|  |
| --- |
|  |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА - Российский технологический университет»**  **РТУ МИРЭА** |

РТУ МИРЭА г. Москва

Кафедра Информационно-аналитические системы кибербезопасности (КБ - 2)

**ОТЧЕТ О ВЫПОЛНЕНИИ ПРАКТИКИ № 1**

по дисциплине

«Проектирование и разработка безопасного программного обеспечения информационно-аналитических систем»

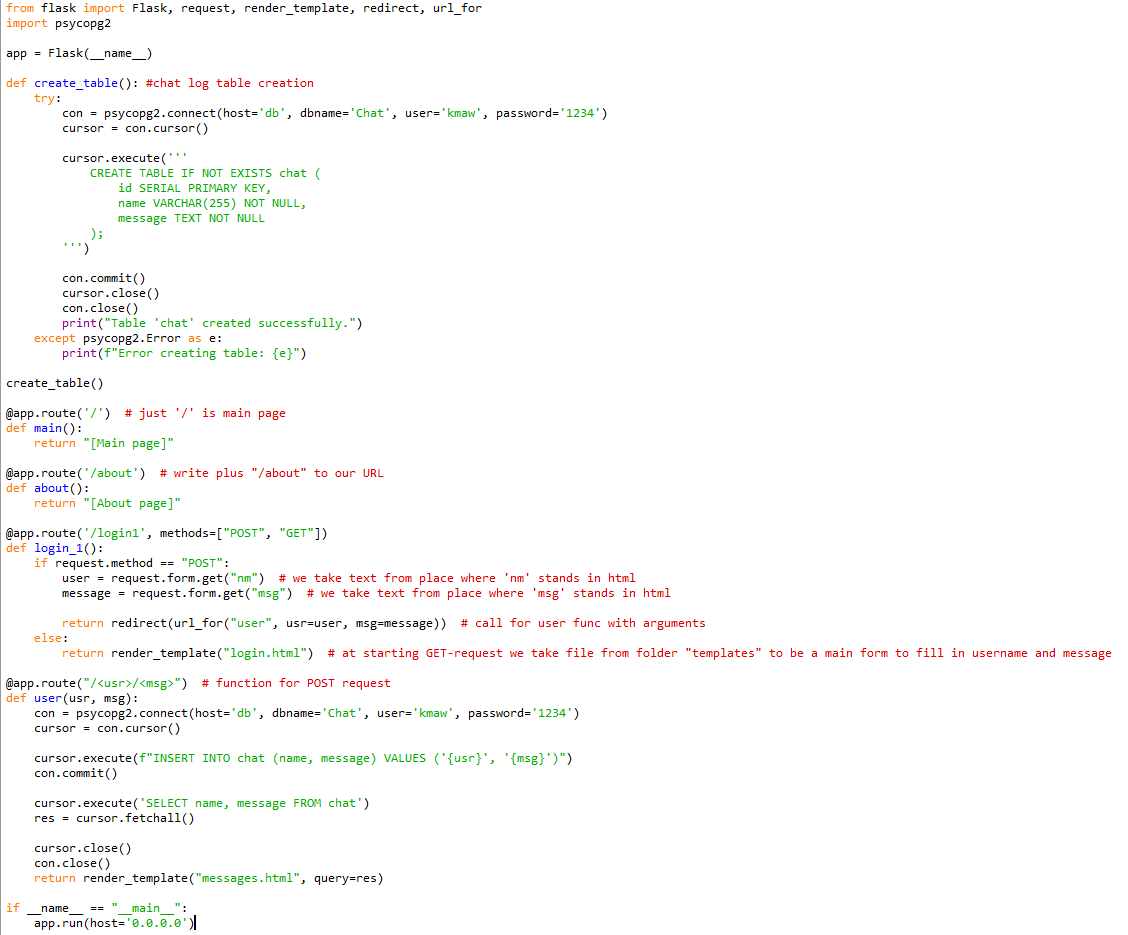
|  |  |
| --- | --- |
| Выполнил студент группы БИСО-03-19 | *Иванов Е. А.* |
| Принял | *доцент*  *Латыпов И. Т.* |

|  |  |
| --- | --- |
| Работа выполнена | «\_\_»\_\_\_\_\_\_\_2024г. |
|  |  |
| «Оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_» | «\_\_»\_\_\_\_\_\_\_2024г. |

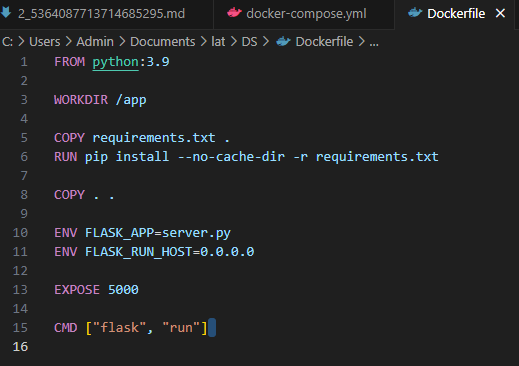
Москва 2024

Окружение представляет собой сайт «чата», написанный на Python с помощью фреймворка Flask. Сообщения из чата сохраняются в базу данных Postgres и выводятся при отправлении нового сообщения.

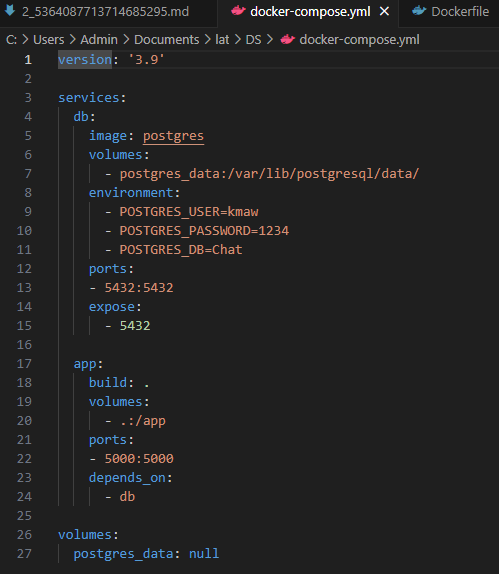
Код приложения на Python:

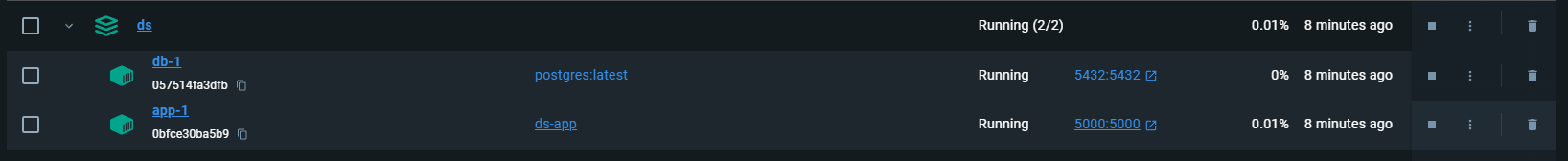


Dockerfile:

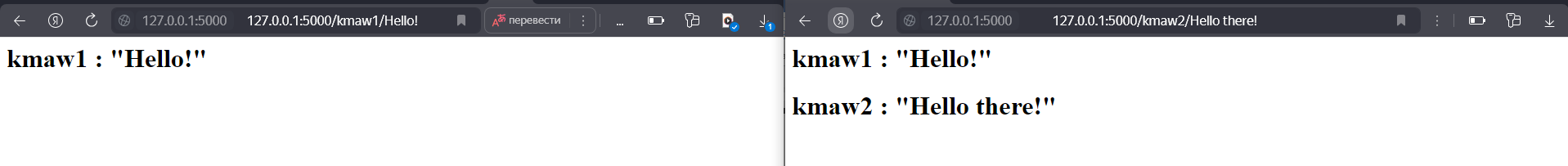
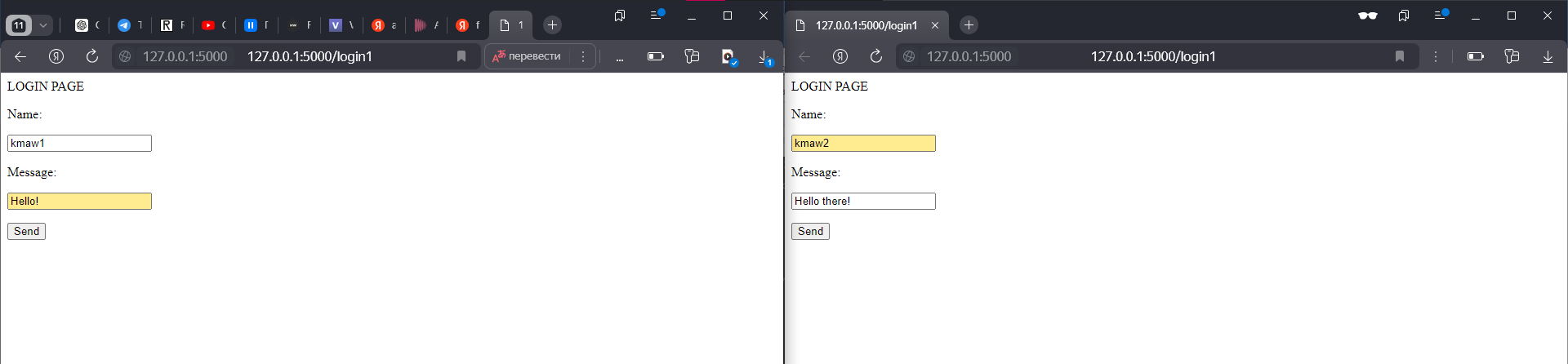


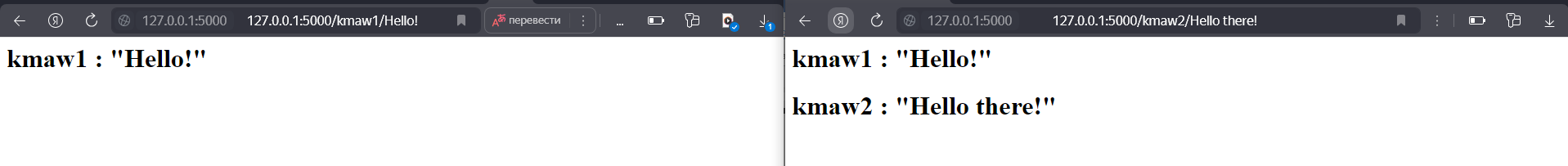
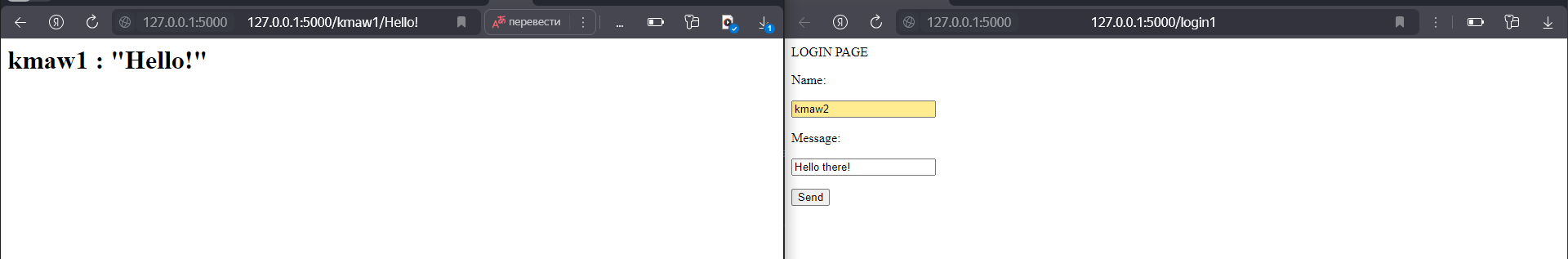
Docker-compose.yml для формирования единого контейнера из python-приложения и базы данных:





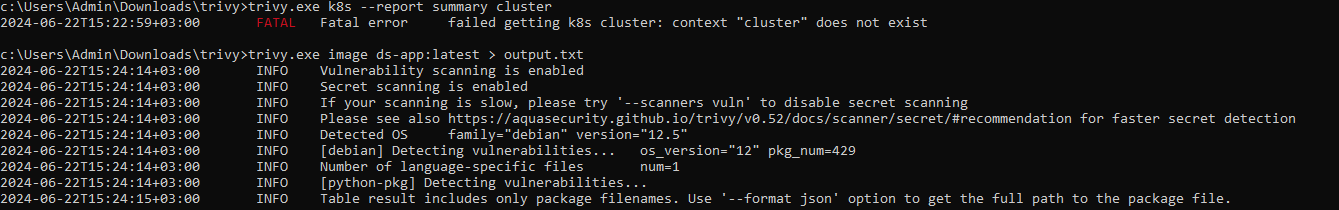
Скриншоты работы чата:



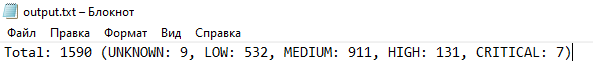


Проверка образа инструментом Trivy:

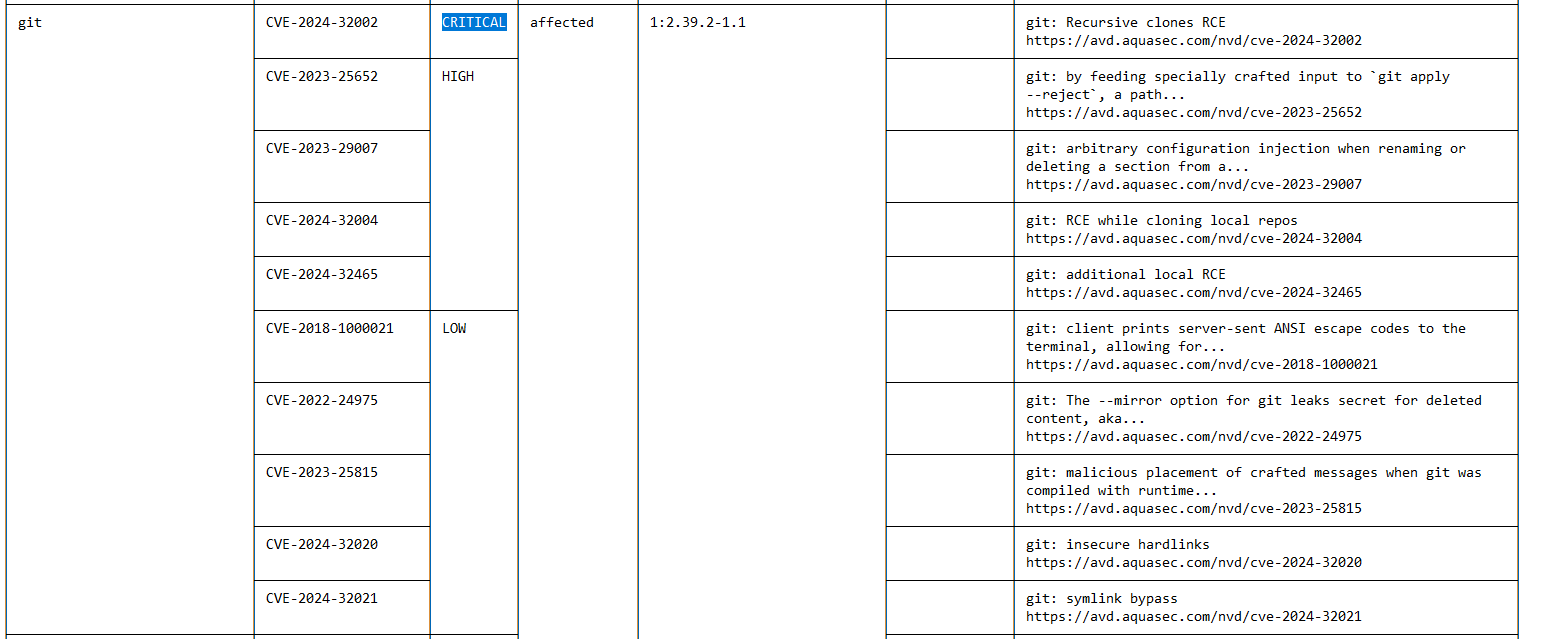
Для удобства сделаем вывод в отдельный текстовый файл:

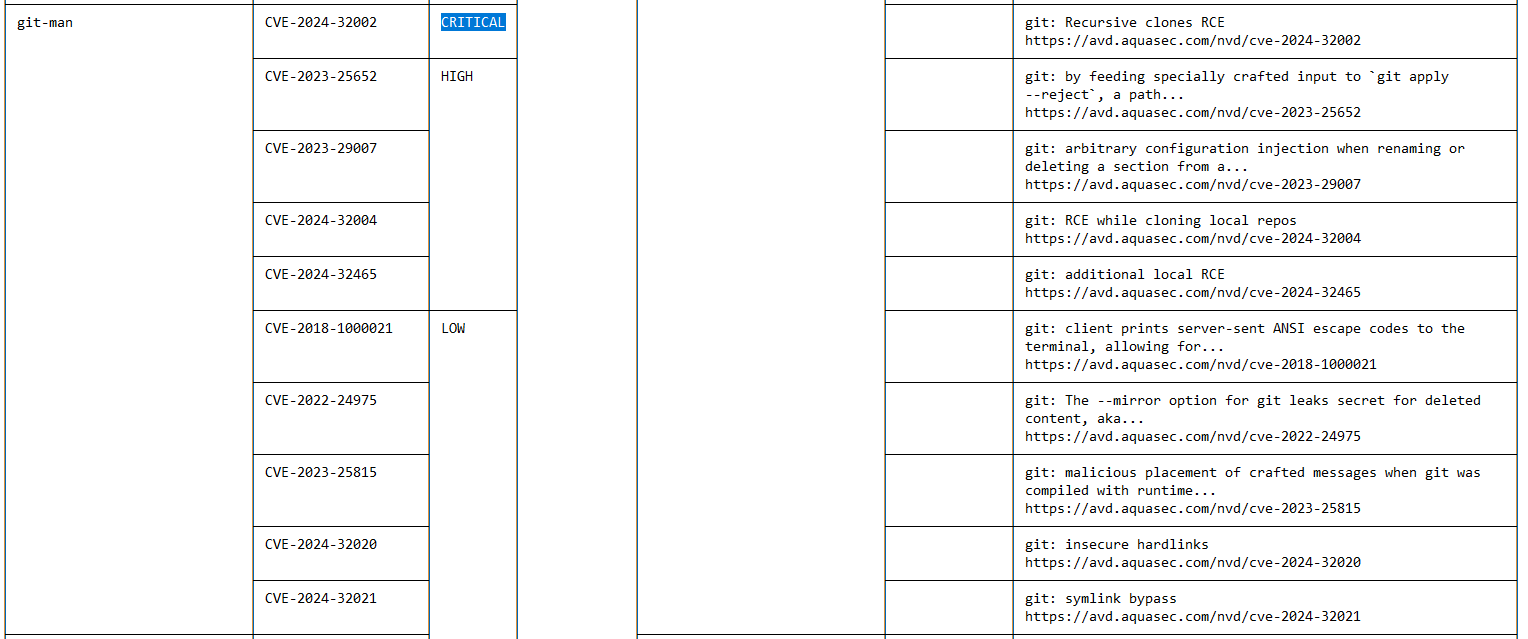


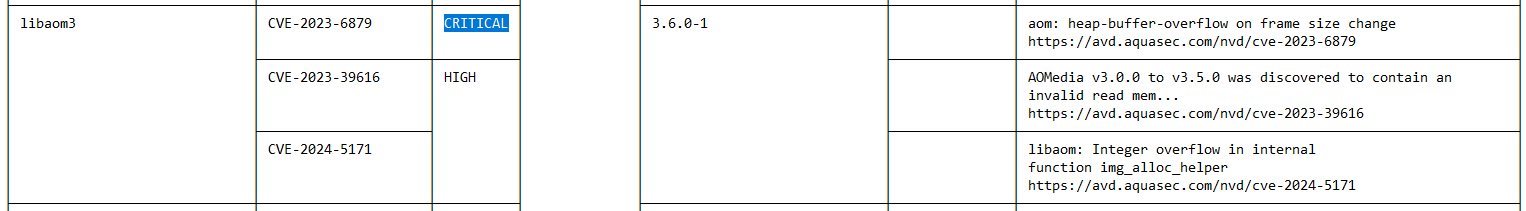
Результат:

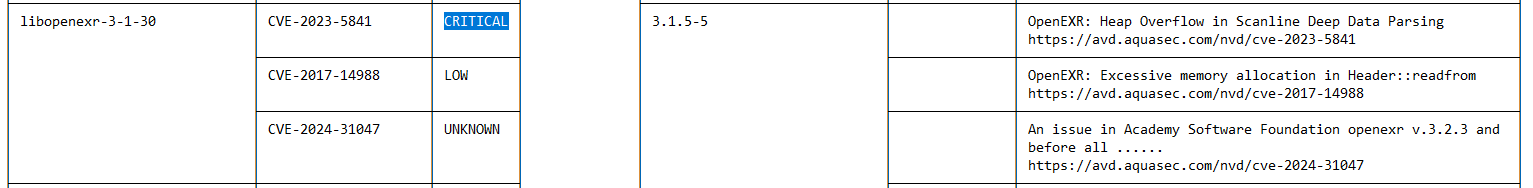


Рассмотрим CRITICAL уязвимости:

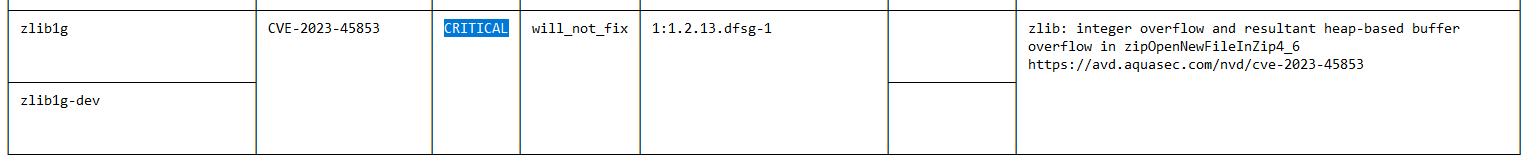






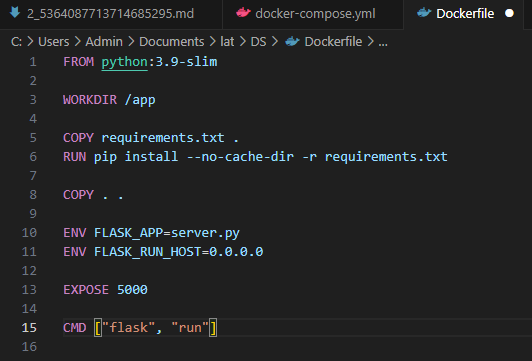




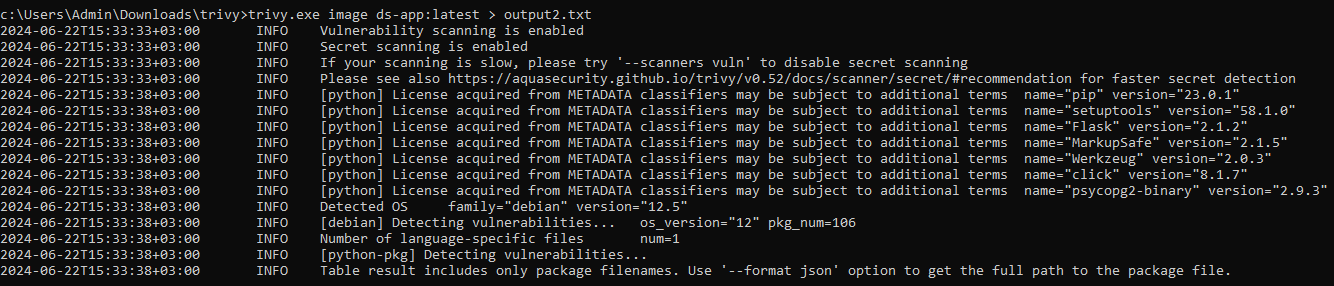


Уязвимости связаны с возможностью выполнения стороннего кода или приведение к отказу в обслуживании через удаленный репозиторий Git или через переполнение буфера в определенных библиотеках.

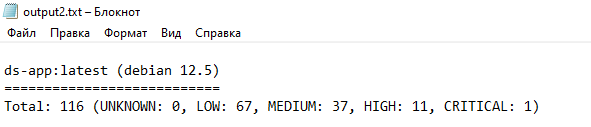
Одним из решений будет являться выбор более минималистичной версии python (3.9-slim) в Dockerfile для исключения использования дополнительных библиотек.

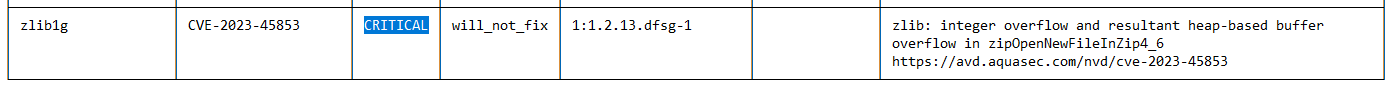


Проводим проверку еще раз:



Кол-во критических уязвимостей снизилось до одной:



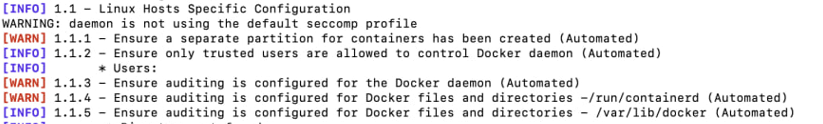


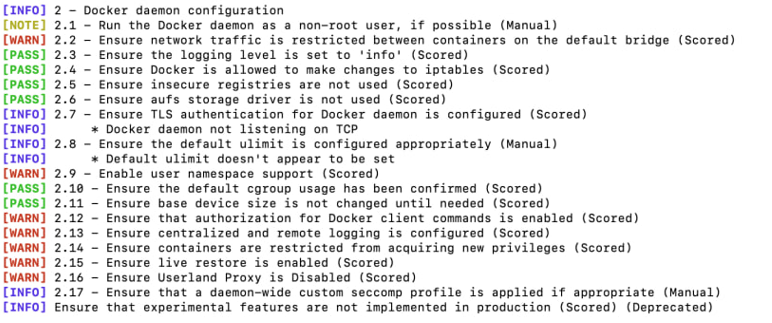
Проверка с помощью Bench Security:

Запуск скрипта для нашего образа:



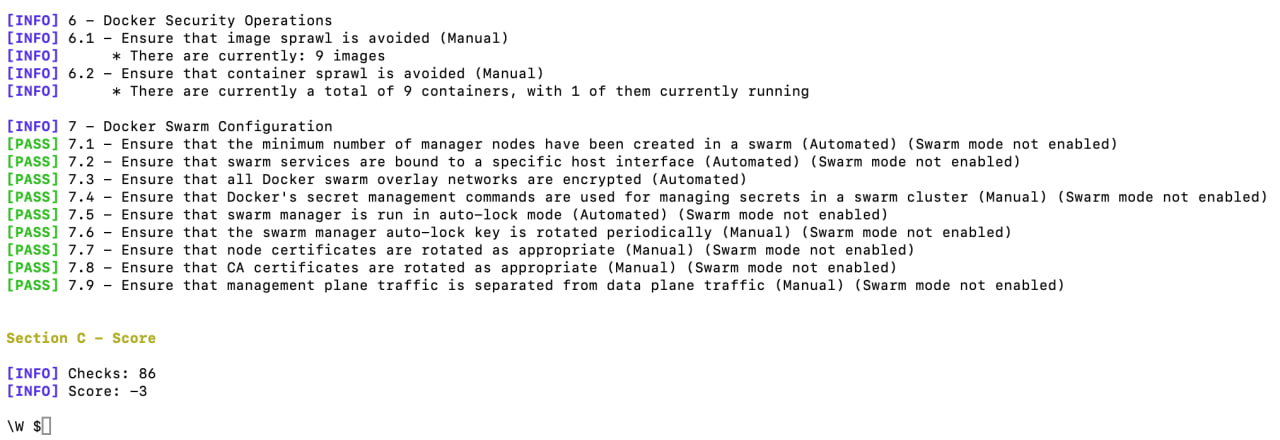
Результат – следующие предупреждения:



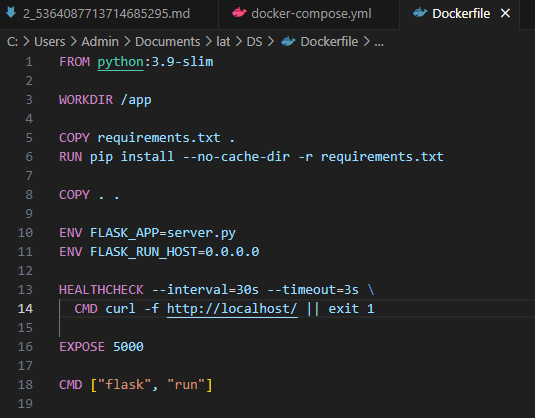




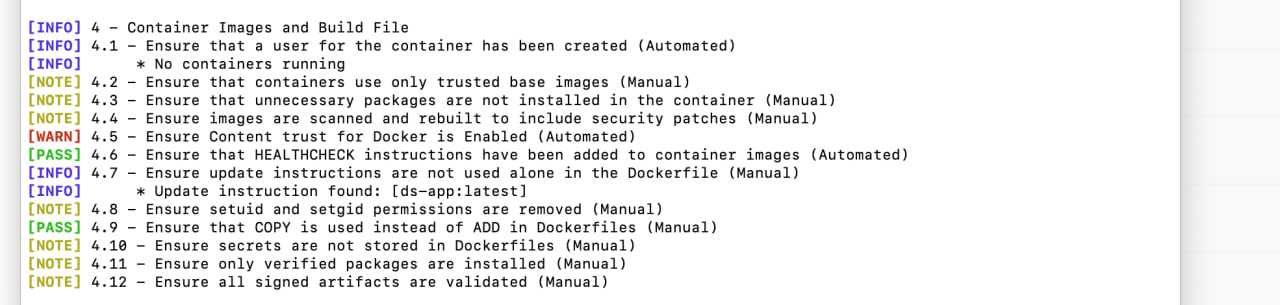


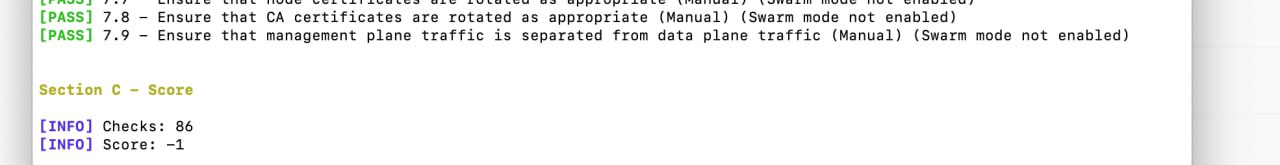


Добавим в докерфайл инструкции для отслеживания состояние контейнеров и автоматического перезапуска их при сбоях:

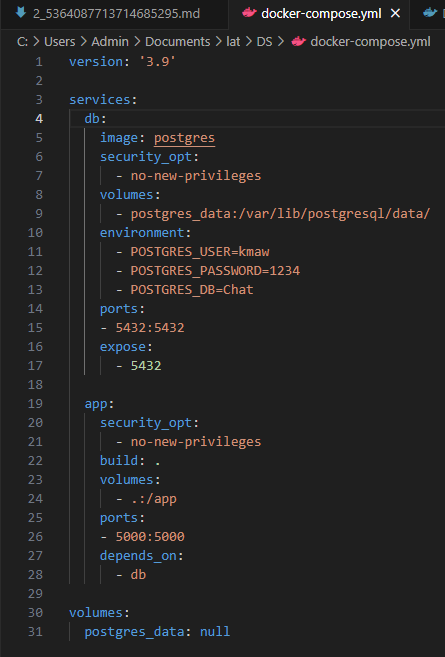


Предупреждение исчесзло, результат проверки повысился:





Ограничим контейнеры от получения новых привилегий, добавив опцию в docker-compose.yml:



К сожалению, предупреждение не исчезло:



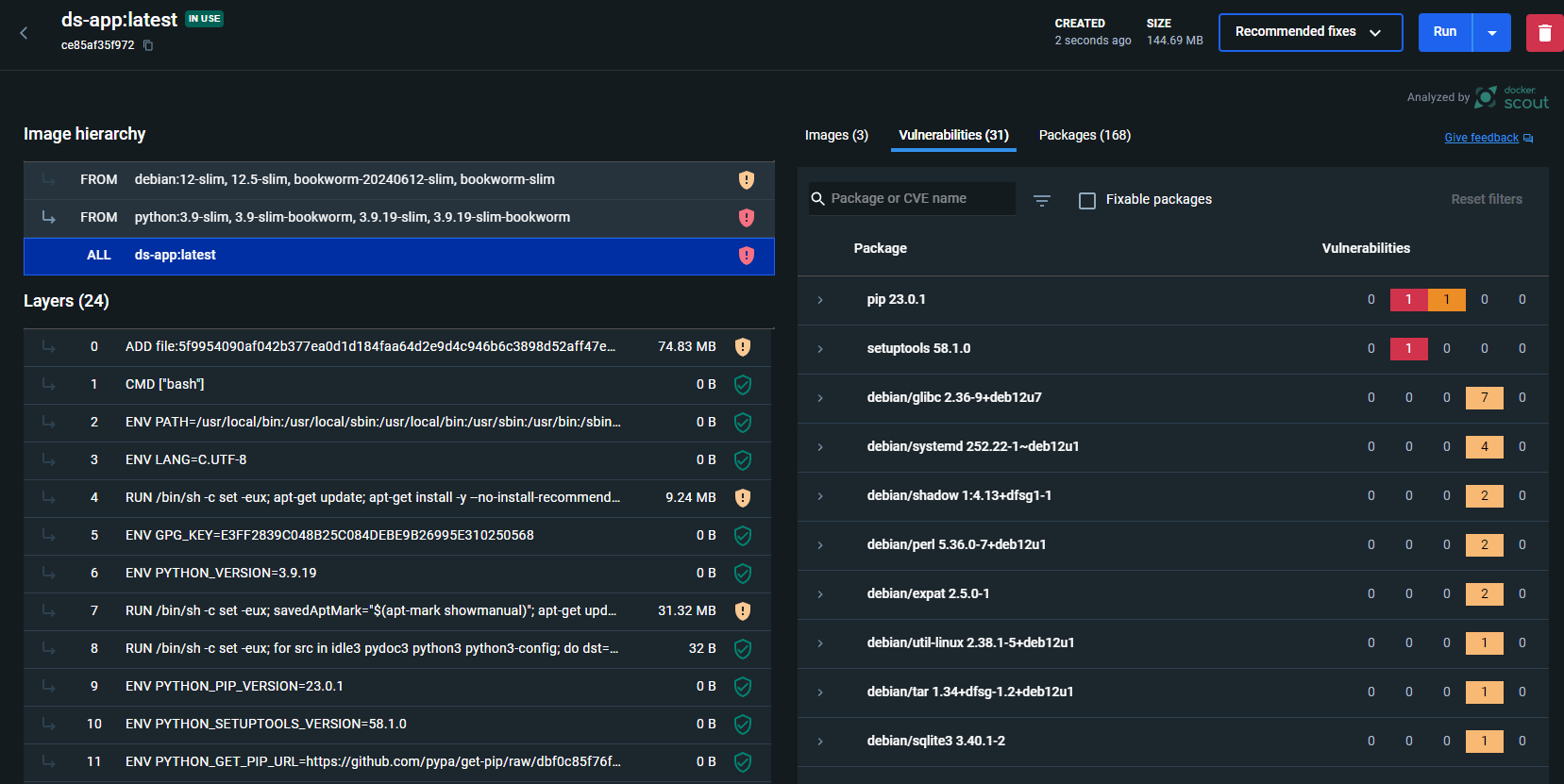
Команда «docker run --rm -it --security-opt=no-new-privileges ds-app bash» так же не помогла.

Остальные предупреждения исправляются изменением конфигураций в файловой системе Docker. Например,

* Ensure a separate partition for containers has been created - создать вручную отдельный раздел и смонтировать его в каталог /var/lib/docker, чтобы предотвратить исчерпание дискового пространства.
* Ensure auditing is configured for the Docker daemon - добавить отдельные правила в конфигурацию аудита Docker daemon для отслеживания действий и событий, связанных с безопасностью.
* Ensure userland proxy is disabled - отключить userland proxy в конфигурации Docker daemon.

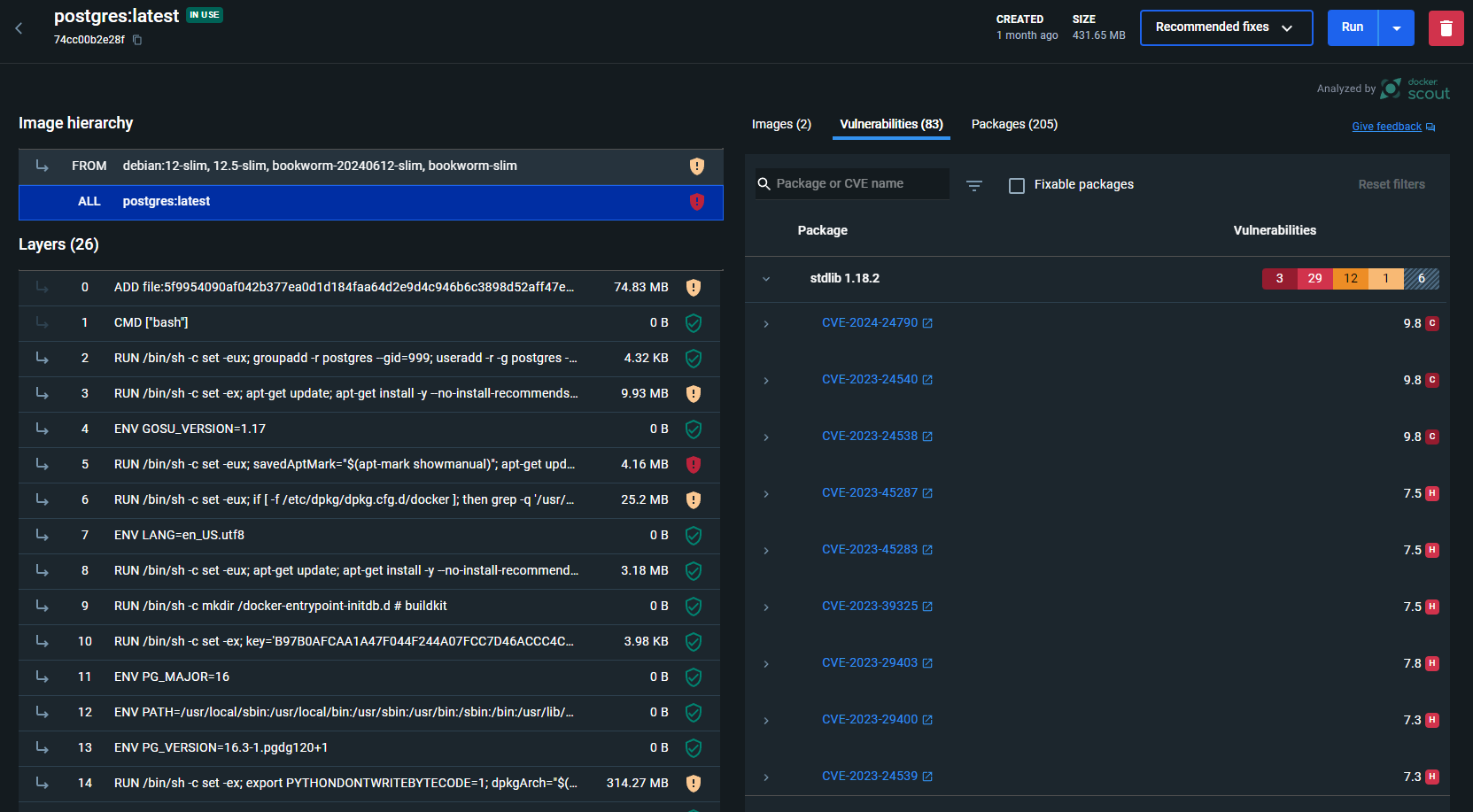
Проверка через Docker Scout:

Приложения:



Уязвимости некритические и связаны с версиями pip и setuptools используемой версии python.

Базы данных:



Критические уязвимости связаны с исходным кодом – версией stdlib в последней официального образа postgres, которую нельзя изменить.