The tool will be designed to integrate seamlessly into existing CI pipelines by providing both a Python library and a command line tool, both having ample support in the AI and software development community. There it will analyze changes in code, identify code relevant to the changes, and analyze them together for potential security risks. We anticipate challenges such as ensuring the accuracy of our model, identifying relevant code in different programing languages and meassuring results. We plan to address these through rigorous testing and iterative development. In the long term we plan to build a larger secure development dataset and explore fine-tunning a model, to be able to identify security vulnerabilities with higher accuracy, faster response time and less costs.

Expected Results

We anticipate several key outcomes from this project. The primary result will be a fully functional AI-powered security reviewer that can be integrated into CI pipelines. This tool will automate the process of identifying security vulnerabilities in code changes and provide actionable recommendations to developers, significantly reducing the time and resources spent on manual code reviews. Additionally, we will provide several open-source example implementations of the tool integration into popular CI pipelines (like Github Actions,

GitLab, etc.). This will demonstrate the versatility of our tool and its compatibility with various CI pipelines. We expect an improvement in the overall security of the software developed incorporating our tool. We will measure these outcomes through metrics such as the total number of vulnerabilities identified and corrected, the detection rate and the false alarm rate. We expect time savings from MR creation until merge to be substantial, and a noticeable reduction in security incidents related to reviewed code.

Timeline

We propose a timeline of 8 months for this project, with an expected completion date of April 1, 2024. Key milestones will include the collection and labeling of training data (Month 1-2), the development and initial testing of the AI model (Month 3-4), the integration of the tool into CI pipelines and further testing (Month 5-6), and the final refinement and launch of the tool (Month 7-8). This timeline allows for potential delays and ensures that we have sufficient time to thoroughly test and refine the tool before launch.

Budget

The total budget of $111,420 including API credits and funding will cover costs such as data collection and labeling, development and testing of the AI model, and integration of the tool into CI pipelines.

API Credits

We estimate a total of 315,000,000 prompt tokens for the development and testing phase, costing approximately $18,900. Additionally, we estimate 21,000,000 sampled tokens for providing suggestions, costing approximately $2,520. These costs are based on the prices for GPT-4-32k, which are $0.06/1k prompt tokens and $0.12/1k sampled tokens. We used

the following estimates: 15 tokens per line of code (LoC), 300 LoC changed per MR and 10 times that for context, 50 MR per development day and a development timeline of 6 months. For sampling we estimate 350 tokens per suggestion, up to 5 suggestions per MR and the same ammount for intermediate results. This assumes no token usage during early data collection and final launch phases. Total requirement $18,900 + $2,520 = $21,420.

Funding

Two researchers will be working on this project full-time for 8 months. We estimate a total cost of $80,000 for salaries, based on a salary of $5,000 per month per researcher. We expect researchers to generally bring their own hardware for development and use OpenAI API for inference, so we do not expect extra costs in hardware, software or servers. Finally, we will require a budget of $10,000 for miscellaneous expenses, including conference tickets, travel, accommodation, and other unexpected costs. This brings the total budget to $90,000.

Conclusion

In conclusion, our project “AI Security Code Review for CI Pipelines” aims to significantly enhance the security of software development by automating the process of identifying security vulnerabilities in code changes. By leveraging the power of AI, we can reduce the time and resources spent on manual code reviews and improve development speed and the overall security of the software. We are grateful for the opportunity to submit this proposal and look forward to the possibility of contributing to the field of AI-powered cybersecurity.