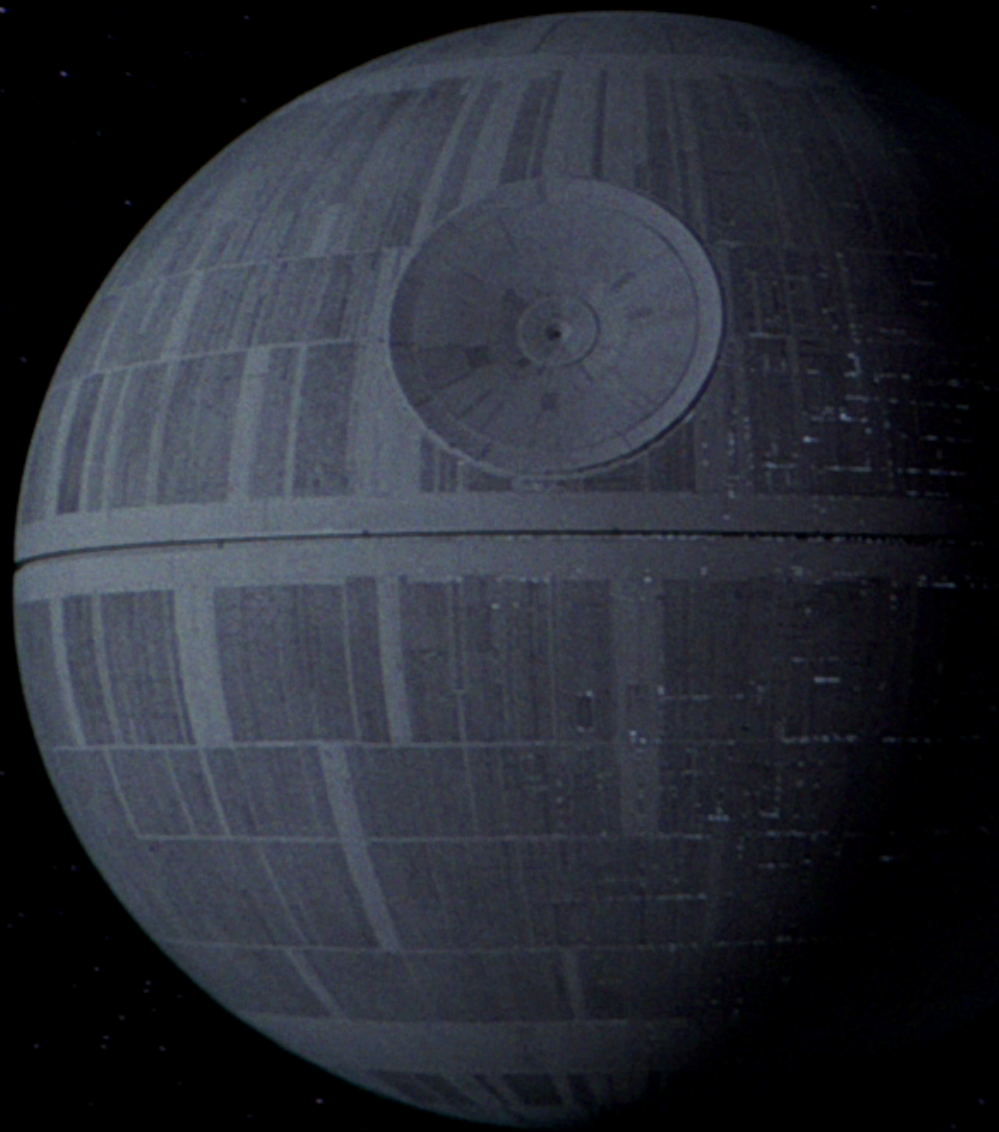
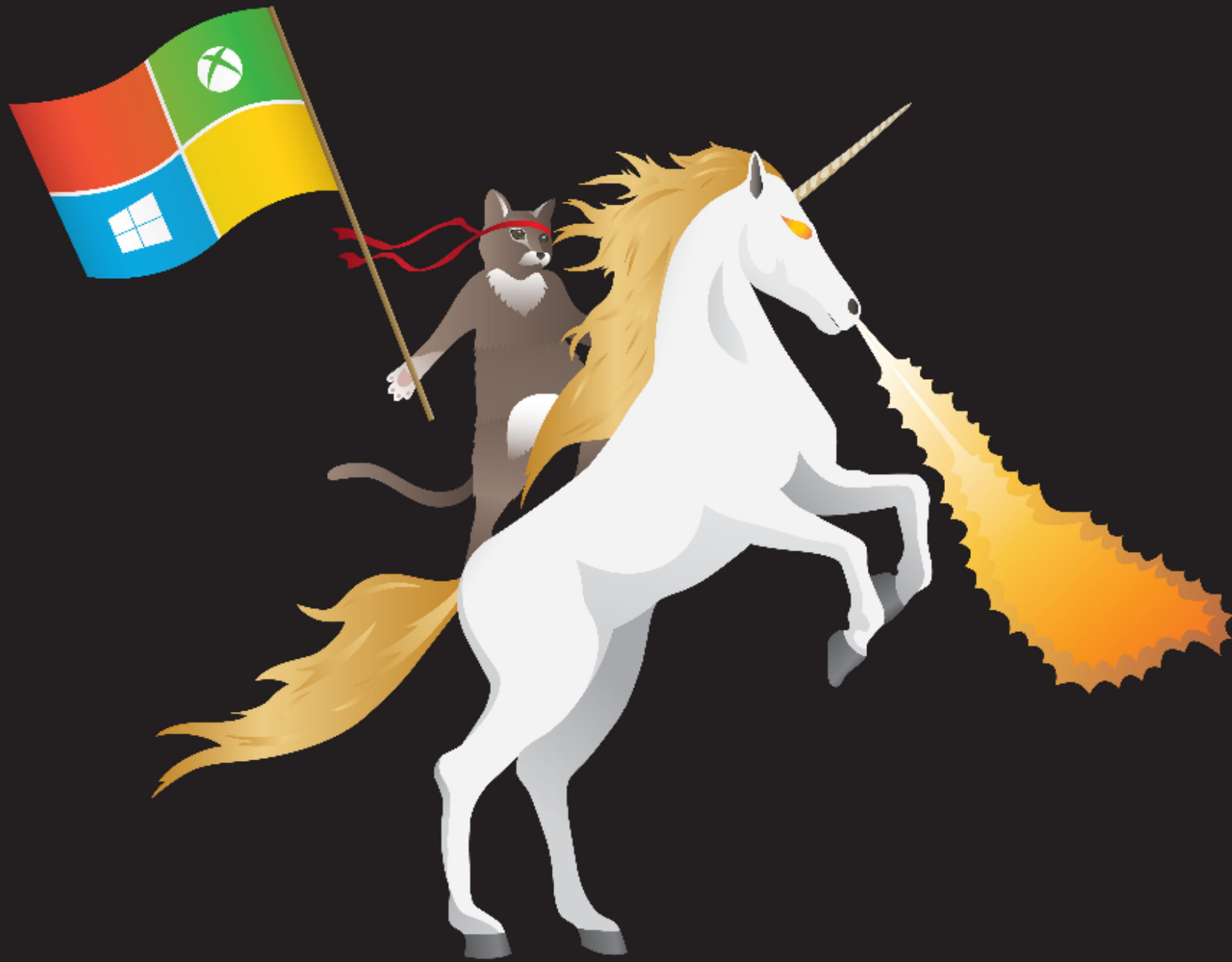


From Dev to Security

Rey Bango (@reybango)












Microsoft Edge



Rey Bango 

@reybango



I would love to go to [@defcon](#) but I'm scare
shitless to go to Def Con



Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

CMT from Mandiant's Pdd...

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)



Send \$300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

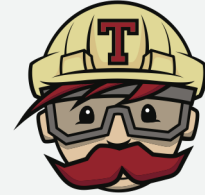
Copy

Check Payment

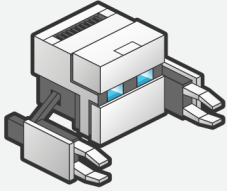
Decrypt

AppSec is hard





BABEL



Knockout.



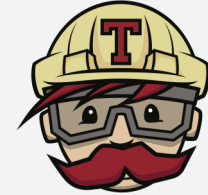
Lo



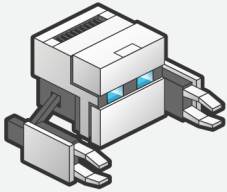
GitHub







BABEL



Knockout.



Lo



GitHub







Will Dormann

@wdormann

Following



Replying to @jmaxxz

Note to developers:
It doesn't matter how "good" your password
is if you tell everybody what it is.

```
Constants.java — W:\mycar — Atom
File Edit View Selection Find Packages Help
Project
mycar
  android
  ca
    automobility
      mycar
        models
        other
          Constants.java
          NotificationType.java
        services
        ui
        utils
      BuildConfig.java
      Manifest.java
      MyCarApplication.java
      R.java
    com
    fr
    jp
    ru
  a.java
  aa.java
ca\automobility\mycar\other\Constants.java 90:1 (1, 33)
CRLF UTF-8 Java GitHub Git (0)

Constants.java
88 public static String m2mMasterDistributorPassword() {
89     return "XXXXXXXXXX";
90 }
91
92 public static String m2mMasterDistributorUsername() {
93     return "api@solutionstlm.com";
94 }
95
96 public static String masterAccountId() {
97     return "100000";
98 }
99
```

8:01 PM - 8 Apr 2019

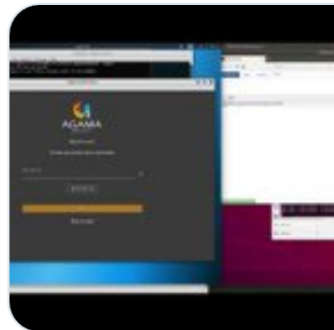


yan
@bcrypt

Following



“The attack was carried out by using a pattern that is becoming more and more popular; publishing a ‘useful’ package (electron-native-notify) to npm, waiting until it was in use by the target, and then updating it to include a malicious payload.”



Plot to steal cryptocurrency foiled by the npm sec...

Yesterday, the npm, Inc. security team, in collaboration with Komodo, helped protect over \$13 million USD in cryptocurrency assets as we found and responded to ...

blog.npmjs.org

12:20 PM - 6 Jun 2019



Gary Bernhardt

@garybernhardt

Follow



This is exactly what many of us predicted when NPM introduced a world of thousands of separate dependencies per app. The main reactions to that skepticism were "stop being so negative" and "don't try to stop progress."

yan @bcrypt

"The attack was carried out by using a pattern that is becoming more and more popular; publishing a 'useful' package (electron-native-notify) to npm, waiting until it was in use by the target, and then updating it to include a malicious payload." blog.npmjs.org/post/185397814...

Show this thread

1:40 PM - 8 Jun 2019

The screenshot shows the GitHub interface for the repository `vector-im/riot-web`. The top navigation bar includes links for Pull requests, Issues, Marketplace, and Explore. The repository statistics show 104 Watchers, 1,310 Stars, and 238 Forks. The left sidebar contains navigation options: Pulse, Contributors, Community, Commits, Code frequency, Dependency graph (selected), Network, and Forks.

Dependency graph

Dependencies Dependents

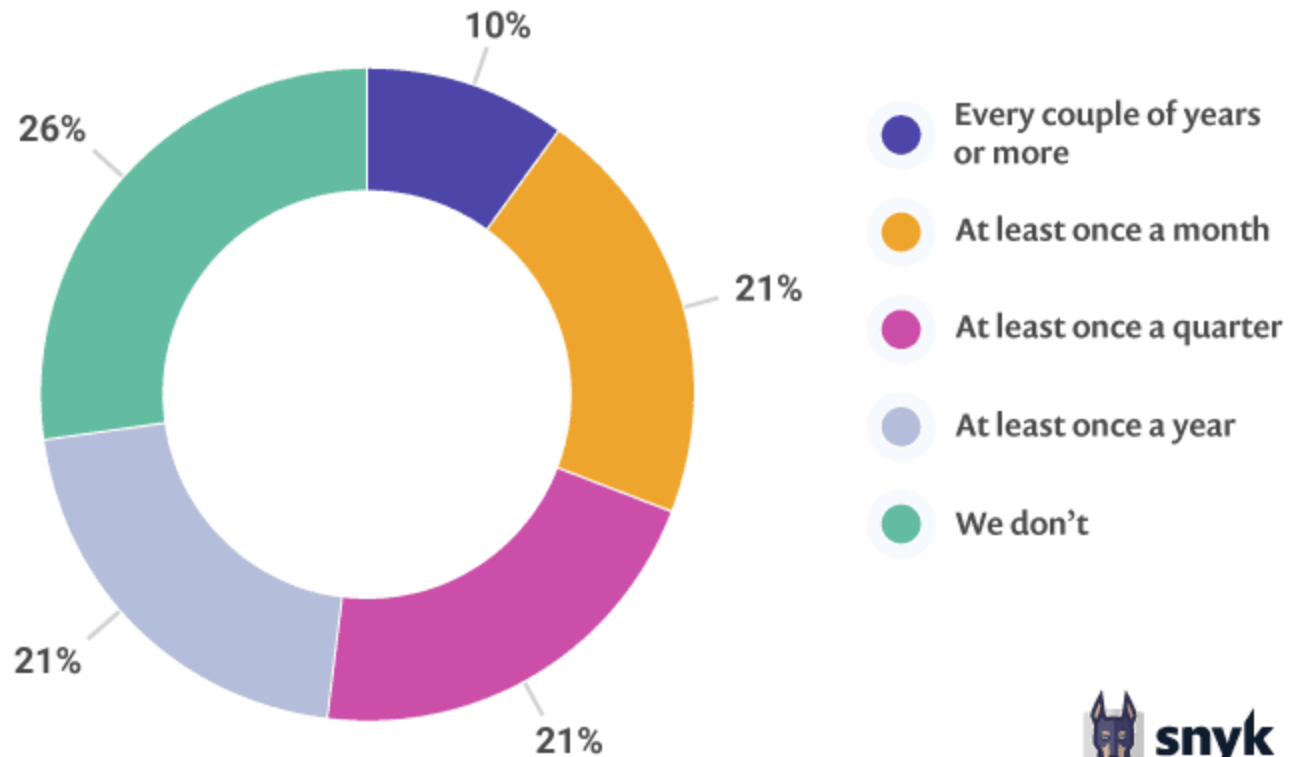
These dependencies have been defined in `riot-web`'s manifest files, such as `package.json`

Dependencies defined in `package.json` (9)

<code>postcss / autoprefixer</code>	^6.0.0
<code>browserify / browserify</code>	^14.1.0
<code>NodeGuy / assert</code>	^1.4.0
<code>mochajs / mocha</code>	~ 3.23.4
<code>jshkenas / coffee-script</code>	~ 1.8.0
<code>jshkenas / doctoc</code>	~ 0.6.2
<code>ty / commander</code>	== 0.5.2
<code>shouldjs / should</code>	^ 11.2.1
<code>pelusantono / bluebird</code>	^ 3.6.0
<code>evore / eslint</code>	^ 3.0.0

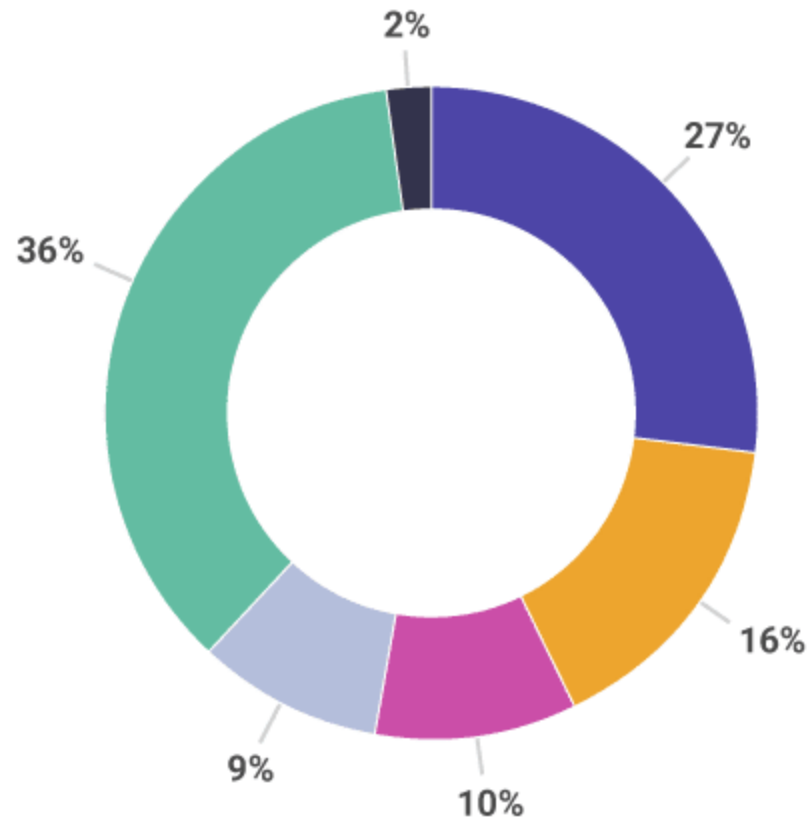
Credit: <https://imgur.com/user/PipePistoleer>







OS maintainers differ in their code auditing cadence



Implicit trust

How do you find about vulnerabilities?



-  I probably won't
-  I read the release notes of most of my direct and indirect dependencies
-  When my security team reports a severe vulnerability, we search for apps using this component
-  We track the list of dependencies against public databases (e.g. CVEs) ourselves
-  We use a dependency management/ scanning tool that notifies us
-  Other

On average, each Web application that Positive Technologies inspected contained **33 vulnerabilities**. Of those, six were high-severity flaws, compared to just two the prior year.

More than two-thirds of the apps (**67%**) contained **critical vulnerabilities such as insufficient authorization errors, arbitrary file upload, path traversal, and SQL injection flaws**.

<https://www.darkreading.com/vulnerabilities---threats/web-apps-are-becoming-less-secure/>

VeraCode polled 400 app developers from the UK, US and Germany and ***found just 52% update these components when a new vulnerability is announced.*** The research revealed that 83% of respondents use either commercial and/or open source components, with an average of 73 used per application.

Some 71 vulnerabilities per application are introduced on average through use of third-party components, ***with only 23% of respondents claiming they test for bugs in components at every release.***

<https://www.darkreading.com/vulnerabilities---threats/web-apps-are-becoming-less-secure/>

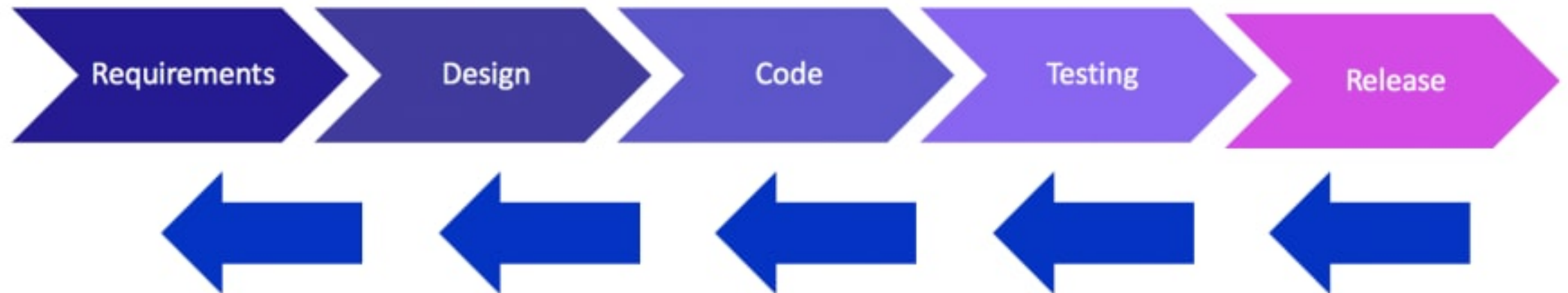
Web apps & APIs are the
new attack endpoints



OWASP Top 10 - 2017

The Ten Most Critical Web Application Security Risks

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project



Credit: Tanya Janca, Cloud Security Advocate at MSFT

Security Champions



Jerry Bell

@Maliciouslink

Following



Replying to @ElissaBeth @IanColdwater

Great question. I would summarize what I heard Ian say is that infosec needs to build bridges to better communicate with devops, which seems right. One of the major challenges, I find, is that developers often lack the perspective on the adversarial mindset.

2:38 PM - 31 Mar 2019







7:46:53

The Complete Ethical Hacking Course for 2019!

Joseph Delgadillo ✓ 429K views • 4 months ago

Get the 19 course holiday bundle! <https://josephdelgadillo.com/product/holiday-course-bundle-sale/> Get The Complete Ethical ...



HACKER
HOUSE™





eLearnSecurity
Forging security professionals



SANS



Practice makes permanent

OWASP Juice Shop



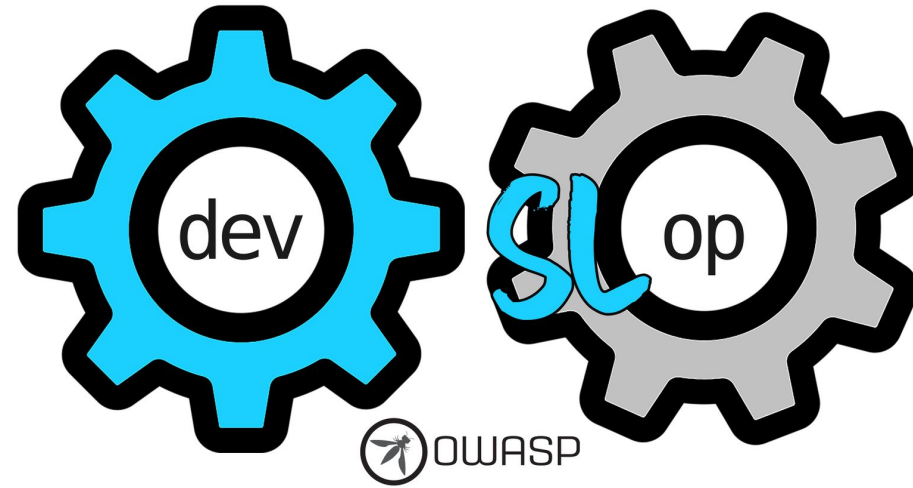
https://www.owasp.org/index.php/OWASP_Juice_Shop_Project

Damn Vulnerable Web Application (DVWA)



<http://www.dvwa.co.uk>

OWASP DevSlop Project



https://www.owasp.org/index.php/OWASP_DevSlop_Project

Automate Security

BEFORE AUTOMATING YOUR OPEN SOURCE...



Over 75% were aware to only 50% of their open source inventory.



It takes **6 weeks** on average to approve a new component.



90% have at least **1 vulnerability**, over 45% have 5 and up.



There's at least **1 license** that doesn't meet company policy on average.

* Based on first scan results for 250 applications and end of PoC questionnaire



Home

Alerts 27

Ignore Selected

<input type="checkbox"/>	Library	Type	Description	Occurrences	Creation Date	
<input type="checkbox"/>	esapi-2.0.1.jar	Security Vulnerability	Medium: 1 (0) Low: 1...	1 project details	07-05-2018	ignore
<input type="checkbox"/>	bcprov-jdk15-1.46.jar	Security Vulnerability	Medium: 1 (0) details	1 project details	07-05-2018	ignore
<input type="checkbox"/>	jackson-dataformat-xm...	Security Vulnerability	High: 1 (1) details	1 project details	07-05-2018	ignore
<input type="checkbox"/>	commons-beanutils-1.8...	Security Vulnerability	High: 1 (0) details	5 projects details	08-05-2018	ignore
<input type="checkbox"/>	commons-fileupload-1....	Security Vulnerability	High: 4 (0) Low: 1 (0) ...	5 projects details	08-05-2018	ignore
<input type="checkbox"/>	spring-web-3.1.1.RELEA...	Security Vulnerability	Medium: 6 (0) details	5 projects details	08-05-2018	ignore
<input type="checkbox"/>	struts2-core-2.3.31.jar	Security Vulnerability	High: 2 (1) Medium: ...	5 projects details	08-05-2018	ignore
<input type="checkbox"/>	shiro-web-1.2.0.jar	Security Vulnerability	Medium: 1 (0) details	5 projects details	08-05-2018	ignore
<input type="checkbox"/>	shiro-core-1.2.0.jar	Security Vulnerability	Medium: 1 (0) details	5 projects details	08-05-2018	ignore
<input type="checkbox"/>	mysql-connector-java-5...	Security Vulnerability	Medium: 1 (0) Low: 1...	5 projects details	08-05-2018	ignore

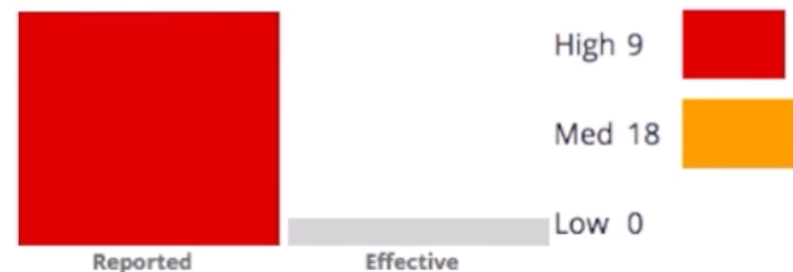
Show Reported Vulnerabilities Show Only Effective Vulnerabilities

view all alerts

Security and Quality

Reported Vulnerability Score: High

Libs. with Vulnera



Outdated and Vulnerable Libs.

Libs. with Known

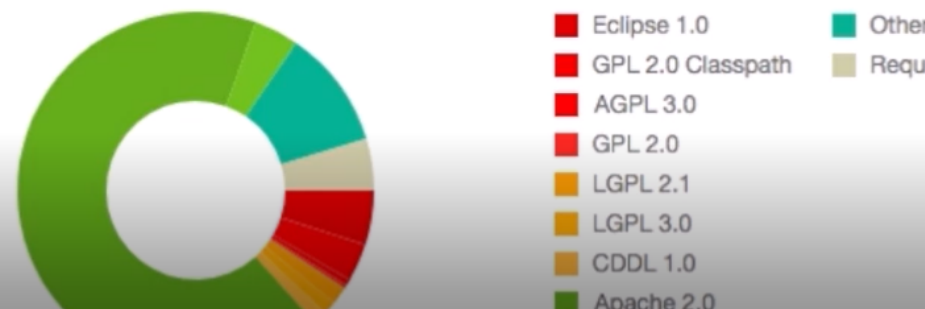


Top 10 Products (8)

Product	Projects	Libraries	Vulnerabilities	Licenses
appserver-working	1	296	High: 8 Medium: 21 Low: 2	25
appserver	1	291	High: 7 Medium: 19 Low: 1	24
Effective_Usage_Demo_1	1	41	High: 7 Medium: 13 Low: 2	8
Effective_Usage_Demo_2	1	41	High: 7 Medium: 13 Low: 2	8
ksa	1	41	High: 7 Medium: 13 Low: 2	8
Effective_Usage_Demo	1	40	High: 7 Medium: 13 Low: 2	8
My_WS_DemoEUA_Prod	1	40	High: 7 Medium: 13 Low: 2	8

appserver-working

License Distribution





VERACODE

BLACKDUCK

BY **SYNOPSYS**[®]

Build a strong network



Tanya Janca
@shehackspurple

Look for non-traditional talent



Do the right thing