Тестирование уязвимостей с помощью SonarQube:

1. Для тестирования приложения нужно иметь:
- установленный Docker
2. Исходники:
- приложение: https://github.com/we45/Vulnerable-Flask-App.git
- создать файл в корневой директории проекта с именем - sonar-project.properties
- содержимое файла sonar-project.properties:

```
# must be unique in a given SonarQube instance
sonar.projectKey=my:project

# --- optional properties ---

# defaults to project key
#sonar.projectName=My project
# defaults to 'not provided'
#sonar.projectVersion=1.0

# Path is relative to the sonar-project.properties file. Defaults to .
#sonar.sources=.

# Encoding of the source code. Default is default system encoding
#sonar.sourceEncoding=UTF-8
```

- запросить images: docker pull sonarqube; docker pull sonarsource/sonar-scanner-cli
3. Запустить сервер:docker run -d --name sonarqube -p 9000:9000 server
4. Зайти из браузера на адрес http://ip_server:9000
5. Создать проект в админке (login/pw:admin/admin)
6. Получив токен от сервера просканировать проект: docker run --rm -e SONAR_HOST_URL="http://ip_server:9000" -v "/root/vuln/Vulnerable-Flask-App:/usr/src" sonarsource/sonar-scanner-cli