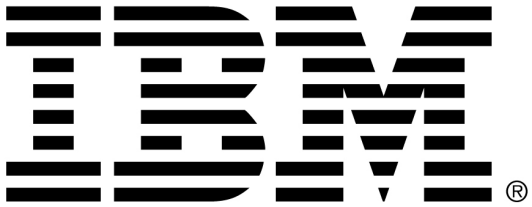
Security Workshops

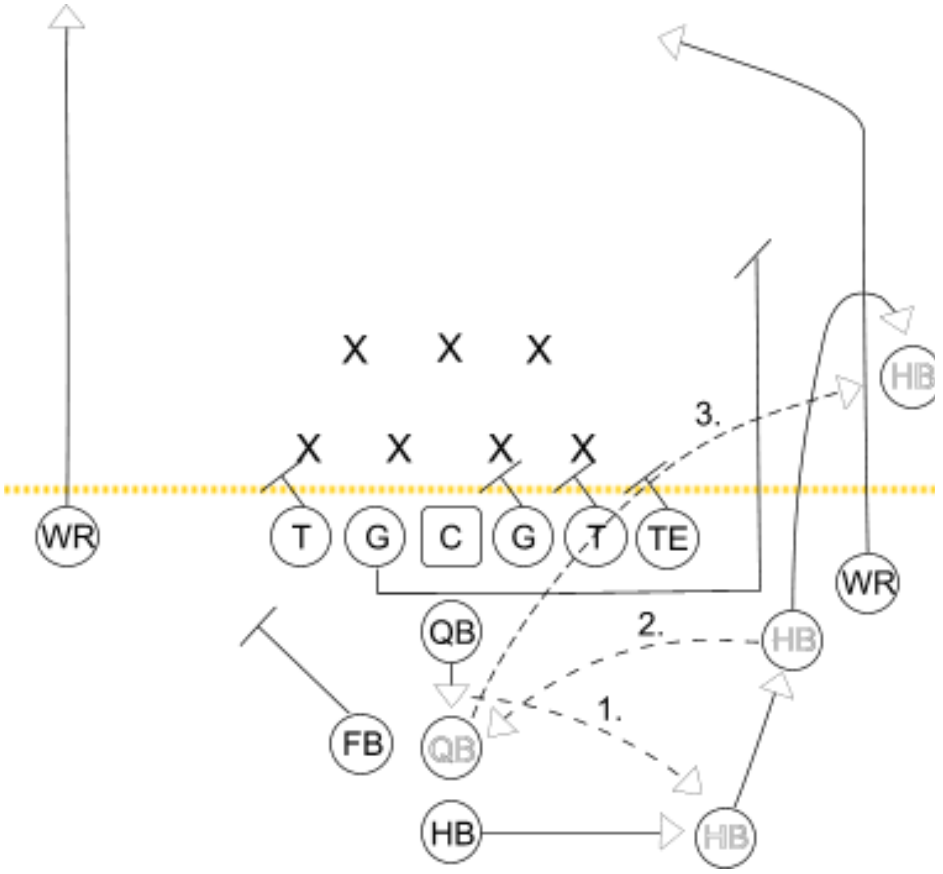


Application Security Management – A Proactive, Risk-based Approach

David Tyrrell, IBM
Paco Hope, Cigital
29/04/14

Four Plays

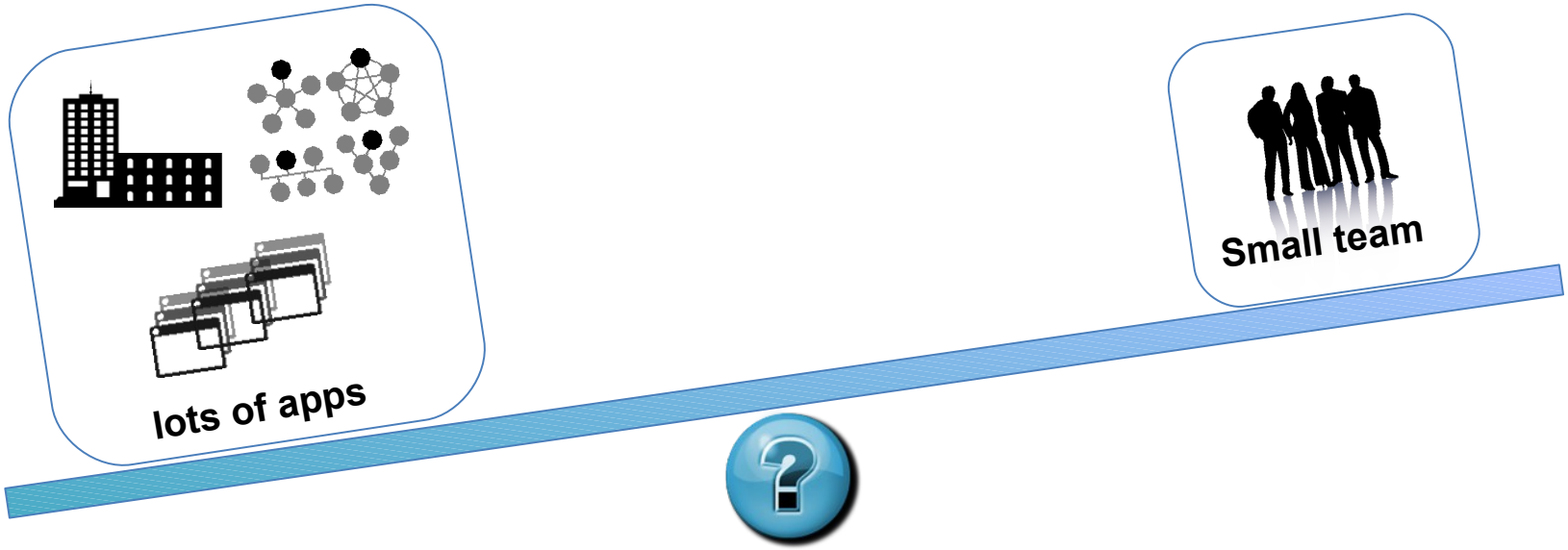
1. Architecture
2. Code Review
3. Security Testing
   (not penetration testing)
4. Training



Picking Plays

(What are we up against?)

Us Versus Them



Us Versus Them

Strategy and Category

List Application Assets

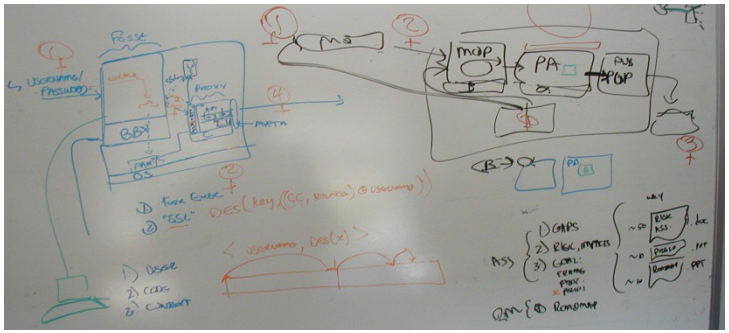
Evaluate Application Risk

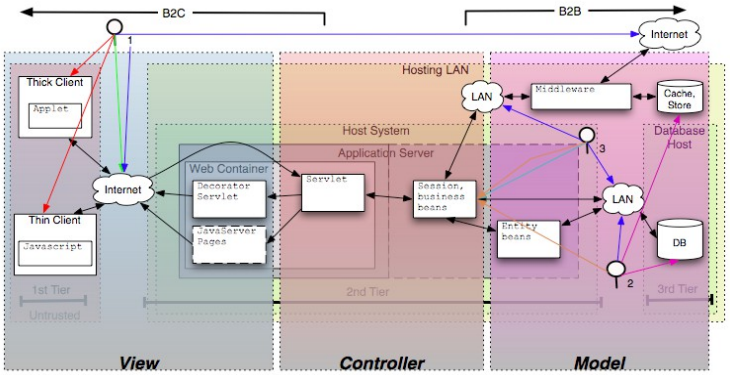
Rank Applications

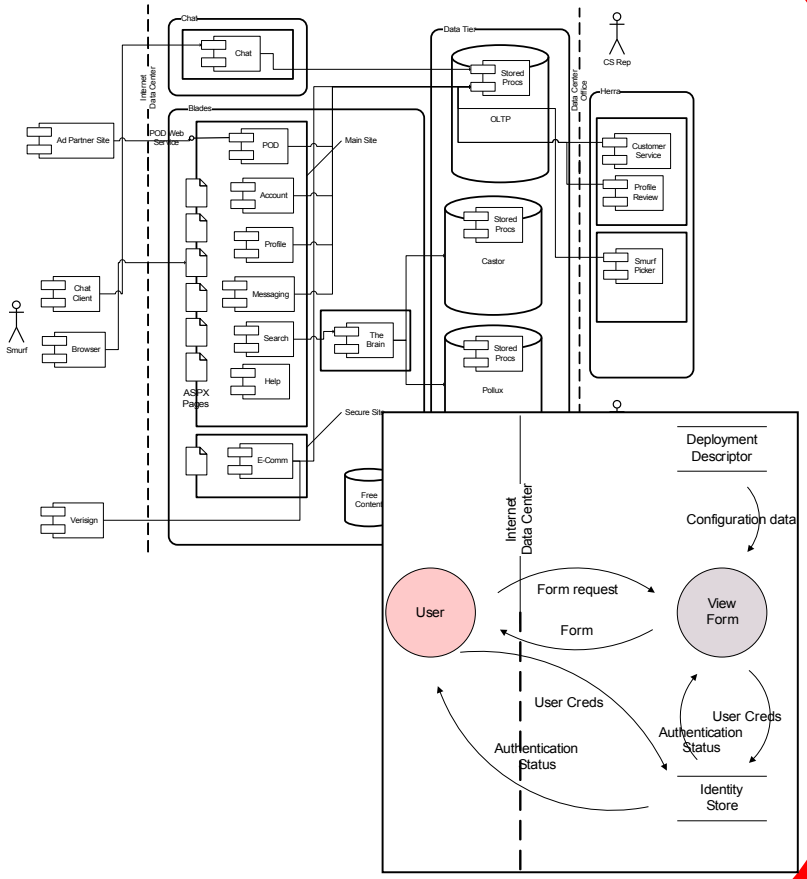
LOW	MEDIUM	HIGH	CRITICAL
· Pre Prod Scan · Annual Prod Test	· Code Scan on builds · Pre Prod Scan · Manual Pen test · Annual Prod Test	· Dev Code Scanning · Code Scan on Builds · QA Dynamic Scan · Pre Prod Scan · Manual Pen test · Bi-Annual Prod Test	· Dev Code Scanning · Code Scan on Builds · QA Dynamic Scan · Pre Prod Scan · Manual Pen test · External Security Test · Quarterly Prod Test

Architecture

Architecture







Two Broad Classes of Security Defects

Bugs

- SQL Injection
- Cross-site scripting
- Input validation problems
- Buffer overflow
- Session problems

Flaws

- Misuse of cryptography
- CSRF
- Failing to authenticate
- Coarse authorisation schemes
- Omitting validation

Architecture

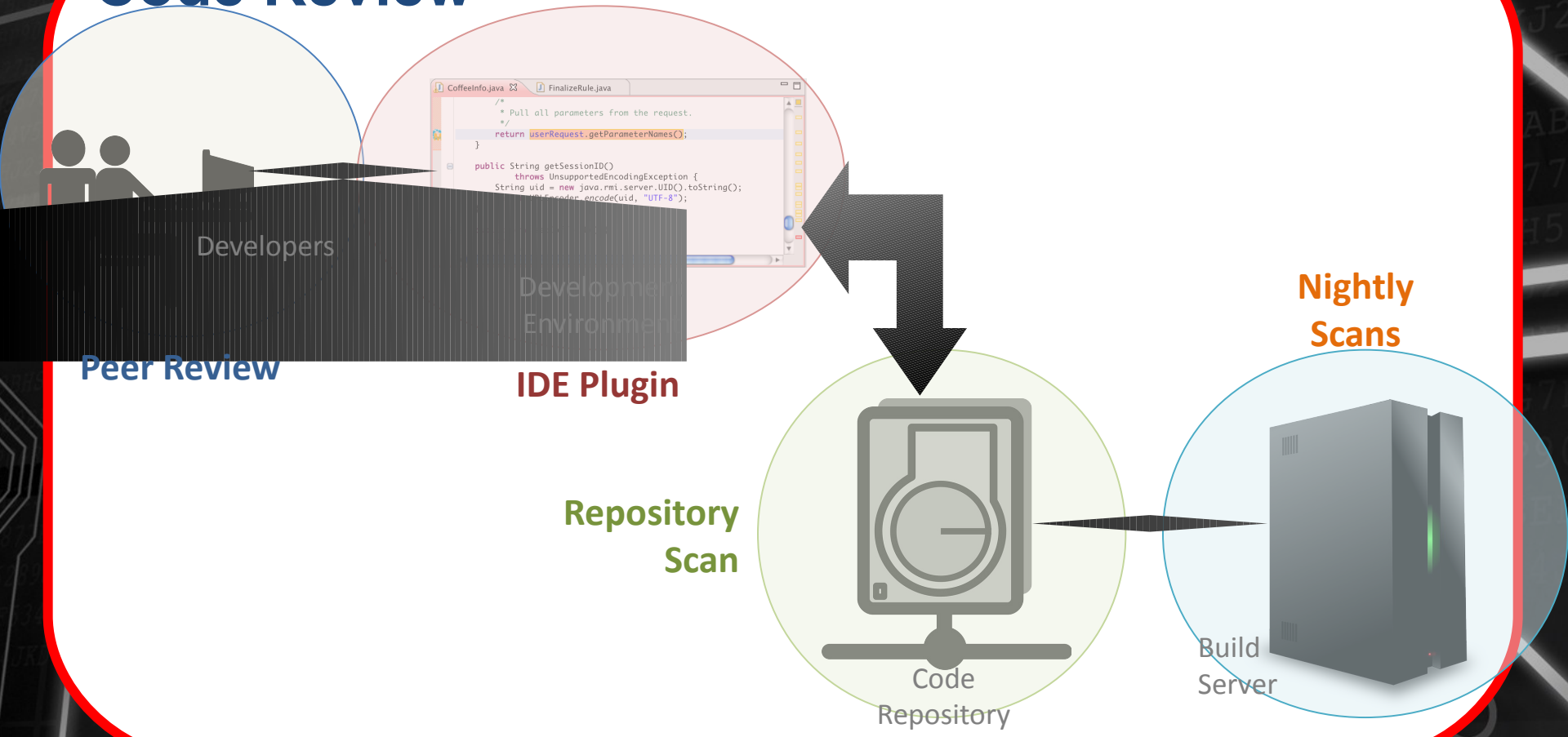
	Bugs	Flaws
Find	• IDE Tools • Code scanning • Peer review • Compiler tools	• Architecture review • Design review
Fix	• Change the code • Use a 3rd party library	1. Change the design 2. Reimplement new code

Architecture Risk Analysis

- Attack Resistance Analysis
  - What do apps like ours usually deal with?
  - How are we dealing with that?
- Underlying Framework Analysis
  - What are we using? Is it vulnerable?
  - How do we handle vulnerabilities in components?
- Ambiguity Analysis
  - Are all interfaces clearly specified?
  - What are we counting on upstream / downstream?
- **Threat Modeling**

Code Review - The Other 50%

Code Review


Developers
Peer Review
IDE Plugin
Repository
Scan
Code
Repository
Nightly
Scans
Build
Server

IBM Security AppScan

Application Security Management

Inventory assets

Assess business impact

Prioritize vulnerabilities

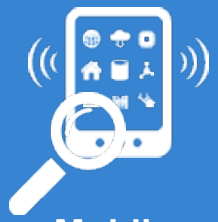
Measure status & progress

Determine compliance

Dynamic Analysis

Static Analysis

Interactive Analysis



Mobile Application Analysis

Company logo

IBM Security AppScan

Application Security Management


Inventory assets


Assess business impact


Prioritize vulnerabilities


Measure status & progress


Determine compliance

AppScan Enterprise Server

- Compile an inventory of your application assets
- Prioritize assets by business impact
- Prioritize vulnerabilities in application context
- Obtain application security status & progress metrics
- View more than 40 compliance reports

Company logo

IBM Security AppScan

Application Security Management

AppScan Standard

- Perform automated dynamic analysis pen testing
- Configure custom dynamic analysis tests
- Test web services

AppScan Enterprise Dynamic Analysis Scanner

- Scale dynamic analysis testing
- Assign test policies and scan templates to security testers
- Schedule and manage multiple scans

IBM Security AppScan

Application Security Management

AppScan Source

- Stronger and more cost-effective software security through source code analysis
- Address security early in SDLC through integration with existing development tools and build frameworks
- Security best practices through centralized management and enforcement of security policies
- Reporting, governance and compliance capabilities that facilitate communication of security status and issues

IBM Security AppScan

Application Security Management

AppScan Standard and AppScan Enterprise Dynamic Analysis Scanner

- Increased scanning accuracy for .NET and Java applications
- Vulnerability detection using runtime analysis
- Detects non-reflected vulnerabilities, such as: command injection, SQLi and path traversal
- Monitors sensitive “sink” calls during each Glass box test
- Results include rich SAST-like information:
  - Vulnerable line of code
  - Vulnerable file name , class, library method (sink)
  - A runtime “snapshot” of the vulnerable code with actual HTTP data

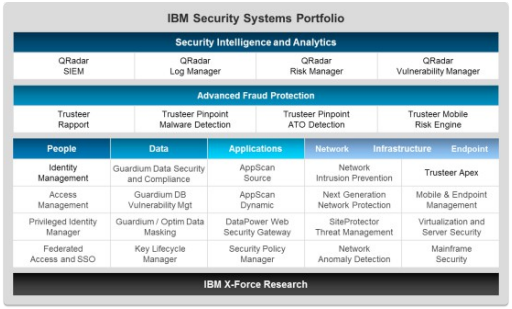
IBM Security AppScan

Application Security Management

AppScan Source for Mobile

- Comprehensive scanning of Native and Hybrid mobile applications
- Security research & risk assessment of over 40k iOS & Android APIs
  - Full call and data flow analysis of
- Objective-C
- JavaScript
- Java
- IBM Worklight integration – a single unified IDE
  - HTML5 / Cordova / JQuery Mobile support
  - Quickly identify where sensitive data are being leaked

IBM Security AppScan



Broad and deep coverage across all security domains

Worldwide research, development, and security experts

X-FORCE

Award-winning global threat research

Intelligence. Integration. Expertise.

Company logo

Testing

Testing

Functional Testers

- Your advocate
- Full, systematic coverage of all user journeys
- Relatively complete test data
- Reasonable domain knowledge
- Lots of time

Penetration Testers

- Independent
- Risk-based coverage of a fraction of possible journeys
- Typically incomplete test data
- Minimal domain knowledge
- Time budgeted

3 Steps to Making the Most of Security Testing

1. Capture test data from penetration tests
   - Give to regression testers
   - Duplicate their results
   - Test every subsequent release
2. Track Defects
   - Use the same defect tracker the devs use
3. Pinpoint training needs based on security results
   - Advanced framework features
   - Cryptography
   - Defensive Programming

Training

Typical Training Programme

- Matrix
  - by role
  - by depth
- Some people need depth
- Everyone needs something

- Instructor-led to bootstrap a core
- Computer-based for refreshers and/or partners
- Track who takes what
- Track which teams have trained people

Example Curricula

Company logo

Wrap-Up

- Inventory and Categorise
- Pick plays based on risk
- Remember bugs versus flaws: cover both!

LOW

- Pre Prod Scan
- Annual Prod Test

MEDIUM

- Code Scan on builds
- Pre Prod Scan
- Manual Pen test
- Annual Prod Test

HIGH

- Dev Code Scanning
- Code Scan on Builds
- QA Dynamic Scan
- Pre Prod Scan
- Manual Pen test
- Bi-Annual Prod Test

CRITICAL

- Dev Code Scanning
- Code Scan on Builds
- QA Dynamic Scan
- Pre Prod Scan
- Manual Pen test
- External Security Test
- Quarterly Prod Test