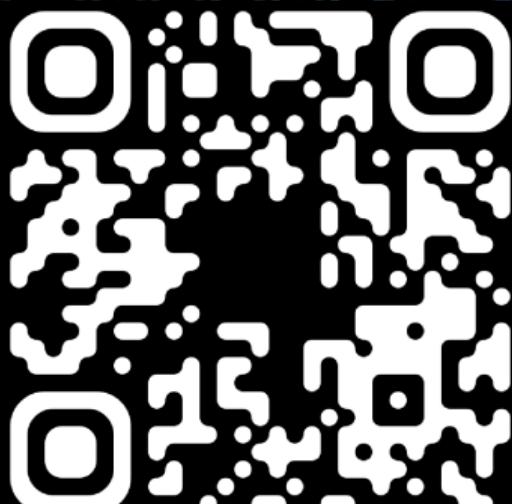


positive
hack // days12

POSI {dev}

Phd 12



MMMCJX#Me\$X" r"
MMF\$e%#mM/ M" #c
M' %8MSX" M #.%^
%@w\$?"m%#^8%w,
+e#SM%@2Wm#^d^
%S%M\$3#e#[_D ,mmmm,)
%#%#%#%#@_D HMMHHMM,
\$C\$w%#%#^NL HMM*""MM
D\$#%#%#%JMB MM[@ %
@AS@%@#FMME MQm Q⁴
2WMWMMWMMQb \MMMWMMW
#XUMM@I5MMMb 'MMMWMP
L*M@%^ -IMMD J%w' "5+S⁷
"- %@#eJMMMW:9 *":~ ?
"Q3 -@3LQMMm#X ?##-CM"6 ~@- 3&%\$%F #%uW%%\$# @%1NNM#m% Q9
%AS @%7MML-# M#x%Q#e" #:#"et#) #e%Q #@@%\$-@ M# MMFX- cW#
\$#t -HMM, #X\$#%#- w%^ Qe@3X#-^M& -Q%Q% gMM+^%#%
"mgb 8\$00 z - #%" 1#z Q30#^g@15m ^

Как обезопасить от санкций ваш открытый проект на GitHub

Александр Попов

Positive Technologies

20.05.2023



- Александр Попов
 - Разработчик ядра Linux с 2012 года
 - Исследователь информационной безопасности в
 - **positive technologies**
 - Докладчик на конференциях:
OffensiveCon, Nullcon Goa, Linux Security Summit, Still Hacking Anyway, Zer0Con, Positive Hack Days, ZeroNights, HighLoad++, Open Source Summit, OS DAY, Linux Plumbers и других
- a13xp0p0v.github.io/conference_talks

- ① Постановка проблемы:
**незащищенность
открытых проектов
на GitHub**

- ② Поиск решений и технические трудности

- ③ Текущее **оптимальное решение** и выводы



- На GitHub зарегистрировано более **100 млн.** разработчиков
- Это дает выход на **огромную аудиторию**
- Поэтому многие open-source-проекты разрабатываются там
- С 2018 года компания Microsoft владеет платформой GitHub
- В последнее время GitHub проводит политику **санкций и блокировок**
- **Свежий пример:** блокировка учетных записей сотрудников компании YADRO и их репозиториев (включая ipmitool)





github.com/a13xp0p0v – это **моя личная** учетная запись

Наиболее значимые проекты по безопасности ядра Linux:

① Linux Kernel Defence Map

github.com/a13xp0p0v/linux-kernel-defence-map

② kconfig-hardened-check

github.com/a13xp0p0v/kconfig-hardened-check



Alexander Popov
a13xp0p0v

Follow

Linux Kernel Developer & Security Researcher. This is my personal account.

573 followers · 3 following

<https://a13xp0p0v.github.io/>
[@a13xp0p0v](https://twitter.com/a13xp0p0v)

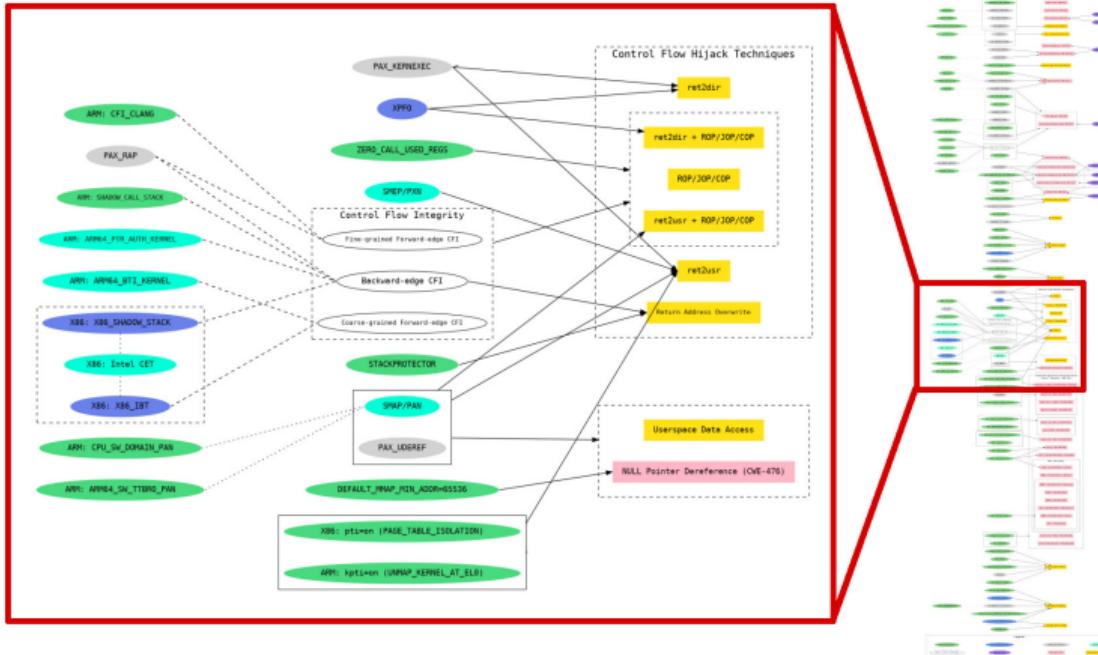
Achievements



Карта средств защиты ядра Linux

phd 12

Linux Kernel Defence Map: github.com/a13xp0p0v/linux-kernel-defence-map



About

Linux Kernel Defence Map shows the relationships between vulnerability classes, exploitation techniques, bug detection mechanisms, and defence technologies

Readme

GPL-3.0 license

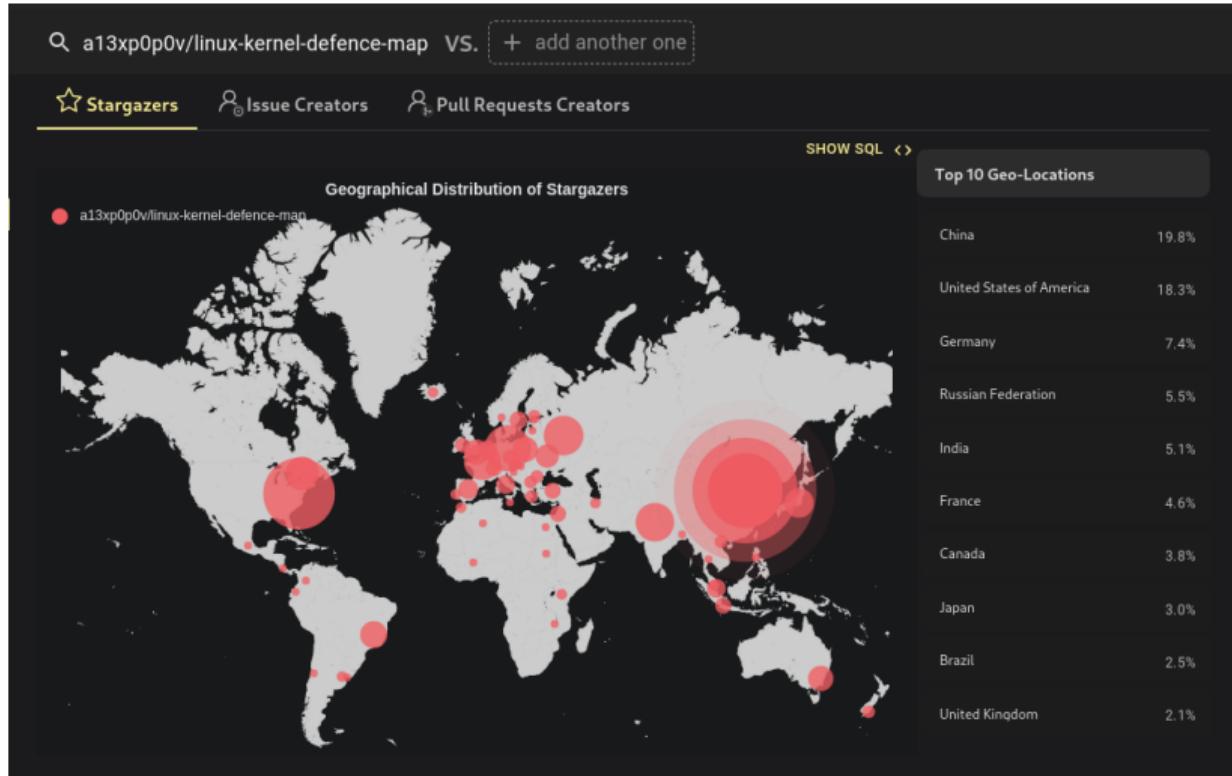
1.6k stars

105 watching

118 forks

Карта средств защиты ядра Linux

phd 12



Карта средств защиты ядра Linux

phd 12



kconfig-hardened-check github.com/a13xp0p0v/kconfig-hardened-check

```
[a13x@hackbase kconfig-hardened-check]$ ./bin/kconfig-hardened-check
usage: kconfig-hardened-check [-h] [--version] [-p {X86_64,X86_32,ARM64,ARM}] [-c CONFIG]
[-l CMDLINE] [-m {verbose,json,show_ok,show_fail}]
```

A tool for checking the security hardening options of the Linux kernel

optional arguments:

- h, --help show this help message and exit
- version 1 show program's version number and exit
- p {X86_64,X86_32,ARM64,ARM}, --print {X86_64,X86_32,ARM64,ARM} 2
print security hardening preferences for the selected architecture
- c CONFIG, --config CONFIG 3
check the kernel kconfig file against these preferences
- l CMDLINE, --cmdline CMDLINE 4
check the kernel cmdline file against these preferences
- m {verbose,json,show_ok,show_fail}, --mode {verbose,json,show_ok,show_fail}
choose the report mode

About

A tool for checking the security hardening options of the Linux kernel

Readme

GPL-3.0 license

832 stars

49 watching

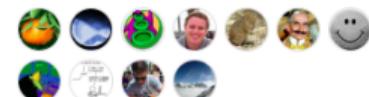
106 forks

Report repository

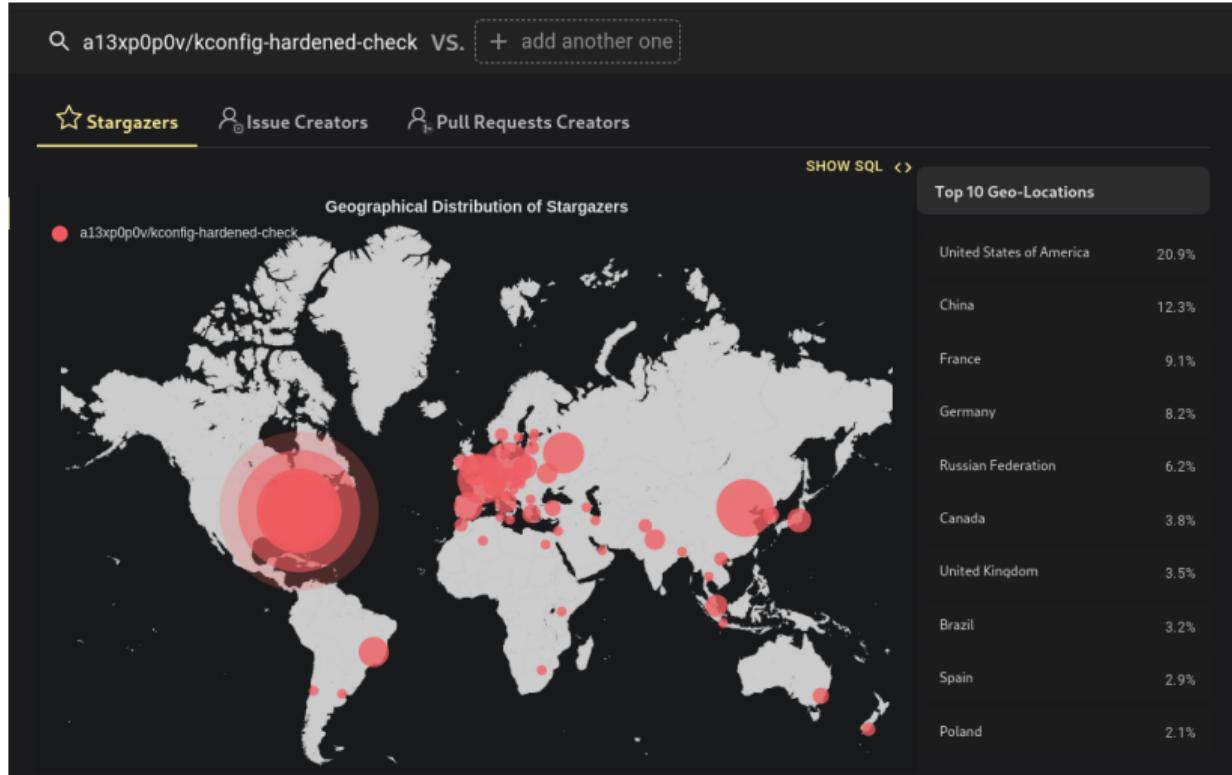
Releases

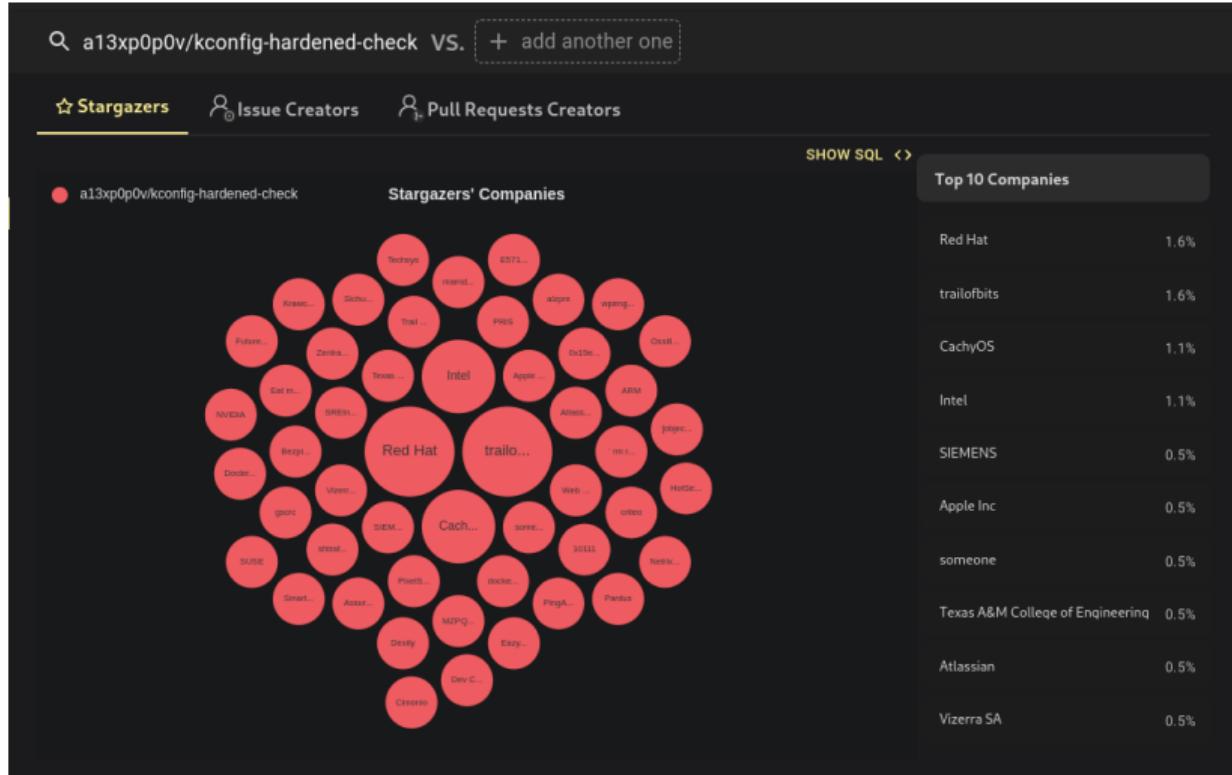
9 tags

Contributors 15



+ 4 contributors





- ➊ Уйти с GitHub? Это значит **потерять аудиторию и сообщество** вокруг проекта
- ➋ Оставить все как есть? Это значит **потерять все** в случае блокировки (см. ipmitool)
- ➌ Так что же делать? Организовать **зеркалирование проектов**

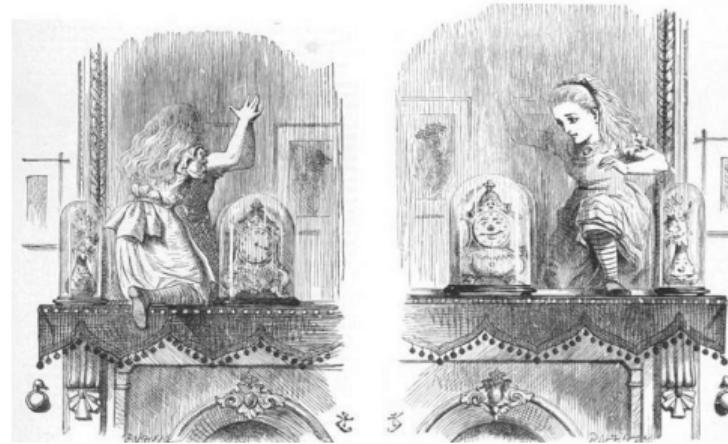


Иллюстрация Джона Тенниела

- Ранее я пользовался зеркалированием GitLab (**pull mirroring**)
- Эта функция копирует из GitHub-репозиториев в GitLab:
 - ▶ код
 - ▶ теги
 - ▶ обсуждения в issues и pull requests
- Внезапно мои GitLab-зеркала стали отставать от основных репозиториев
- С июля 2022 г. платформа GitLab **закрыла доступ к этой функции**
для open-source-проектов (она стала платной)

Alexander Popov > kernel-hack-drill

 Your project is no longer receiving GitLab Ultimate benefits as of 2022-07-01. As notified in-app previously, public open source projects on the Free tier can apply to the GitLab for Open Source Program to receive GitLab Ultimate benefits. Please refer to the [FAQ](#) for more details.

X

NOT SEEKING PROFIT

I certify that project maintainers are not seeking to make profit from this project by, for example, selling services or higher tiers.
Make sure your use case qualifies.

(Optional) Please provide additional details to help us verify you aren't seeking profit with your project.

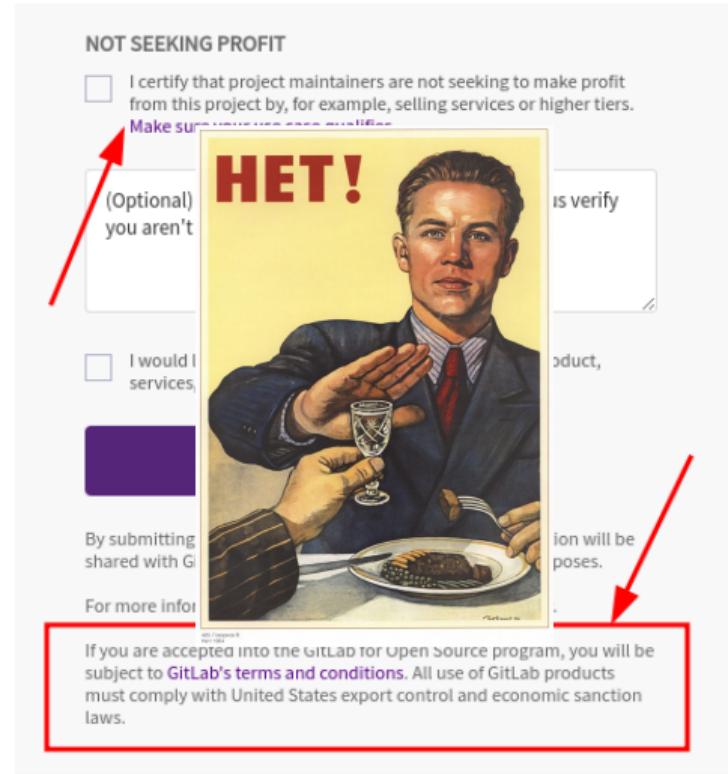
I would like to receive emails from GitLab about its product, services, and events.

Submit

By submitting this form, you understand that your information will be shared with GitLab by SheerID and used for verification purposes.

For more information please see the [GitLab's Privacy Policy](#).

If you are accepted into the GitLab for Open Source program, you will be subject to [GitLab's terms and conditions](#). All use of GitLab products must comply with United States export control and economic sanction laws.



- Включить GitLab pull mirroring бесплатно более **невозможно**



- Покупка премиум-поддержки GitLab (Premium Tier) **невозможна в России**
- GitLab **запрещает** использовать даже пробную версию (Trial)
- Я стал искать **другие решения** для зеркалирования моих GitHub-проектов

- Может развернуть свой отдельный сервер разработки **Forgejo (Gitea)** или **GitLab CE**?
- Нет, изолированный сервер **мне не подходит**:
 - ▶ Это ограничит взаимодействие с сообществом
 - ▶ Это станет препятствием для контрибуторов



OPEN-SOURCE-РАЗРАБОТКА
НА ИЗОЛИРОВАННОМ СЕРВЕРЕ

Я рассмотрел следующие платформы коллективной разработки:

- Китайская платформа [Gitee](#)
 - [–] слабая поддержка английской локализации
- [BitBucket](#)
 - [–] не умеет импортировать issues и pull requests с GitHub
 - [–] компания Atlassian «ушла из России»
- Пиринговая сеть [Radicle](#)
 - [–] «мощные функциональные возможности, основанные на блокчейне» 😕
- [SourceHut](#)
 - [–] предоставляет только платные услуги
 - [–] несовместимый с GitHub процесс разработки (email-driven)
- [Salsa](#) (сервер сообщества Debian на GitLab CE)
 - [–] функция pull mirroring тоже отключена (как на gitlab.com в бесплатном режиме)

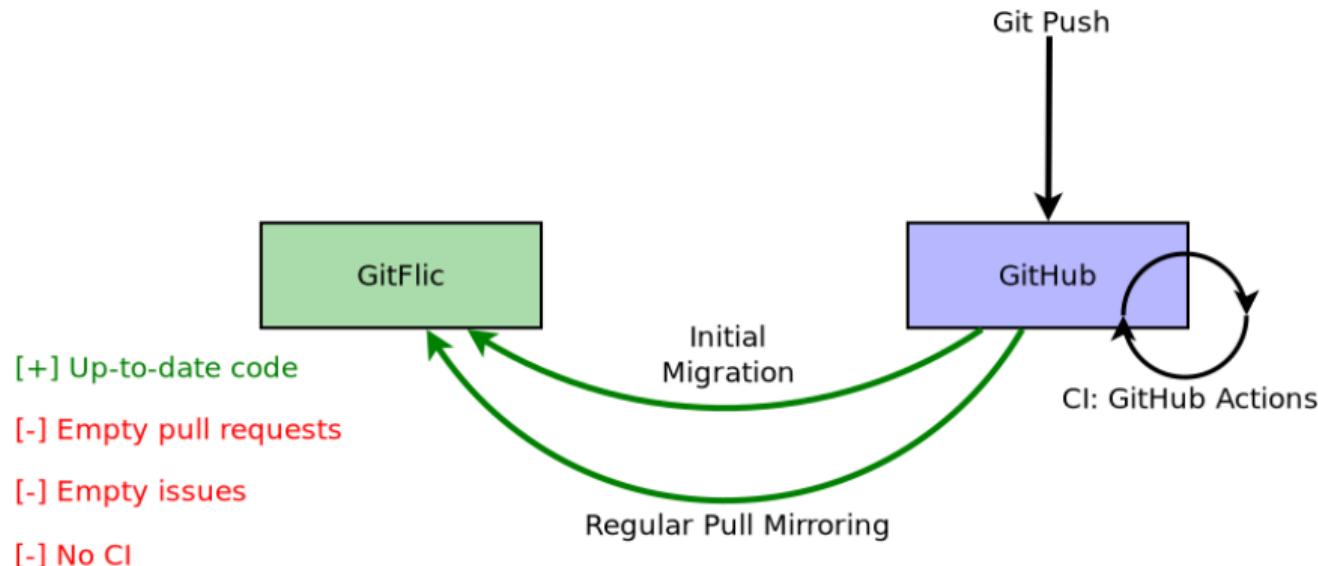
Это небольшая российская платформа коллективной разработки.

Мои впечатления:

- [+] есть функция зеркалирования для кода (git pull по расписанию)
- [?] публичные репозитории создаются по запросу в службу поддержки
(или с помощью учетки Yandex/VK)
- [–] нет копирования информации из issues и pull requests с GitHub
- [–] нет CI
- [–] закрытый код платформы
- [–] их типичный ответ на выявленные мной ошибки (цитата):

«С этим будем обязательно разбираться,
но позже, в данный момент у нас задачи»

Очевидно, зеркала на GitFlic **не стали** для меня окончательным решением



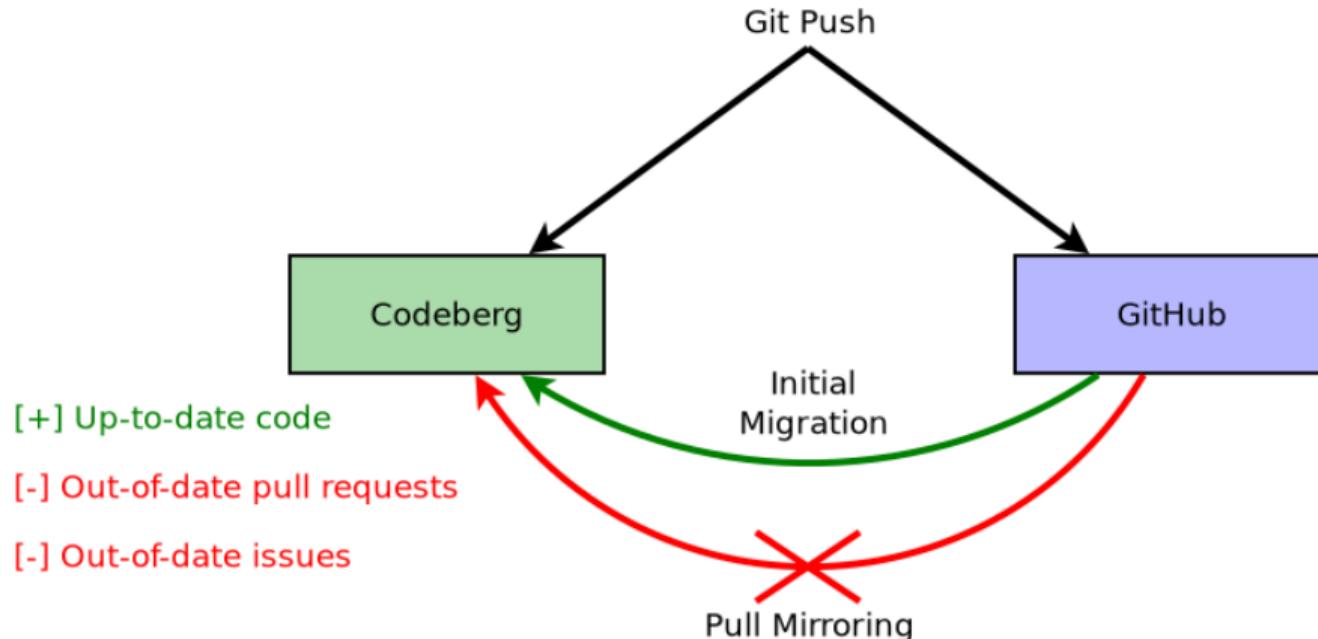
- [+] поддерживается некоммерческой организацией, продвигающей идеи FOSS
- [+] имеет довольно крупную аудиторию — более 50000 разработчиков
- [+] работает на открытом коде — [Forgejo \(Gitea\)](#)
- [+] поддерживает копирование информации из issues и pull requests с GitHub
- [+] имеет интеграцию с open-source CI — [Woodpecker CI](#)
- [—] В марте 2020 г. они отключили функцию зеркалирования

Mirror repos: easily created, consuming resources forever

Wed 11 March 2020

At launch we considered the Gitea mirror feature a great way to smoothly transition repos for projects to Codeberg.org, also as nice way to quickly test-drive Codeberg's features. Over time it turned out however, that many if not the majority of all mirrors become abandoned, and mirror repositories tend ...

Category: [Announcement](#)



Вопрос:

Что делать с устаревающей информацией
в issues и pull requests на Codeberg?*

* Вручную удалять и воссоздавать проекты на Codeberg —

это не очень хорошее решение



- Сделать обсуждения в issues и pull requests **частью кода** проекта
- Открытый проект **gh2md** позволяет выгрузить эти данные в Markdown-документ
- Под капотом **gh2md** использует интерфейсы **GraphQL** платформы GitHub
- Поэтому нужно сгенерировать **личный токен доступа** GitHub

The screenshot shows the GitHub developer settings page. On the left, there is a sidebar with options: GitHub Apps, OAuth Apps, Personal access tokens (which is the active tab), Fine-grained tokens (Beta), and Tokens (classic). The main area displays a list of personal access tokens. One token is shown in detail: "issue_reader_token — public access" with an expiration date of "Expires on Sun, Jan 1 2023".

- Теперь мои проекты содержат **резервную копию** всех задач и обсуждений
- Также это можно сделать с помощью трекера **git-bug** (выгрузка в git-хранилище)

Второе решение: внешний трекер задач для Codeberg

The screenshot shows the 'Issues' section of the repository settings. It includes the following configuration:

- Enable Repository Issue Tracker
- Use Built-In Issue Tracker
- Enable Time Tracking
- Let Only Contributors Track Time
- Enable Dependencies For Issues and Pull Requests

Below these options is a note: "Close an issue via a commit made in a non default branch".

A red box highlights the "External Issue Tracker" section:

- Use External Issue Tracker

Under "External Issue Tracker URL", the value is set to <https://github.com/a13xp0p0v/linux-kernel-defence-map/issues>. A note below states: "Visitors are redirected to the external issue tracker URL when clicking on the issues tab."

Under "External Issue Tracker URL Format", the value is set to <https://github.com/{user}/{repo}/issues/{index}>. A note below states: "Use the placeholders {user}, {repo} and {index} for the username, repository name and issue index."

A red box highlights the "External Issue Tracker Number Format" section, which contains three radio button options:

- Numeric #1234
- Alphanumeric ABC-123 , DEFG-234
- Regular Expression (ISSUE-(\d+), ISSUE-(\d+))

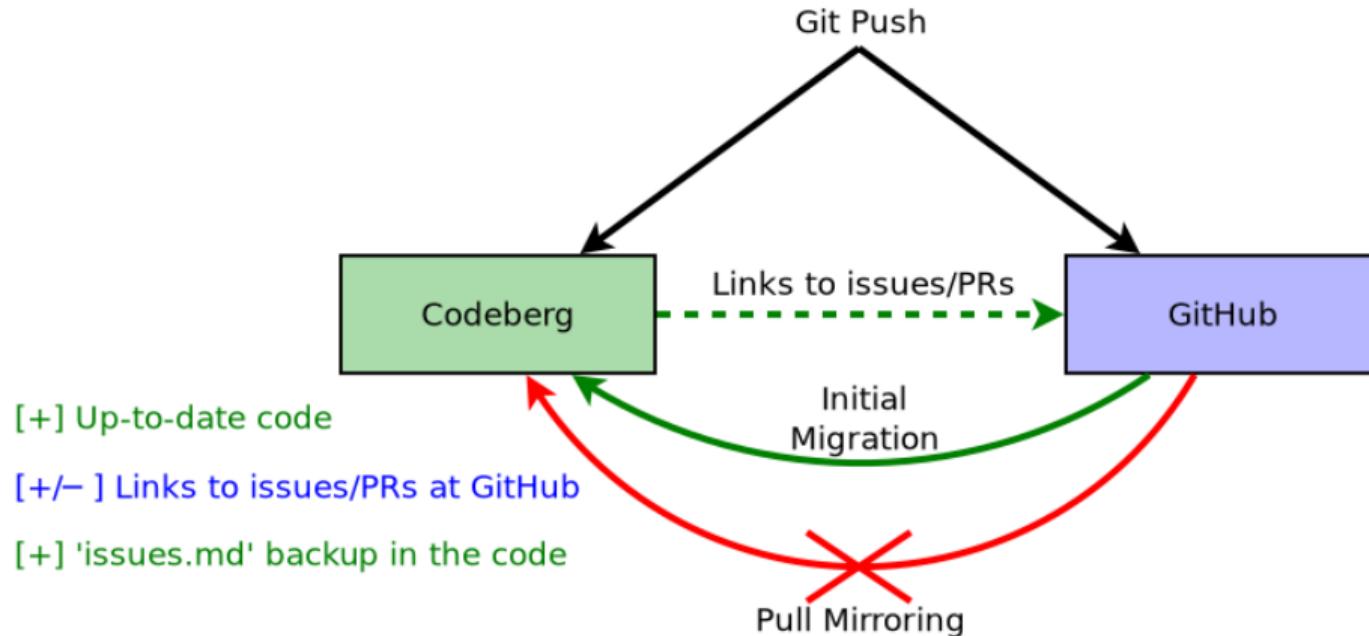
Below this is a "Regular Expression Pattern" section with the placeholder: "The first captured group will be used in place of {index}."

At the bottom of the page, another red box highlights the "Pull Requests" section:

- Enable Repository Pull Requests

Under "Pull Requests", the following checkboxes are checked:

- Ignore Whitespace for Conflicts
- Enable Commit Merging
- Enable Rebasing to Merge Commits
- Enable Rebasing with explicit merge commits (--no-ff)
- Enable Squashing to Merge Commits



Паритет с GitHub Actions:

Чтобы зеркало репозитория было полноценным,
для него нужно внедрить непрерывную интеграцию

GitHub Actions для kconfig-hardened-check

phd 12

- ① Функциональные тесты инструмента с подсчетом покрытия кода
- ② Unit-тесты движка инструмента с подсчетом покрытия кода

[a13xp0p0v / kconfig-hardened-check](#) Public

Code Issues Pull requests Actions Security Insights

← functional test

✓ Improve the COMPAT_VDSO check #47

Summary

Jobs

- ✓ functional_test (3.7)
- ✓ functional_test (3.8)
- ✓ functional_test (3.9)
- functional_test (3.10)**
- ✓ functional_test (3.11)

Run details

Usage

Workflow file

functional_test (3.10)
succeeded 2 weeks ago in 2m 25s

- ✓ Set up job
- ✓ Set up Python 3.10
- ✓ Install package
- ✓ Check all configs with the installed tool
- ✓ Get source code for collecting coverage
- ✓ Collect coverage for the basic functionality
- ✓ Collect coverage for error handling
- ✓ Prepare final coverage report
- ✓ Handle coverage
- ✓ Post Get source code for collecting coverage
- ✓ Post Set up Python 3.10
- ✓ Complete job

[a13xp0p0v / kconfig-hardened-check](#) Public

Code Issues Pull requests Actions Security Insights

← engine unit-test

✓ Improve the COMPAT_VDSO check #48

Summary

Jobs

- engine_unit-test (3.11)**

Run details

Usage

Workflow file

engine_unit-test (3.11)
succeeded 2 weeks ago in 11s

- ✓ Set up job
- ✓ Set up Python 3.11
- ✓ Get source code for collecting coverage
- ✓ Install coverage
- ✓ Run unit-tests and collect coverage
- ✓ Handle coverage
- ✓ Post Get source code for collecting coverage
- ✓ Post Set up Python 3.11
- ✓ Complete job

README.md

kconfig-hardened-check

release v0.6.1

functional test passing 98%

engine unit-test passing 100%

Motivation

There are plenty of security hardening options for the Linux kernel. We have to enable those options ourselves.

GitHub Actions:

- проприетарный код
- имеет Marketplace
- функции для своего CI берешь из этого Marketplace
- yml-конфигурация проекта в `.github/workflows/`

Woodpecker-CI:

- свободное ПО
- основан на Docker-контейнерах
- функции для своего CI запекаешь в свой Docker-образ
- yml-конфигурация проекта в `.woodpecker/`

Woodpecker-CI для kconfig-hardened-check

phd 12

← Конвейер №54 - Fix CI output style and move `pip install coverage` to the proper place

Задачи Конфигурация Изменённые файлы (2) 1 week ago 2 мин., 41 сек.

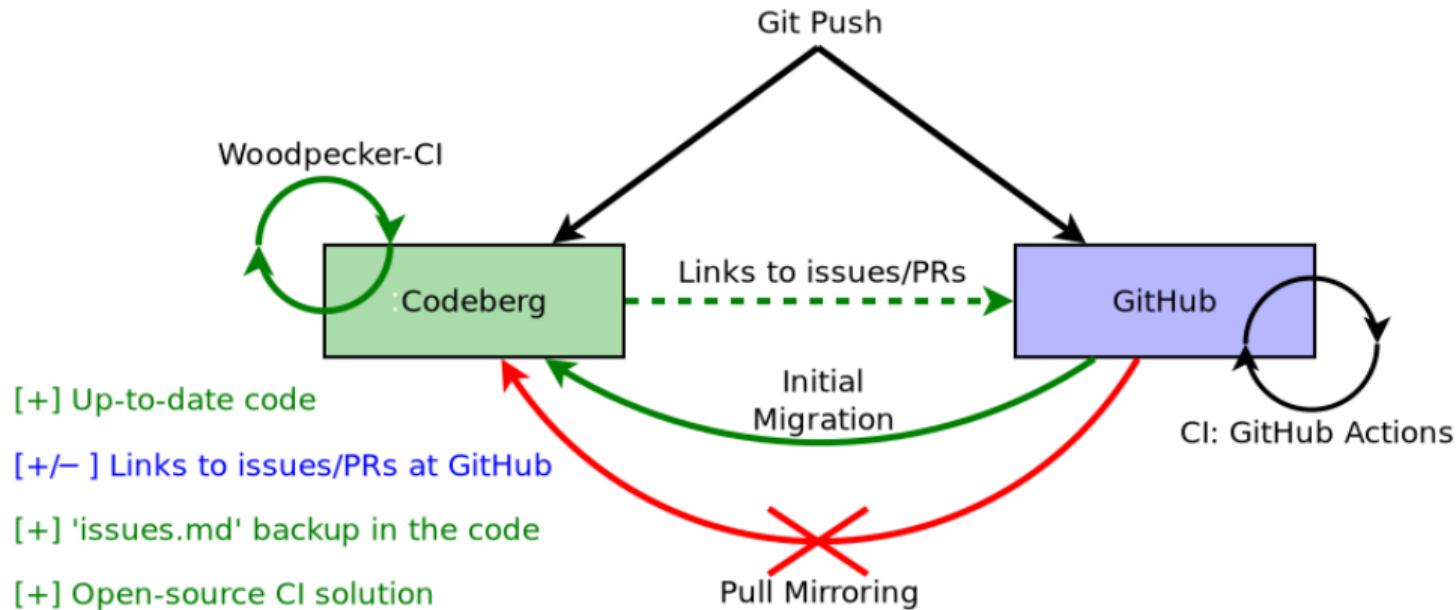
a13xp0p0v master fb93b0f133

engine_unit-test 00:39 ✓ clone 00:17 ✓ unit-test 00:14

functional_test 02:41 ✓ clone 00:20 ✓ installation-test 00:20 ✓ functional-test-with-covera... 01:56

```
14 [notice] To update, run: pip install --upgrade pip
15 + echo "Run unit-tests and collect coverage..."
16 Run unit-tests and collect coverage...
17 + coverage run --include=kconfig_hardened_check/engine.py,kconfig_hardened_check/test_engine.py -m
  unittest -v -b
18 test_complex_and (kconfig_hardened_check.test_engine.TestEngine.test_complex_and) ... ok
19 test_complex_or (kconfig_hardened_check.test_engine.TestEngine.test_complex_or) ... ok
20 test_simple_cmdline (kconfig_hardened_check.test_engine.TestEngine.test_simple_cmdline) ... ok
21 test_simple_kconfig (kconfig_hardened_check.test_engine.TestEngine.test_simple_kconfig) ... ok
22 test_stdout (kconfig_hardened_check.test_engine.TestEngine.test_stdout) ... ok
23 test_value_overriding (kconfig_hardened_check.test_engine.TestEngine.test_value_overriding) ... ok
24 test_version (kconfig_hardened_check.test_engine.TestEngine.test_version) ... ok
25
26 -----
27 Ran 7 tests in 0.004s
28
29 OK
30 + echo "Show the coverage report..."
31 Show the coverage report...
32 + coverage report
33 Name           Stmts   Miss  Cover
34 -----
35 kconfig_hardened_check/engine.py      187     0  100%
36 kconfig_hardened_check/test_engine.py 187     0  100%
37 -----
38 TOTAL                  374     0  100%
```

Код завершения 0



The screenshot shows a GitHub repository page for 'kconfig-hardened-check'. The URL in the address bar is github.com/a13xp0p0v/kconfig-hardened-check. The page displays the 'README.md' file. Below it, the 'Repositories' section lists three mirrors:

- Main at GitHub: <https://github.com/a13xp0p0v/kconfig-hardened-check>
- Mirror at Codeberg: <https://codeberg.org/a13xp0p0v/kconfig-hardened-check>
- Mirror at GitFlic: <https://gitflic.ru/project/a13xp0p0v/kconfig-hardened-check>

Если что-то пойдет не так с GitHub, то я сделаю следующее:

- ① пересоздам репозитории в Codeberg
- ② включу в них внутренний трекер
- ③ включу в них запросы на слияние
- ④ анонсирую для сообщества и дистрибутивов GNU/Linux,
что разработка переведена на Codeberg



Продумайте аварийный сценарий для своих открытых проектов!

Спасибо! Ваши вопросы?

Контакты:

✉ alex.popov@linux.com

    a13xp0p0v

Личный блог:

a13xp0p0v.github.io



■ positive technologies

/ Оцените этот доклад

(после окончания всего трека,
пожалуйста)

phd 12

