Debricked

Anton Duppils and Magnus Tullberg

anton.duppils@gmail.com and magnus.tullberg@gmail.com

Who are we?

- Lead Data Engineers at Debricked
- Computer Science - Security @LTH
- Master Thesis at Debricked 2019
  - Detect undisclosed vulnerabilities on GitHub

What is Debricked?

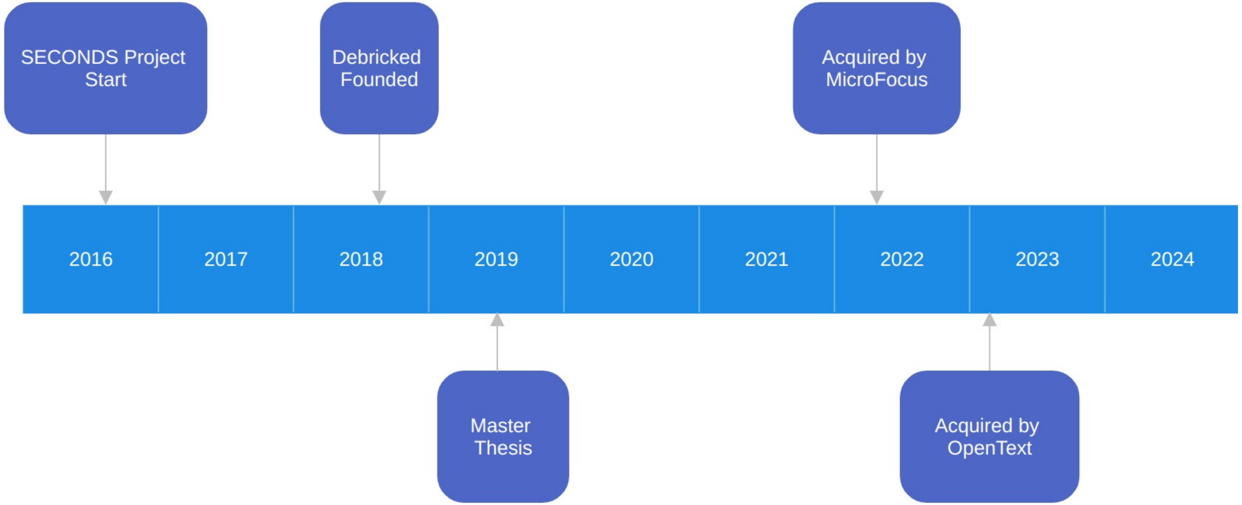
Software Composition Analysis (SCA) tool

- Vulnerability
- License
- Health
- Policies

https://debricked.com/

Debricked Journey

- Research project from LTH, a vinnova backed project – SECONDS
  https://www.vinnova.se/en/p/seconds-securing-connected-devices/
- An explosion in open source projects and new vulnerabilities
- Focus shift to provide solutions to vulnerability and license management for the growing use of open source.



What we’ve done - Part 1/3

- Rule Engine
  - Heuristic based vulnerability matching

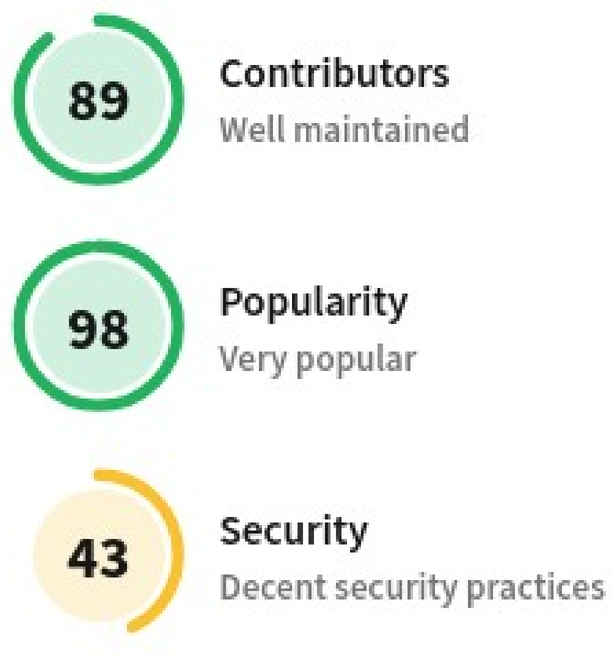
- Data Lake

- Security Entity Classification
  - Detect undisclosed vulnerabilities via ML on version control data

- File fingerprinting
  - Match existing open source in your project

What we’ve done - Part 2/3

- Open Source Health
  - Metrics on open source projects
  - Master Thesis on finding right metrics
  - Master Thesis on what’s important to



89 Contributors

Well maintained

98 Popularity

Very popular

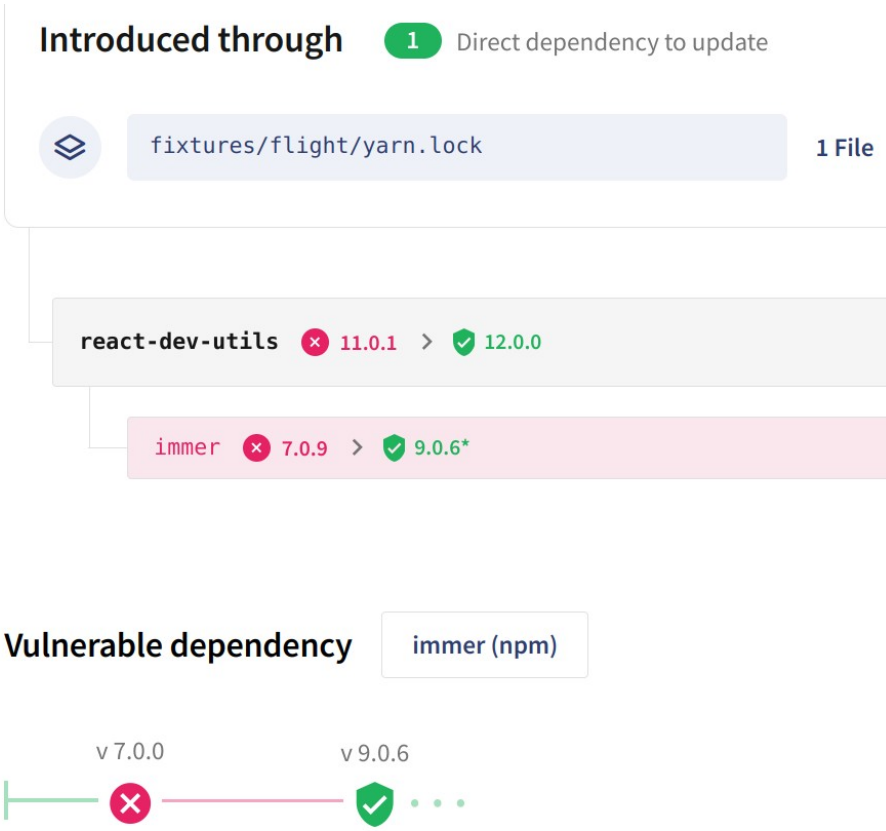
43 Security

Decent security practices

What we’ve done - Part 2/3

- Open Source Health
  - Metrics on open source projects

- Open Source Dependency Graph
  - Approximate PM resolution
  - Vulnerability fix recommendation



Introduced through 1 Direct dependency to update

fixtures/flight/yarn.lock 1 File

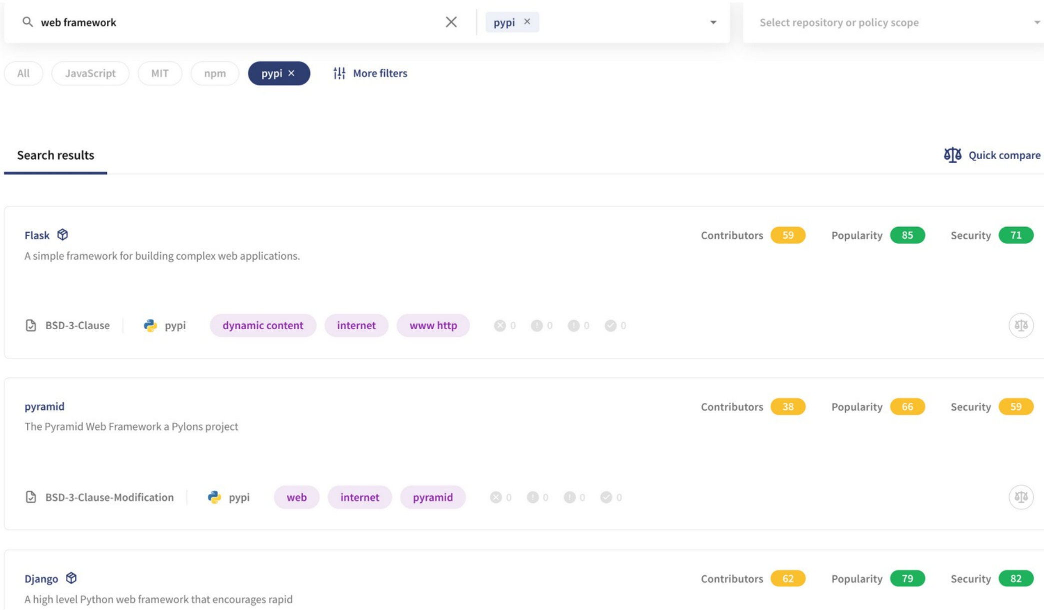
react-dev-utils ✗ 11.0.1 > ✓ 12.0.0

immer ✗ 7.0.9 > ✓ 9.0.6*

Vulnerable dependency immer (npm)

What we’ve done - Part 2/3

- Open Source Health
  - Metrics on open source projec
- Open Source Dependency Grap
  - Approximate PM resolution
  - Vulnerability fix recommendat
- Open Source Select
  - Search engine for open sourc



web framework ✕ | pypi ✕ | Select repository or policy scope

All | JavaScript | MIT | npm | pypi ✕ | More filters

Search results | Quick compare

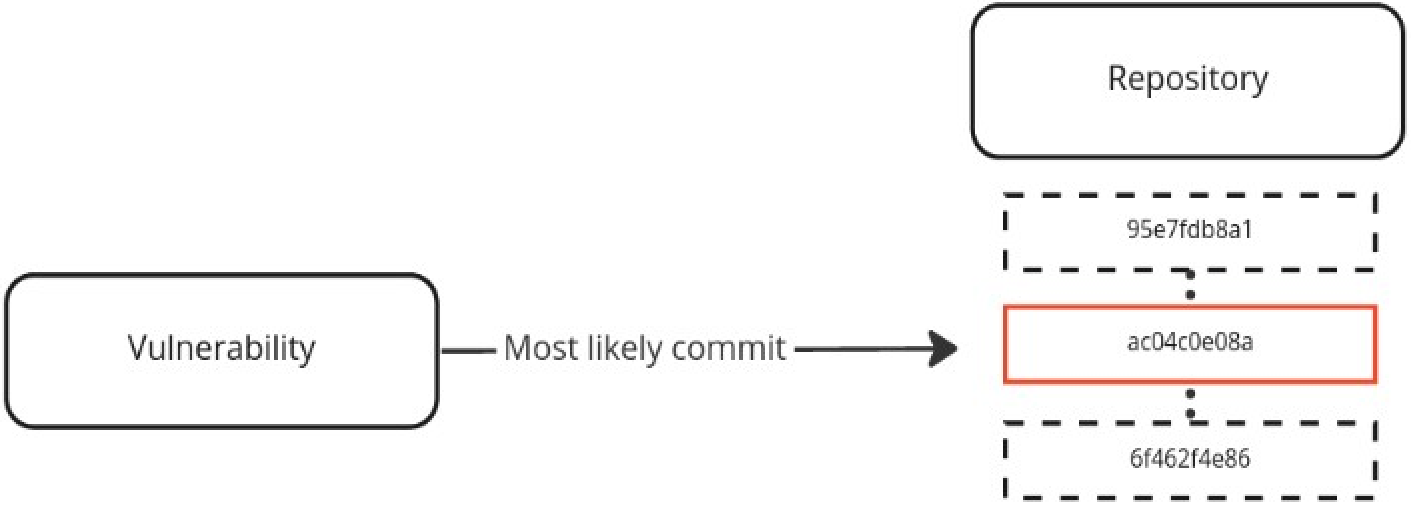
Flask
A simple framework for building complex web applications.
Contributors 59 | Popularity 85 | Security 71
BSD-3-Clause | pypi | dynamic content | internet | www http | 0 | 0 | 0 | 0

pyramid
The Pyramid Web Framework a Pylons project
Contributors 38 | Popularity 66 | Security 59
BSD-3-Clause-Modification | pypi | web | internet | pyramid | 0 | 0 | 0 | 0

Django
A high level Python web framework that encourages rapid
Contributors 62 | Popularity 79 | Security 82

What we’ve done - Part 3/3

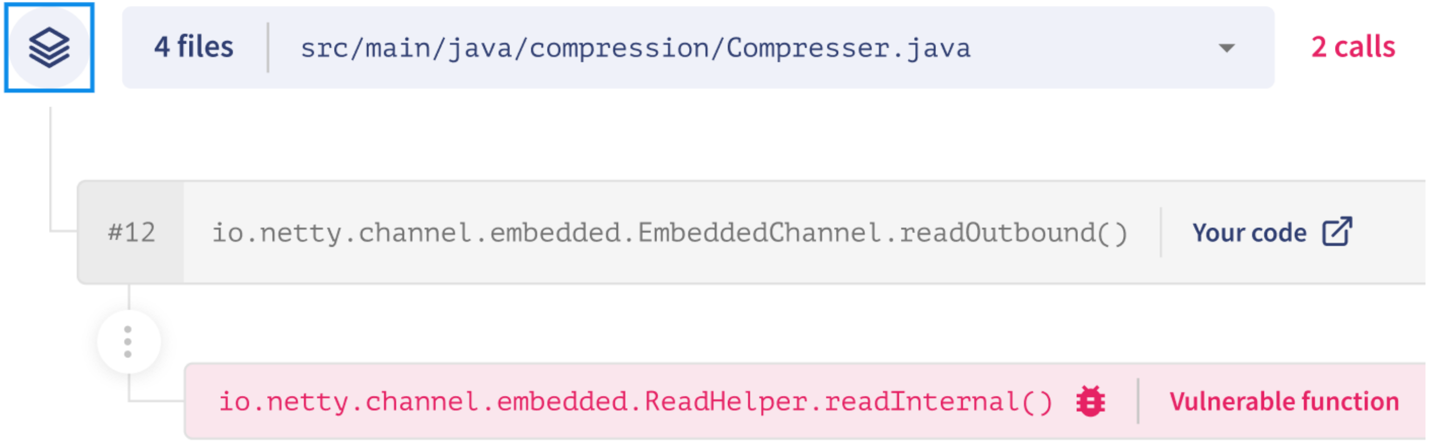
- Vulnerable Functionality
  - Detect vulnerable code via version diff



What we’ve done - Part 3/3

- Vulnerable Functionality
  - Detect vulnerable code via version diff

- Vulnerability Reachability Analysis
  - Check reachability statically for vulnerable functionality



4 files | `src/main/java/compression/Compresser.java`

2 calls

#12 `io.netty.channel.embedded.EmbeddedChannel.readOutbound()` Your code

`io.netty.channel.embedded.ReadHelper.readInternal()` Vulnerable function

What we’ve done - Part 3/3

- Vulnerable Functionality
  - Detect vulnerable code via version diff

- Vulnerability Reachability Analysis
  - Check reachability statically for vulnerable functionality

- ARVOS
  - Check reachability dynamically for vulnerable functionality

Shifting Left at Debricked (1/2)

Has been a focus since early 2022

(we called it StartLeft, but ShiftLeft sounds cooler)

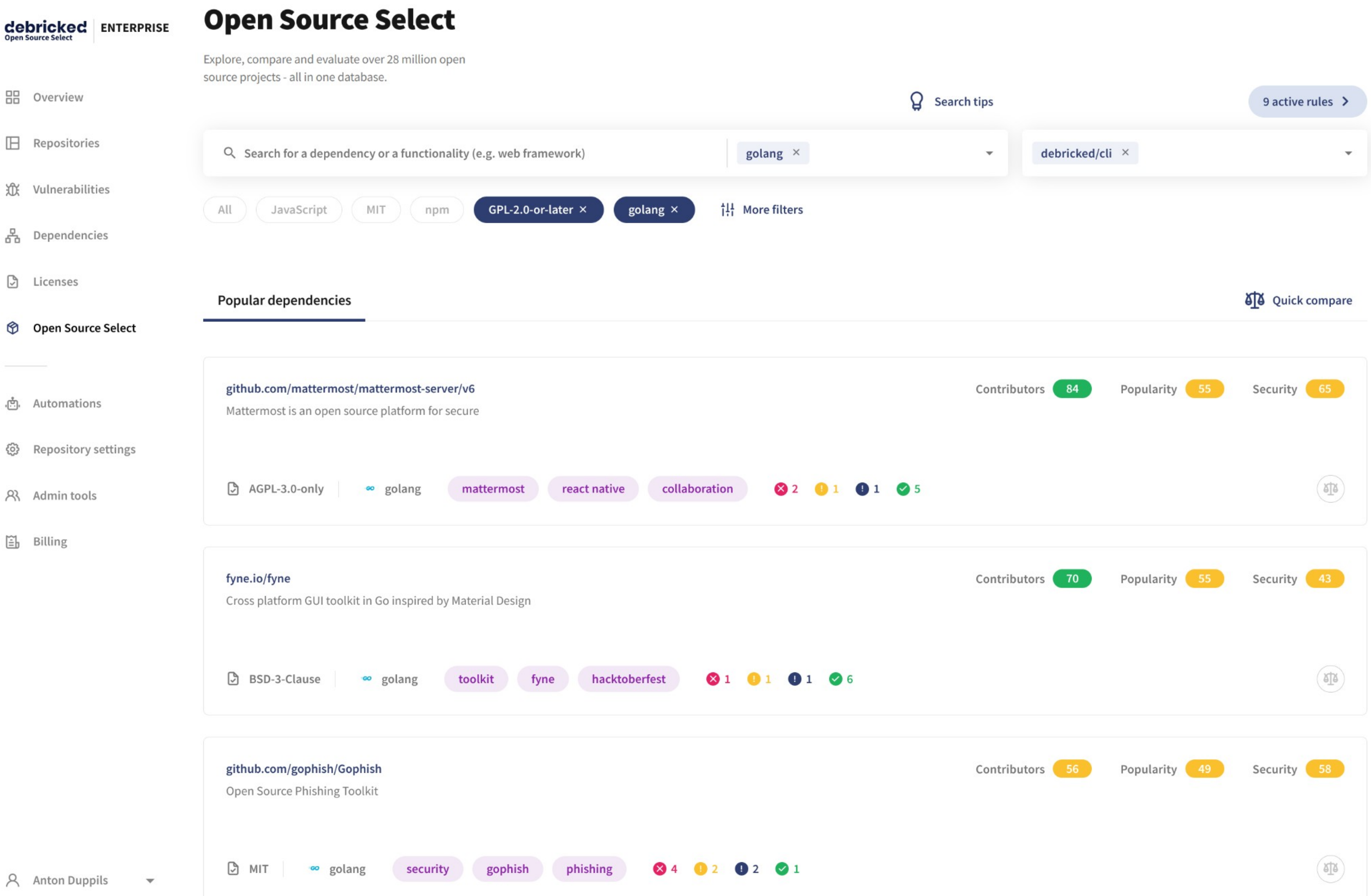
Policies - collection of rules

- If dependency has vulnerability severity (CVSS) >= 5 → **FAIL**
- If dependency has risky license use case → **FAIL**
- If dependency has very low health score or end-of-life → **WARNING**

Shifting Left at Debricked (2/2)

How can problematic open source use be detected earlier?

- **Search engine** - OSS search based on health metrics
- **Chrome extension** - searching on e.g. npm or Github
- **IDE integration** - e.g. mark on import
- **CI/CD** - warn/fail pipeline
- **Monitoring** - detecting issues on branches - *not developer centric*



Open Source Select

Explore, compare and evaluate over 28 million open source projects - all in one database.

github.com/mattermost/mattermost-server/v6

Mattermost is an open source platform for secure

Contributors 84 | Popularity 55 | Security 65

AGPL-3.0-only | golang | mattermost | react native | collaboration | ✕ 2 | ! 1 | ! 1 | ✓ 5

fyne.io/fyne

Cross platform GUI toolkit in Go inspired by Material Design

Contributors 70 | Popularity 55 | Security 43

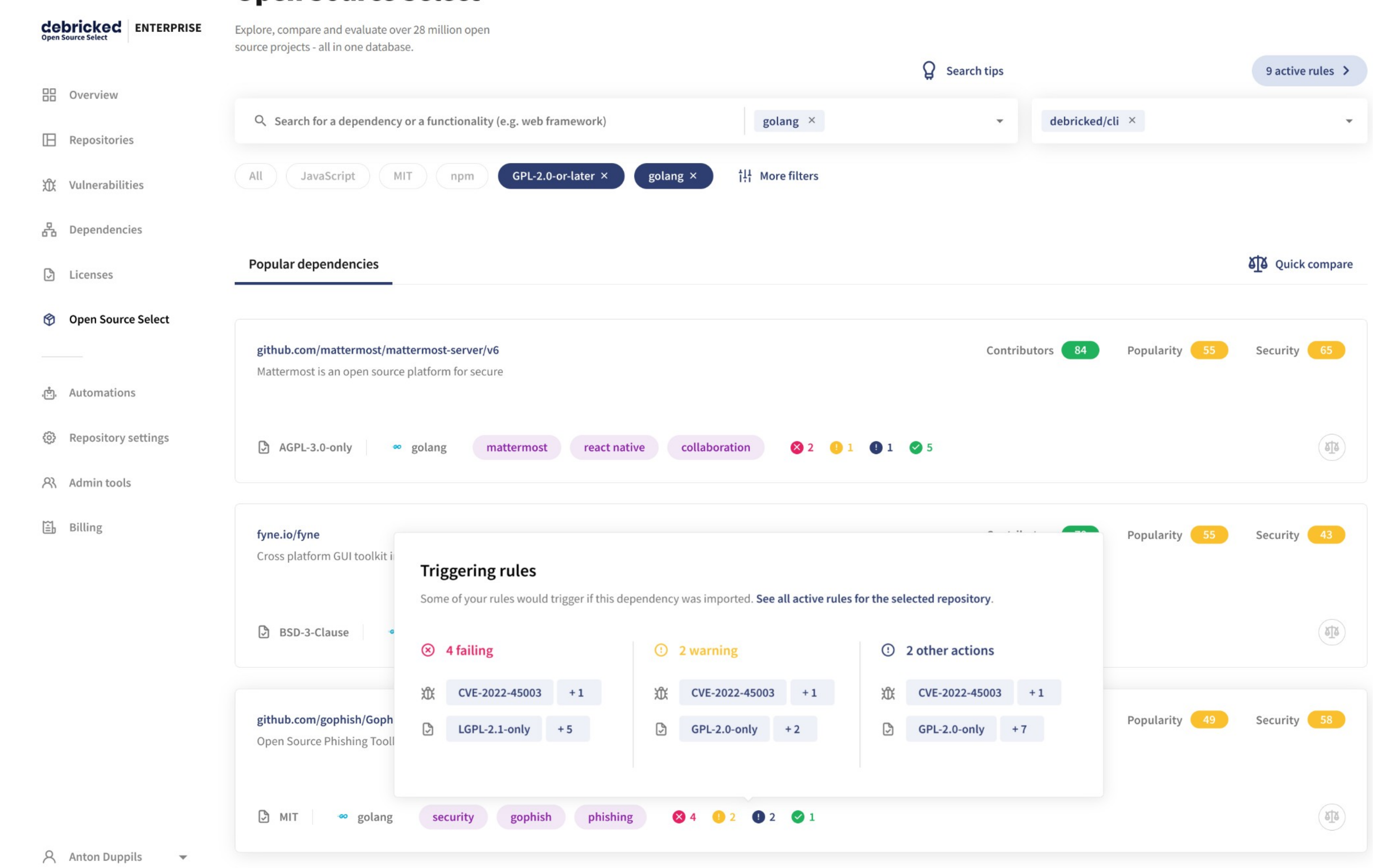
BSD-3-Clause | golang | toolkit | fyne | hacktoberfest | ✕ 1 | ! 1 | ! 1 | ✓ 6

github.com/gophish/Gophish

Open Source Phishing Toolkit

Contributors 56 | Popularity 49 | Security 58

MIT | golang | security | gophish | phishing | ✕ 4 | ! 2 | ! 2 | ✓ 1



Explore, compare and evaluate over 28 million open source projects - all in one database.

github.com/mattermost/mattermost-server/v6
Mattermost is an open source platform for secure

Contributors 84 Popularity 55 Security 65

AGPL-3.0-only | golang | mattermost | react native | collaboration | ✕ 2 ! 1 ! 1 ✓ 5

fyne.io/fyne
Cross platform GUI toolkit i

Popularity 55 Security 43

BSD-3-Clause

Triggering rules

Some of your rules would trigger if this dependency was imported. **See all active rules for the selected repository**.

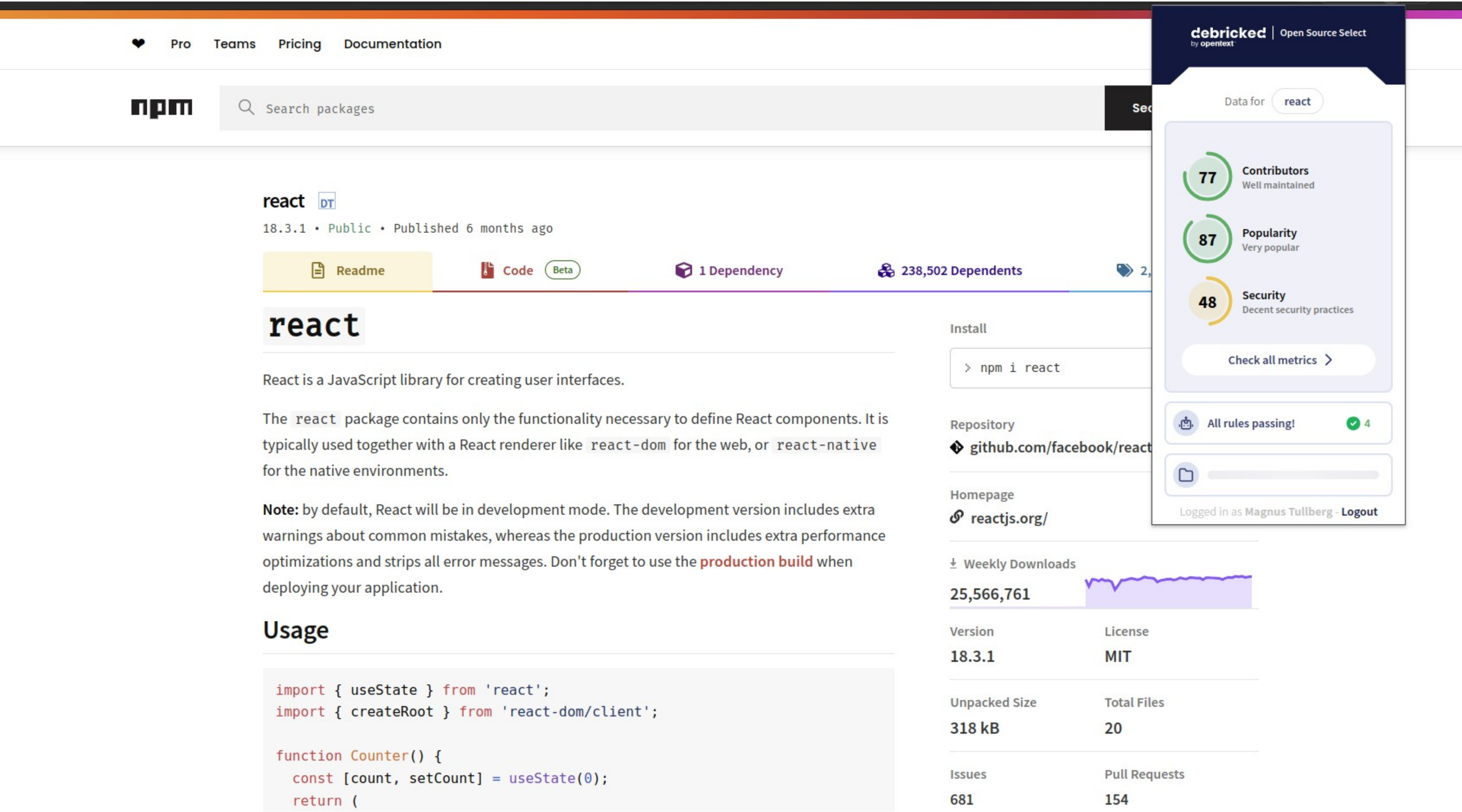
⊗ 4 failing	ⓘ 2 warning	ⓘ 2 other actions
CVE-2022-45003 +1	CVE-2022-45003 +1	CVE-2022-45003 +1
LGPL-2.1-only +5	GPL-2.0-only +2	GPL-2.0-only +7

github.com/gophish/Goph
Open Source Phishing Tool

Popularity 49 Security 58

MIT | golang | security | gophish | phishing | ✕ 4 ! 2 ! 2 ✓ 1

Search url: https://debricked.com/select?license=GPL-2.0-or-later&package-manager=golang&slp-scope=r_46940



react DT

18.3.1 • Public • Published 6 months ago

react

React is a JavaScript library for creating user interfaces.

The `react` package contains only the functionality necessary to define React components. It is typically used together with a React renderer like `react-dom` for the web, or `react-native` for the native environments.

Note: by default, React will be in development mode. The development version includes extra warnings about common mistakes, whereas the production version includes extra performance optimizations and strips all error messages. Don't forget to use the **production build** when deploying your application.

Usage

```
import { useState } from 'react';
import { createRoot } from 'react-dom/client';

function Counter() {
  const [count, setCount] = useState(0);
  return (
```

Install

```
> npm i react
```

Repository
github.com/facebook/react

Homepage
reactjs.org/

Weekly Downloads
25,566,761

Version	License
18.3.1	MIT

Unpacked Size	Total Files
318 kB	20

Issues	Pull Requests
681	154

debricked by opentext | Open Source Select

Data for react

77 Contributors
Well maintained

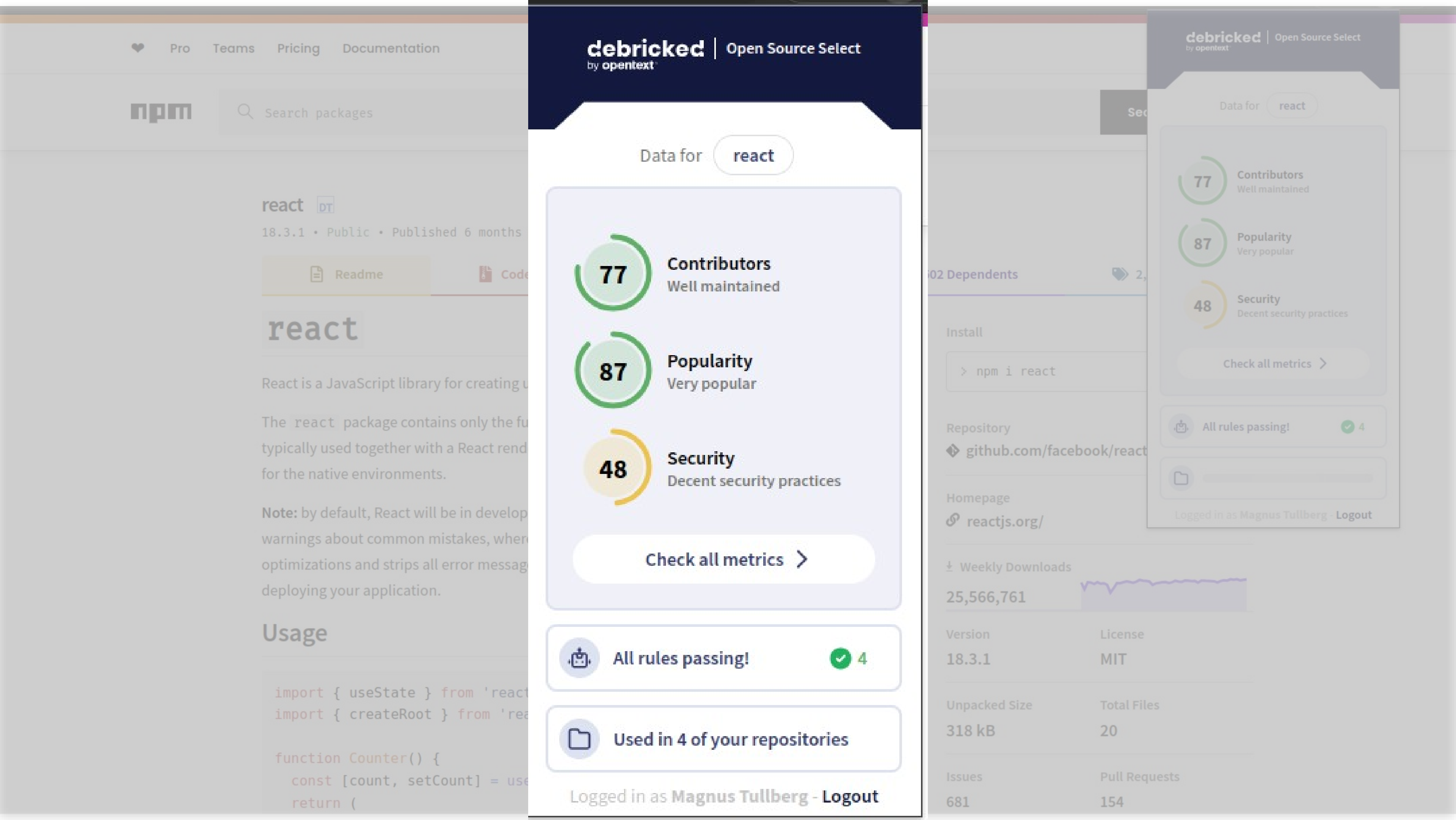
87 Popularity
Very popular

48 Security
Decent security practices

Check all metrics >

All rules passing! ✓ 4

Logged in as Magnus Tullberg - Logout



Data for react

77 Contributors
Well maintained

87 Popularity
Very popular

48 Security
Decent security practices

Check all metrics >

All rules passing! ✓ 4

Used in 4 of your repositories

Logged in as Magnus Tullberg - Logout

react DT
18.3.1 • Public • Published 6 months

Readme | Code | 02 Dependents | 2,

react

React is a JavaScript library for creating u

The `react` package contains only the fu typically used together with a React rend for the native environments.

Note: by default, React will be in develop warnings about common mistakes, where optimizations and strips all error messag deploying your application.

Usage

```
import { useState } from 'react
import { createRoot } from 'rea

function Counter() {
  const [count, setCount] = use
  return (
```

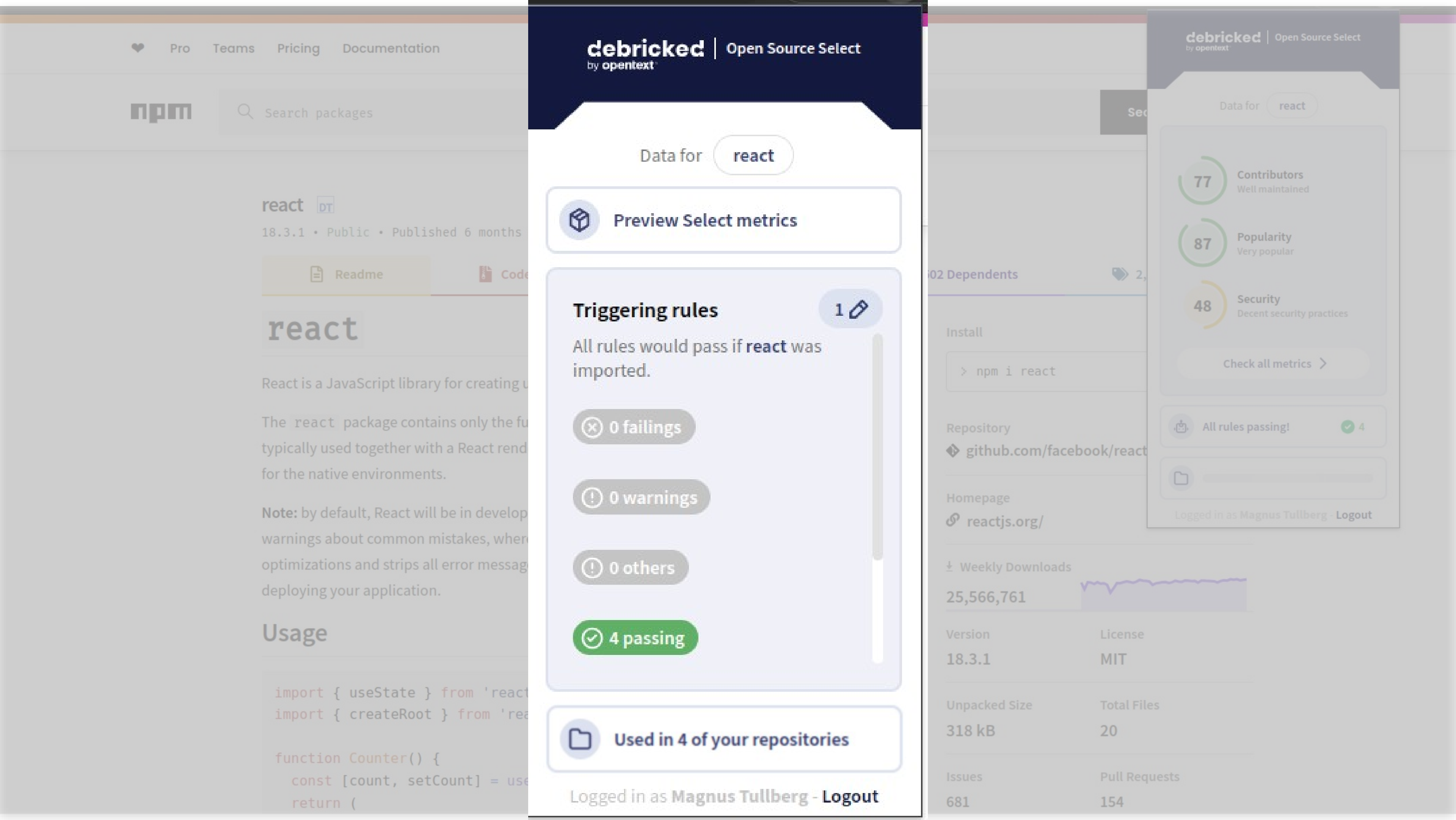
Install
```
> npm i react
```

Repository
github.com/facebook/react

Homepage
reactjs.org/

Weekly Downloads
25,566,761

Version	License
18.3.1	MIT
Unpacked Size	Total Files
318 kB	20
Issues	Pull Requests
681	154



debricked by opentext | Open Source Select

Data for react

Preview Select metrics

Triggering rules 1

All rules would pass if **react** was imported.

0 failings

0 warnings

0 others

4 passing

Used in 4 of your repositories

Logged in as Magnus Tullberg - Logout

debricked by opentext | Open Source Select

Data for react

77 Contributors Well maintained

87 Popularity Very popular

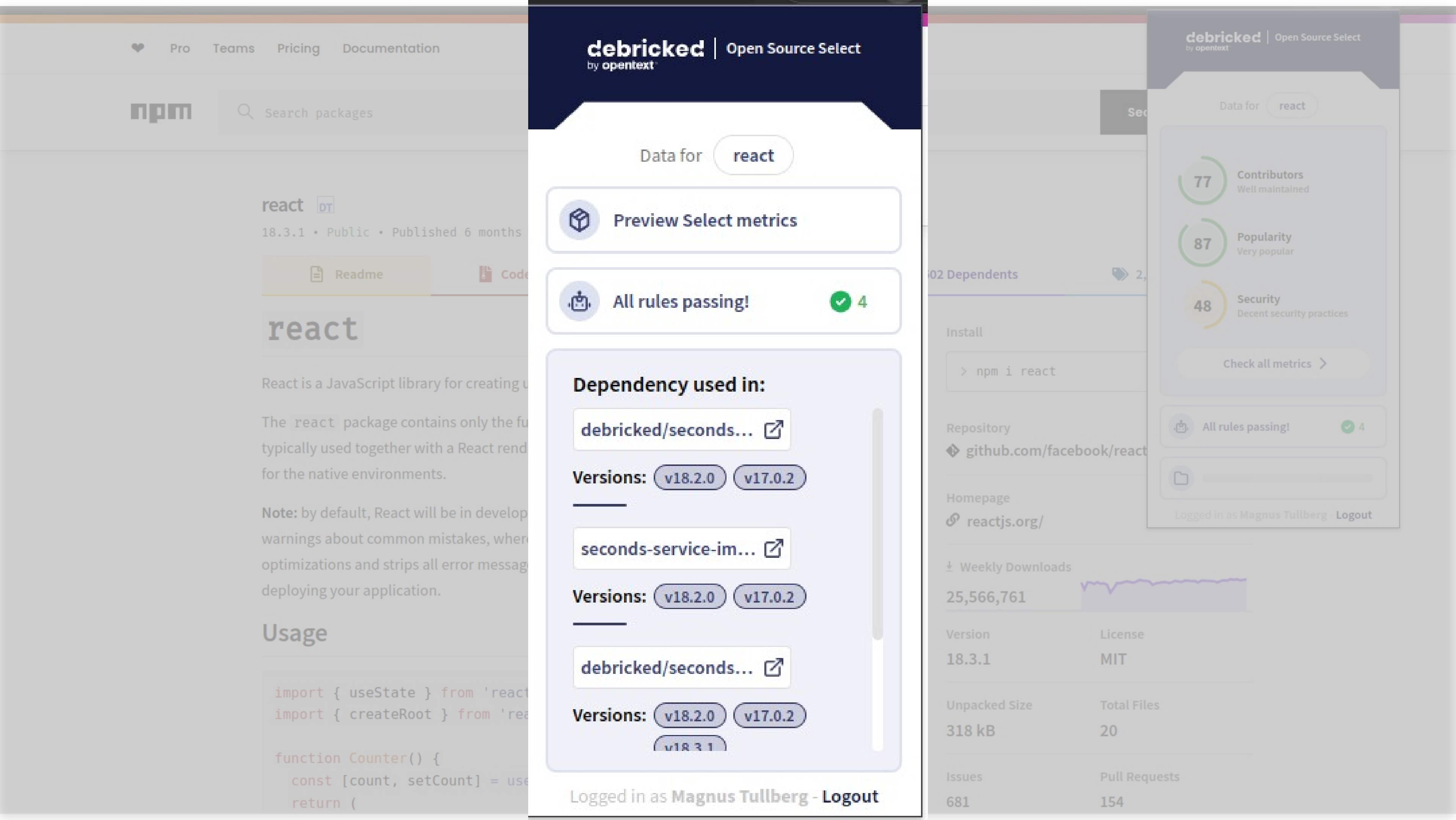
48 Security Decent security practices

Check all metrics

All rules passing! 4

Logged in as Magnus Tullberg - Logout

Pro
Teams
Pricing
Documentation
npm
Search packages
react DT
18.3.1 • Public • Published 6 months
Readme
Code
02 Dependents
react
React is a JavaScript library for creating u
The react package contains only the fu
typically used together with a React rend
for the native environments.
Note: by default, React will be in develop
warnings about common mistakes, where
optimizations and strips all error messag
deploying your application.
Usage
import { useState } from 'react
import { createRoot } from 'rea
function Counter() {
const [count, setCount] = use
return (
Install
npm i react
Repository
github.com/facebook/react
Homepage
reactjs.org/
Weekly Downloads
25,566,761
Version
18.3.1
License
MIT
Unpacked Size
318 kB
Total Files
20
Issues
681
Pull Requests
154



debricked by opentext | Open Source Select

Data for react

Preview Select metrics

All rules passing! ✓ 4

Dependency used in:

debricked/seconds…

Versions: v18.2.0 v17.0.2

seconds-service-im…

Versions: v18.2.0 v17.0.2

debricked/seconds…

Versions: v18.2.0 v17.0.2 v18.3.1

Logged in as Magnus Tullberg - Logout

react DT

18.3.1 • Public • Published 6 months

react

React is a JavaScript library for creating u

The `react` package contains only the fu
typically used together with a React rend
for the native environments.

Note: by default, React will be in develop
warnings about common mistakes, where
optimizations and strips all error messag
deploying your application.

Usage

```
import { useState } from 'react
import { createRoot } from 'rea

function Counter() {
  const [count, setCount] = use
  return (
```

Install

```
> npm i react
```

Repository
github.com/facebook/react

Homepage
reactjs.org/

Weekly Downloads
25,566,761

Version	License
18.3.1	MIT

Unpacked Size	Total Files
318 kB	20

Issues	Pull Requests
681	154

debricked by opentext | Open Source Select

Data for react

77 Contributors
Well maintained

87 Popularity
Very popular

48 Security
Decent security practices

Check all metrics >

All rules passing! ✓ 4

Logged in as Magnus Tullberg - Logout

Thank you for listening!

With the lack of time, feel free to reach out if you have any questions.

Thank you for inviting us to be a part of this exciting project! :)