DEV SEC OPS DAYS

Why Organizations Need DevSecOps Now More Than Ever

Krishna Guru

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Agenda

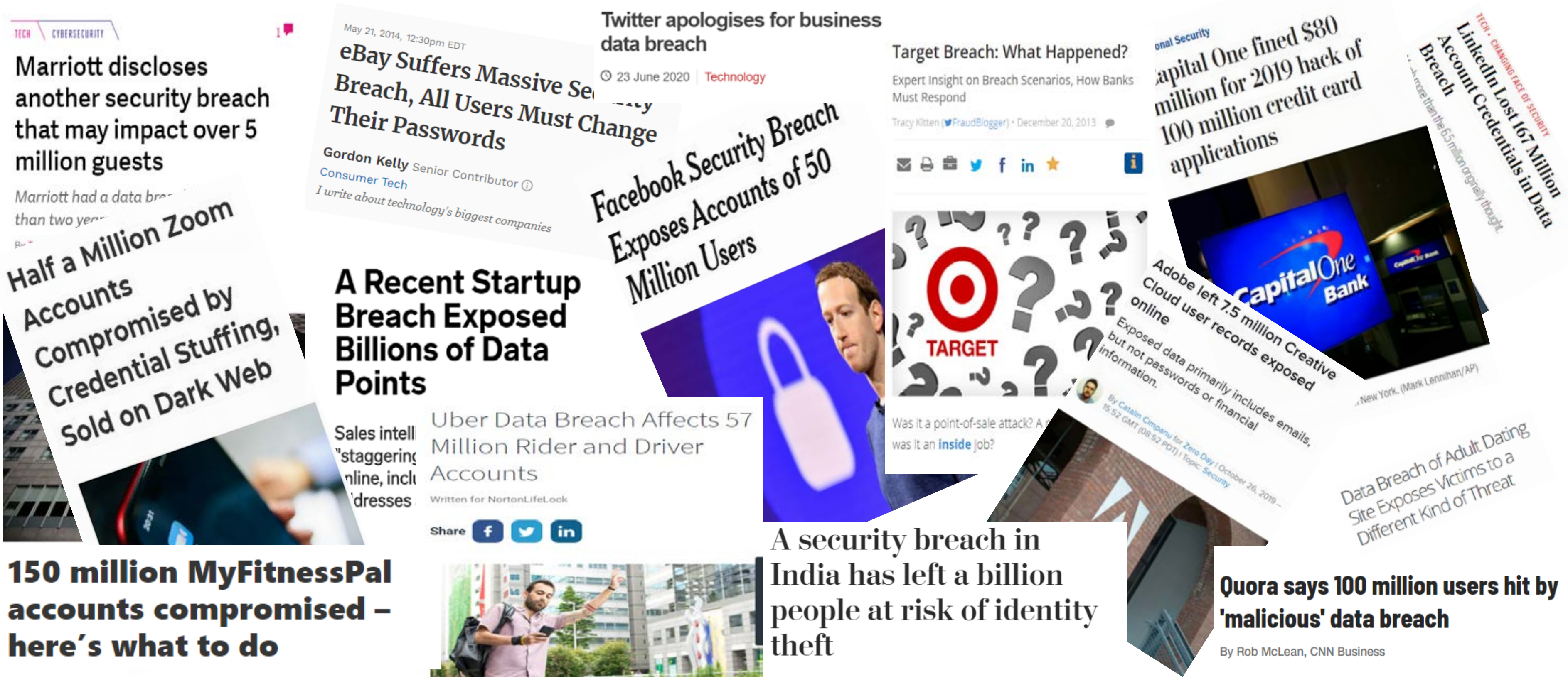
- Data breach
- Open-source software
- DevSecOps
- The current situation
- Transforming from DevOps to DevSecOps
- Q & A

DEV SEC OPS DAYS

Why Organizations Need DevSecOps Now More Than Ever

Data breach

Data Breach



TECH CYBERSECURITY

Marriott discloses another security breach that may impact over 5 million guests

Marriott had a data bre… than two year…

May 21, 2014, 12:30pm EDT

eBay Suffers Massive Se…ity Breach, All Users Must Change Their Passwords

Gordon Kelly Senior Contributor
Consumer Tech
I write about technology's biggest companies

Twitter apologises for business data breach

23 June 2020 | Technology

Target Breach: What Happened?

Expert Insight on Breach Scenarios, How Banks Must Respond

Tracy Kitten (FraudBlogger) • December 20, 2013

Was it a point-of-sale attack? A … was it an inside job?

…onal Security

…apital One fined $80 million for 2019 hack of 100 million credit card applications

…New York. (Mark Lennihan/AP)

TECH • CHANGING FACE OF SECURITY

LinkedIn Lost 167 Million Account Credentials in Data Breach

…more than the 6.5 million originally thought.

Half a Million Zoom Accounts Compromised by Credential Stuffing, Sold on Dark Web

Facebook Security Breach Exposes Accounts of 50 Million Users

A Recent Startup Breach Exposed Billions of Data Points

Sales intelli… "staggering… …nline, inclu… …dresses…

Uber Data Breach Affects 57 Million Rider and Driver Accounts

Written for NortonLifeLock

Share f in

Adobe left 7.5 million Creative Cloud user records exposed online

Exposed data primarily includes emails, but not passwords or financial information.

By Catalin Cimpanu for Zero Day | October 26, 2019 -- 15:52 GMT (08:52 PDT) | Topic: Security

Data Breach of Adult Dating Site Exposes Victims to a Different Kind of Threat

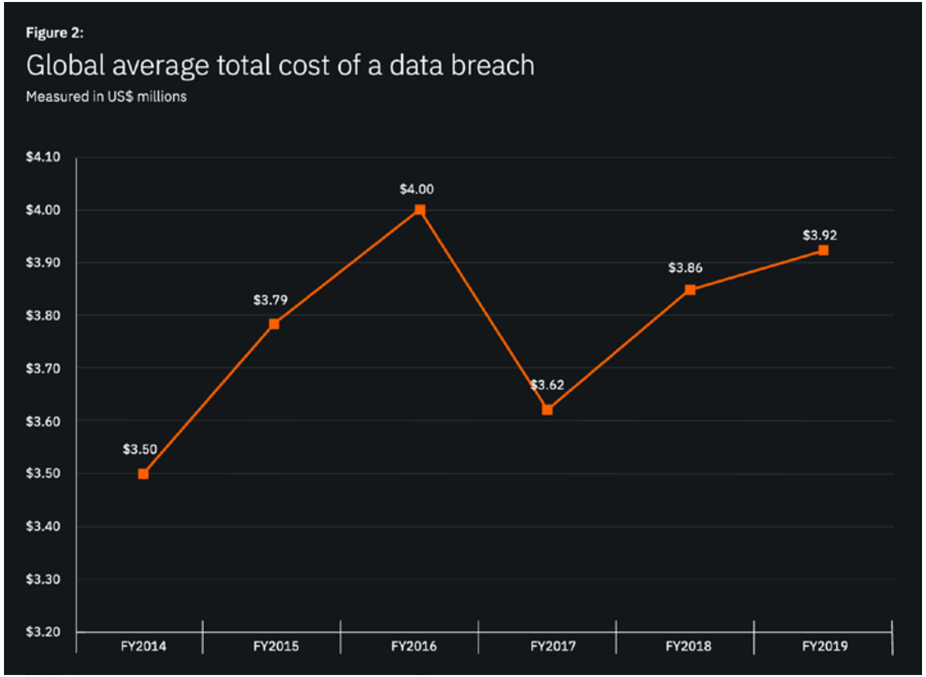
150 million MyFitnessPal accounts compromised – here's what to do

A security breach in India has left a billion people at risk of identity theft

Quora says 100 million users hit by 'malicious' data breach

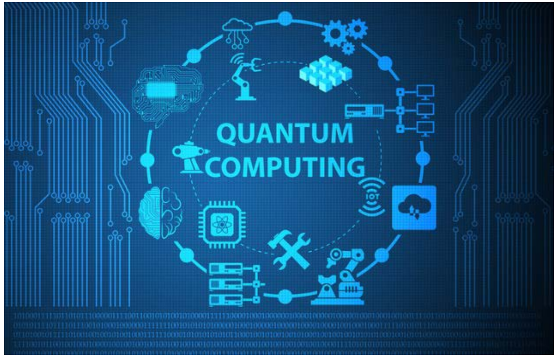
By Rob McLean, CNN Business

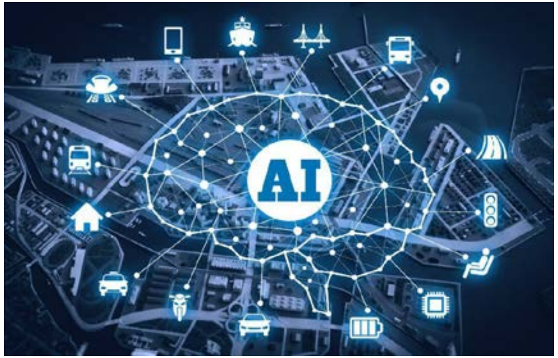
Cost of a breach



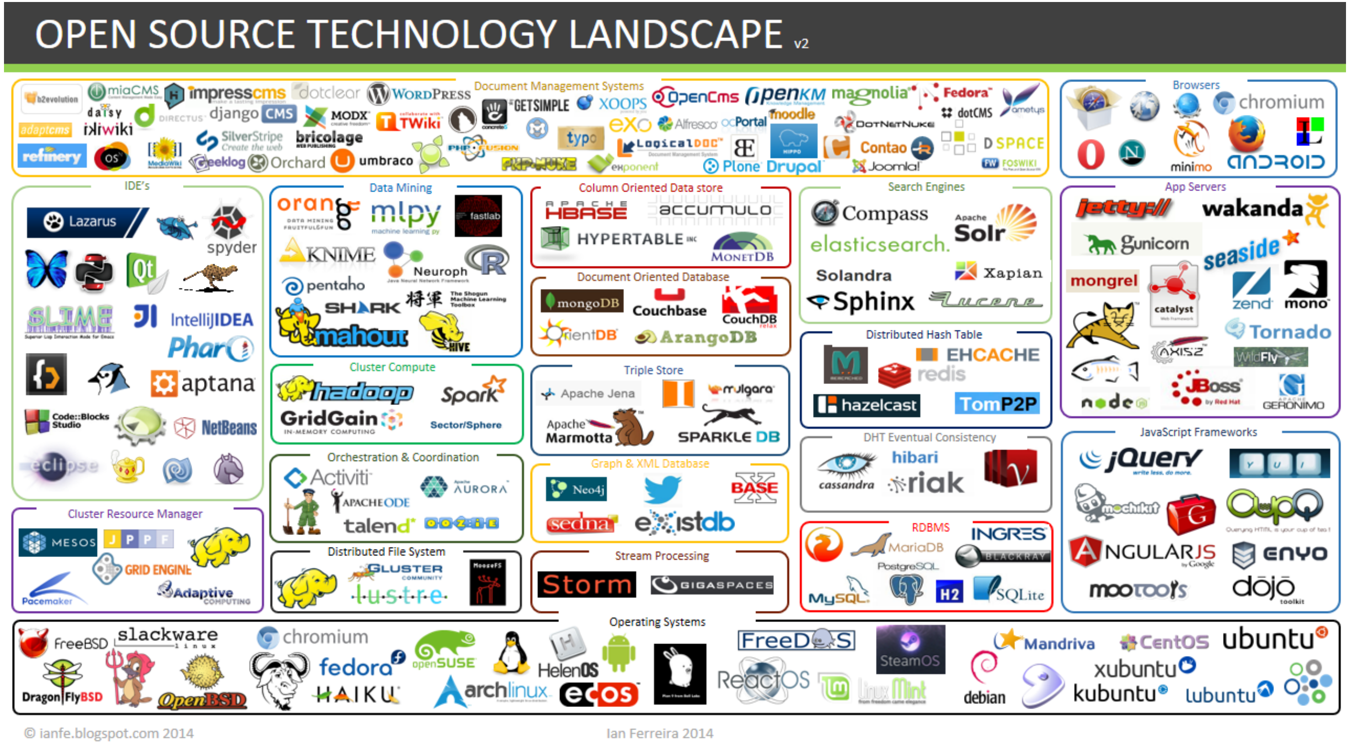
Source - IBM and the Ponemon Institute's annual Cost of a Data Breach report

Threat to emerging technologies

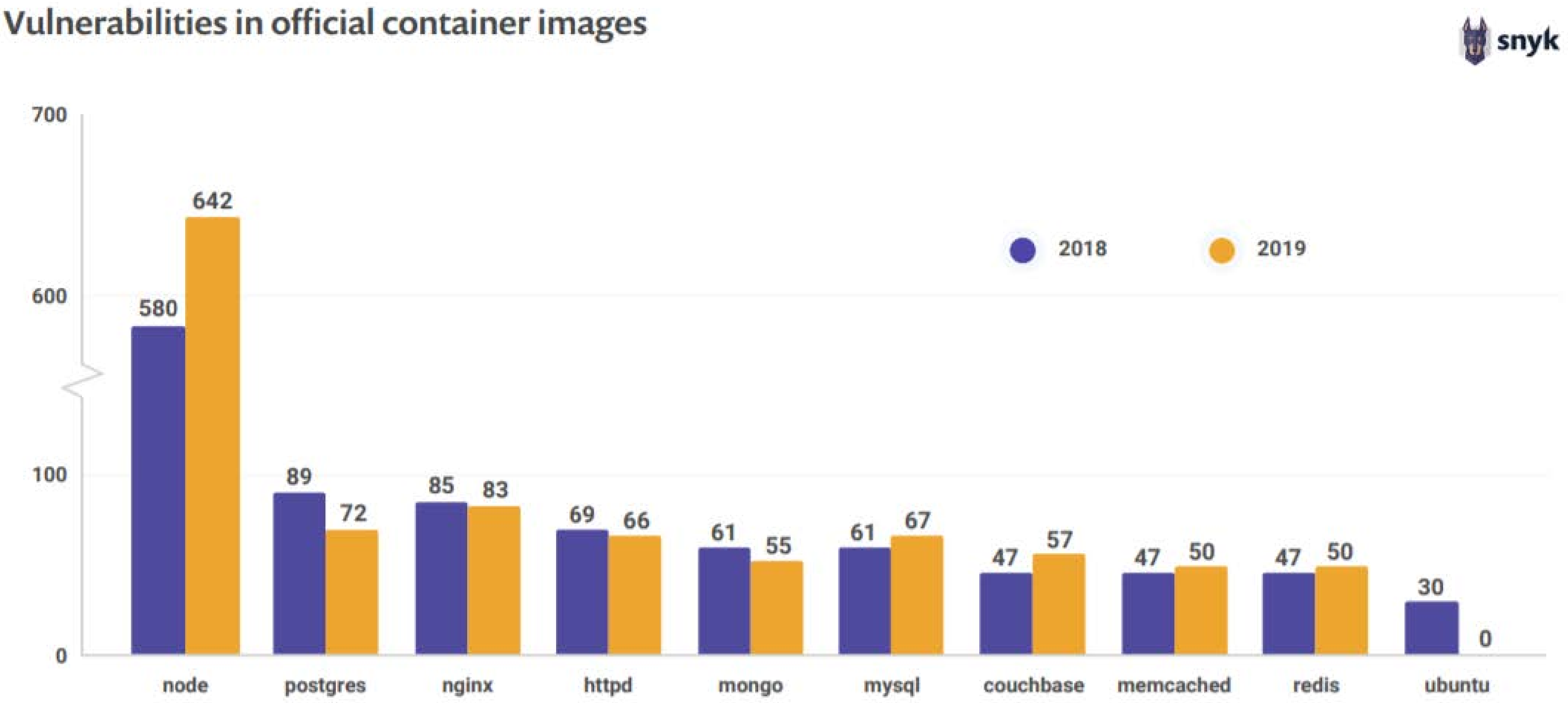




Open-source software


OPEN SOURCE TECHNOLOGY LANDSCAPE v2
Document Management Systems
miaCMS impresscms dotclear WordPress daisy django CMS MODX TWiki GETSIMPLE XOOPS OpenCms openKM magnolia Fedora dotCMS ametys ikiwiki adaptcms refinery SilverStripe bricolage exo Alfresco Portal moodle DotNetNuke typo LogicalDOC Contao DSPACE Geeklog Orchard umbraco PHP-NUKE exponent Plone Drupal Joomla! FOSWIKI MediaWiki
Browsers
chromium minimo android
IDE's
Lazarus spyder Qt SLIME IntelliJIDEA Pharo aptana Code::Blocks Studio NetBeans eclipse
Data Mining
orange mlpy fastlab KNIME Neuroph R pentaho SHARK Shogun mahout HIVE
Column Oriented Data store
APACHE HBASE accumulo HYPERTABLE MonetDB
Document Oriented Database
mongoDB Couchbase CouchDB OrientDB ArangoDB
Search Engines
Compass Apache Solr elasticsearch Solandra Xapian Sphinx Lucene
App Servers
jetty:// wakanda Gunicorn seaside mongrel catalyst zend mono Tornado AXIS2 WildFly node JBoss GERONIMO
Cluster Compute
hadoop Spark GridGain Sector/Sphere
Triple Store
Apache Jena mulgara Apache Marmotta SPARKLE DB
Distributed Hash Table
EHCACHE redis hazelcast TomP2P
Orchestration & Coordination
Activiti APACHEODE AURORA talend OOZIE
Graph & XML Database
Neo4j BASE sedna existdb
DHT Eventual Consistency
cassandra hibari riak
JavaScript Frameworks
jQuery YUI mochikit CupQ ANGULARJS enyo mootools dojo toolkit
Cluster Resource Manager
MESOS JPPF GRID ENGINE Adaptive COMPUTING Pacemaker
Distributed File System
GLUSTER lustre MooseFS
Stream Processing
Storm GIGASPACES
RDBMS
MariaDB INGRES BLACKRAY PostgreSQL MySQL H2 SQLite
Operating Systems
FreeBSD slackware chromium fedora openSUSE HelenOS FreeDOS SteamOS Mandriva CentOS ubuntu DragonFlyBSD OpenBSD HAIKU archlinux ecos ReactOS Linux Mint debian xubuntu kubuntu lubuntu
© ianfe.blogspot.com 2014
Ian Ferreira 2014

Threats in Open-source software

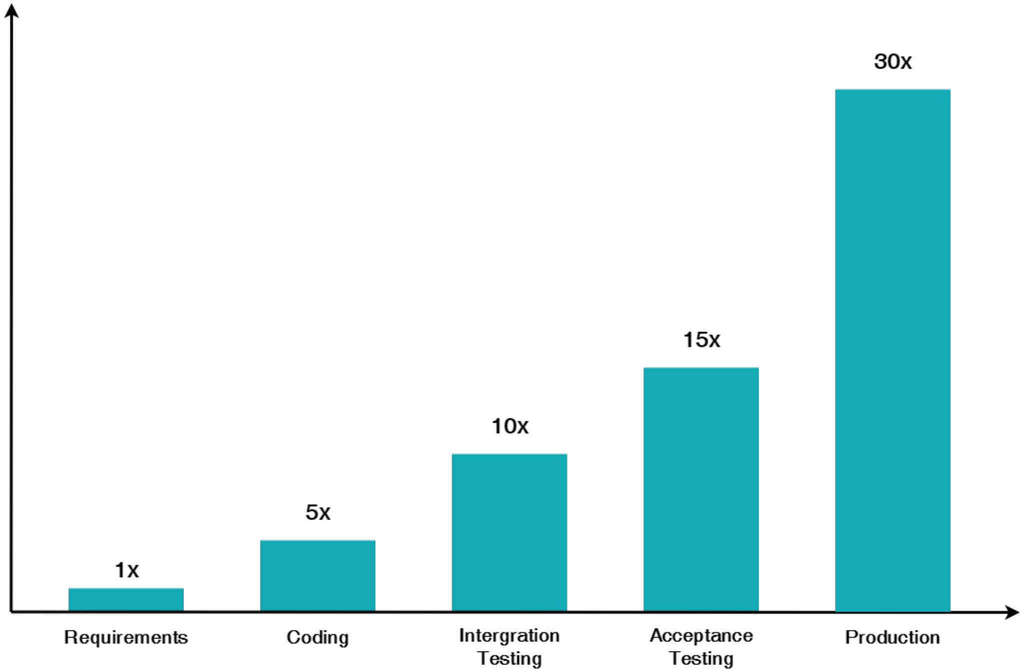


DEV SEC OPS DAYS

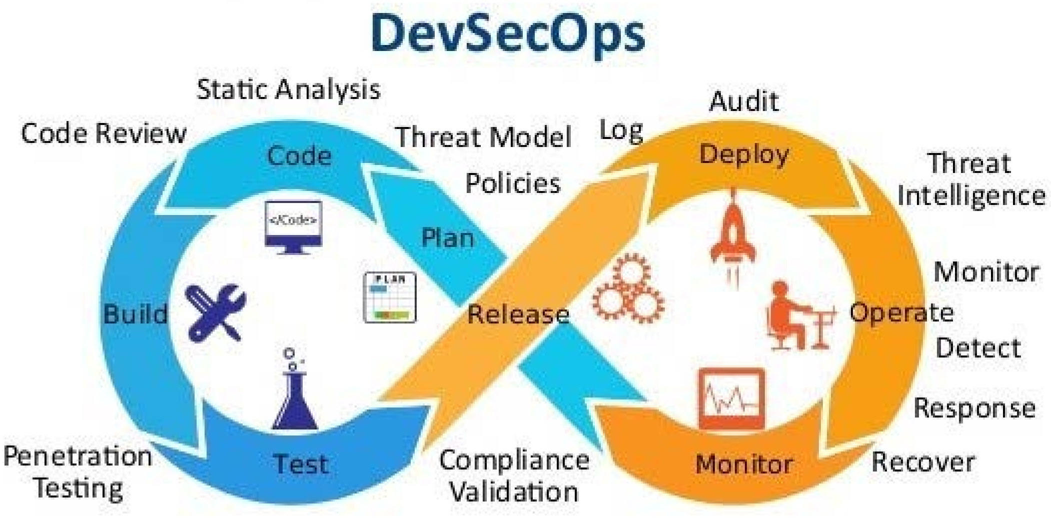
Why Organizations Need DevSecOps Now More Than Ever

DevSecOps

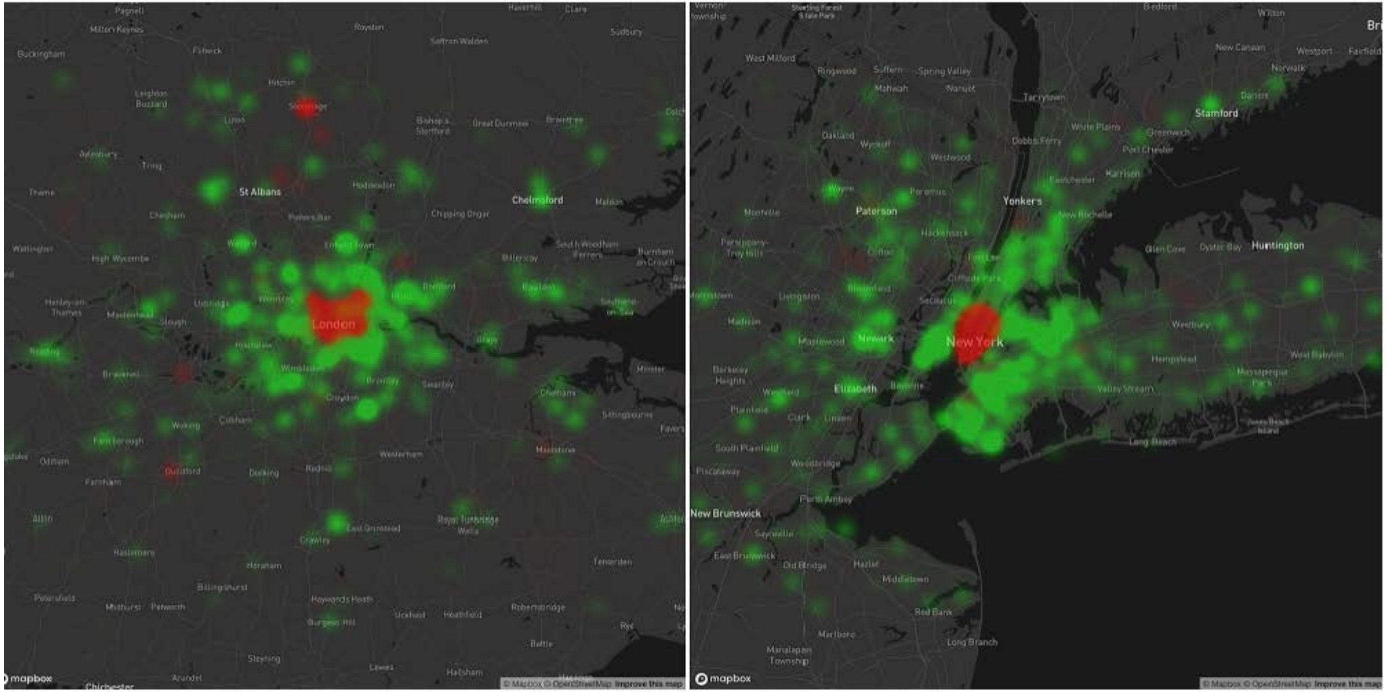
The cost of fixing defects



DevSecOps


DevSecOps
Static Analysis
Code Review
Code
</Code>
Threat Model
Policies
Plan
PLAN
Build
Release
Test
Penetration Testing
Compliance Validation
Log
Audit
Deploy
Threat Intelligence
Monitor
Operate
Detect
Response
Recover
Monitor

The situation now



Change in internet use in London (left) and New York (right) between Wednesday 19 February and Wednesday 18 March. Red shows a decrease in traffic, green shows an increase. (Cloudfare)

Why Organizations Need DevSecOps Now More Than Ever

DevOps to DevSecOps

It starts with culture

Automation Architect
Software Developer/Tester
Release Manager
UX Professional
DevOps Evangelist
Security Engineer
A
B
C
D
E
F

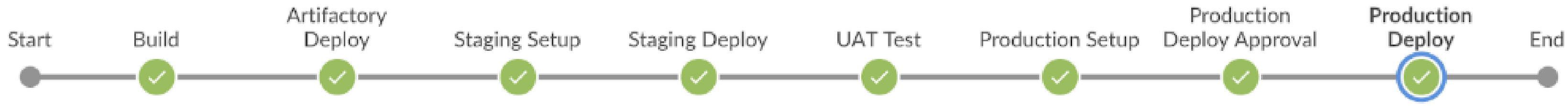
The more integrated and familiar your team is with each other, the less painful and costly communication will be.

Realize the importance of collaboraton

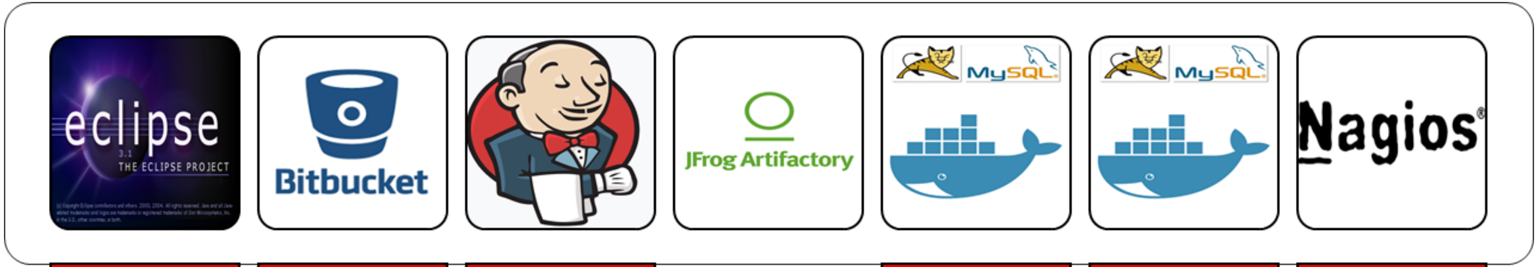
Be transparent and lean

Invest time in innovation

Creating a DevSecOps pipeline



Source: NotSoSecure



Developer

- Pre-commit Hooks
- IDE Plugins
- Linters

Secrets Management

- Token based secret management service

CI/CD Server

- Static Application Security Testing(SAST)
- Software Composition Analysis(SCA)

QA/Staging

- Dynamic Application Security Testing(DAST)
- Vulnerability Management

Production

- Compliance as Code
- Security in IaaC
- Vulnerability Assessment
- Manual Pentesting
- Business Logic Flaws

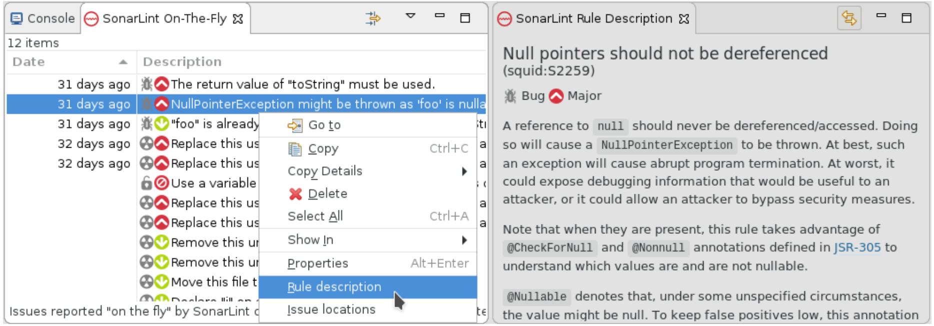
Monitoring

- Alerting and monitor the deployed instance for Vulnerability OWASP Top 10

Source : NotSoSecure

Security plugins in IDE

SonarLint



12 items

Date	Description
31 days ago	The return value of "toString" must be used.
31 days ago	NullPointerException might be thrown as 'foo' is nulla
31 days ago	"foo" is already
32 days ago	Replace this us
32 days ago	Replace this us
	Use a variable
	Replace this us
	Replace this us
	Remove this ur
	Remove this ur
	Move this file t

Issues reported "on the fly" by SonarLint c

Null pointers should not be dereferenced
(squid:S2259)

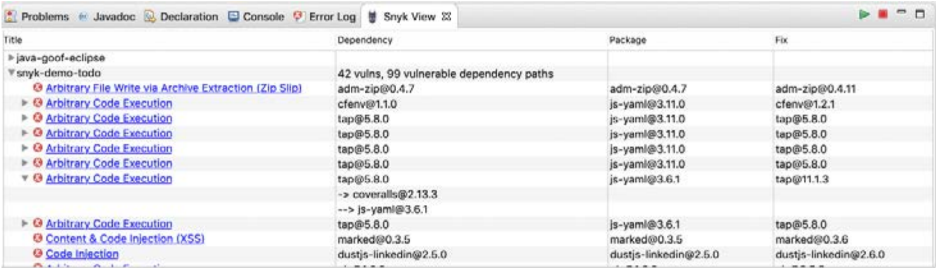
Bug Major

A reference to `null` should never be dereferenced/accessed. Doing so will cause a `NullPointerException` to be thrown. At best, such an exception will cause abrupt program termination. At worst, it could expose debugging information that would be useful to an attacker, or it could allow an attacker to bypass security measures.

Note that when they are present, this rule takes advantage of `@CheckForNull` and `@Nonnull` annotations defined in JSR-305 to understand which values are and are not nullable.

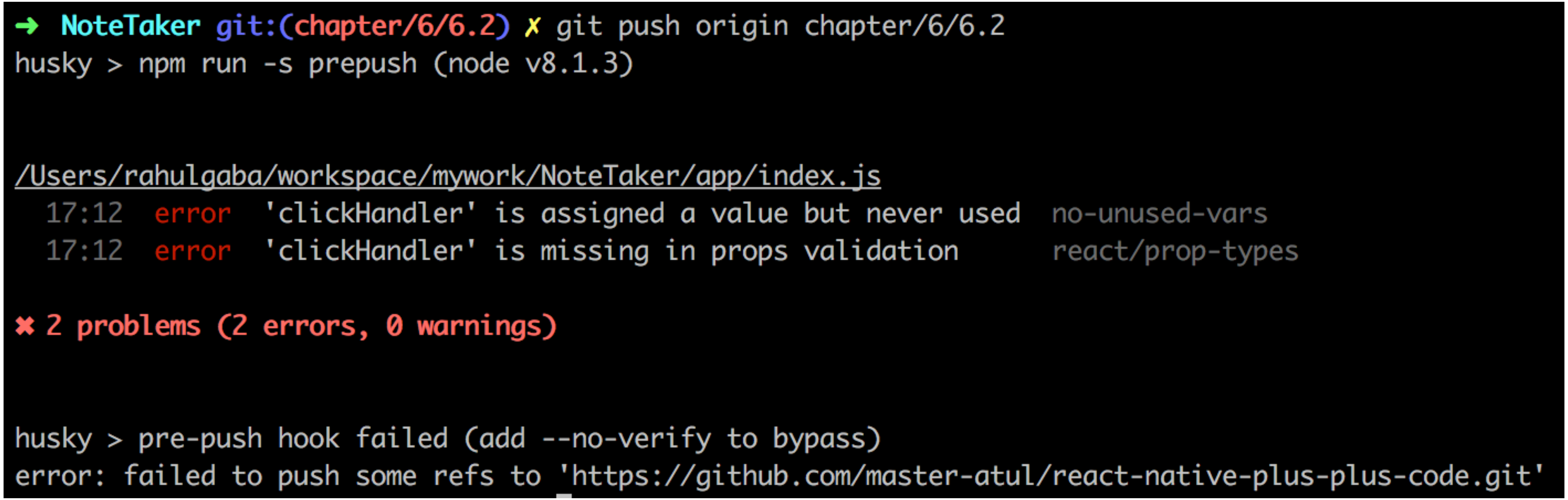
`@Nullable` denotes that, under some unspecified circumstances, the value might be null. To keep false positives low, this annotation

Snyk Vuln Scanner



Title	Dependency	Package	Fix
java-goof-eclipse			
snyk-demo-todo	42 vulns, 99 vulnerable dependency paths		
Arbitrary File Write via Archive Extraction (Zip Slip)	adm-zip@0.4.7	adm-zip@0.4.7	adm-zip@0.4.11
Arbitrary Code Execution	cfenv@1.1.0	js-yaml@3.11.0	cfenv@1.2.1
Arbitrary Code Execution	tap@5.8.0	js-yaml@3.11.0	tap@5.8.0
Arbitrary Code Execution	tap@5.8.0	js-yaml@3.11.0	tap@5.8.0
Arbitrary Code Execution	tap@5.8.0	js-yaml@3.11.0	tap@5.8.0
Arbitrary Code Execution	tap@5.8.0	js-yaml@3.11.0	tap@5.8.0
Arbitrary Code Execution	tap@5.8.0	js-yaml@3.6.1	tap@11.1.3
	-> coveralls@2.13.3		
	--> js-yaml@3.6.1		
Arbitrary Code Execution	tap@5.8.0	js-yaml@3.6.1	tap@5.8.0
Content & Code Injection (XSS)	marked@0.3.5	marked@0.3.5	marked@0.3.6
Code Injection	dustjs-linkedin@2.5.0	dustjs-linkedin@2.5.0	dustjs-linkedin@2.6.0

Pre commit hooks

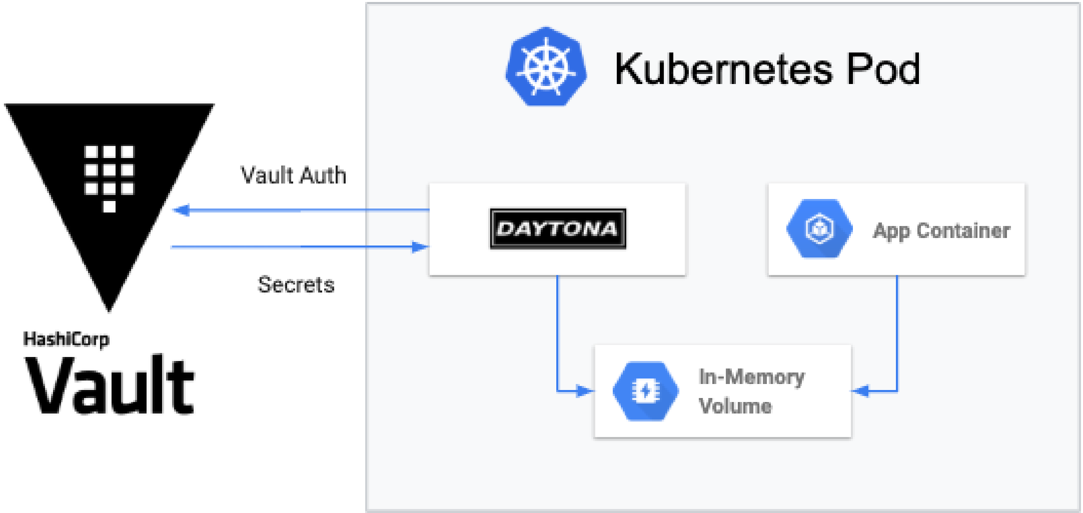


```
➜  NoteTaker git:(chapter/6/6.2) ✗ git push origin chapter/6/6.2
husky > npm run -s prepush (node v8.1.3)


/Users/rahulgaba/workspace/mywork/NoteTaker/app/index.js
  17:12  error  'clickHandler' is assigned a value but never used  no-unused-vars
  17:12  error  'clickHandler' is missing in props validation       react/prop-types

✖ 2 problems (2 errors, 0 warnings)


husky > pre-push hook failed (add --no-verify to bypass)
error: failed to push some refs to 'https://github.com/master-atul/react-native-plus-plus-code.git'
```

Talisman

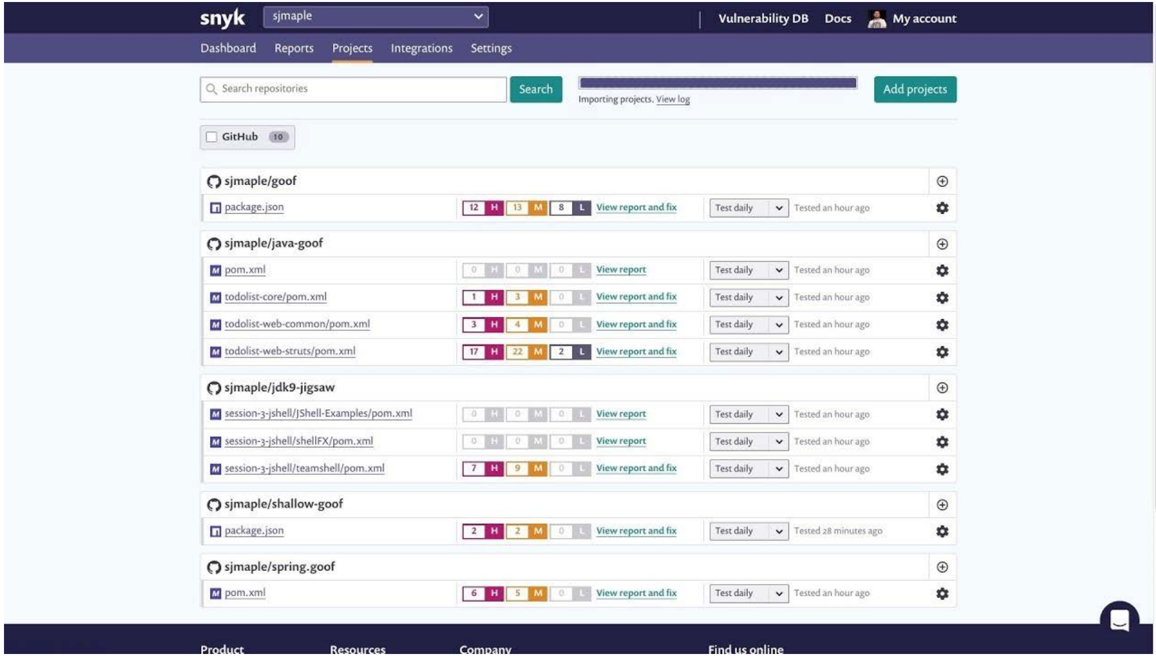
Git hooks

Secrets Management



AWS Secrets manager

Software composition analysis

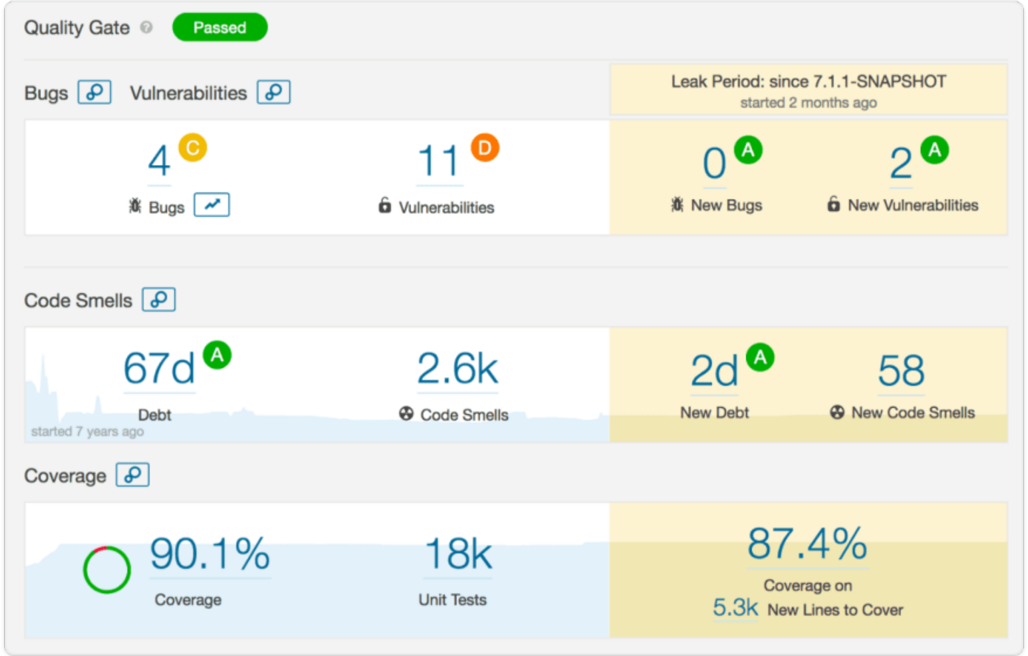


Project	H	M	L	Report	Schedule	Last tested
sjmaple/goof						
package.json	12	13	8	View report and fix	Test daily	Tested an hour ago
sjmaple/java-goof						
pom.xml	0	0	0	View report	Test daily	Tested an hour ago
todolist-core/pom.xml	1	3	0	View report and fix	Test daily	Tested an hour ago
todolist-web-common/pom.xml	3	4	0	View report and fix	Test daily	Tested an hour ago
todolist-web-struts/pom.xml	17	22	2	View report and fix	Test daily	Tested an hour ago
sjmaple/jdk9-jigsaw						
session-3-jshell/JShell-Examples/pom.xml	0	0	0	View report	Test daily	Tested an hour ago
session-3-jshell/shellFX/pom.xml	0	0	0	View report	Test daily	Tested an hour ago
session-3-jshell/teamshell/pom.xml	7	9	0	View report and fix	Test daily	Tested an hour ago
sjmaple/shallow-goof						
package.json	2	2	0	View report and fix	Test daily	Tested 28 minutes ago
sjmaple/spring.goof						
pom.xml	6	5	0	View report and fix	Test daily	Tested an hour ago

Owasp dependency check

Sonatype

Static Analysis



Quality Gate Passed

Bugs Vulnerabilities

Leak Period: since 7.1.1-SNAPSHOT
started 2 months ago

4 C Bugs

11 D Vulnerabilities

0 A New Bugs

2 A New Vulnerabilities

Code Smells

67d A Debt
started 7 years ago

2.6k Code Smells

2d A New Debt

58 New Code Smells

Coverage

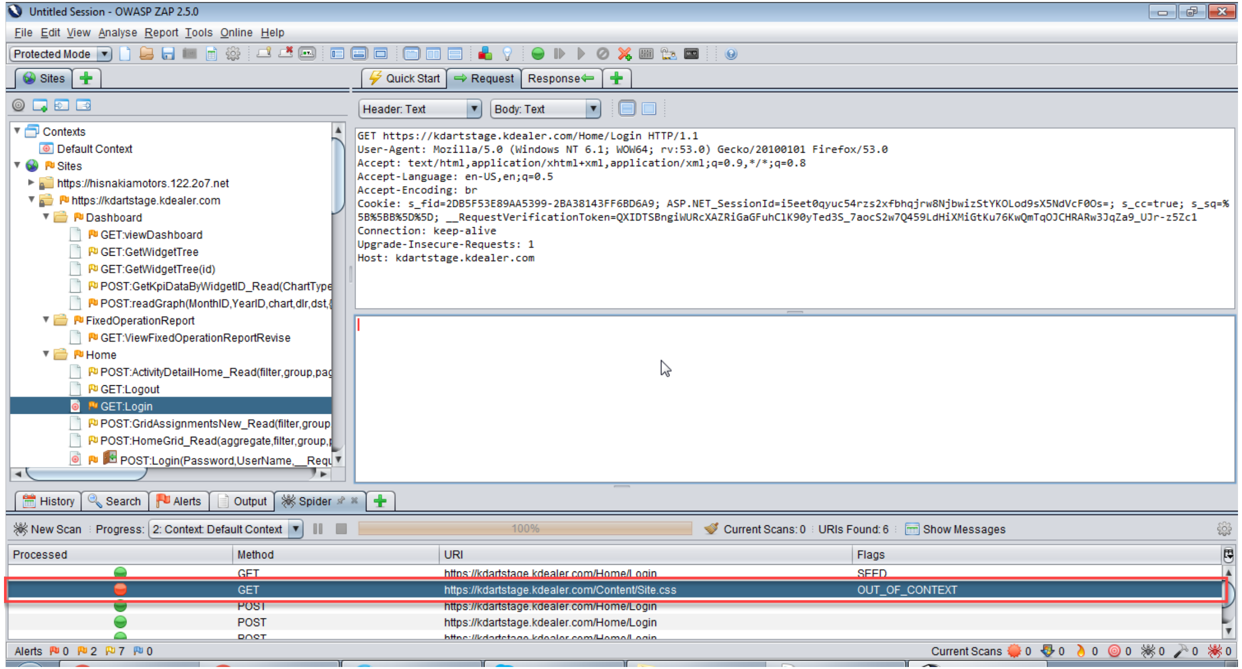
90.1% Coverage

18k Unit Tests

87.4%
Coverage on
5.3k New Lines to Cover

Tools that can be used – SonarQube, Bandit

Dynamic Analysis

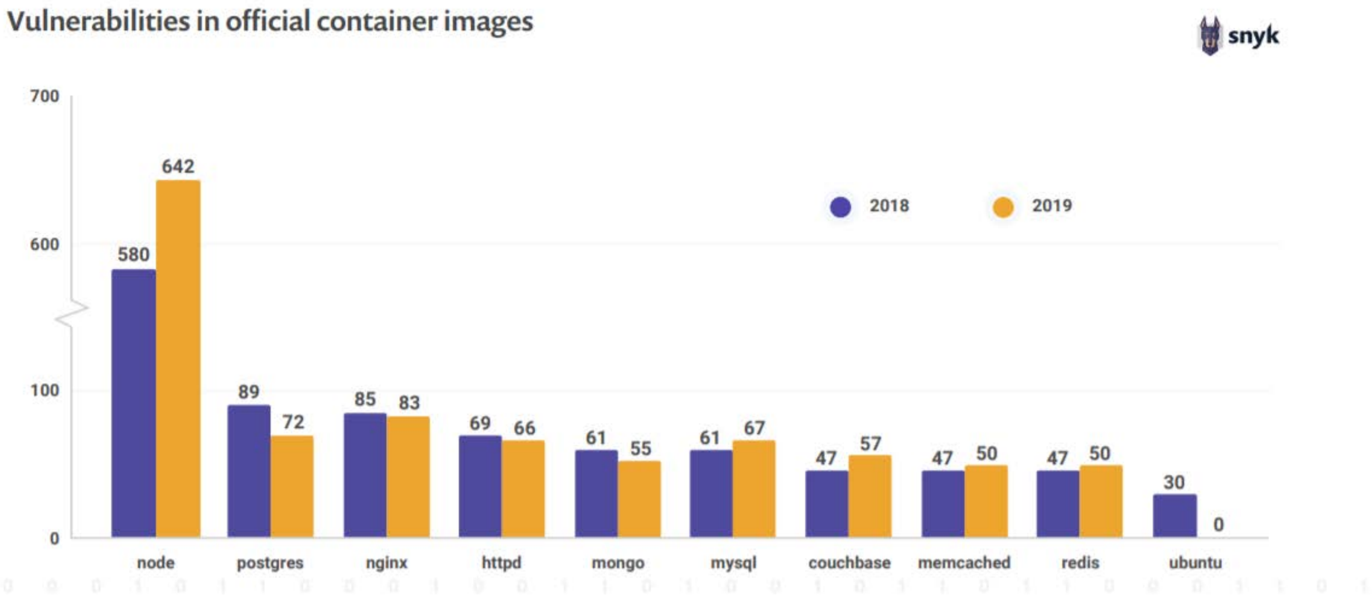

Untitled Session - OWASP ZAP 2.5.0
File Edit View Analyse Report Tools Online Help
Protected Mode
Sites
Quick Start
Request
Response
Header: Text
Body: Text
Contexts
Default Context
Sites
https://hisnakiamotors.122.2o7.net
https://kdartstage.kdealer.com
Dashboard
GET:viewDashboard
GET:GetWidgetTree
GET:GetWidgetTree(id)
POST:GetKpiDataByWidgetID_Read(ChartType
POST:readGraph(MonthID,YearID,chart,dlr,dst,
FixedOperationReport
GET:ViewFixedOperationReportRevise
Home
POST:ActivityDetailHome_Read(filter,group,pag
GET:Logout
GET:Login
POST:GridAssignmentsNew_Read(filter,group
POST:HomeGrid_Read(aggregate,filter,group,
POST:Login(Password,UserName,__Requ
History
Search
Alerts
Output
Spider
New Scan
Progress: 2: Context: Default Context
100%
Current Scans: 0
URIs Found: 6
Show Messages
Alerts 0 2 7 0
Current Scans 0 0 0 0 0 0 0

```
GET https://kdartstage.kdealer.com/Home/Login HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:53.0) Gecko/20100101 Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: br
Cookie: s_fid=2DB5F53E89AA5399-2BA38143FF6BD6A9; ASP.NET_SessionId=i5eet0qyuc54rzs2xfbhqjrw8NjbwizStYKOLod9sX5NdVcF0Os=; s_cc=true; s_sq=%
5B%5BB%5D%5D; __RequestVerificationToken=QXIDTSBngiWURcXAZRiGaGFuhClK90yTed3S_7aocS2w7Q459LdHiXMiGtKu76KwQmTqOJCHRARw3JqZa9_UJr-z5Zc1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: kdartstage.kdealer.com
```

Processed	Method	URI	Flags
●	GET	https://kdartstage.kdealer.com/Home/Login	SEED
●	GET	https://kdartstage.kdealer.com/Content/Site.css	OUT_OF_CONTEXT
●	POST	https://kdartstage.kdealer.com/Home/Login	
●	POST	https://kdartstage.kdealer.com/Home/Login	
●	POST	https://kdartstage.kdealer.com/Home/Login	

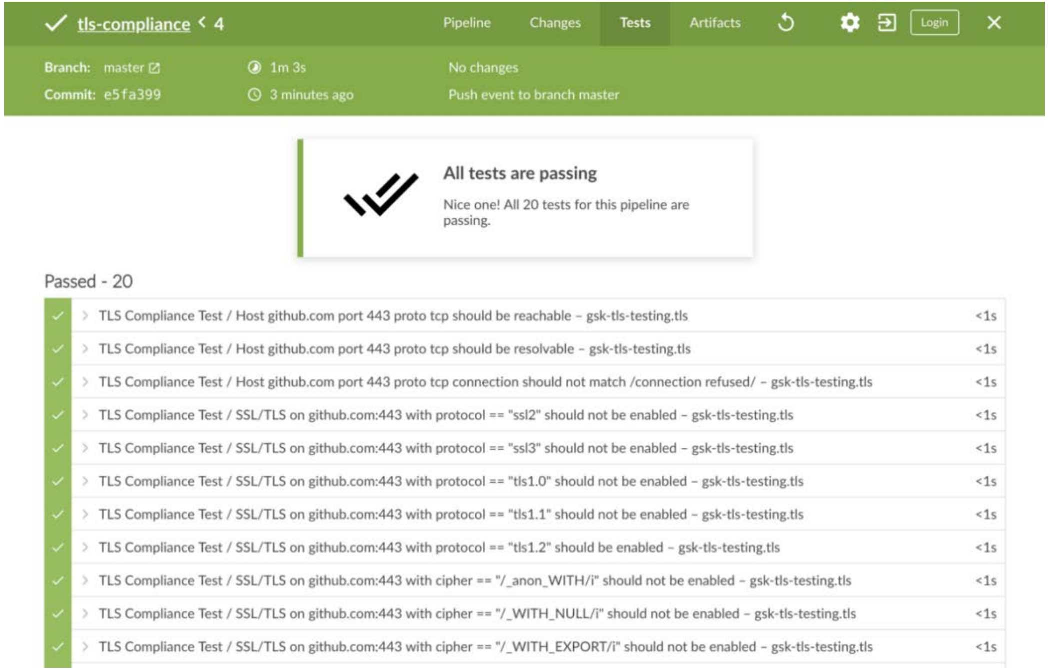
Tools that can be used – OWASP ZAP, Nikto

Embedding security into IaaS



Tools that can be used – Snyk, Docksan

Compliance as Code



Branch: master

Commit: e5fa399

1m 3s

3 minutes ago

No changes

Push event to branch master

All tests are passing

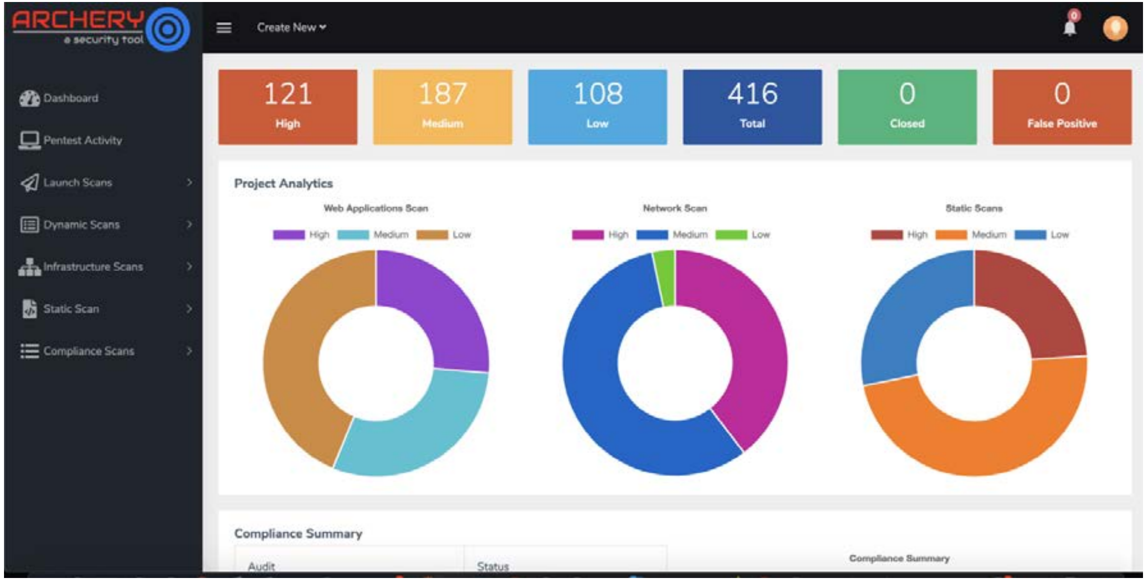
Nice one! All 20 tests for this pipeline are passing.

Passed - 20

✓	TLS Compliance Test / Host github.com port 443 proto tcp should be reachable – gsk-tls-testing.tls	<1s
✓	TLS Compliance Test / Host github.com port 443 proto tcp should be resolvable – gsk-tls-testing.tls	<1s
✓	TLS Compliance Test / Host github.com port 443 proto tcp connection should not match /connection refused/ – gsk-tls-testing.tls	<1s
✓	TLS Compliance Test / SSL/TLS on github.com:443 with protocol == "ssl2" should not be enabled – gsk-tls-testing.tls	<1s
✓	TLS Compliance Test / SSL/TLS on github.com:443 with protocol == "ssl3" should not be enabled – gsk-tls-testing.tls	<1s
✓	TLS Compliance Test / SSL/TLS on github.com:443 with protocol == "tls1.0" should not be enabled – gsk-tls-testing.tls	<1s
✓	TLS Compliance Test / SSL/TLS on github.com:443 with protocol == "tls1.1" should not be enabled – gsk-tls-testing.tls	<1s
✓	TLS Compliance Test / SSL/TLS on github.com:443 with protocol == "tls1.2" should be enabled – gsk-tls-testing.tls	<1s
✓	TLS Compliance Test / SSL/TLS on github.com:443 with cipher == "/_anon_WITH/i" should not be enabled – gsk-tls-testing.tls	<1s
✓	TLS Compliance Test / SSL/TLS on github.com:443 with cipher == "/_WITH_NULL/i" should not be enabled – gsk-tls-testing.tls	<1s
✓	TLS Compliance Test / SSL/TLS on github.com:443 with cipher == "/_WITH_EXPORT/i" should not be enabled – gsk-tls-testing.tls	<1s

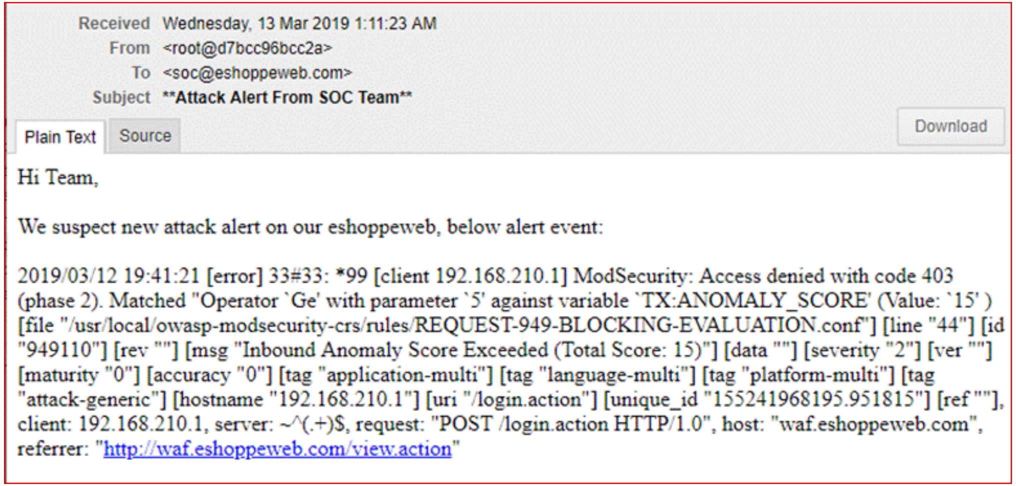
Tools that can be used – Inspec, Kitchen CI

Vulnerability Dashboard



Tools that can be used – ArcherySec, DefectDojo

Alerts and Monitoring



Received Wednesday, 13 Mar 2019 1:11:23 AM
From <root@d7bcc96bcc2a>
To <soc@eshoppeweb.com>
Subject **Attack Alert From SOC Team**

Hi Team,

We suspect new attack alert on our eshoppeweb, below alert event:

```
2019/03/12 19:41:21 [error] 33#33: *99 [client 192.168.210.1] ModSecurity: Access denied with code 403
(phase 2). Matched "Operator `Ge' with parameter `5' against variable `TX:ANOMALY_SCORE' (Value: `15' )
[file "/usr/local/owasp-modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "44"] [id
"949110"] [rev ""] [msg "Inbound Anomaly Score Exceeded (Total Score: 15)"] [data ""] [severity "2"] [ver ""]
[maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag
"attack-generic"] [hostname "192.168.210.1"] [uri "/login.action"] [unique_id "155241968195.951815"] [ref ""],
client: 192.168.210.1, server: ~^(.+)$, request: "POST /login.action HTTP/1.0", host: "waf.eshoppeweb.com",
referrer: "http://waf.eshoppeweb.com/view.action"
```

Modsecurity notification

References

https://www.synopsys.com/blogs/software-security/devsecops-pipeline-checklist/

https://notsosecure.com/achieving-devsecops-with-open-source-tools/

https://www.slideshare.net/notsosecure/devsecops-what-why-and-how-blackhat-2019

https://www.ciodive.com/news/devsecops-security-CIO-infosec/576379/

https://www.technologyreview.com/2020/04/07/998552/why-the-coronavirus-lockdown-is-making-the-internet-better-than-ever/

https://www.crn.com/news/cloud/refactr-ceo-coronavirus-crisis-is-rapidly-accelerating-shift-to-devsecops?itc=refresh

Q and A