Домашняя работа № 5

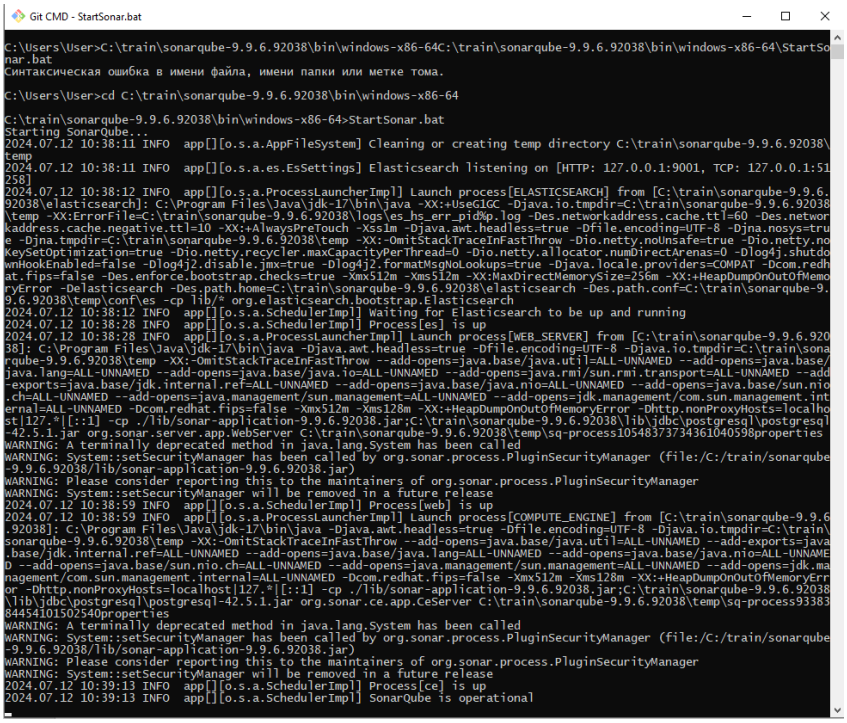
Выполнила Вишняк Евгения

1. По приведенным на скриншоте результатам сканирования Metasploit составить отчет по шаблону, выбрав CVE-уязвимости. Подробности о CVE можно найти на https://cve.mitre.org/ .
   Описание методики можно оставить из шаблона.
   Описания уязвимостей можно оставить на английском языке.
   Формат сдачи: документ на google drive.

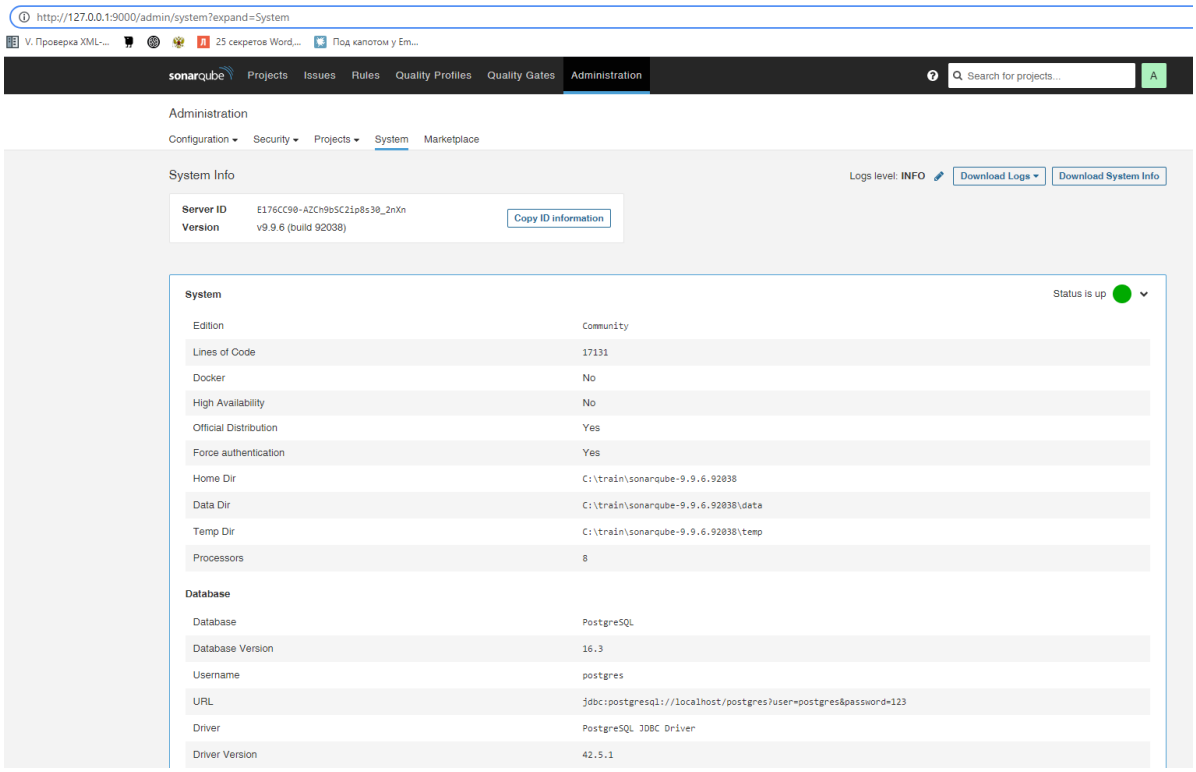
   Документ в формате pdf прилагаю к отчету.
   Ссылка на документ google drive:
   https://docs.google.com/document/d/1EZdthodobpJD3mCdSuir9tymr4ld-Fqx9HVF9gKy60g/edit?usp=sharing

2. Распаковать архив DVWA-master в подкаталог bin папки сканера. Запустить сканирование, дождаться окончания. По полученным результатам сканирования Sonarqube составить отчет по шаблону, выбрав CWE-уязвимости. Подробности о CWE можно найти на https://cwe.mitre.org/.
   Описание уязвимостей можно оставить на английском языке.
   Если вероятность эксплойта не указана, поле оставить пустым.
   В качестве решения прикрепить документ с отчетом.

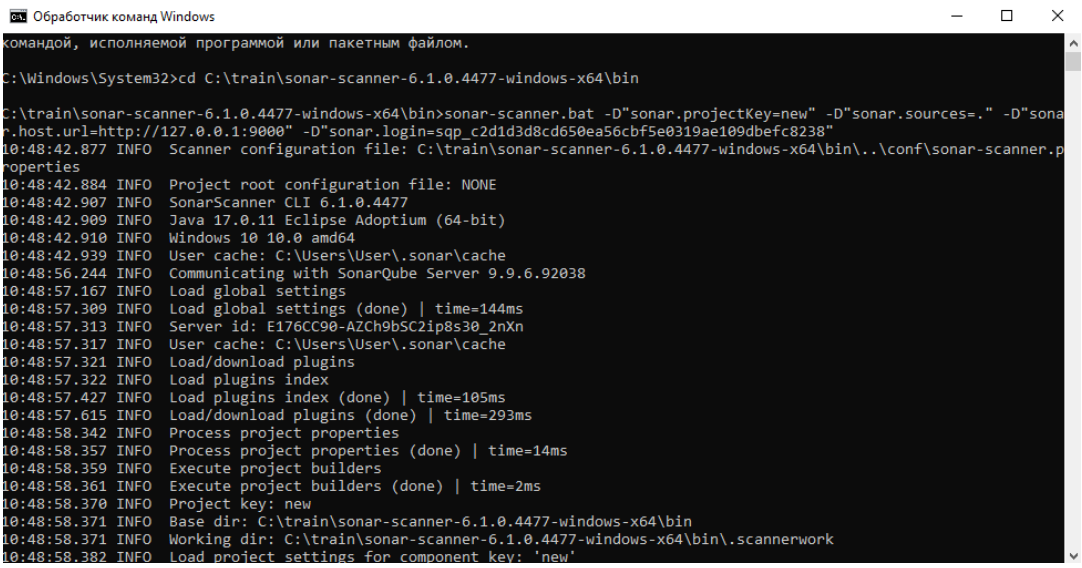
   Перед выполнением задания убеждаюсь в том, что в системе установлена jdk 17, а также postgresql и pgadmin4. В pgadmin4 запущен сервер localhost. Скачиваю и распаковываю архив DVWA-master в подкаталог bin папки сканера. Запускаю SonarQube в командной строке Git:



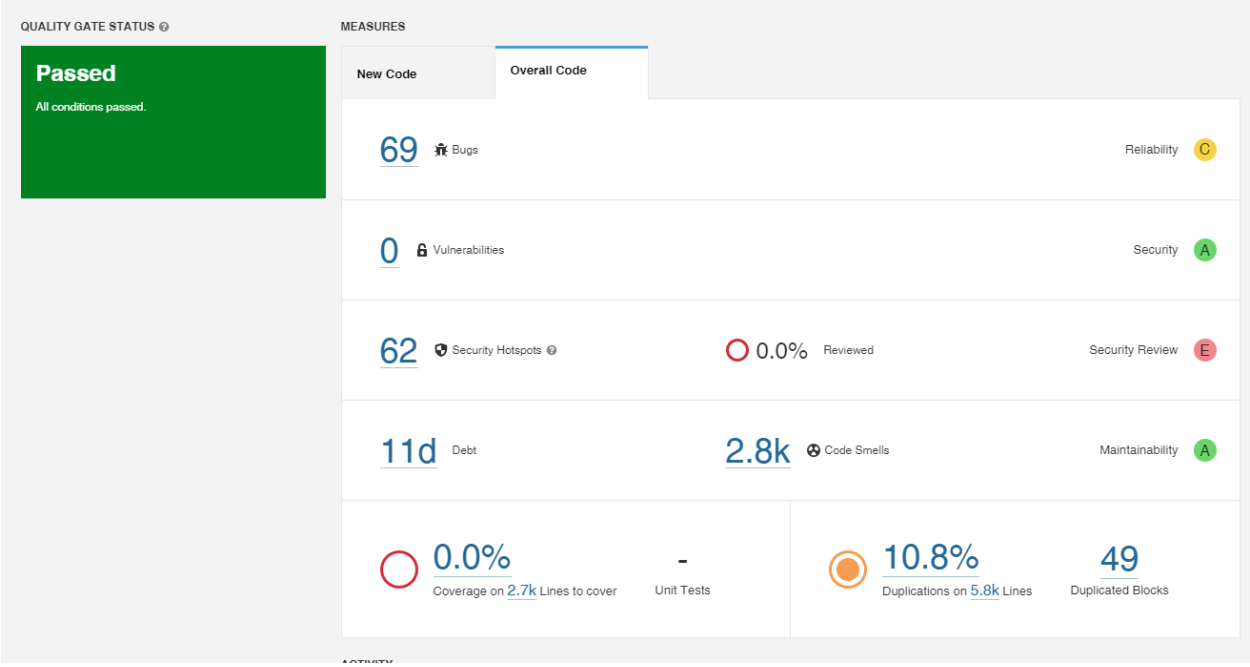
В браузере по ссылке http://127.0.0.1:9000/ открывается графический интерфейс SonarQube, база данных успешно подключилась:



Создаю новый проект. Копирую команду и запускаю ее в командной строке внутри папки, где расположен сканер:

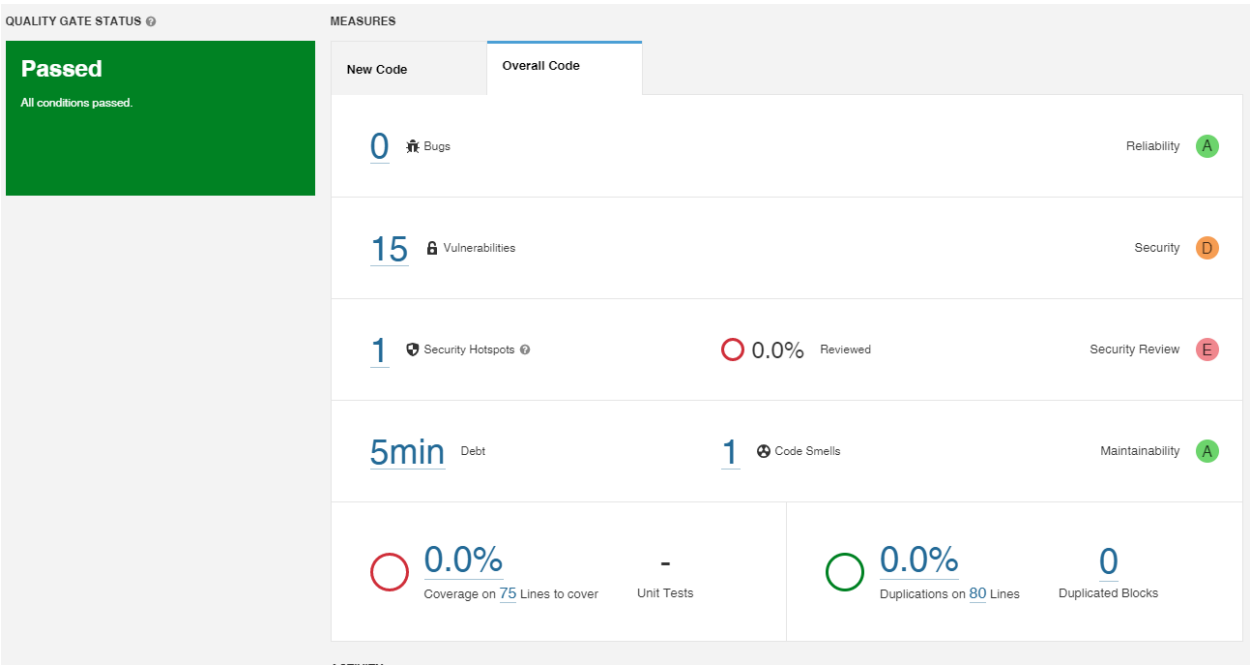


Жду, пока завершится сканирование, и возвращаюсь в веб-интерфейс:

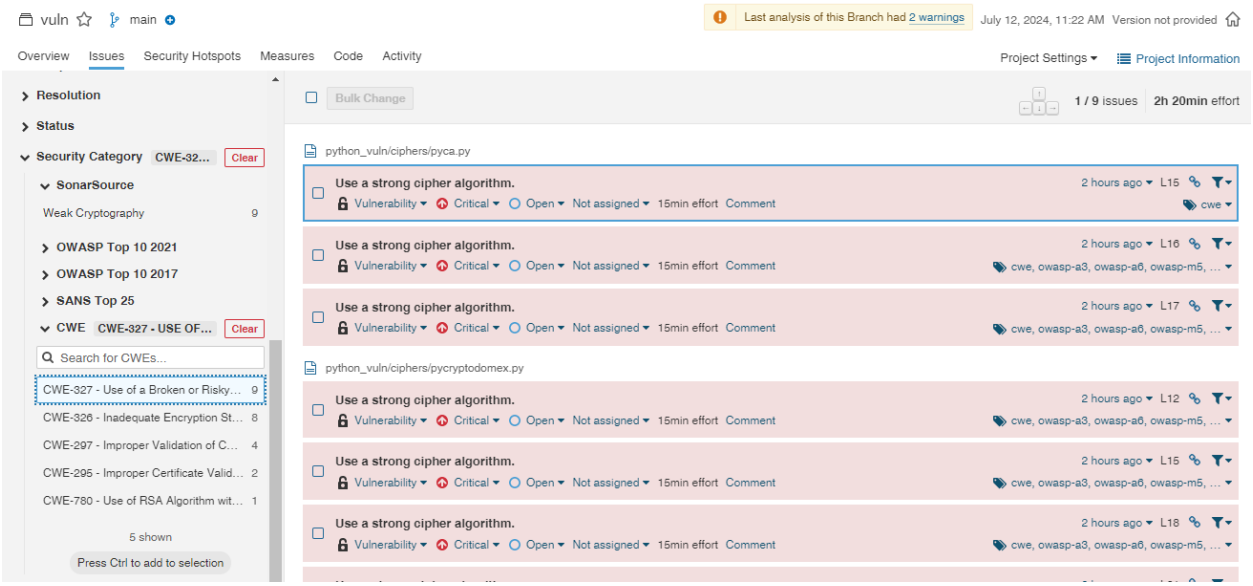


В результате сканирование прошло успешно, но уязвимостей не обнаружено. Сканирование данного архива было произведено на другой машине, с полной настройкой параметров и установкой необходимого программного обеспечения, но результат не изменился. Это подтверждает отсутствие в данном архиве уязвимостей.

Беру другой архив, python_vuln, и проделываю те же действия. Результат:



В разделе Issues можно найти подробную информацию о найденных CWE, а также их количестве:



Все найденные уязвимости описаны в отчете, документ в формате pdf прилагаю.
Ссылка на документ google drive:
https://docs.google.com/document/d/1v9UerqhvFkH1WeNyW1oKBuqX_vY82cecDZjRTefgUSw/edit?usp=sharing