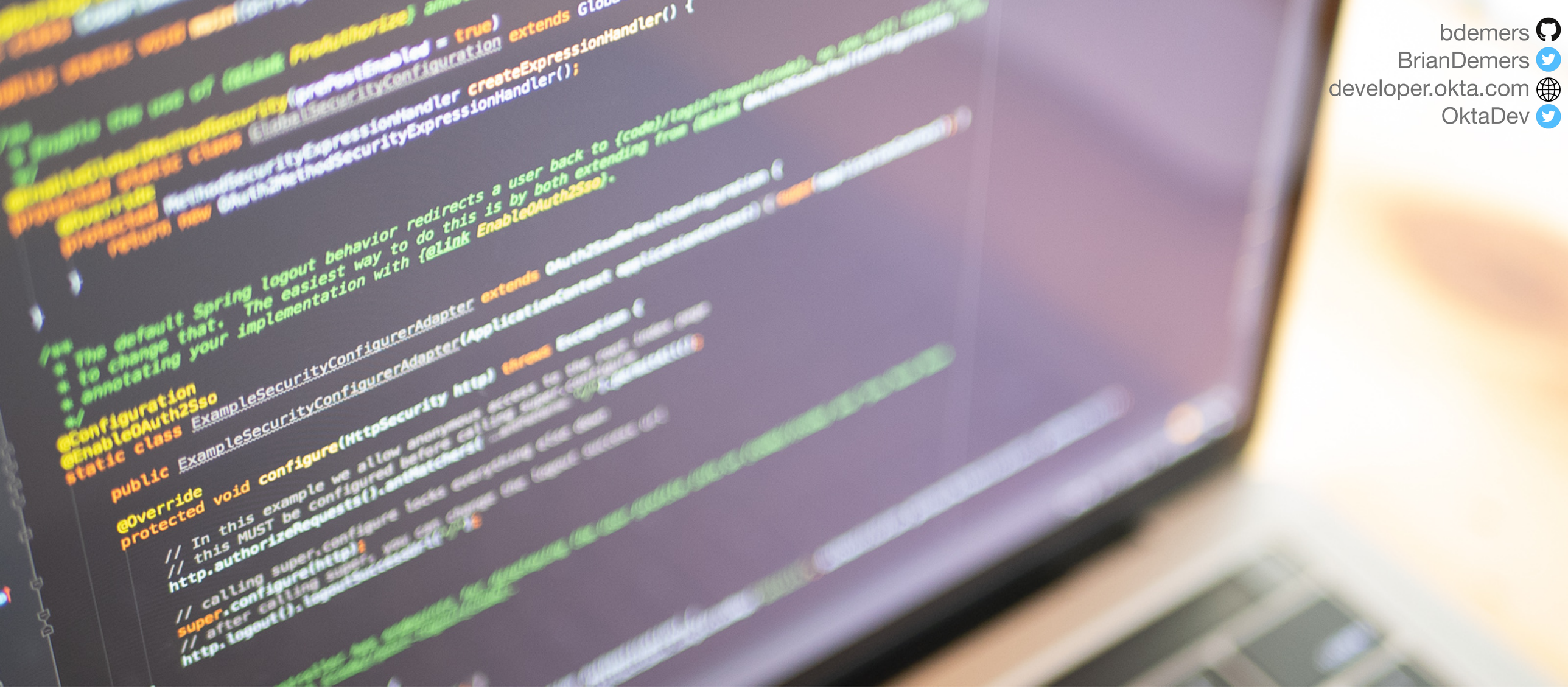


How to Report a Vulnerability:

Responsible Disclosure for Developers

Brian Demers
Developer Experience
bdemers@apache.org

okta

Who is this guy?

Stormpath

okta

THE APACHE SOFTWARE FOUNDATION

codemonkey.fm

Java™

Warner River Bees

CHEF™

openstack™

Sonatype Nexus

Maven™

FRIENDS DON’T LET FRIENDS WRITE AUTH

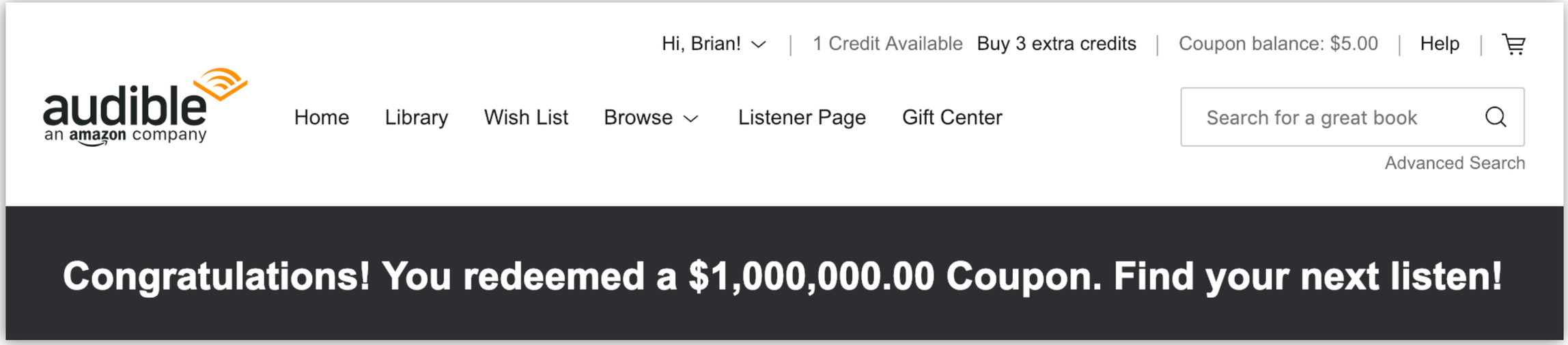
Topics

- What is a Vulnerability
- What is Responsible Disclosure
- How they are Reported
- What you can do for your Projects

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

Quick Example

audible.com/typ/promo?couponValue=1000000.0



What is a Vulnerability

vulnerability

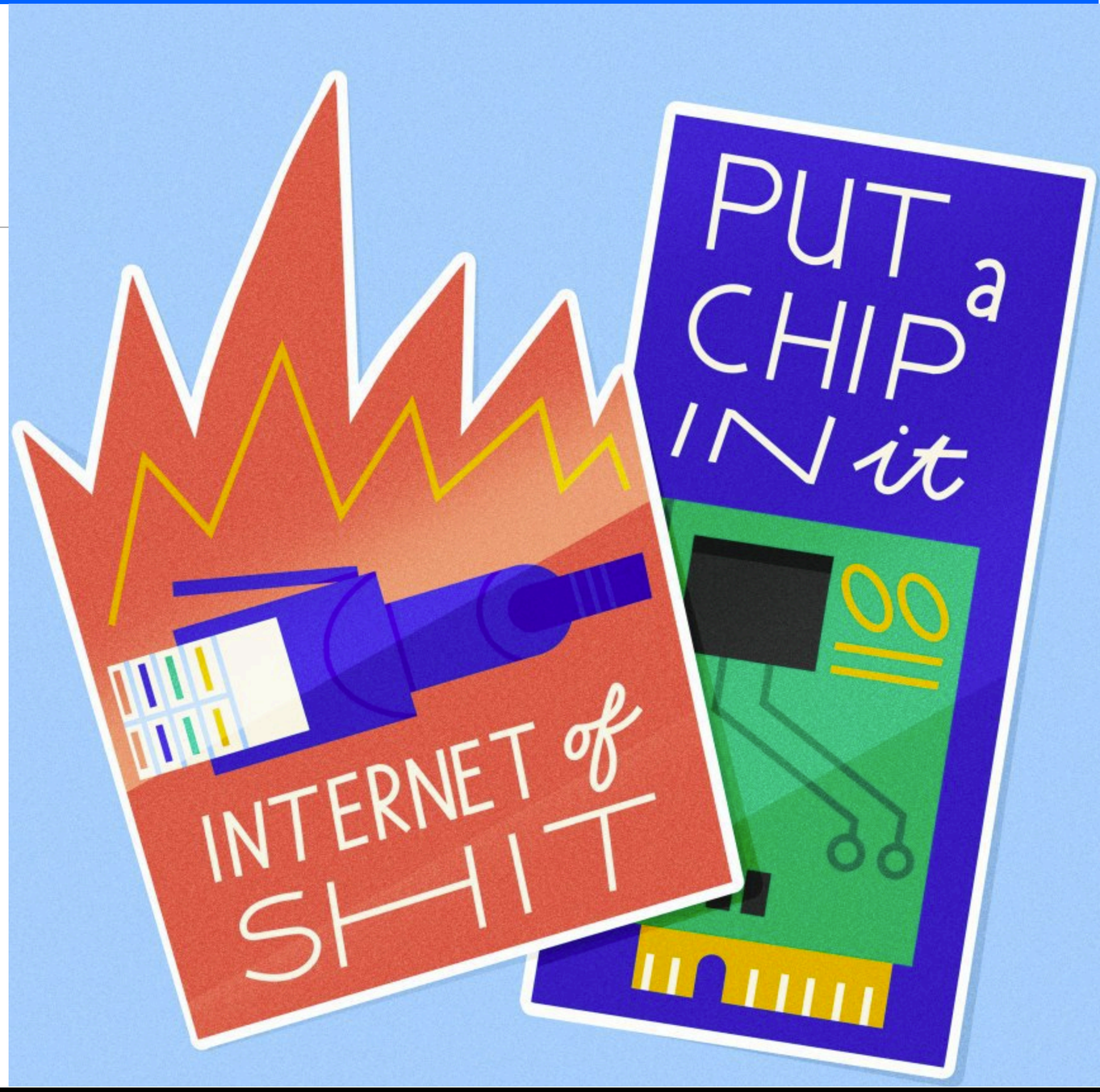
NOUN (**vulnerabilities**)

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.



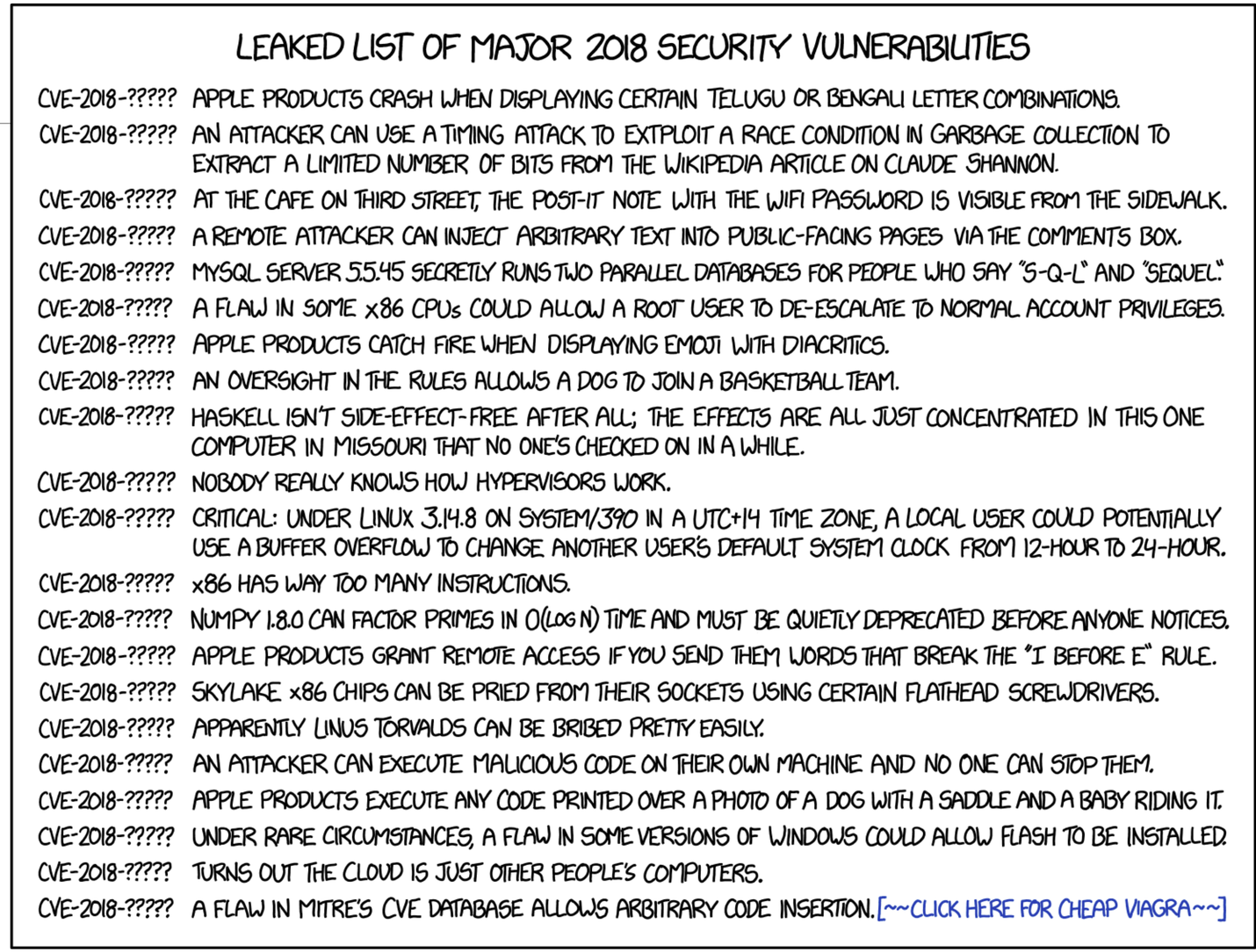
CVE vs Vulnerability

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

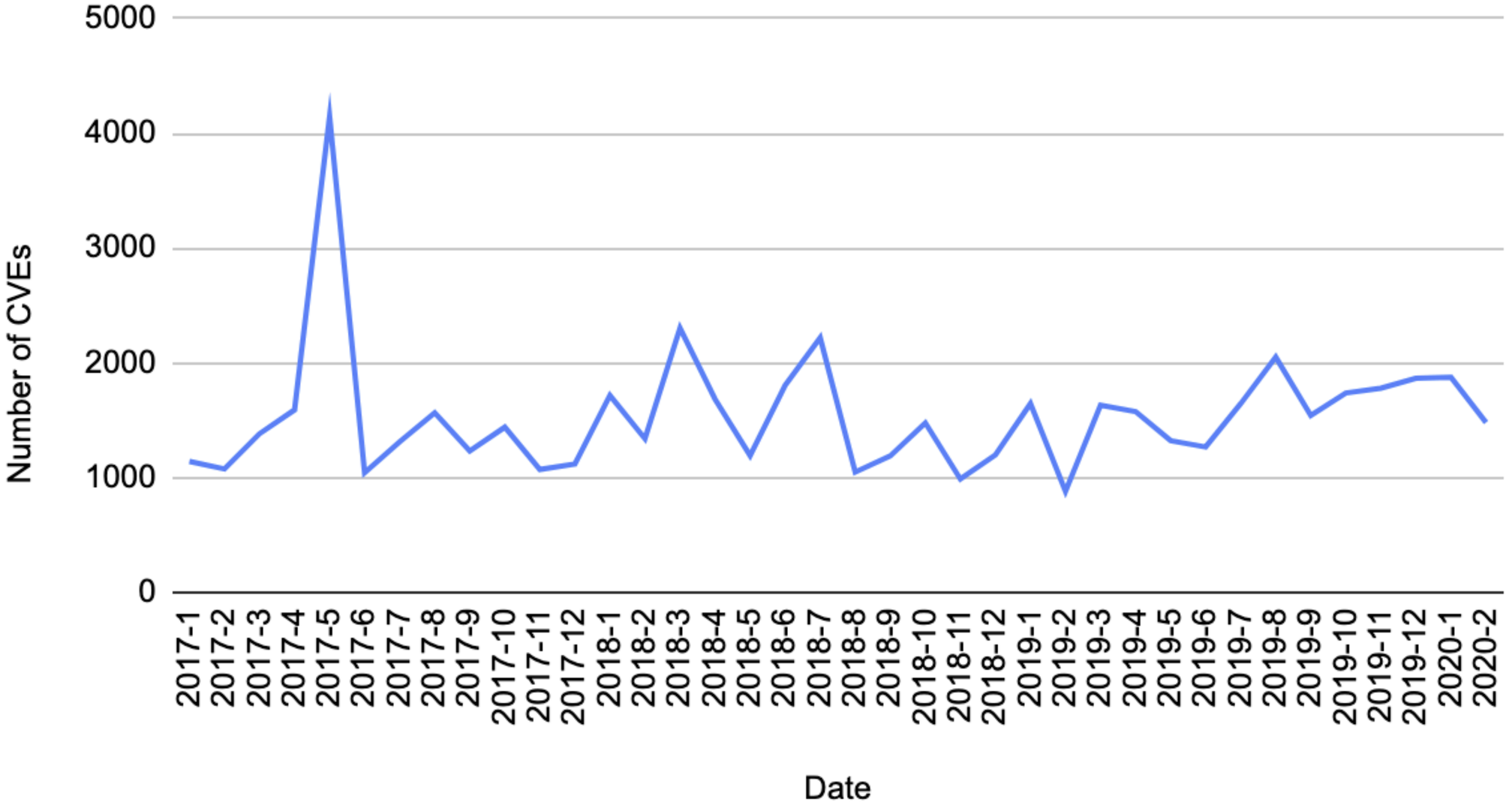
- An ID for Vulnerabilities

CVE-2018-17793

<year>-<number>

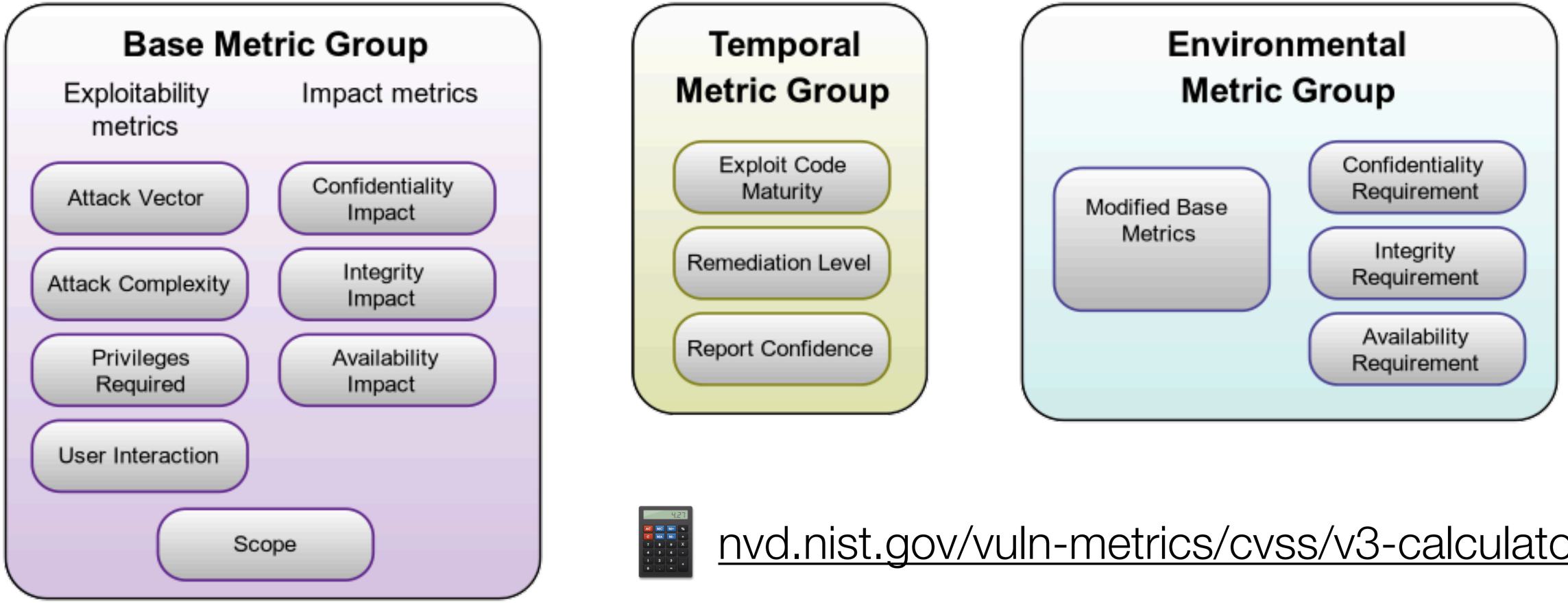


Number of CVEs / Month



(Data from nvd.nist.gov)

CVSS Score



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

Common Weakness Enumeration (CWE)

CWE-250: Execution with Unnecessary Privileges

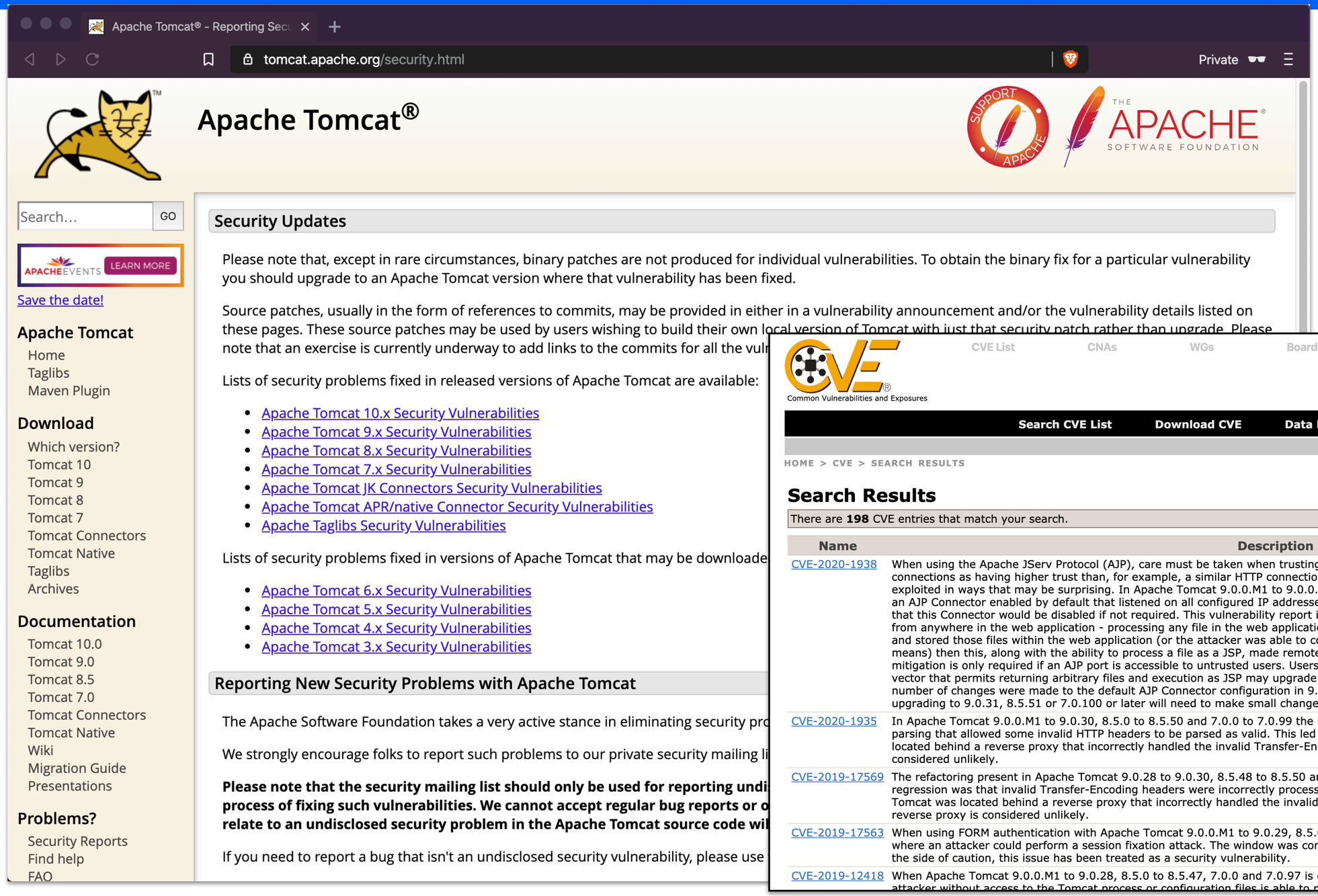
CWE-94: Improper Control of Generation of Code ('Code Injection')

Common Platform Enumeration (CPE)

```
cpe:2.3:o:microsoft:windows_xp:-:sp3:*:*:*:*:*:x86:*
cpe:2.3:a:apache:struts:*:*:*:*:*:*:*:*:*
```

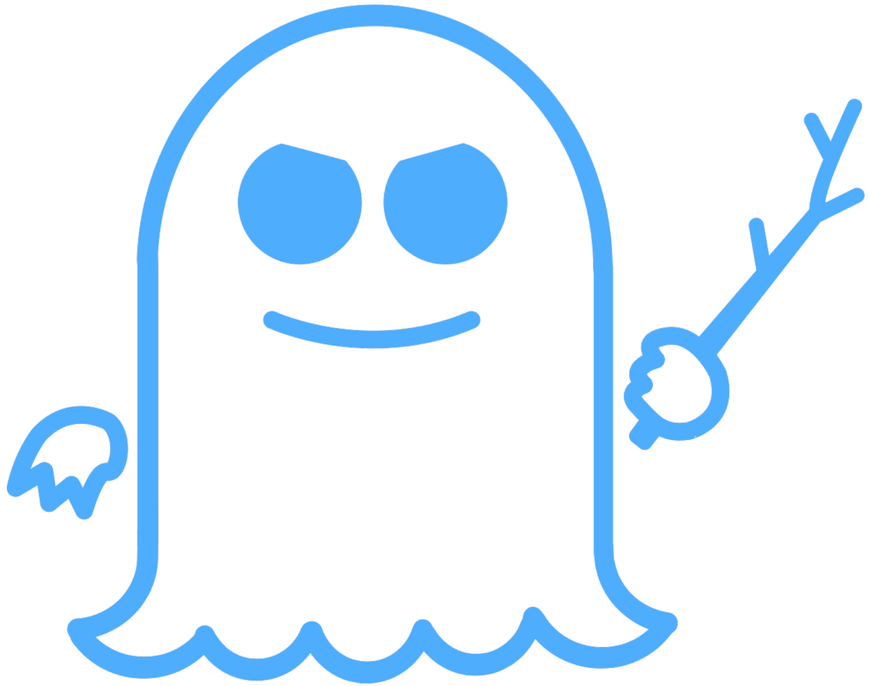
```
org.apache.struts:struts2-core:2.5.0
```

CVEs are Bad?



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

The Bad...



SPECTRE

Responsible Disclosure

- Give vendor time to fix vulnerability before telling public

Full Disclosure

- Tell public ASAP

okta

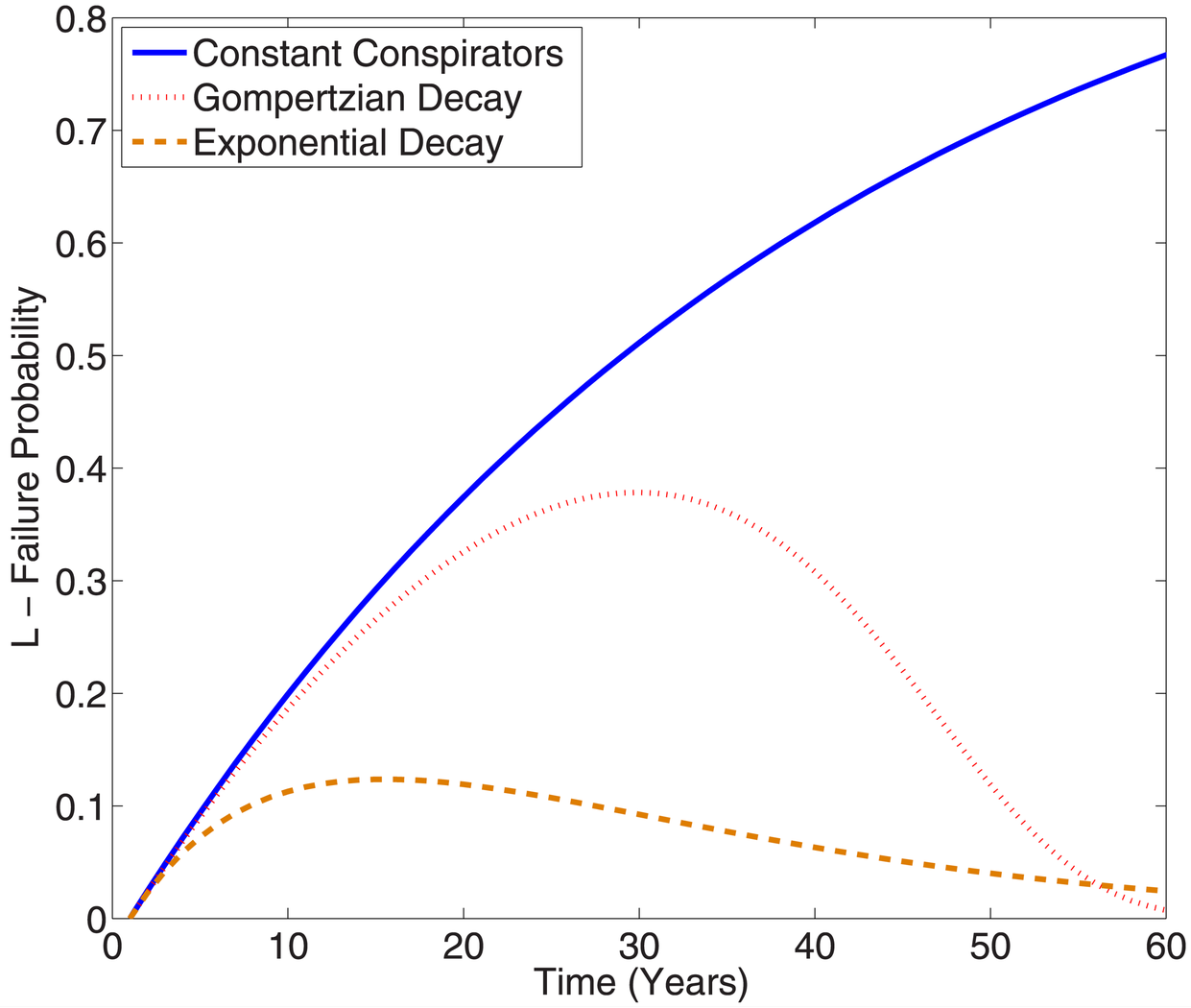
How long to wait?

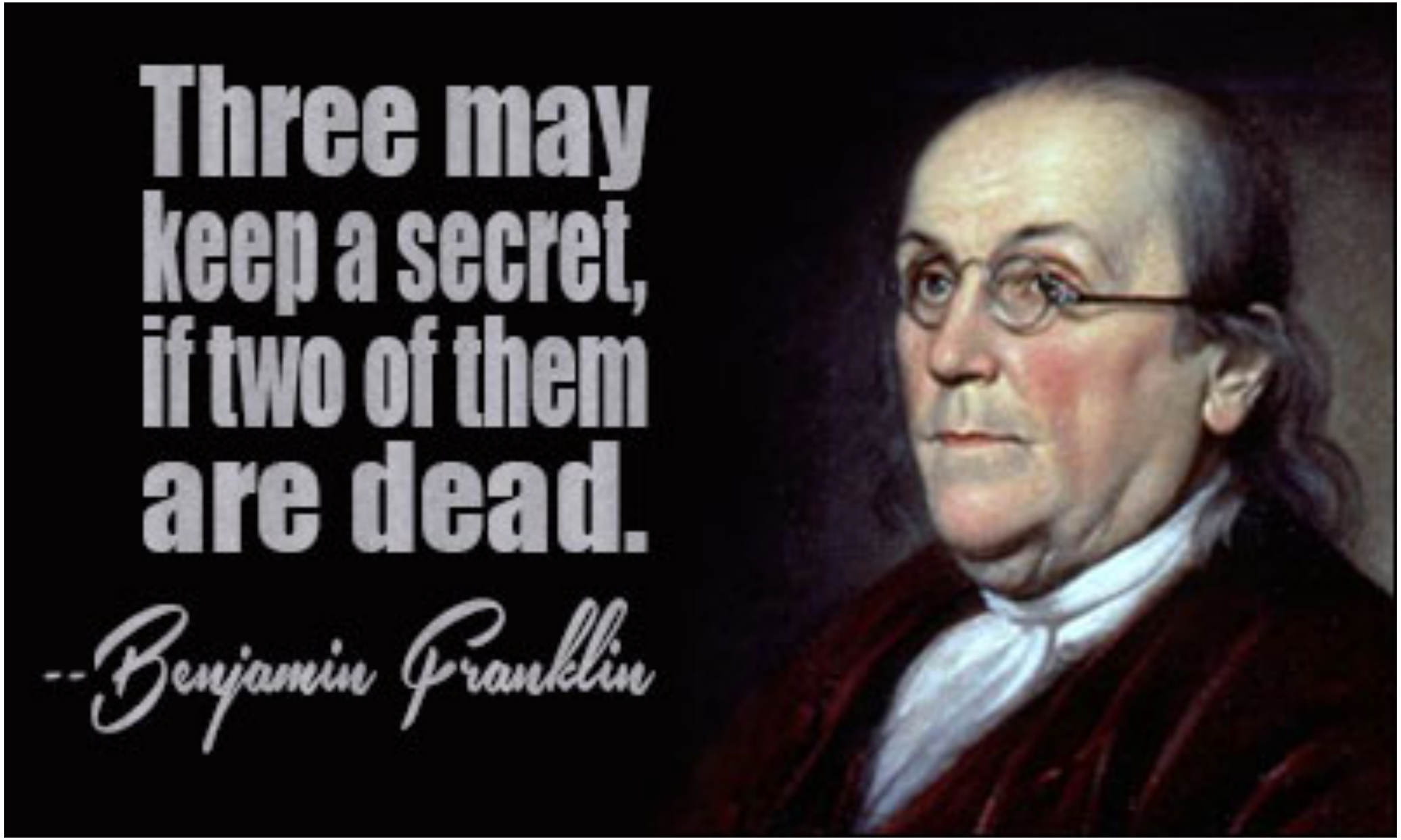
- Google Project Zero - 90 days
- Linux Kernel - 2 weeks
- HackerOne - 30 days
- CERT - 45 days

On the Viability of Conspiratorial Beliefs

David Robert Grimes

TL;DR - The more people that know the more likely it will get out.

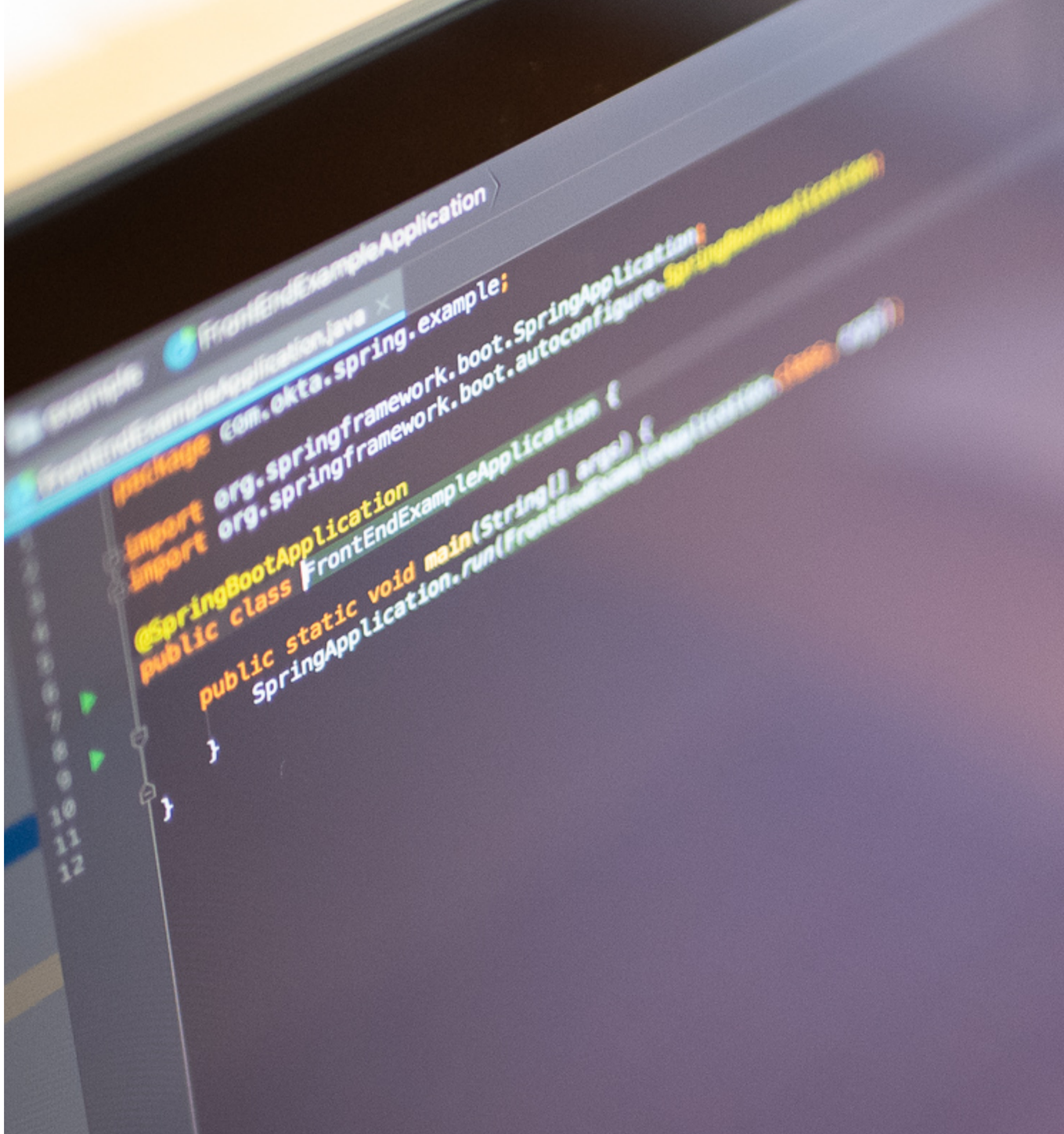



Three may keep a secret, if two of them are dead.
--Benjamin Franklin

How are Vulnerabilities Reported?

- **Report** the issue to the project
  - Wait for response
- Vendor releases patch/**fix**
  - Wait for customers to apply fix
- **Disclose** issue publicly

Report, Fix, Disclose



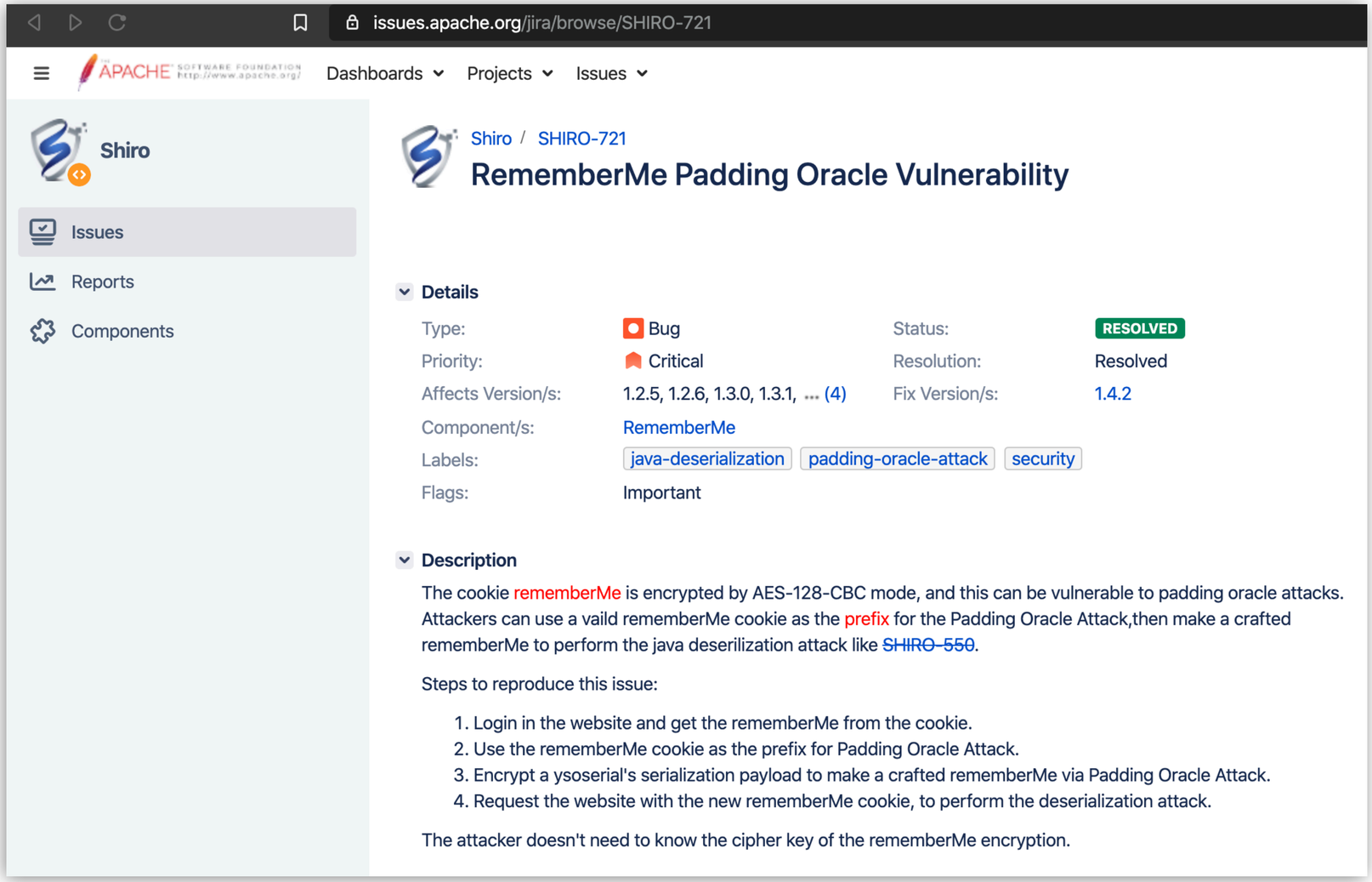
okta

Report (Privately)

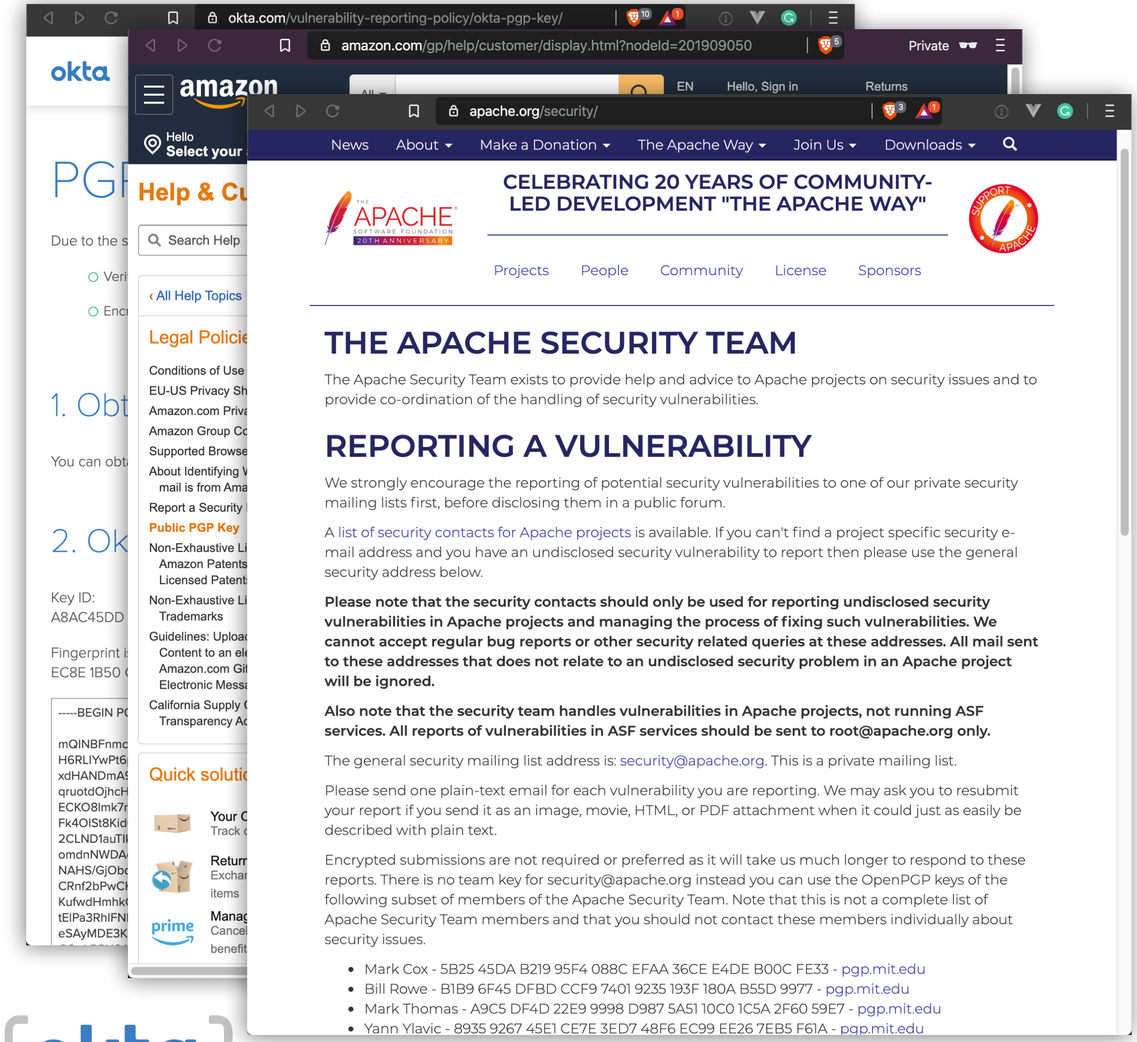
- **NOT** on StackOverflow
- **NOT** on an Email list
- **NOT** on an open forum (Slack)

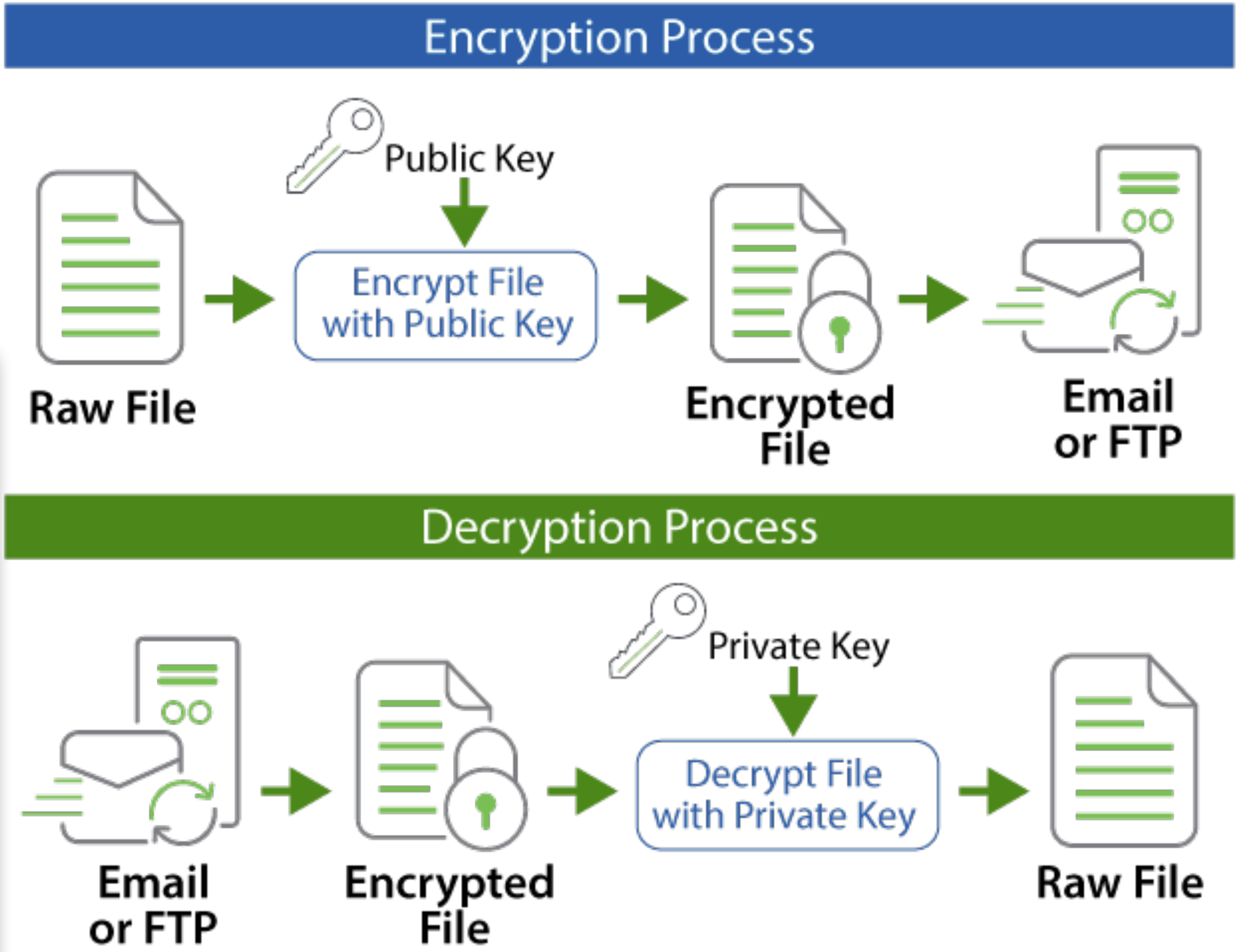
- Look for a security mailing list
- Check Bugcrowd or HackerOne
- If you are worried use an anonymous email account

Don’t use a public bug tracker



Encrypt Content If Needed






```
$ gpg --recipient <key-id/email>\
      --encrypt <input-file>
```

okta

Fix

- It’s up to the project to fix the issue
- If it’s an open source project get involved!
- The project publishes a release/patch/fix publicly
- The project _should_ contact you with details and a timeline of the fix

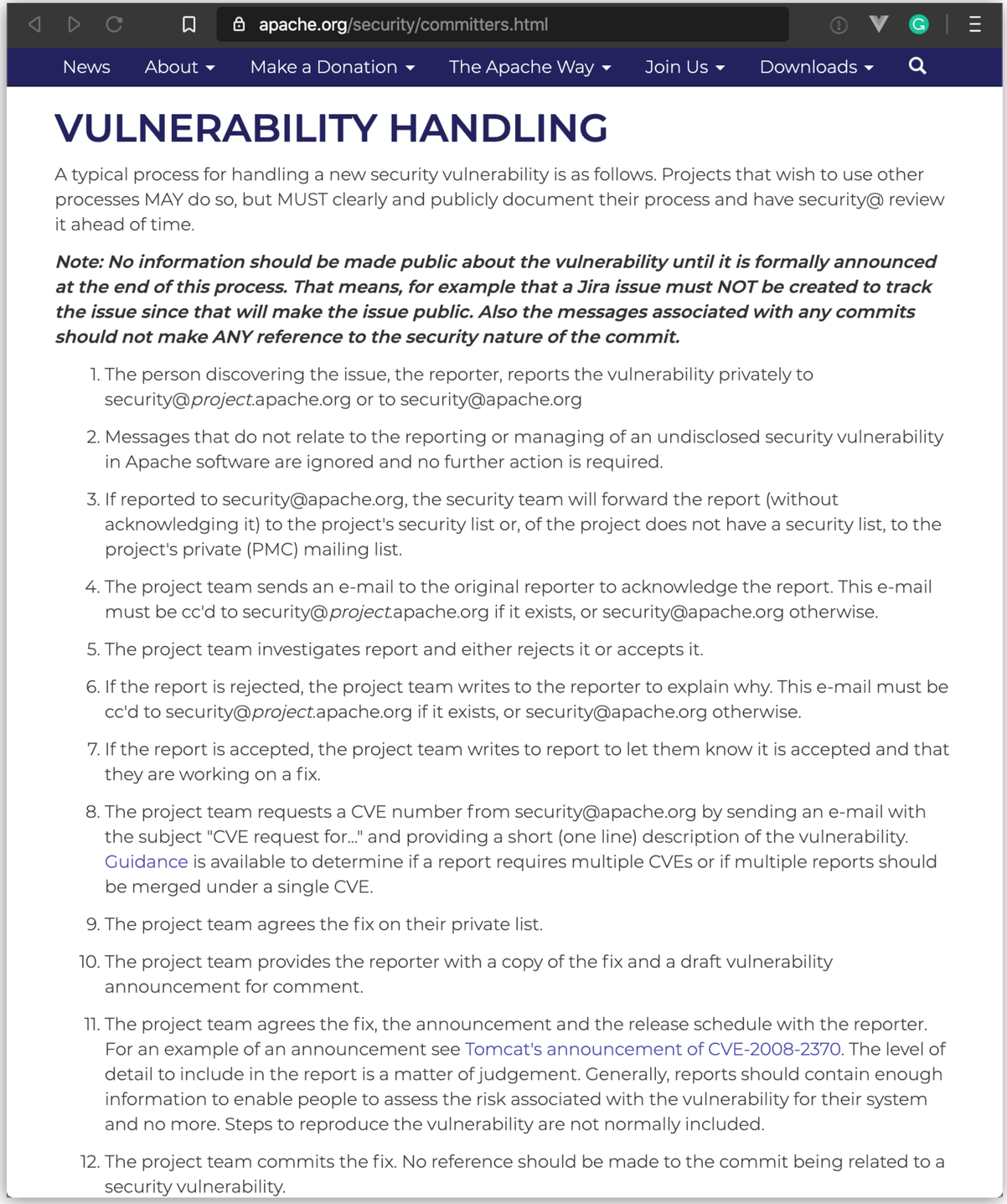
Disclose

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

The ASF Process

- A detailed 16 step process

- apache.org/security/committers.html




ASK WHAT YOU CAN DO
FOR YOUR PROJECT
imgflip.com

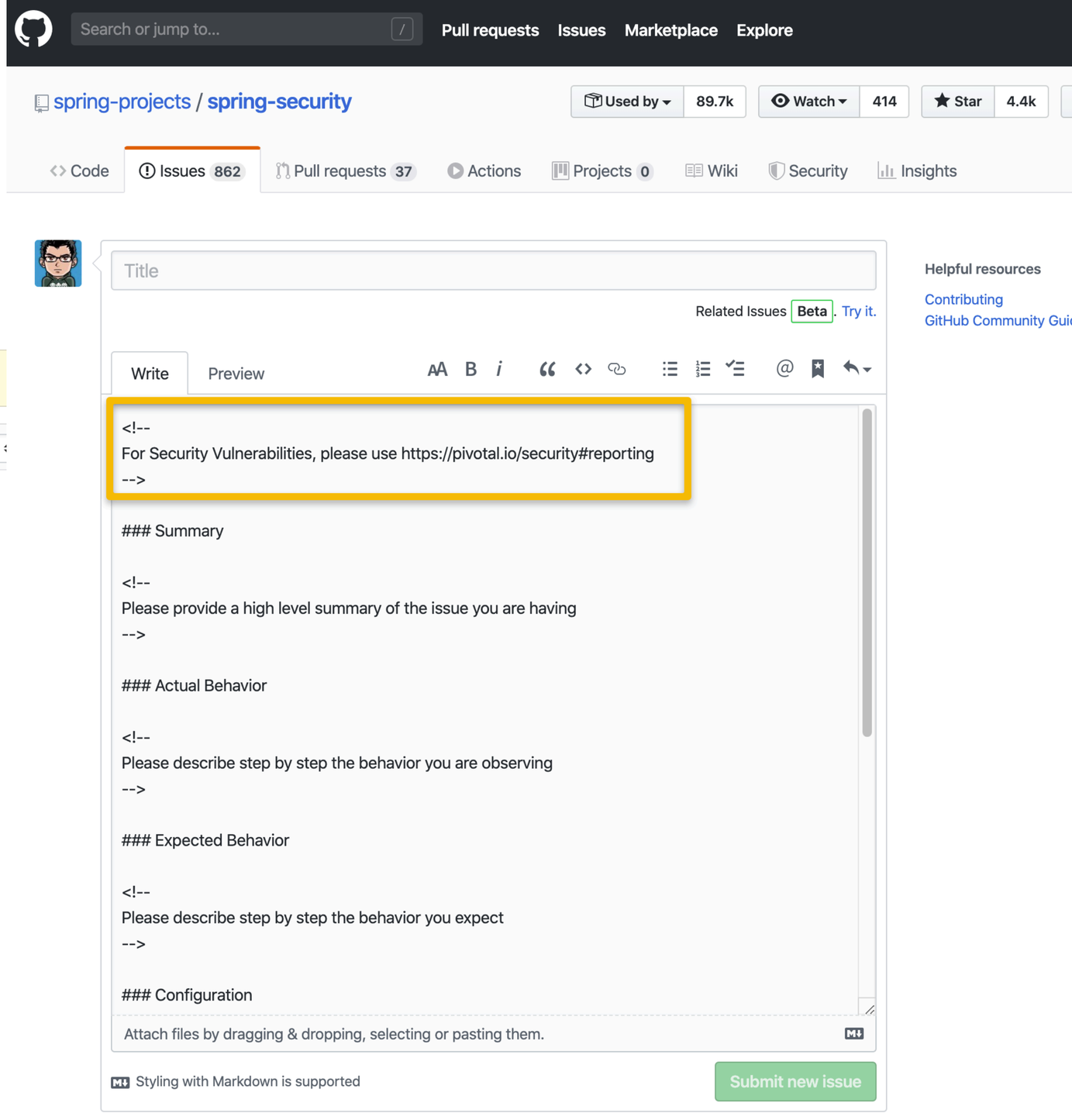
Create a GitHub Issues Template

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

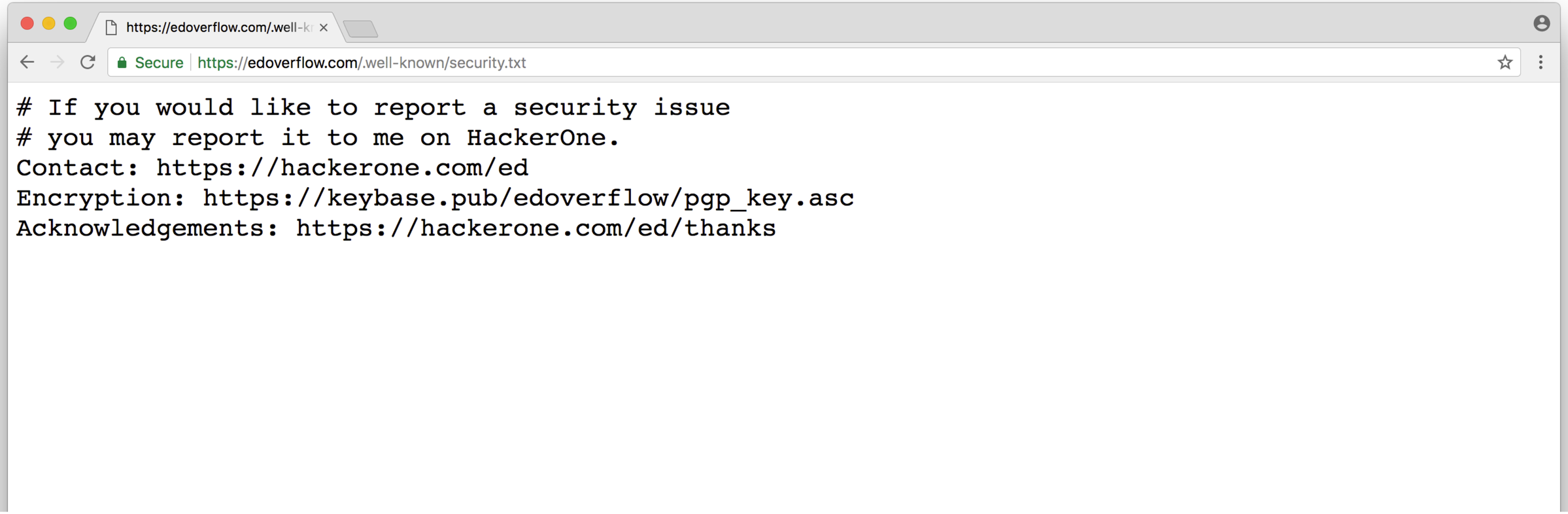
```
<!--
For Security Vulnerabilities, please use https://pivotal.io/security#reporting
-->

### 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

securitytxt.org

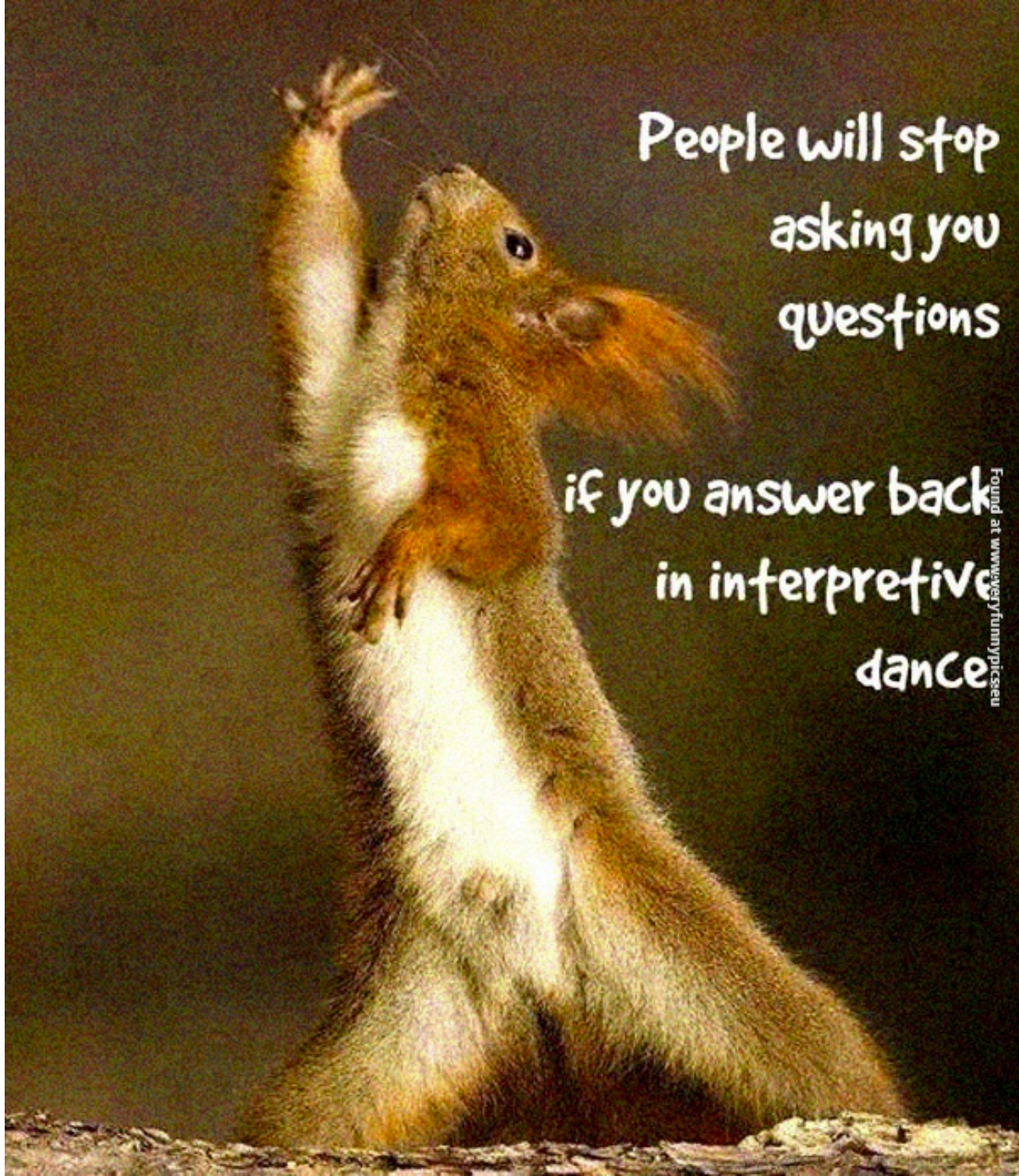
Add a .well-known/security.txt



Questions?

- @BrianDemers

https://developer.okta.com



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/