Innovate2011
The Rational Software Conference
11th and 12th of October
Let's build a smarter planet.

Strategies to Ensure Applications are Secure by Design

Simon Norrington
IBM Rational Quality Management

Agenda

- **What happens when applications are not secure?**
- **How are applications not secure?**
- SQL Injection
- Cross Site Scripting (XSS)
- **How do we address Web Application Security?**
- **The mindset for Web Application Security**
- Rational Requirements Composer
- Rational Team Concert
- Rational Quality Manager
- Rational AppScan family
- **Beyond Rational, IBM’s Commitment and Investment in Security**

Hacked: *When Things are Not Secure by Design*

The Reliable Times Daily

Popular Gaming Console Company Sued by Customer for $6.6 M Over Security Breach and Data Theft

Daily

Fun Games Corp. network entertainment unit was sued by a customer claiming it failed to protect users' personal information and credit card data that the company says been stolen by a hacker.

The Post t

Company Found Negligent Over Security Breach

State Appeal Court issued ruling which found ABC Motors Corp. was negligent over a security breach…

Hacked By S|A|M|E|T & ▫ bax-bbs - Mozilla Firefox
File Edit View History Bookmarks Tools Help
[redacted]
Google
Hacked By S|A|M|E|T & ׀ bax-bbs
HackeD
Done

CKED BY S|A|M|E|T

I AM S|A|M|E|T(PERSIAN BOY)

SAMET & BAX-BBS TEAM

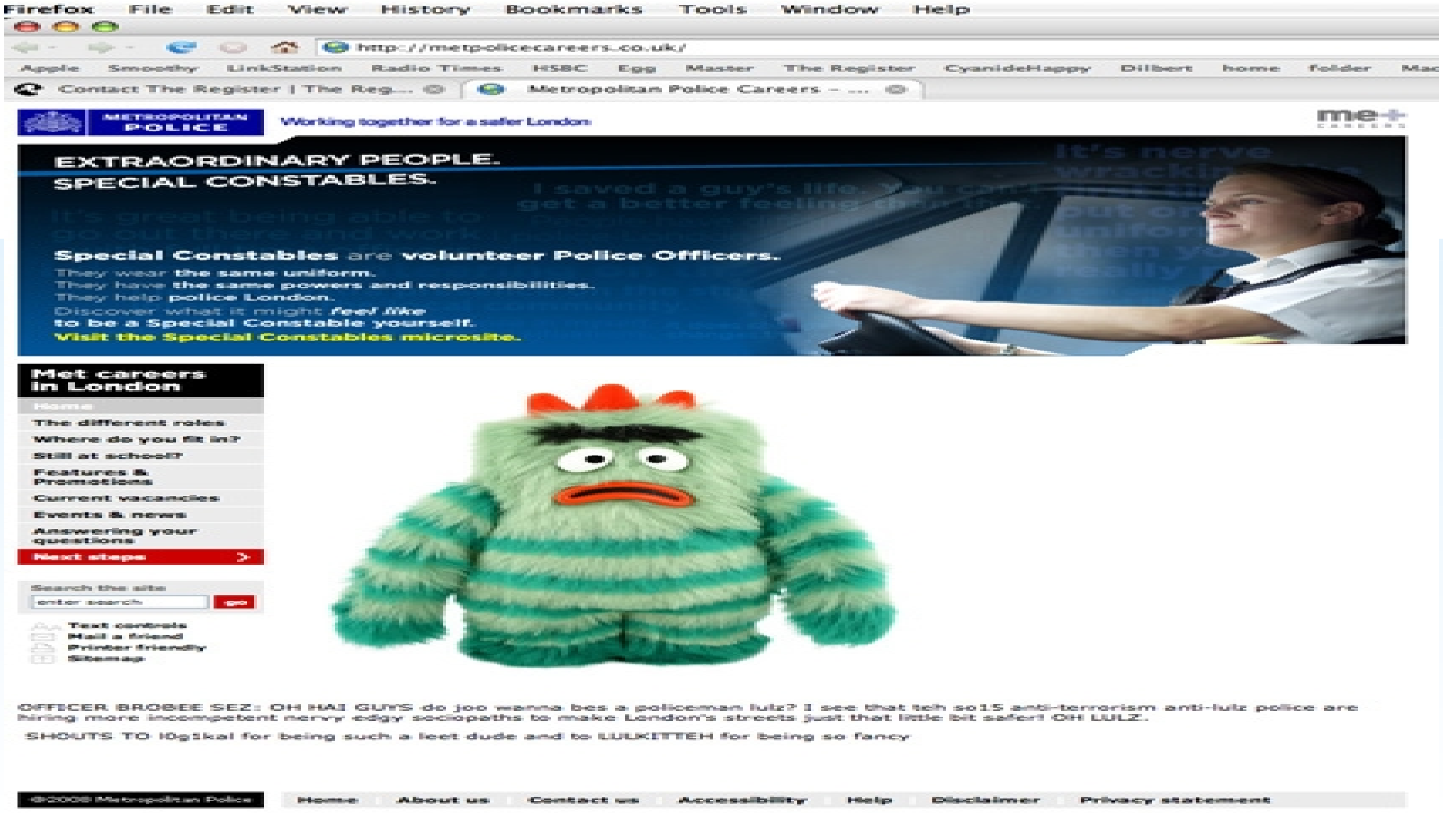
EMAIL: iran_boy_lovely@YAHOO.COM

How could this have been prevented?

Sony: 19 compromises April 26 – June 11, 2011

When?	Site	How?	What?	Who?
26-Apr-11	PlayStaion Network (PSN)	[unknown]	77 million customer profiles. Unknown number of credit cards.	[unknown]
2-May-11	Sony Online Entertainment (SOE)	[unknown]	24.6 million customer profiles. 12,700 credit card numbers. 10,700 direct debit cards.	[unknown]
7-May-11	products.sel.sony.com sweepstakes	Google	2,500 names and addresses of sweepstakes entrants.	Sony
17-May-11	PSN Password Reset	Application Logic Flaw	With this vulnerability, an attacker has the ability to change a user's password using only their account's email and date of birth. Rumors suggest it was being exploited by bad guys.	[unknown]
20-May-11	Sony Thailand	[unknown]	A phishing site was found on the server, indicating evidence of intrusion. Most likely vectors include patch management or web server configuration.	[unknown]
21-May-11	So-Net Entertainment Subsidiary	Login brute-force attack	128 accounts were drained of "virtual cash"	[unknown]
21-May-11	Sony Music Indonesia	[unknown]	Site defaced.	k4L0ng666
22-May-11	Sony BMG Greece	SQL Injection	8,500 customer profiles. Data posted publicly.	b4d_vipera
23-May-11	Sony Music Japan	SQL Injection	Databases compromised, but no user data published.	LulzSec
24-May-11	Sony Ericsson Canada	SQL Injection	2,000 email addresses, passwords, and names compromised. 1,000 of those were publicly posted.	Idahc
2-Jun-11	Sony Pictures	SQL Injection	1 million user records, ~3.575 million music codes and coupons.	LulzSec
2-Jun-11	Sony BMG Belgium	SQL Injection	Unknown number of user accounts including usernames, email addresses, and cleartext passwords.	LulzSec
2-Jun-11	Sony BMG Netherlands	SQL Injection	Unknown number of user accounts including usernames, email addresses, and cleartext passwords.	LulzSec
3-Jun-11	Sony Europe	SQL Injection	120 names, phone numbers, and email addresses.	Idahc
5-Jun-11	Sony Pictures Russia	SQL Injection	All databases of Sony Pictures Russia claimed, later posted publicly.	[unknown]
6-Jun-11	Sony Computer Entertainment Developer Network (SCE Devnet)	[unknown]	Source code to SCE Devnet	LulzSec
6-Jun-11	Sony BMG	[unknown]	Internal network maps	LulzSec
8-Jun-11	Sony Portugal	SQL Injection	Customer email addresses	Idahc
8-Jun-11	My Sony Club (Sonisutoa)	Phishing	Through "spoofing", an attacker used 95 accounts to exchange online shopping coupons worth 278,000 points at Sonisutoa (My Sony Club), defrauding Sony of ~ 280,000 yen (~ US$3,500). Sony cannot confirm if e-mail addresses or passwords were leaked.	[unknown]

Closer to home…



Firefox File Edit View History Bookmarks Tools Window Help
http://metpolicecareers.co.uk/
Apple Smoothy LinkStation Radio Times HSBC Egg Master The Register CyanideHappy Dilbert home folder Mac
Contact The Register | The Reg...
Metropolitan Police Careers – ...
METROPOLITAN POLICE
Working together for a safer London
me+ CAREERS

EXTRAORDINARY PEOPLE.
SPECIAL CONSTABLES.

Special Constables are volunteer Police Officers.
They wear the same uniform.
They have the same powers and responsibilities.
They help police London.
Discover what it might *feel like*
to be a Special Constable yourself.
Visit the Special Constables microsite.

Met careers in London
Home
The different roles
Where do you fit in?
Still at school?
Features & Promotions
Current vacancies
Events & news
Answering your questions
Next steps
Search the site
enter search
go
Text controls
Mail a friend
Printer friendly
Sitemap

OFFICER BROBEE SEZ: OH HAI GUYS do joo wanna bes a policeman lulz? I see that teh so15 anti-terrorism anti-lulz police are hiring more incompetent nervy edgy sociopaths to make London's streets just that little bit safer! OH LULZ.

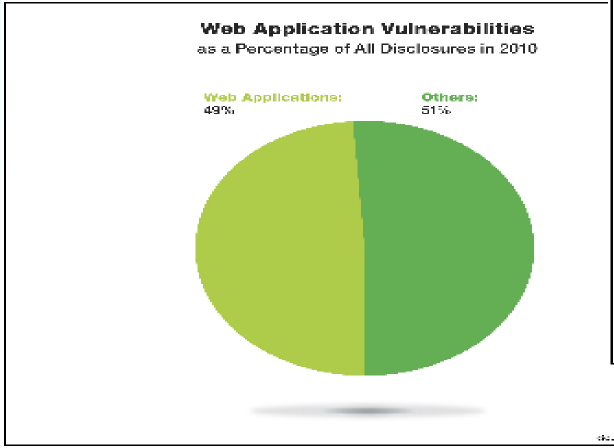
SHOUTS TO l0g1kal for being such a leet dude and to LULKITTEH for being so fancy

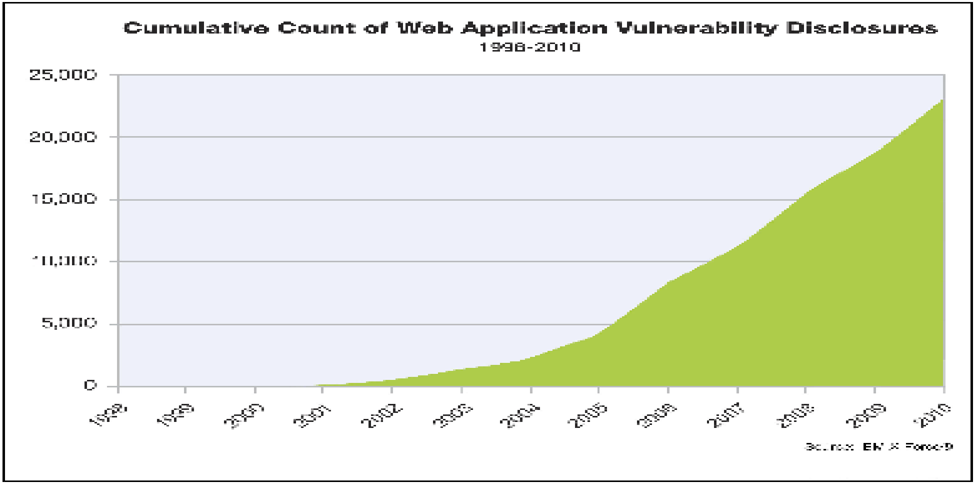
©2008 Metropolitan Police

Home About us Contact us Accessibility Help Disclaimer Privacy statement

Application Vulnerabilities Continue to Grow

- **Web application vulnerabilities represent the largest category in vulnerability disclosures**
- **49% of all vulnerabilities were Web application vulnerabilities**
- **SQL injection and Cross-Site Scripting are neck and neck in a race for top spot**

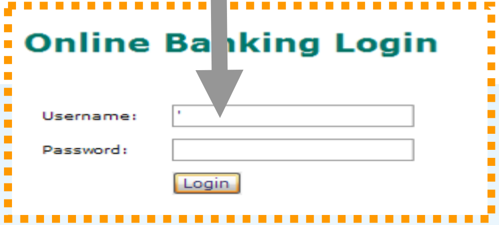




IBM Internet Security Systems
2010 X-Force® Trend & Risk Report

SQL Injection

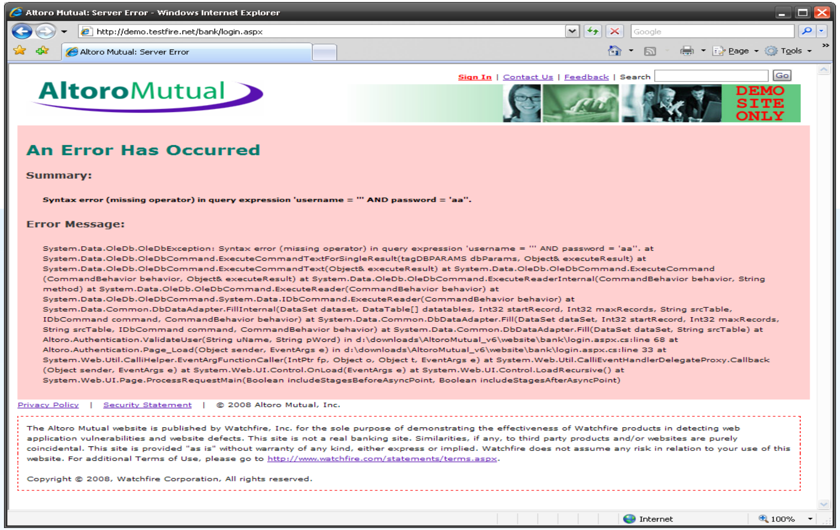
Put apostrophe into textbox



Online Banking Login

Username: '

Password:



Altoro Mutual: Server Error - Windows Internet Explorer
http://demo.testfire.net/bank/login.aspx
Google
Altoro Mutual: Server Error
Page
Tools
Sign In | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY
Internet
100%

An Error Has Occurred

Summary:

Syntax error (missing operator) in query expression 'username = ''' AND password = 'aa''.

Error Message:

```
System.Data.OleDb.OleDbException: Syntax error (missing operator) in query expression 'username = ''' AND password = 'aa''. at
System.Data.OleDb.OleDbCommand.ExecuteCommandTextForSingleResult(tagDBPARAMS dbParams, Object& executeResult) at
System.Data.OleDb.OleDbCommand.ExecuteCommandText(Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteCommand
(CommandBehavior behavior, Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteReaderInternal(CommandBehavior behavior, String
method) at System.Data.OleDb.OleDbCommand.ExecuteReader(CommandBehavior behavior) at
System.Data.OleDb.OleDbCommand.System.Data.IDbCommand.ExecuteReader(CommandBehavior behavior) at
System.Data.Common.DbDataAdapter.FillInternal(DataSet dataset, DataTable[] datatables, Int32 startRecord, Int32 maxRecords, String srcTable,
IDbCommand command, CommandBehavior behavior) at System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, Int32 startRecord, Int32 maxRecords,
String srcTable, IDbCommand command, CommandBehavior behavior) at System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, String srcTable) at
Altoro.Authentication.ValidateUser(String uName, String pWord) in d:\downloads\AltoroMutual_v6\website\bank\login.aspx.cs:line 68 at
Altoro.Authentication.Page_Load(Object sender, EventArgs e) in d:\downloads\AltoroMutual_v6\website\bank\login.aspx.cs:line 33 at
System.Web.Util.CalliHelper.EventArgFunctionCaller(IntPtr fp, Object o, Object t, EventArgs e) at System.Web.Util.CalliEventHandlerDelegateProxy.Callback
(Object sender, EventArgs e) at System.Web.UI.Control.OnLoad(EventArgs e) at System.Web.UI.Control.LoadRecursive() at
System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint)
```

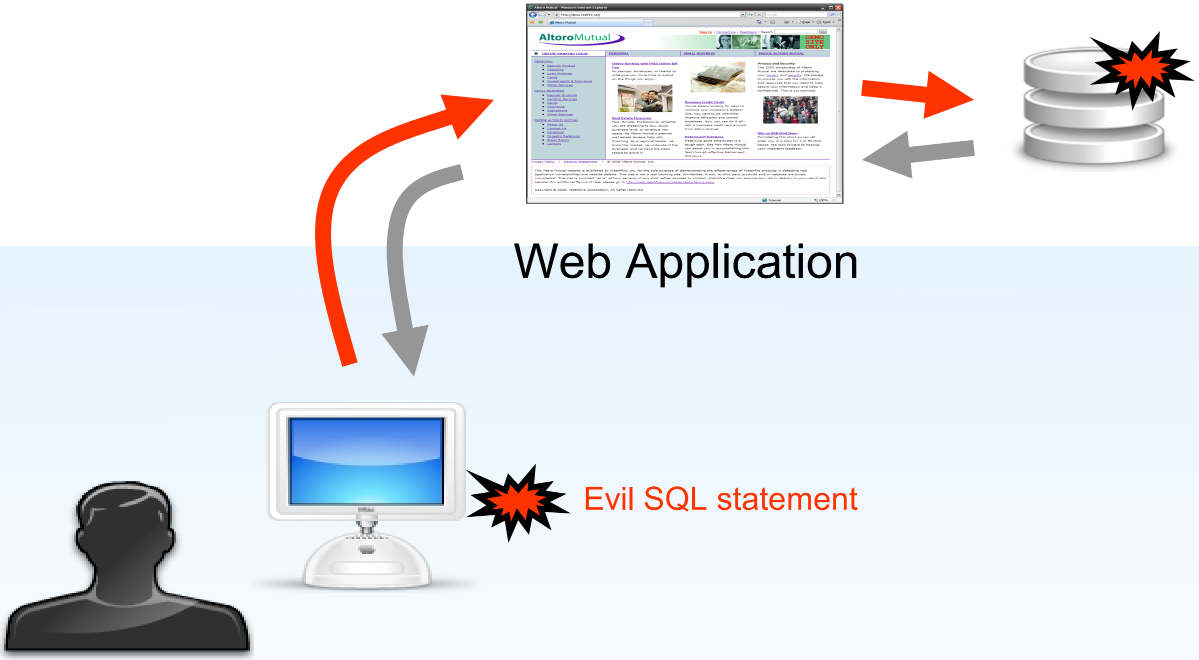
Privacy Policy | Security Statement | © 2008 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any risk in relation to your use of this website. For additional Terms of Use, please go to http://www.watchfire.com/statements/terms.aspx.

Copyright © 2008, Watchfire Corporation, All rights reserved.

Application responds with SQL error, suggesting to the attacker that string is being used to construct SQL query

SQL Injection



Web Application

Steal information;
Modify information;
Deface application;
Denial of Service

Evil SQL statement

Attacker

Altoro Mutual - Windows Internet Explorer

http://demo.testfire.net/

Altoro Mutual

AltoroMutual

Sign In | Contact Us | Feedback | Search

DEMO SITE ONLY

ONLINE BANKING LOGIN | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers

Online Banking with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.

Real Estate Financing
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it

Business Credit Cards
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.

Retirement Solutions
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.

Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

Win an 8GB iPod Nano
Completing this short survey will enter you in a draw for 1 of 50 iPod Nanos. We look forward to hearing your important feedback.

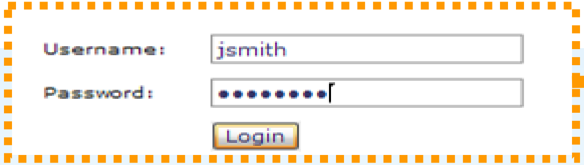
Privacy Policy | Security Statement | © 2008 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any risk in relation to your use of this website. For additional Terms of Use, please go to http://www.watchfire.com/statements/terms.aspx.

Copyright © 2008, Watchfire Corporation, All rights reserved.

SQL Injection in Code

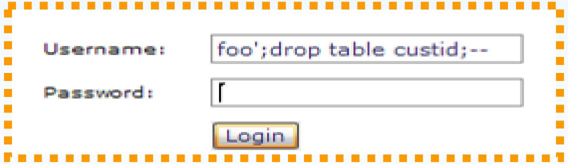
```
String query = “SELECT * FROM users WHERE name=‘” +
    userName + “’ AND pwd=‘” + pwd + “’”;
```



Username: jsmith

Password: ●●●●●●●●●

```
SELECT * FROM users WHERE name='jsmith' AND pwd='Demo1234'
```



Username: foo';drop table custid;--

Password:

Ouch!

Cross-Site Scripting (XSS)

What is it?

- Malicious script echoed back into HTML returned from a trusted site, and runs under trusted context

What are the implications?

- Session Tokens stolen (browser security circumvented)
- Complete page content compromised
- Future pages in browser compromised

Cross Site Scripting (XSS)

Online Banking with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.

Real Estate Financing
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it

Business Credit Cards
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.

Retirement Solutions
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.

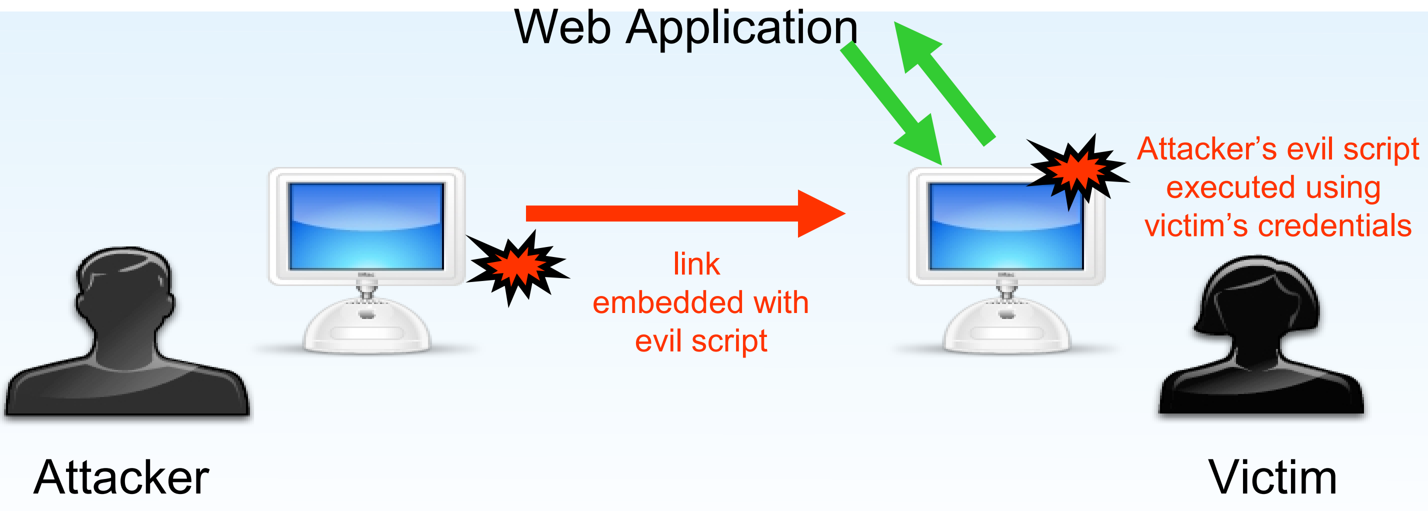
Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

Win an 8GB iPod Nano
Completing this short survey will enter you in a draw for 1 of 50 iPod Nanos. We look forward to hearing your important feedback.

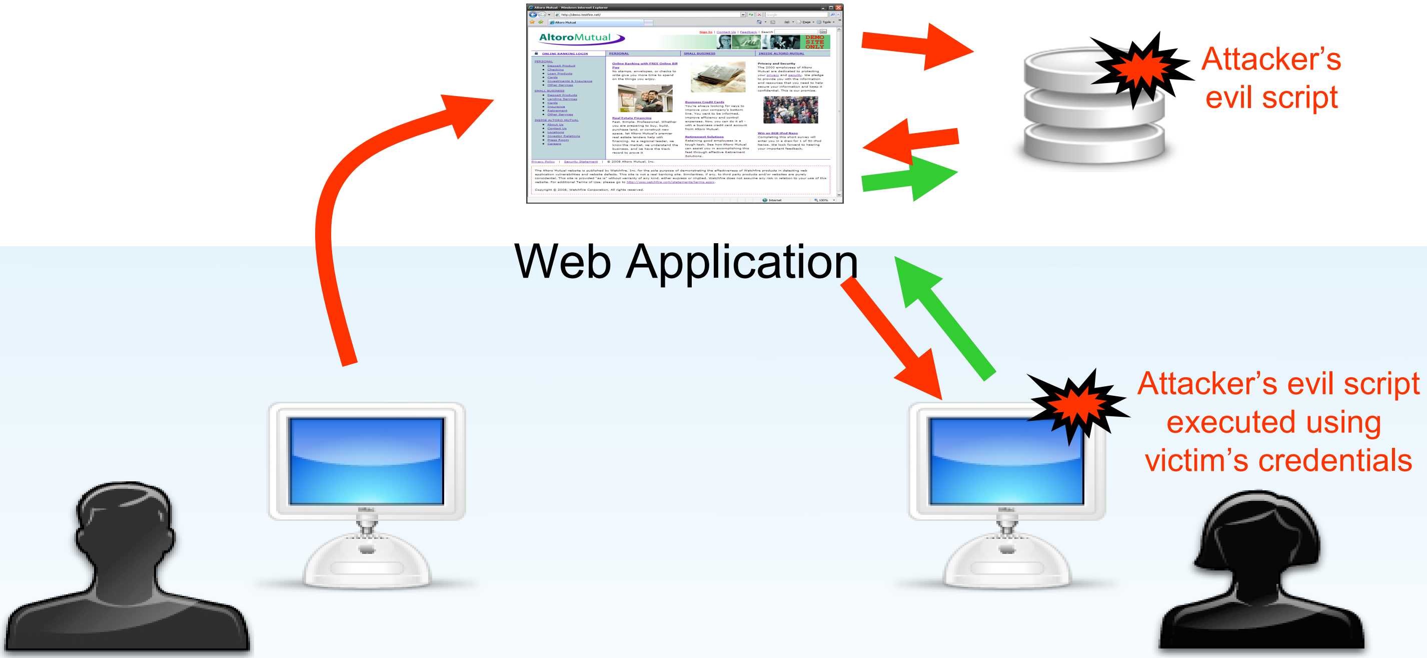
Privacy Policy | Security Statement | © 2008 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any risk in relation to your use of this website. For additional Terms of Use, please go to http://www.watchfire.com/statements/terms.aspx.

Copyright © 2008, Watchfire Corporation, All rights reserved.


Web Application
Attacker's evil script executed using victim's credentials
link embedded with evil script
Attacker
Victim

Stored XSS



Attacker's evil script

Web Application

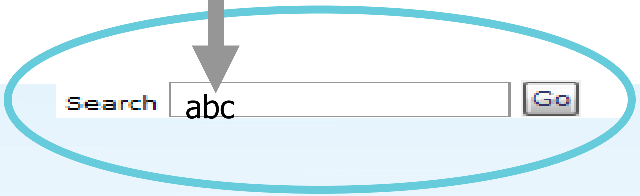
Attacker's evil script executed using victim's credentials

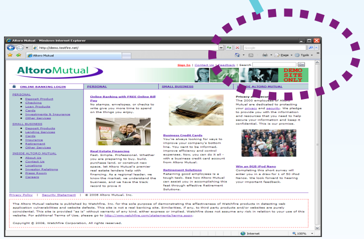
Attacker

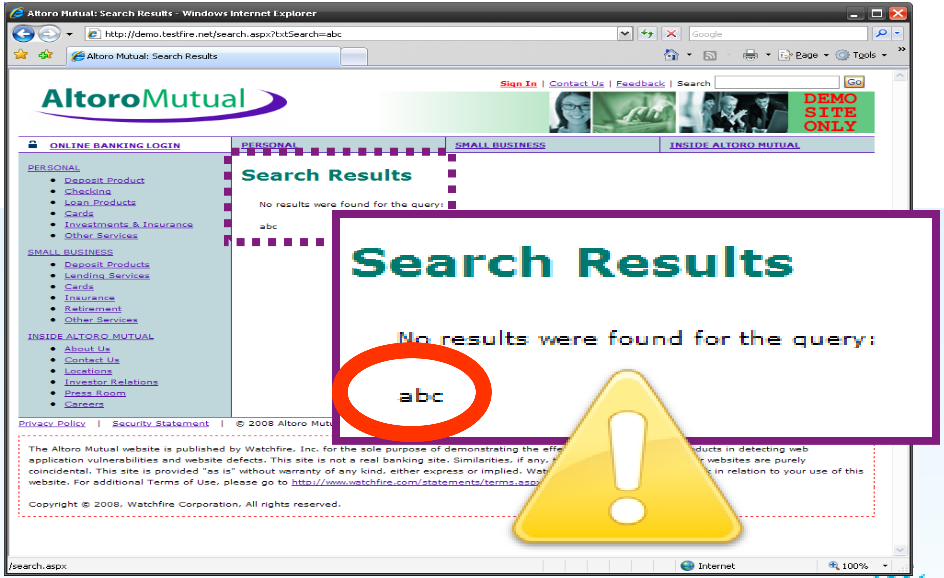
Victim

Checking for XSS

Input some text into textbox







Search Results

No results were found for the query:

abc

Search Results

No results were found for the query:

abc

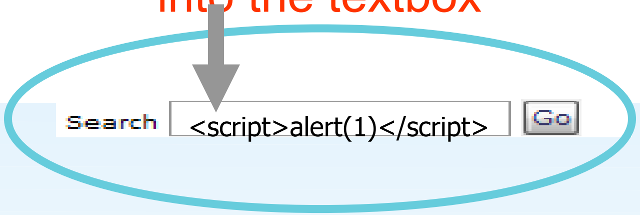
The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effe ducts in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. Wat in relation to your use of this website. For additional Terms of Use, please go to http://www.watchfire.com/statements/terms.asp

Copyright © 2008, Watchfire Corporation, All rights reserved.

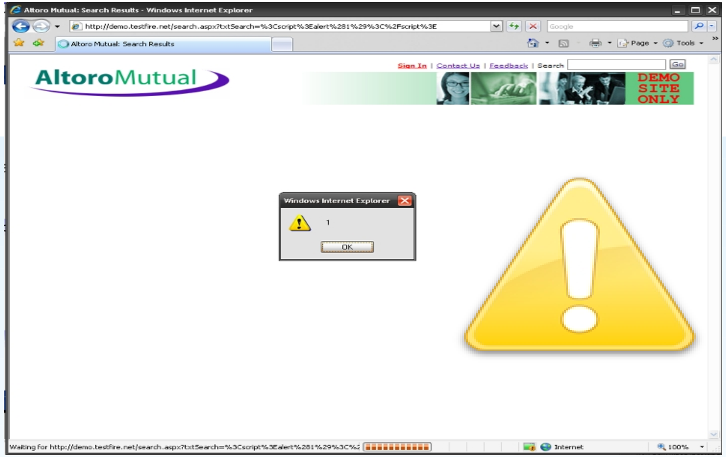
- The warning sign:
  User input embedded in HTML response

Checking for XSS (cont.)

Put an evil JavaScript into the textbox



<script>alert(1)</script>



Altoro Mutual: Search Results - Windows Internet Explorer
Altoro Mutual: Search Results
Page
Tools
Sign In | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY
Windows Internet Explorer
OK
Internet
100%

http://demo.testfire.net/search.aspx?txtSearch=%3Cscript%3Ealert%281%29%3C%2Fscript%3E

1

Waiting for http://demo.testfire.net/search.aspx?txtSearch=%3Cscript%3Ealert%281%29%3C%2

- Evil script was executed by browser
- Cause: Application did not apply HTML encoding
- Link containing this script could be sent to victim

The Application Security Challenge

What?

Need to mitigate the risk **of a Security breach**

Need to find **and** remediate **these vulnerabilities**

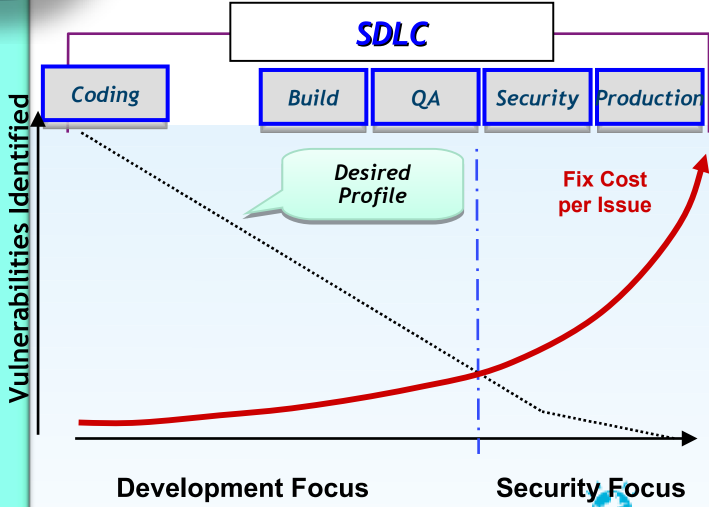
Must utilize a cost effective **way of doing this that makes sense**

Who?

Software security represents the intersection between security & development **– solution needs to be a joint collaboration**

Starts with Security Auditor (can also be outsourced)

Larger organizations require the scaling of security testing into the development organization



Drivers for Application Security

Increase in vulnerability reports and hacking incidents

- Application security has become the top threat

Regulatory Compliance

- Requirements such as PCI, HIPAA, GLBA, etc.

User demand

- For rich applications is pushing development to advanced code techniques; Web 2.0 introduces additional threats

Enterprise Modernization

- Driving traditional applications to online world (SOA), increasing corporate risk

Cost cutting

- Demands increased efficiencies

Point solutions fail to address full the problem

Vulnerability scanners (Network Scanners)

- Traditional vulnerability scanners don’t cover Web applications

Penetration testing

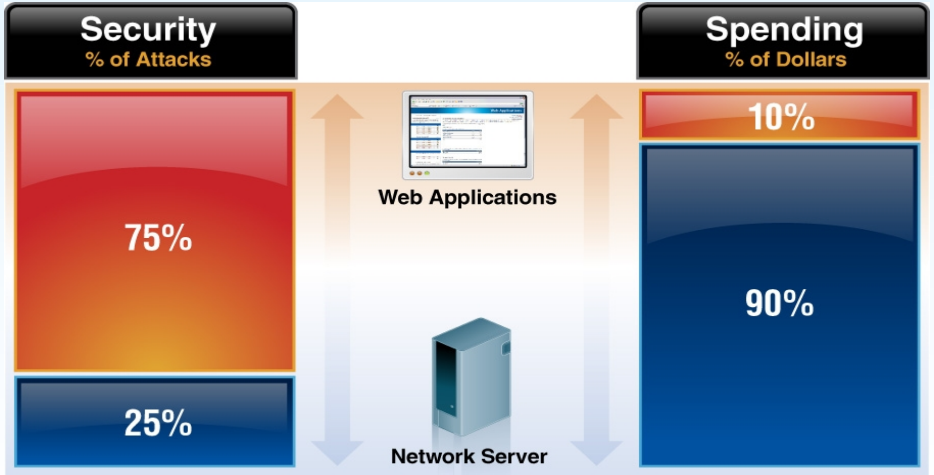
- Effective at finding vulnerabilities but not scalable for ongoing tests
- Not focused on remediation

Network firewall and IPS

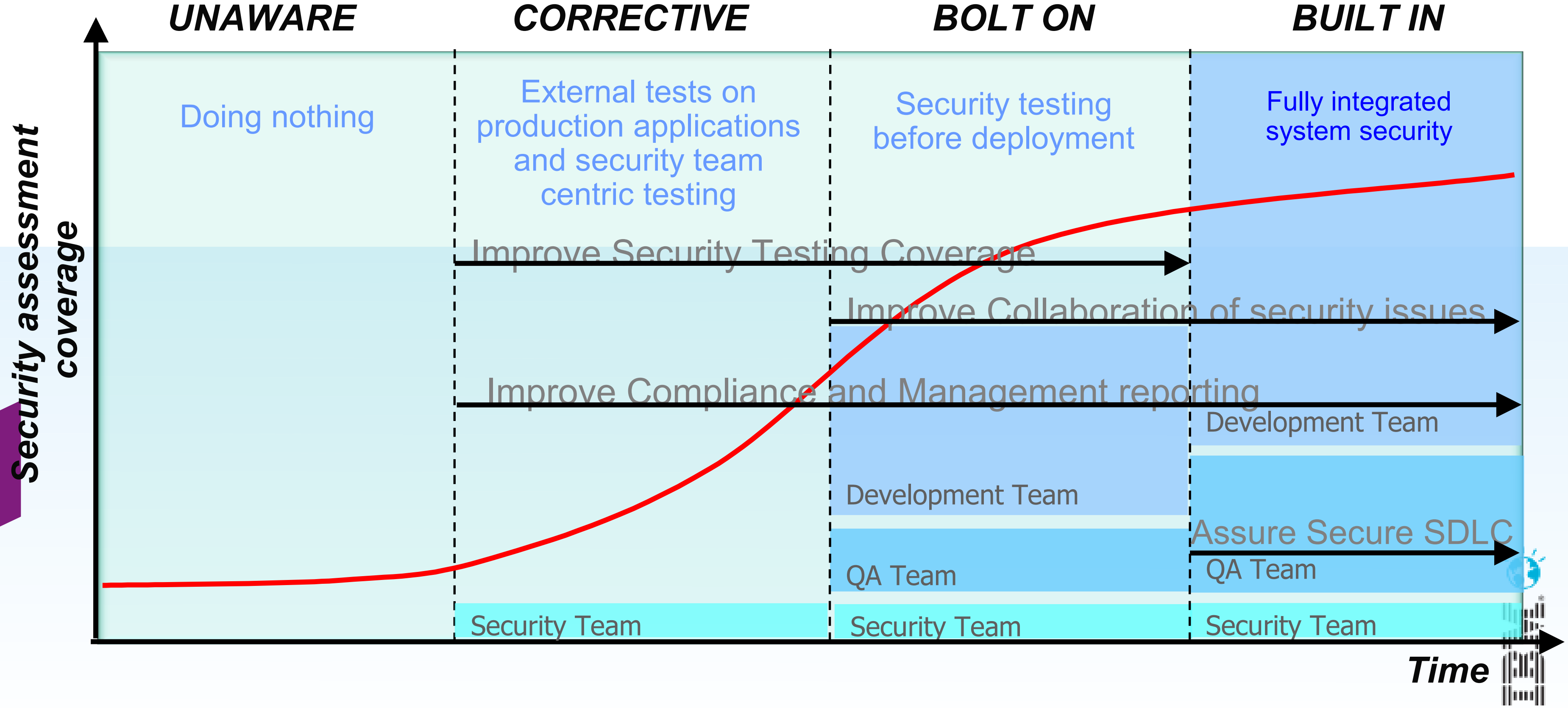
- Generic Web application protection (if any) so most custom Web applications not covered
- Most IPS solutions focus on exploits as opposed to Web application vulnerabilities

Web application firewall

- Can be effective, but difficult to deploy, tune and manage
- Does not address the root cause of identified problems
- Building policies can be as time consuming as remediating the vulnerability



Application Security Maturity Model


UNAWARE
CORRECTIVE
BOLT ON
BUILT IN
Security assessment coverage
Doing nothing
External tests on production applications and security team centric testing
Security testing before deployment
Fully integrated system security
Improve Security Testing Coverage
Improve Collaboration of security issues
Improve Compliance and Management reporting
Development Team
Development Team
Assure Secure SDLC
QA Team
QA Team
Security Team
Security Team
Security Team
Time

Make Applications Secure, by Design

Security as an Intrinsic Property of the Development Process

Design Phase

- Consideration is given to security requirements of the application
- Issues such as required controls and best practices are documented on par with functional requirements

Development Phase

- Software is checked during coding for:
  - Implementation error vulnerabilities
  - Compliance with security requirements

Build & Test Phase

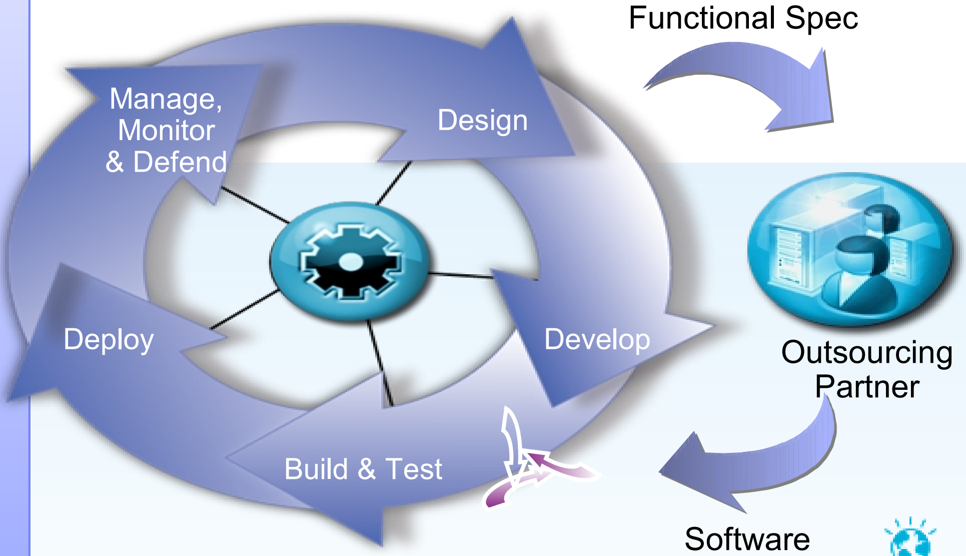
- Testing begins for errors and compliance with security requirements across the entire application
- Applications are also tested for exploitability in deployment scenario

Deployment Phase

- Configure infrastructure for application policies
- Deploy applications into production

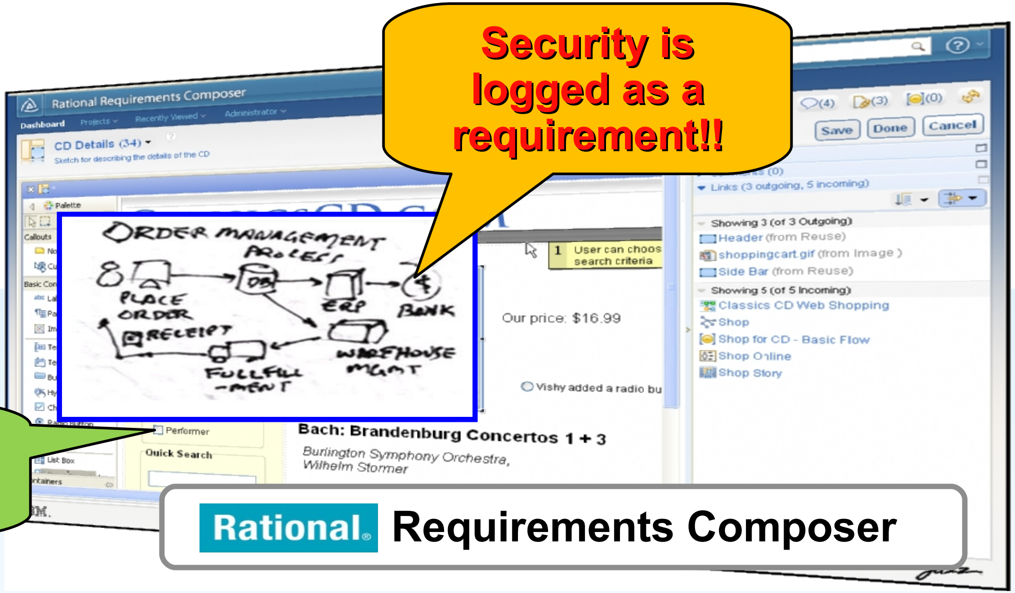
Operational Phase

- Continuously monitor applications for appropriate application usage, vulnerabilities and defend against attacks



A Secure by Design Universe: *Secure Requirements*

Project stakeholders gather information



Security is logged as a requirement!!

Requirements logged into Rational Requirements Composer

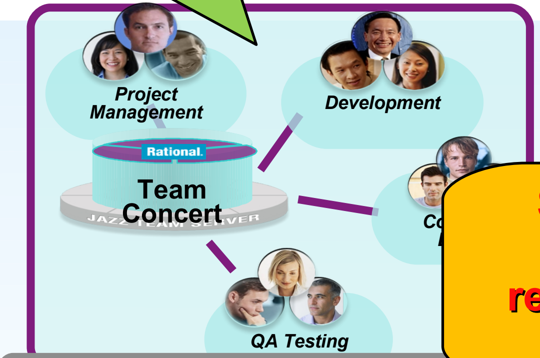
Rational. Requirements Composer

IBM's Secure Engineering Framework Redbook is used as a security guide

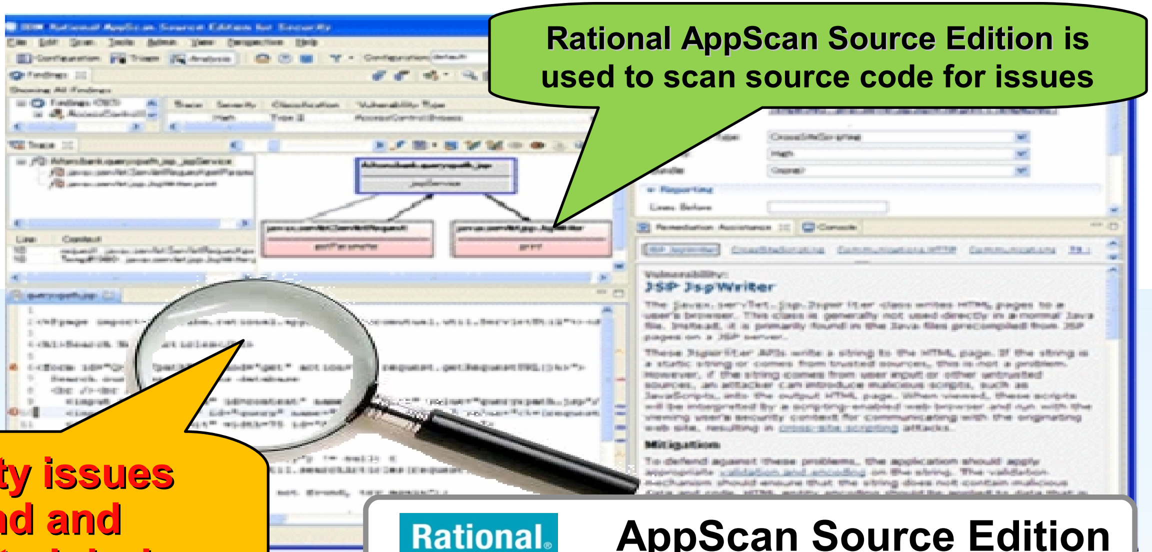
- Threat models are built and security requirements are added
- A security "champion" is appointed for the project

A Secure by Design Universe: *Secure Development*

Stories, tasks and defects logged in Rational Team Concert
- Security controls are added as stories / tasks



Rational. Team Concert



Rational AppScan Source Edition is used to scan source code for issues

Rational. AppScan Source Edition

Security issues found and remediated during development!!

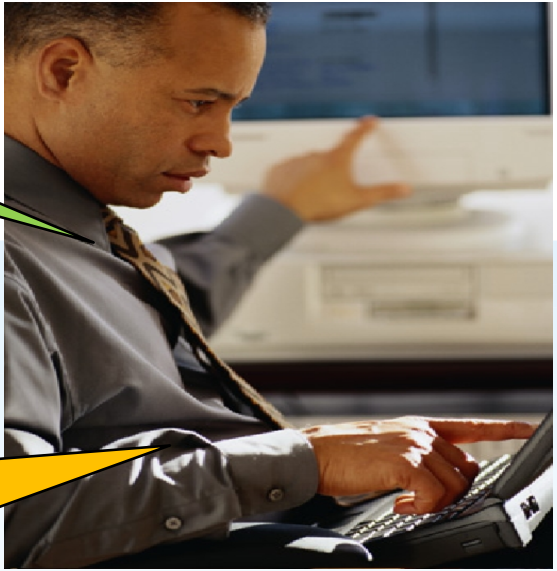
Rational AppScan Build Edition is used during the nightly builds

Rational. AppScan Build Edition

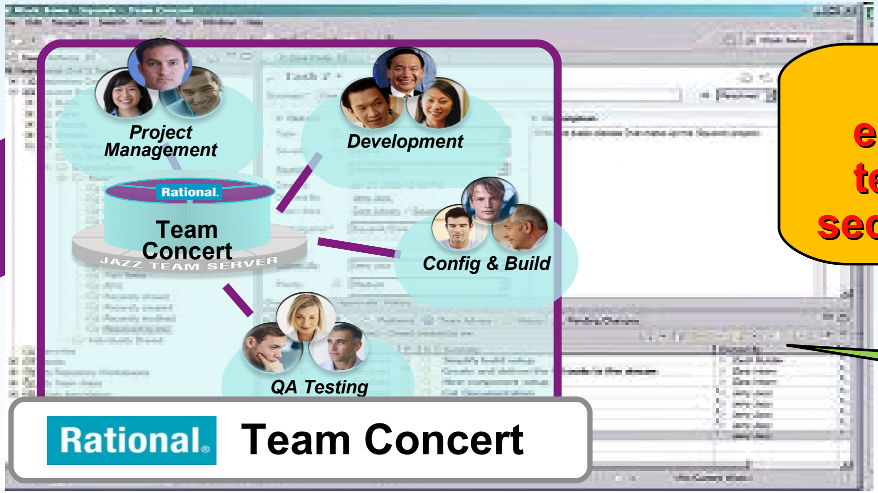
A Secure by Design Universe: *Secure QA Testing*

QA team educated on application security and tools

QA teams build test plans for functional, UI and security controls



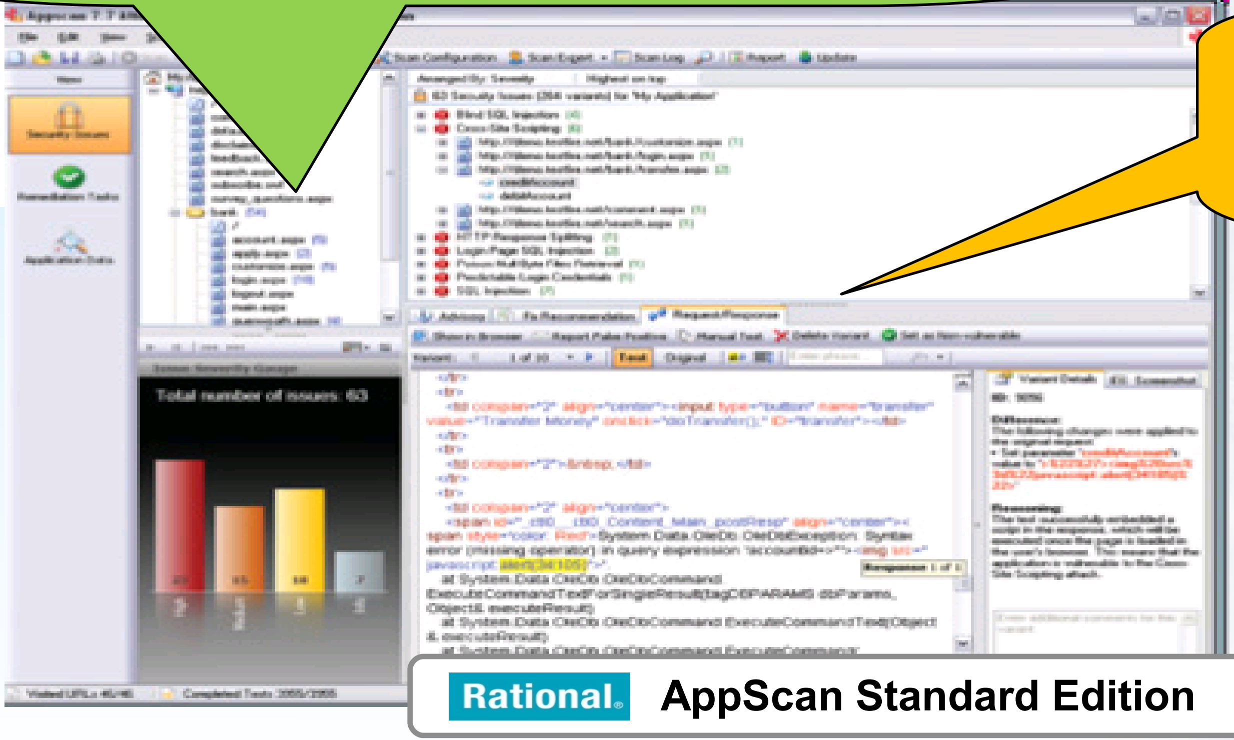
Security educated QA team detects security issues!!



QA team locates functional, UI and security defects and logs them into Rational Team Concert

A Secure by Design Universe: *Secure Deployment*

Rational AppScan Standard Edition is used to verify application prior to deployment



63 Security Issues (264 variants) for 'My Application'

- Blind SQL Injection
- Cross-Site Scripting
  - http://demo.testfire.net/bank/customize.aspx
  - http://demo.testfire.net/bank/login.aspx
  - http://demo.testfire.net/bank/transfer.aspx
    - creditAccount
    - debitAccount
  - http://demo.testfire.net/comment.aspx
  - http://demo.testfire.net/search.aspx
- HTTP Response Splitting
- Login Page SQL Injection
- Poison Null Byte Files Retrieval
- Predictable Login Credentials
- SQL Injection

Total number of issues: 63

Infrastructure issues in underlying platforms are found and patched!!

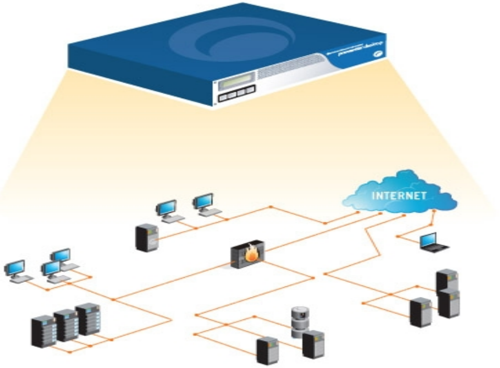
Rational. AppScan Standard Edition

How does Rational AppScan work?

Automates Application Security Testing

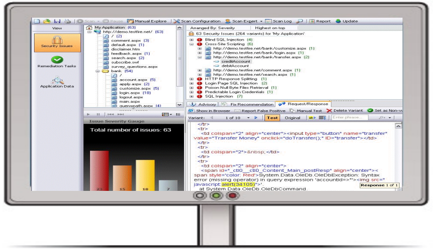
Same process for whitebox & blackbox

Scan applications



Analyze

(identify issues)



```
My Application (63)
  http://demo.testfire.net/ (63)
    / (2)
    comment.aspx (3)
    default.aspx (1)
    disclaimer.htm
    feedback.aspx (1)
    search.aspx (2)
    subscribe.swf
    survey_questions.aspx
    bank (54)
      /
      account.aspx (5)
      apply.aspx (2)
      customize.aspx (5)
      login.aspx (18)
      logout.aspx
      main.aspx
      queryxpath.aspx (4)
```

Total number of issues: 63

```
Arranged By: Severity    Highest on top
63 Security Issues (264 variants) for 'My Application'
  Blind SQL Injection (4)
  Cross-Site Scripting (6)
    http://demo.testfire.net/bank/customize.aspx (1)
    http://demo.testfire.net/bank/login.aspx (1)
    http://demo.testfire.net/bank/transfer.aspx (2)
      creditAccount
      debitAccount
    http://demo.testfire.net/comment.aspx (1)
    http://demo.testfire.net/search.aspx (1)
  HTTP Response Splitting (1)
  Login Page SQL Injection (2)
  Poison Null Byte Files Retrieval (1)
  Predictable Login Credentials (1)
  SQL Injection (7)
```

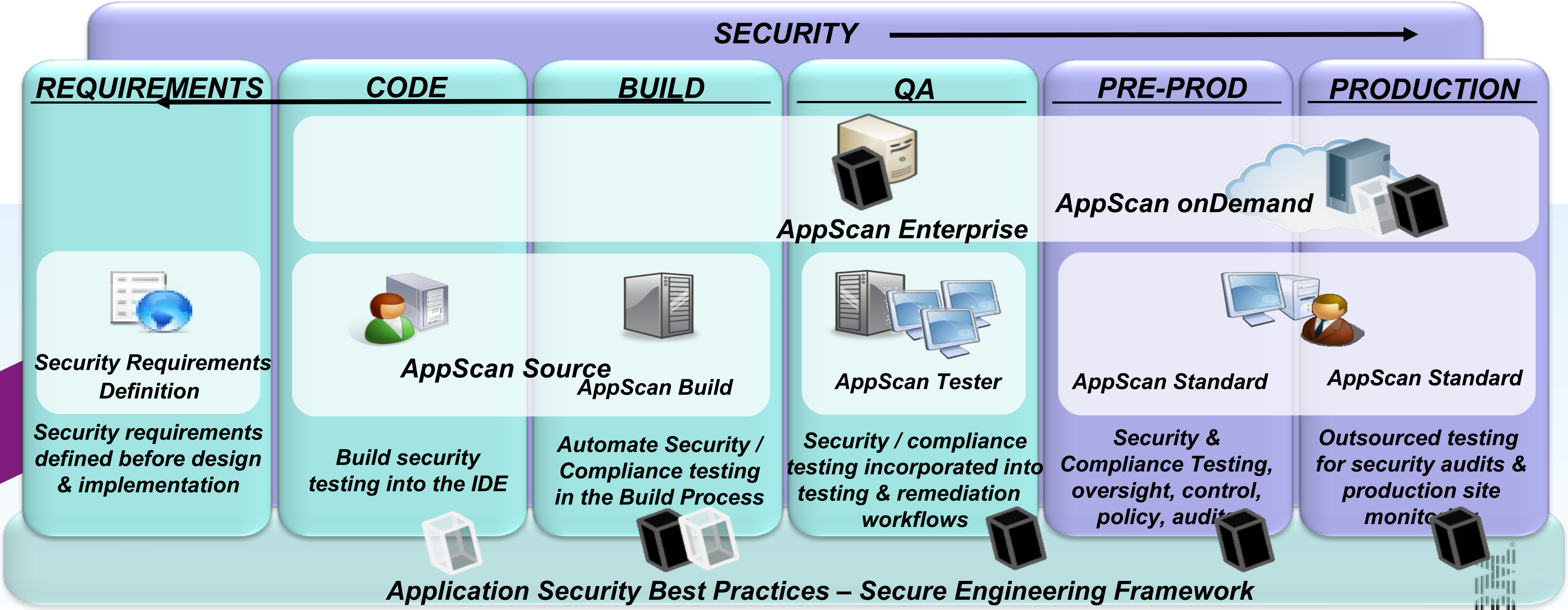
```
  </tr>
  <tr>
    <td colspan="2" align="center"><input type="button" name="transfer"
value="Transfer Money" onclick="doTransfer();" ID="transfer"></td>
  </tr>
  <tr>
    <td colspan="2">&nbsp;</td>
  </tr>
  <tr>
    <td colspan="2" align="center">
    <span id="_ctl0__ctl0_Content_Main_postResp" align="center"><
span style='color: Red'>System.Data.OleDb.OleDbException: Syntax
error (missing operator) in query expression 'accountid=>"><img src="
javascript:alert(34105)">'.
   at System.Data.OleDb.OleDbCommand.
```

Report

(detailed & actionable)

IBM Rational AppScan Suite

Comprehensive Application Vulnerability Management across SDLC



SECURITY

REQUIREMENTS

CODE

BUILD

QA

PRE-PROD

PRODUCTION

AppScan Enterprise

AppScan onDemand

Security Requirements Definition

AppScan Source

AppScan Build

AppScan Tester

AppScan Standard

AppScan Standard

Security requirements defined before design & implementation

Build security testing into the IDE

Automate Security / Compliance testing in the Build Process

Security / compliance testing incorporated into testing & remediation workflows

Security & Compliance Testing, oversight, control, policy, audit

Outsourced testing for security audits & production site monito

Application Security Best Practices – Secure Engineering Framework

Dynamic Analysis/Blackbox – ■

Static Analysis/Whitebox - □

Integration Across the Development Lifecycle

Institutionalize Secure by Design with IBM Rational

Rational

Rational ClearQuest

AppScan Enterprise, Source, Standard
Push security defects

Rational Application Developer

AppScan Source
Run scans and view results in RAD (for developers)

Rational Build Forge

AppScan Build, Source
Run static & dynamic scans during build time

Rational Team Concert

AppScan Enterprise, Source Push security defects

Rational Quality Manager

AppScan Enterprise, Source, Test
Push security defects & kick-off AppScan Test edition

WebSphere

WebSphere Portal

AppScan Enterprise
Automatic scan of portal-based applications (through remote REST APIs for URL decoding)

WebSphere Commerce

AppScan Enterprise, Standard
pre-defined scan templates tailored for WSC applications

Tivoli

ISS VPS

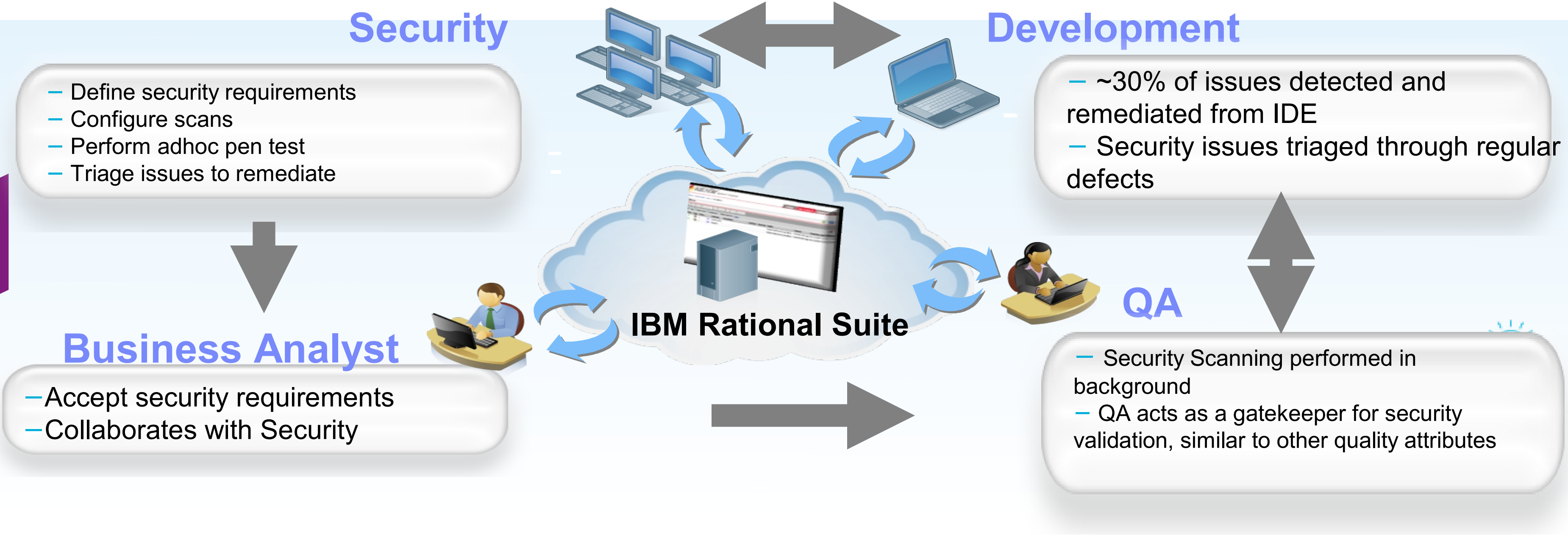
AppScan Standard
Malware scanning for web applications provided by ISS VPS & OrangeFilter API

Productivity: Enabling a Quantum Leap

Security testing and collaborative workflows reduce risk BUT do not create value

- Application security must evolve to go beyond testing and mitigation
- Ex: Quality Management does not begin and end with functional or performance testing

Secure By Design: Confidence to Innovate by Reducing Security Risks



Security

- Define security requirements
- Configure scans
- Perform adhoc pen test
- Triage issues to remediate

Development

- ~30% of issues detected and remediated from IDE
- Security issues triaged through regular defects

IBM Rational Suite

Business Analyst

- Accept security requirements
- Collaborates with Security

QA

- Security Scanning performed in background
- QA acts as a gatekeeper for security validation, similar to other quality attributes

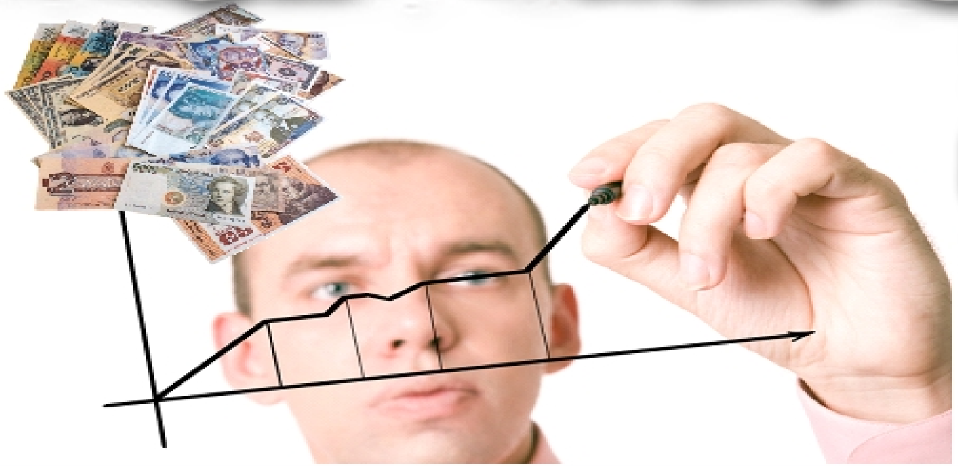
A Secure by Design Universe: *The Success Story*

The Reliable Times Daily

Daily

Hackers Foiled! Popular Gaming Console Company Reputation Soars

Earlier this week, hackers attempted to locate security issues in Fun Games Corp. network entertainment unit online gaming application, but failed due to security controls in place. Consumer confidence and profits soar…



The Post t

No News is Good News

Another boring news week with no security breaches to report for ABC Motors Corp.

IBM Rational Solutions Institutionalize Secure by Design!

Maintaining Application Security Leadership

IBM Advanced Security Research

Understand New Threats

- Stay ahead of web threats related to Rich Internet Applications – HTML5, etc.
- Scanning mapped to OWASP & WASC threat classes

Threat Modeling for New Attack Vectors

- Mobile applications
- Packaged applications
- Embedded systems
- Cloud-based platforms

Deliver Precise Results

- Actionable results
- Trusted findings with supported data
- Correlation, Glassbox (runtime analysis), SAST feeding DAST

Application Security Analysis & Testing Technology

Dynamic **Static** **Hybrid**

IBM’s Commitment and Investment in Security

7,000,000,000+ security events managed daily

48,000+ vulnerabilities tracked in the IBM X-Force® research and development database

15,000 researchers, developers and subject matter experts on security initiatives

4,000+ customers managed in security operations centers around the world

3,000+ security & risk management patents

40+ years of proven success with security and virtualization on IBM System

IBM announces new IBM Security Systems division

www.ibm/software/rational