**基于Ghidra的自动化二进制漏洞分析工具项目**

**使用说明书说明书**

# 引言

随着软件应用程序的复杂性和数量的增加，二进制漏洞的发现和修复变得至关重要。传统的手动漏洞分析方法耗时且容易出错，因此需要一种自动化工具来加速漏洞检测和分析的过程。本项目旨在开发一款高效、准确且易于使用的二进制漏洞分析工具，以帮助安全专业人员和开发人员提高漏洞检测的效率和准确性。

该项目旨在开发一款强大的二进制漏洞分析工具，能够自动化检测和分析二进制程序中的漏洞，并提供相关的报告和建议。该工具将结合使用Ghidra反编译器、Semgrep分析工具和OpenAI模型，以提供全面的漏洞检测和代码分析功能。

# 安装部署

* OpenAI的API token 并且保存到config.txt中
* Ghidra
* Pip install Semgrep
* pip install -r requirements.txt
* 确保config.txt文件的正确路径

# 运行

运行：python callisto.py -b <path\_to\_binary> -ai -o <path\_to\_output\_file>

* -ai=> 启用 OpenAI GPT-3.5-Turbo Analysis。需要在配置.txt文件中放置一个有效的 OpenAI API 密钥
* -o=> 如果要保存输出，请定义输出文件
* -ai并且是可选参数-o
* -all将通过 OpenAI 分析运行所有功能，无论 Semgrep 的任何发现如何。此标志需要先决条件标志-ai
* 例如:python callisto.py -b vulnProgram.exe -ai -all -o results.txt