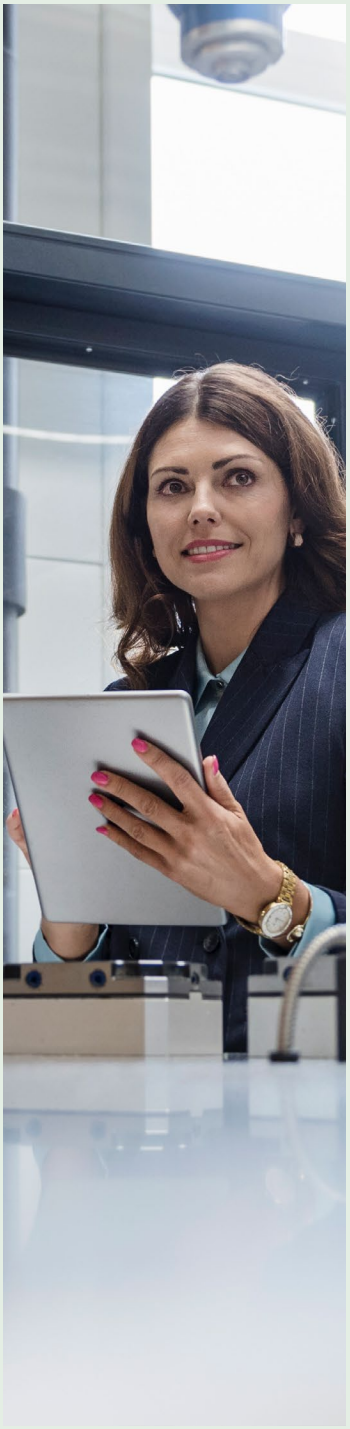
WHITE PAPER



ROLE OF GENERATIVE AI IN SECURITY TESTING

Abstract

Artificial Intelligence (AI) has emerged as a transformative technology in various sectors, including Cyber Security. This whitepaper explores the use of AI to enhance security through Static Application Security Testing (SAST) and Software Composition Analysis (SCA) scans using Python scripts. It also talks about generating Software Bill of Materials (SBOM), and licensing information of the different components used. It addresses the benefit and challenges, backed by a proof of concept (POC) to validate its potential.

Infosys®
Navigate your next

Overview and Industry Problem

This paper aims to address the following challenges with traditional security assessment tools:

Multiple Tools and Fragmented Processes

Using multiple tools for security assessments increases complexity, overhead costs, and management challenges. This fragmented approach needs improvement.

Integration and Compatibility Issues

Different security tools often lack compatibility, leading to inefficiencies and inconsistencies in evaluations.

Complex decision making and Human error factor

Employing various tools can result in overlapping or conflicting results, requiring time-consuming manual analysis.

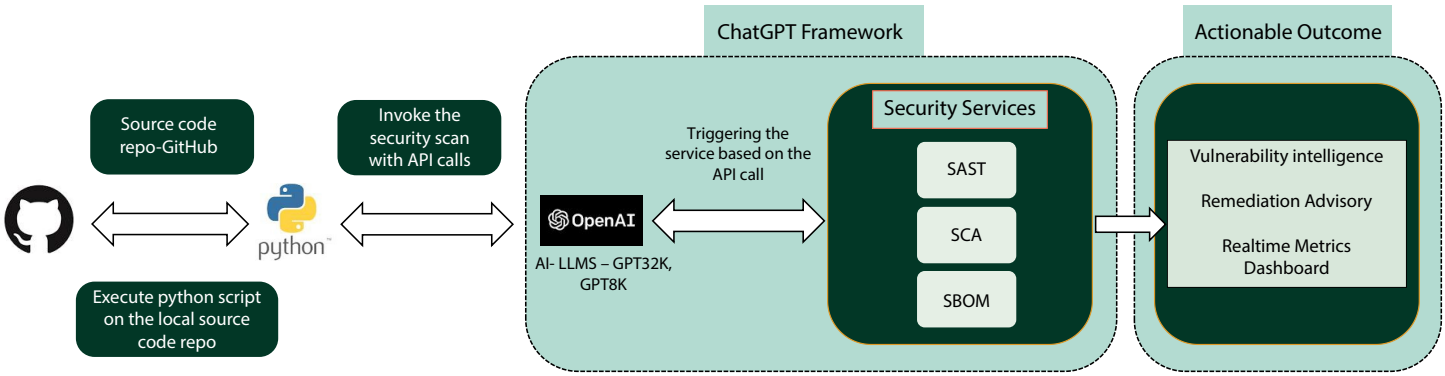
Proposed Solution: Unified AI Tool

Solution Overview

The paper proposes a unified AI command-line tool written in Python language as a solution to the challenges posed by traditional security assessment tools. The CLI tool uses OpenAI's GPT-4 8K/32K models to automate the security scanning (SAST & SCA) and generate SBOM report based on the user's choice, employing distinct prompts for each type of scanning.

Functional Architecture

As depicted in the diagram below, the Python script will invoke the security scan on the GitHub application source code folder by using API calls to the OpenAI's GPT-4 8K/32k models. Depending on the type of security scan selected (Static Application Security Testing (SAST), Software Composition Analysis (SCA) and SBOM issues), the OpenAI LLM will process the input prompt and will display the actionable outcome.

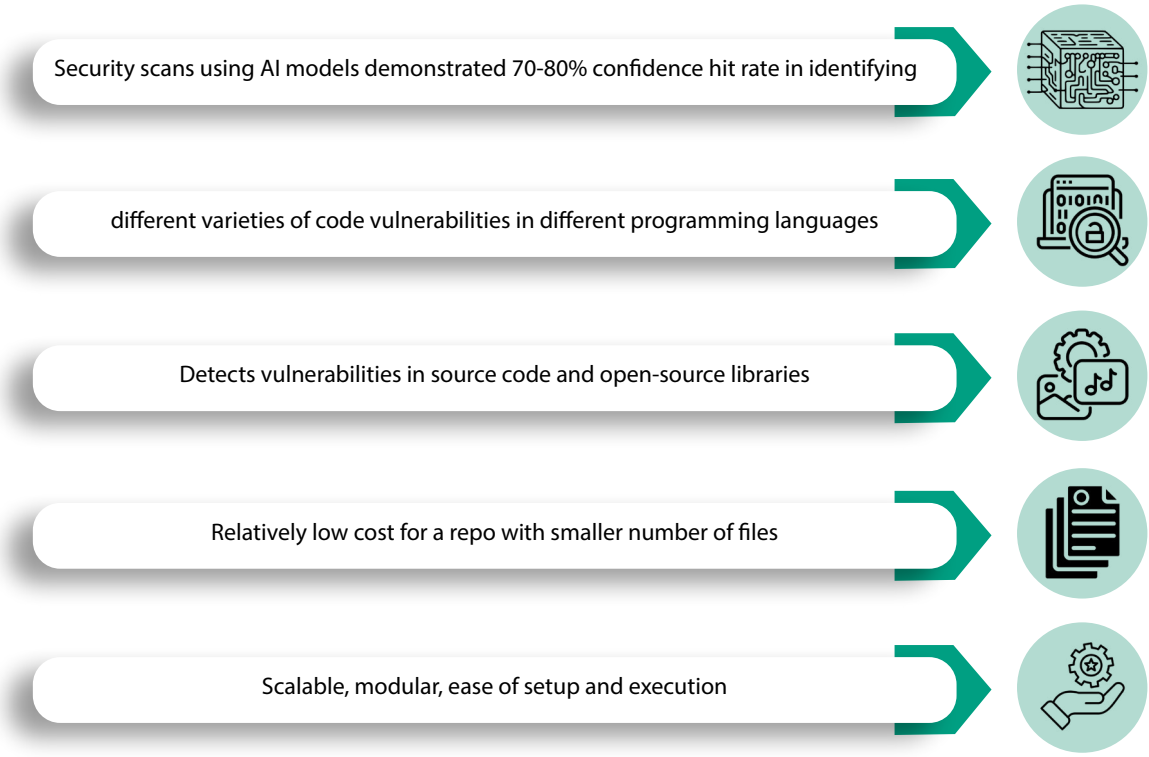


Upon scan completion, the CLI tool displays a summary of critical, high, medium, and low vulnerabilities identified for each scan type (SAST and SCA) in the console. It generates separate detailed reports for each scan in a text file simultaneously.

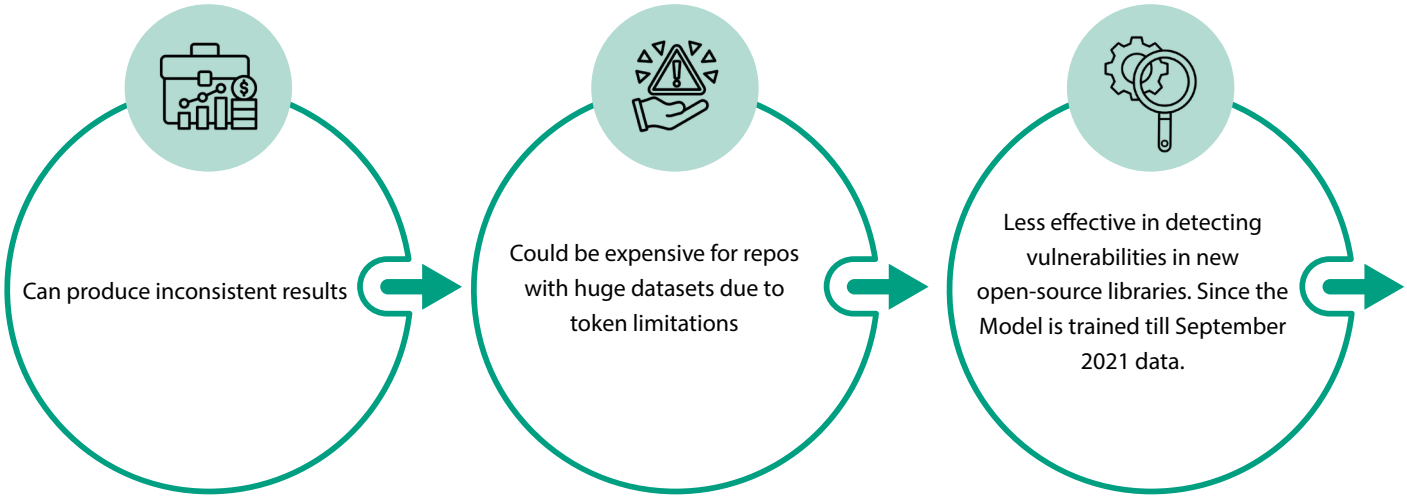
Inferences

Our testing involved running the python scripts for 10 iterations on multiple code languages such as .Net, Java and Python for SAST and SCA issues and then compared the security issues detected by standard SAST and SCA tools like SonarQube and Mend. Here are our findings.

Advantages:



Disadvantages:



Utilizing a unified AI tool for security assessments offers a practical solution to challenges posed by multiple tools. It streamlines processes, improves efficiency, and provides comprehensive reporting. While AI-driven technologies represent a significant advancement, AI models require further enhancements and data to replace traditional security tools fully. This generative AI-based approach in application security holds promise for the future, despite its current limitations.

References

https://platform.openai.com/docs/guides/gpt/chat-completions-api

About the Author

Abhijit Vaze

Abhijit is the Practice Lead for Vulnerability Management and Application Security with Infosys CyberSecurity. He has 26 years of experience in IT industry and 12 years in the domain of cyber security.

Satya Krishna

Satya works as a Principal Consultant with Infosys CyberSecurity. He has over 20 years of experience in IT industry, with over 8+ years of experience in security architecture reviews, threat modeling, web application security testing, penetration testing and vulnerability assessments.

Rakesh Ratheesan

Rakesh works as a Consultant with Infosys CyberSecurity. He has over 9 years of experience in IT industry across Application Security, Software Development, and Automation.

For more information, contact askus@infosys.com

Infosys®
Navigate your next