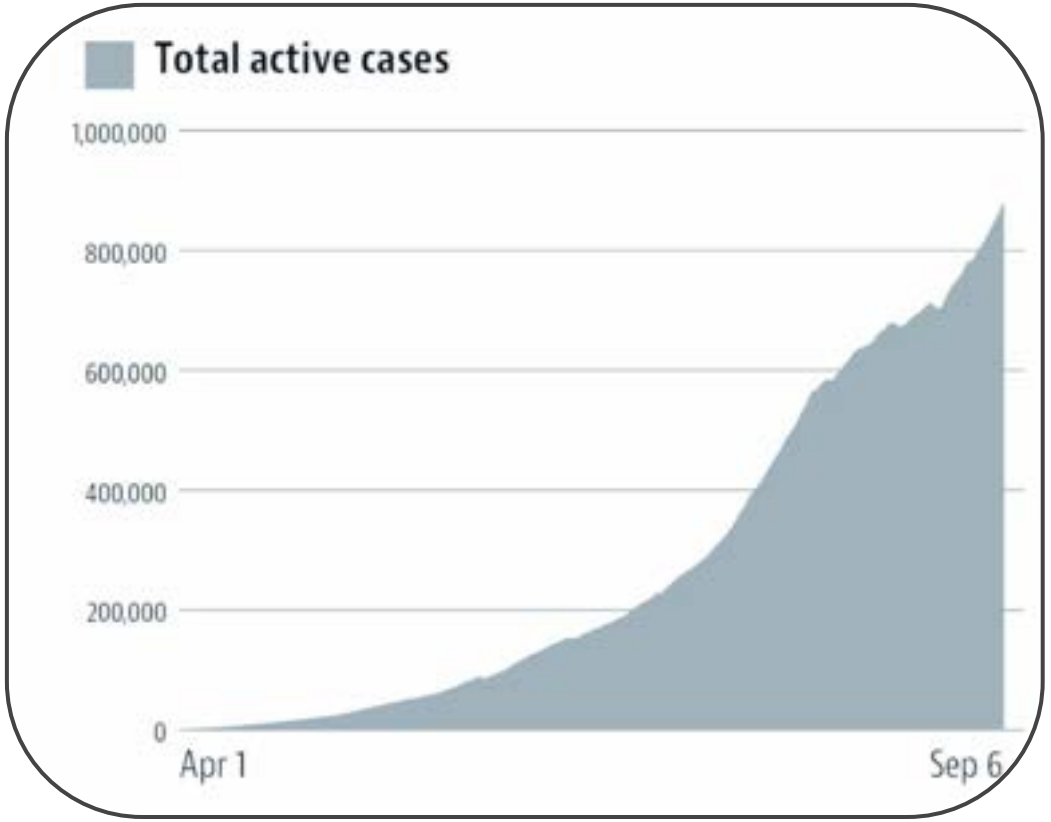
Lessons from Covid-19

A Community-Based Approach to Securing Open Source Software

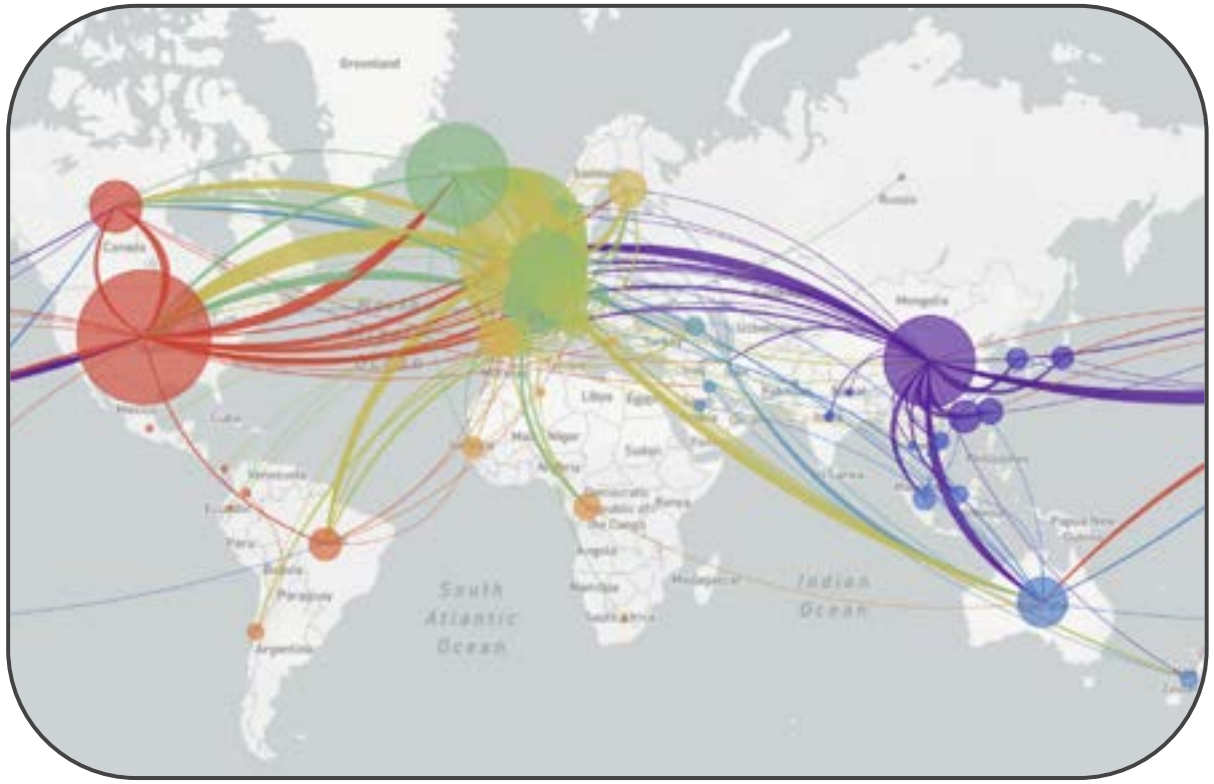
Pedro Nacht, Software Engineer
Google Open Source Security Team
LinkedIn: pedro-nacht

Nikita Jain, Product Marketing Manager
Cybersecurity, Google
LinkedIn: nikitajain88

Exponential growth of Covid

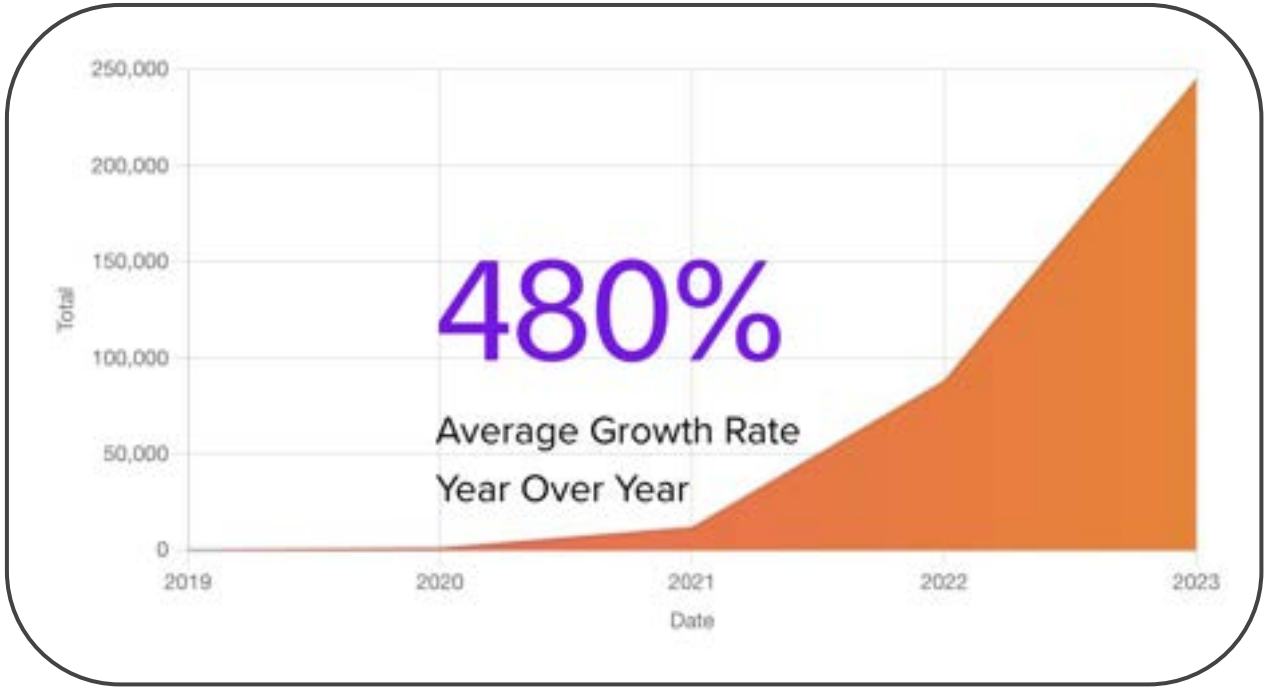


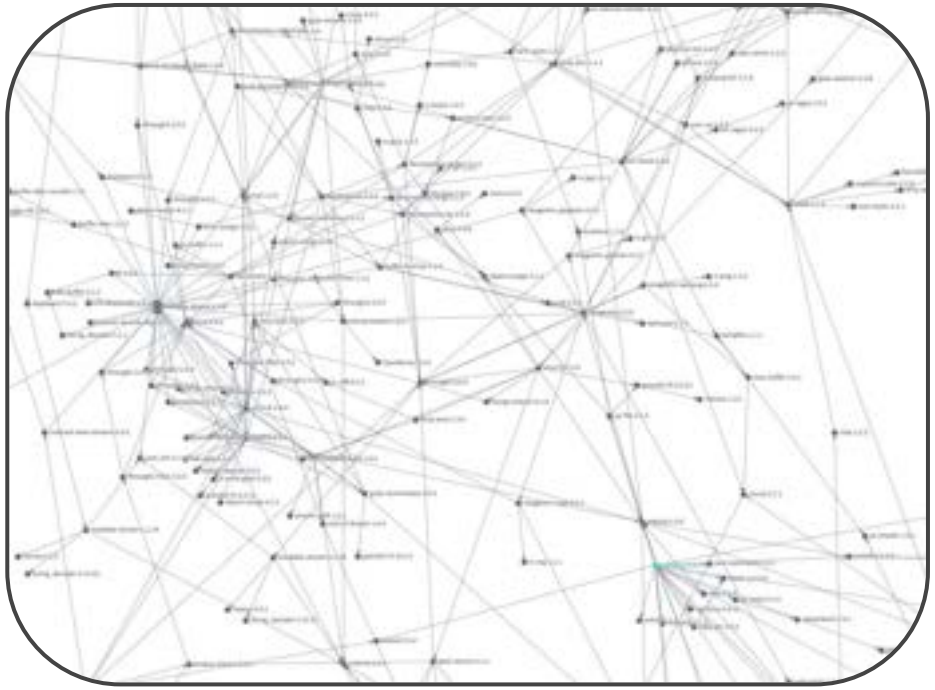
source: hindustantimes.com



source: nextstrain.com

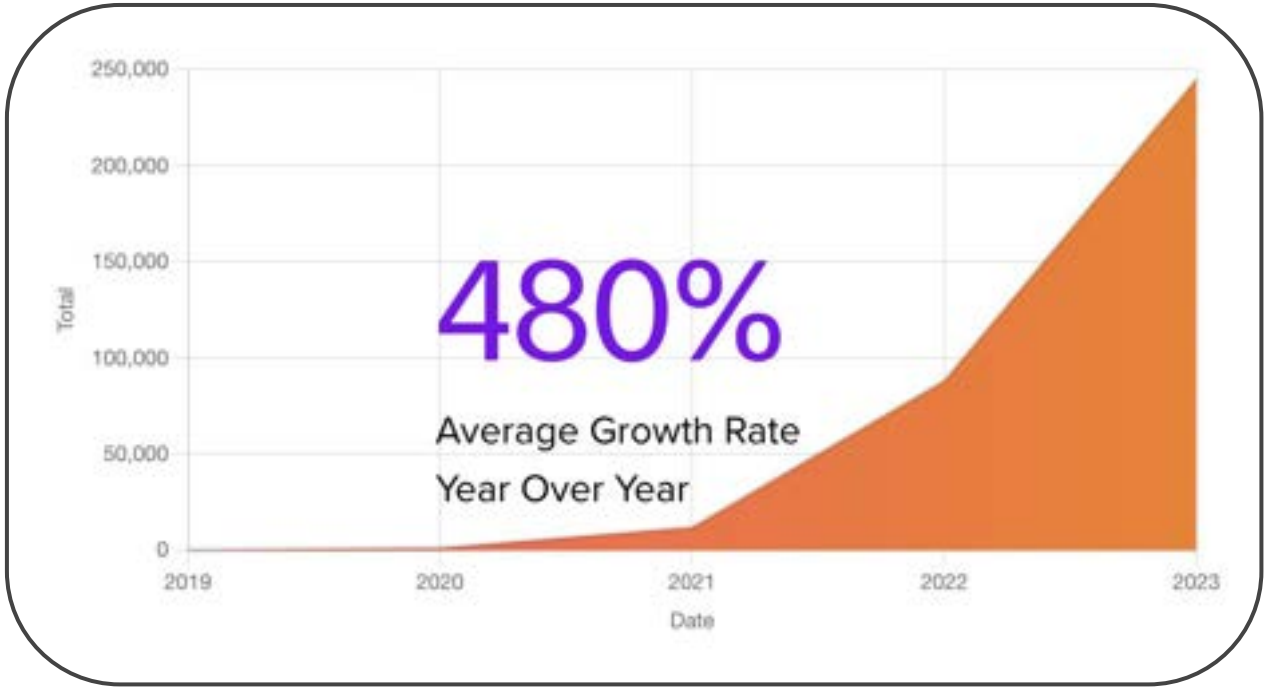
Exponential growth of Covid



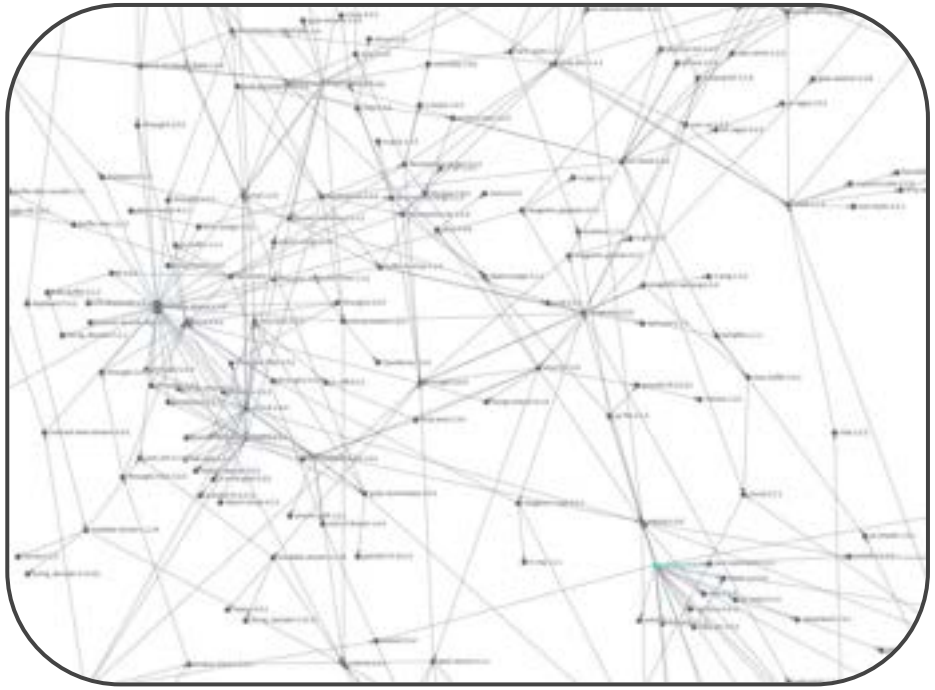


Exponential growth of ~~Covid~~

software supply chain attacks

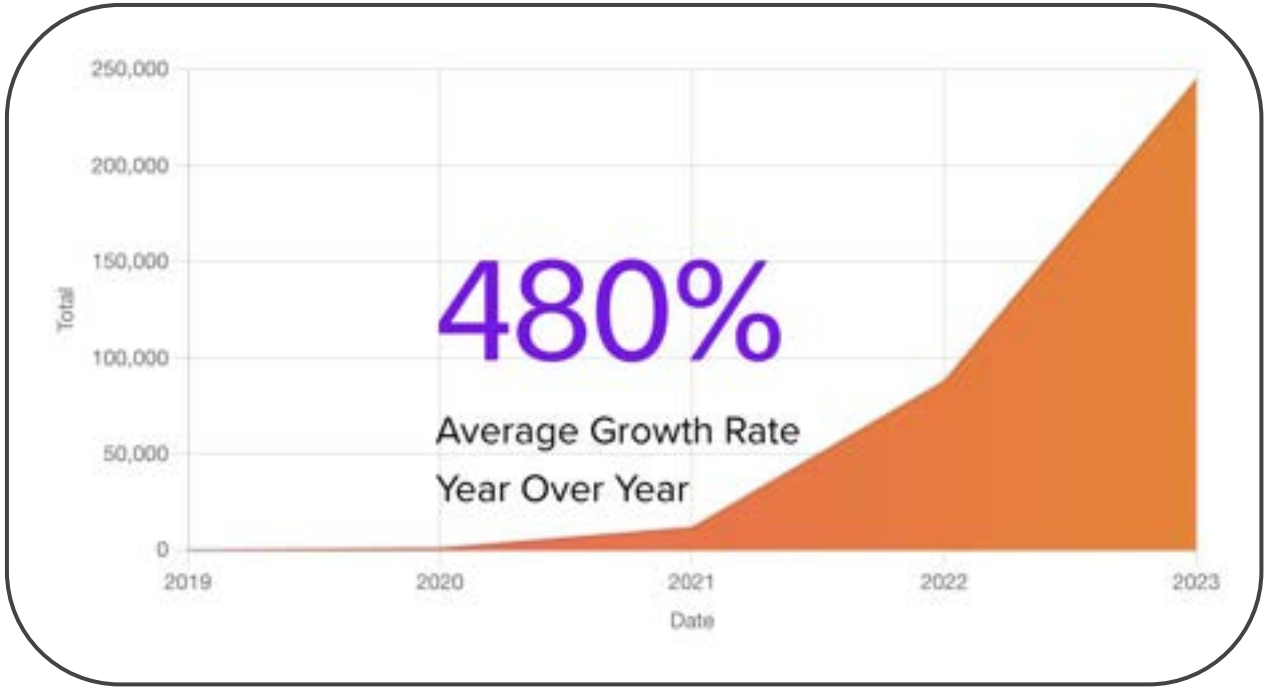


Increase in software supply chain attacks, 2019-2023 (source: Sonatype [modified])



An open source project and its dependencies (source: deps.dev)

Exponential growth of ~~Covid~~ software supply chain attacks



Increase in software supply chain attacks, 2019-2023 (source: Sonatype [modified])

An open source project and its dependencies (source: deps.dev)

AGENDA

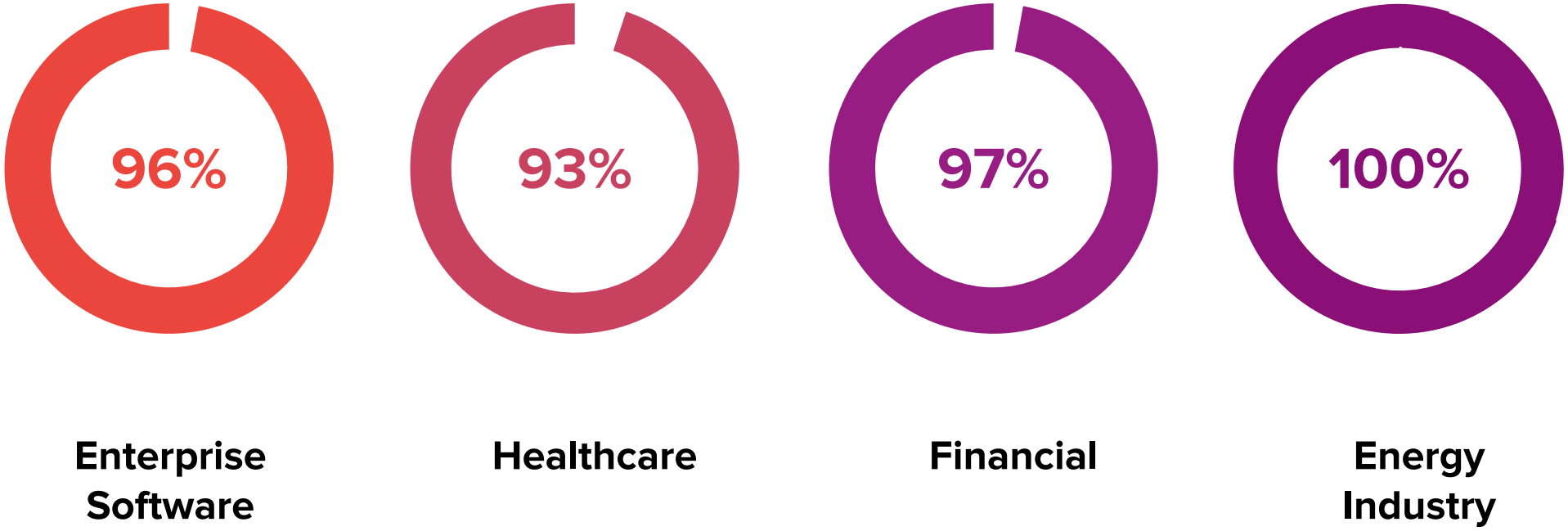
1. What is open source security?
2. What are supply chain attacks?
3. A side trip into your dependencies!
4. Lessons from Covid
5. Questions

AGENDA

1. What is open source security?
2. What are supply chain attacks?
3. A side trip into your dependencies!
4. Lessons from Covid
5. Questions

Open Source Software is everywhere

Including in essential infrastructure

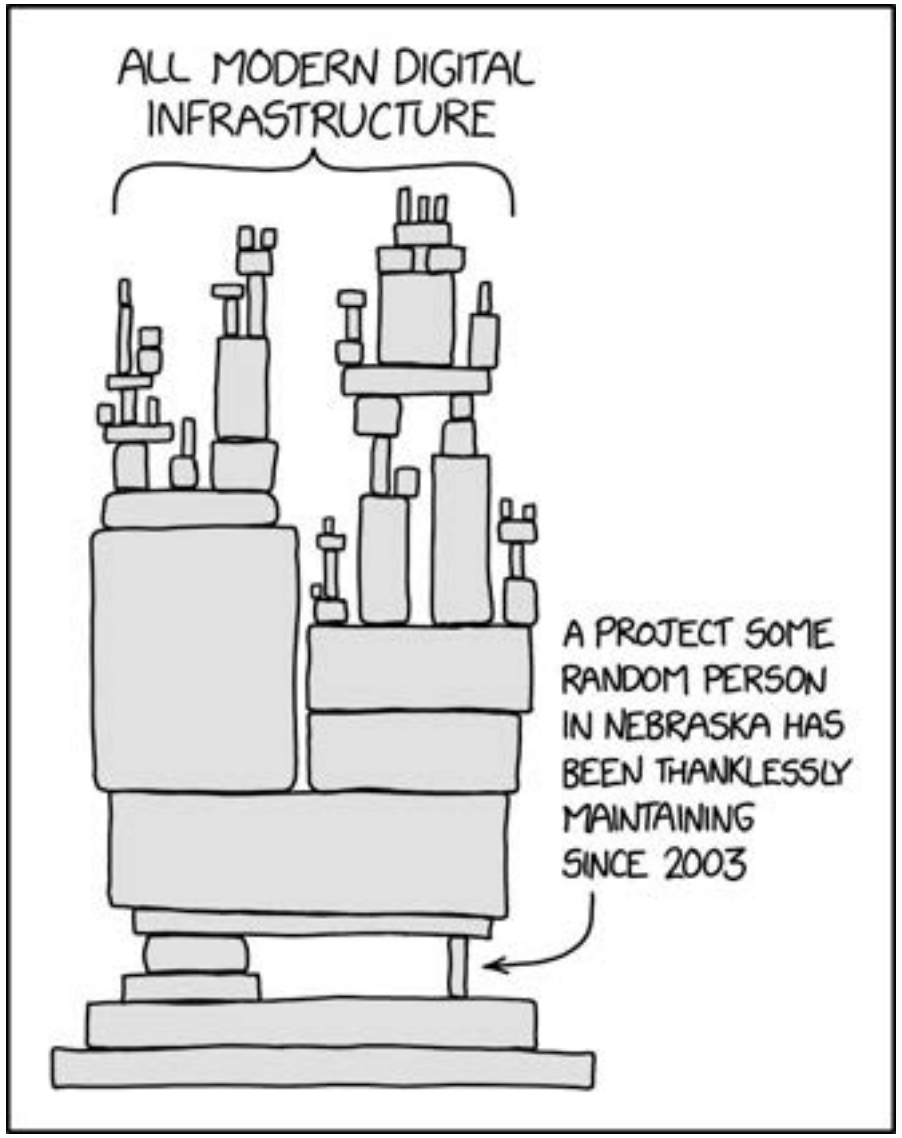


Percentage of surveyed codebases that contain open source code

source: Synopsys

MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity



source: xkcd.com

An overview of supply chain attacks...

Software supply chain attack: when a cyber threat actor infiltrates a software vendor's network and employs malicious code to compromise the software before the vendor sends it to their customers. The compromised software then compromises the customer's data or system. (cisa.gov)

i.e., injecting code into your project to harm those who depend on you

The Next Supply Chain Attack Vector: Open-Source Software

‘The Internet Is on Fire’

A vulnerability in the Log4j logging framework has security teams scrambling to put in a fix.

The Next Supply Chain Attack Vector: Open-Source Software

‘The Internet Is on Fire’

A vulnerability in the Log4j logging framework has security teams scrambling to put in a fix.

The Next Supply Chain Attack Vector: Open-Source Software

Rage-quit: Coder unpublished 17 lines of JavaScript and “broke the Internet”

‘The Internet Is on Fire’

A vulnerability in the Log4j logging framework has security teams scrambling to put in a fix.

The Next Supply Chain Attack Vector: Open-Source Software

Attacks on Software Supply Chains To Increase in Severity in 2023: Report

Rage-quit: Coder unpublished 17 lines of JavaScript and “broke the Internet”

‘The Internet Is on Fire’

A vulnerability in the Log4j logging framework has security teams scrambling to put in a fix.

The Next Supply Chain Attack Vector: Open-Source Software

Banking Sector Targeted in Open-Source Software Supply Chain Attacks

Attacks on Software Supply Chains To Increase in Severity in 2023: Report

Rage-quit: Coder unpublished 17 lines of JavaScript and “broke the Internet”

‘The Internet Is on Fire’

A vulnerability in the Log4j logging framework has security teams scrambling to put in a fix.

Software Supply Chain Attacks Hit 61% of Firms

The Next Supply Chain Attack Vector: Open-Source Software

Banking Sector Targeted in Open-Source Software Supply Chain Attacks

Attacks on Software Supply Chains To Increase in Severity in 2023: Report

Rage-quit: Coder unpublished 17 lines of JavaScript and “broke the Internet”

Researchers find 633% increase in cyber-attacks aimed at open source repositories

'The Internet Is on Fire'

A vulnerability in the Log4j logging framework has security teams scrambling to put in a fix.

Software Supply Chain Attacks Hit 61% of Firms

The Next Supply Chain Attack Vector: Open-Source Software

Banking Sector Targeted in Open-Source Software Supply Chain Attacks

Attacks on Software Supply Chains To Increase in Severity in 2023: Report

Rage-quit: Coder unpublished 17 lines of JavaScript and "broke the Internet"

But the code is open to inspect!

So what’s the problem??

But the code is open to inspect!

So what’s the problem??

[redacted] commented on Nov 22, 2018 Owner •••

he emailed me and said he wanted to maintain the module, so I gave it to him. I don't get any thing from maintaining this module, and I don't even use it anymore, and havn't for years.

👍 346 👎 580 😄 179 🎉 60 😕 110 ❤️ 135

Link

[redacted] commented on Nov 22, 2018 Owner •••

he emailed me and said he wanted to maintain the module, so I gave it to him. I don't get any thing from maintaining this module, and I don't even use it anymore, and havn't for years.

👍 346 👎 580 😄 179 🎉 60 😕 110 ❤️ 135

Link

Open source security...

...and public health lessons??

Int J Environ Res Public Health. 2023 Feb; 20(3): 1785.
Published online 2023 Jan 18. doi: 10.3390/ijerph20031785

PMCID: PMC9914715
PMID: 36767152

Lessons Learned from the Lessons Learned in Public Health during the First Years of COVID-19 Pandemic

Alessia Marcassoli,[1,*] Matilde Leonardi,[1,*] Marco Passavanti,[1] Valerio De Angelis,[2] Enrico Bentivegna,[2] Paolo Martelletti,[2] and Alberto Raggi[1]

Paul B. Tchounwou, Academic Editor

Three lessons to come!

1) Evaluating risks
2) Monitoring
3) Communication

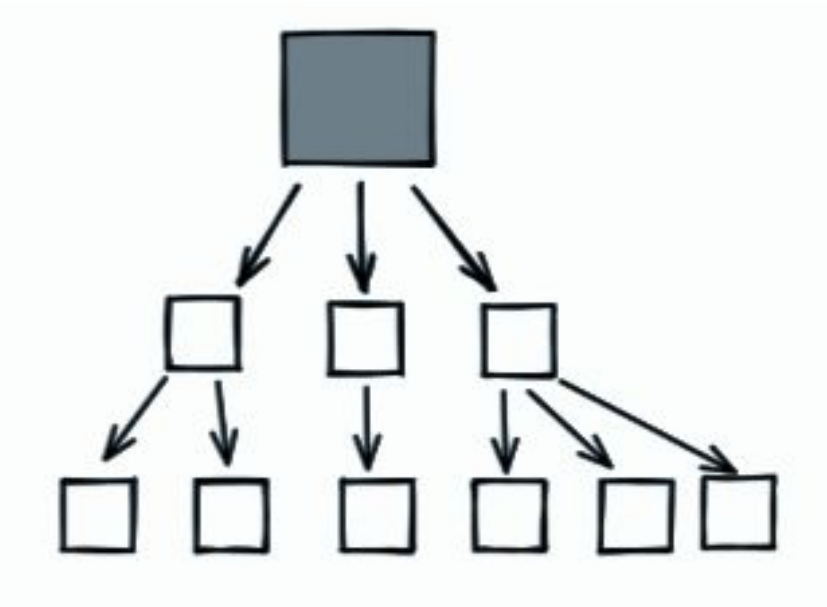
A quick side trip...

into your **dependencies**

Thank you to Nicky Ringland (@nickyringland),
Josie Anugerah, and Eve Martin-Jones of Google's deps.dev team
for sharing the following dependency diagrams and stats!

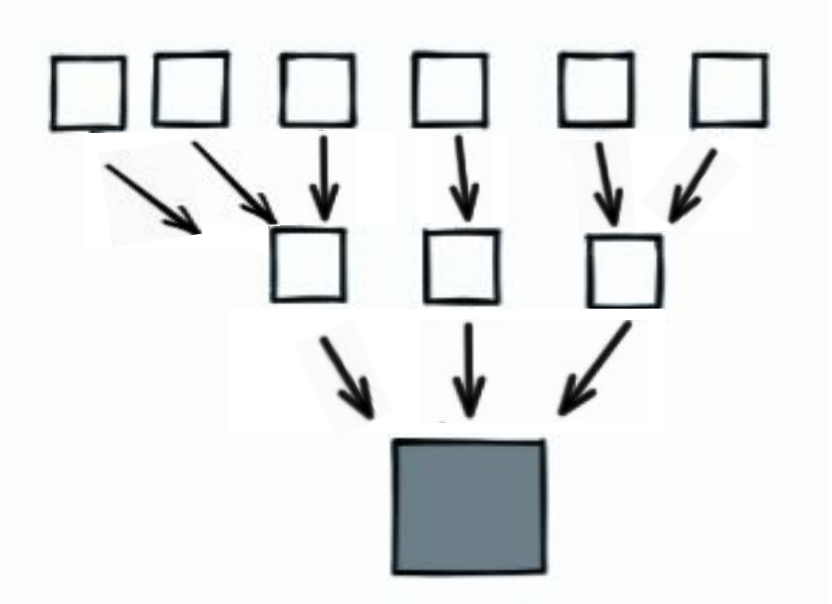
Dependencies

the projects you rely on

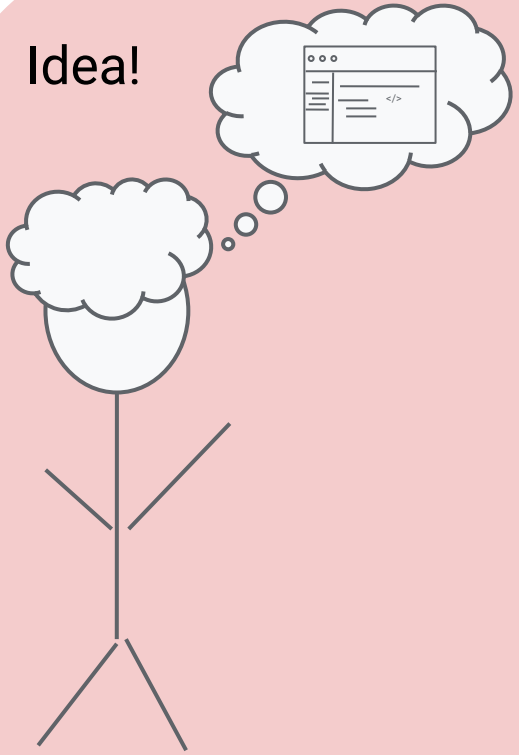


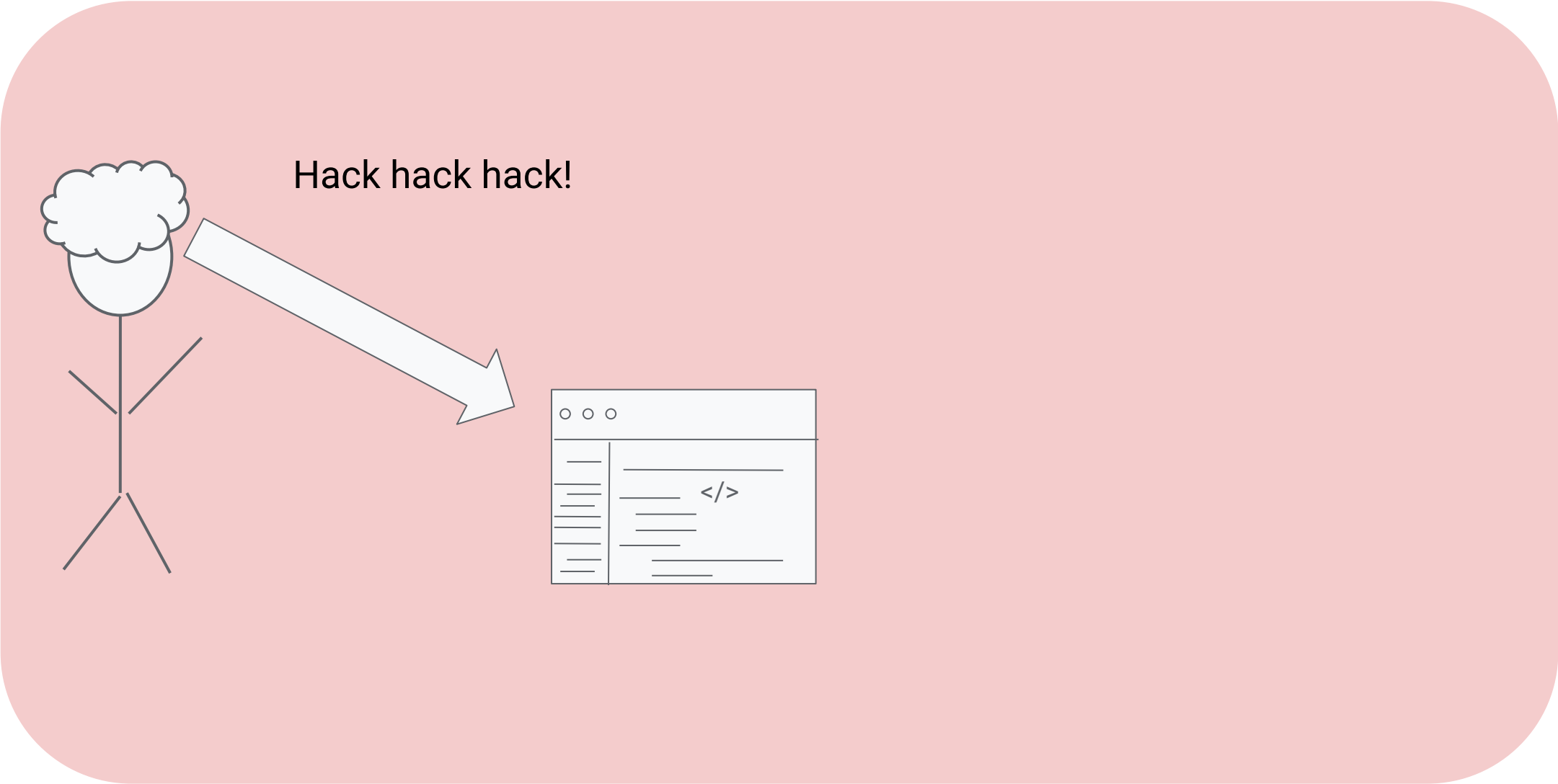
Dependents (or reverse dependencies)

the projects that rely on you

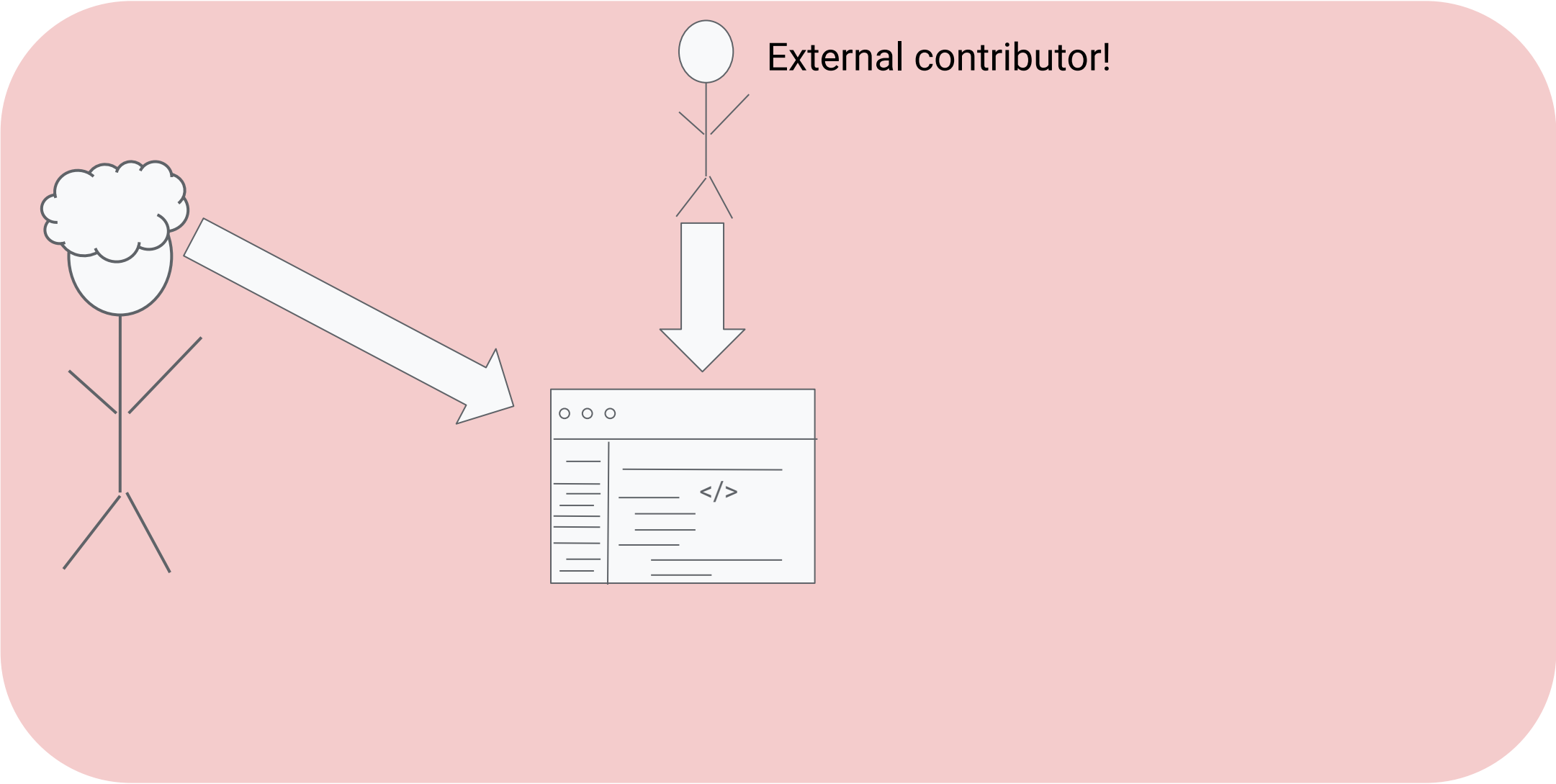


Idea!



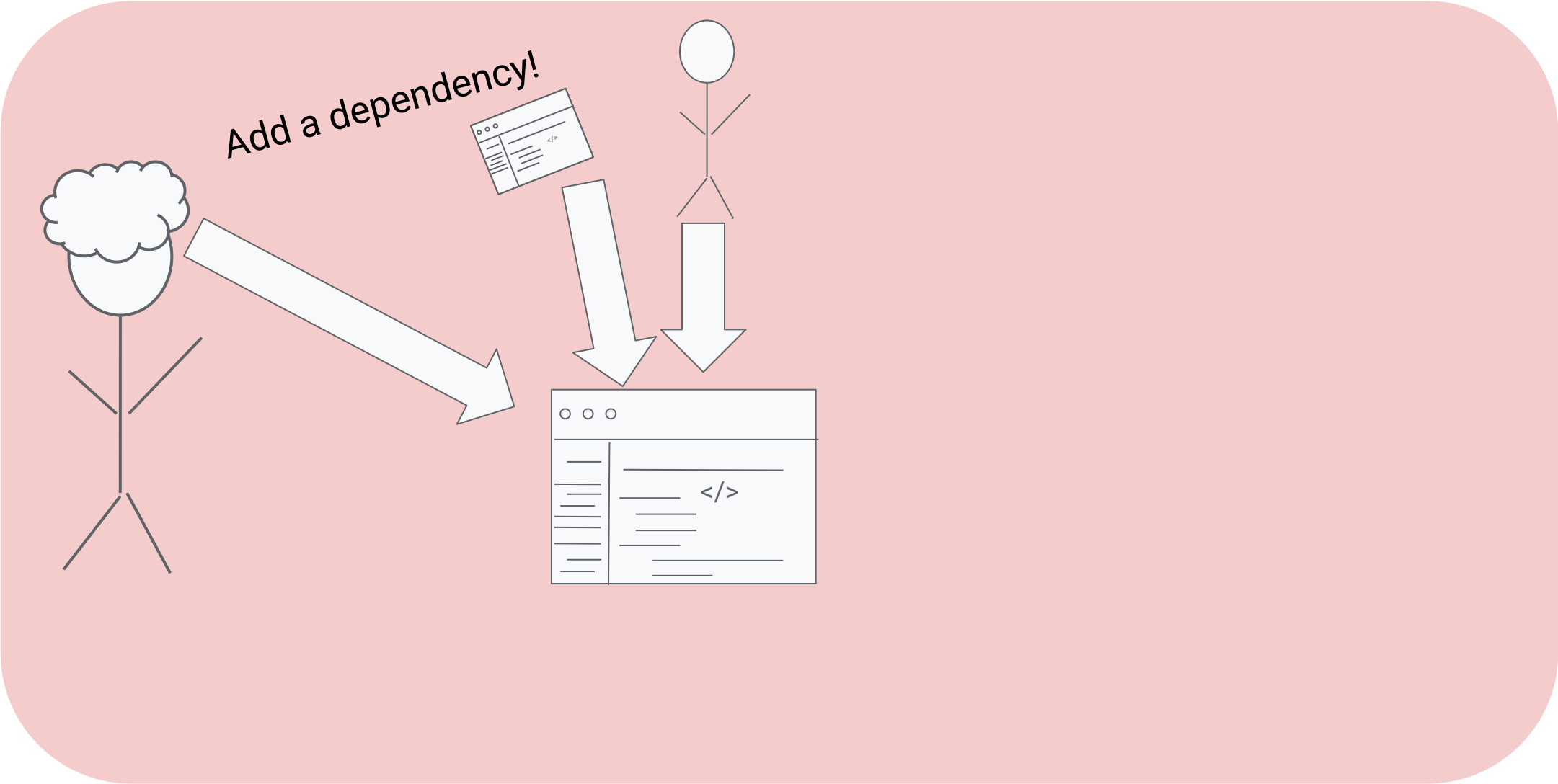


YOUR
code



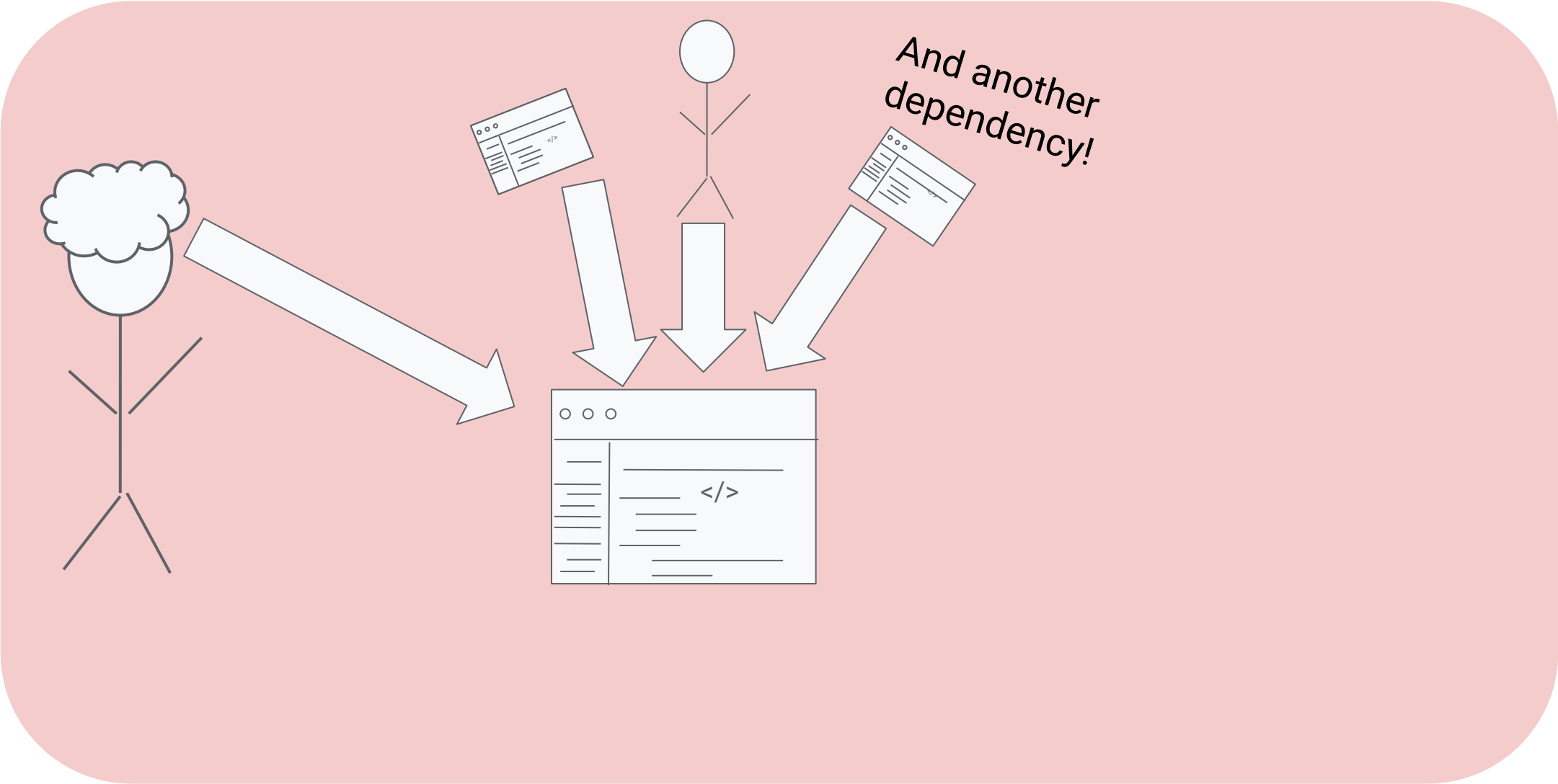
YOUR
code

OTHER
code



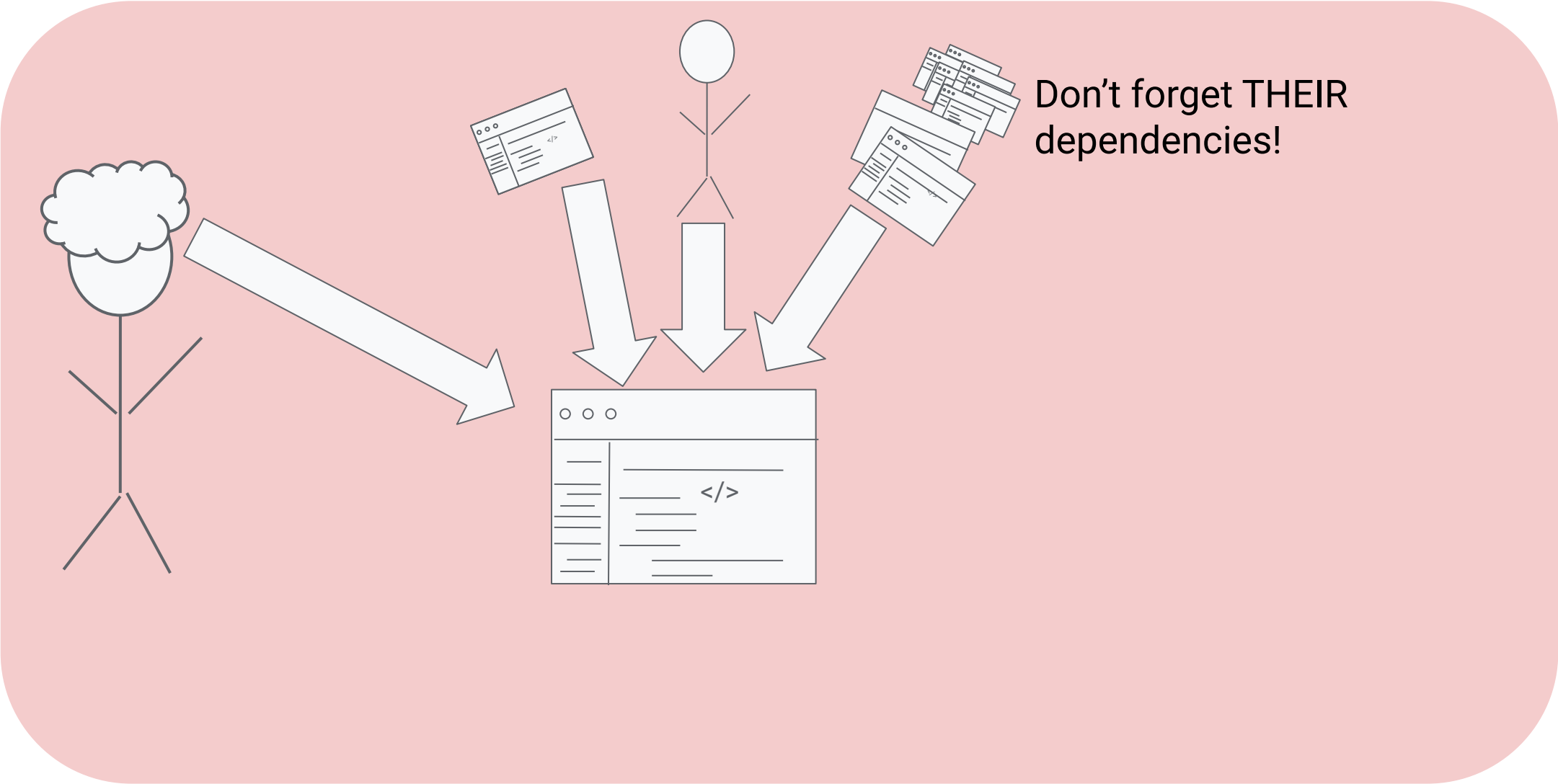
YOUR
code

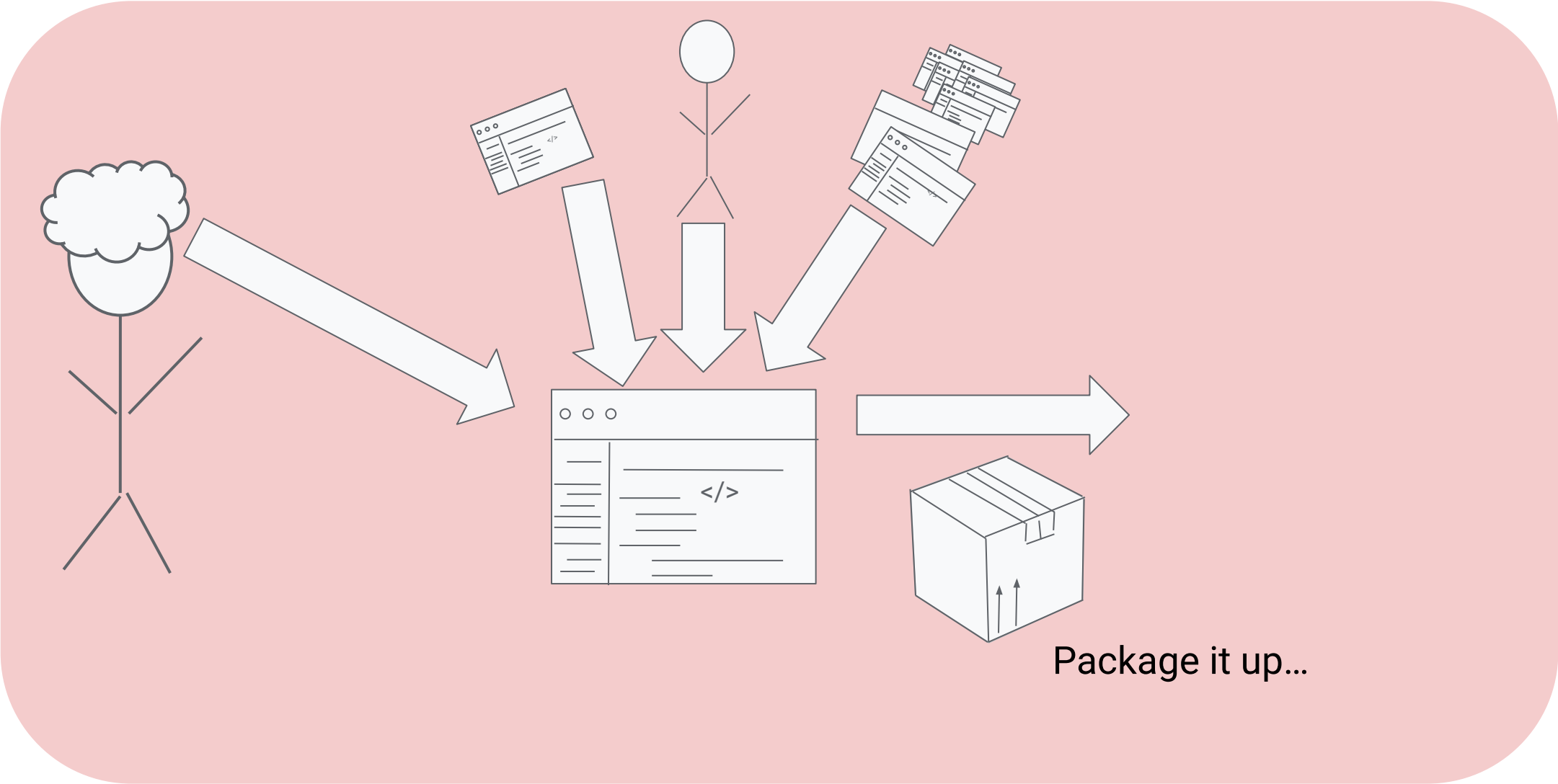
OTHER
code



YOUR code

OTHER code


Don’t forget THEIR dependencies!
YOUR code
OTHER code



YOUR code

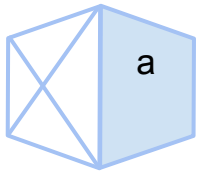
OTHER code

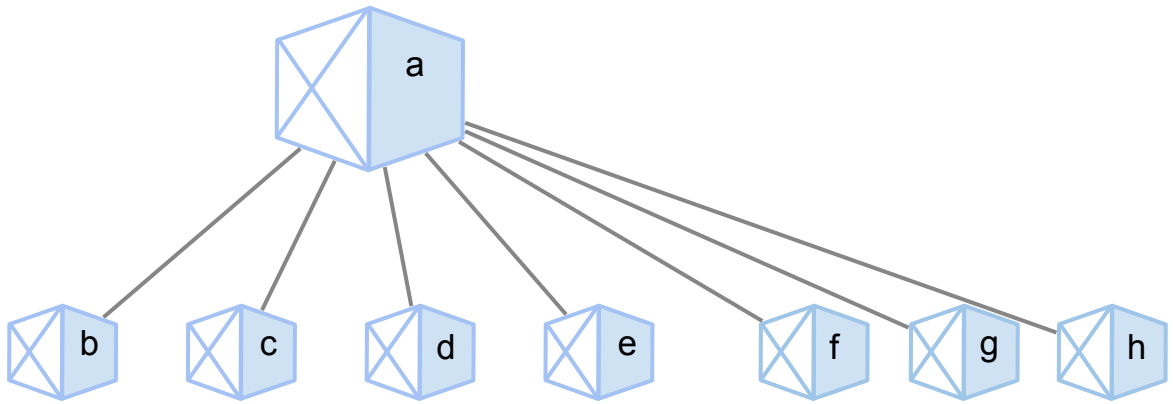
SHARING code

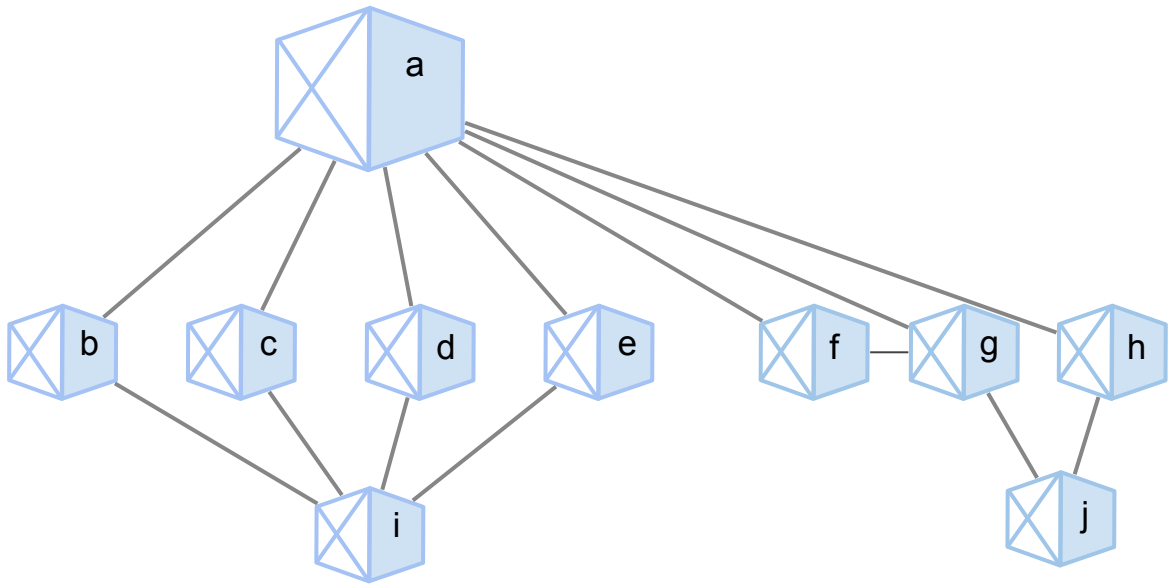
YOUR
code

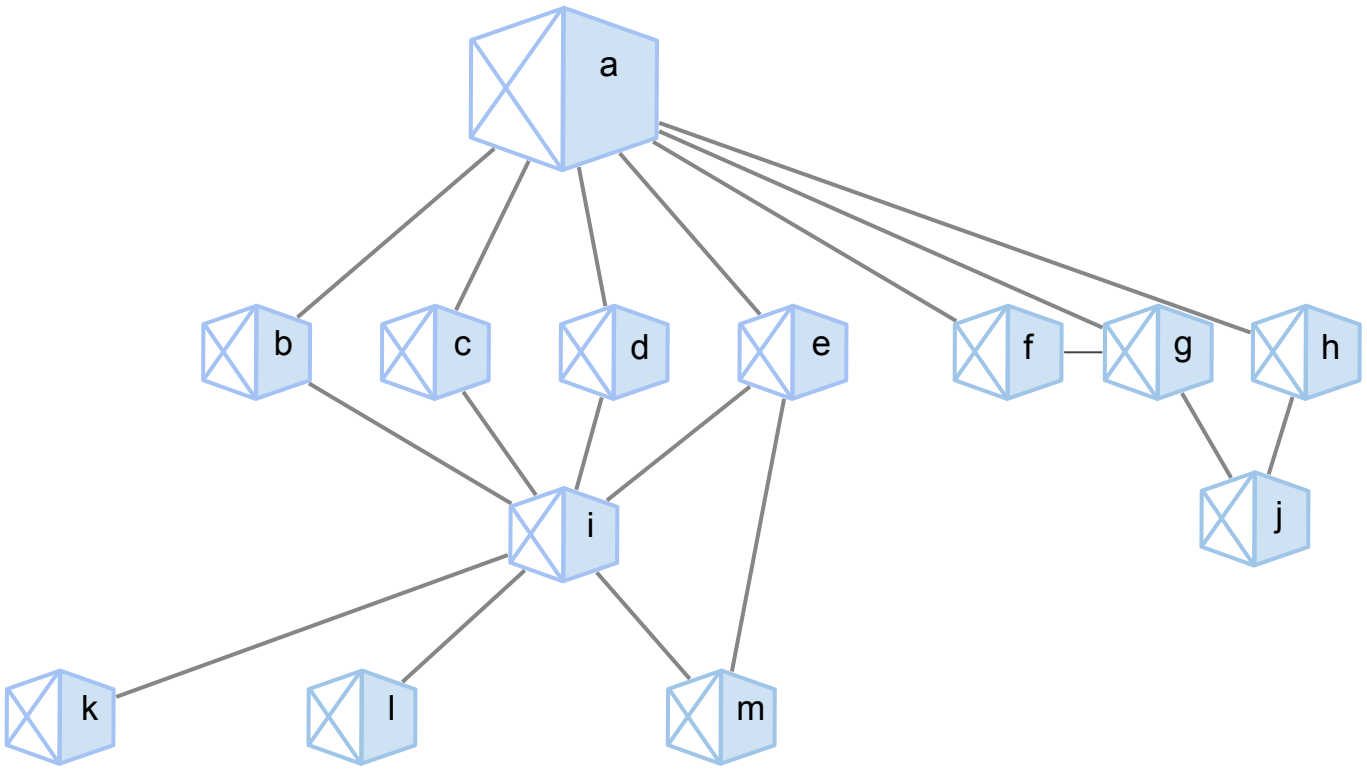
OTHER
code

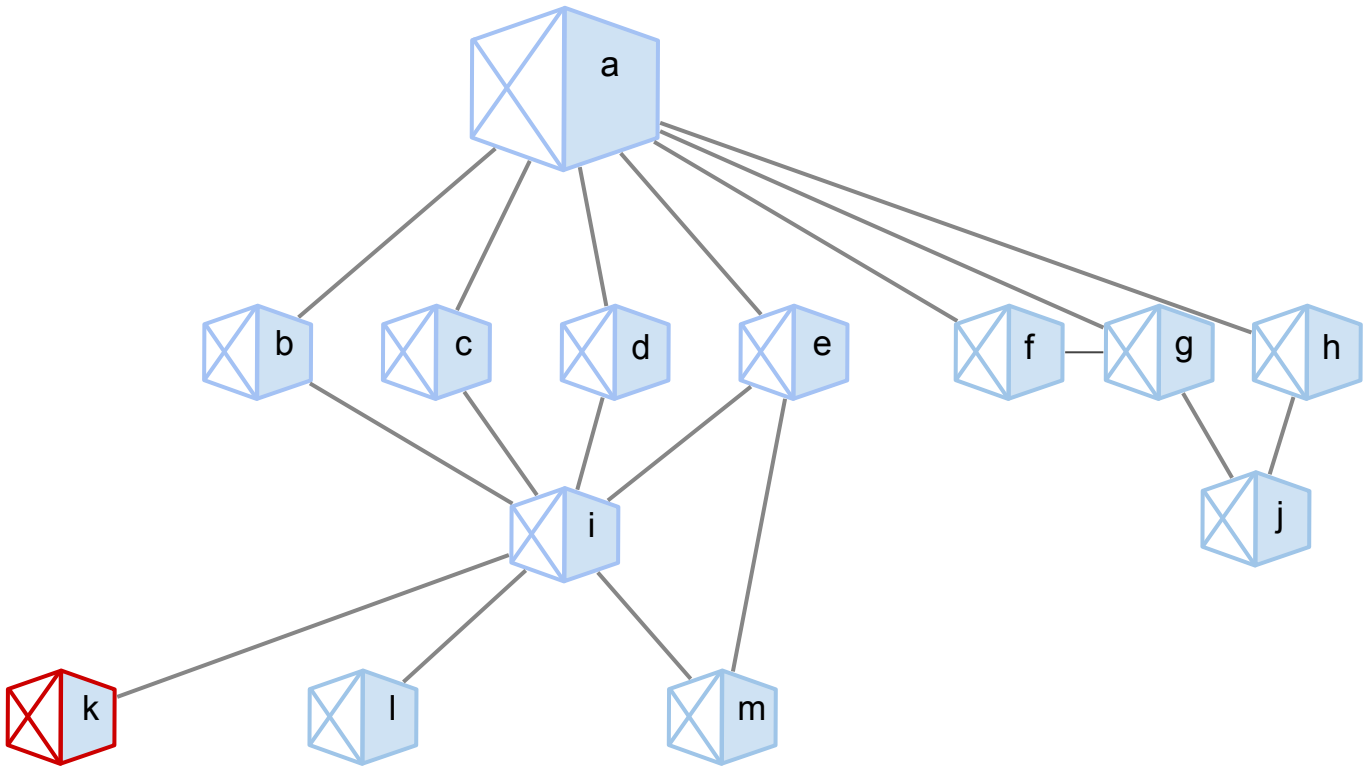
SHARING
code

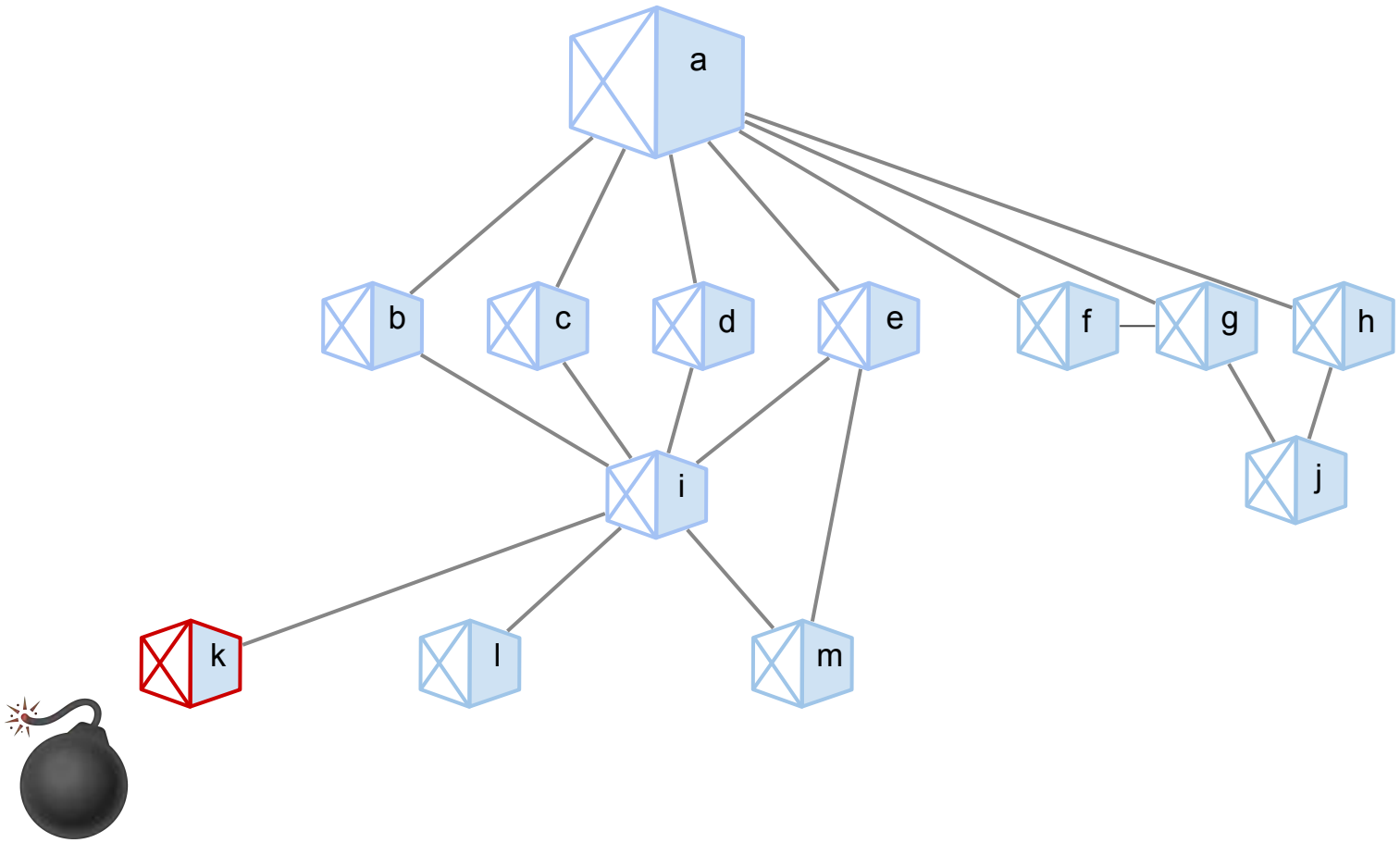

a

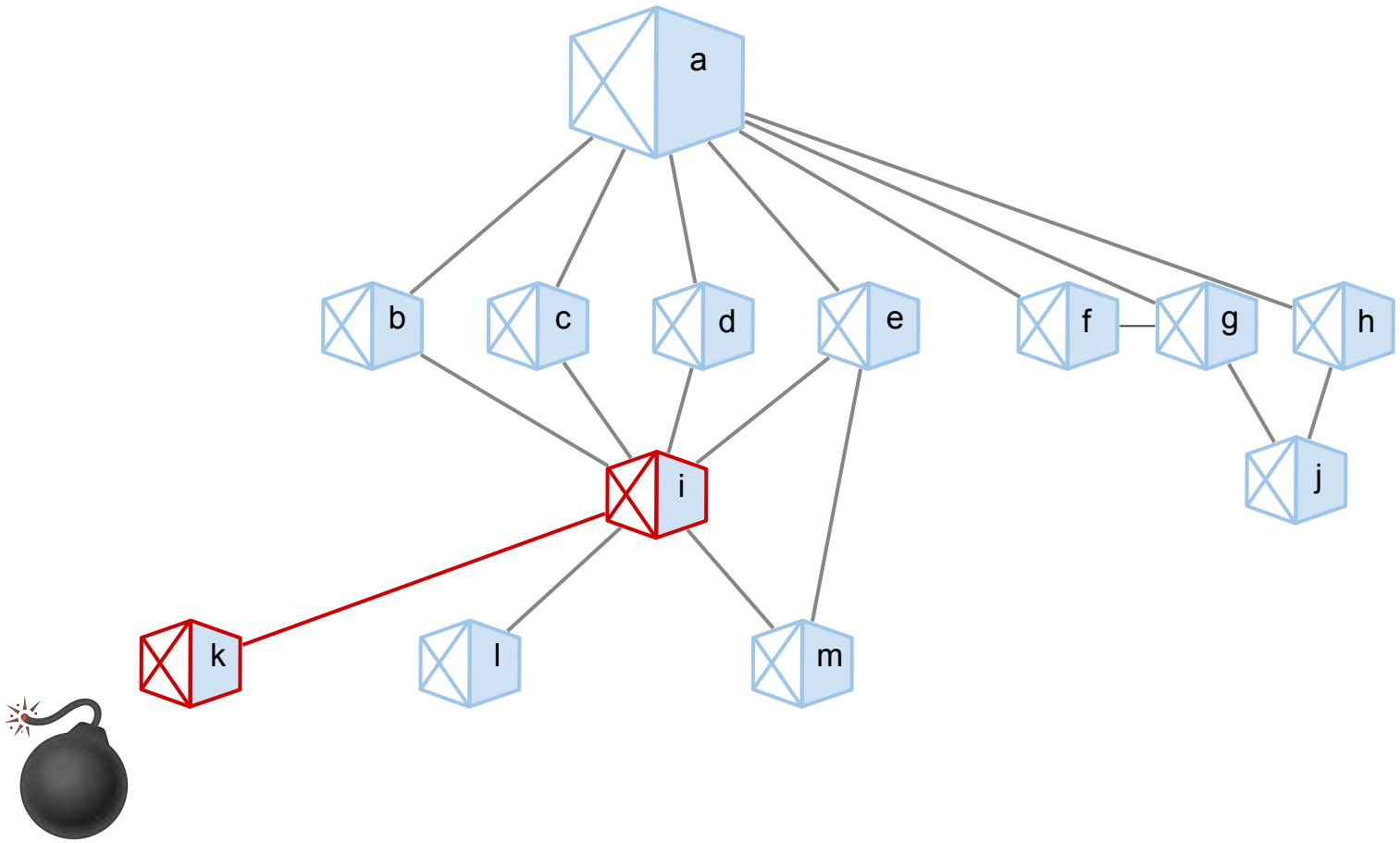

a
b
c
d
e
f
g
h

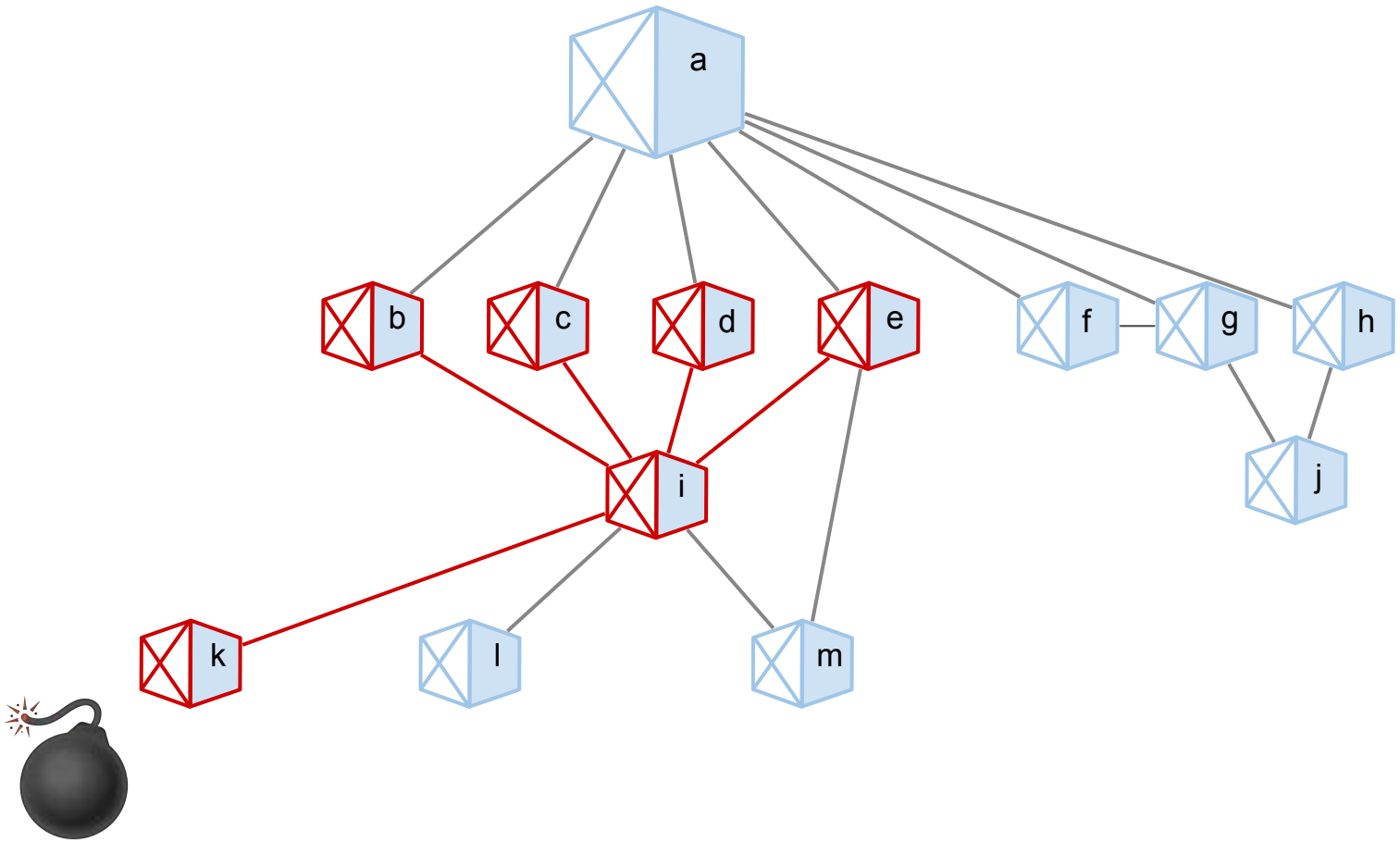

a
b
c
d
e
f
g
h
i
j

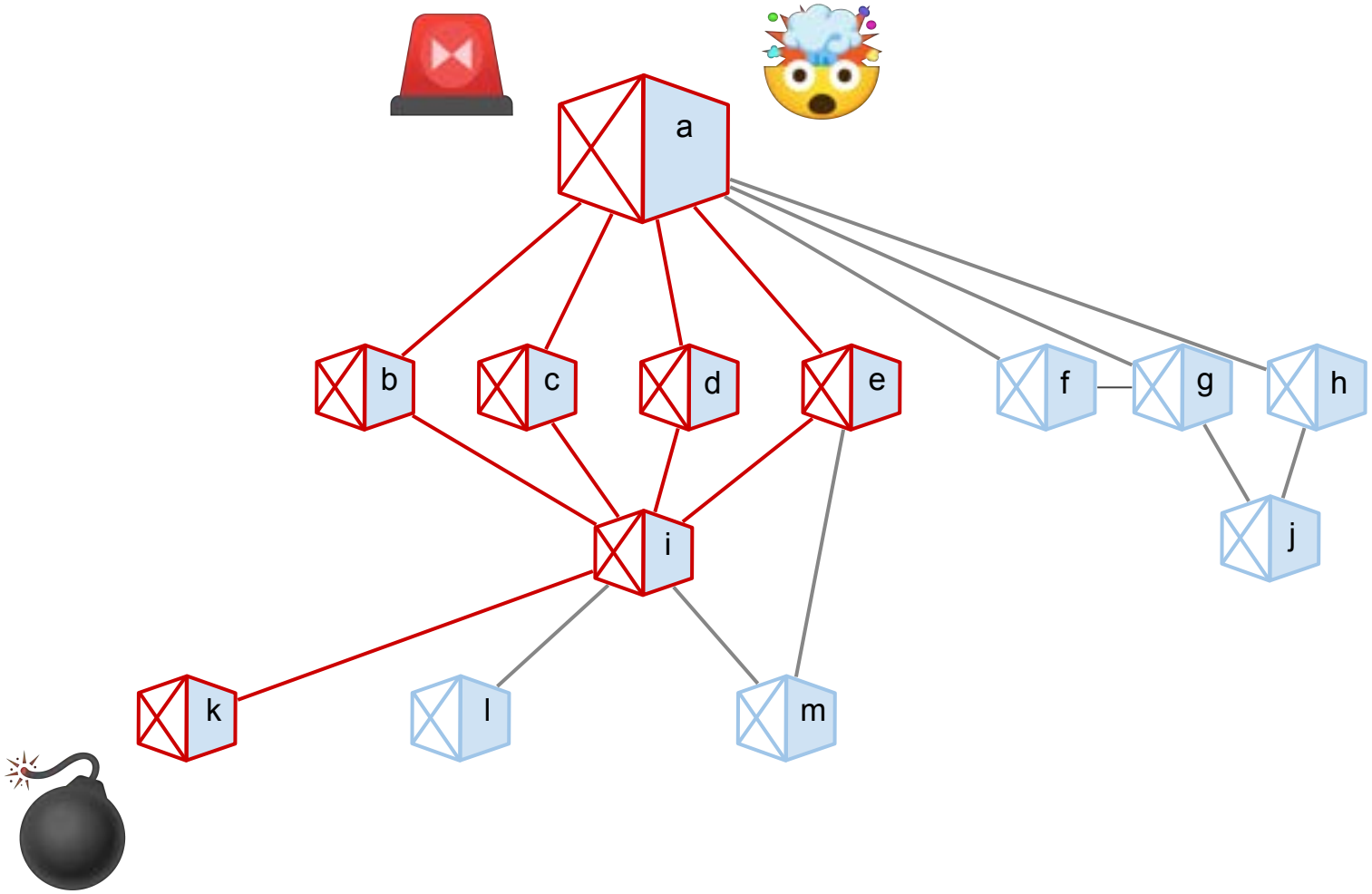

a
b
c
d
e
f
g
h
i
j
k
l
m


a
b
c
d
e
f
g
h
i
j
k
l
m


a
b
c
d
e
f
g
h
i
j
k
l
m


a
b
c
d
e
f
g
h
i
j
k
l
m


a
b
c
d
e
f
g
h
i
j
k
l
m

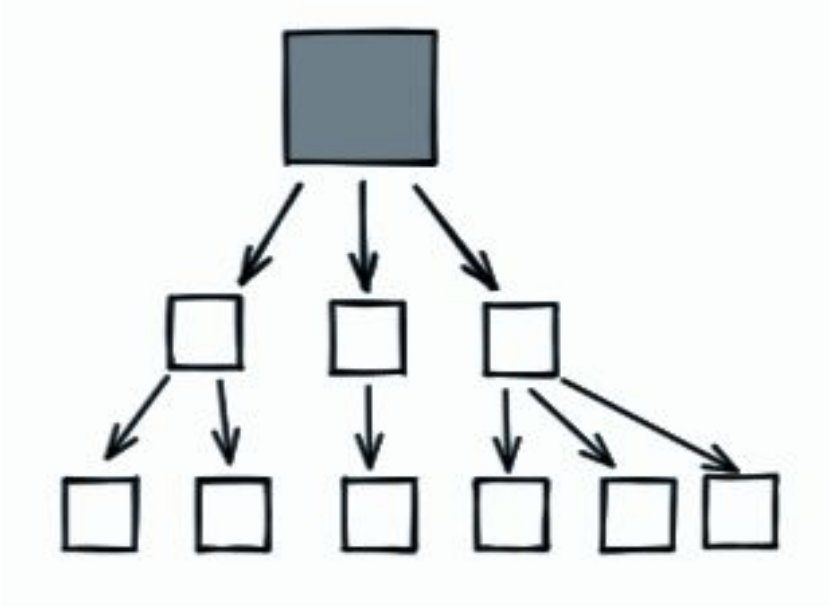

a
b
c
d
e
f
g
h
i
j
k
l
m

98%

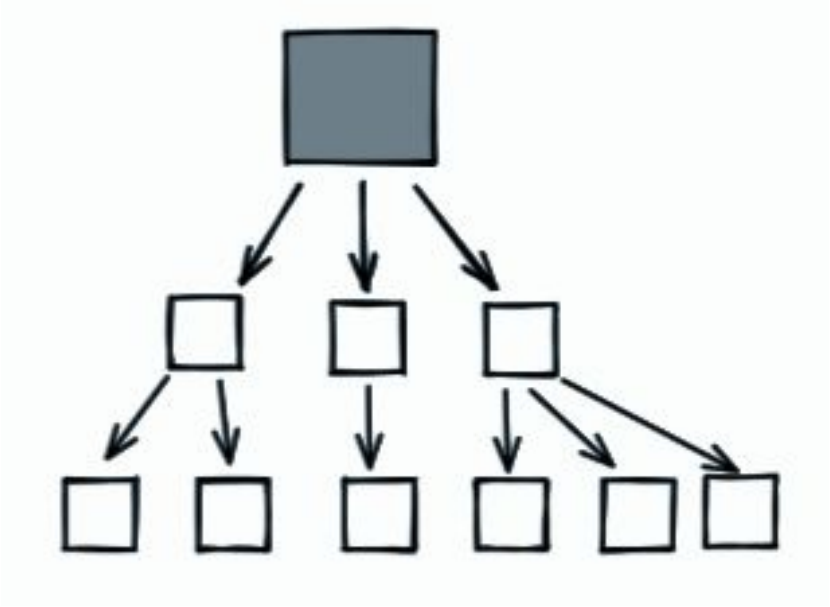
Of the time a package is affected by a vulnerability, it's affected *indirectly*.

Computed by deps.dev: From all published libraries across npm, Go, Maven, PyPI, and Cargo

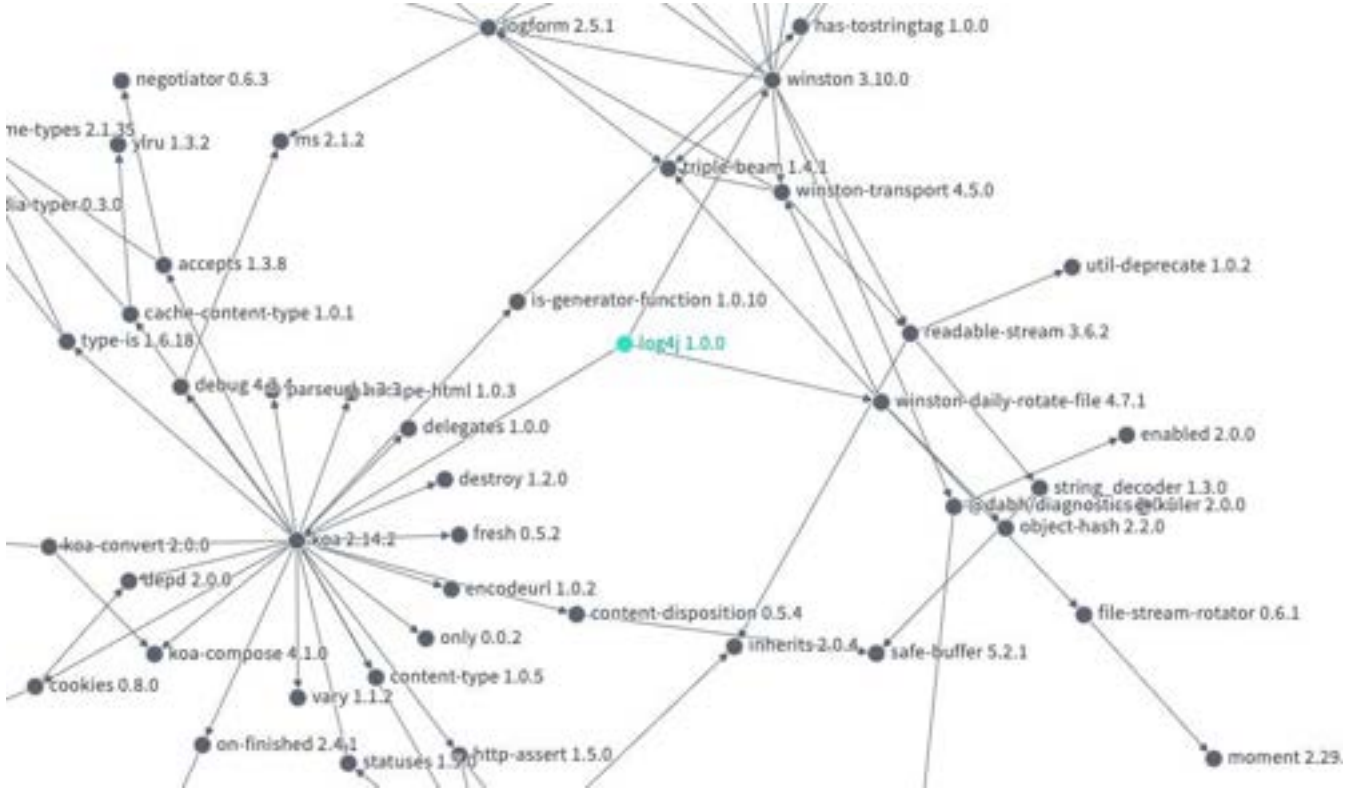
But it’s not actually this...



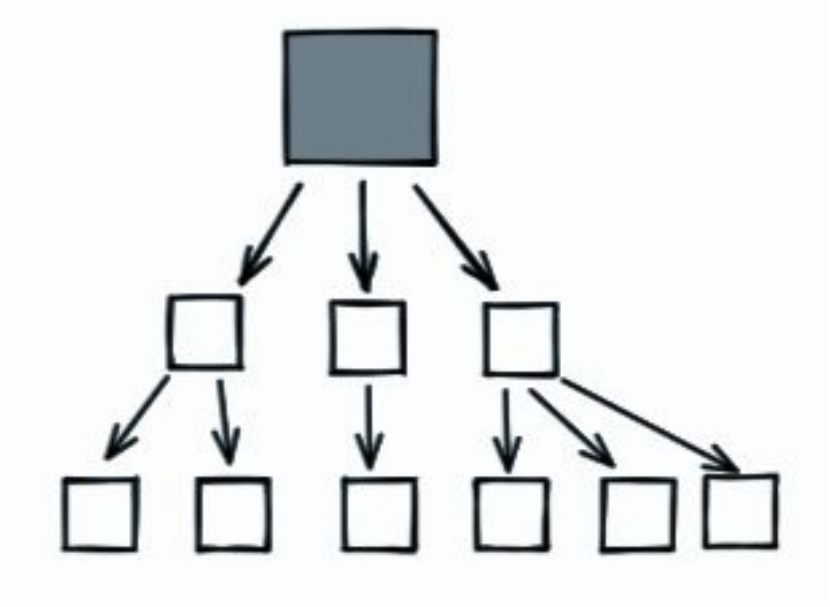
But it’s not actually this...



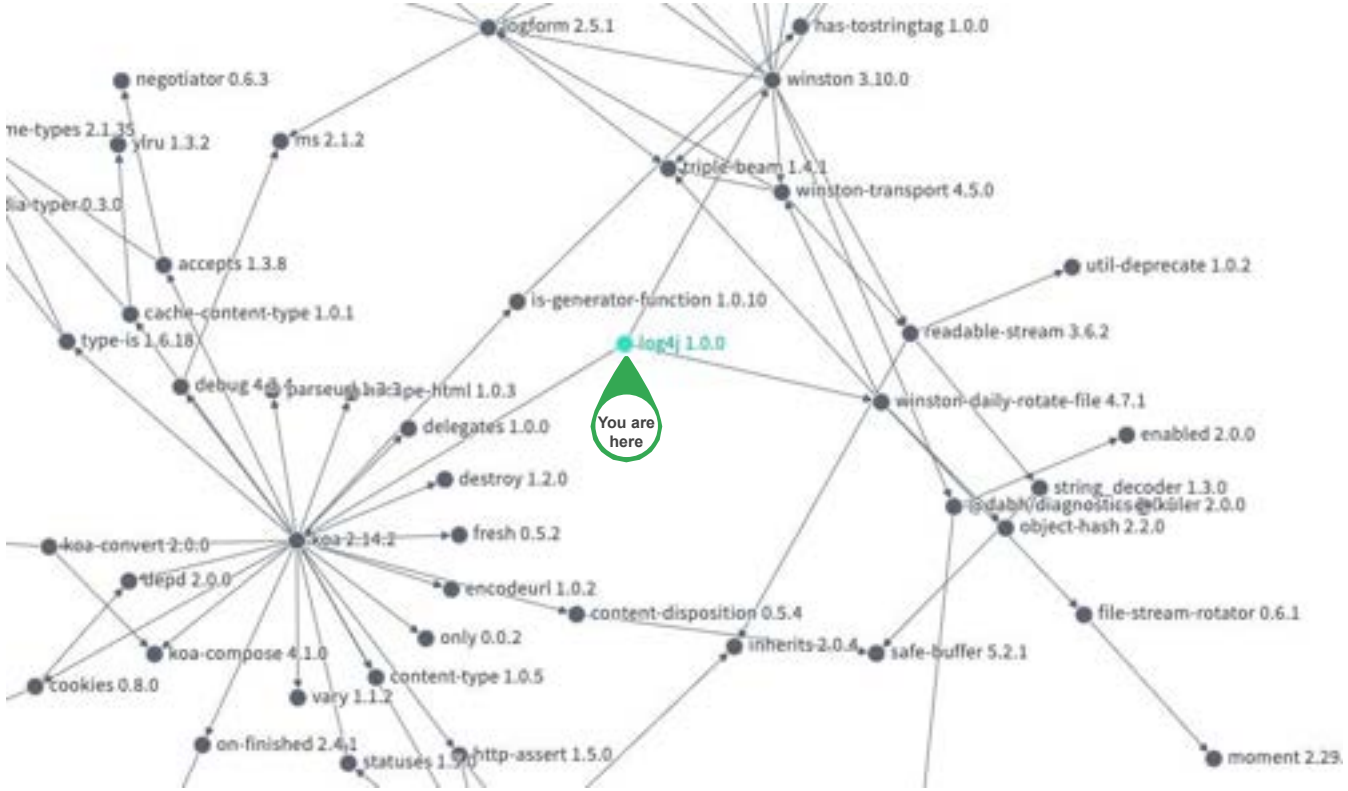
It’s THIS.



But it’s not actually this...



It’s THIS.



average number of *direct* dependencies for an npm package

6

Computed by deps.dev.

average number of *direct* dependencies for an npm package

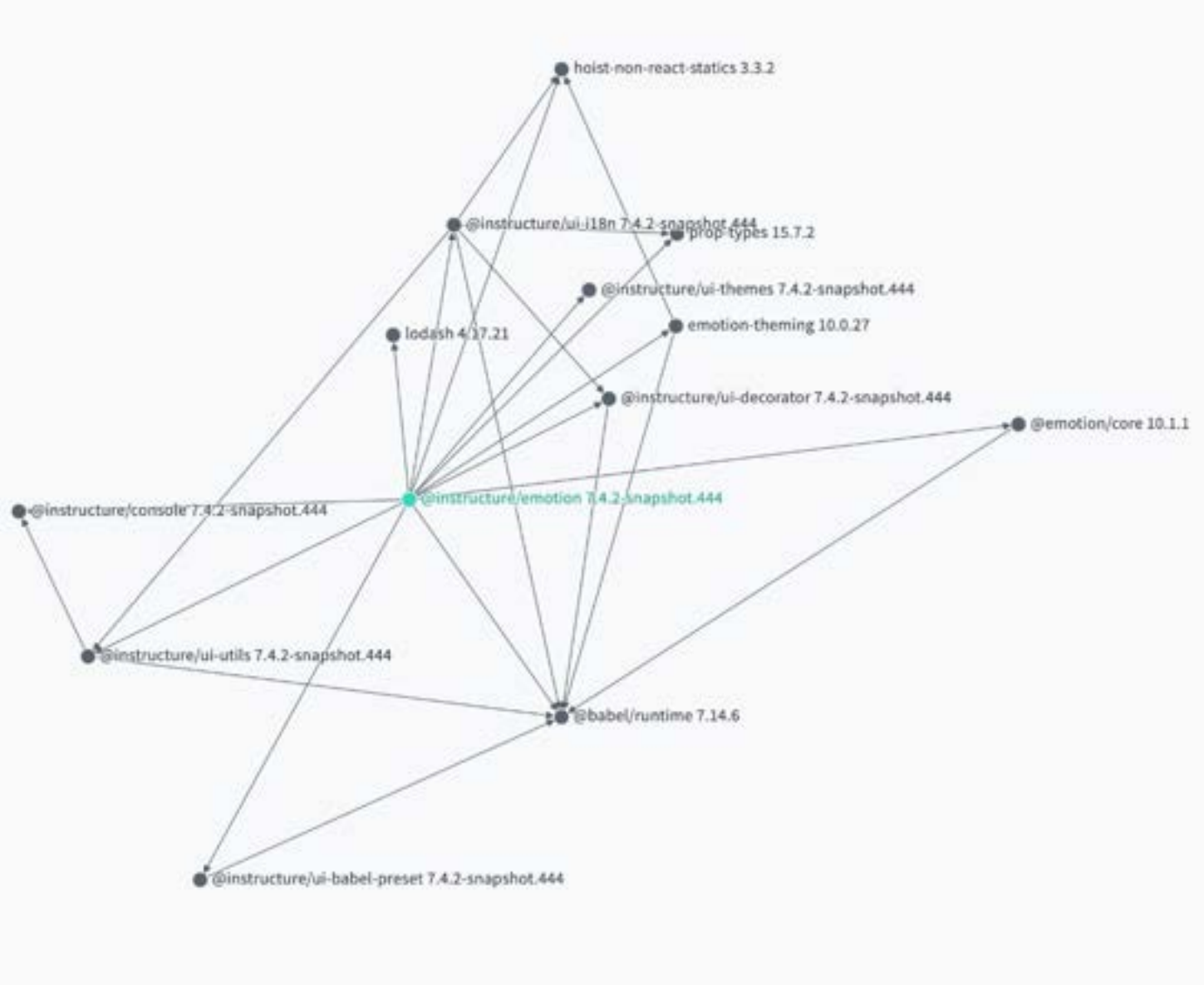
6

average number of *indirect* dependencies for an npm package

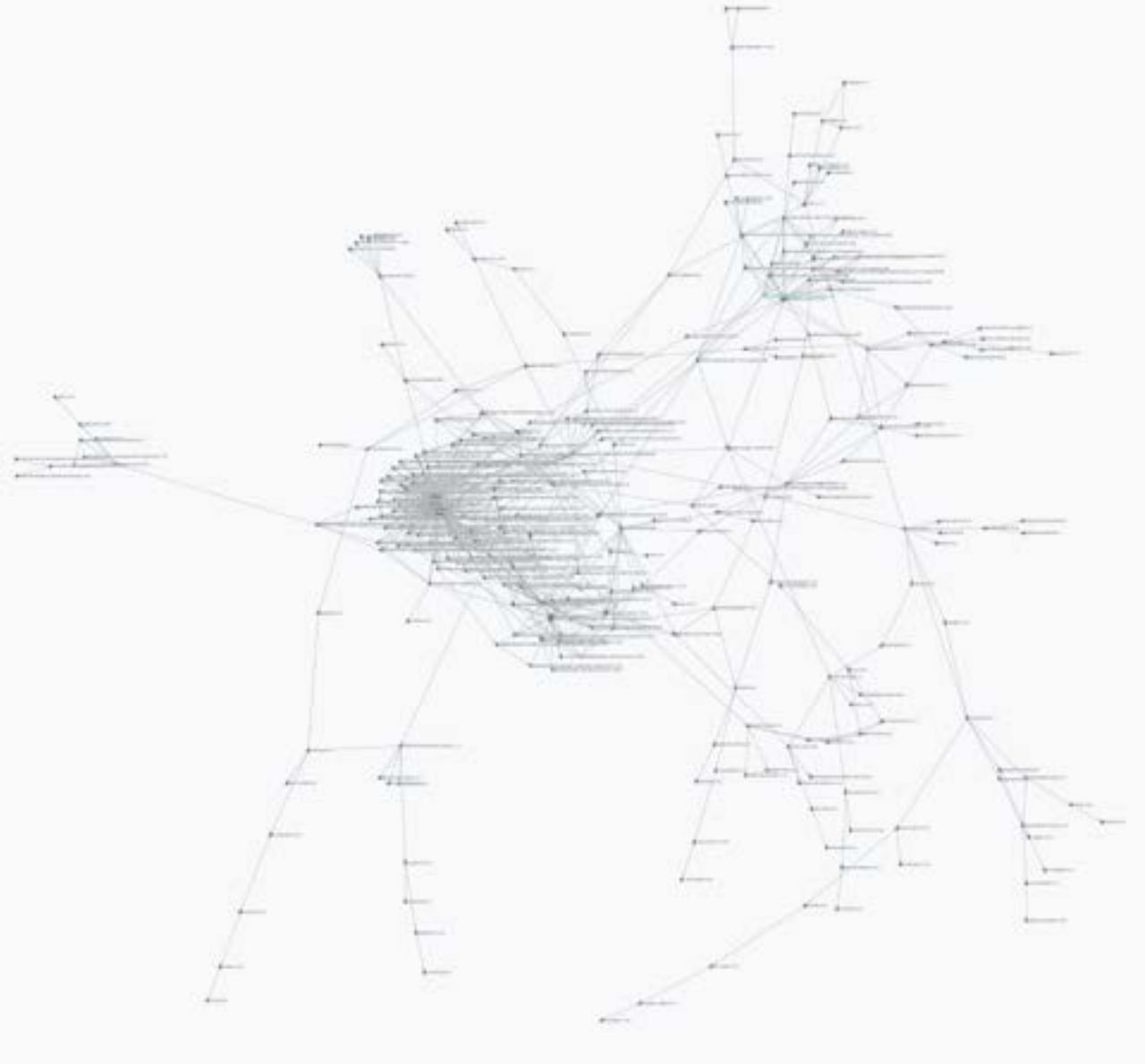
110

Computed by deps.dev.

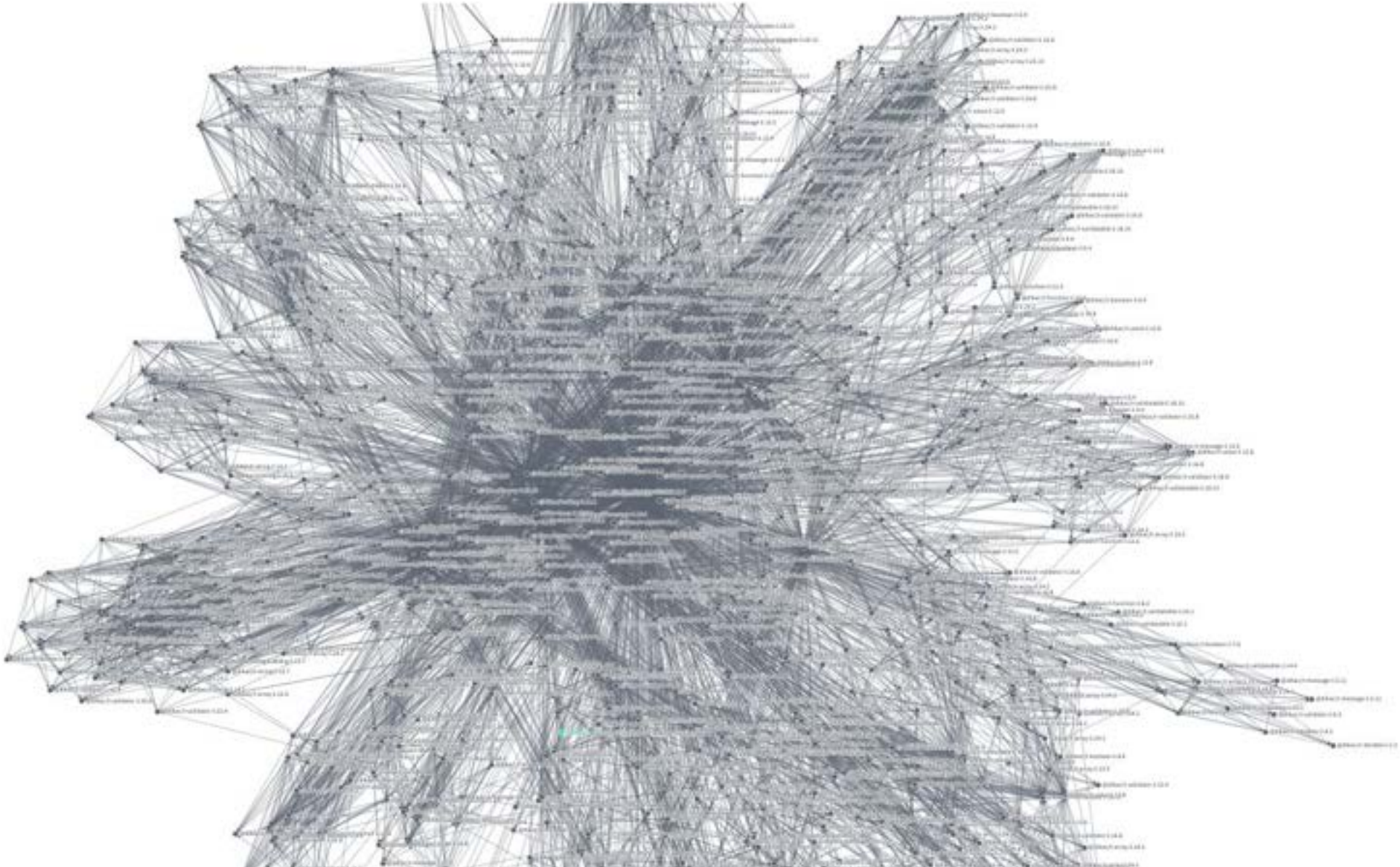
Direct dependencies



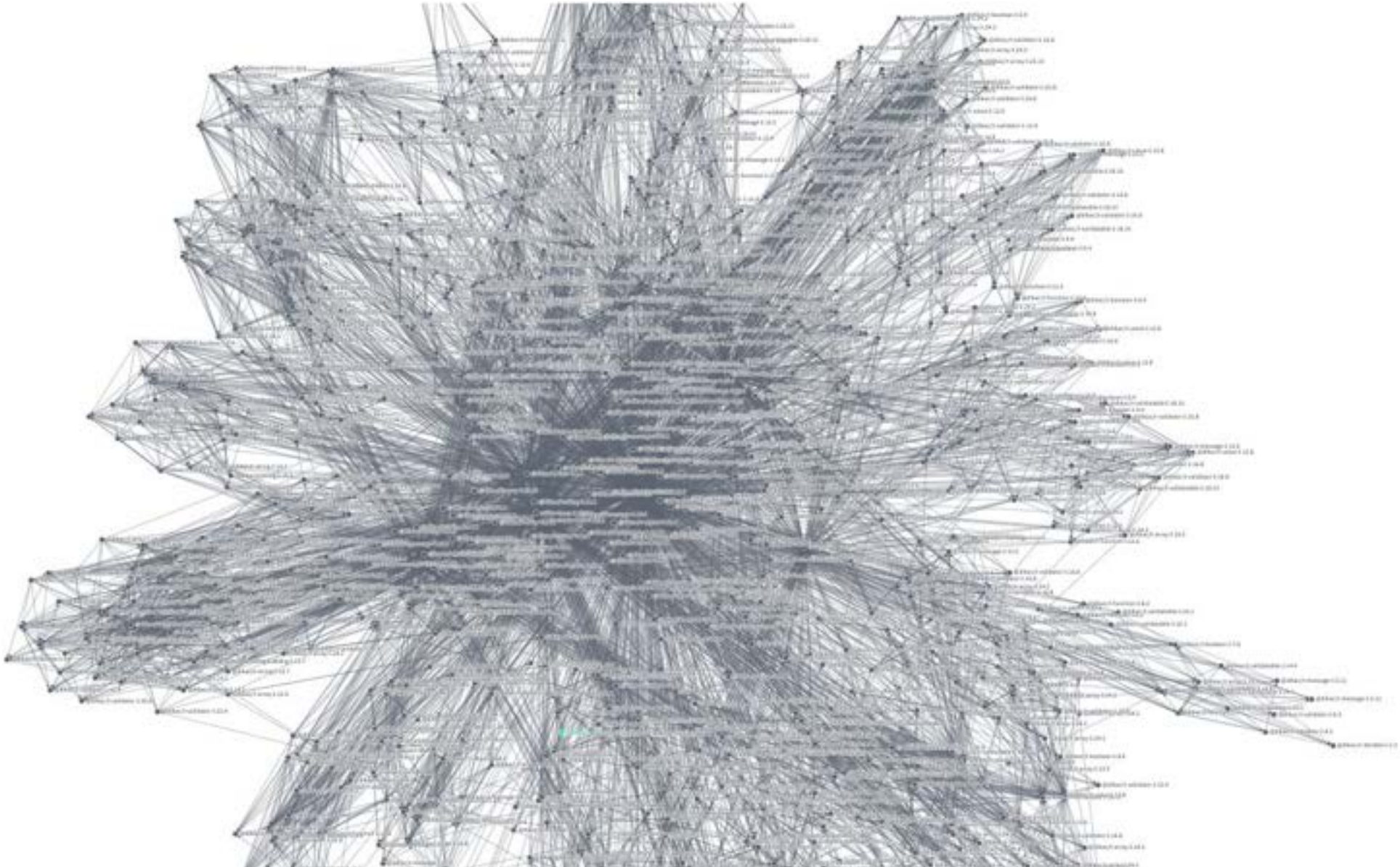
Indirect dependencies



Yikes!



Yikes!



Lesson 1

Knowledge is key: know the actual risk

01

Lesson 1

Knowledge is key: know the actual risk

01

Free tools!

- OpenSSF Scorecard — to understand a project's risks
- Deps.dev website — to understand connections between projects

OpenSSF Scorecard Report

9.4

github.com/ossf/scorecard

COMMIT: 52a4843bf158e4009bb4f67f41e1903cb8f

GENERATED AT: 2023-09-06T16:39:13Z

10 Dangerous-Workflow CRITICAL
Determines if the project's GitHub Action workflow

8 Vulnerabilities HIGH
Determines if the project has open, known unfixed

9 Signed-Releases HIGH
Determines if the project cryptographically signs

9 Token-Permissions HIGH
Determines if the project's workflows follow the

10 Binary-Artifacts HIGH
Determines if the project has generated execu

10 Code-Review HIGH
Determines if the project requires human cod

10 Dependency-Update-Tool HIGH
Determines if the project uses a dependency

OpenSSF Scorecard Report

6.3

github.com/pnacht/cronk

COMMIT: 8b5162c2cdd5a2afa250ff012ef61d2f59bf1fa6

GENERATED AT: 2023-09-06

10 Dangerous-Workflow CRITICAL
Determines if the project's GitHub Action workflows avoid dangero

0 Branch-Protection HIGH
Determines if the default and release branches are protected w

0 Code-Review HIGH
Determines if the project requires code review before pull r

0 Maintained HIGH
Determines if the project is "actively maintained".

10 Binary-Artifacts HIGH
Determines if the project has generated executable

10 Dependency-Update-Tool HIGH
Determines if the project uses a dependency up

10 Signed-Releases HIGH
Determines if the project cryptographically s

10 Token-Permissions HIGH
Determines if the project's workflows foll

OpenSSF Scorecard Report

8.1

github.com/tensorflow/tensorflow

COMMIT: 5d4fe8a712cbe1cce1d8af663ab5ac54fcd42baf

GENERATED AT: 2023-09-07

SORT: Risk level (desc

10 Dangerous-Workflow CRITICAL
Determines if the project's GitHub Action workflows avoid dangerous patterns.

0 Token-Permissions HIGH
Determines if the project's workflows follow the principle of least privilege.

7 Binary-Artifacts HIGH
Determines if the project has generated executable (binary) artifacts in the source repository.

10 Code-Review HIGH
Determines if the project requires code review before pull requests (aka merge requests) are mer...

10 Dependency-Update-Tool HIGH
Determines if the project uses a dependency update tool.

10 Maintained HIGH
Determines if the project is "actively maintained".

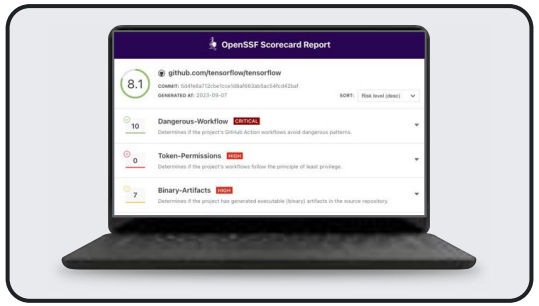
10 Vulnerabilities HIGH
Determines if the project has open, known unfixed vulnerabilities.

0 SAST MEDIUM
Determines if the project uses static code

10 Fuzz

OpenSSF Scorecard

Info how YOU want it



Webviewer

CLI tool

GitHub action

Security-Policy

Open in `main` 31 minutes ago

```
score is 0: security policy file not detected
```

Remediation (click "Show more" below):

- Place a security policy file `SECURITY.md` in the root directory of your repository. This makes it easily discoverable by a vulnerability reporter.
- The file should contain information on what constitutes a vulnerability and a way to report it securely (e.g. issue tracker with private issue support, encrypted email with a published public key). Follow the coordinated vulnerability disclosure guidelines to respond to vulnerability disclosures.
- For GitHub, see more information here.

Severity: Medium

Details:

Risk: `Medium` (possible insecure reporting of vulnerabilities)

This check tries to determine if the project has published a security policy. It works by looking for a file named `SECURITY.md` (case-insensitive) in a few well-known directories.

A security policy (typically a `SECURITY.md` file) can give users information about what constitutes a vulnerability and how to report one securely so that information about a bug is not publicly visible.

This check examines the contents of the security policy file awarding points for those policies that express vulnerability process(es), disclosure timelines, and have links (e.g., URL(s) and email(s)) to support the users.

open / source / insights

deps.dev

About Documentation Blog

Understand your dependencies

Your software and your users rely not only on the code you write, but also on the code your code depends on, the code *that* code depends on, and so on. An accurate view of the complete dependency graph is critical to understanding the state of your project. And it's not just code: you need to know about security vulnerabilities, licenses, recent releases, and more.

Search for open source packages, advisories and projects | All systems | Search

npm PACKAGES	2.49M
Go MODULES	1.03M
Maven ARTIFACTS	564k
PyPI PACKAGES	455k
NuGet PACKAGES	368k
Cargo CRATES	124k

PyPI package

tensorflow

2.13.0

Overview | Dependencies | Dependents | Compare | Versions

Filter dependencies by name, license, security advisory and more

Table | Graph

Package	Notes	Relation	License	Dependencies
absl-py 1.4.0		Direct	Apache-2.0	0
astunparse 1.6.3		Direct	non-standard	2
flatbuffers 23.5.26	13 ADVISORIES	Direct	Apache-2.0	0
gast 0.4.0		Direct	BSD-3-Clause	0

PyPI package

tensorflow

2.13.0

Overview | Dependencies | Dependents | Compare | Versions

Filter dependencies by name, license, security advisory and more

Table | Graph

Package	Notes	Relation	License	Dependencies
absl-py 1.4.0		Direct	Apache-2.0	0
astunparse 1.6.3		Direct	non-standard	2
flatbuffers 23.5.26	13 ADVISORIES	Direct	Apache-2.0	0
gast 0.4.0		Direct	BSD-3-Clause	0

Lesson 2

Monitoring supports action

02

Lesson 2

Monitoring supports action

02

More free tools!

- OSV (Open Source Vulnerabilities) or ecosystem-specific vulnerability monitoring
- Dependency update bots (Dependabot or Renovatebot)

A distributed vulnerability database for Open Source

An open, precise, and distributed approach to producing and consuming vulnerability information for open source.

Search Vulnerability Database | Use the API | CLI Tools

osv.dev

Ecosystems

Linux	Alpine	Android	crates.io	Debian	Go	Linux	Maven	npm	NuGet	OSS-Fuzz	Packagist	PyPI	Rocky Linux	Ruby
2286	3254	722	1174	9379	1588	13573	3864	11989	495	2929	2154	10781	919	717

A distributed vulnerability database for Open Source

An open, precise, and distributed approach to producing and consuming vulnerability information for open source.

Search Vulnerability Database | Use the API | CLI Tools

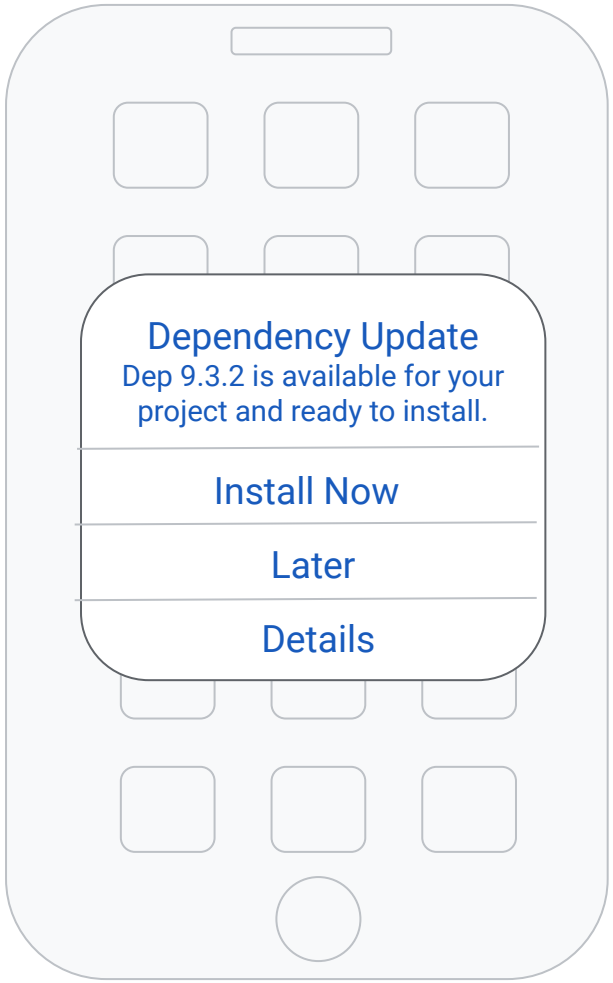
osv.dev

Ecosystems

Linux	Alpine	Android	crates.io	Debian	Go	Linux	Maven	npm	NuGet	OSS-Fuzz	Packagist	PyPI	Rocky Linux	Ruby
2286	3254	722	1174	9379	1588	13573	3864	11989	495	2929	2154	10781	919	717

Use a dependency update tool to stay on top of these changes!

- Dependabot
- Renovatebot



Lesson 3

Messengers support success

03

Lesson 3

Messengers support success

03

Code contributions, but also...

- Communication!
- Awareness!
- Soft skills!
- Documentation!
- Community education!
- Helping others!

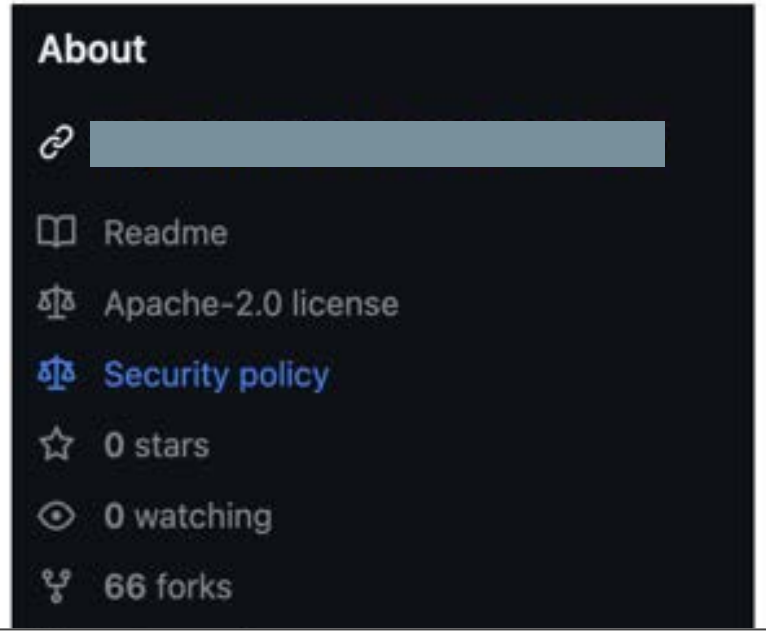
Code contributions, but also...

- Communication!
- Awareness!
- Soft skills!
- Documentation!
- Community education!
- Helping others!

joycebrum commented on May 17 Contributor

Hi, I'd like to know if you might have interest on creating a Github Security Policy file for [redacted]. The project already has a very well defined security policy so the file would only allow users to get this information through github standard ways.

It will be shown in the Security Dashboard and in the about section of the project:



Link


commented on Jul 7
Owner
Author
This change got applied to 20 high-profile projects downstream.
1

Link

Closing thoughts…

Just as risks can propagate through communities...

so can proactive, positive actions!

THANK YOU

Special thanks to:

Asra Ali

Josie Anugerah

Jen Barnason

Joyce Brum

Michael Goddard

Eve Martin-Jones

Kara Olive

Yorkim Parmentier

Julie Qiu

Nicky Ringland

James Wetter

Nina Zakharenko