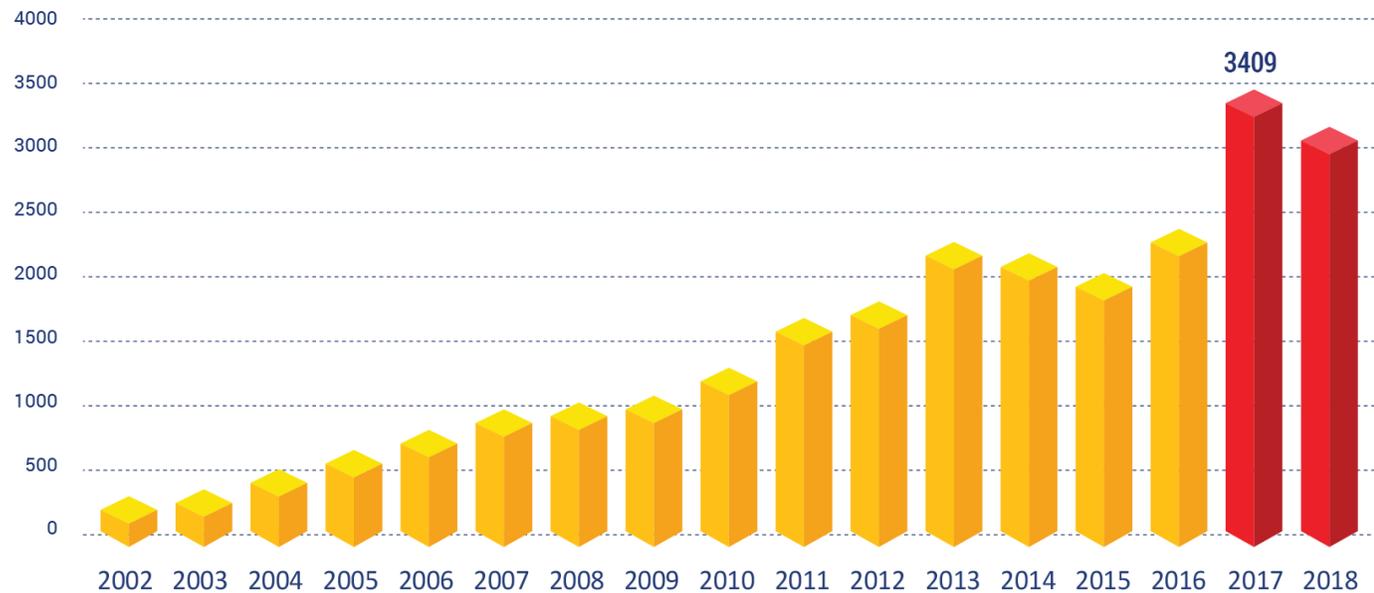


# Helping Developers Do Security The Right Way

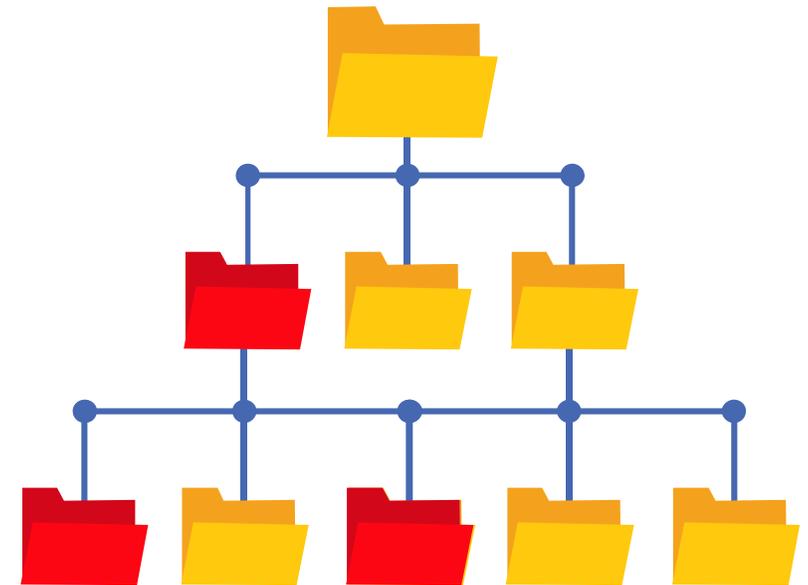


# THE CHALLENGE

## Reported Vulnerabilities Are Rising



## Transitive Dependencies

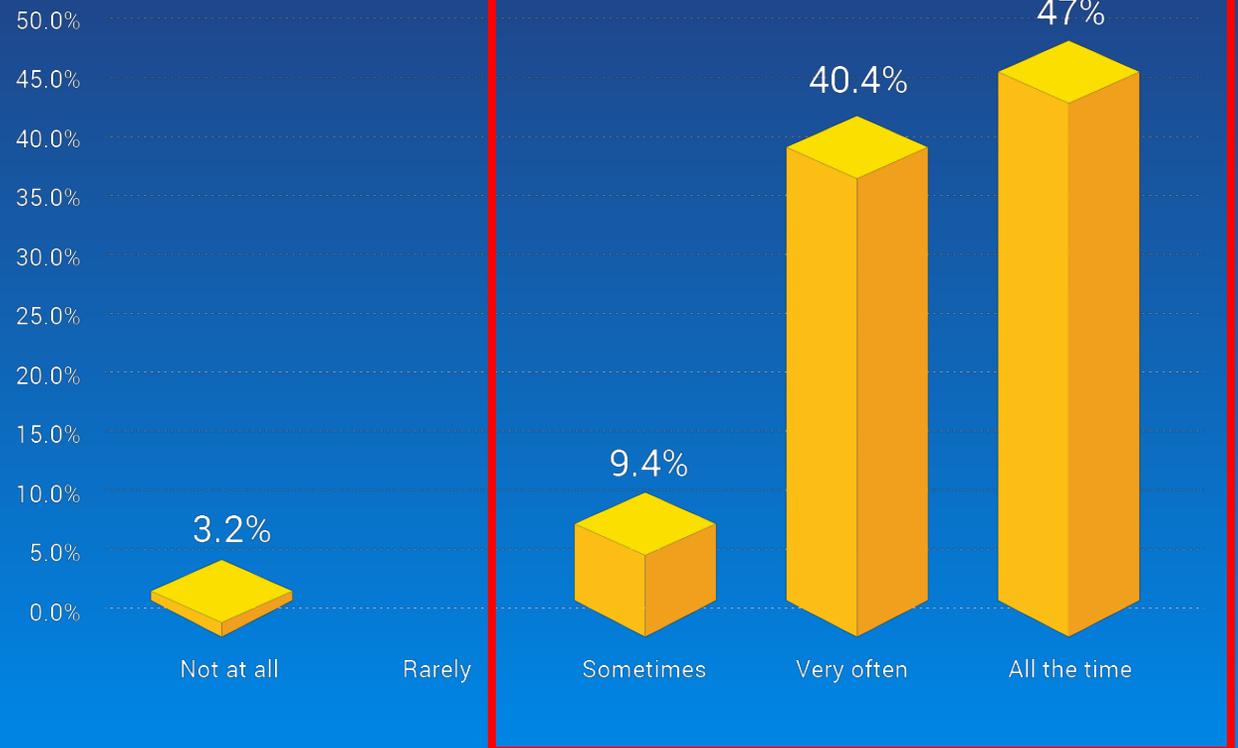


# OPEN SOURCE SECURITY VULNERABILITIES ARE ON THE RISE

A substantial number of developers are affected

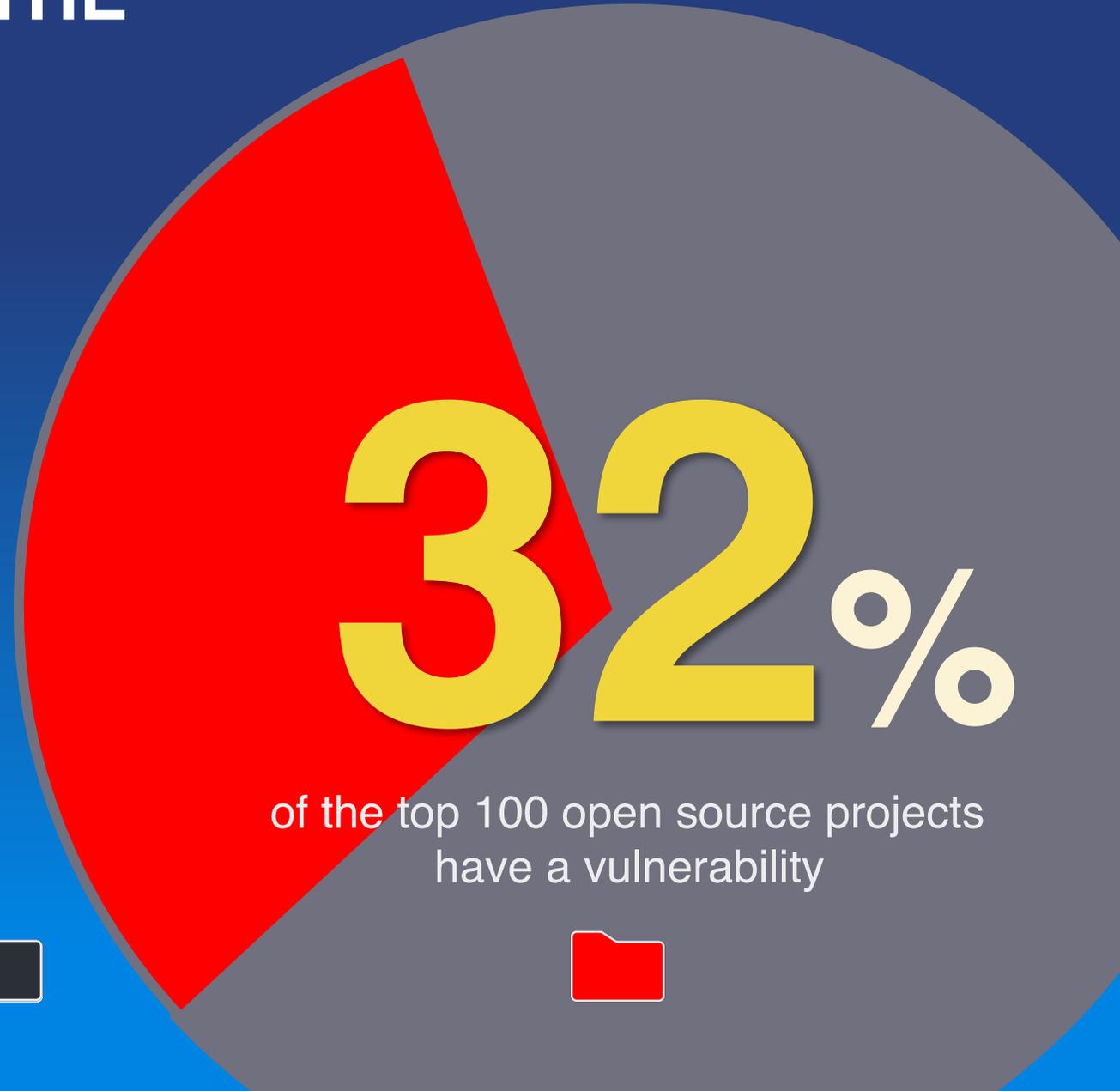
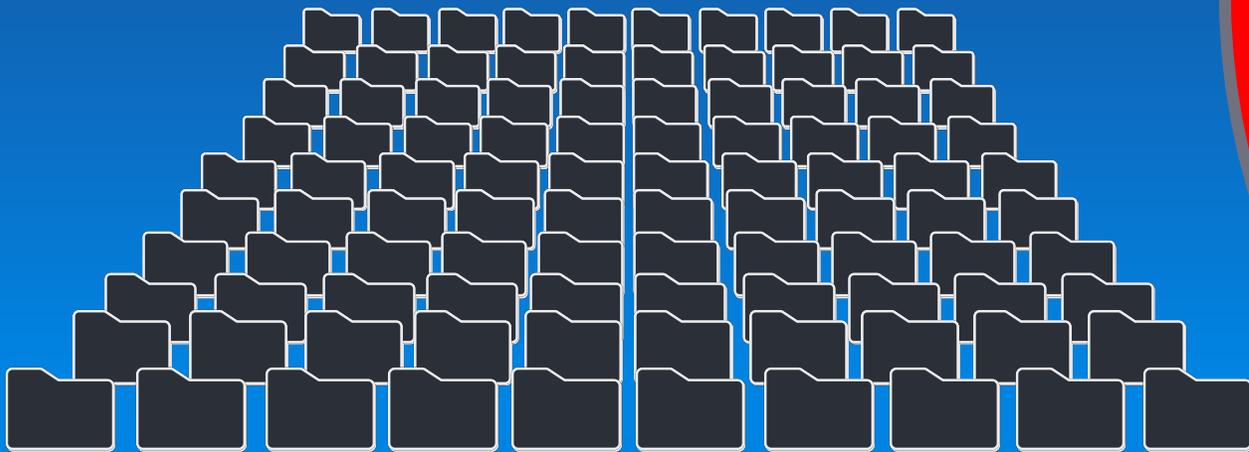
> 96%

of the developers are relying on  
open source components



# OPEN SOURCE SECURITY VULNERABILITIES ARE ON THE RISE

Project prevalence is alarming

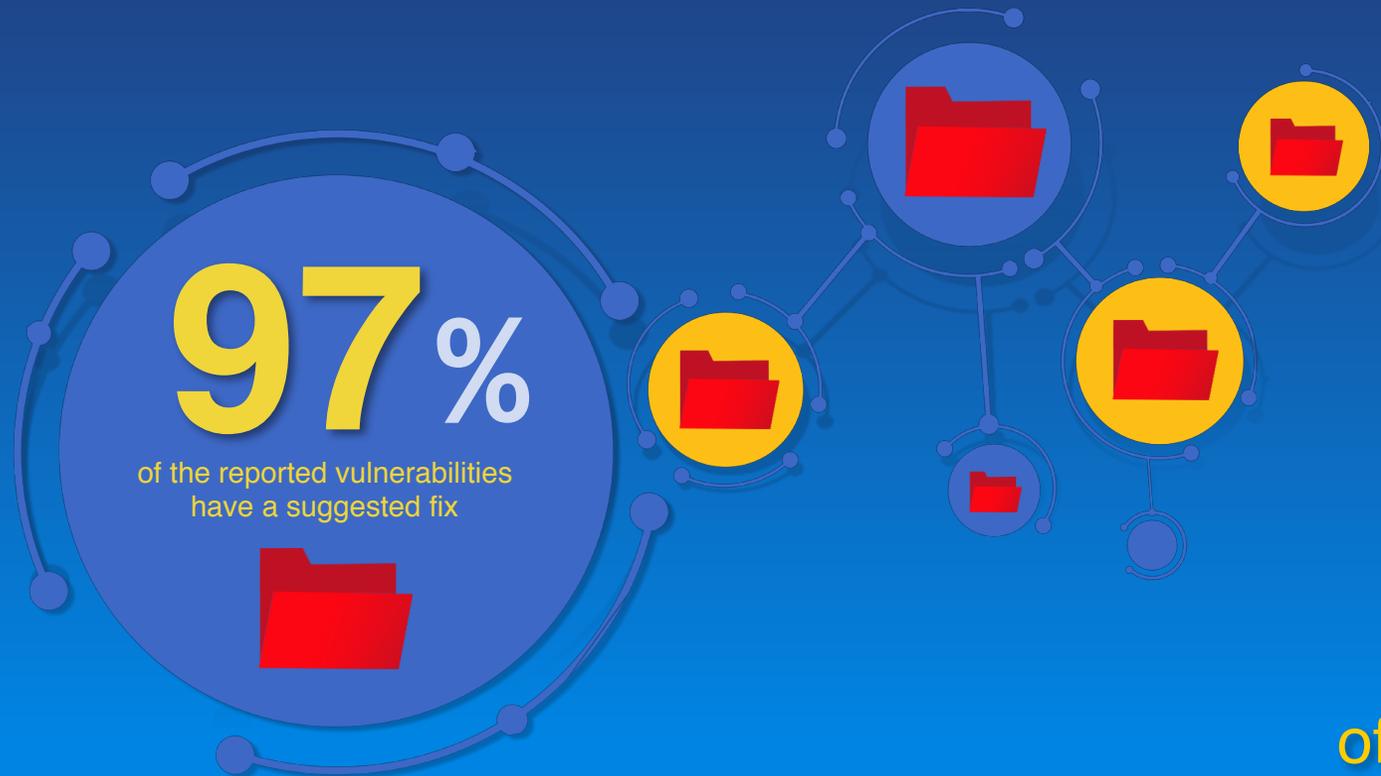


of the top 100 open source projects  
have a vulnerability



# OPEN SOURCE SECURITY VULNERABILITIES ARE ON THE RISE

Ignorance is [not] bliss



Just

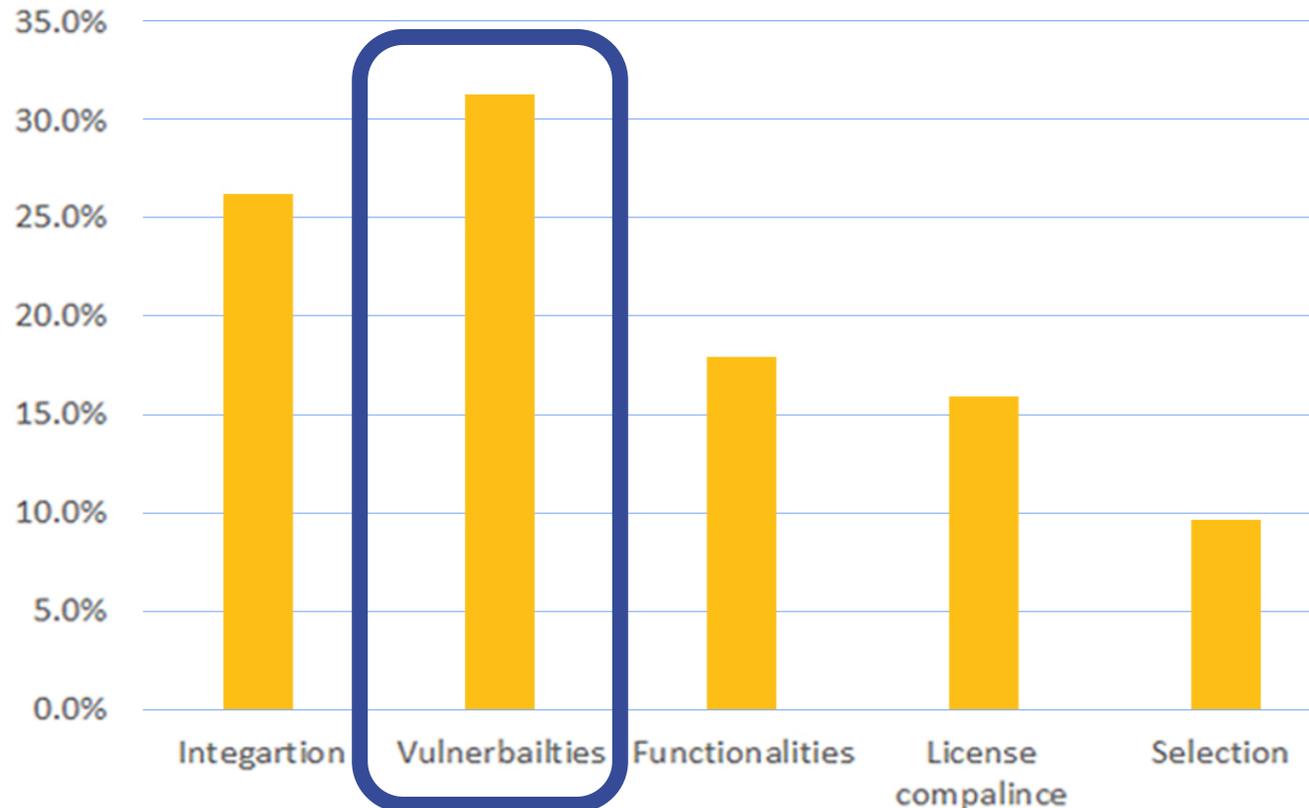
86%

of the reported open source vulnerabilities are in the CVE DB

# DEVELOPERS ARE NOT EFFICIENTLY MANAGING OPEN SOURCE VULNERABILITIES

## Challenges are acknowledged by developers

TOP CHALLENGES IN USING OPEN SOURCE COMPONENTS



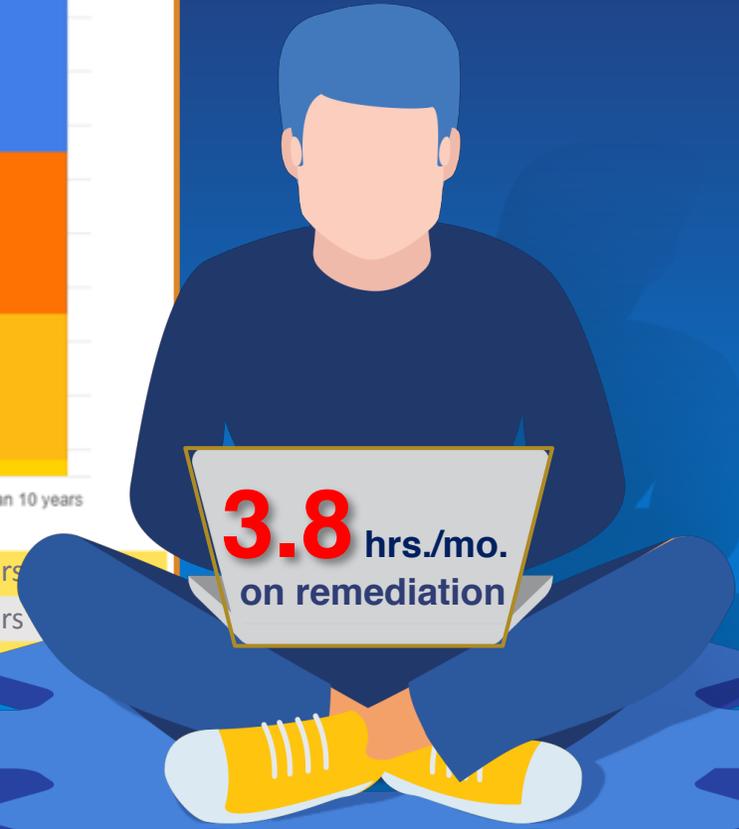
# DEVELOPERS ARE NOT EFFICIENTLY MANAGING OPEN SOURCE VULNERABILITIES

How much time is spent?

# 15

hours/month

spent on average by every developer on security vulnerabilities



# WORK SMARTER, NOT HARDER

Selection

Build

Release

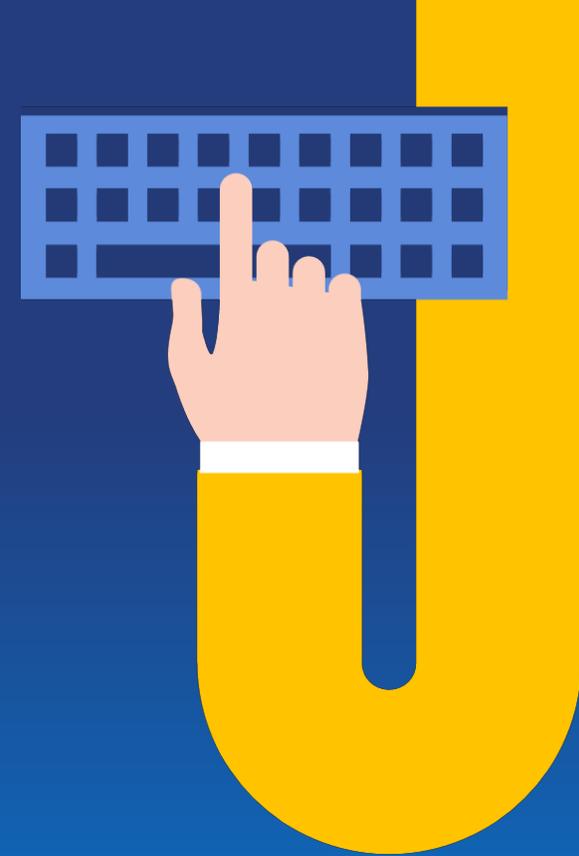
IDE

Post Deployment

Repos

# Handling Security Vulnerabilities

*The Common Way*



# THE COMMON WAY OF HANDLING SECURITY VULNERABILITIES



Security teams analyze and prioritize vulnerabilities



Sending emails or opening issues/tickets

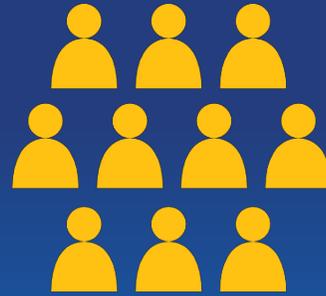


Closing the loop on resolution is hard

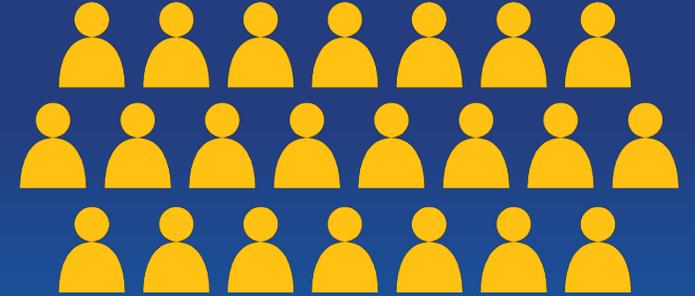
# BRIDGING THE GAP IS A MUST



Security



DevOps



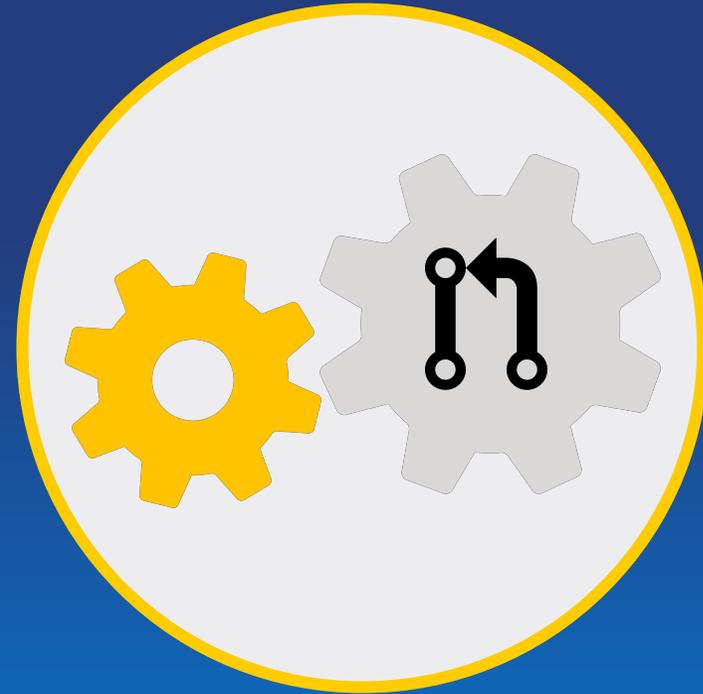
Developers

# How to Bake Security Into Existing Workflows





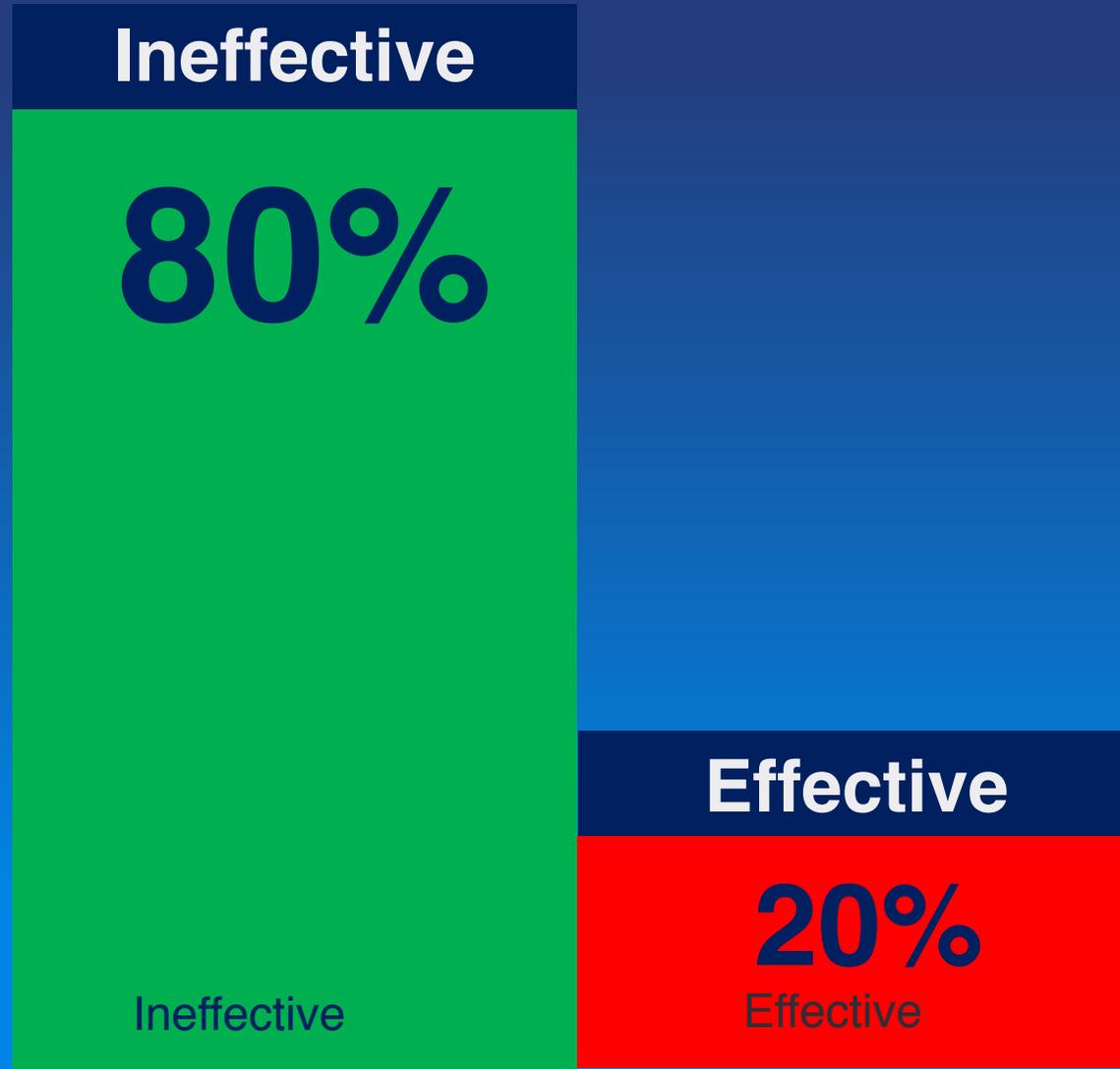
**Prioritization of  
effective vulnerabilities**



**Transparent integration  
with existing environment**

# INEFFECTIVE VS. EFFECTIVE VULNERABILITIES

Only some of the reported security vulnerabilities in open source libraries are referenced by the developers' code

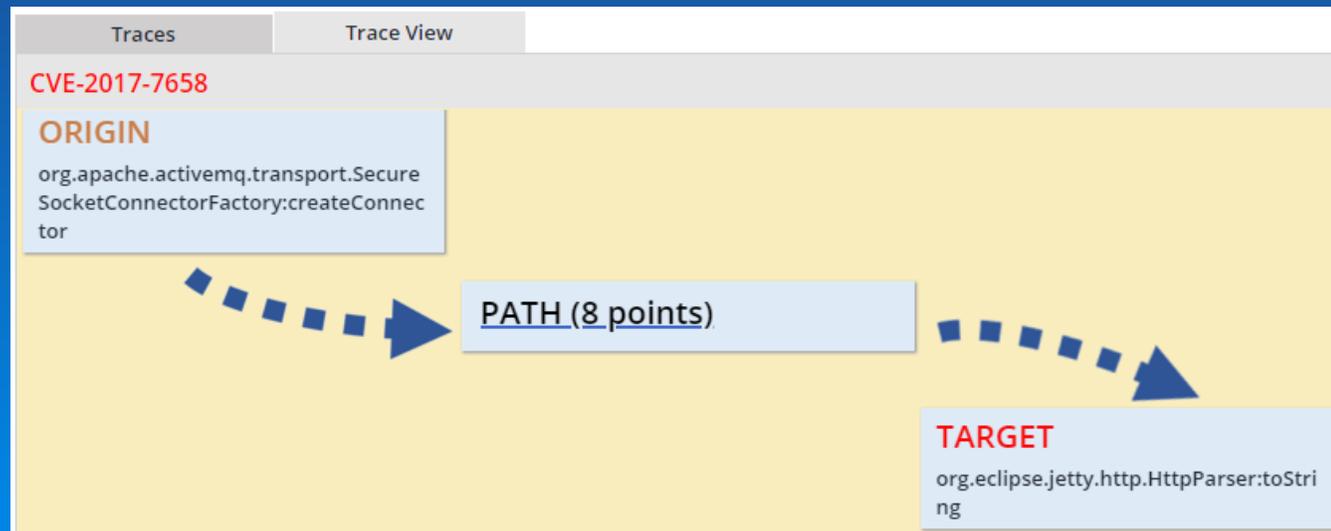


# How Do You Prioritize?



# A modern approach to prioritize open source security vulnerabilities should be based on the **effective** impact on the product security

Top Alerts			
<input type="checkbox"/>	Library	Type	Description
<input type="checkbox"/>	● jetty-http-9.2.22.v20170606.jar	Security Vulnerability	Medium: 1 (1) details
<input type="checkbox"/>	● ant-1.8.4.jar	Security Vulnerability	High: 1 (0) details
<input type="checkbox"/>	● commons-codec-1.9.jar	Security Vulnerability	Medium: 1 (0) details



# BAKING SECURITY CHECKS AND REMEDIATION INTO DEV WORKFLOWS

IDE integrations

Repos integration

WhiteSource Advise

WhiteSource  
Remediate

**WHITESOURCE**  
*for*  
**DEVELOPERS**

# WhiteSource Advise

Search...

5

pip install django==1.4

or

pip install django==1.6

or

pip install django

share improve this answer

edited Jul 30 '14 at 6:03

arulmr 5,977 6 36 60

add a comment

3

pip is not run from the Python shell . Run this from the Command prompt

pip install Django

It will install the latest Django 1.5.

Component: Django

Version 1.4 Outdated

License BSD 3

Organizational Policies: 1 Projects: 0

Organization: David H Demo

Violations: Reject GPL

Conditions: None

Approvals: None

Vulnerabilities

WhiteSource

pip install fails with "connection error: [SSL: CERTIFICATE\_VERIFY\_FAILED] certificate verify failed (\_ssl.c:598)"

Network Questions

wasn't DOSKEY integrated with MAND.COM?

Does the math work when buying airline ?

audio cues to encourage good posture

ok about people trapped in a series of s they imagine

ows 7 doesn't support WSL, then what does subsystem option mean?

o find all the available tools in mac terminal?

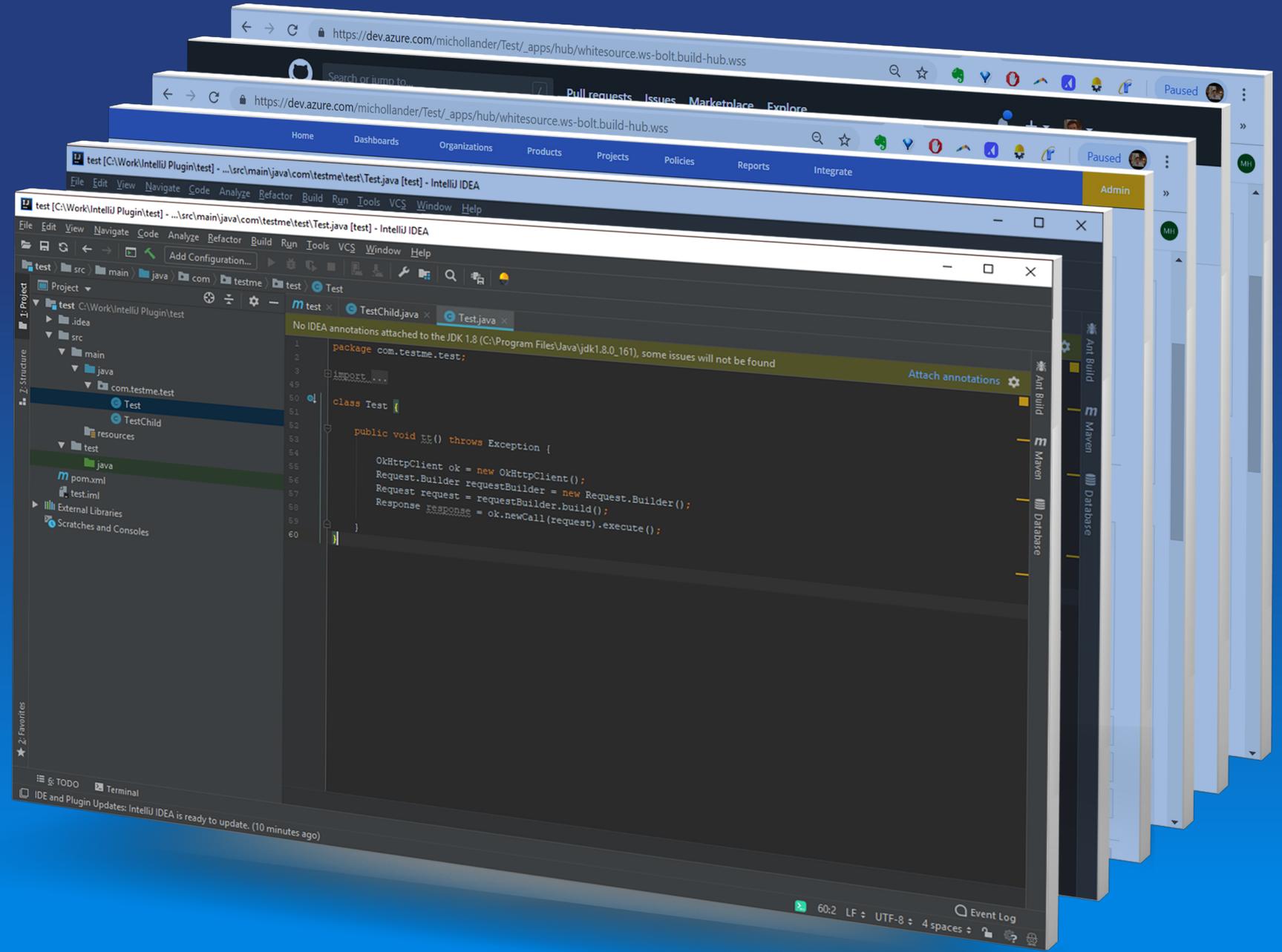
did Roosevelt decide to implement a num wage through taxation rather than a ceiling?

and boarding although I have proper visa and mentation. To whom should I make a complaint?

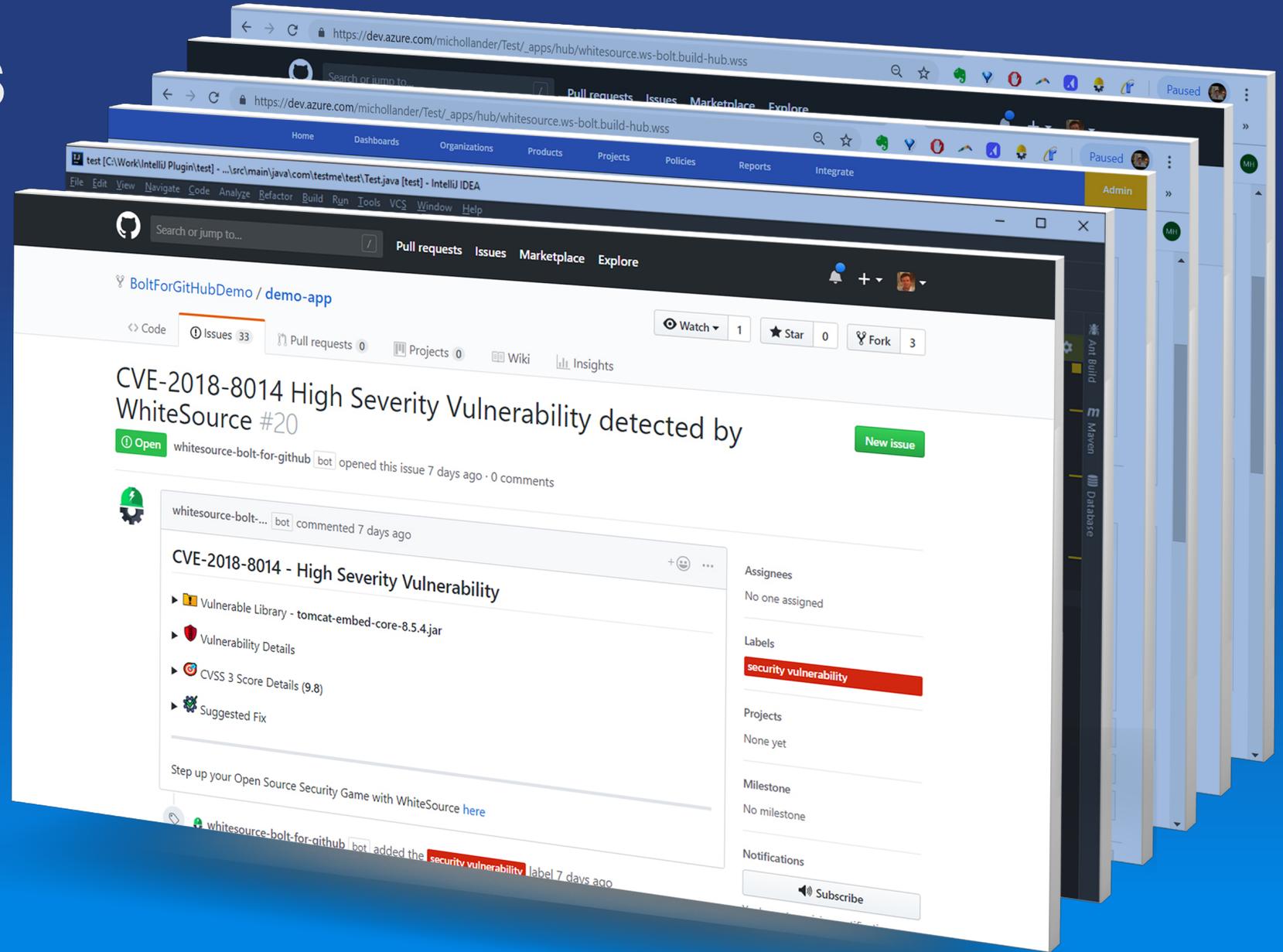
Should I use a zero-interest credit card for a large one-time purchase?

Is the Standard Deduction better than Itemized when both are the same amount?

# IDE Integration



# Repositories Integration





# Thank You

***Tamir Verthim***

*tamir.verthim@whitesourcesoftware.com*

***Terry Riley***

*terry.riley@whitesourcesoftware.com*