



NGRSOFTLAB

Дорога навстречу Великому и Ужасному РБПО

Что мы делали, с какими сложностями столкнулись и что у нас получилось в итоге

Ильмар Хабибулин, NGR Softlab

NGR SOFTLAB

Создаем интеллектуальные
решения для защиты
цифрового пространства
организации и повышения
эффективности ИБ

#РАМ #SIEM #ХВА

- ✓ Лицензии ФСТЭК России
№1939 от 30.03.2020 (СЗКИ),
№3743 от 30.03.2020 (ТЗКИ)
- ✓ СМК соответствует требованиям
ГОСТ Р ИСО 9001-2015



ПОЧЕМУ МЫ РЕШИЛИ СТУПИТЬ НА «ДОРОГУ ИЗ ЖЕЛТОГО КИРПИЧА»

- ✓ Регуляторные требования
- ✓ Запросы заказчиков
- ✓ Проблемы с Интернет-центричной разработкой

ЛЕГКАЯ ПРОГУЛКА?



ТЕКУЩИЙ НАБОР ИСПОЛЬЗУЕМЫХ ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ

Было



sonarqube



GO



JS



Добавили



CODE
SCORING

КЛЮЧЕВАЯ ПРОБЛЕМА: РАСТУЩИЙ ОБЪЕМ ВНЕШНЕГО КОДА

	Внутренние строки кода	Внешние строки кода	Соотношение
C/C++	80 K+	10 M+	120
Go	~190 K	11 M+	58
Java	600 K+	15 M+	25
Javascript	~750 K	30 M+	40
Python	~105 K	2 M+	20
Ruby	~900	140 K+	155

КОМПОЗИЦИОННЫЙ АНАЛИЗ

Зависимости	Количество
Все зафиксированные	> 60000
Уникальные	> 10000
NPM (JAVASCRIPT)	> 7500
MVN (JAVA)	> 1000
PYPI (PYTHON)	> 200
GO	> 600
Other (DEB и т.п.)	> 300

07

ПРИМЕР РАБОТЫ С ЗАВИСИМОСТЯМИ

Started at	Duration	Startup type	Dependencies count
22.10.2024 12:30	8 minutes	Scheduled scan	1117
15.10.2024 12:35	37 minutes	Scheduled scan	3835
08.10.2024 12:35	24 minutes	Scheduled scan	3912
01.10.2024 12:35	24 minutes	Scheduled scan	3912
24.09.2024 12:35	33 minutes	Scheduled scan	5798
17.09.2024 12:30	30 minutes	Scheduled scan	5793
10.09.2024 12:30	29 minutes	Scheduled scan	5793
03.09.2024 12:25	37 minutes	Scheduled scan	5793
27.08.2024 12:20	41 minutes	Scheduled scan	8945
20.08.2024 12:20	an hour	Scheduled scan	8880

Пример сокращения зависимостей в большом монорепозитории из нескольких подпроектов путем приведения используемых версий заимствованных компонентов к одной

>x2

Реальное сокращение



СТАТИЧЕСКИЙ АНАЛИЗ – ХОРОШО, ЧТО ОН ЕСТЬ

- Секреты
- Адреса
- Потенциальные ошибки в коде



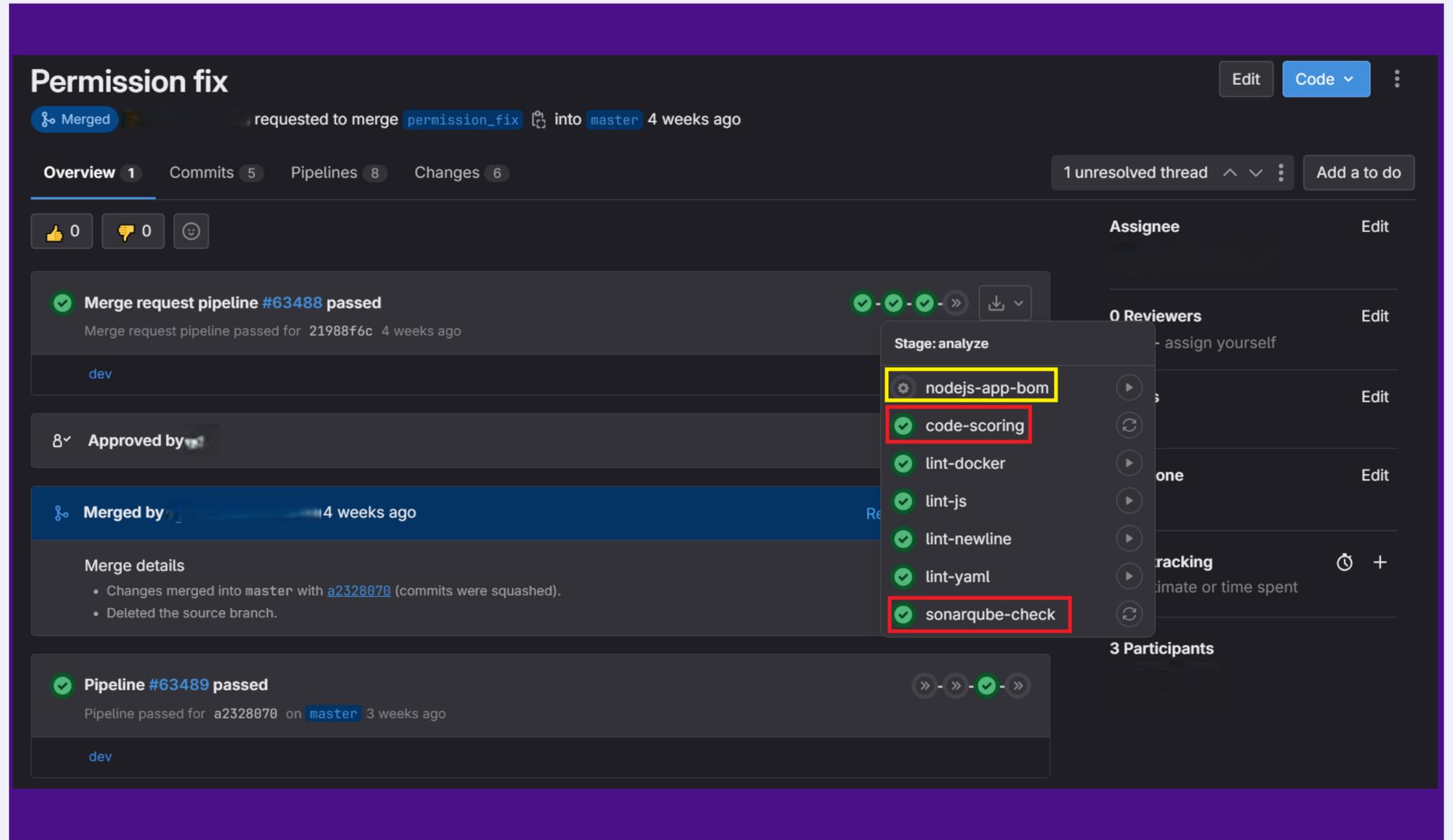
ОСНОВНЫЕ ПРОБЛЕМЫ СТАТИЧЕСКОГО АНАЛИЗА

- Длительность работы
- Несущественные срабатывания

SONARQUBE: ПРОВЕРКА ПРИ MERGE REQUEST

01 Простая интеграция проверок Sonarqube в сочетании с быстротой проверок – залог успеха

02 У каждой команды набор проверок может различаться, но общие инструменты всегда присутствуют



The screenshot displays a GitHub Merge Request titled "Permission fix" for the branch "permission_fix" into "master", requested 4 weeks ago. The interface shows a successful merge request pipeline (#63488) and a pipeline (#63489) that passed. A dropdown menu for the "analyze" stage is open, listing various checks: "nodejs-app-bom", "code-scoring", "lint-docker", "lint-js", "lint-newline", "lint-yaml", and "sonarqube-check". The "sonarqube-check" is highlighted with a red box, indicating its successful execution. The interface also shows 0 reviewers and 3 participants.

SVACE: ОПЫТ ЭКСПЛУАТАЦИИ

01 Длительность
работы

02 Множество
маркеров

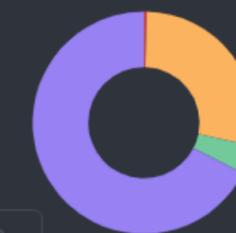
03 Возможность
совместной
работы

Duration: 1680 minutes 48 seconds
 Finished: 1 day ago
 Queued: 0 seconds
 Timeout: 3d (from job) [?](#)
 Runner: #38 (5AJ6dghVt)
 Tags: [Svace](#)

1 Проект 1 Ветка 1 Снимок

Количество маркеров по серьезности [↓](#)

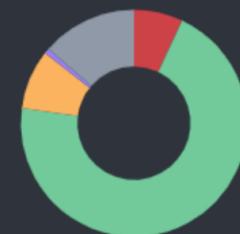
Всего: 6178



● Critical	28 (0.5%)
● Major	1721 (27.9%)
● Normal	261 (4.2%)
● Minor	4168 (67.5%)
● Undefined	0 (0.0%)

Количество маркеров по статусу разметки [↓](#)

Всего: 6178



● Confirmed	433 (7.0%)
● Won't fix	4330 (70.1%)
● Unclear	528 (8.5%)
● False positive	44 (0.7%)
● Undecided	843 (13.6%)

ДИНАМИЧЕСКИЙ АНАЛИЗ И ТЕСТИРОВАНИЕ



Pentest

- Автоматизированный
- Ручной

Fuzzing

- WEB (внешний)
- Кодовый (внутренний)

Нагрузочное тестирование
собственными генераторами

Автотестирование

ОСНОВА – МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ФСТЭК

КРАТКИЕ ВЫВОДЫ

1 Ресурсов мало

2 Минимизируйте

3 Делегируйте

4 Кооперируйтесь

5 Приоритизируйте

6 Используйте разные подходы

7 Лучше меньше, но качественнее

8 Это путь



Полезные новости, обзоры
и приглашения на мероприятия –
в **Telegram-канале NGR Softlab**

Спасибо за внимание! Вопросы?

 + 7 (495) 269-29-59

 info@ngrsoftlab.ru

 ngrsoftlab.ru