Integrating Vulnerability Scanning into the SDLC

Eric Johnson

JavaOne Conference

10/26/2015

Eric Johnson (@emjohn20)

- Senior Security Consultant
- Certified SANS Instructor
- Certifications
  - CISSP, GWAPT, GSSP-Java, GSSP-.NET
- Contact Info
  - eric.johnson@cypressdefense.com

Agenda

- Case Study
- Secure Development Lifecycle
- Continuous Integration
- Continuous Delivery
- Demo
- Questions

Case Study #1

- Company A provides a video sharing service
- Over 1 billion users per month

Case Study #1

- Client-side AJAX request
- Web service endpoint deletes any event with a valid session token:

```
POST https://companyA.com/live_events_edit_status_ajax?
action_delete_live_event=1

event_id: ANY_EVENT_ID
session_token: SESSION_TOKEN
```

Case Study #1

- YouTube
- Bug bounty program paid $5,000

"I fought the urge to clean up Justin Bieber's channel" - Kamil Hismatullin

Case Study #2

- Company B
- Social media web site with over 380 million users

Case Study #2

- Company B has a request vulnerable to SQL injection
- Example request:

```
POST https://companyB.com/search

searchTerm=' OR 1=1; UPDATE Users SET IsAdmin = 1 WHERE
UserName = 'Milton'; --
```

Case Study #2

- An automated SQL injection tool (sqlmap) is used to extract the database
- User table contains 6.5 million password hashes
- Investigation reveals SHA1 hashes are unsalted

Case Study #2

- LinkedIn
- 4 million SHA1 hashes reversed

"The enhanced security we just recently put in place…includes hashing and salting of our current password databases.

We sincerely apologize for the inconvenience this has caused our members." – Vincent Silveira, LinkedIn

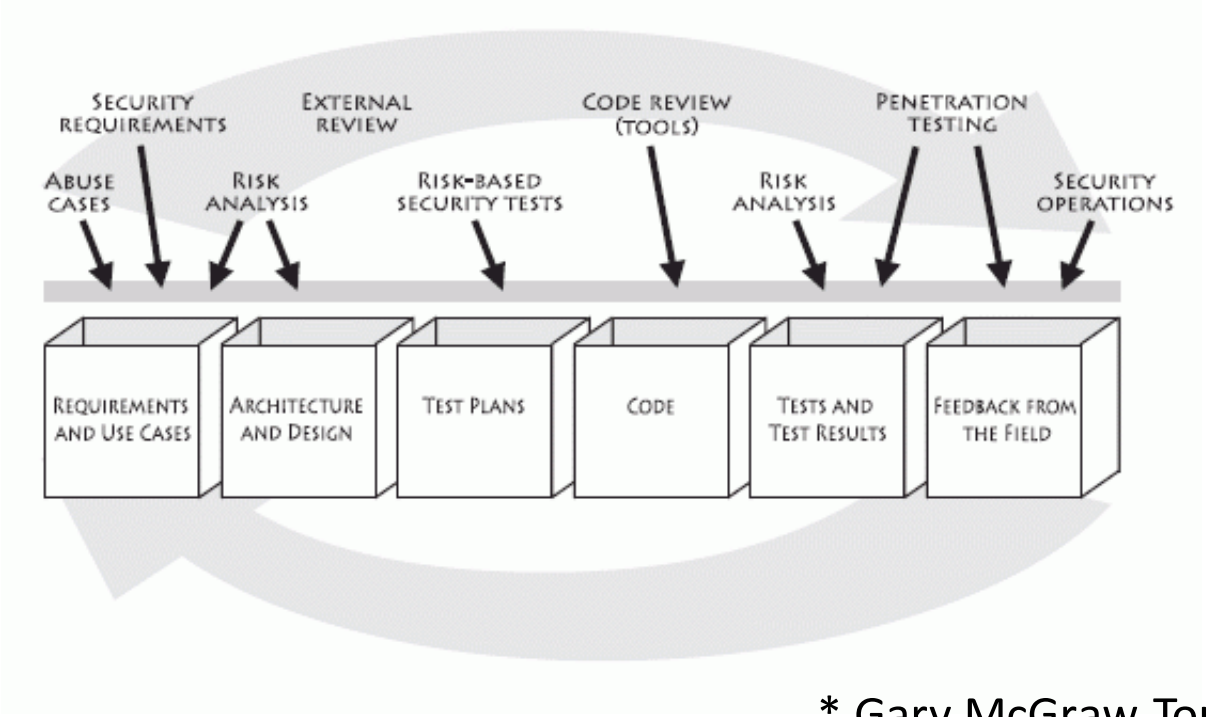
And the list goes on…..

The Root Cause

- Silos / politics between enterprise groups
- Leaving security until the very end
- Legacy applications
- Fear of breaking production code
- Slow deployment cycles leave vulnerability windows open

Securing the Development Lifecycle

- Security is baked into all phases of development



* Gary McGraw Touchpoint Model

Meet Your Security Team

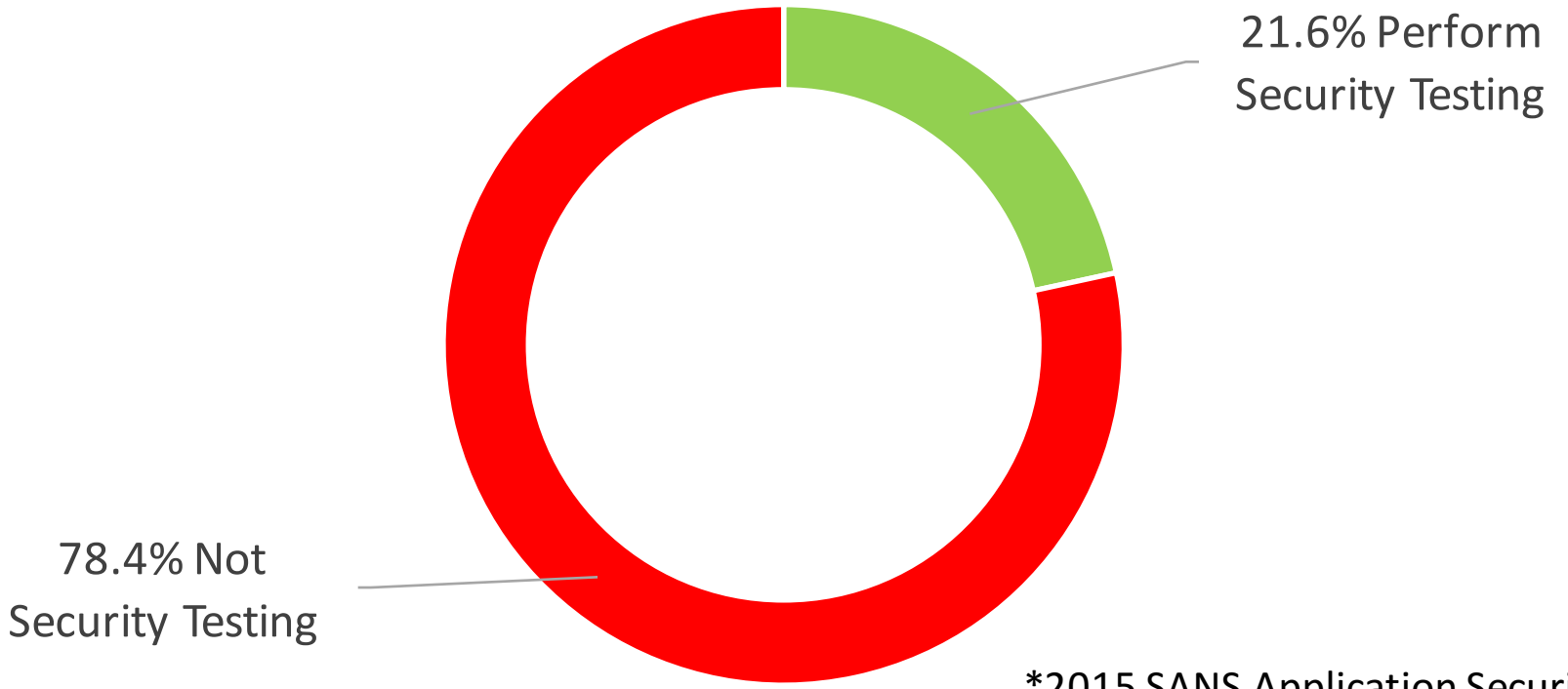
- Security is everyone's job:
  - Developers
  - Quality Assurance
  - Operations
  - Security Team
  - Management
  - C-Level Executives

Iteration Zero

- Assign a security expert to the project team
- Define the security requirements
- Privacy assessment
- Attack surface analysis
- Threat modeling

Security Testing in Development

- Percentage of development teams performing security testing:



*2015 SANS Application Security Survey

The Sprint

- Agile & DevOps move too fast for traditional security processes
- Security must adapt using incremental / automated testing
  - Continuous Integration
  - Continuous Delivery

Continuous Integration

- Check-in triggers automated tests
- Provides fast feedback to developers (minutes)
- Security has a limited role:
  - Security-specific unit testing
    - Authentication, user management, password, access control, validation
  - Developer driven static / dynamic analysis
    - Dangerous function calls, OWASP Top 10
    - Rules sets must produce very few false positives

Continuous Integration Tools

- Jenkins Static Analysis Plugins
  - Find Security Bugs, Checkstlye, OWASP Dependency Check
- Find Security Bugs
- Eclipse Security Testing Plug-in

Find Security Bugs

- Written by Philippe Arteau (@h3xstream)
- FindBugs plug-in with 67 security-specific rules
  - OWASP TOP 10, SANS CWE Top 25
  - http://h3xstream.github.io/find-sec-bugs/
- WebGoat Scan
  - 15 security issues found out of the box
  - 101 security issues found with FSB installed

Eclipse Security Testing Plug-in

- Written by Gregory Leonard (@appsecgreg)
  - [CON5653] Managing 3rd Party Security Risks
  - Wednesday @ 3:00 PM
- Integrates dynamic scanning into the IDE
- Currently supports:
  - ZED Attack Proxy (ZAP) spider and active scan

Continuous Delivery

- Code changes are pushed into the automated deployment pipeline (test, staging, prod)
- Required security checkpoints:
  - Automated dynamic testing
  - Deep static analysis
- Pass / fail criteria determine if the build fails

Continuous Delivery Frameworks

- Security-specific testing:
  - Yahoo Gryffin
    - https://github.com/yahoo/gryffin
    - http://bit.ly/1LQqlGj
  - Mozilla Minion
    - https://wiki.mozilla.org/Security/Projects/Minion
  - Gauntlt
    - http://gauntlt.org/

The Sprint Retrospective

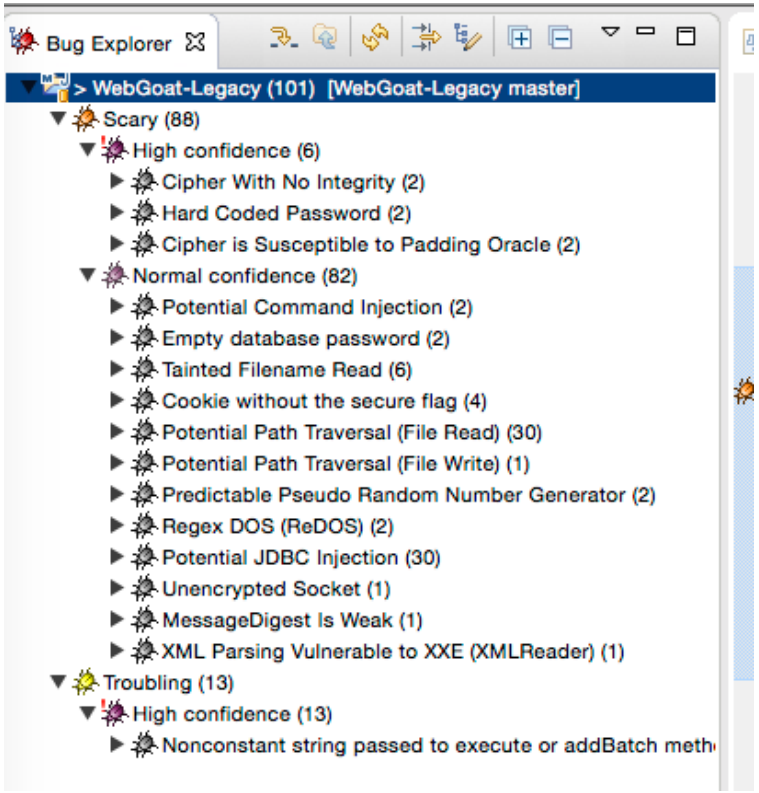
- Security issues
  - # of security issues identified vs. # remediated?
- Schedule external assessments
  - Security-specific source code reviews
  - Penetration testing
- Feed security issues to the backlog / defect tracking systems
- If needed, scheduled a hardening sprint

The Benefits

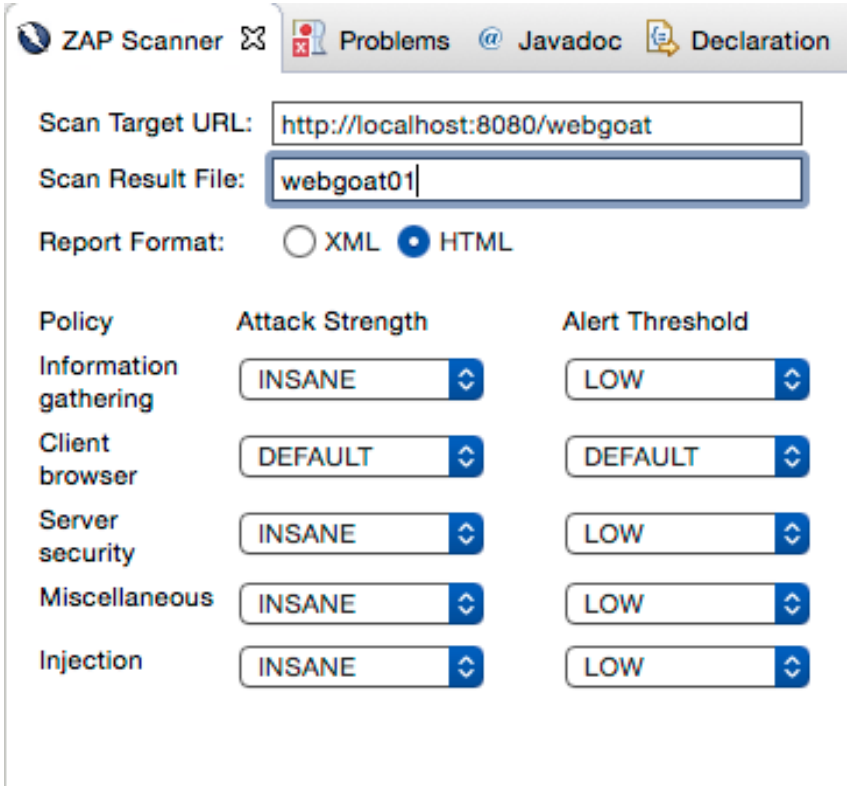
- Scans occurs as code is written
- Consistent and repeatable process
- Incremental security testing
- Release more secure code to production

Demo! Demo! Demo!

Find Security Bugs



Eclipse Security Testing



Eclipse Dynamic Security Testing

- Future enhancements:
  - Add to Eclipse Marketplace
  - Additional IDE / build support
    - Visual Studio, Maven, Ant, TFS
  - Provide additional scanner support
    - Burp Suite, w3af, Arachni
- Limitations
  - ZAP REST API (session state not enabled)

SANS AppSec

APPLICATION & SOFTWARE SECURITY

Website

http://software-security.sans.org

Free resources, white papers, webcasts, and more

Blog

http://software-security.sans.org/blog

Twitter

@sansappsec

Latest news, promos, and other information

Secure Coding Assessment

http://software-security.sans.org/courses/assessment

SANS AppSec CURRICULUM

Core

STH.DEVELOPER
Application Security Awareness Modules
CBT

DEV522
Defending Web Applications Security Essentials
GWEB

Secure Coding

DEV541
Secure Coding in Java/JEE
GSSP-JAVA

DEV544
Secure Coding in .NET
GSSP-.NET

DEV543
Secure Coding in C/C++

Specialization

SEC542
Web App Penetration Testing and Ethical Hacking
GWAPT

SEC642
Advanced Web App Penetration Testing and Ethical Hacking

Thanks for attending!

- Questions?
- Contact Info
  - Twitter: @emjohn20
  - Email: eric.johnson@cypressdefense.com