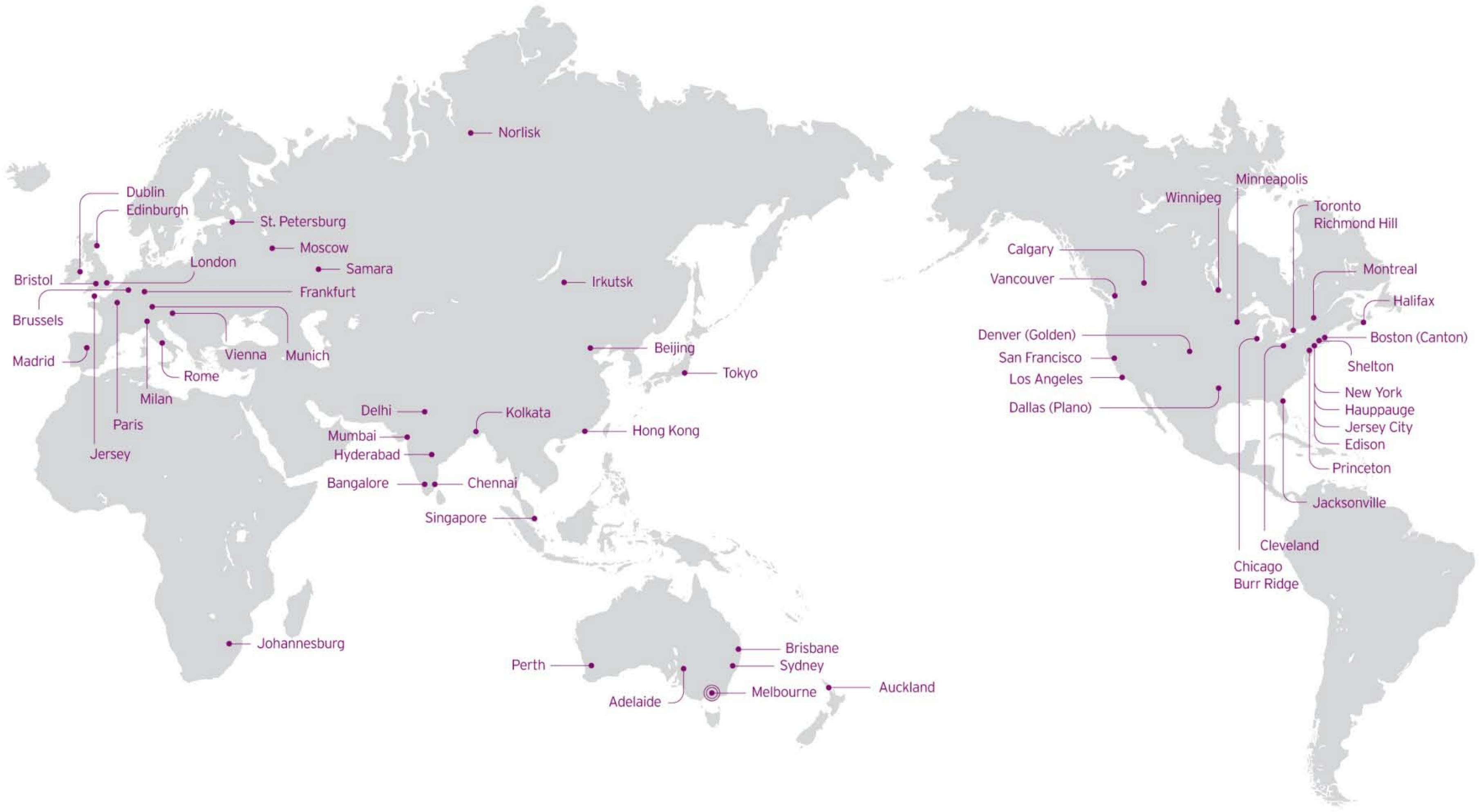
Using AppScan Enterprise to Gain Insight Into Your Company's Application Security.

John Paul Lonie, CISSP
4-6th August 2009
Innovation 2009 Conference

Agenda

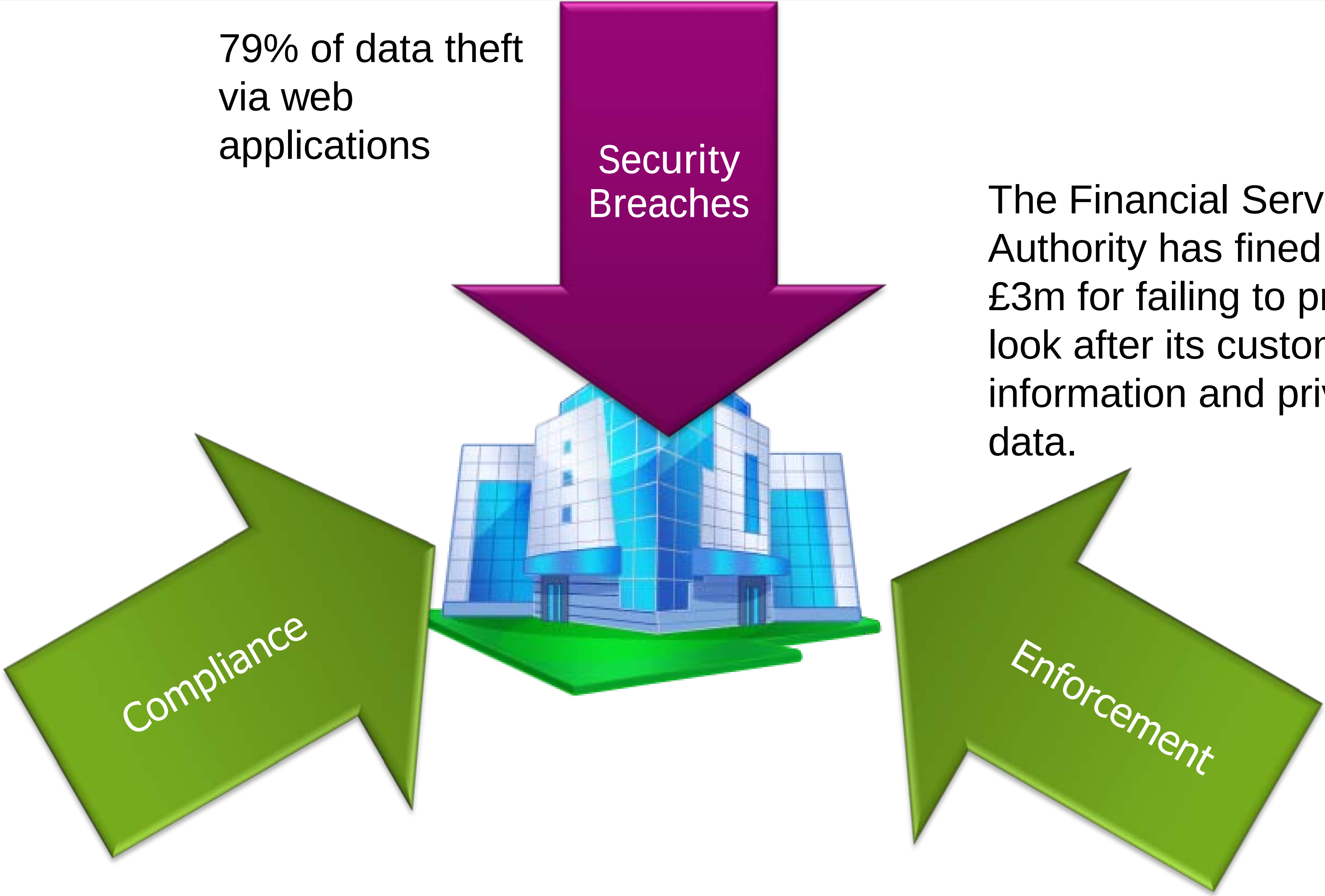
- About Computershare…
- Problem definition…
- Our solution…
- Outcomes…
- Questions?

Computershare is bigger than you think!



Web Application Security and Business Risk

79% of data theft via web applications

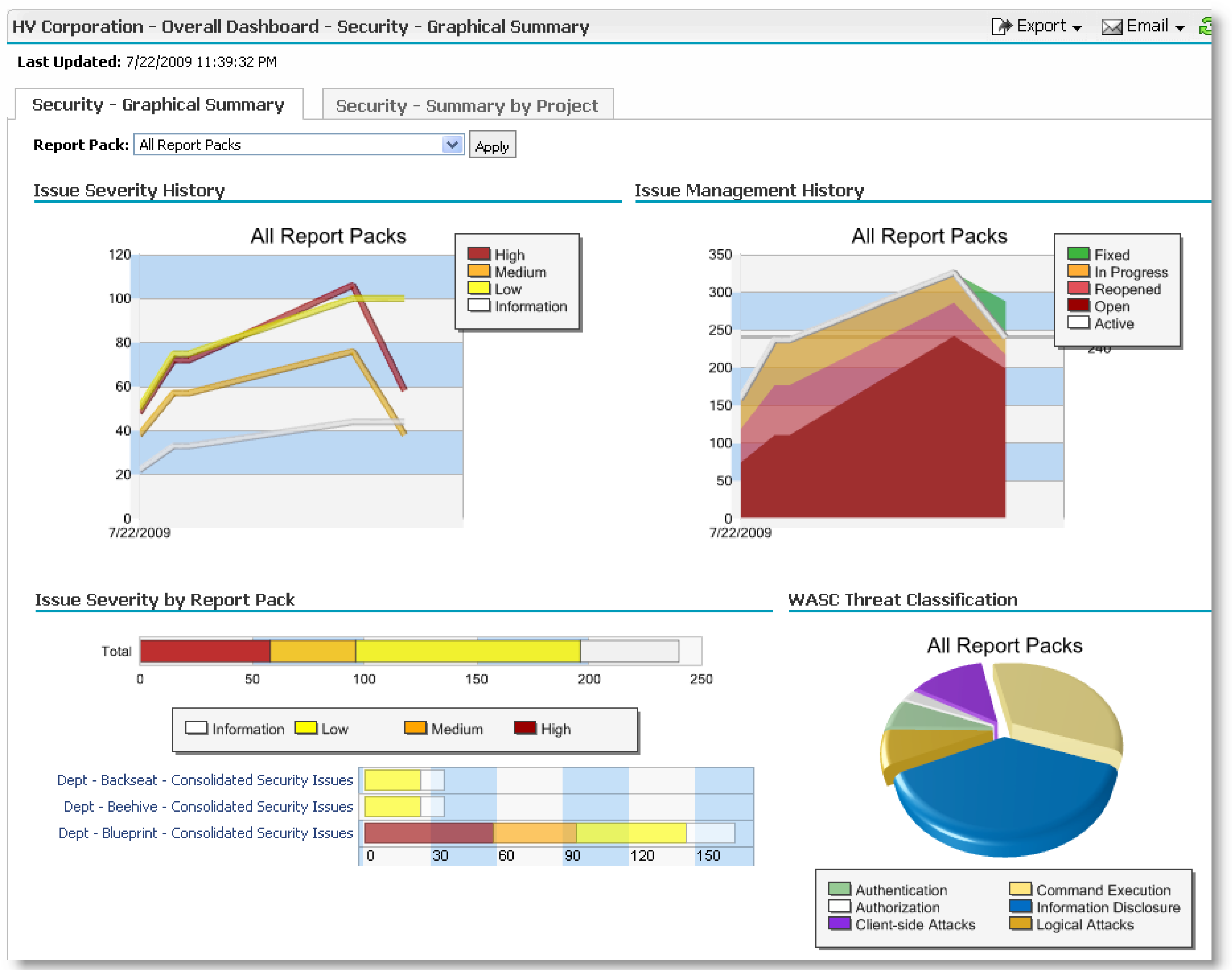


The Financial Services Authority has fined HSBC £3m for failing to properly look after its customers' information and private data.

Gaining insight into your application security - Goals

- Understand the security posture of all the web applications you know about and more importantly the ones you don’t.
- Be quick about it. 2-3 months; This isn't meant to be conclusive.
- Identify the CRITICAL issues and deal with them quickly.
- Store the information in order to track it and analyse it.
- Extract as much information from your findings as you can
- Identify what sites need further testing
- Provide ongoing process; Guidance for development.

Why use ASE ? - Corporate Summary



HV Corporation - Overall Dashboard - Security - Graphical Summary

Last Updated: 7/22/2009 11:39:32 PM

Security - Graphical Summary | Security - Summary by Project

Report Pack: All Report Packs

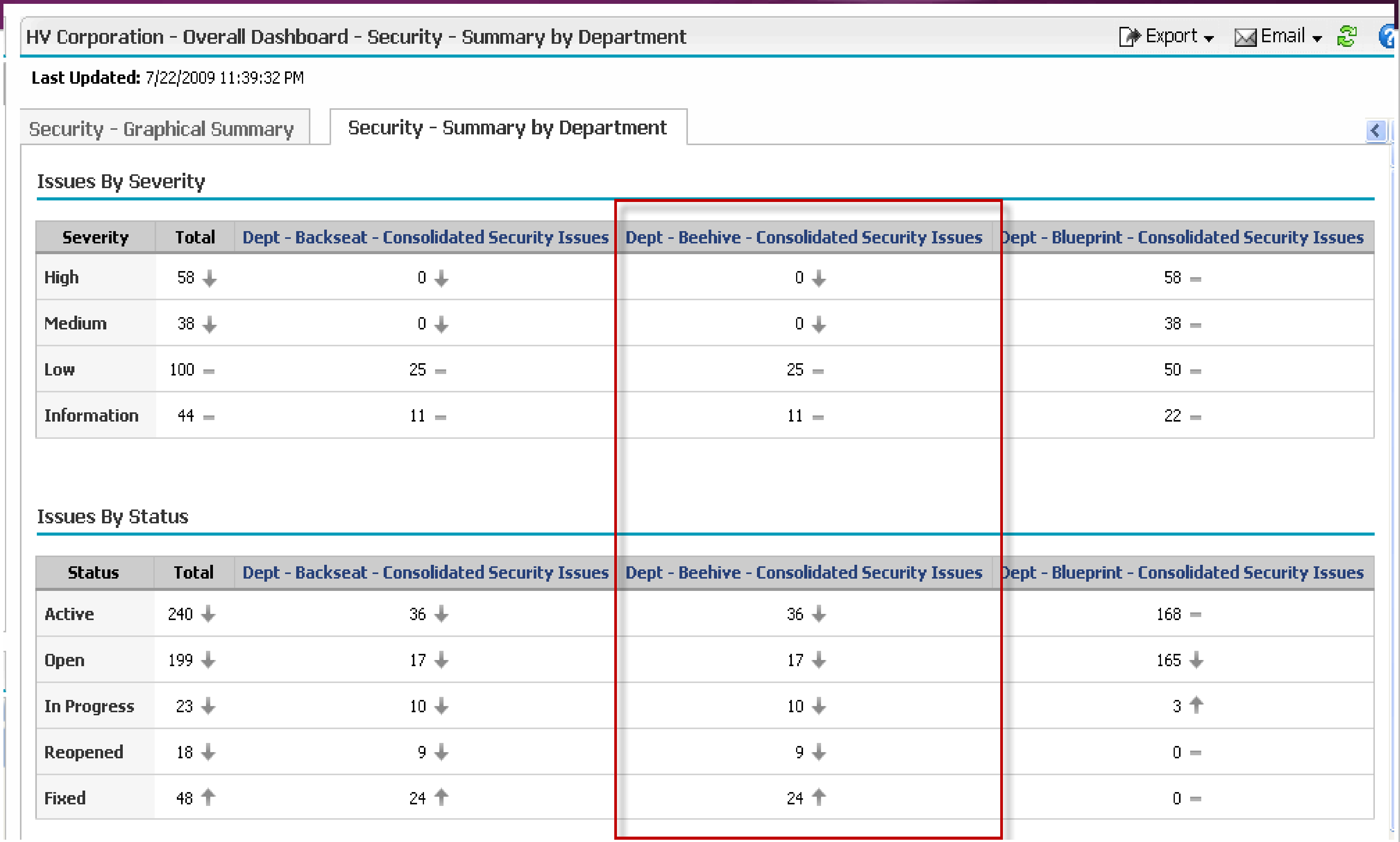
Issue Severity History

Issue Management History

Issue Severity by Report Pack

WASC Threat Classification

Summary by Department



HV Corporation - Overall Dashboard - Security - Summary by Department

Last Updated: 7/22/2009 11:39:32 PM

Security - Graphical Summary | Security - Summary by Department

Issues By Severity

Severity	Total	Dept - Backseat - Consolidated Security Issues	Dept - Beehive - Consolidated Security Issues	Dept - Blueprint - Consolidated Security Issues
High	58 ↓	0 ↓	0 ↓	58 —
Medium	38 ↓	0 ↓	0 ↓	38 —
Low	100 —	25 —	25 —	50 —
Information	44 —	11 —	11 —	22 —

Issues By Status

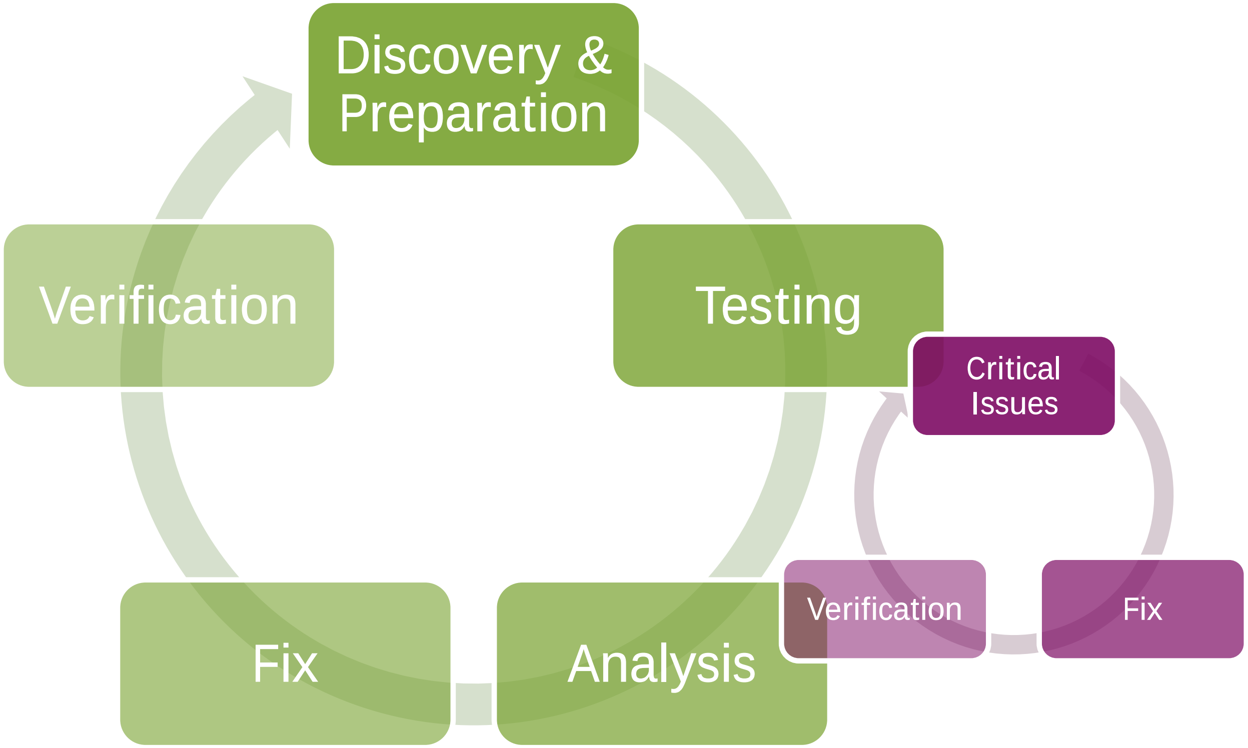
Status	Total	Dept - Backseat - Consolidated Security Issues	Dept - Beehive - Consolidated Security Issues	Dept - Blueprint - Consolidated Security Issues
Active	240 ↓	36 ↓	36 ↓	168 —
Open	199 ↓	17 ↓	17 ↓	165 ↓
In Progress	23 ↓	10 ↓	10 ↓	3 ↑
Reopened	18 ↓	9 ↓	9 ↓	0 —
Fixed	48 ↑	24 ↑	24 ↑	0 —

Different to your normal Pen testing process

- The goal is different..

...to have some knowledge of all, not all knowledge of some...

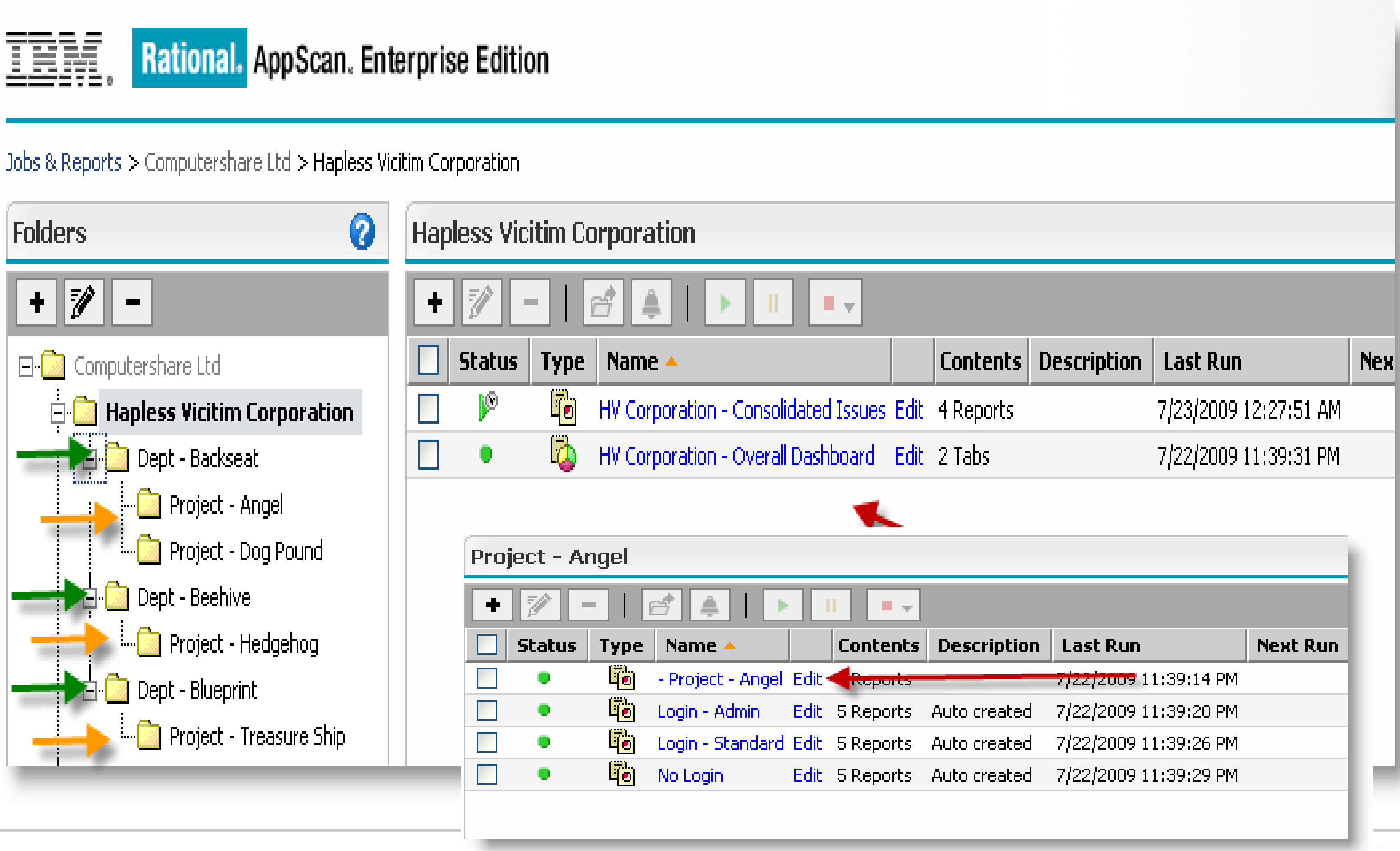
Process Stages



Discovery and Preparation

- Supporting Infrastructure
  - SharePoint
- Sites List
  - How do you discover all your sites?
  - What is a site anyway?
  - What information should you collect about a site?
- Testing Groups
  - Used to reduce the testing effort.
- Risk Profiles
  - Rank the sites to highlight the important sites.
- Testing Sheets
  - Make sure you have your testing sheets before testing starts.

AppScan – Folder Structure



IBM Rational. AppScan. Enterprise Edition

Jobs & Reports > Computershare Ltd > Hapless Vicitim Corporation

Folders

- Computershare Ltd
  - Hapless Vicitim Corporation
    - Dept - Backseat
      - Project - Angel
      - Project - Dog Pound
    - Dept - Beehive
      - Project - Hedgehog
    - Dept - Blueprint
      - Project - Treasure Ship

Hapless Vicitim Corporation

□	Status	Type	Name ▲		Contents	Description	Last Run	Nex
□			HV Corporation - Consolidated Issues	Edit	4 Reports		7/23/2009 12:27:51 AM	
□	●		HV Corporation - Overall Dashboard	Edit	2 Tabs		7/22/2009 11:39:31 PM	

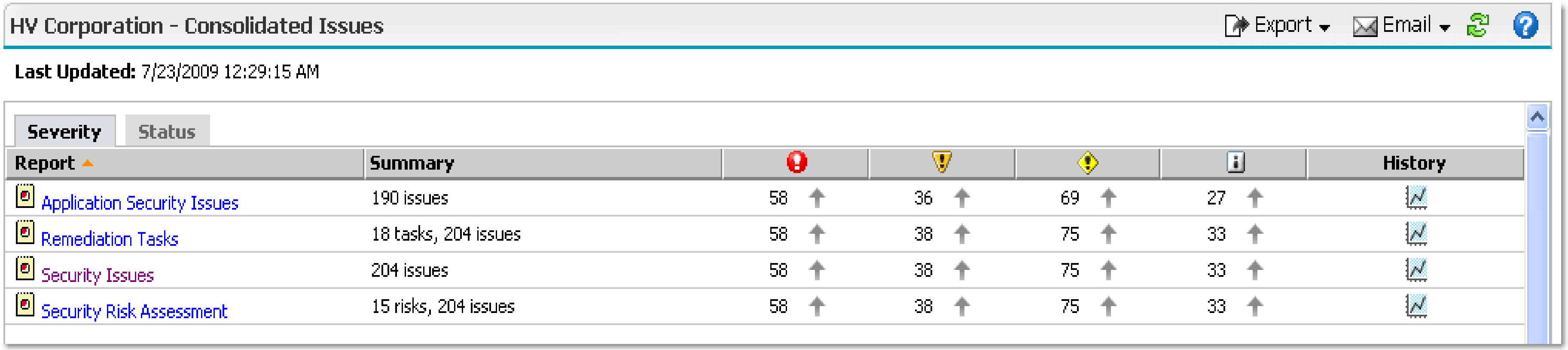
Project - Angel

□	Status	Type	Name ▲		Contents	Description	Last Run	Next Run
□	●		- Project - Angel	Edit	Reports		7/22/2009 11:39:14 PM	
□	●		Login - Admin	Edit	5 Reports	Auto created	7/22/2009 11:39:20 PM	
□	●		Login - Standard	Edit	5 Reports	Auto created	7/22/2009 11:39:26 PM	
□	●		No Login	Edit	5 Reports	Auto created	7/22/2009 11:39:29 PM	

Testing

- What skill sets will you need?
- Each testing group consists of 1 or more scans (no login, user login, admin login)
- Each testing group has a summary report which groups all the scan results.
- Each of the group summary reports are rolled up into a global report

Triaging Issues – looking for the CRITICAL issues

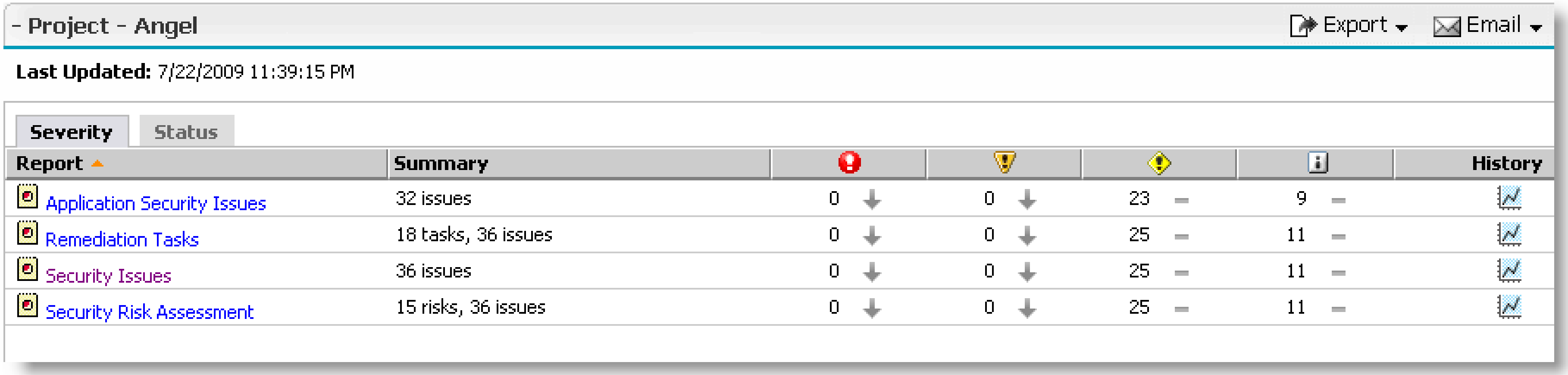


HV Corporation - Consolidated Issues

Last Updated: 7/23/2009 12:29:15 AM

Severity | Status

Report ▲	Summary	❗		⚠		◆		ℹ		History
Application Security Issues	190 issues	58	↑	36	↑	69	↑	27	↑	📈
Remediation Tasks	18 tasks, 204 issues	58	↑	38	↑	75	↑	33	↑	📈
Security Issues	204 issues	58	↑	38	↑	75	↑	33	↑	📈
Security Risk Assessment	15 risks, 204 issues	58	↑	38	↑	75	↑	33	↑	📈



- Project - Angel

Last Updated: 7/22/2009 11:39:15 PM

Severity | Status

Report ▲	Summary	❗		⚠		◆		ℹ		History
Application Security Issues	32 issues	0	↓	0	↓	23	—	9	—	📈
Remediation Tasks	18 tasks, 36 issues	0	↓	0	↓	25	—	11	—	📈
Security Issues	36 issues	0	↓	0	↓	25	—	11	—	📈
Security Risk Assessment	15 risks, 36 issues	0	↓	0	↓	25	—	11	—	📈

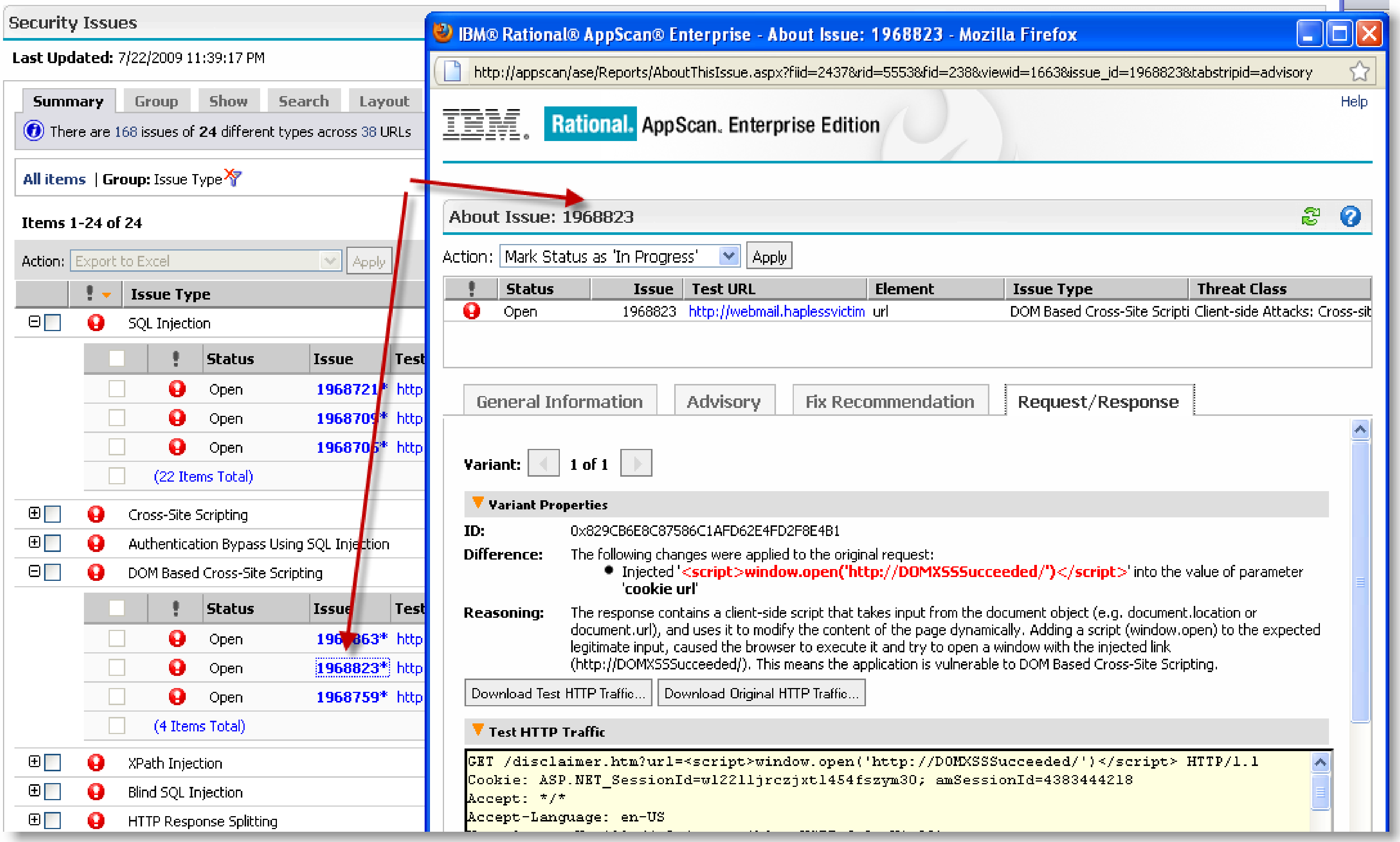
Critical Issues

- Chances are you will find something nasty during the testing.
- You need to have a process in place that allows you to fix these quickly.
- The team leaders are the ones looking for these issues in the results because they look across the result sets.

Analysis

- Clean up the results.
- Extrapolate the results.
- Validate findings within testing groups.
- Provide the reports to the development teams.
- Work with the dev teams to help them understand the results.
- Verify the fixes.
- Communicate with management.

Issue Information



Security Issues

Last Updated: 7/22/2009 11:39:17 PM

There are 168 issues of **24** different types across 38 URLs

All items | **Group:** Issue Type

Items 1-24 of 24

Action: Export to Excel Apply

	!	Issue Type
⊟ □	●	SQL Injection

□	!	Status	Issue	Test
□	●	Open	1968721*	http
□	●	Open	1968709*	http
□	●	Open	1968705*	http
□		(22 Items Total)		

	!	Issue Type
⊞ □	●	Cross-Site Scripting
⊞ □	●	Authentication Bypass Using SQL Injection
⊟ □	●	DOM Based Cross-Site Scripting

□	!	Status	Issue	Test
□	●	Open	1968863*	http
□	●	Open	1968823*	http
□	●	Open	1968759*	http
□		(4 Items Total)		

	!	Issue Type
⊞ □	●	XPath Injection
⊞ □	●	Blind SQL Injection
⊞ □	●	HTTP Response Splitting

IBM® Rational® AppScan® Enterprise - About Issue: 1968823 - Mozilla Firefox

http://appscan/ase/Reports/AboutThisIssue.aspx?fiid=2437&rid=5553&fid=238&viewid=1663&issue_id=1968823&tabstripid=advisory

Help

IBM. Rational. AppScan. Enterprise Edition

About Issue: 1968823

Action: Mark Status as 'In Progress' Apply

!	Status	Issue	Test URL	Element	Issue Type	Threat Class
●	Open	1968823	http://webmail.haplessvictim	url	DOM Based Cross-Site Scripti	Client-side Attacks: Cross-sit

Variant: 1 of 1

Variant Properties

ID: 0x829CB6E8C87586C1AFD62E4FD2F8E4B1

Difference: The following changes were applied to the original request:

- Injected '<script>window.open('http://DOMXSSSucceeded/')</script>' into the value of parameter 'cookie url'

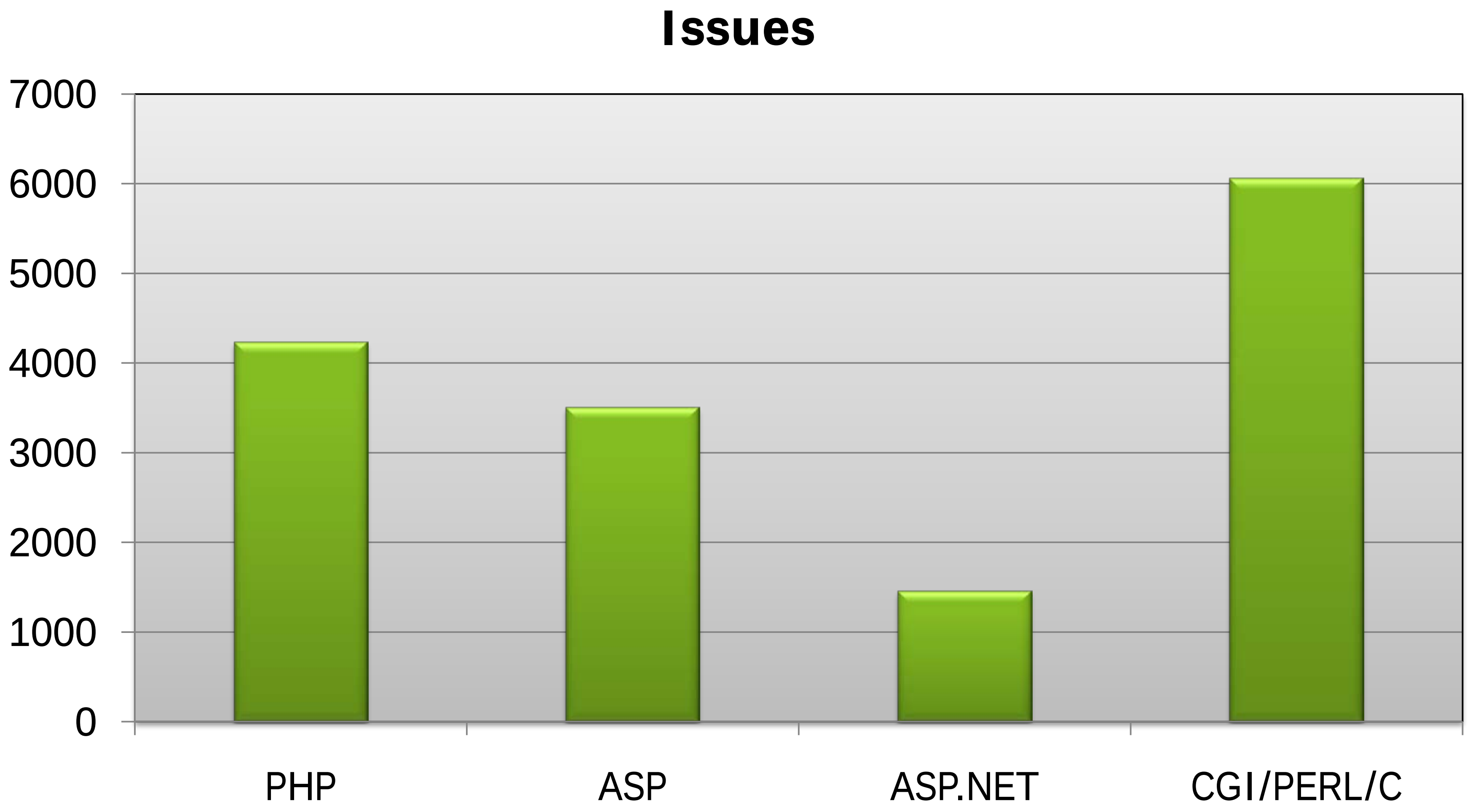
Reasoning: The response contains a client-side script that takes input from the document object (e.g. document.location or document.url), and uses it to modify the content of the page dynamically. Adding a script (window.open) to the expected legitimate input, caused the browser to execute it and try to open a window with the injected link (http://DOMXSSSucceeded/). This means the application is vulnerable to DOM Based Cross-Site Scripting.

Download Test HTTP Traffic...
Download Original HTTP Traffic...

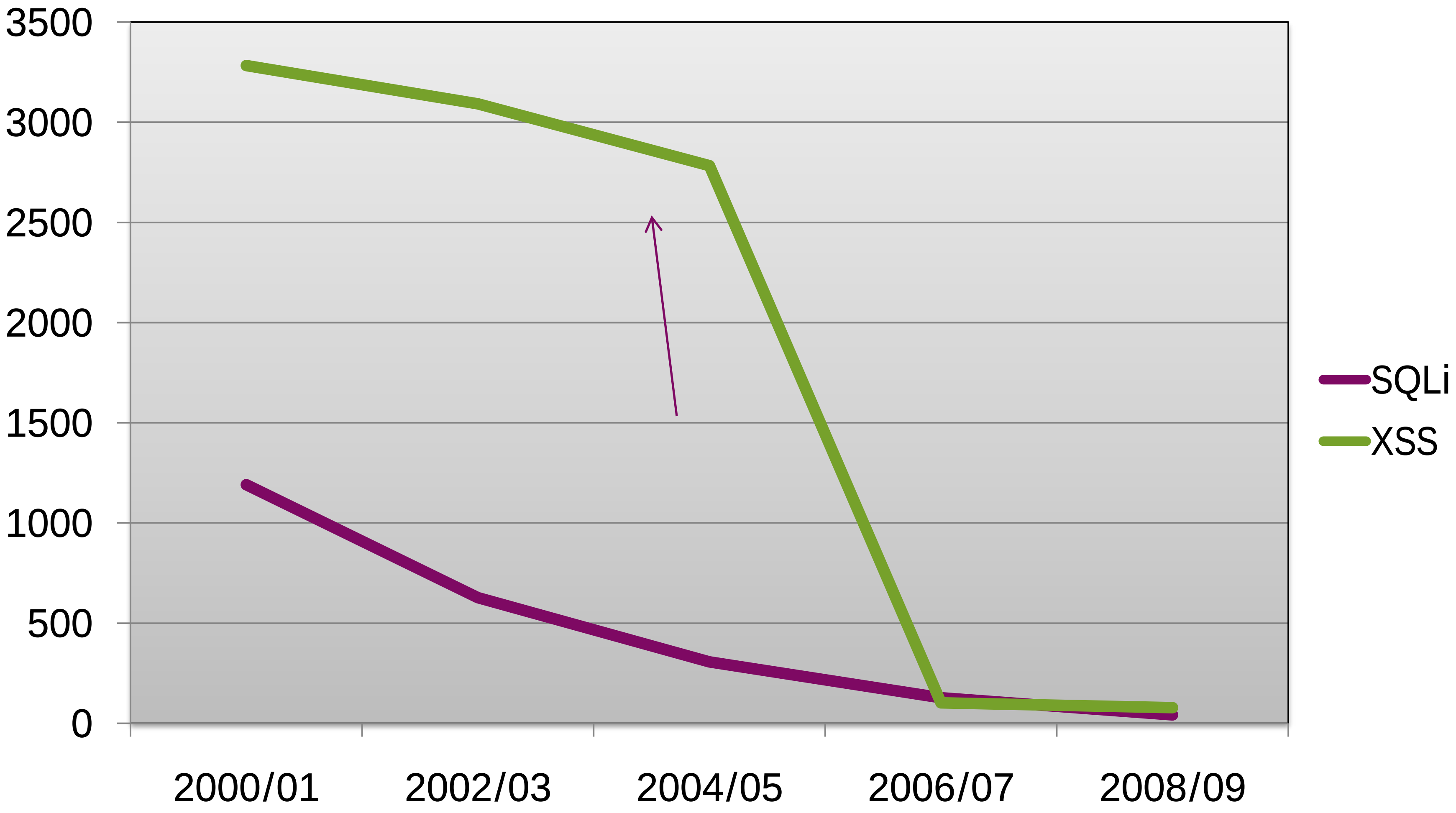
Test HTTP Traffic

```
GET /disclaimer.htm?url=<script>window.open('http://DOMXSSSucceeded/')</script> HTTP/1.1
Cookie: ASP.NET_SessionId=wl22lljrczjxtl454fszym30; amSessionId=4383444218
Accept: */*
Accept-Language: en-US
```

Issues with different languages



Are we getting better with age?



So what are the benefits?

- Understanding your security posture and your weaknesses.
- You can now answer questions like;
  - What groups need more training and on what topics?
  - How good or bad are my frameworks?
  - How does development methodology affect security? Agile?
  - Yes really ASP.NET is much more secure then ASP, and its worth spending money on converting it, Mr PHB

Because you have the stats to show it.

Lessons Learnt

- Preparation makes all the difference.
- Consider bringing in outside help.
- Make sure your testing environment is humming...
- Spend some time optimizing ASE.
- Have your critical issue process well documented before you need it.
- Its not that you can’t write secure code in PHP, its just that nobody does.

Thank you for listening!

Questions ?

John Paul Lonie, CISSP – Global IT Security Architect.

john.paul.lonie@computershare.com.au

About Computershare Limited (CPU)

Computershare (ASX:CPU) is a global market leader in transfer agency and share registration, employee equity plans, proxy solicitation and stakeholder communications. We also specialise in corporate trust services, tax voucher solutions, bankruptcy administration and a range of other diversified financial and governance services.

Founded in 1978, Computershare is renowned for its expertise in data management, high volume transaction processing, payments and stakeholder engagement. Many of the world's leading organisations use these core competencies to help maximise the value of relationships with their investors, employees, creditors, members and customers.

Computershare is represented in all major financial markets and has over 10,000 employees worldwide.

For more information, visit www.computershare.com