

# Why appsec tools suck

TOORCAMP 2009

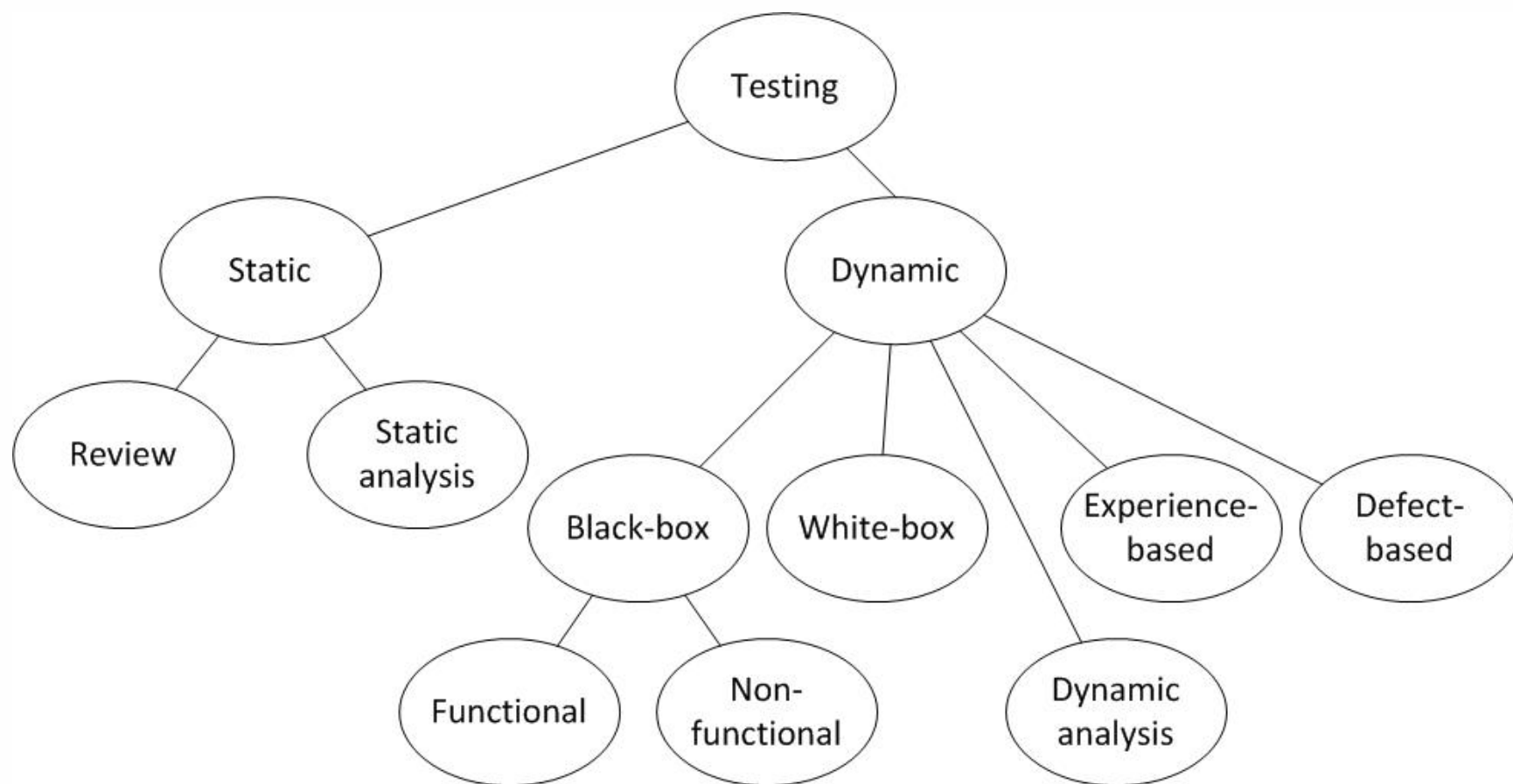
# My story

Andre Gironde

- Interest in appsec tools
- Write for [tssci-security.com](https://tssci-security.com)
- Involved with OWASP



# How I view appsec



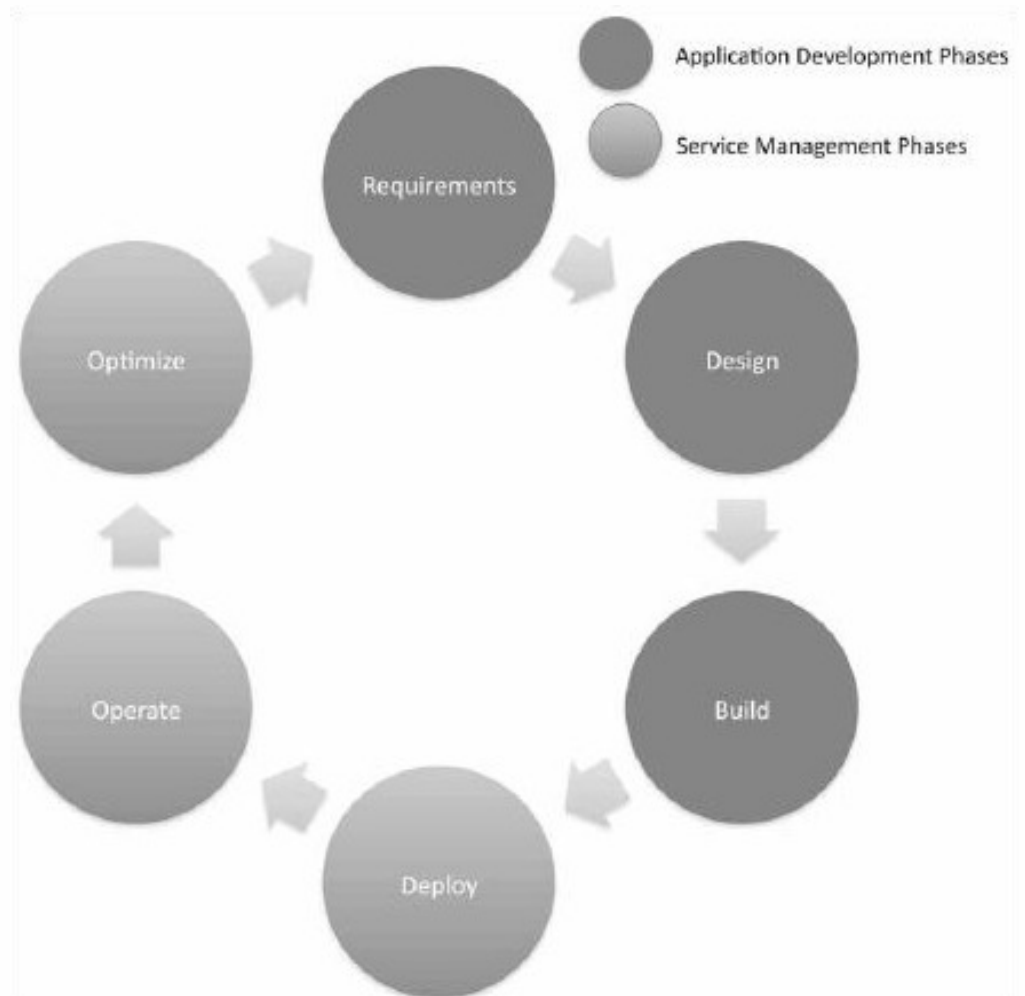
# Operators = Narcissists

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.



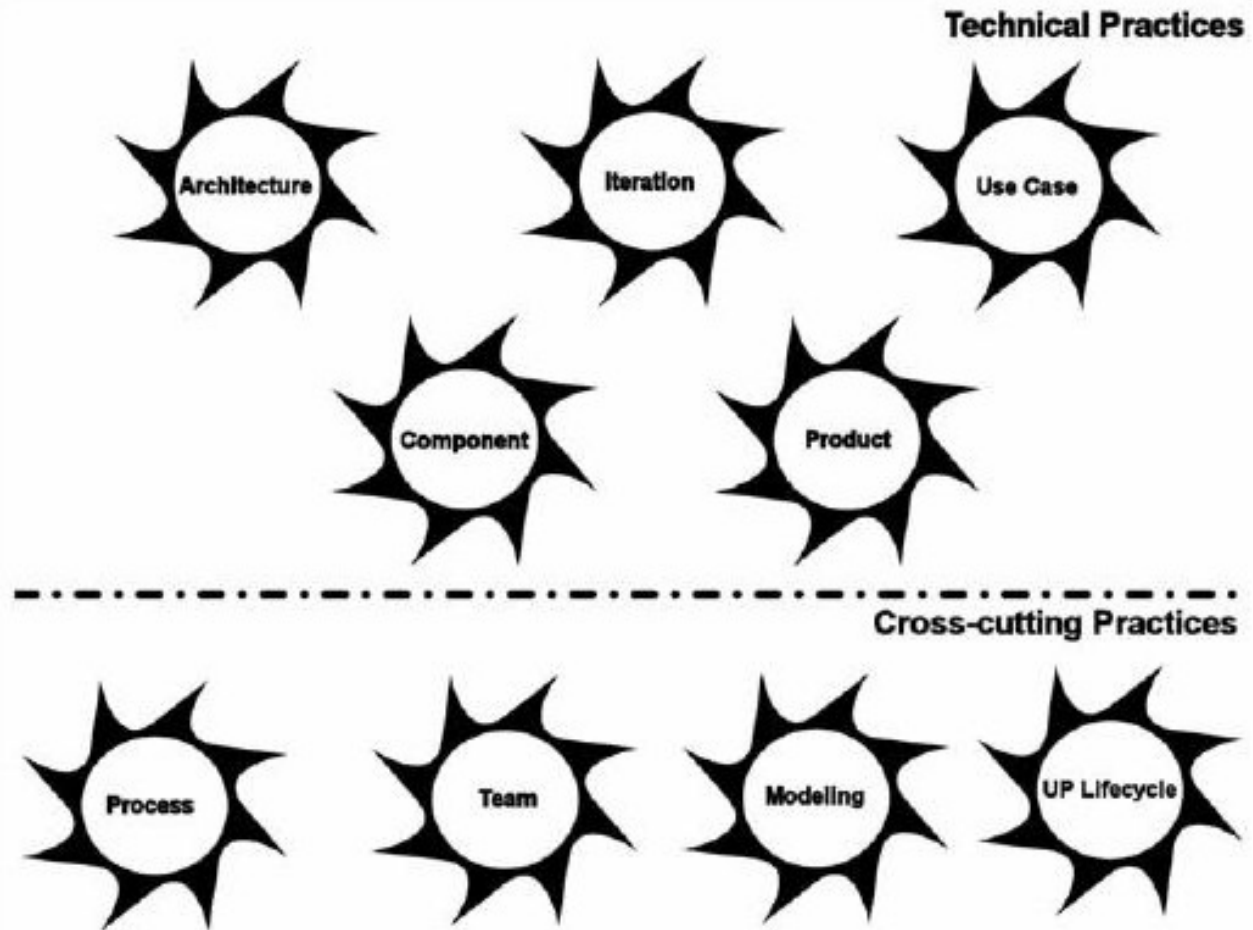
# Developers = Bipolar Bears

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.



ts/sci security

01110100 01110011 00101111 01110011 01100011 01101001 00100000 01110011 01100101 01100011 01110101 01110010 01101001 01110100 01111001

# IBM CALMs everyone down

Rational  
Quality  
Manager

Rational  
AppScan  
Tester Edition

Templates

Security Levels

The screenshot displays the Rational Quality Manager web interface. At the top, the header includes the Rational Quality Manager logo, the user name 'Tammy', and a 'Log Out' link. Below the header, there is a search bar labeled 'Type to Search' and links for 'Preferences' and 'Help'. The main content area features a 'Home' button and a 'Create Test Script' button. A yellow folder icon represents the 'Basic Scan of Altoro Mutual web application' test script. Below this, the 'Originator' is listed as 'Tammy'. The 'Type' is set to 'Rational AppScan Tester Edition', and the 'Test Data' is 'Unassigned'. A note states: 'This AppScan Tester Edition test script will scan the website for common security vulnerabilities.' To the right, there are buttons for 'Discard Changes' and 'Save', with a message 'Contains Unsaved Changes'. Below these, the 'State' is 'Draft'. The 'Work Item' is 'Create', and the 'Action' is 'Select Action'. A section titled 'Rational AppScan Tester Edition' contains a description: 'Rational AppScan Tester Edition will scan your web application for security vulnerabilities.' Below this, a 'Template' section allows selecting a template type, currently set to 'Accessibility Scan'. A 'Verdict Strategy' section explains that the strategy determines the criteria for a test execution record to pass or fail. It includes a 'Severity Threshold' section with four radio button options: 'High' (red exclamation mark), 'Medium' (yellow exclamation mark), 'Low' (yellow exclamation mark), and 'Information' (blue exclamation mark). The 'High' option is selected. At the bottom left, there is a 'Create Scan' button.

ts/sci security

01110100 01110011 00101111 01110011 01100011 01101001 00100000 01110011 01100101 01100011 01110101 01110010 01101001 01110100 01111001

# AppScan, Monkey Edition

AppScan  
Tester Ed.

Security  
Issues,  
Remediation  
Tasks

Submit  
Rational  
Quality  
Manager  
Defect

The screenshot displays the Rational AppScan Tester Edition interface. The top navigation bar includes 'Setup', 'Progress', and 'Results' tabs. The 'Results' tab is active, showing a summary of 5 issues across 1 URL. A table lists the following items:

	Status	Issue	Work It	Test URL	Element	Issue Type	Threat Class	Last Updated
<input checked="" type="checkbox"/>	Open	275		http://www.altorom. uid		Cross-Site Scripting	Client-side Attacks: C	9/12/2008 7:02:57 P
<input type="checkbox"/>	Open	314		http://www.altorom. passw		SQL Injection	Command Execution:	9/12/2008 7:02:57 P
<input type="checkbox"/>	Open	270		http://www.altorom. uid		SQL Injection	Command Execution:	9/12/2008 7:02:57 P
<input type="checkbox"/>	Open	318		http://www.altorom. passw		Application Error	Application Quality Tr	9/12/2008 7:02:57 P
<input type="checkbox"/>	Open	303		http://www.altorom. uid		Application Error	Application Quality Tr	9/12/2008 7:02:57 P

At the bottom of the interface, there are buttons for 'Discard Changes' and 'Save'.

ts/sci security

01110100 01110011 00101111 01110011 01100011 01101001 00100000 01110011 01100101 01100011 01110101 01110010 01101001 01110100 01111001

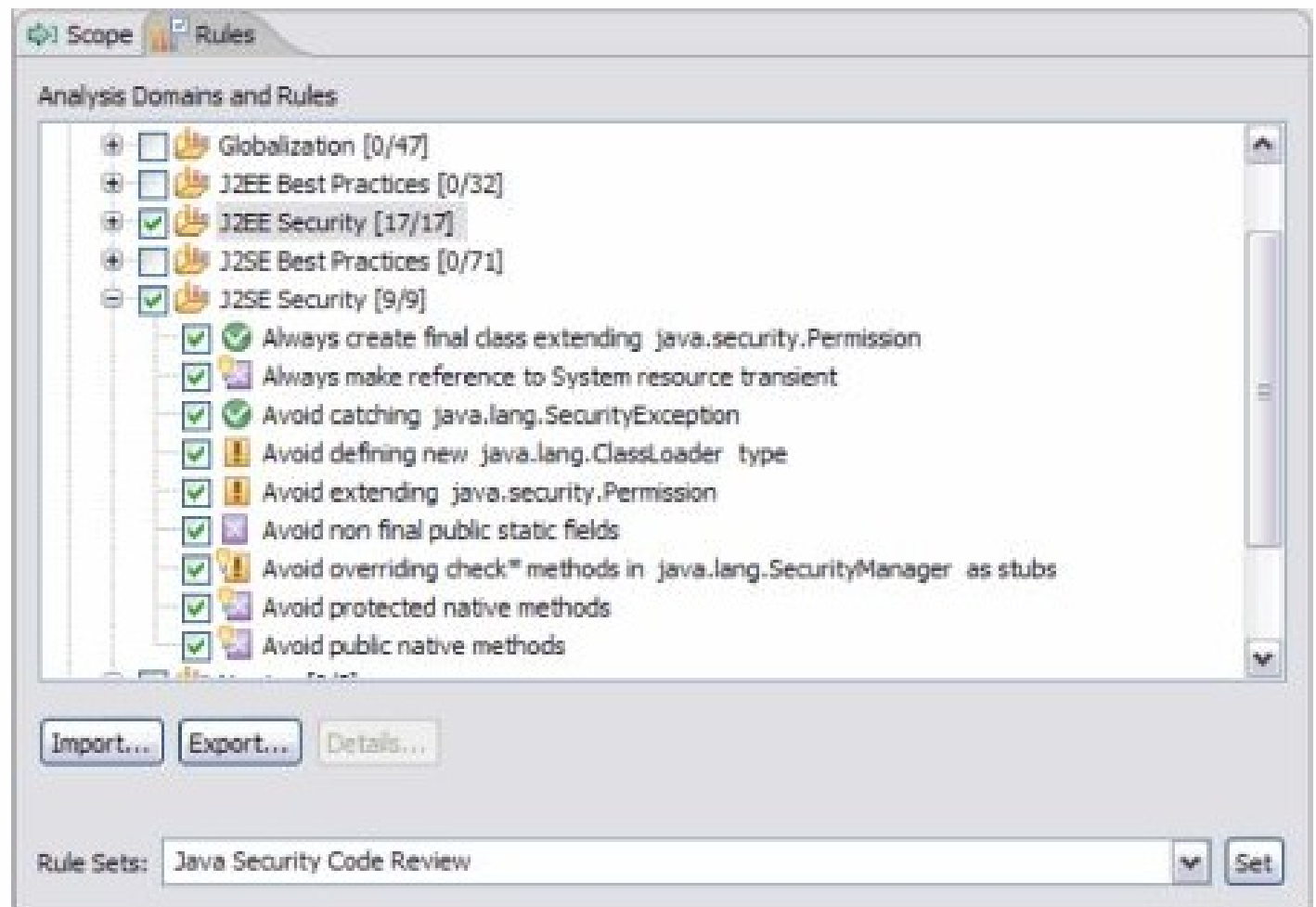


# Slowest IDE in the world

Rational  
Application  
Developer for  
WebSphere  
Software V7

Code Review  
(really analyzing  
source code with  
static analysis)

J2EE Security  
Rules



ts/sci security

01110100 01110011 00101111 01110011 01100011 01101001 00100000 01110011 01100101 01100011 01110101 01110010 01101001 01110100 01111001



# HP also has ALM

HP  
Quality  
Center

Test Plan,  
Test Lab,  
Defects

Security  
Defect  
Description

The screenshot displays the HP Quality Center web application. The top navigation bar includes links for BACK, FORWARD, TOOLS, HELP, and LOGOUT. The domain is set to DEFAULT, and the project is QualityCenter\_Demo. The user is alex\_qc.

The main interface shows a list of defects under the 'Defects' tab. The filter is set to 'Assigned To alex\_qc; Severity [4-Very High]'. The table below lists the defects:

Defect ID	Status	Assigned To	Priority	Severity	Summary	Detected on	Detected By	Detected in C	Detected in F	Target Cycle	Target Release
878	New	alex_qc		4-Very High	Security Defect: Cross-Site Scripting	1/15/2008	alex_qc				
880	New	alex_qc		4-Very High	Security Defect: Cross-Site Scripting	1/15/2008	alex_qc				
882	New	alex_qc		4-Very High	Security Defect: SQL Injection (confirmed)	1/15/2008	alex_qc				
892	New	alex_qc		4-Very High	Security Defect: PUT Method Arbitrary File Upload	1/15/2008	alex_qc				
928	New	alex_qc		4-Very High	Security Defect: SQL Injection (confirmed)	1/15/2008	alex_qc				
1267	New	alex_qc		4-Very High	Security Defect: Database Server Error Message	1/16/2008	alex_qc				

The detailed view of defect 1267 is shown below. It includes a summary, description, and comments section.

**\* Summary:** Security Defect: Database Server Error Message

**Description:**

Test Set Name: Application Security  
Test Name: Business Logic Unauthenticated  
Run Name: Run\_1-15\_22-4-52  
Bug Date: 1/16/2008  
URL Scanned: http://www.training.freebank.com:80/login1.asp  
Policy: Standard  
Check Name: Database Server Error Message

**Summary:** Critical database server error message vulnerabilities were identified in the web application, indicating that an unhandled exception was generated in your web application code. Unhandled exceptions are circumstances in which the application has received user input that it did not expect and does not know how to handle. When successfully exploited, an attacker can gain unauthorized access to the database by using the information recovered from seemingly innocuous error messages to pinpoint flaws in the web application and to discover additional avenues of attack. Recommendations include designing and adding consistent error-handling mechanisms that are capable of handling any user input to your web application, providing meaningful detail to end-users, and preventing error messages that might provide information useful to an attacker from being displayed.

**Comments:**

Add Comment

Defect 6 of 6

Server Time: 5/6/2008 12:05 PM

ts/sci security

01110100 01110011 00101111 01110011 01100011 01101001 00100000 01110011 01100101 01100011 01110101 01110010 01101001 01110100 01111001

# HP also has Monkey scripts

HP  
QAInspect  
V7

AMP Tab

Defect  
Reporting,  
Linked  
Defects

Required /  
Optional  
Fields

Test Instance Properties

Test Name: [1]FlightSecurity Cycle: Test Type: QAInspect-TEST

Manual Automated Run Events

General Scan Settings Auto Status Settings Web Macros/Forms AMP SmartUpdate Licensing

**QAInspect**

Scan Setup

Scan Type: Web Site Assessment Settings File: C:\Documents and Settings\All Users\Application Data\SPI Dynamics\QAInspect for Quality Center\4.0\Settings\Default.xml

Scan Mode: Crawl and Audit Policy: Standard

Starting URL: http://zero.webappsecurity.com/

☐ Restrict to folder Directory only (self)

Defect Reporting

Log new defects: For each test Assign new defects to: administrator

Report Critical-Risk defects as: 4-Very High Report High-Risk defects as: 3-High

Report Medium-Risk defects as: 2-Medium Report Low-Risk defects as: 1-Low

Defect Rollup Settings: No Rollup Save Defects to: To Staging Area

Required / Optional Fields

Field...	Field Name	User Label	Type	Default Value
Optional	BG_ACTUAL_FIX_TIME	Actual Fix Time	number	
Optional	BG_CLOSING_DATE	Closing Date	date	
Optional	BG_CLOSING_VERSION	Closed in Version	char	
Optional	BG_DETECTED_IN_RCYC	Detected in Cycle	char	
Optional	BG_DETECTED_IN_REL	Detected in Release	char	
Optional	BG_DETECTION_VERSION	Detected in Version	char	
Optional	BG_DEV_COMMENTS	Comments	char	
Optional	BG_ESTIMATED_FIX_TIME	Estimated Fix Time	number	
Optional	BG_PLANNED_CLOSING_VER	Planned Closing Version	char	
Optional	BG_PRIORITY	Priority	char	
Optional	BG_PROJECT	Project	char	
Optional	BG_TARGET_RCYC	Target Cycle	char	
Optional	BG_TARGET_REL	Target Release	char	

Advanced Settings

Help Save Cancel

Close

ts/sci security

01110100 01110011 00101111 01110011 01100011 01101001 00100000 01110011 01100101 01100011 01110101 01110010 01101001 01110100 01111001

# HP adds assessment mgmt

HP AMP  
Console V8

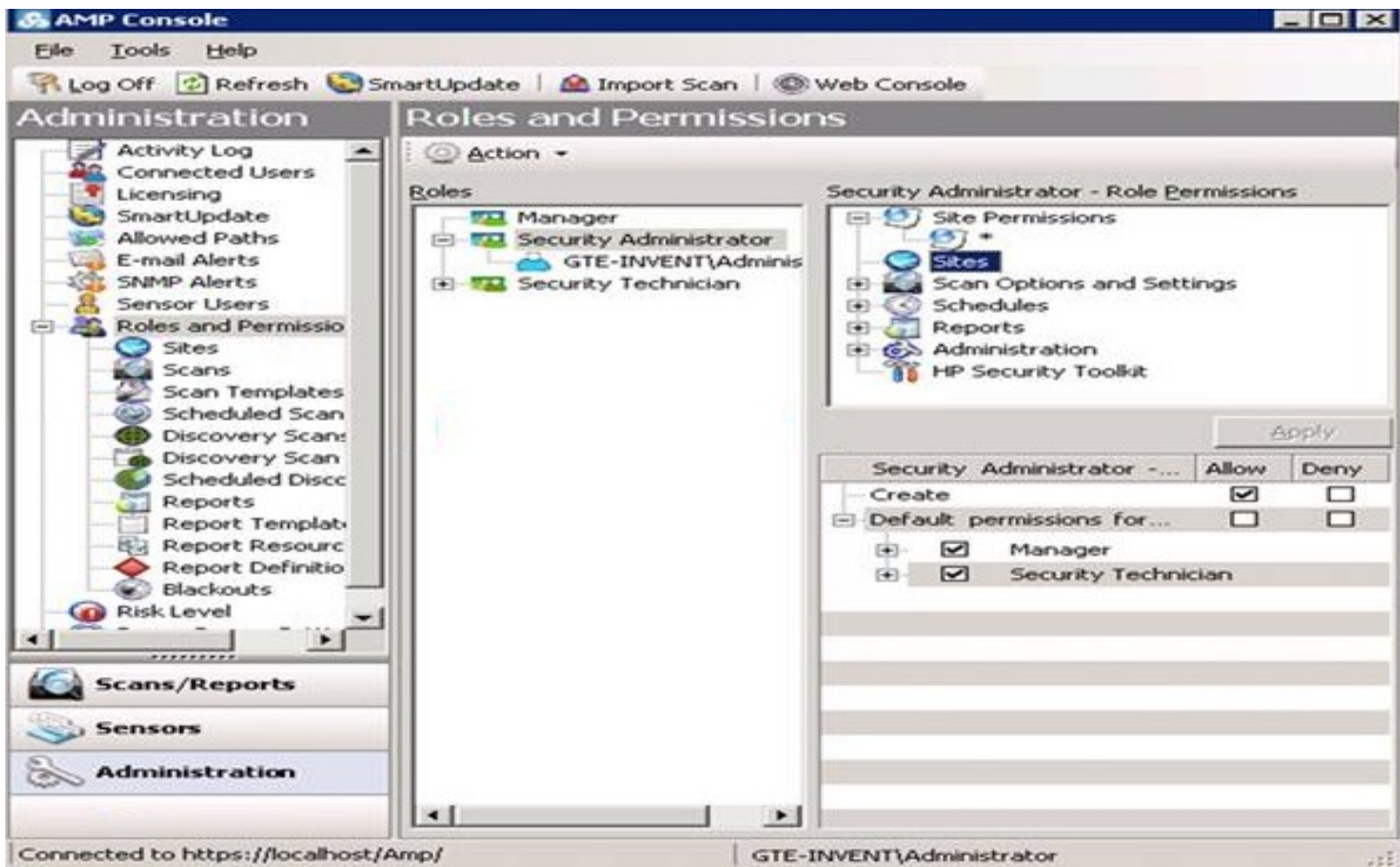
Sites

Scans

Reports

Sensors

Administer



ts/sci security

01110100 01110011 00101111 01110011 01100011 01101001 00100000 01110011 01100101 01100011 01110101 01110010 01101001 01110100 01111001

# Monkeys & Devs hold hands

HP AMP  
Console V7

Devices,  
Sensors,  
Clients

DevInspect  
WebInspect  
QAInspect

Coming  
October 2009:  
Fortify 360

The screenshot displays the HP AMP Console V7 interface. The left sidebar contains a tree view with 'Devices' selected, showing sub-items: 'Sensors', 'Clients', 'WebInspect Clients', 'QAInspect Clients', and 'DevInspect Clients'. Below this are buttons for 'Sites', 'Scans', 'Schedules', 'Reports', 'Devices' (highlighted), and 'Administration'. The main pane shows a table of devices with columns: Name, IP Address, Last Connect, Connection Expiration, Type, App Type, App Subtype, Status, Status Message, Group, and Current. The table lists several devices, including 'DevInspect-VS.NET' which is connected. Below the table is a 'Device Detail' section for 'DevInspect-VS.NET', showing details like App Type (DevInspect), App Subtype (VS.NET), User (none), Group (none), Last Connect (8/26/2008 10:58:38 AM), Expiration (8/26/2008 11:03:38 AM), Status (Connected), and Message (none). The bottom status bar shows 'Connected to https://localhost/amp/' and 'Administrator'.

Name	IP Address	Last Connect	Connection Expiration	Type	App Type	App Subtype	Status	Status Message	Group	Current
DevInspect-VS.NET		8/26/2008 10:58:38 AM	8/26/2008 11:03:38 AM	DevInspect	DevInspect	VS.NET	Connected			
WebInspect		8/26/2008 5:11:50 AM	8/26/2008 5:11:50 AM	WebInspect	WebInspect		Disconnect...			
DevInspect-D...		8/26/2008 5:11:50 AM	8/26/2008 5:11:50 AM	DevInspect	DevInspect	DevInspect...	Disconnect...			
QAInspect-H...		8/26/2008 5:11:50 AM	8/26/2008 5:11:50 AM	QAInspect	QAInspect	HPMerc	Disconnect...			
asu-WebInsp...	asu	6/5/2008 10:...	N/A	Sensor	WebInspect	AmpSensor	Offline			
blee33\WebI...	blee33	6/5/2008 5:5...	N/A	Sensor	WebInspect	AmpSensor	Offline			
D1-1014292...	D1-1014292	6/5/2008 6:0...	N/A	Sensor	WebInspect	AmpSensor	Offline			
spidlcserver...	spidlcserver	8/26/2008 1...	N/A	Sensor	WebInspect	AmpSensor	Available	Web sca...		
Suprapat-We...	Suprapat	6/6/2008 1:0...	N/A	Sensor	WebInspect	AmpSensor	Offline			

Device Detail

Device Name: DevInspect-VS.NET  
App Type: DevInspect  
User: (none)  
Last Connect: 8/26/2008 10:58:38 AM  
Status: Connected  
Message: (none)

IPAddress: (none)  
App Subtype: VS.NET  
Group: (none)  
Expiration: 8/26/2008 11:03:38 AM

Connected to https://localhost/amp/ Administrator

ts/sci security

01110100 01110011 00101111 01110011 01100011 01101001 00100000 01110011 01100101 01100011 01110101 01110010 01101001 01110100 01111001

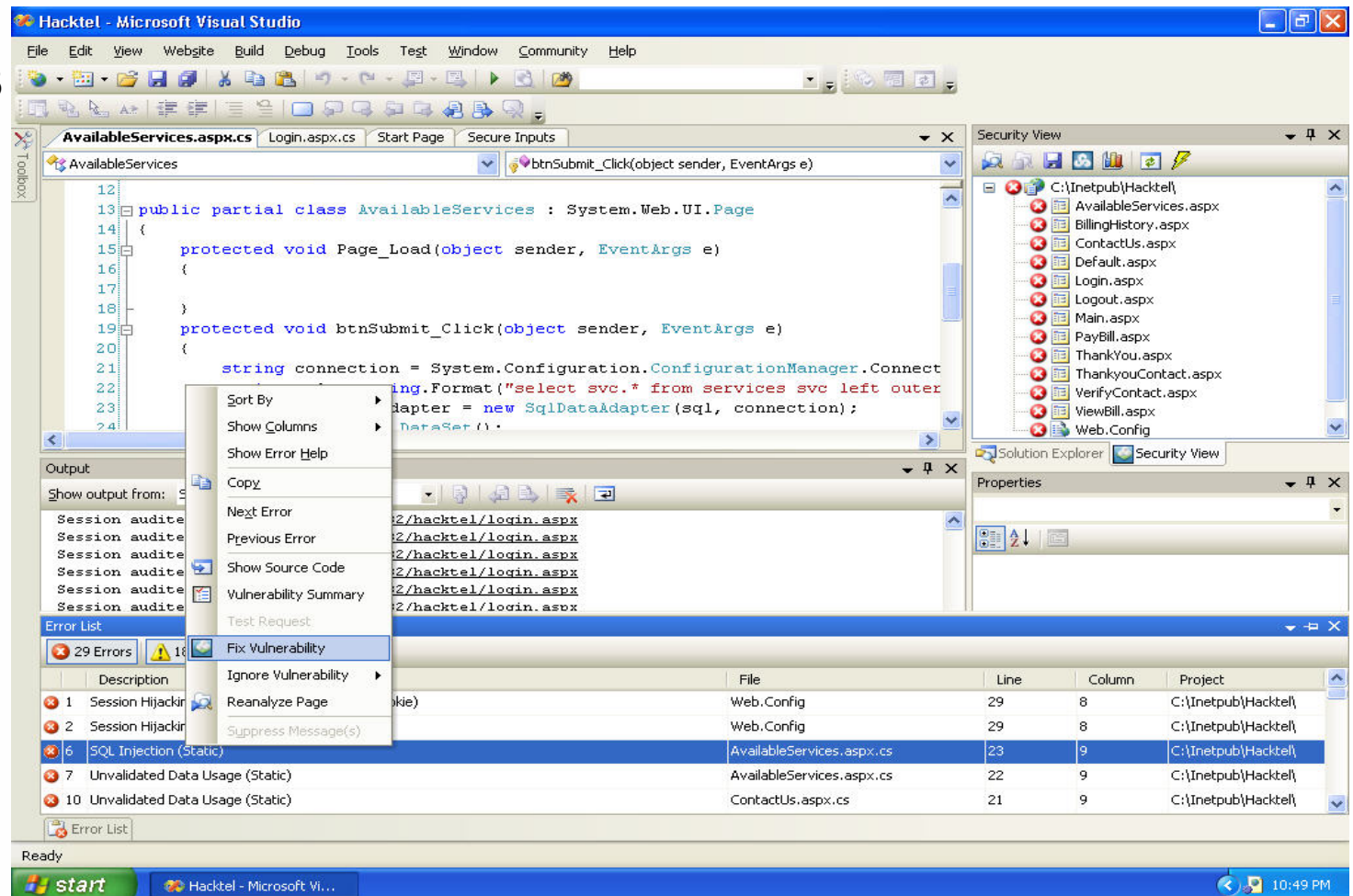
# Second slowest IDE

Microsoft Visual  
Studio 2005, 2008  
with HP  
DevInspect

Secure Inputs,  
Security View

SecureObjects

Fix Vulnerability



ts/sci security

01110100 01110011 00101111 01110011 01100011 01101001 00100000 01110011 01100101 01100011 01110101 01110010 01101001 01110100 01111001



# Security Bugfixers exist?

HP DevInspect

Secure Inputs,  
Security View

Detected Inputs

Validator

Output

The screenshot displays the HP DevInspect application running within Microsoft Visual Studio. The main window shows a table of detected inputs with columns for Threat Level, Name, Page, Location, Validator, and Apply. The table lists various inputs like txtZipcode, Connection, Pragma, Host, Referer, and User-Agent, each with a corresponding threat level and validator. The Security View pane on the right shows a tree of files and folders, including AvailableServices.aspx, BillingHistory.aspx, ContactUs.aspx, Default.aspx, Login.aspx, Logout.aspx, Main.aspx, PayBill.aspx, ThankYou.aspx, ThankyouContact.aspx, VerifyContact.aspx, ViewBill.aspx, and Web.Config. The Properties pane at the bottom right shows the Web Site Security Properties, including checks for Ignored Checks, Forms, Permissions, Excluded Cookies, Excluded Form Values, Excluded Query Parameters, and Status. The Output pane at the bottom shows the session crawl results, including the URLs of the pages crawled and the time taken for each session.

Threat Level	Name	Page	Location	Validator	Apply
Low	txtZipcode	AvailableServices...	Control	Alphanumeric ...	Apply Validator
Low	Connection	Main.aspx	Header	Alphanumeric ...	Apply Valid...
Low	Pragma	ContactUs.aspx	Header	Alphanumeric ...	Apply Valid...
Low	Host	Default.aspx	Header	Text: U.S. ASCII	Apply Valid...
Low	Referer	ContactUs.aspx	Header	URL	Apply Valid...
Low	Connection	PayBill.aspx	Header	Alphanumeric ...	Apply Valid...
Low	Host	Login.aspx	Header	Text: U.S. ASCII	Apply Valid...
Low	Referer	Login.aspx	Header	URL	Apply Valid...
Low	Connection	Logout.aspx	Header	Alphanumeric ...	Apply Valid...
Low	User-Agent	ContactUs.aspx	Header	Text: U.S. ASCII	Apply Valid...

Output

Show output from: Scan

Session crawl completed: <http://localhost:1082/hacktel/contactus.aspx>

Session crawl completed: <http://localhost:1082/hacktel/login.aspx>

Session crawl completed: <http://localhost:1082/hacktel/verifycontact.aspx>

Session crawl completed: <http://localhost:1082/hacktel/contactus.aspx>

Session crawl completed: <http://localhost:1082/hacktel/login.aspx>

Session crawl completed: <http://localhost:1082/hacktel/login.aspx>

Scan complete at 10:54:39 PM.

ts/sci security

01110100 01110011 00101111 01110011 01100011 01101001 00100000 01110011 01100101 01100011 01110101 01110010 01101001 01110100 01111001

# 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](https://wivet.googlecode.com)

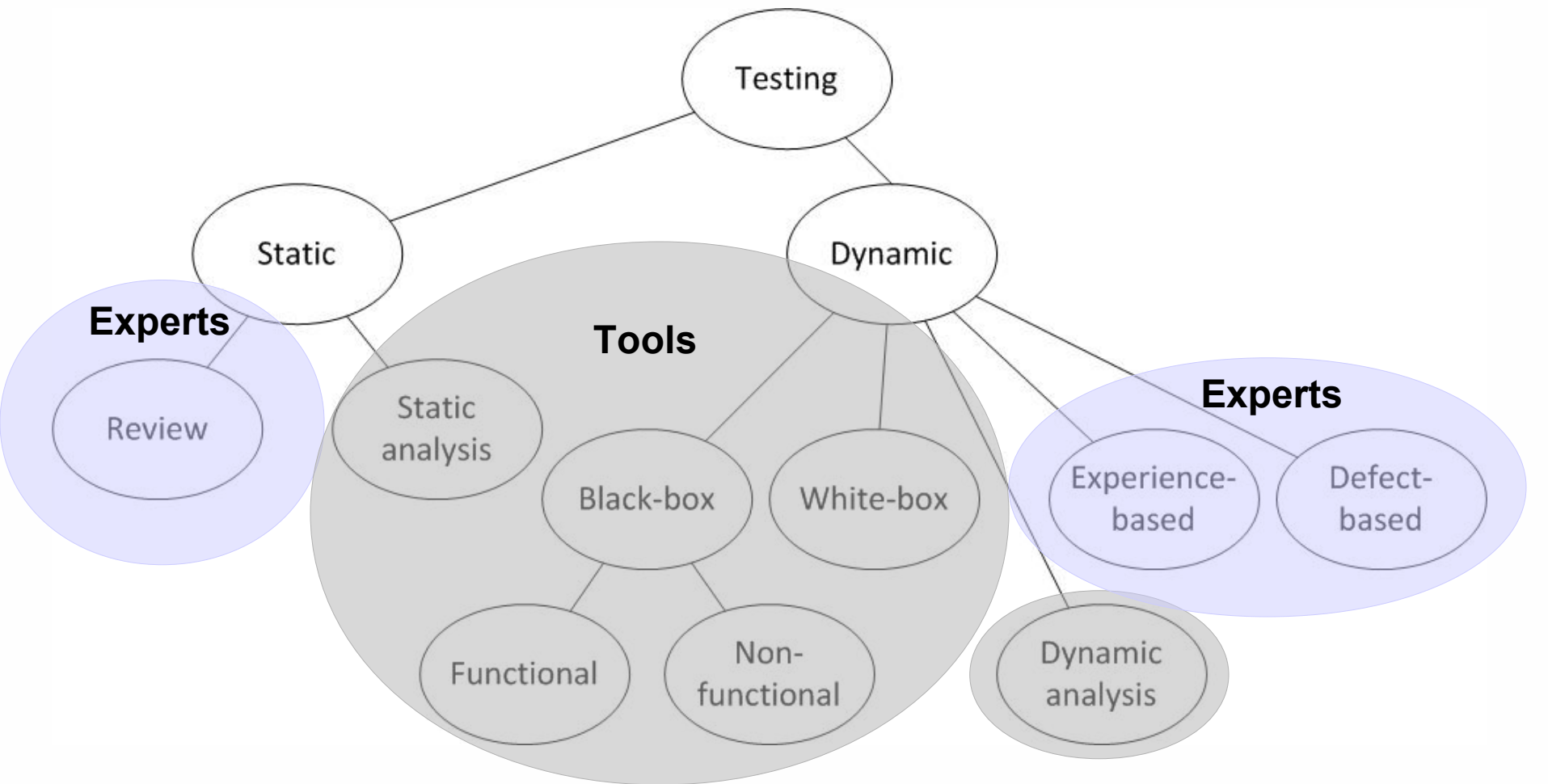
- No tool achieved 100%, No open-source tool achieved over 50%



# 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://scrumforteamssystem.com>  
<http://msdn.microsoft.com/en-us/security/dd670265.aspx>  
[http://news.cnet.com/8301-13505\\_3-10218777-16.html](http://news.cnet.com/8301-13505_3-10218777-16.html)  
[http://en.wikipedia.org/wiki/Rational\\_Application\\_Developer#Criticisms](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://weblogs.java.net/blog/inder/archive/2007/01/fortifying_web.html)  
[http://www.owasp.org/index.php/Man\\_vs.\\_Code](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