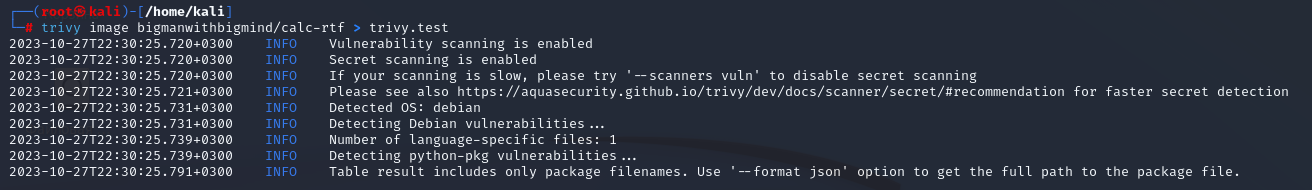
**Trivy и semgrep**

Выполнил: Попков Руслан

Студент группы РИ-400034

**1.Trivy**

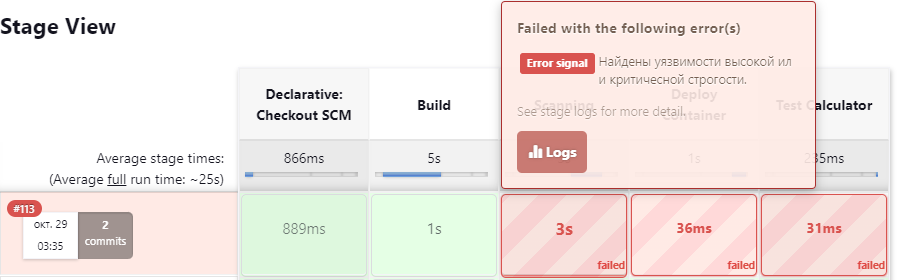
После установки trivy, был просканирован image калькулятора командой **trivy image название-образа.**



Была добавлена стадия Scanning, которая выполняет сканирование при помощи trivy и создает отчет, если найденные уязвимости имеют уровень высокий или критический, то пайплайн останавливается



Пример запуска пайплайна и остановка при нахождении уязвимости уровня HIGH:



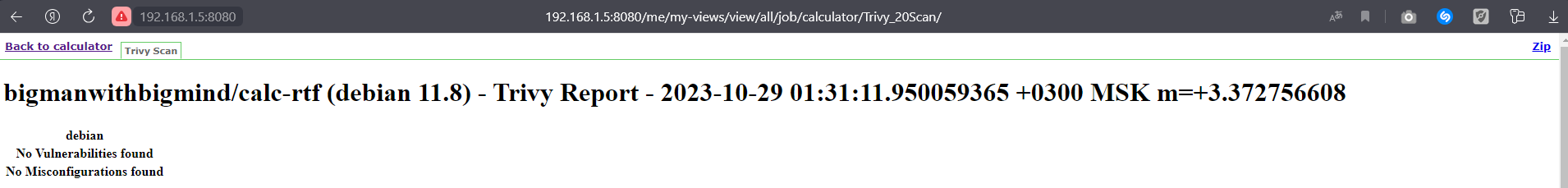
Теперь после запуска сборки, генерируется отчет о найденных уязвимостях:

s

Обратим внимание на уязвимость:

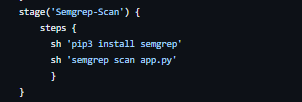
* **Setuptools** уязвимость высокой строгости, связана с недостаточной проверкой ввода при обработке содержимого HTML. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, передать приложению специально созданные данные и выполнить атаку типа «отказ в обслуживании» с помощью регулярных выражений.

Для закрытия уязвимости, требуется обновить setuptools до рекомендованной версии, а именно – 65.5.1. Для этого внесем корректировку в файл DockerFile, добавив строчку **RUN pip install setuptools==65.5.1.** После изменения, запустим сборку и увидим отсутствие уязвимости в отчете Trivy.



**2.Semgrep**

В пайплайн была встроена стадия проверки сканером Semgrep:



В результате было выявлено следующее:



Сканирование кода калькулятора проводилось с использованием 1099 правил, в итоге в коде было обнаружено следующее замечание:

* Running flask app with host 0.0.0.0 could expose the server publicly

Что означает следующее: запуск фласк приложения с хостом 0.0.0.0 может привести к публичному доступу к серверу. То есть любой хост может спокойно обращаться к калькулятору, что в нашем случае не страшно, потому что злоумышленник никак не сможет это проэксплуатировать.