**基于Ghidra的自动化二进制漏洞分析工具项目**

**安装部署说明书**

# 引言

## 编写目的

安装部署说明书的编写目的是为了提供清晰的指导，使用户能够正确地安装、配置和部署软件或工具。它的主要目标是帮助用户快速、顺利地完成安装过程，并确保软件能够在用户的系统上正常运行。

## 软件背景

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。

# Ghidra安装

## JDK 17

安装 JDK 17 64-bit ，并且添加至环境变量

## Gradle

git clone https://github.com/gradle/gradle-completion ~/.zsh/gradle-completion

添加变量echo "\nfpath=($HOME/.zsh/gradle-completion \$fpath)" >> ~/.zshrc

## Gcc 和 G++

sudo apt-get install g++

sudo apt-get install gcc

## 安装Ghidra

git clone <https://github.com/NationalSecurityAgency/ghidra.git>

将其他构建依赖项下载到源储存库中gradle -I gradle/support/fetchDependencies.gradle init

创建开发版本gradle buildGhidra，位于build/dist/

# Semgrep

## 方法一 CLI入门

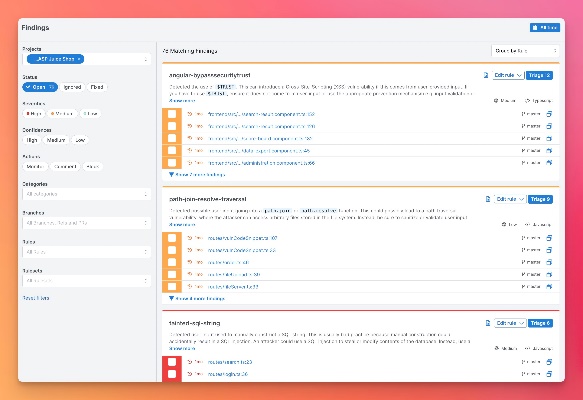
（1）安装 semgrep CLI

# For Ubuntu/WSL/Linux/macOS

python3 -m pip install semgrep

（2）转到应用的根目录并运行 。这将使用默认设置扫描您的项目。semgrep scan --config auto

## 方法二 semgrep云平台入门



* 注册以 [semgrep.dev](https://go.semgrep.dev/login-ghrmgo)
* 探索演示应用
* 通过导航到扫描项目Projects > Scan New Project > Run scan in CI
* 选择版本控制系统，然后按照向导添加项目。完成此设置后，Semgrep 将在每次拉取请求后扫描您的项目。
* 如果要在本地运行 Semgrep，请按照 CLI 部分中的步骤操作。

# Requirements

## WEB应用程序发布

Requirements.txt的内容：

openai==0.27.7

prettytable==3.8.0

tiktoken==0.4.0

pip install -r requirements.txt，一次性安装所有的依赖项

# OpenAI API

如果要使用 GPT-3.5-Turbo 功能，则必须在 OpenAI 上创建一个 API 令牌并保存到此文件夹中的 config.txt 文件中确保在文件中设置了 Ghidra 目录的正确路径config.txt