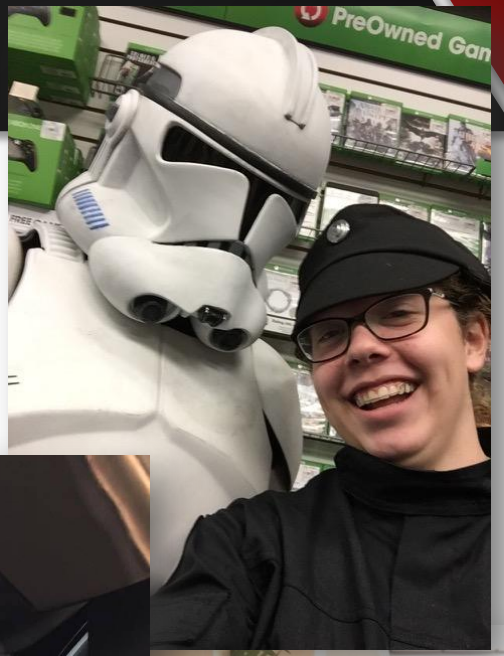
What Could It Hurt?

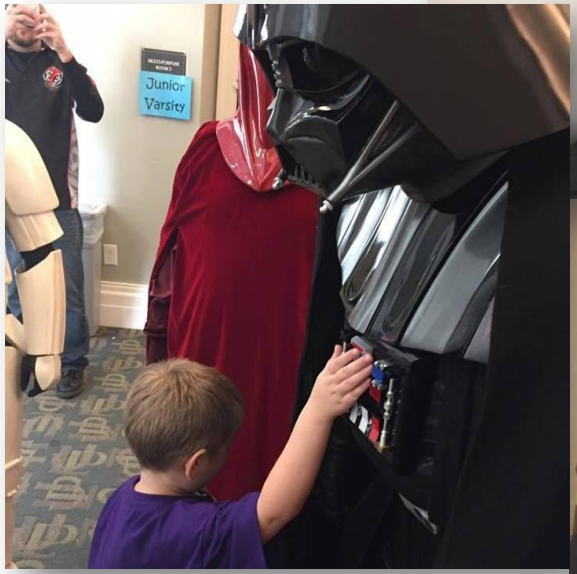
How Framework and Library Dependence is Weakening our Development

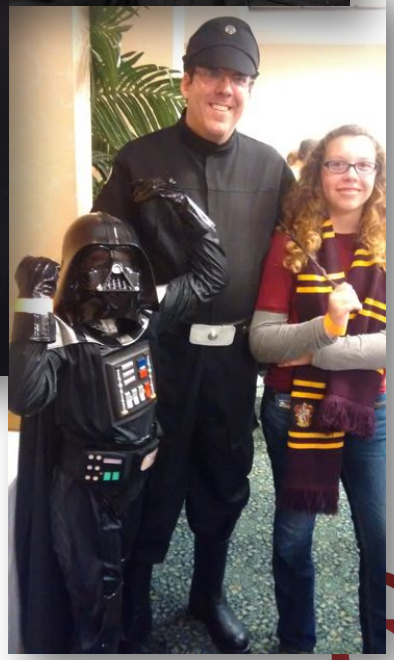
Kevin Johnson
@secureideas
kevin@secureideas.com
866.404.7837 x700

Kevin Johnson

- Founder and CEO of Secure Ideas
- IANS Faculty Member
- Course Author and Instructor
  - Web Application and Mobile Testing
  - PEWAPT 101
  - BlackHat, DerbyCon, OWASP
- Podcaster
  - Professionally Evil Perspective
- Open Source Project Lead
  - SamuraiWTF, Laudanum, Yokoso, WeaponizedFlash, etc.
- 501st Member - TI-42265
- Father, Husband and Christian

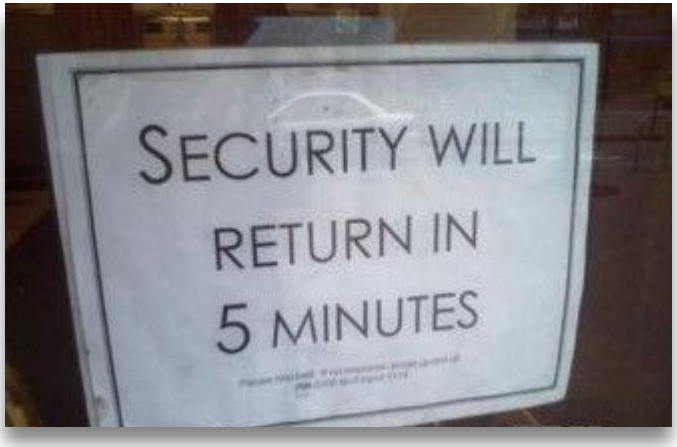




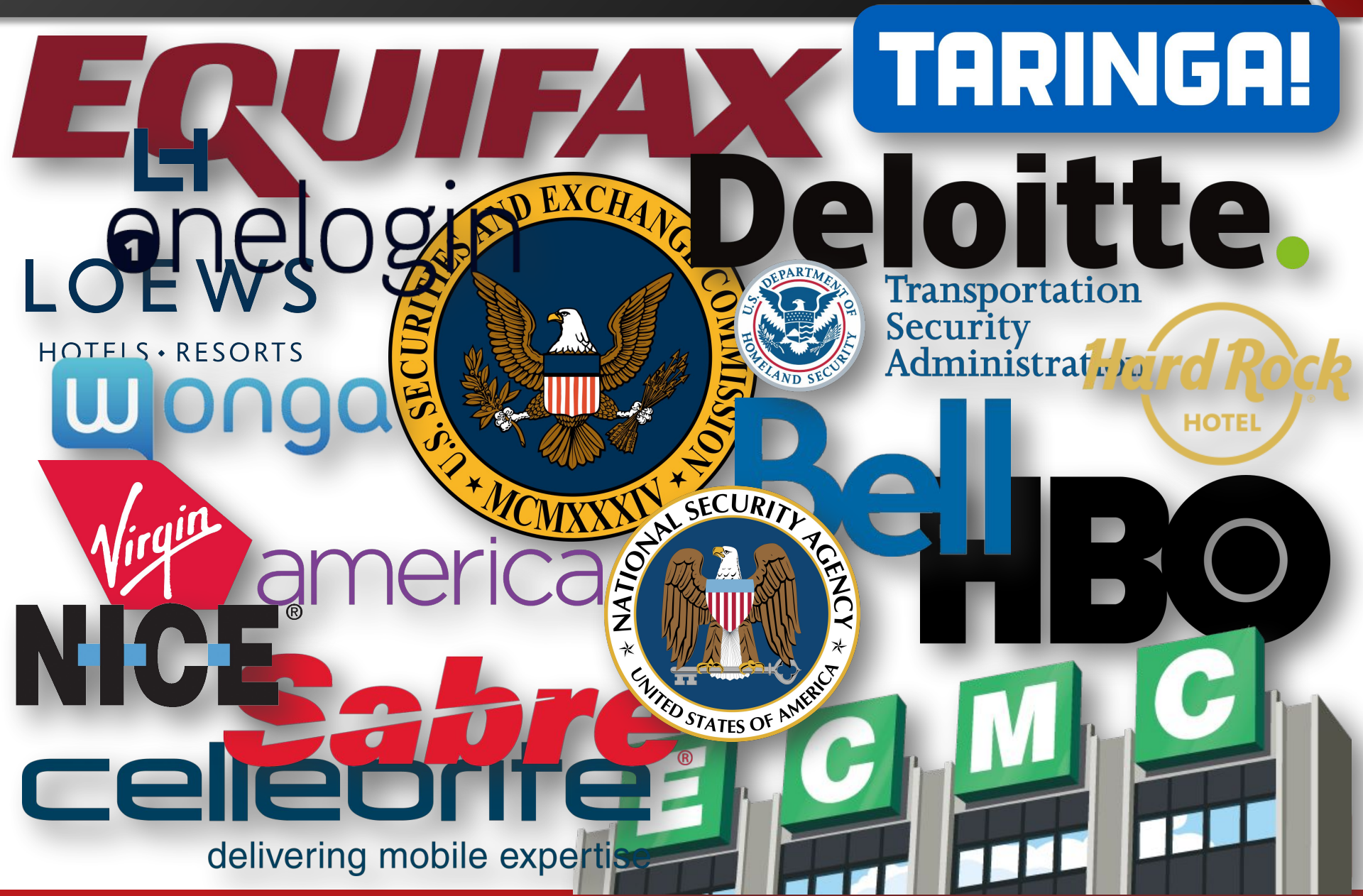


Security..... really?

- Important Topic
  - Or so they say
- I am biased
  - It is my job
- Business critical feature
  - Often ignored



2017 Breaches (Sadly a Sample!)

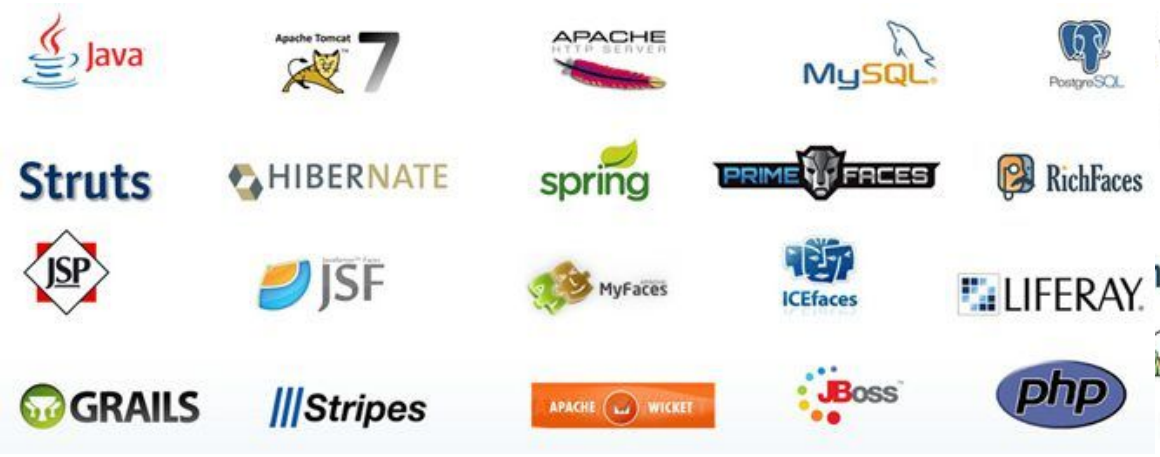


Quick, Good and Cheap…. Pick 2 (Really pick 1)

- Development is seen as easy
  - Microsoft and PluralSight encourage this
- Organizations often don't understand
  - Focus on release cycles
- Security is an afterthought
  - Or a nice-to-have

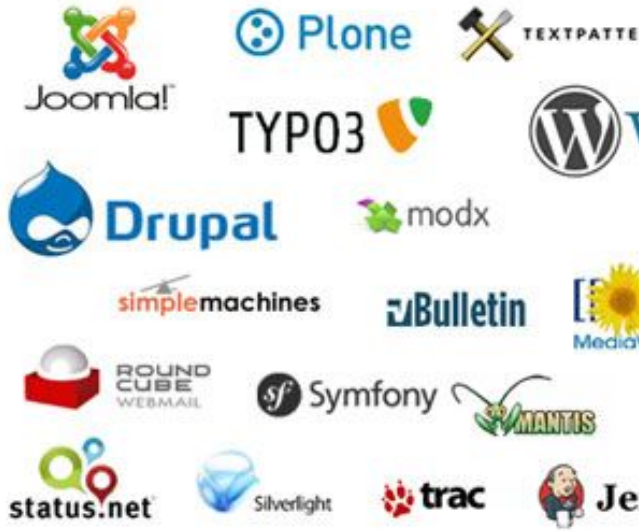
- Even when Devs want it

Frameworks


Java
Apache Tomcat 7
APACHE HTTP SERVER
MySQL
PostgreSQL
Struts
HIBERNATE
spring
PRIMEFACES
RichFaces
JSP
JSF
MyFaces
ICEfaces
LIFERAY
GRAILS
Stripes
APACHE WICKET
JBoss
php

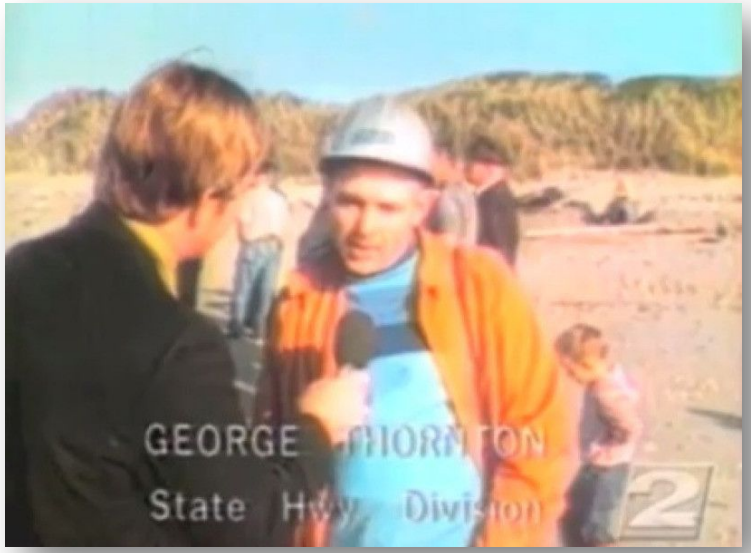

TEXTPATTERN
MOVABLE TYPE
osCommerce
PRESTASHOP
WORDPRESS
OXID esales
Magento
zikula
RAILS
MediaWiki
phpBB
SPIP
ZEND FRAMEWORK
MANTIS
sonar
Jenkins
Code Igniter
django
Java
php


JAVA
eclipse
web service
SWING!
JSP
EJB 3
JavaFx
spring
HIBERNATE
LOG4J
JDBC
PRIMEFACES
jQuery
JUnit
Struts 2
Apache Tomcat
XML
Java Servlets
Java EE
maven
{JSON}


Joomla!
Plone
TEXTPATTE
TYPO3
Drupal
modx
simplemachines
vBulletin
ROUND CUBE WEBMAIL
Symfony
MANTIS
status.net
Silverlight
trac
Je

Efficiences

- Development is easier
  - Heavy lifting is done
- Better support across teams
  - Publicly available frameworks
- Much of the security needs are handled
  - SQLi prevention
  - CSRF tokens
  - XSS encodings
  - Open Redirect validations



Security Fails

- Django
  - XSS
  - Open Redirects
  - HardCoded Password (2016)
- Struts
  - Deserialization Flaw
  - Command Execution
  - CSRF
- Ruby-on-Rails
  - SQLi (Sorta… ActiveRecord Injection)
- JQuery
  - Lots!
  - Migrate library reintroduces flaws!

What Could It Hurt?

How Framework and Library Dependence is Weakening our Development

Kevin Johnson
@secureideas
kevin@secureideas.com
866.404.7837 x700