Why appsec tools suck

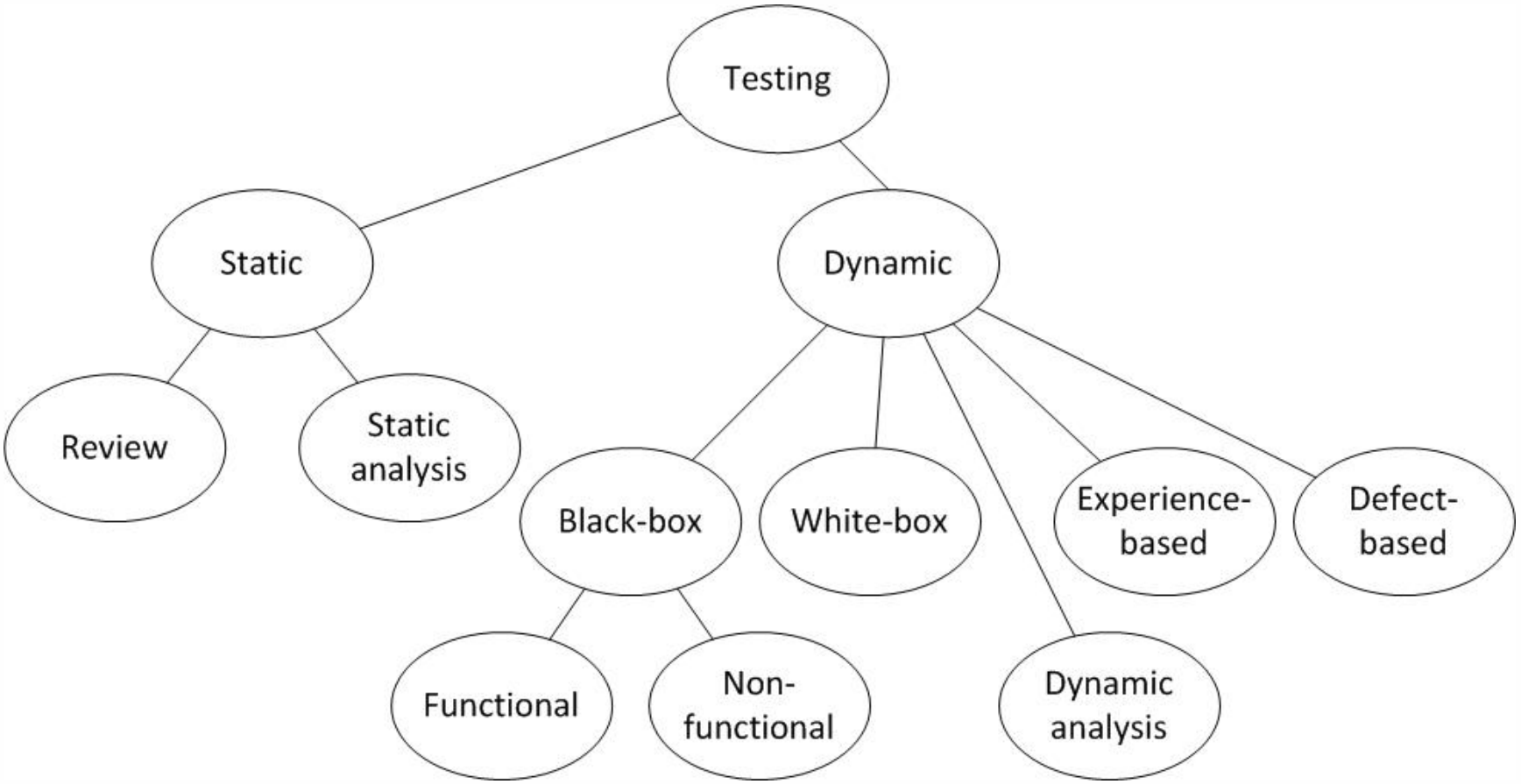
TOORCAMP 2009

My story

Andre Gironda

- Interest in appsec tools
- Write for tssci-security.com
- Involved with OWASP

How I view appsec



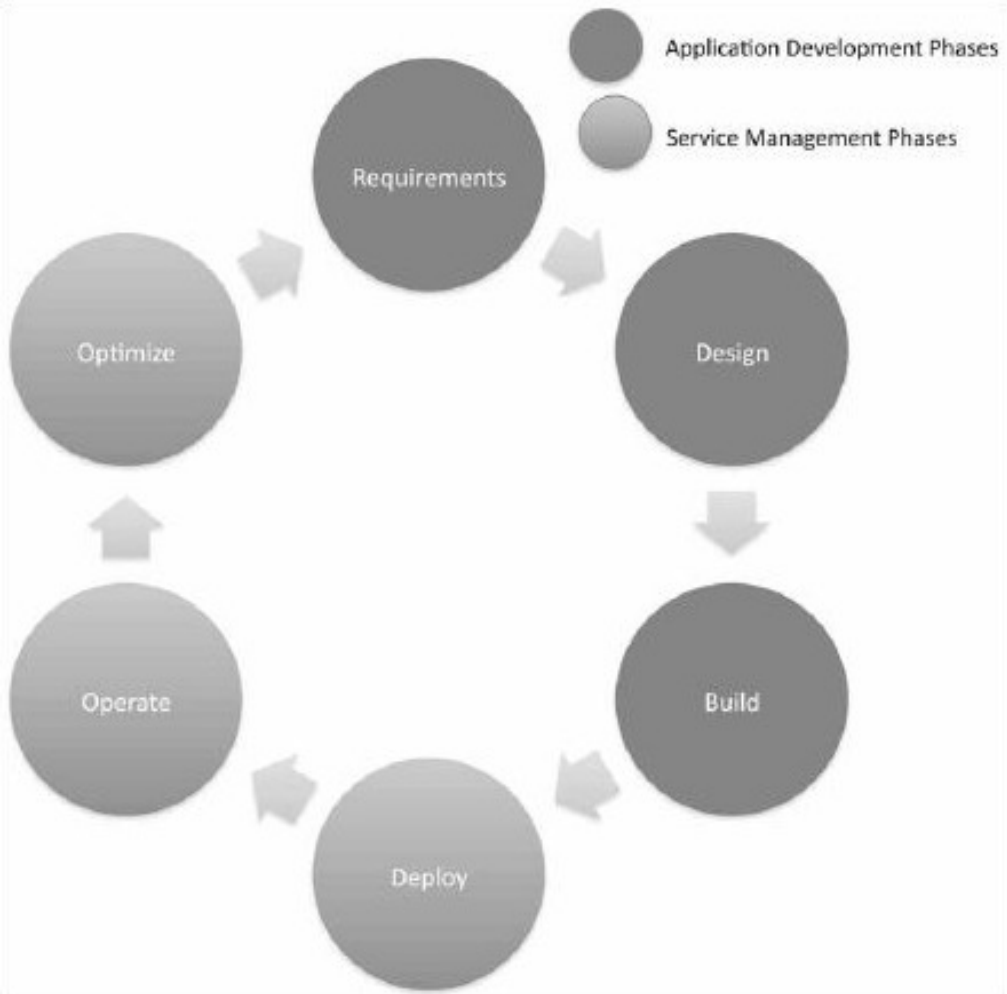
Operators = Narcissists

Operators have no idea about anything related to application development.

80%+ of vulnerability problems occur in the first three dark phases.

If operators never work with developers, their jobs will grow in difficulty.

You can only optimize so much before you have to fix problems at the root of their cause.



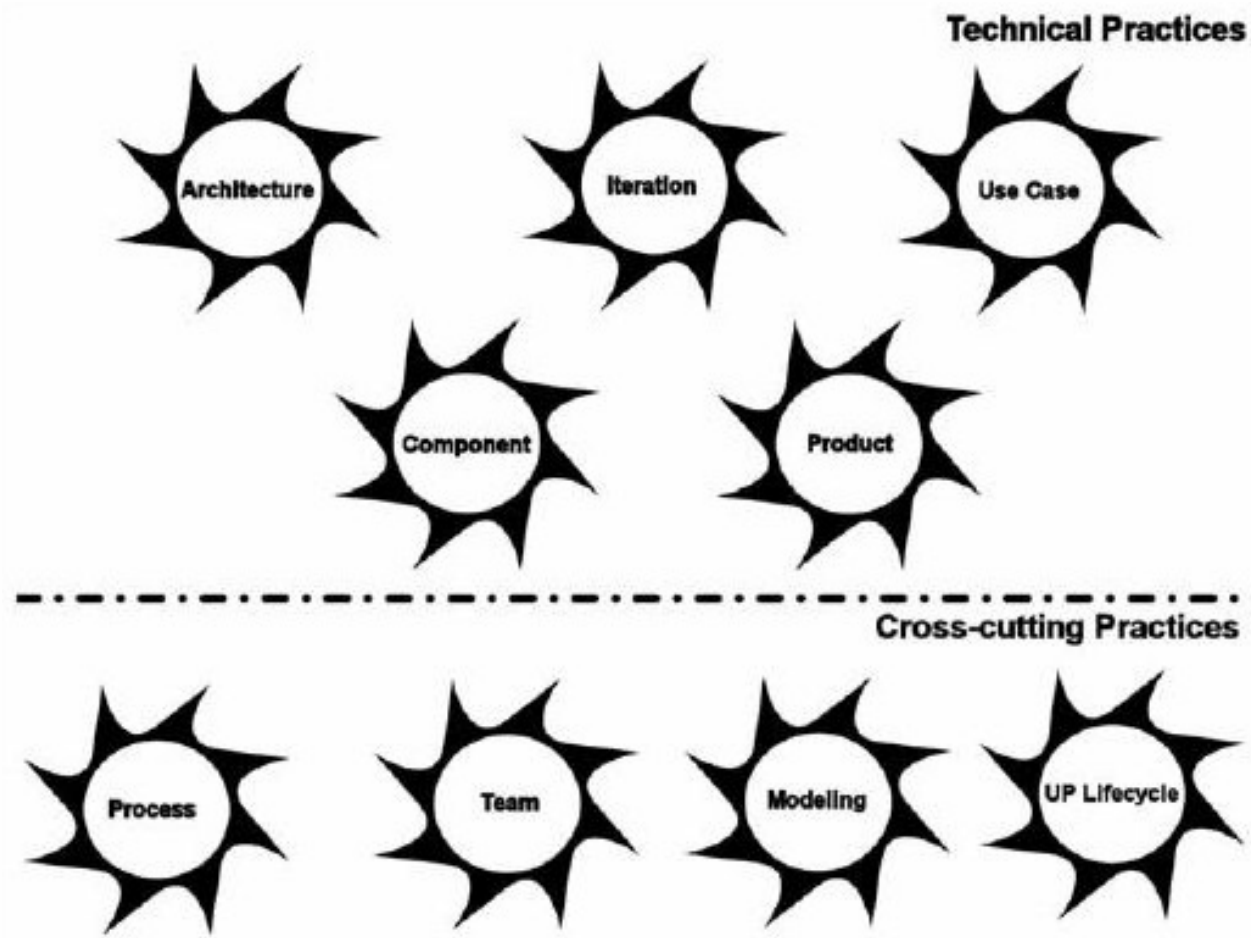
Developers = Bipolar Bears

There is no unified process. There is only Zuul

Agile and CMM mean something different to everyone. Just ask.

Dev shops rarely follow e.g. Waterfall or SCRUM exactly as written.

This diagram is EssUP from Ivar Jacobson. It uses an unpopular but relevant programming concept, AOP, and applies it to process.



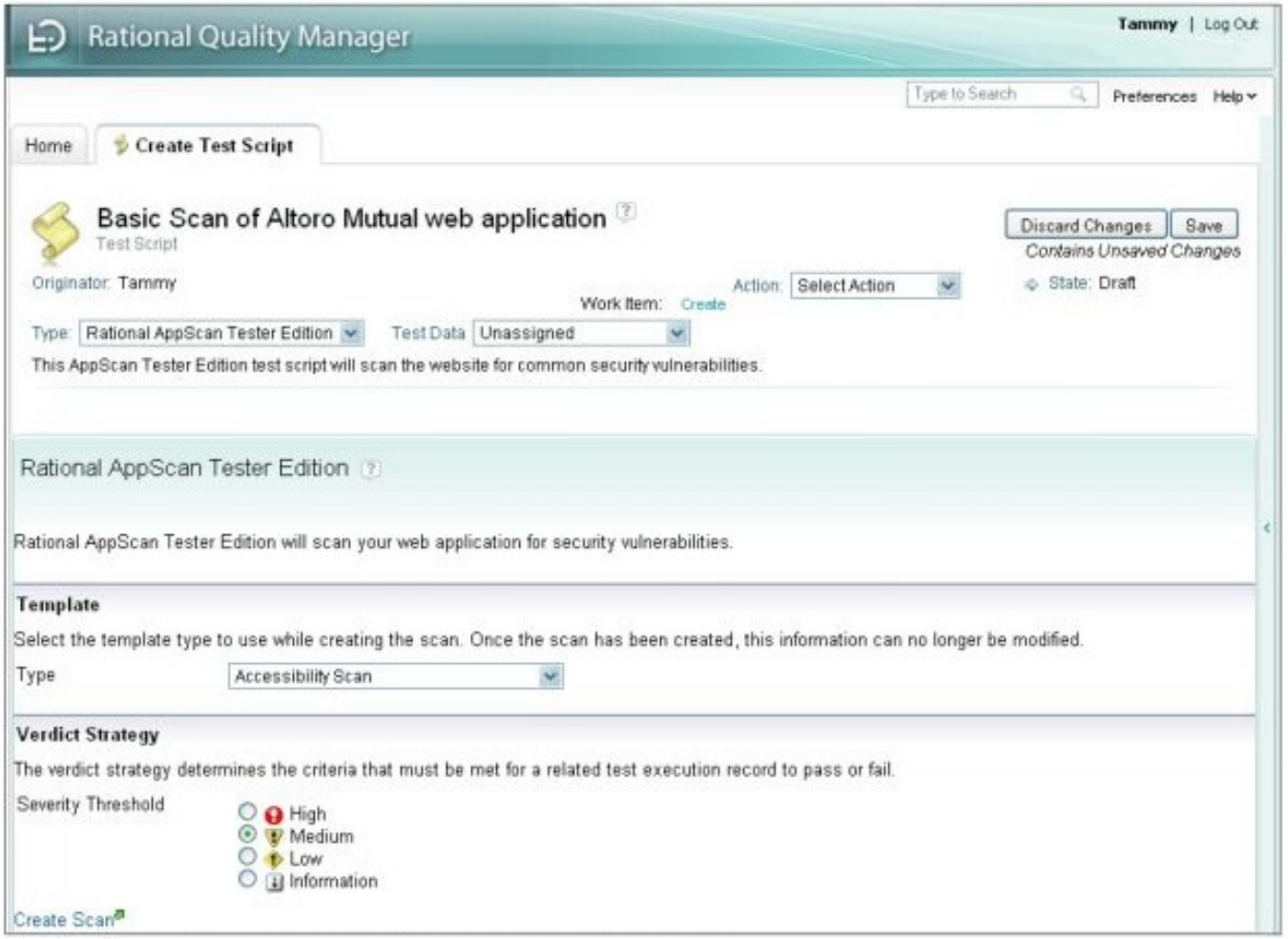
IBM CALMs everyone down

Rational Quality Manager

Rational AppScan Tester Edition

Templates

Security Levels

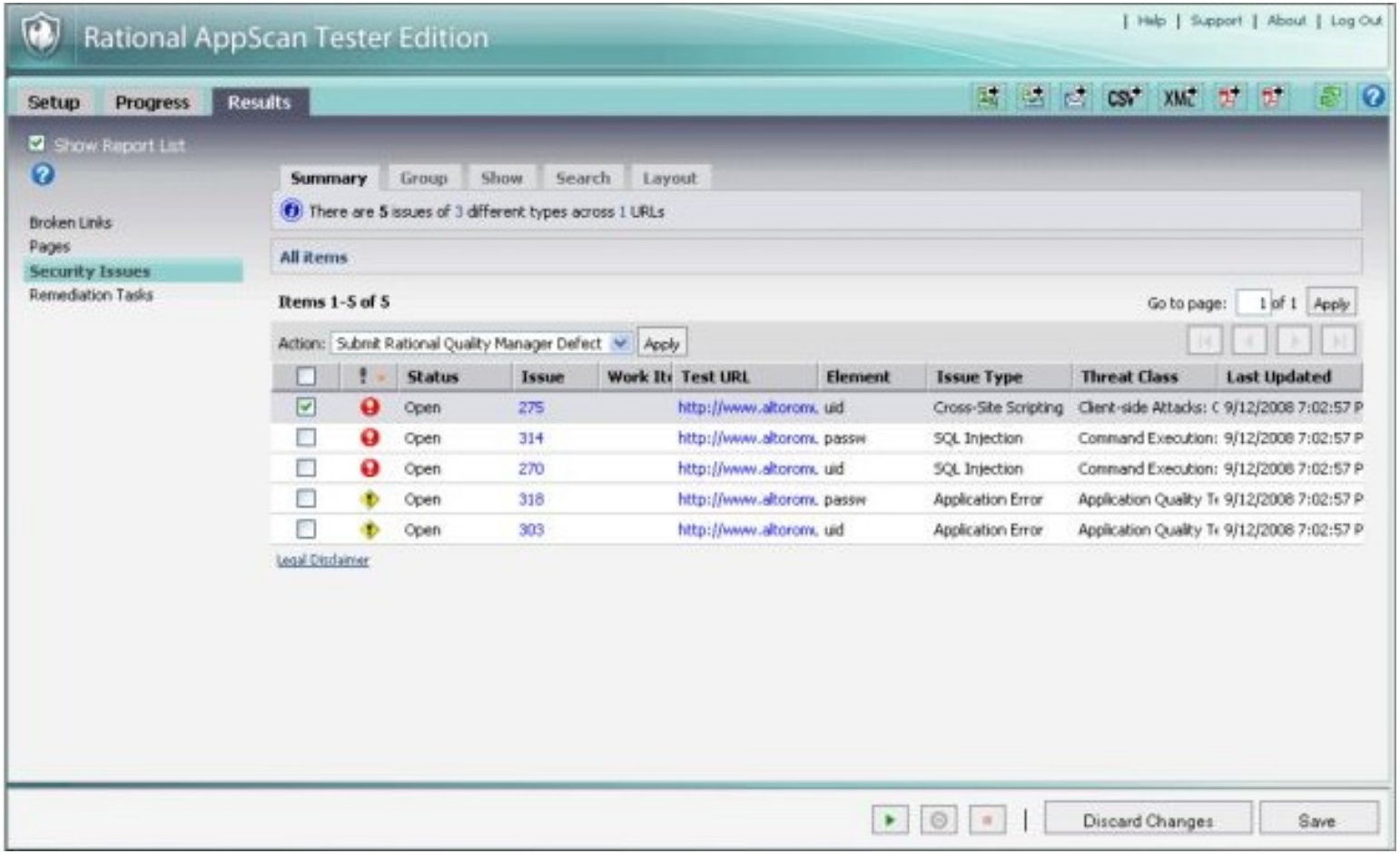


AppScan, Monkey Edition

AppScan Tester Ed.

Security Issues, Remediation Tasks

Submit Rational Quality Manager Defect

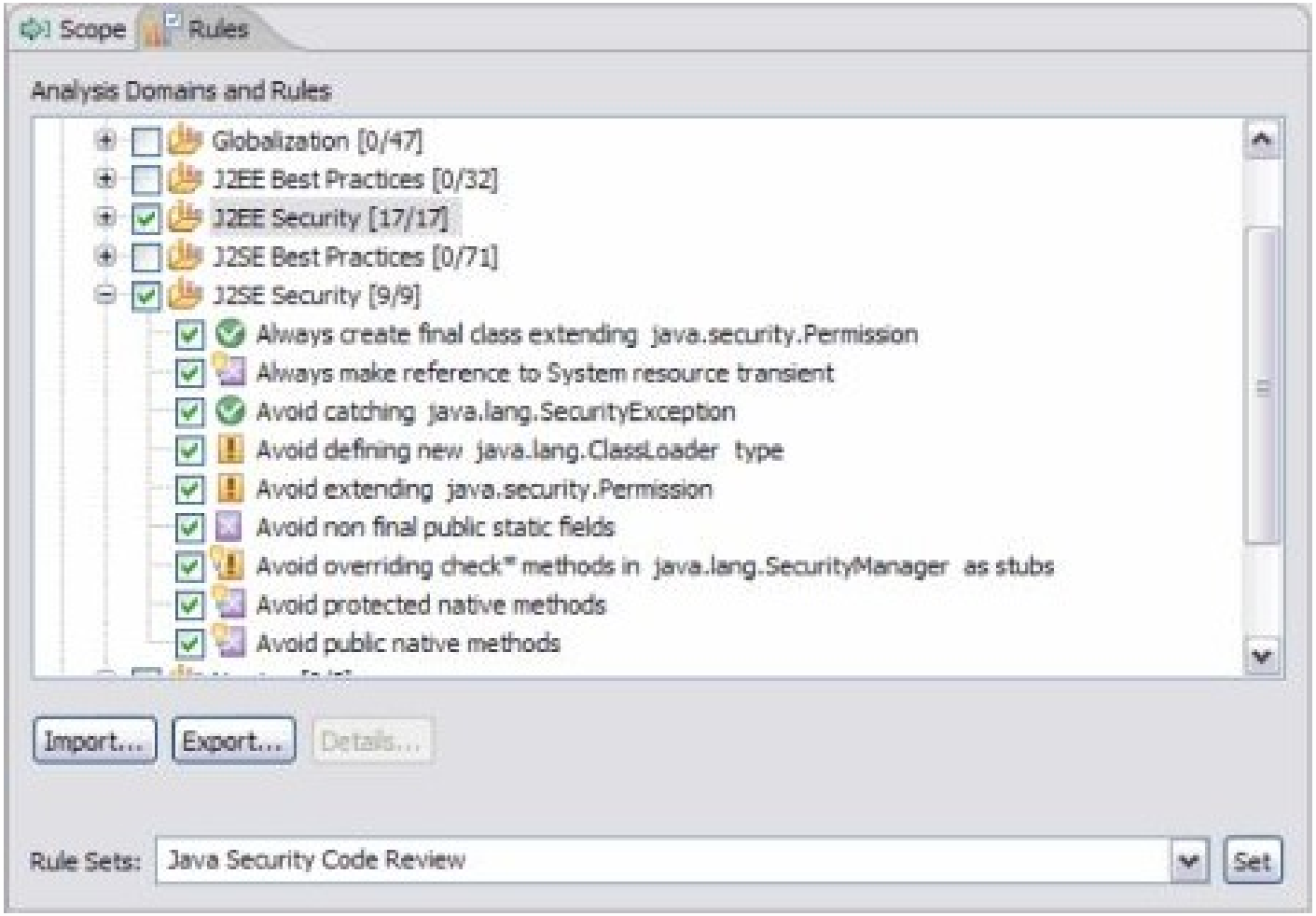


Slowest IDE in the world

Rational Application Developer for WebSphere Software V7

Code Review (really analyzing source code with static analysis)

J2EE Security Rules

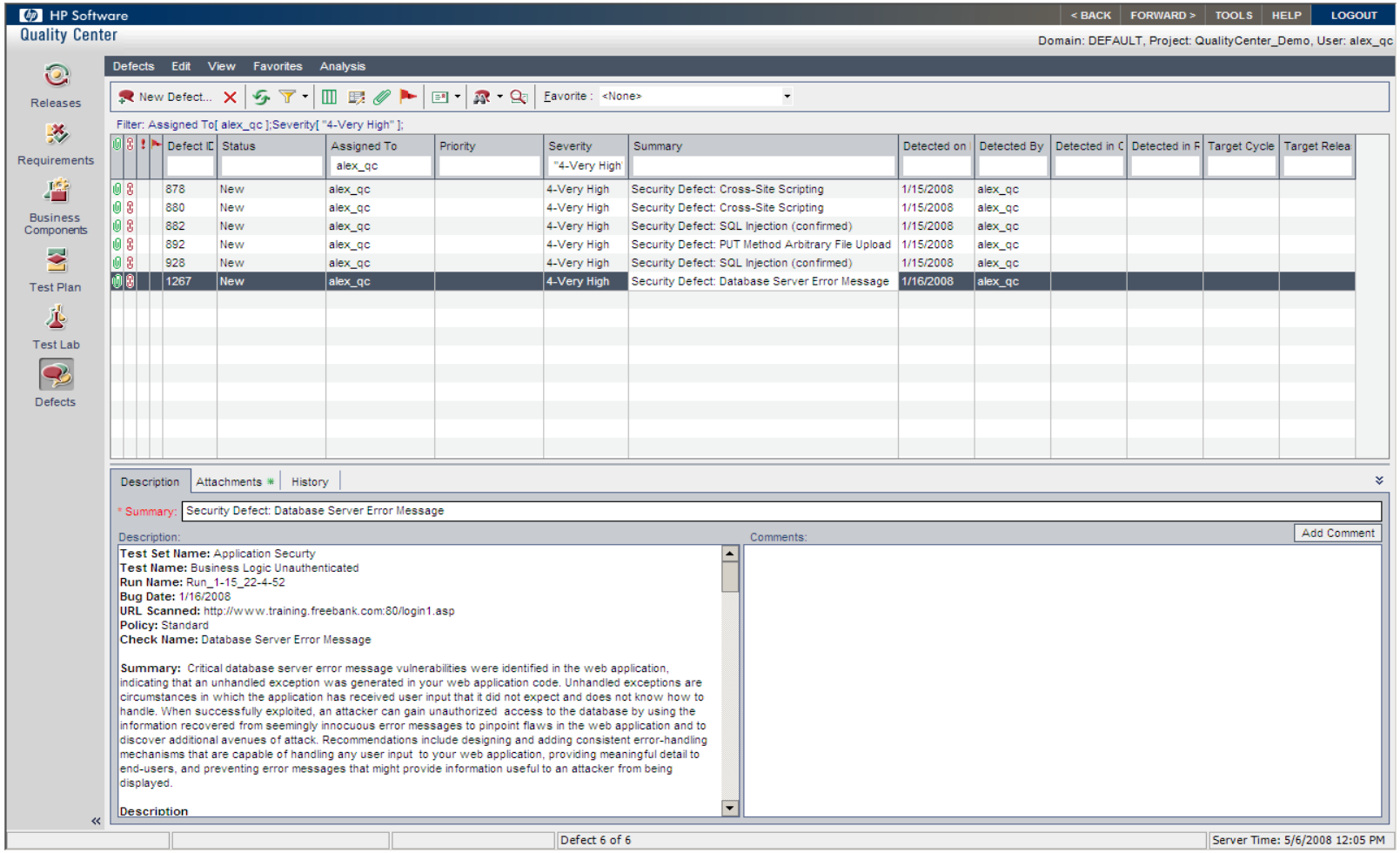


HP also has ALM

HP Quality Center

Test Plan, Test Lab, Defects

Security Defect Description



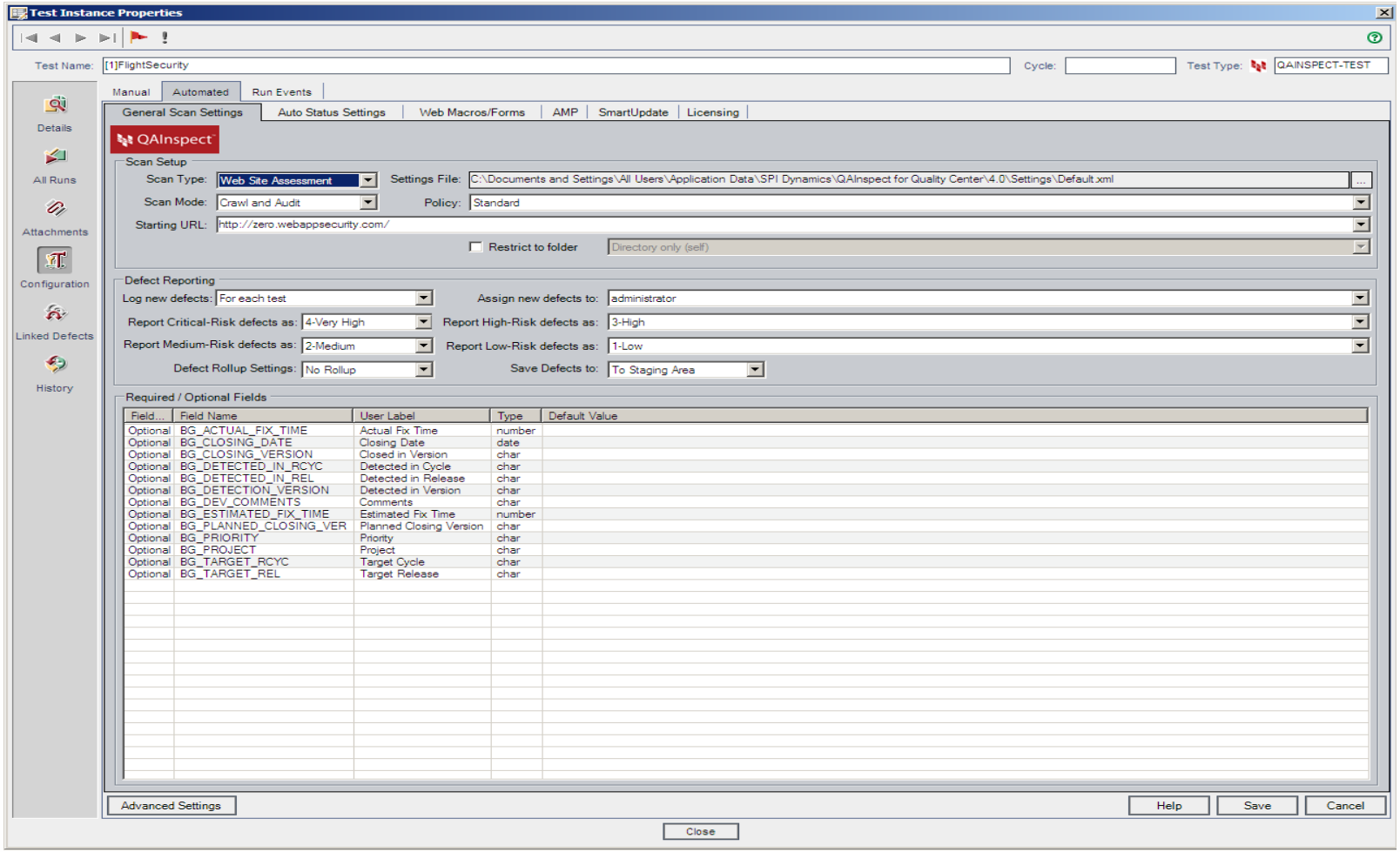
HP also has Monkey scripts

HP QAInspect V7

AMP Tab

Defect Reporting, Linked Defects

Required / Optional Fields



HP adds assessment mgmt

HP AMP Console V8

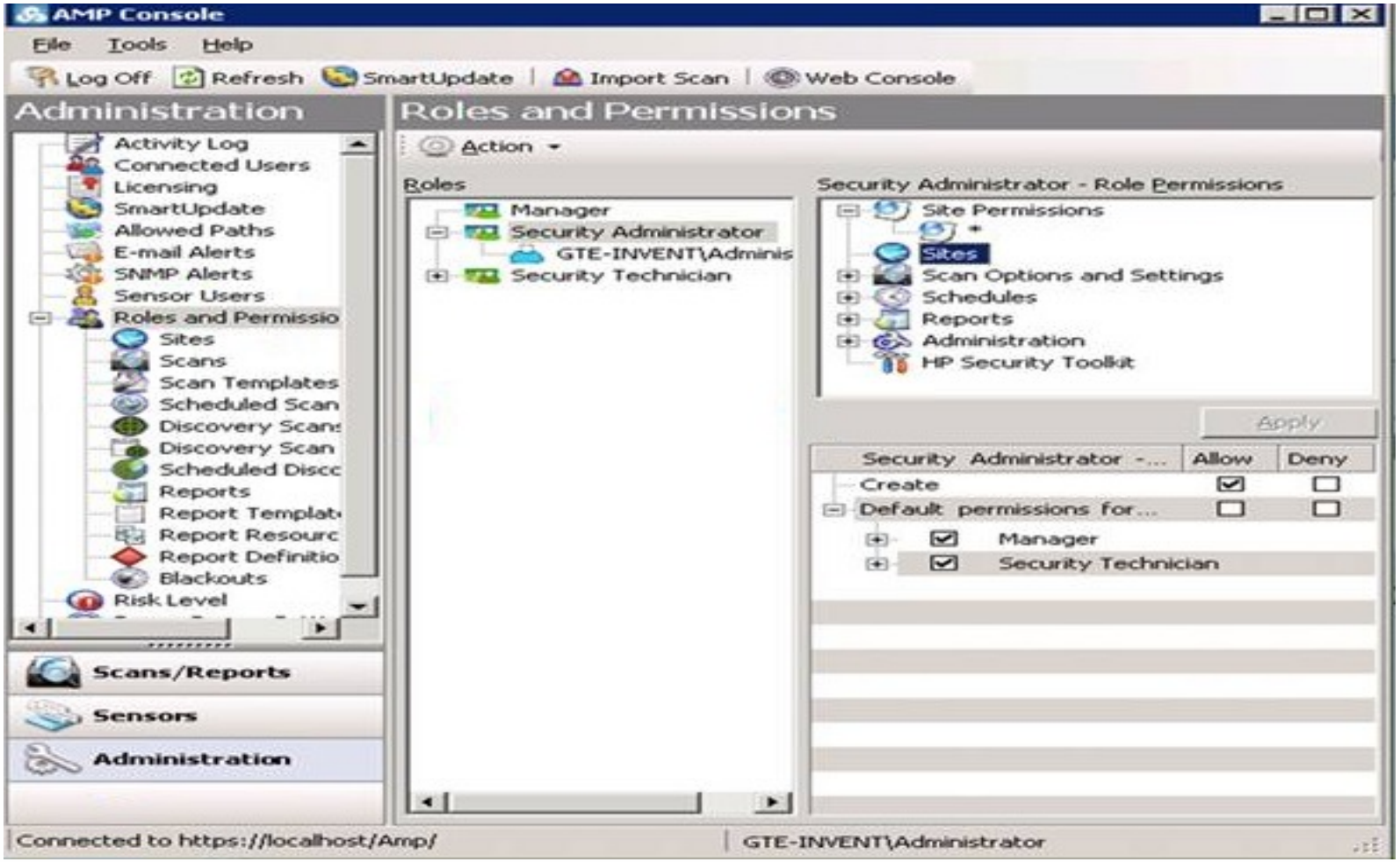
Sites

Scans

Reports

Sensors

Administer



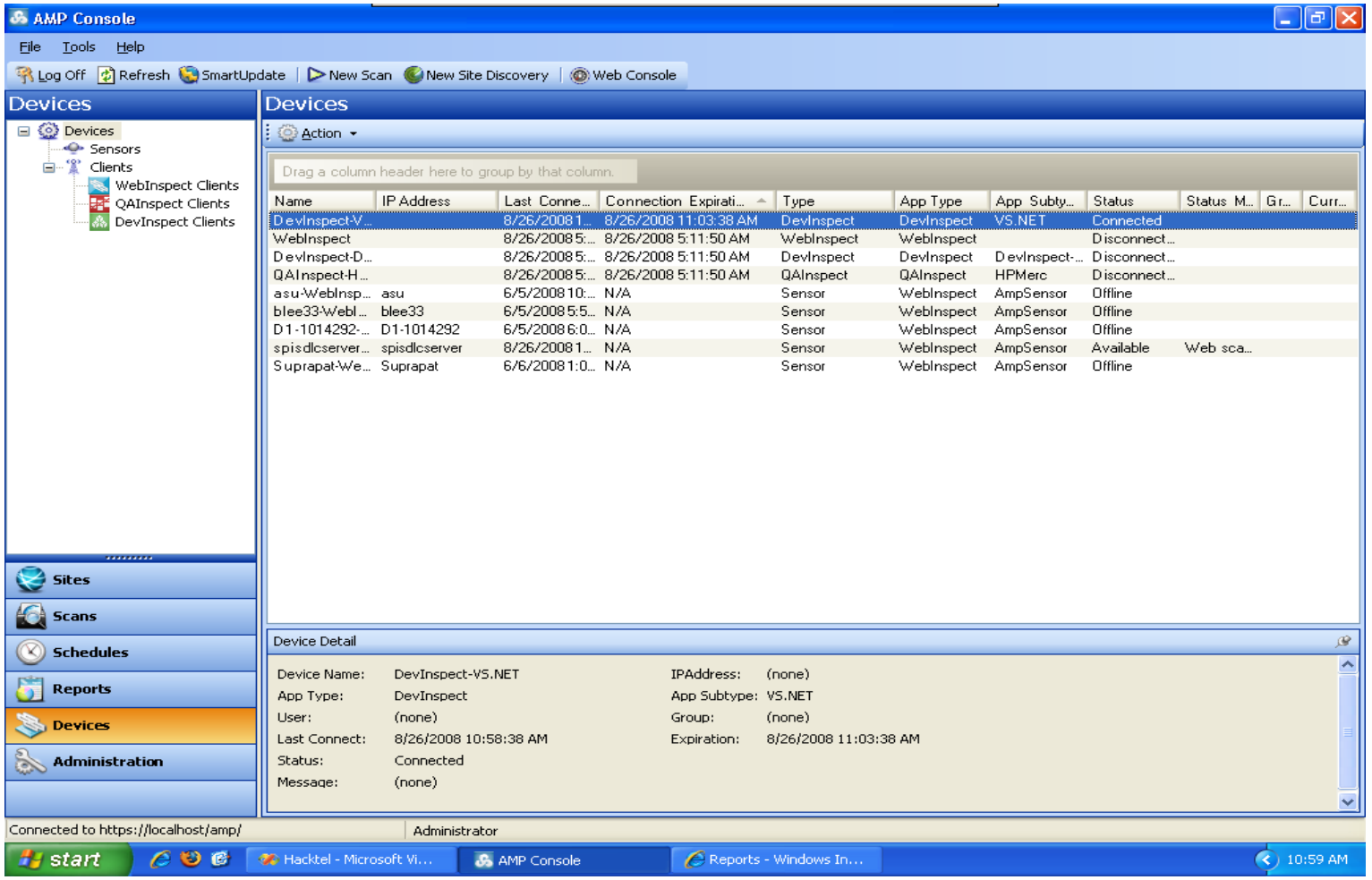
Monkeys & Devs hold hands

HP AMP Console V7

Devices, Sensors, Clients

DevInspect
WebInspect
QAInspect

Coming October 2009: Fortify 360



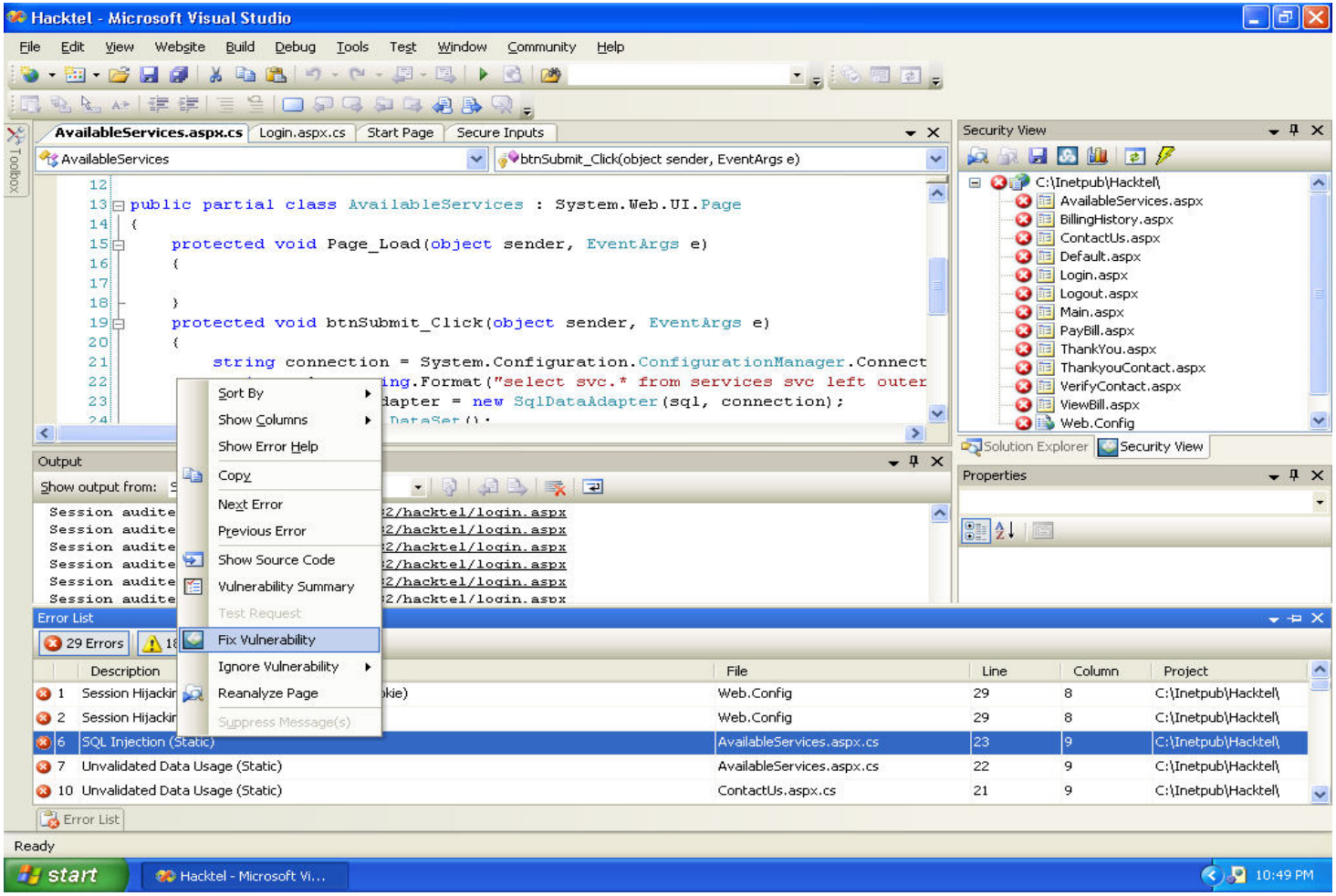
Second slowest IDE

Microsoft Visual Studio 2005, 2008 with HP DevInspect

Secure Inputs, Security View

SecureObjects

Fix Vulnerability



Security Bugfixers exist?

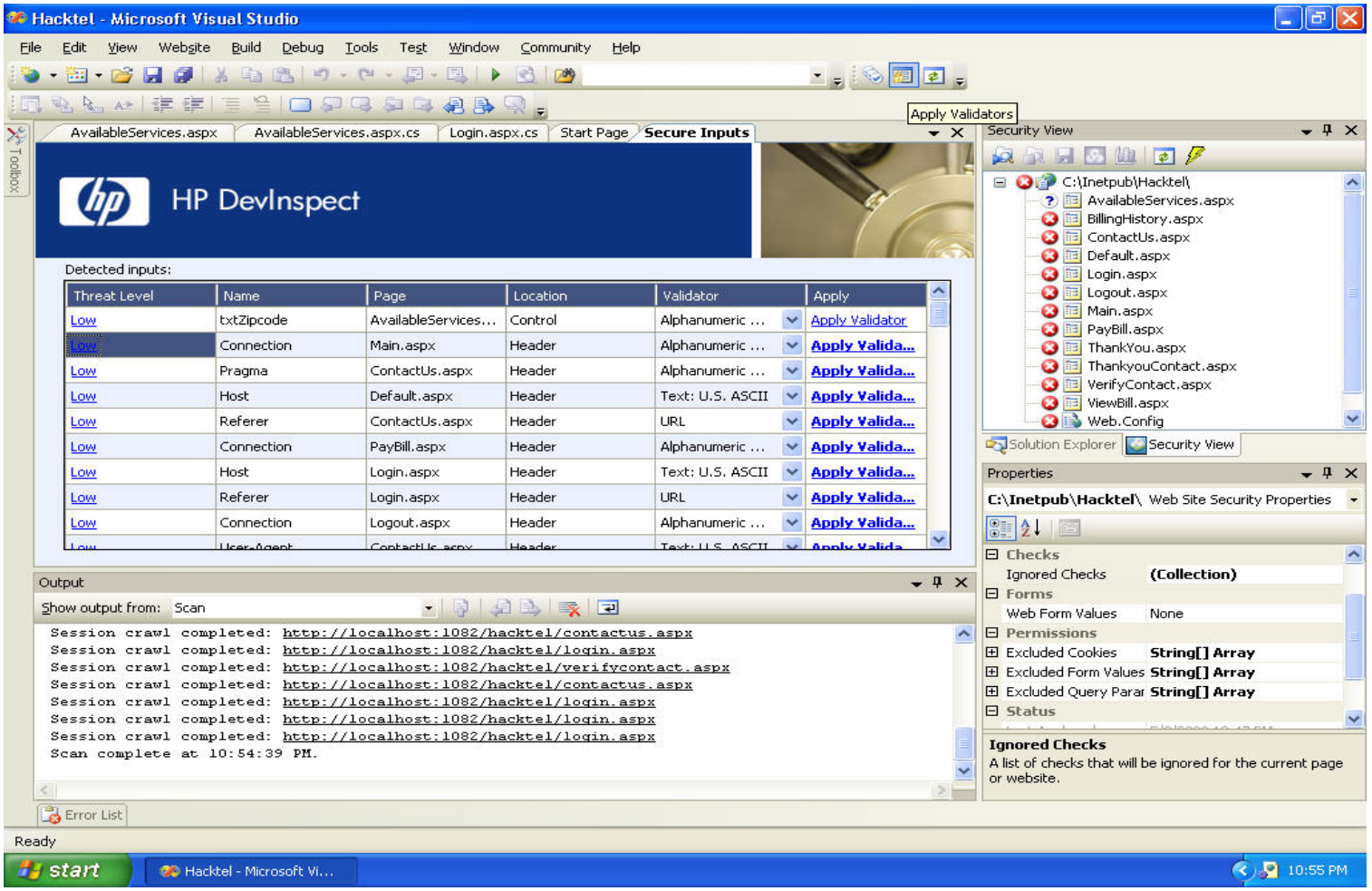
HP DevInspect

Secure Inputs, Security View

Detected Inputs

Validator

Output



90%+ False Pos/Neg Rates

Static Analysis Tools Exposition (SATE)

- 48k warnings reported: 6 people reviewed a 6k subset over several months, resulting in 1800 findings
- After tuning, tools still had a false-positive error rate of 96%
- After sampling a subset, false-positive rate was still over 70%

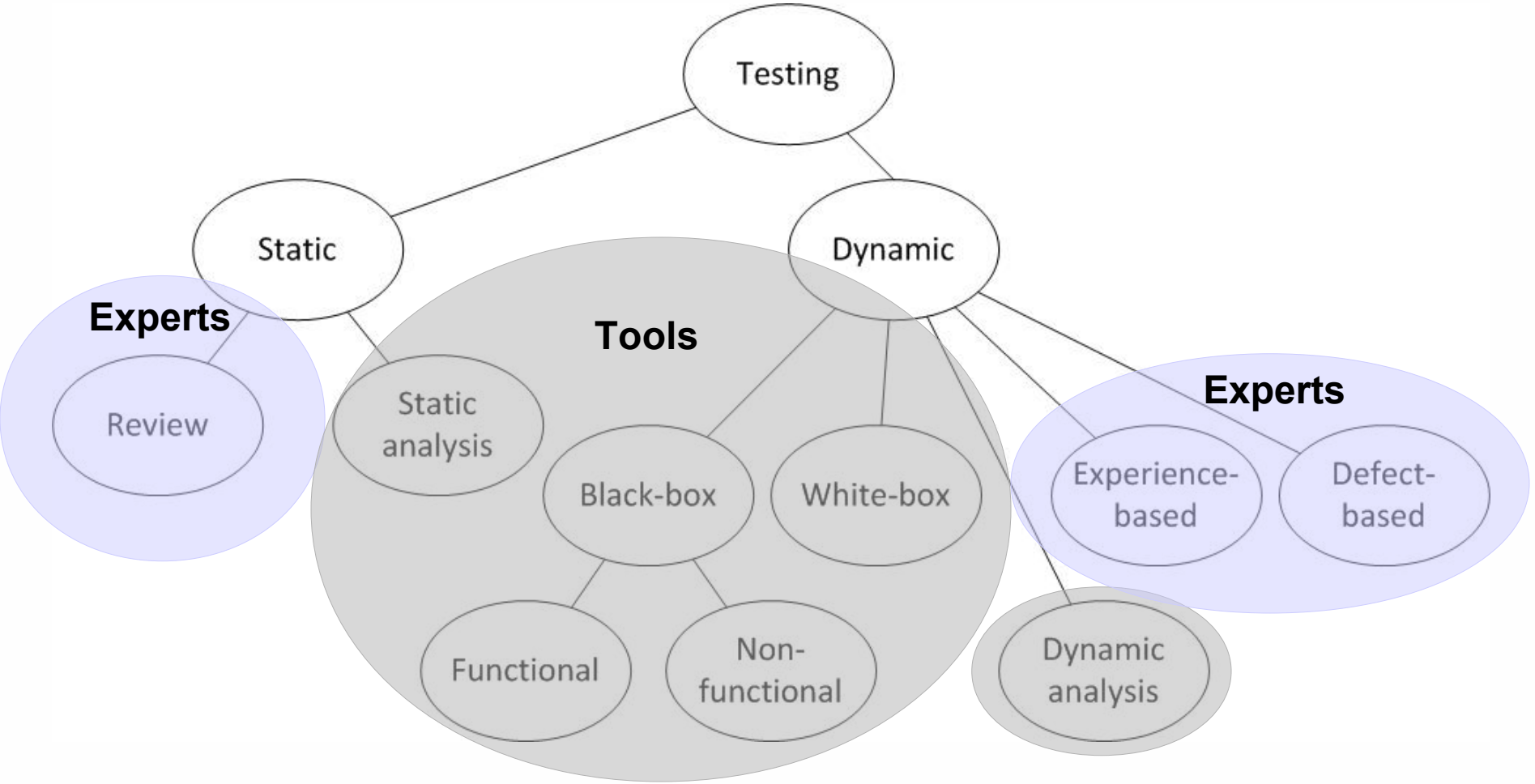
Link extraction – wivet.googlecode.com

- No tool achieved 100%, No open-source tool achieved over 50%

Notoriously don't work with

- Popular frameworks and languages
- Annotations, @OP, DI, IoC, ORM
- And other words you've never heard of
- Serialized objects or applets
  - Java, Flash remoting, Flex, ViewState, XML|JSON|Javascript| Ajax in the DOM
- One language inside (embedded in) another

People vs. Tools



Solution

- People who verify code by reading it
  - Source Insight
  - Notepad++
  - Follow ASVS, map tools to activities
- Desire to learn
  - Training or community should follow
- Governance and appsec policies

How I know this

http://isbn.nu/1933952199/ (Advanced Software Testing)
http://isbn.nu/143021080X/ (Pro Visual Studio Team System Application Lifecycle Management)
http://isbn.nu/0738431974/ (Collaborative Application Lifecycle Management with IBM Rational)
https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/code/212-BSI.html
http://www.ivarjacobson.com/products/essup.cfm
http://msdn.microsoft.com/en-us/teamsystem/aa718795.aspx
http://vstsscrum.codeplex.com
http://scrumforteamsystem.com
http://msdn.microsoft.com/en-us/security/dd670265.aspx
http://news.cnet.com/8301-13505_3-10218777-16.html
http://en.wikipedia.org/wiki/Rational_Application_Developer#Criticisms
http://www.isecpartners.com/files/SD%20Best%20Practices%20-%20Code%20Scanning%20Case%20Studies.pdf
http://www.cigital.com/justiceleague/2009/03/30/maturity-models-vs-top-10-lists/
http://samate.nist.gov/index.php/SATE.html
http://deblaze-tool.appspot.com/
http://www.matasano.com/log/1739/ruby-for-pentesters-a-viewstate-deserializer/
http://weblogs.java.net/blog/inder/archive/2007/01/fortifying_web.html
http://www.owasp.org/index.php/Man_vs._Code
http://www.greebo.net/2009/06/18/using-asvs-for-real/

Extra Credit: WAFs

- WAFs are Monkey scripts cleverly marketed as network-based firewalls
- WAFs can be helpful for improving findings in the lab
  - Microsoft AntiXSS SRE config generator
  - GDS Security SPF and IIS7 features
  - Mod-security can find XSS on the outbound, R.Barnett BlackHat DC 09