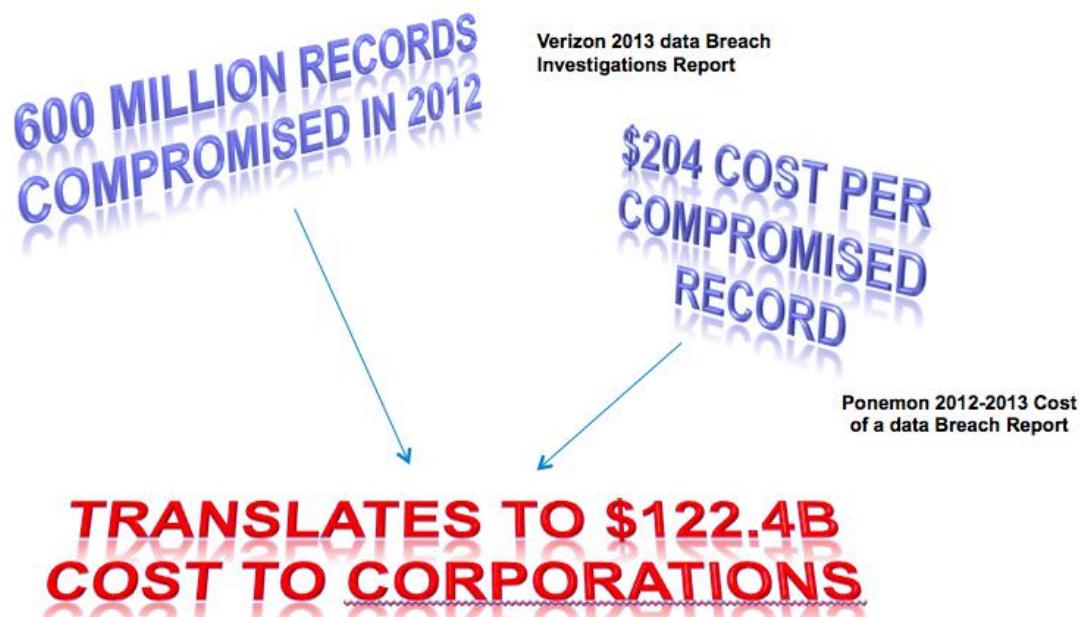


# 利用黑白箱安全檢測 - 降低應用程式資安風險

文章來源：叡揚資訊 資訊安全事業處

至 2012 年，偵測到有 6 億筆的系統入侵紀錄，而入侵的紀錄，單筆需平均 204 美元來做處理，所以光是入侵所需的解決花費為 1224 億美元。

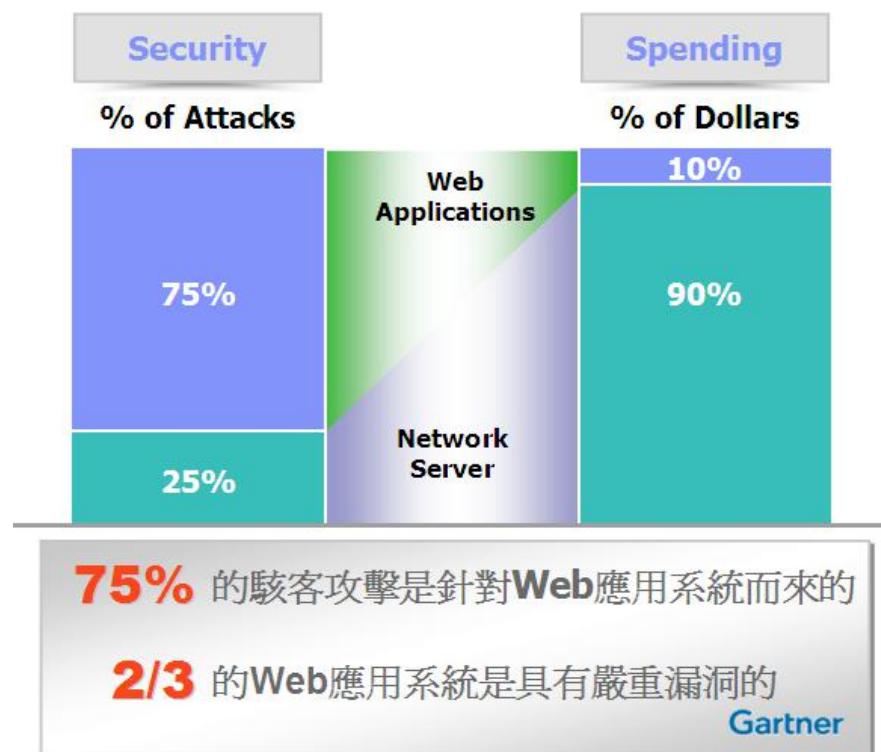


## 今日駭客主攻防禦較弱的地方：應用程式本身

根據 Gartner 的調查，資訊安全攻擊有 75% 都是發生在 Web 應用程式層而非網路層面上，2/3 的 Web 站點都相當脆弱，易受攻擊。另外，在今年 4 月國家電腦網路應急技術處理協調中心最新發佈的報告中指出，“2012 年度，網路仿冒、網頁惡意程式碼、網站篡改等增長速度接近 200%。”而隨著 Web2.0 應用程式的推廣，相關安全問題逐漸凸顯，針對該類網站的攻擊事件也在不斷增多。

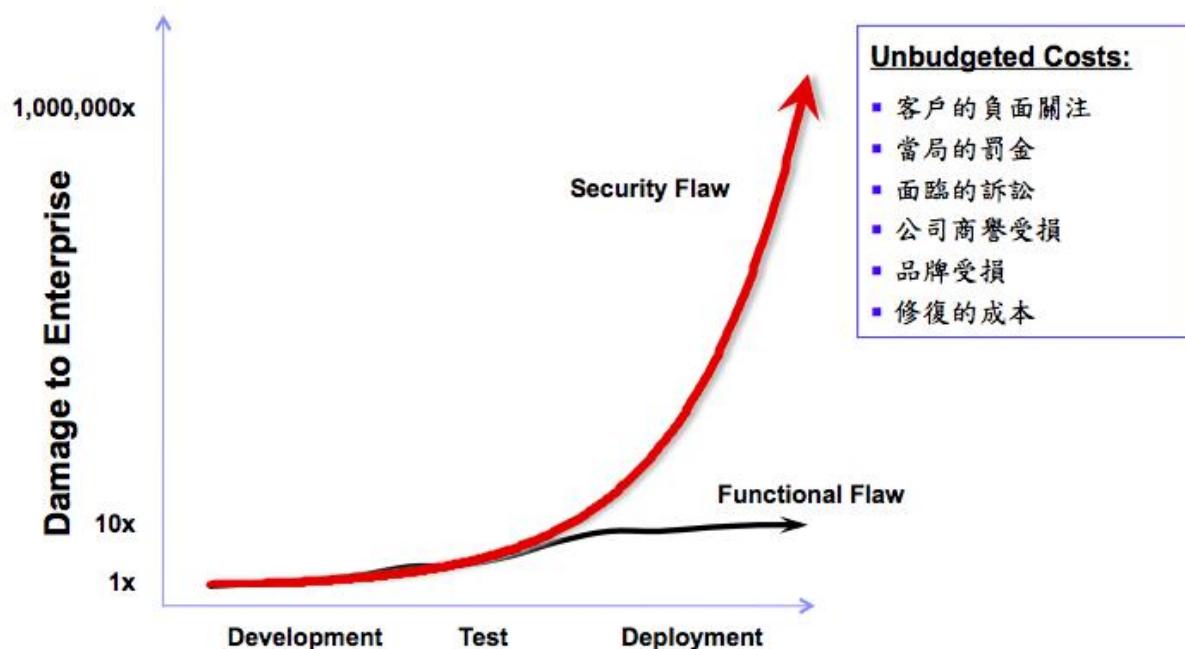
## Web 應用程式成為攻擊的門戶

ST 支援多協定以及提供穩定的傳輸、完善的權限控管，平台上每位使用者皆有自己的獨立空間，彼此無法互相干擾，利用檔案繞送的機制，完成帳號與帳號、伺服器與伺服器間的檔案交換，並且可針對帳號、IP、目錄 / 檔案做交叉配合權限控管，另亦提供檔案落地儲存時加密（就算是最高權限管理者也无法觀看檔案內容）及 PGP 加密 ... 等機制，有效防堵資料外洩的可能，讓檔案的保護更加完善。



- 現今 75% 的網路攻擊發生在應用程式層面，但是公司在此方面的投資僅為資訊安全防護花費的 10%
- 到 2012 年，80% 的企業都會經歷至少一次應用程式安全的攻擊
- 內部安全攻擊的成本，美國企業每年要花費 400 億
- 64% 的 CIOs 認為安全，遵規和資料保護是所面臨意義重大的主要挑戰
- 安全和遵規風險對於公司的商譽，客戶關係和業務發展有著深遠的影響

## 資安面的缺陷將比功能面的缺陷造成更大的代價



資安在開發期及測試期的缺陷，損害只占上限期的  $100,000/1$ ，由此可知資安在越前面的階段執行，損害代價越小：

- 組織內的資安專家 / 設備，多專長在網路 / 作業系統 / 伺服器等基礎建設
- 應用程式功能愈來愈多，架構愈來愈複雜，時程壓力又大，程式人員往往不瞭解 / 忽視安全問題
- 即使被告知應用系統漏洞，可能也不曉得從何處理起
- 處理應用程式安全問題變成上線的瓶頸
- 無法密集委外檢測 Web 應用程式是否有新的漏洞
- 網站是否符合政府 / 產業資安法規
- 委外開發的 Web 應用程式，難以驗收其安全性

其實，在一般企業內部，懂得網路設備，作業伺服器等基礎建設資安的人比較多，而應用程式方面比較少，隨著程式架構越來越龐大，跟上線的時程越來越緊，程式設計師往往會忽略安全的問題，也不知從何著手，所以上線成為了安全的瓶頸，再加上漏洞是日新月異，企業也不太可能可以密集的委外掃描，這將是一筆龐大的支出。委外開發也需驗收其安全性。

## 利用 AppScan 強化應用程式體質

- (What) AppScan 是什麼？

AppScan 是一套自動化弱點掃描工具，用來檢測 Web 應用程式的安全性，找出應用系統的資安漏洞，並一一提供詳盡的處理建議

- (Why) 為什麼需要使用 AppScan？

簡化發現與修復 Web 應用程式的安全性問題的工作，降低維護資訊安全的成本

- (How) AppScan 如何辦到的？

黑箱測試：模擬各種駭客攻擊的手法，以無害的方式去測試運行中的 Web 應用程式的回應，判斷系統是否存在各種安全性問題，並按照問題的輕重緩急順序，提供可立即處理問題的建議做法

白箱測試（又稱源碼檢測）：分析提供的原始碼，以理論模式去判斷系統是否存在各種安全性問題，指出有安全問題的原始碼位置，並按照問題的輕重緩急順序，提供可立即處理問題的建議做法

所以這些 AppScan 特點可用來證明與測試專注於弱點或漏洞的掃描技術；AppScan 是可以執行掃描一個站點的安全漏洞的自動化分析的工具。並所產生的報告上有關漏洞的問題，能有效提供有關如何解決問題的建議。它可用於由一個團隊的許多不同的成員包括資安管理人員，開發人員和測試人員。

## 範例：SQL Injection 盜取帳戶資料

The screenshot shows a Windows Internet Explorer window with the URL <http://altoromutual-testsite.net/testsite/transaction.aspx>. The page title is "Altoro Mutual - Recent Transactions". The main content area is titled "Recent Transactions" and contains a table with the following data:

TransactionID	AccountID	Description	Amount
20	1001180140	Rent	1100
21	1001180140	Deposit	1050.00
22	1001180140	Deposit	1050.00
23	1001180140	Car Payment	369.12
24	1001180140	Deposit	1050.00
27	1001180140	Car Payment	369.12
68	1001180141	Deposit	677.5
74	1001180141	Deposit	878.5
77	1001180141	Deposit	901.1
1			

The sidebar on the left lists options like "View Account Summary", "View Recent Transactions", and "Transfer Funds". A note at the bottom of the page states: "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 reverse defects. This site is not a real banking site. Similarities to any 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>".

基本上，標準流程的功能，我們可以從 01/01 號開始查詢所有的交易資料

The screenshot shows a web browser displaying the 'Recent Transactions' page of the Altoro Mutual website. The URL is <http://altoro-testsite.netbanktransaction.aspx>. The page has a sidebar on the left with links like 'View Account Summary', 'View Recent Transactions', 'Transfer Funds', 'Search News Articles', and 'Customize Site Language'. The main content area is titled 'Recent Transactions' and contains a table of transaction data. A user has injected the SQL command 'union select user' into the 'After' field of a search form, resulting in the display of user account information in the transaction table.

TransactionID	AccountId	Description	Amount
20	1001160140	Rent	1100
21	1001160140	Deposit	1050.00
22	1001160140	Deposit	1050.00
23	1001160140	Car Payment	369.12
24	1001160140	Deposit	1050.00
27	1001160140	Car Payment	369.12
68	1001160141	Deposit	877.0
74	1001160141	Deposit	878.0
77	1001160141	Deposit	891.1
1			

The page also includes a note about the website being a demo site and a copyright notice for Watchfire Corporation.

但是，當我們了解到這樣的查詢功能，如同就是輸入 sql 指令一般的方式，所以我們在這例子上，可以嘗試輸入其他指令來執行動作，以此為例，我們加上了 union 來查詢額外的資訊，ex.USER 表

This screenshot shows the same 'Recent Transactions' page after the user has injected a more complex SQL query. The 'After' field now contains 'union select \* from USER'. The result is a full dump of the 'USER' table, listing various user accounts with their names and passwords.

AccountId	Name	Password
24	1001160140	DEPOSIT
23	1001160140	Car Payment
24	1001160140	Deposit
27	1001160140	Car Payment
68	1001160141	Deposit
74	1001160141	Deposit
77	1001160141	Deposit
285	1003160121	Deposit
357	1005160101	878.0
363	1005160101	878.0
366	1005160101	882.12
376	1006160141	878.0
394	1006160141	878.0
397	1006160141	882.12
419	1006160141	1500.00
100616014	jimith,Demo1234	
100616018	speed,Demo1234	
100616012	hosen,User	
100416018	admin,admin	
100516010	ejen,Prader	
100616014	ctley,Ali	
1		

所以我們可以發現到，經過我們加上額外的 sql 指令後，系統輸入的畫面不僅僅只有交易的資料，同樣的也把帳號的用戶資訊與密碼也列出。

## 應用程式安全性的黑箱測試和白箱測試比較

### 黑箱：**AppScan Standard**

- 特點：
  - 檢測範圍較廣。無論後端使用什麼程式語言、運行在什麼平台、使用什麼 DB 都能檢測
  - 就像駭客用工具找漏洞一樣，直接使用系統，準確度較高
  - 不需提供任何程式碼
- 限制：
  - 以檢測 Web 系統和 Web Service 為主

### 白箱：**AppScan Source**

- 特點：
  - 找出程式碼的安全漏洞，直接點出有問題的程式碼，加快開發人員進行問題的修正
  - 不侷限於 Web 系統
  - 不需要先部署系統，讓系統運行
- 限制：
  - 工具必須完整認識受測系統採用的開發語言（例：Java, .NET, C++）及開發架構（例：Struts, Spring）

## Rational AppScan: 全面的應用程式安全檢測解決方案

- IBM 是業界首先全面取得系統安全動態檢測（黑箱測試）和程式碼安全分析檢測（白箱測試）技術的公司，推出整合的解決方案，實現全面的應用程式安全防護
- IBM 解決方案是目前業界唯一完成全面中文化的（同時亦具備多國語言支援）
- 黑箱測試工具直接模擬駭客的攻擊，是應用程式安全的基礎設施，應優先考慮，方便於已上線的系統，簡便地找出須即刻被修正的錯誤
- 白箱測試工具便利開發人員在開發早期使用，讓問題早期治療；成本最低，避免在整測、上線階段造成更大的時程壓力，且幫助開發人員從做中學習

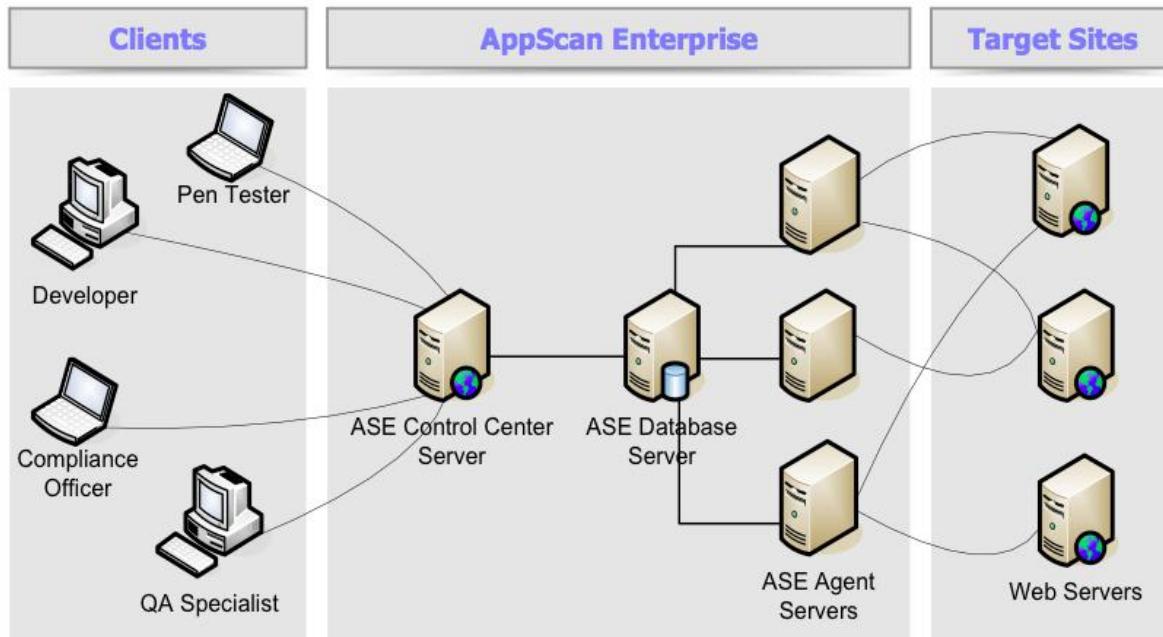


## Rational AppScan 黑箱測試的競爭優勢何在？

掃描弱點廣度	>1700種弱點類型
技術研發能力	>全球跨地域研發團隊 >密集線上更新弱點類型
售後服務支援	>專業技術支援體系 >問題修正迅速
掃描結果報告	>全中文化(多國語言) >可依不同對象調整產出項目與詳細程度 >超過40種遵規標準報告
市佔率與口碑	>全球市佔率最高 >久經市場驗證
額外附加值功能	>惡意軟體與鏈結檢測 >浮動式授權適合開發團隊使用 >進階排程功能 >客製化延伸彈性

## AppScan Enterprise Edition

- 集中化管理、精細的權限控管、可擴充的架構、建立安全導向的企業

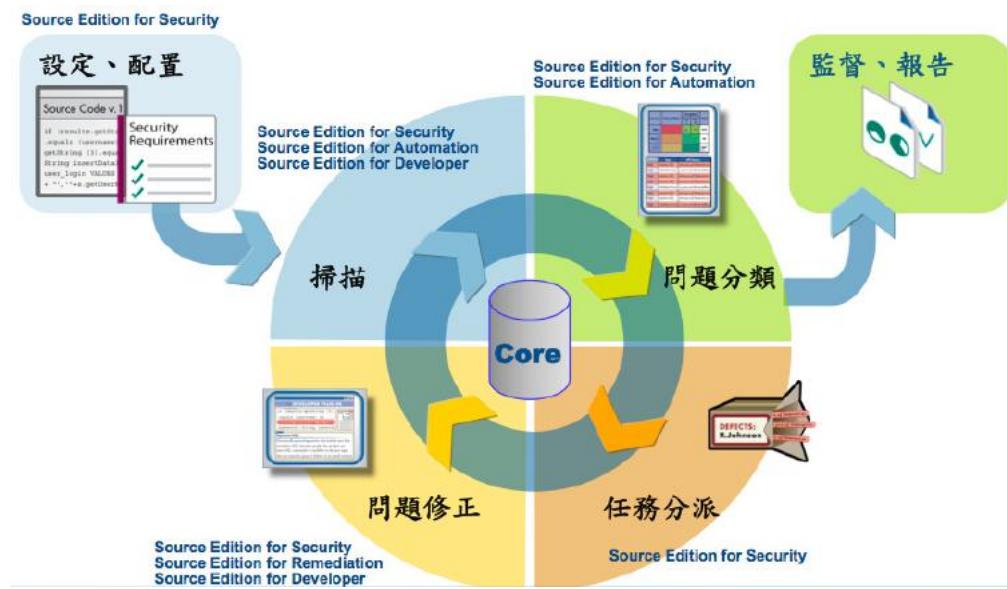


## 白箱測試工具 : AppScan Source Edition 概覽

### 一、容易上手使用 - Day One Productivity

- 開箱即用 Works Out-of-the-Box**
  - 設定精靈 (Configuration wizards)
  - 可將 Eclipse Workspaces 或 .NET Solutions 直接匯入使用
- 弱點矩陣分析 (Vulnerability Matrix)**
  - 除了風險程度之外，還將不同信心水準的漏洞區分開來
  - 加速資安分析員的問題分派
  - 彌補資安專業知識不足的限制
- 強大的過濾功能**
  - 降低誤判的可能性，避免困擾開發人員
  - 可以專注於處理少數較高優先性的漏洞
  - 中央設定，全組織適用，標準一致

## 二、面面俱到的工作流程



## 三、掃描分析能力：速度、深度、完整度與創新

### • 較快的分析

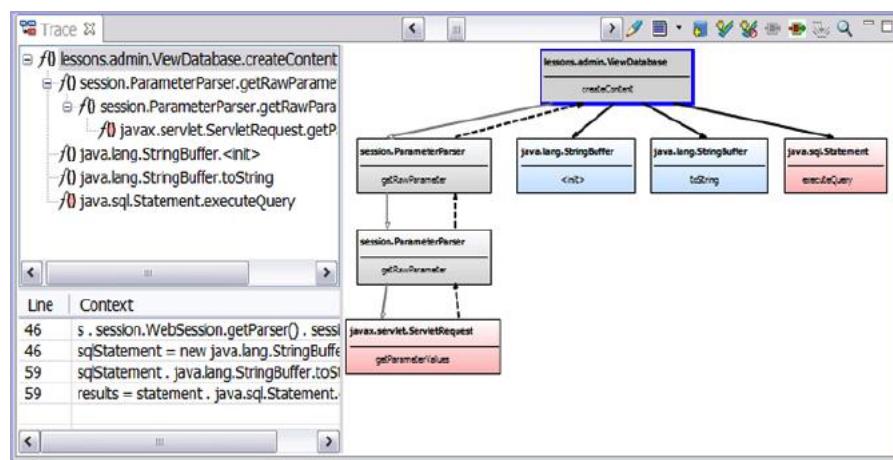
- 卓越的記憶體管理和快取能力
- 再掃描 (Re-scan) 的最佳化
- 超過 100 項的專利技術

### • Data Flow / Call Flow

- 支援長流程追蹤 (long traces)
- 容易識別資料輸入來源 (sources) 與危險輸出元 (sinks)

### • 在分析過程中，資訊不足的灰色地帶也會被揭露

- 寧可錯殺一百，也不放過一個
- 歸類於低信心水準的漏洞



#### 四、稽核能力

User	Hostname	IP Address	Event Type	Product Name	Time	Result	Modified Assessment
admin	TOMMULVE	9.32.240.241	Publish assessment	AppScanSourceSec 8.0.0	Sep 29, 2010 4:01:28 PM	Succeeded	WebGoat - 9/29/10 3:37PM
admin	TOMMULVE	9.32.240.241	Publish assessment	AppScanSourceSec 8.0.0	Oct 1, 2010 11:18:19 AM	Succeeded	WebGoat - 9/29/10 3:37PM

- 提供特化的視圖去稽核一些關鍵的 AppScan Source Edition 作業：

- Authentication
- 使用者管理
- 掃瞄結果 (Assessment) 管理
- 自訂規則 (Customer Rules) 異動
- 掃描規則異動

- 更容易去管理企業級的佈署
- 保護您應用程式安全的方案

#### 利用 IBM Rational AppScan 降低應用程式資安風險

##### 一、黑箱 / 白箱 測試結果關聯性分析

The screenshot shows the 'Correlated Security Issues' page in Rational AppScan. It displays a grid of 31 issues found across 2 URLs, with 25 static analysis issues correlated. The columns include Action, Export to Excel, Apply, Test URL, Element, Issue Type, Static Line, Source File, API, and Line. A yellow callout box points to the message: 'Issues discovered using both dynamic and static analysis (URL, element, source file, API, etc.)'.

- 將實地動態測試的結果和靜態源碼掃描的結果關聯在一起
- 可以從 URL drill down 到程式碼行的角度去檢視應用程式漏洞
- 提供更準確的資訊
- 在 AppScan Enterprise 上進行
- 超過 40 種開箱即用的資安遵規報告 (security compliance reports)

## 二、利用 IBM Rational AppScan 降低應用程式資安風險

