心得分享之

Fortify SCA 與 IBM Appscan

張維廷　網路管理組

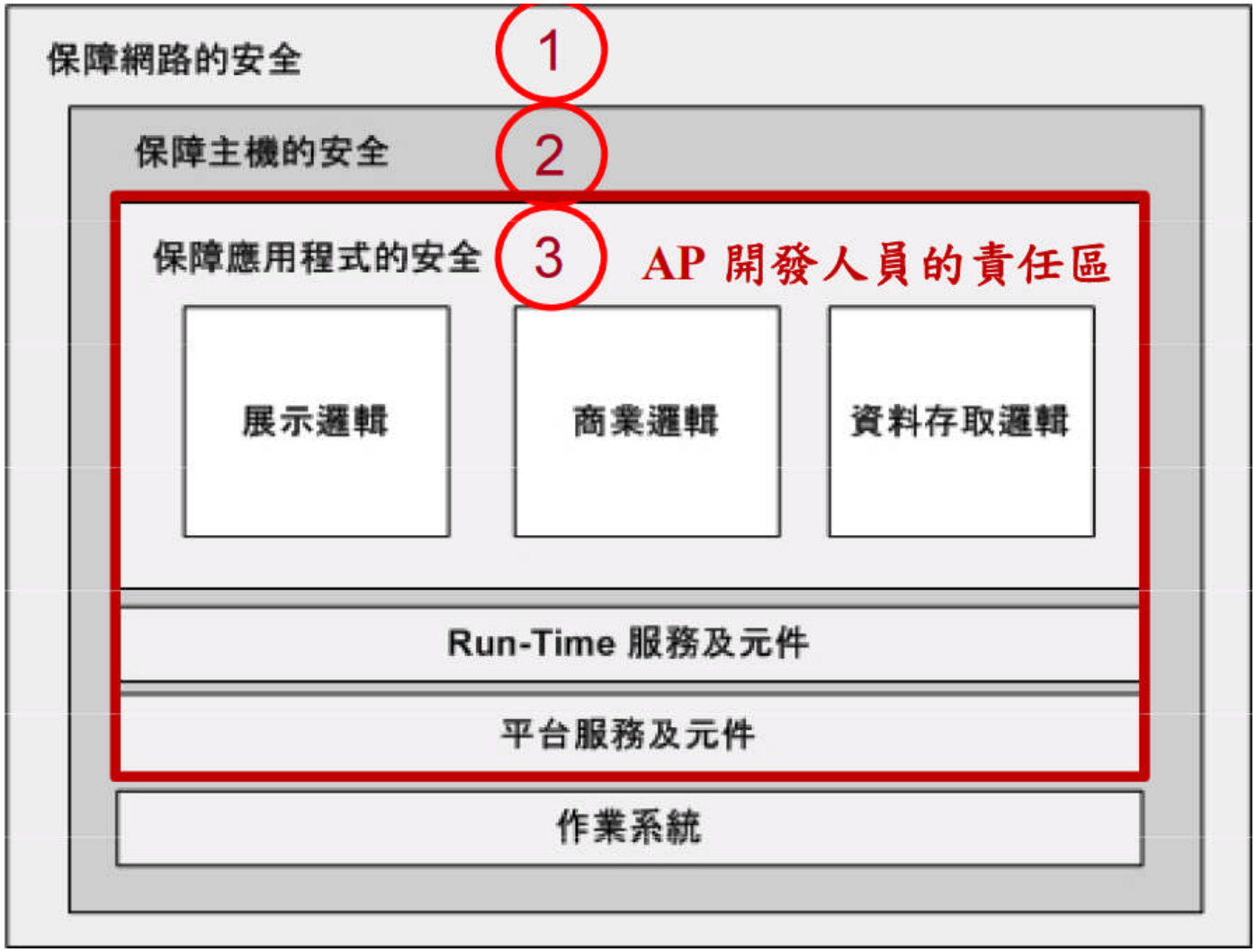
Before we go……

- **White-Box Testing**
- **Black-Box Testing**
- **Gray-Box Testing**
- **OWASP**

  Open Web Application Security Project

  是一個開放社群、非營利組織，主要目標是研議Web軟體安全之標準、工具與技術文件，長期致力於協助政府或企業瞭解並改善網頁應用程式與網頁服務的安全性。
- CWE
- SANS

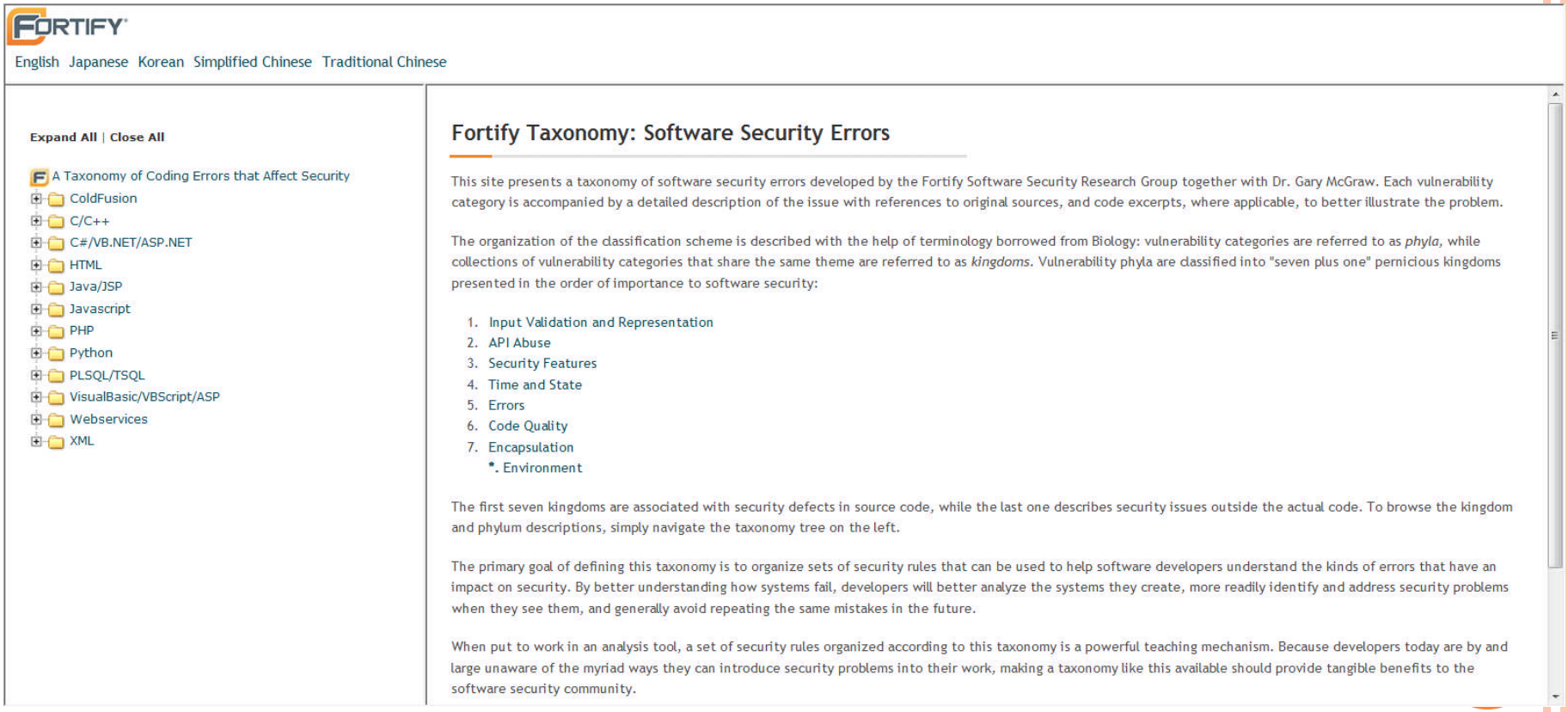
網站安全基本的三個區域防禦



Fortify 360 SCA

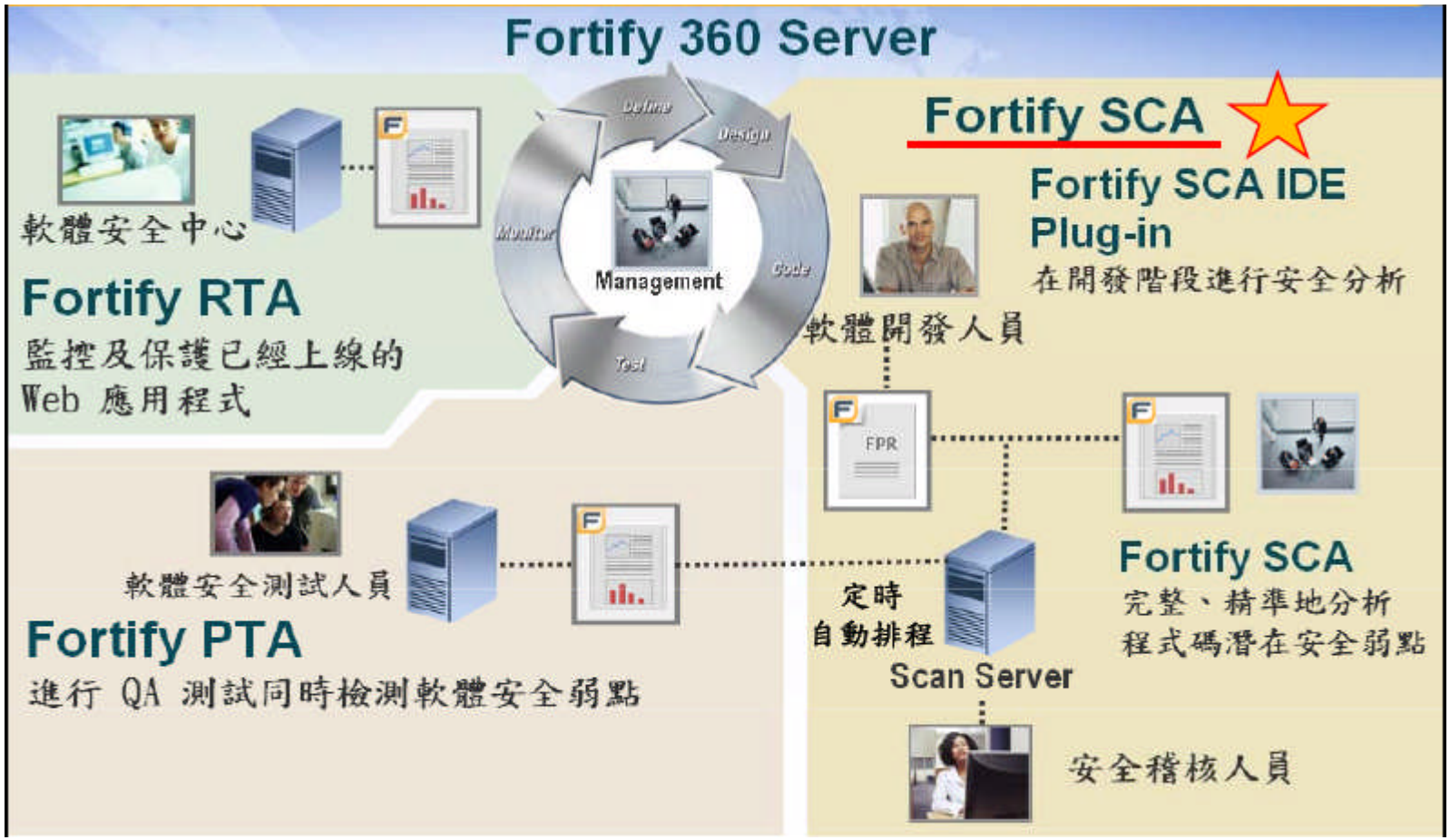
FORTIFY

- 提供程式語言已知安全漏洞說明

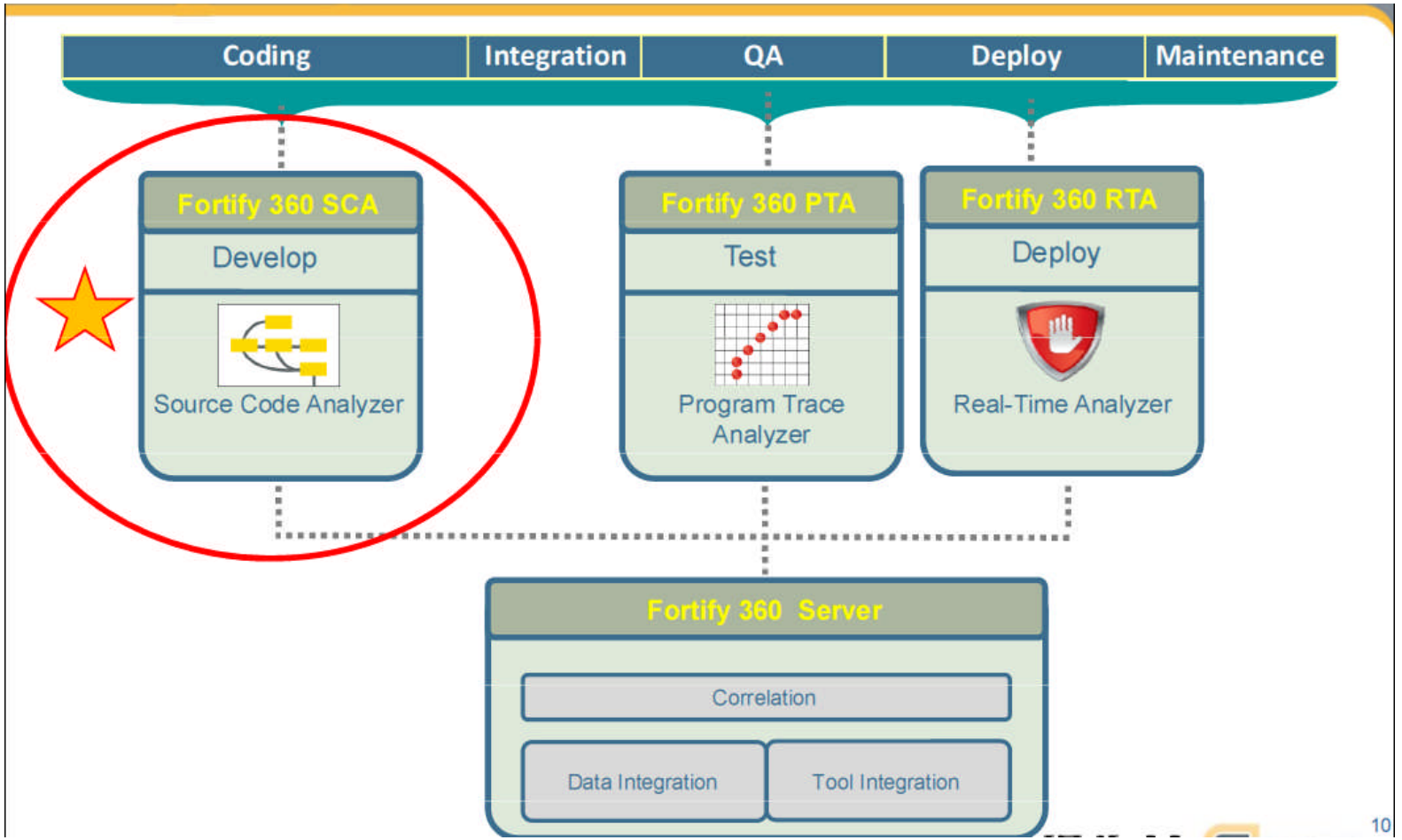


FORTIFY

- Fortify 360 軟體安全開發週期的完整解決方案



FORTIFY


Coding
Integration
QA
Deploy
Maintenance
Fortify 360 SCA
Develop
Source Code Analyzer
Fortify 360 PTA
Test
Program Trace Analyzer
Fortify 360 RTA
Deploy
Real-Time Analyzer
Fortify 360 Server
Correlation
Data Integration
Tool Integration
10

FORTIFY

- 支援 17 種程式語言安全檢測

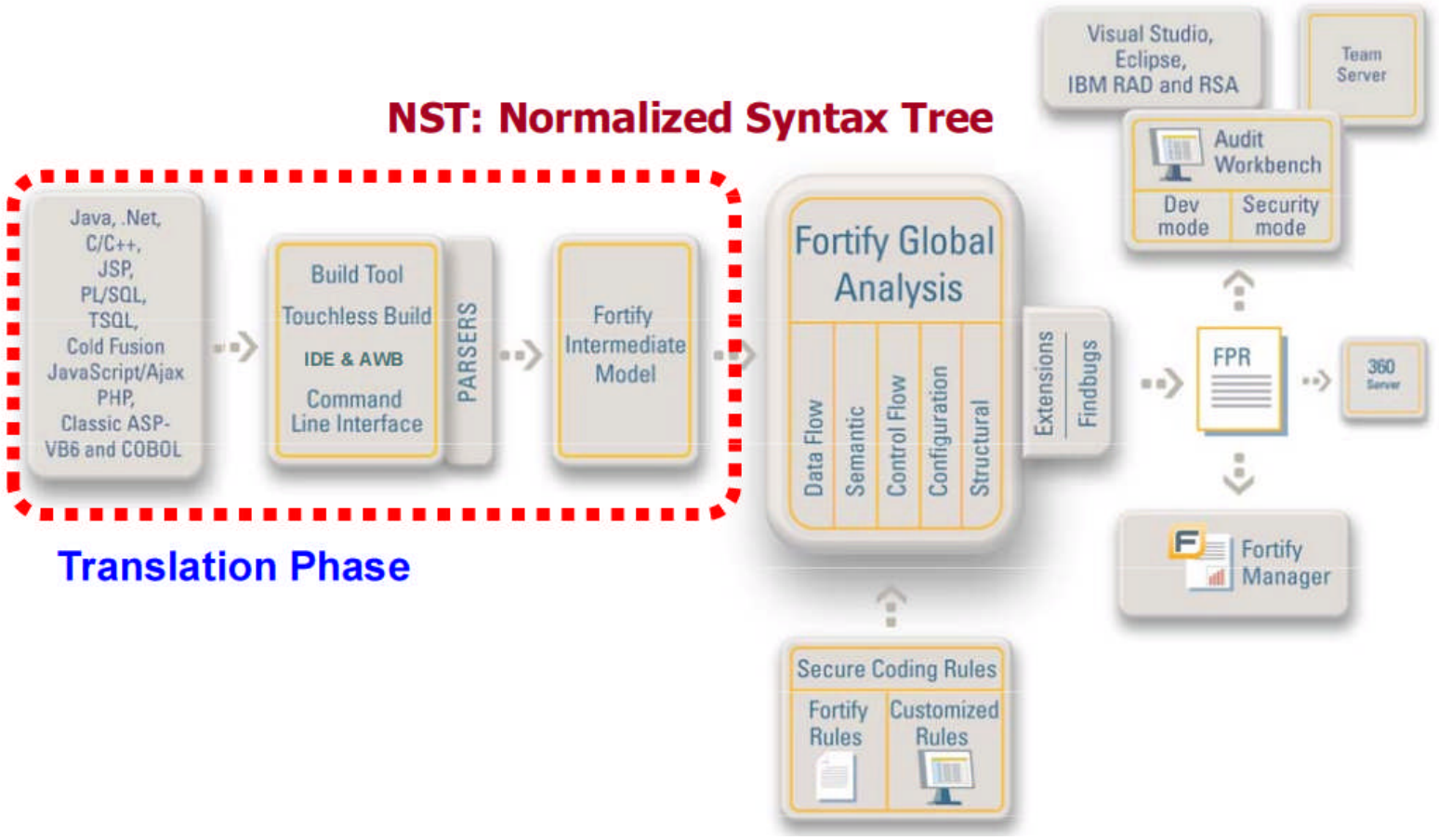
1. ASP.Net
2. VB.Net
3. C#.Net
4. ASP
5. VBScript
6. VB6
7. Java
8. JSP
9. JavaScript
10. HTML
11. C/C++
12. ColdFusion 5.0
13. PHP
14. T-SQL (MSSQL DB)
15. PL/SQL (Oracle DB)
16. XML
17. COBOL - 獨立購買的產品

(.Net Framework 1.1、2.0、3.0、3.5)

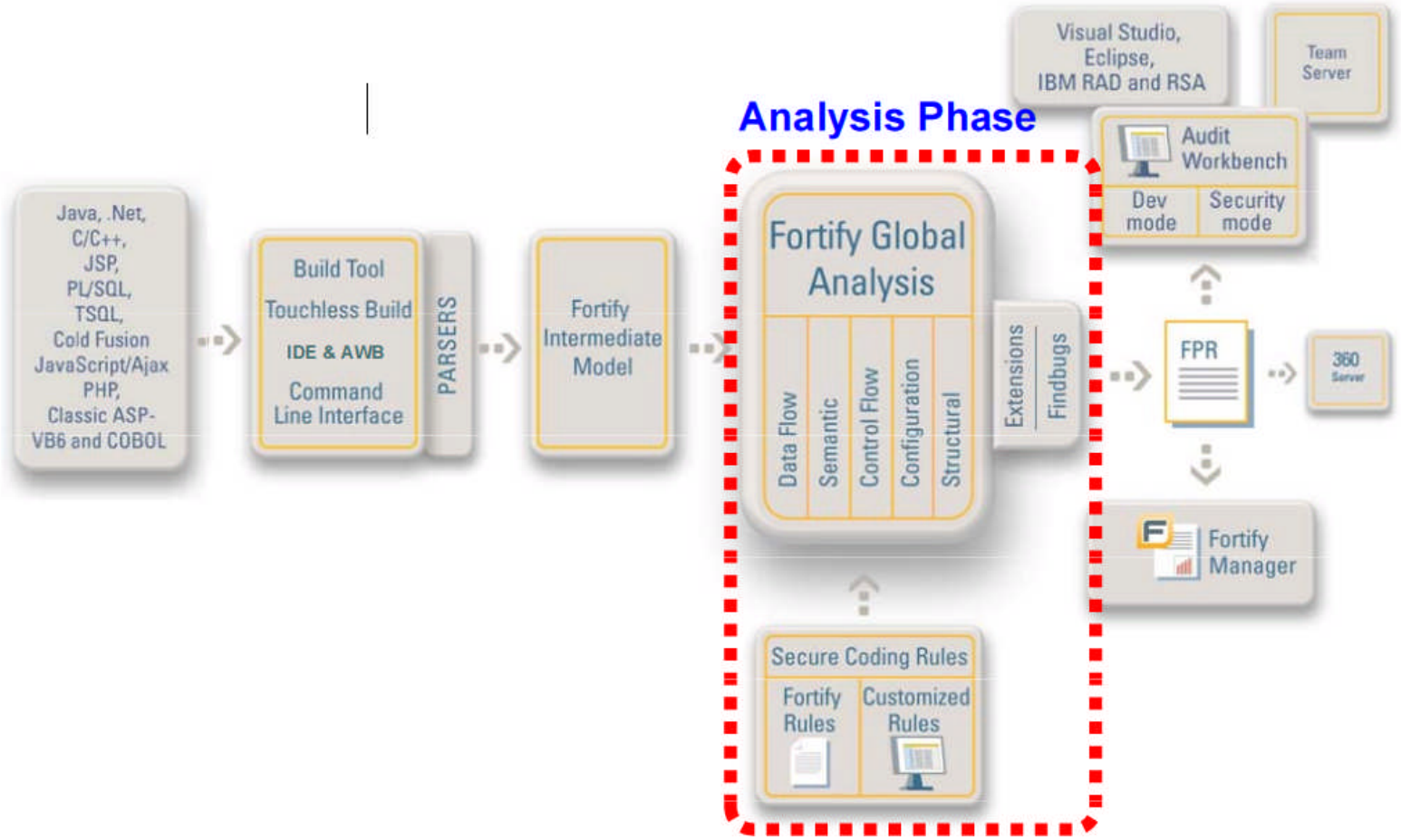
Fortify

- **Fortify 360 SCA** 檢測程式碼安全的程序
- 轉譯階段 **Translation Phase**
- 分析階段 **Analysis Phase**
- 稽核階段 **Audit Phase**

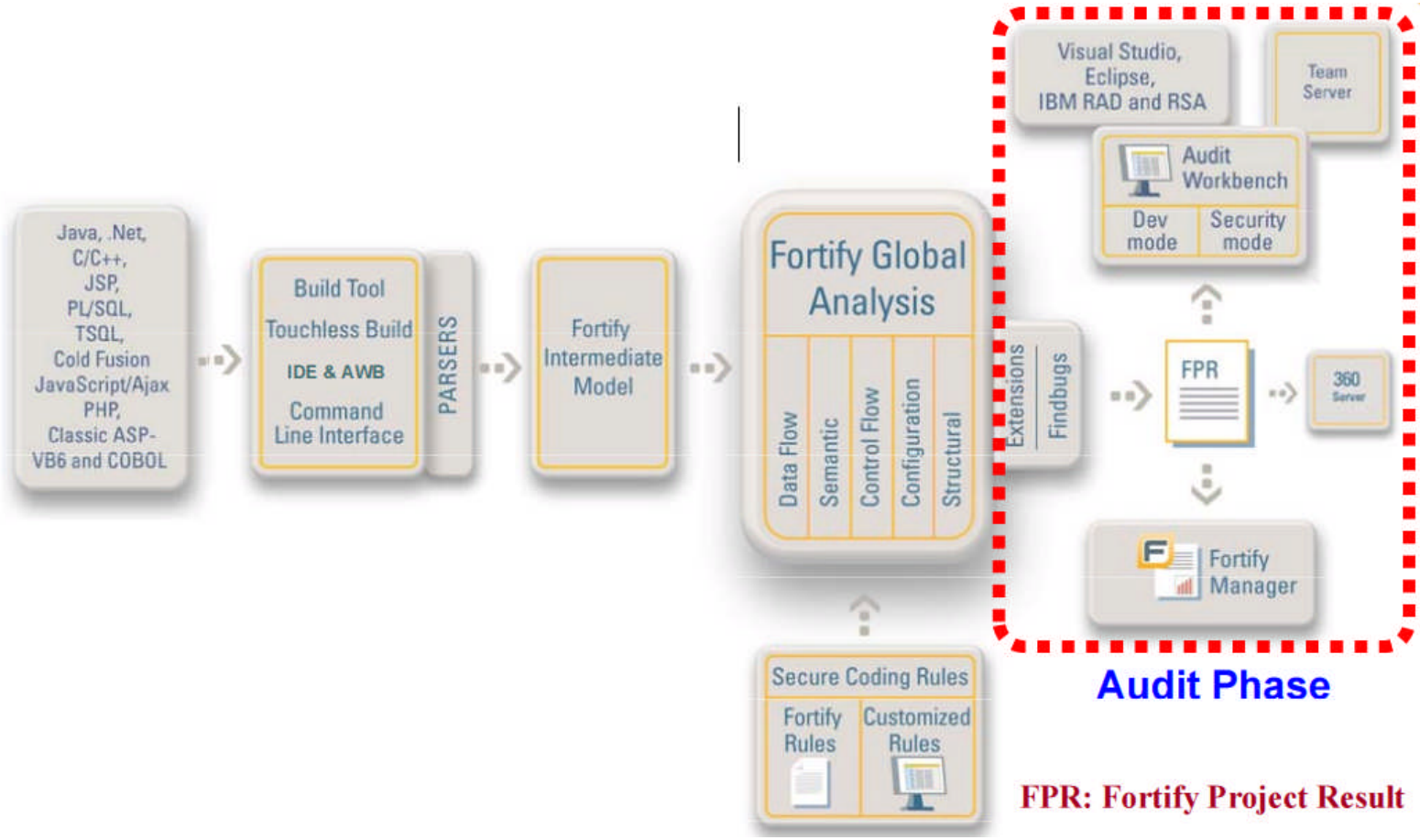
Fortify Translation Phase



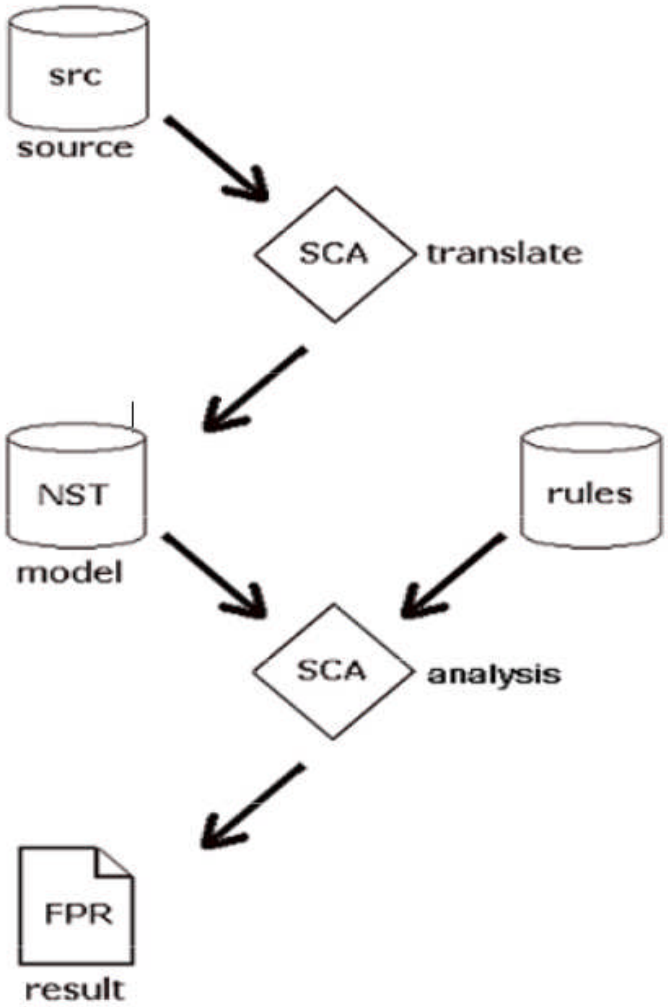
Fortify Analysis Phase



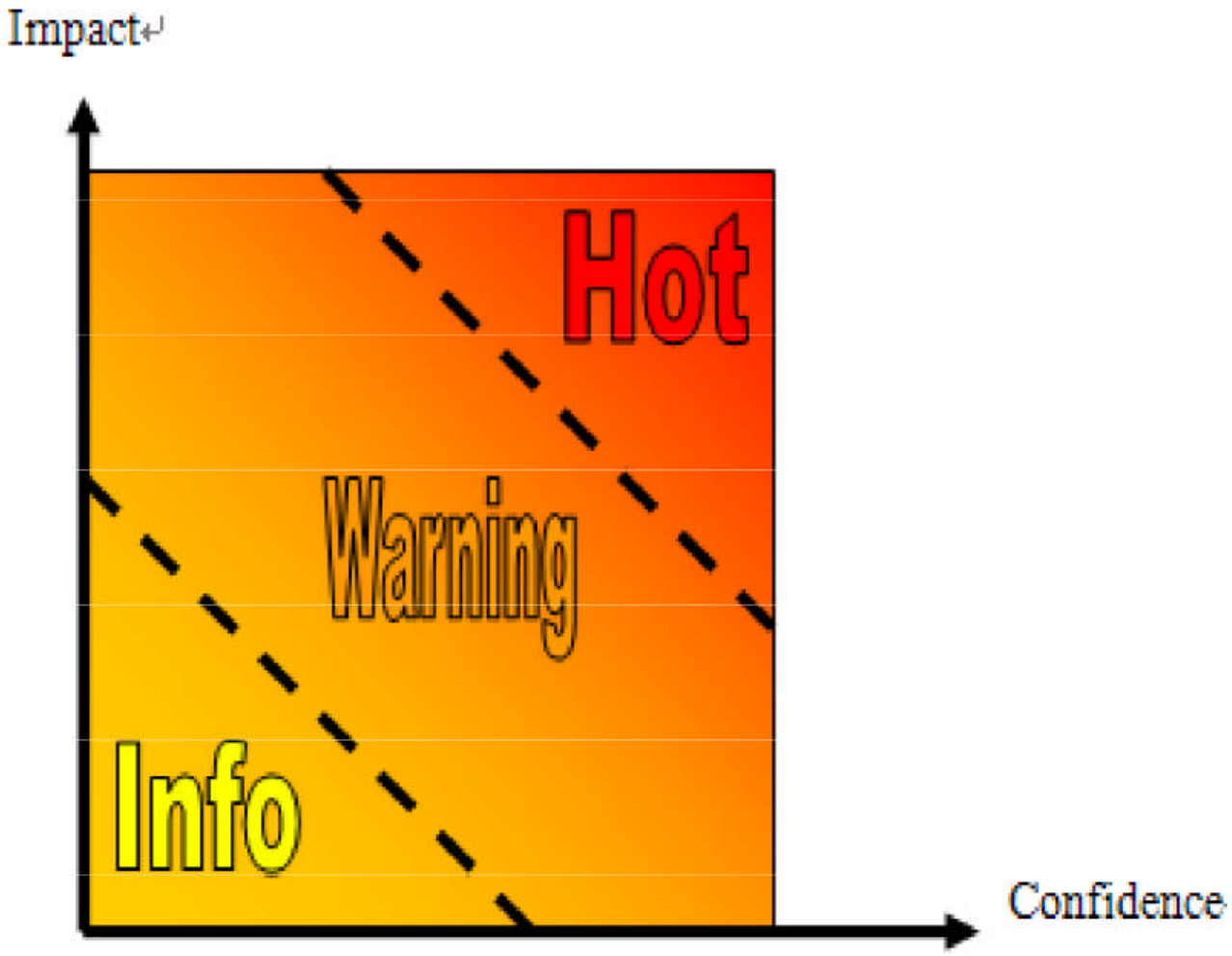
Fortify Audit Phase



Fortify Process Flow Summary



FORTIFY 360 SCA 嚴重等級分類



新版本的分類方式

- **檢測問題等級的歸類方式**

  是以兩個座標值做為量化區分依據

  (1) Likelihood

  (問題準確度的可能性)

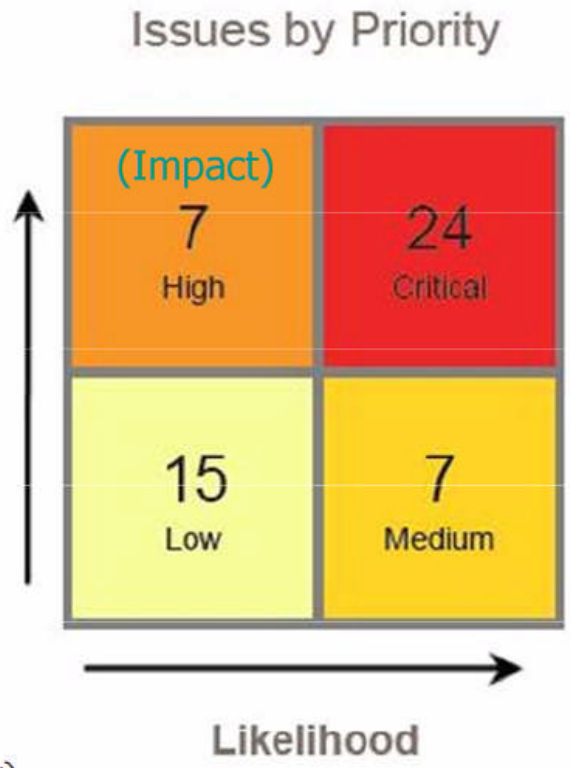
  (2) Impact

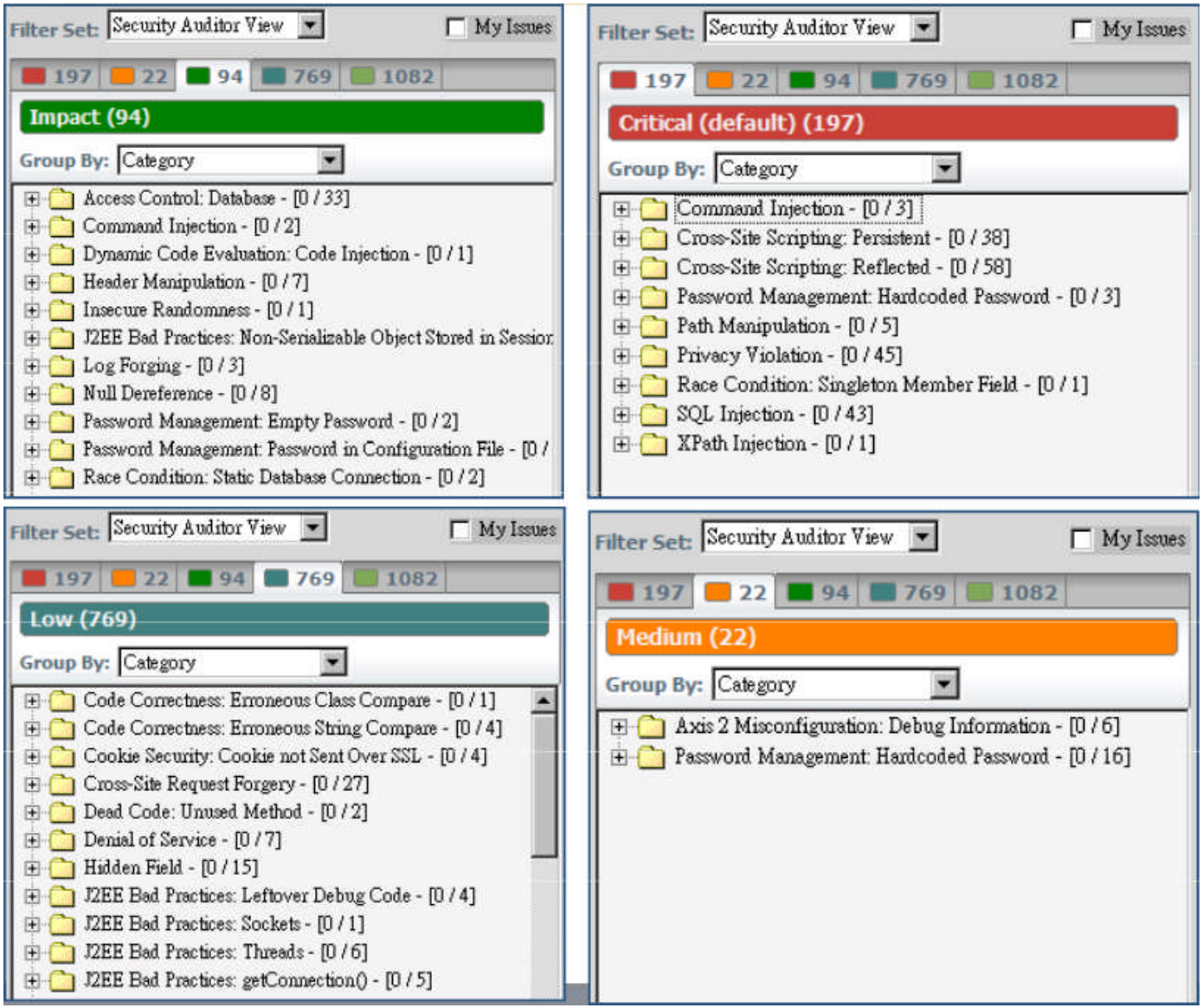
  (一旦發生對部門或企業的影響衝擊性)

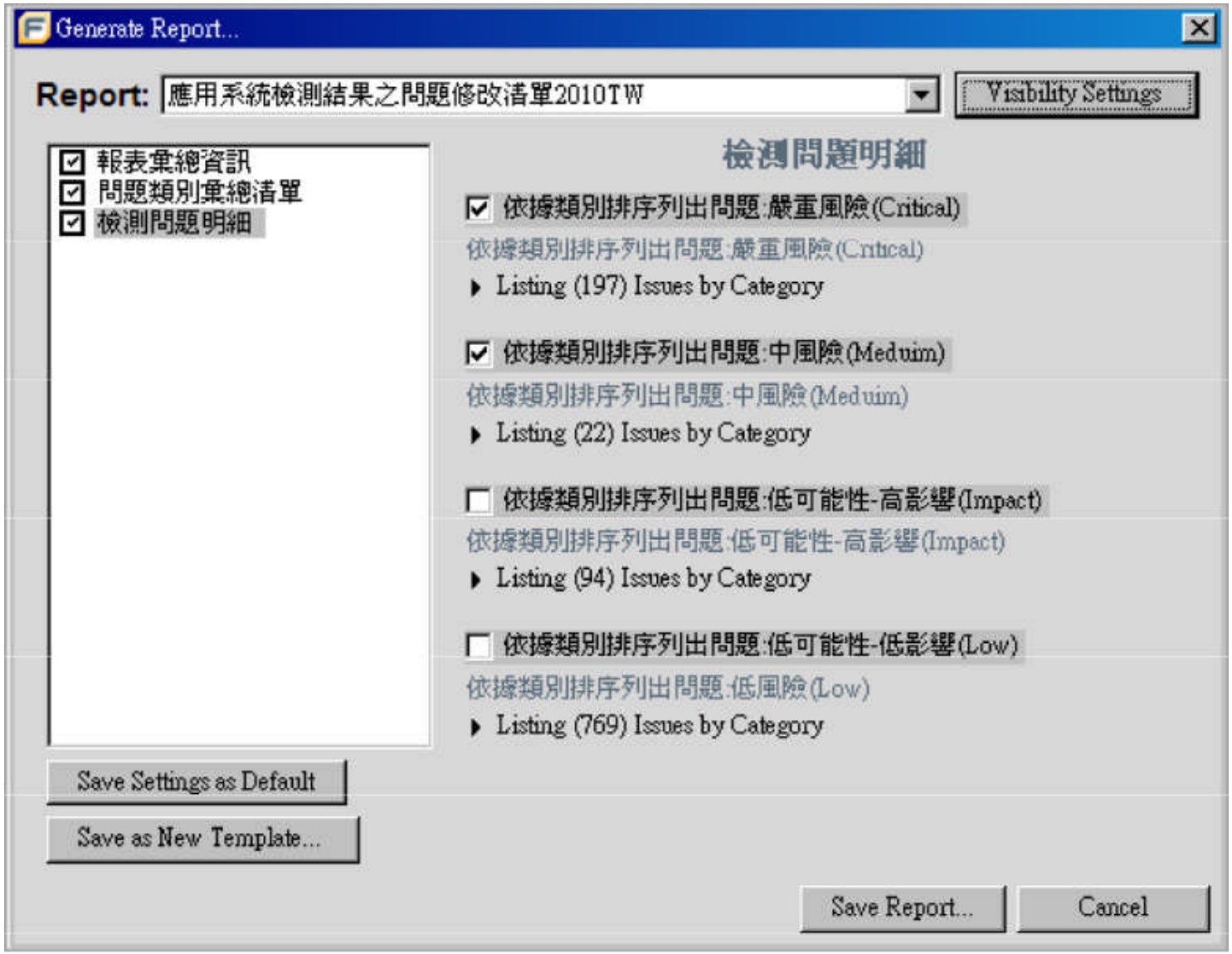
- **高準確度區：Critical / Medium**

- **低準確度區：High / Low**

  凡有安全漏洞或品質問題的嫌疑就列出的部分
  需要資安人員再人工複核是否真的會造成問題

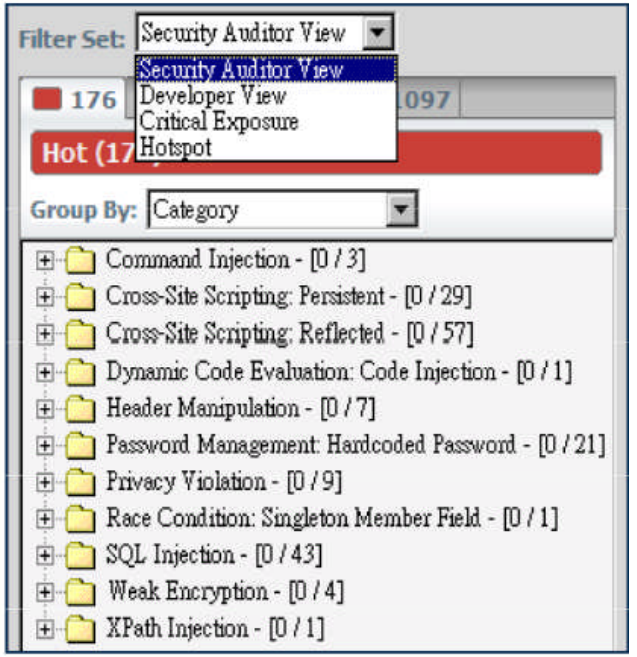



Filter Set: Security Auditor View
My Issues
197 22 94 769 1082
Impact (94)
Group By: Category
Access Control: Database - [0 / 33]
Command Injection - [0 / 2]
Dynamic Code Evaluation: Code Injection - [0 / 1]
Header Manipulation - [0 / 7]
Insecure Randomness - [0 / 1]
J2EE Bad Practices: Non-Serializable Object Stored in Session
Log Forging - [0 / 3]
Null Dereference - [0 / 8]
Password Management: Empty Password - [0 / 2]
Password Management: Password in Configuration File - [0 /
Race Condition: Static Database Connection - [0 / 2]
Filter Set: Security Auditor View
My Issues
197 22 94 769 1082
Critical (default) (197)
Group By: Category
Command Injection - [0 / 3]
Cross-Site Scripting: Persistent - [0 / 38]
Cross-Site Scripting: Reflected - [0 / 58]
Password Management: Hardcoded Password - [0 / 3]
Path Manipulation - [0 / 5]
Privacy Violation - [0 / 45]
Race Condition: Singleton Member Field - [0 / 1]
SQL Injection - [0 / 43]
XPath Injection - [0 / 1]
Filter Set: Security Auditor View
My Issues
197 22 94 769 1082
Low (769)
Group By: Category
Code Correctness: Erroneous Class Compare - [0 / 1]
Code Correctness: Erroneous String Compare - [0 / 4]
Cookie Security: Cookie not Sent Over SSL - [0 / 4]
Cross-Site Request Forgery - [0 / 27]
Dead Code: Unused Method - [0 / 2]
Denial of Service - [0 / 7]
Hidden Field - [0 / 15]
J2EE Bad Practices: Leftover Debug Code - [0 / 4]
J2EE Bad Practices: Sockets - [0 / 1]
J2EE Bad Practices: Threads - [0 / 6]
J2EE Bad Practices: getConnection() - [0 / 5]
Filter Set: Security Auditor View
My Issues
197 22 94 769 1082
Medium (22)
Group By: Category
Axis 2 Misconfiguration: Debug Information - [0 / 6]
Password Management: Hardcoded Password - [0 / 16]

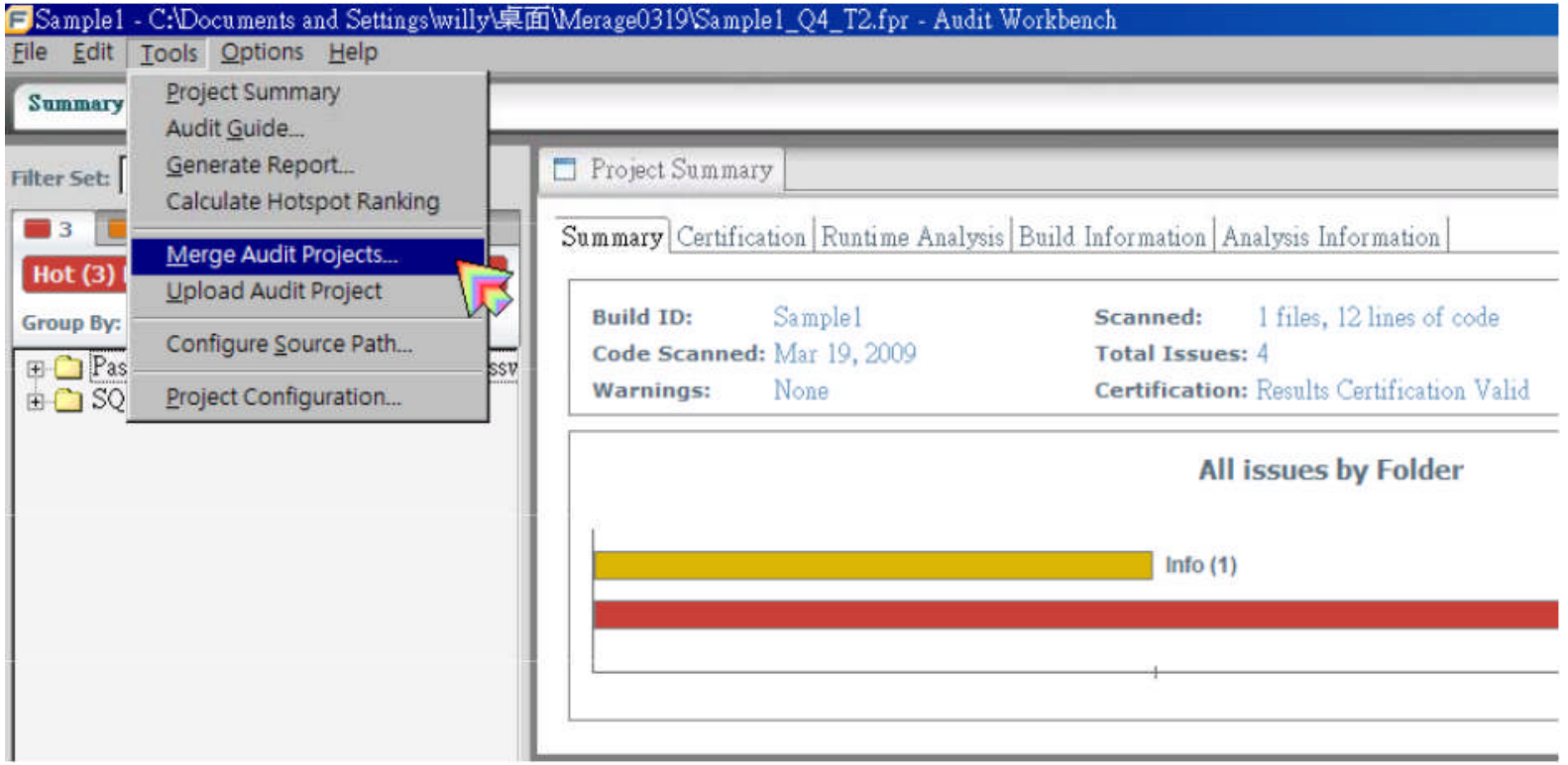

Generate Report...
Report:
應用系統檢測結果之問題修改清單2010TW
Visibility Settings
報表彙總資訊
問題類別彙總清單
檢測問題明細
檢測問題明細
依據類別排序列出問題:嚴重風險(Critical)
依據類別排序列出問題:嚴重風險(Critical)
Listing (197) Issues by Category
依據類別排序列出問題:中風險(Meduim)
依據類別排序列出問題:中風險(Meduim)
Listing (22) Issues by Category
依據類別排序列出問題:低可能性-高影響(Impact)
依據類別排序列出問題:低可能性-高影響(Impact)
Listing (94) Issues by Category
依據類別排序列出問題:低可能性-低影響(Low)
依據類別排序列出問題:低風險(Low)
Listing (769) Issues by Category
Save Settings as Default
Save as New Template...
Save Report...
Cancel

依據不同的需求訂定問題修改政策

- **自用系統**
  - AWB - Critical Exposure Policy
- **For Intranet 使用者**
  - AWB - Developer View Policy
- **For Internet 使用者**
  - AWB - Security Auditor View Policy
- **針對個別系統的需求**
  - AWB – 可以客製化自訂的 Policy

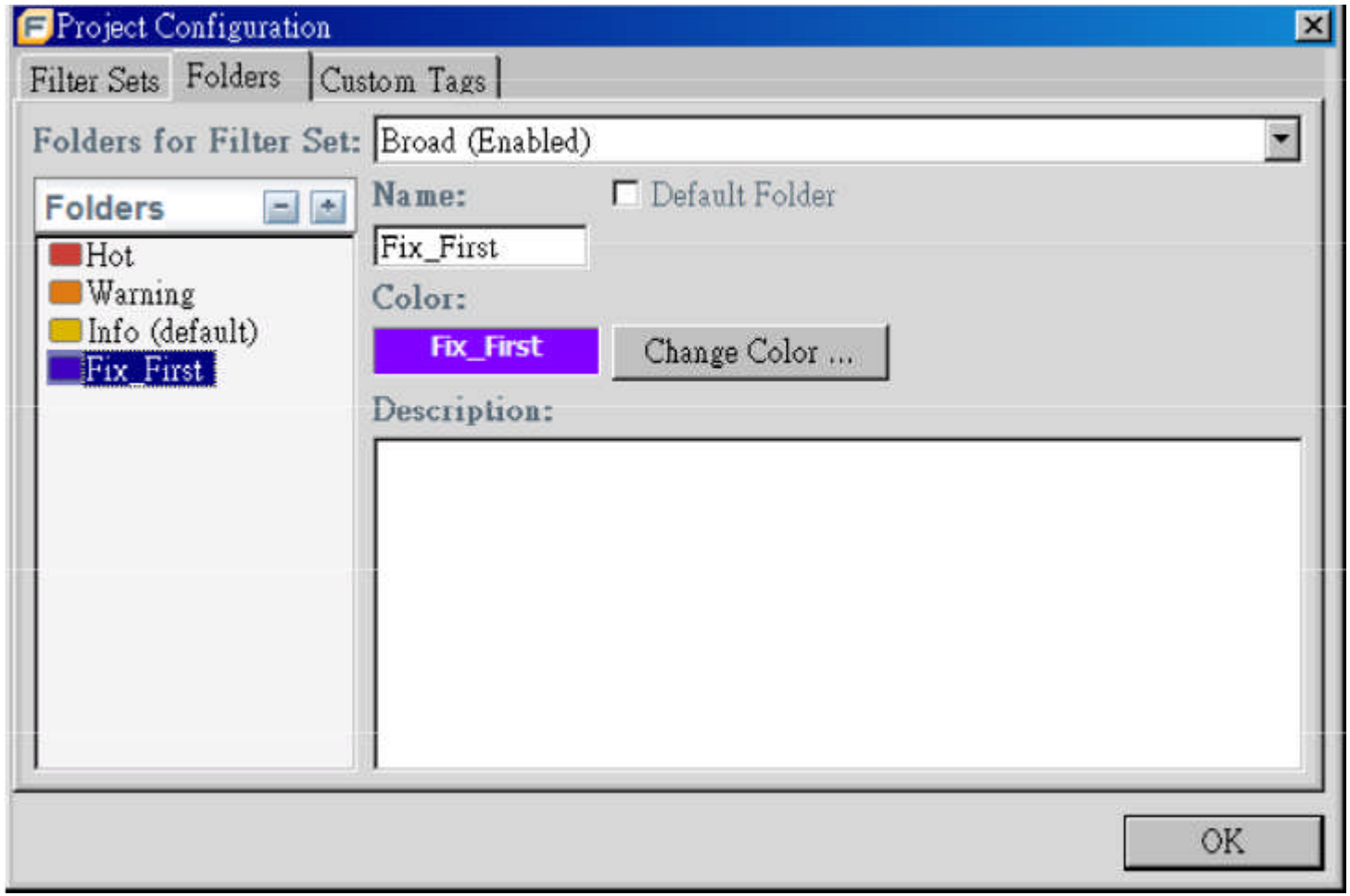


程式碼修復前後的差異分析



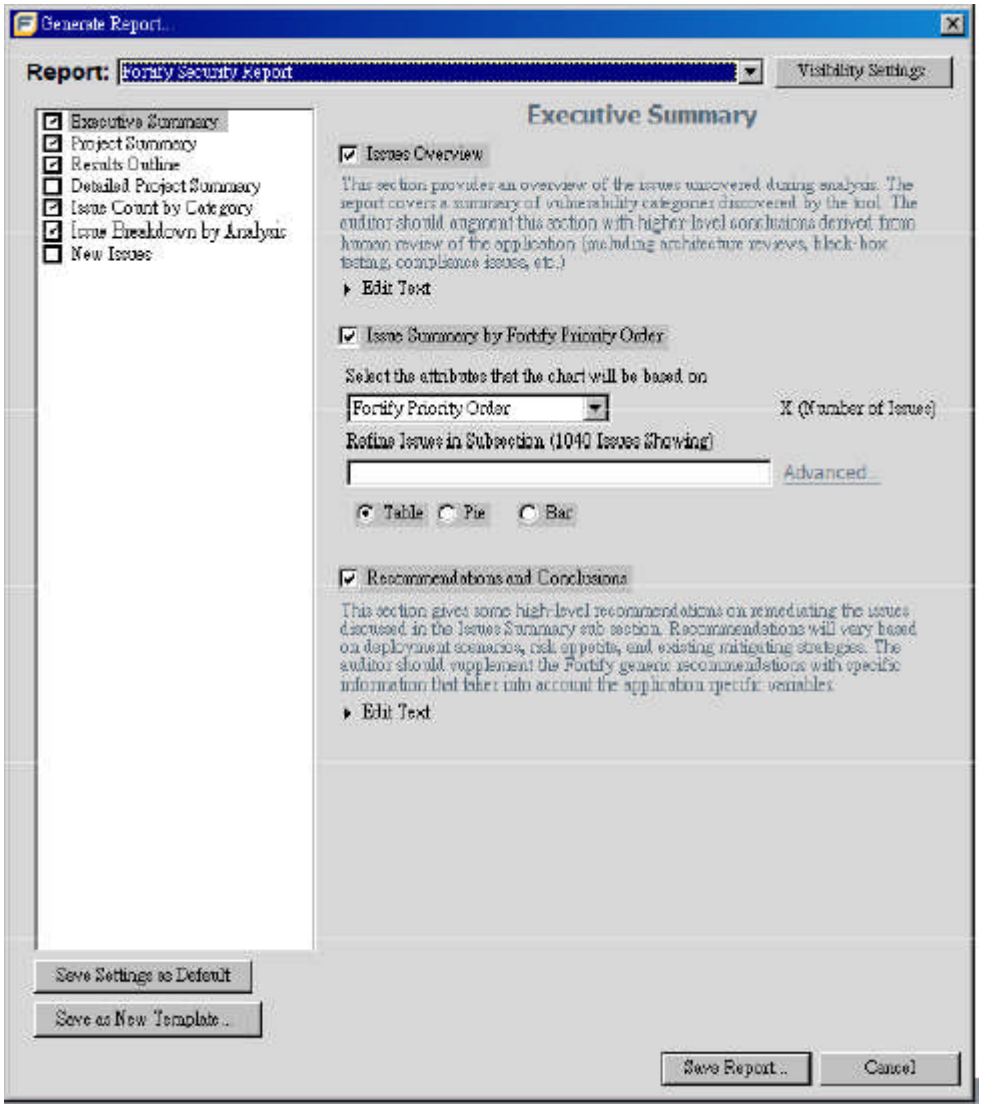
客製化程式碼安全政策

- **SQL Injection and Cross Site Script**



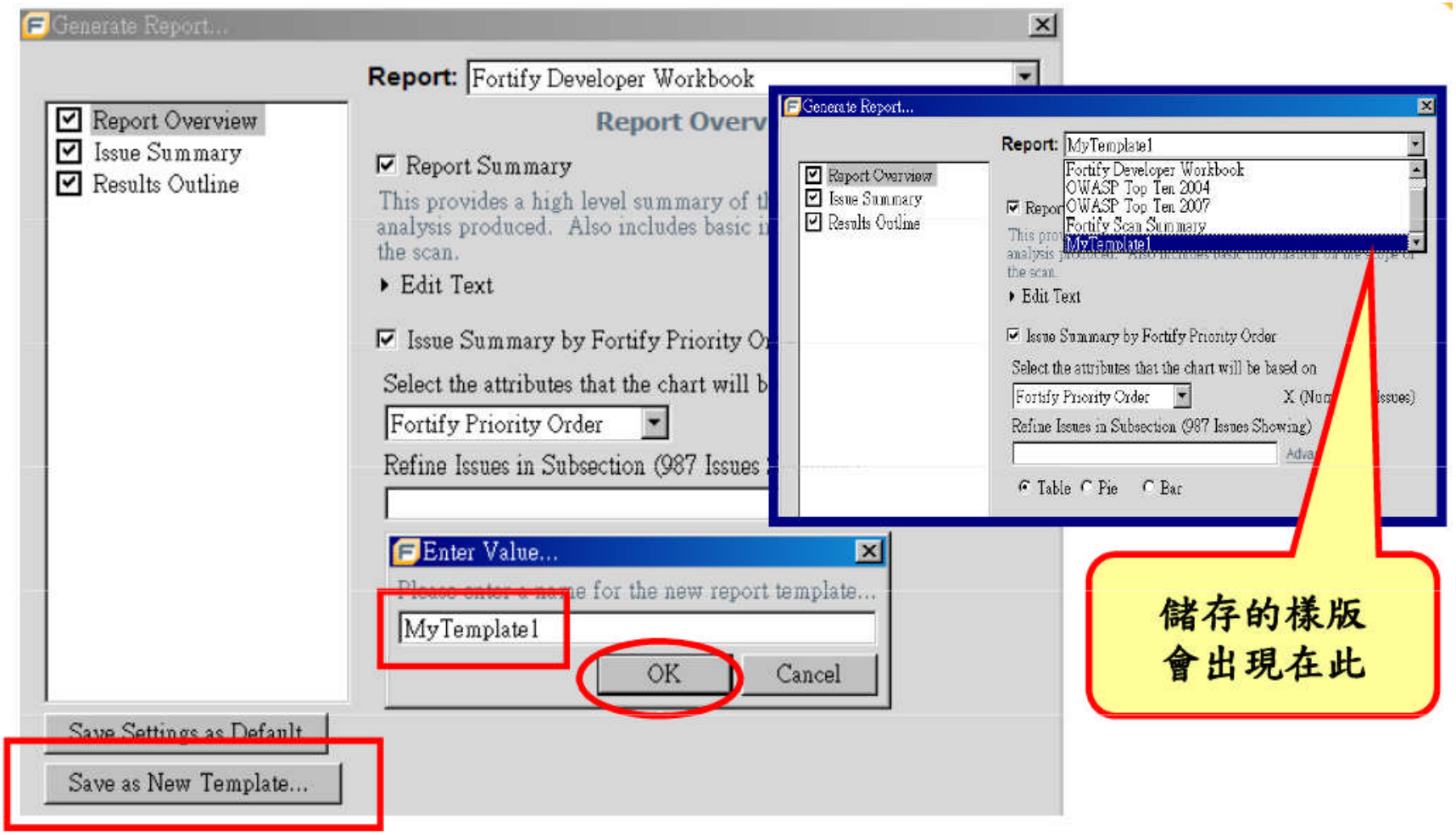
報表功能

- 使用報表精靈
- 預設樣板



自訂報表樣版

- 可供下次直接挑選

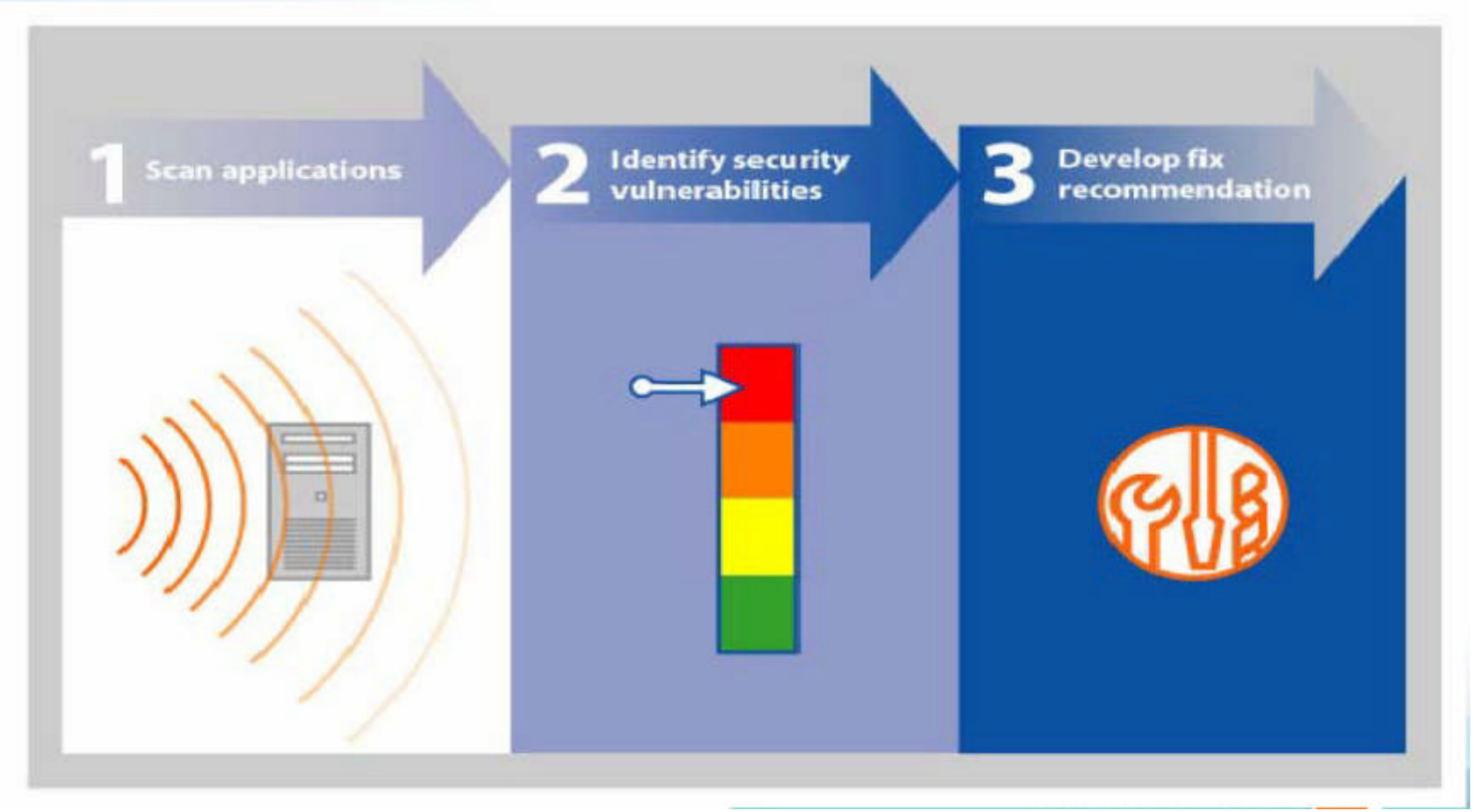


IBM Rational AppScan

簡介

- **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。
- 為什麼需要用**AppScan?**
  - 簡化發現與修復**Web**應用程式安全性問題的工作,降低維護資訊安全的成本。
- **AppScan**如何辦到的?
  - 模擬各種駭客攻擊的手法(**1400**種且持續增加),以無害的方式去測試運行中的**Web**應用程式,根據系統的回應,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。

簡單的使用步驟


1 Scan applications
2 Identify security vulnerabilities
3 Develop fix recommendation

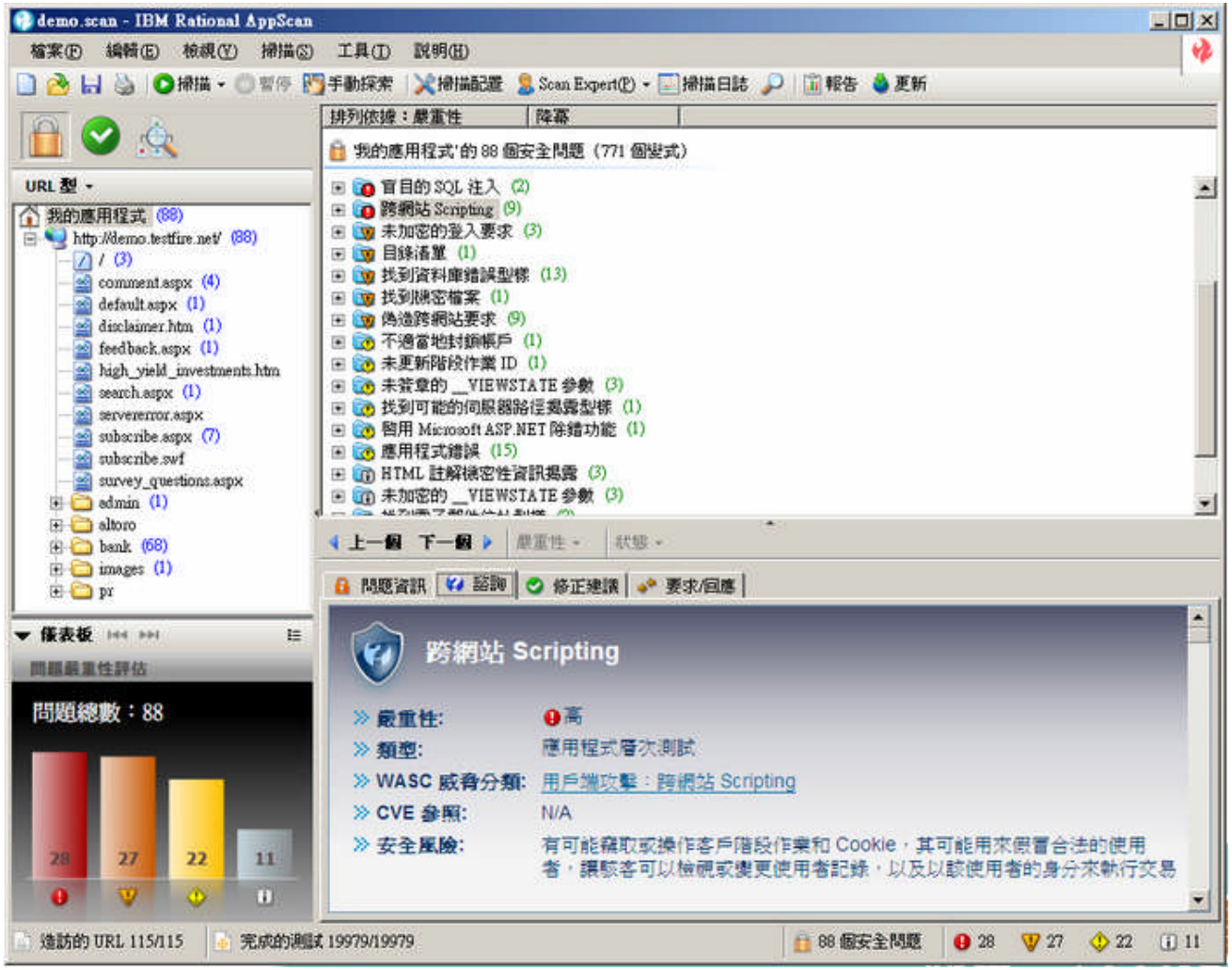
龐大的攻擊手法資料庫


WASC 威脅分類
用戶端攻擊：內容盜用
用戶端攻擊：跨網站 Scripting
指令執行：LDAP 注入
指令執行：OS 接管
指令執行：SQL 注入
指令執行：SSI 注入
指令執行：XPath 注入
指令執行：格式字串攻擊
指令執行：緩衝區溢位
授權：未充分設定階段作業有效期
授權：授權不足
授權：階段作業固定
授權：認證/階段作業預測
資訊揭露：可預測的資源位置
資訊揭露：目錄檢索
資訊揭露：資訊洩漏
資訊揭露：路徑遍訪
應用程式品質測試
應用程式隱私測試
鑑別：強制入侵
鑑別：鑑別不足
邏輯攻擊：功能濫用
邏輯攻擊：阻斷服務
高達1450項且
持續更新中!!!

Scan Expert

- 根據網站特性建議調整掃描設定

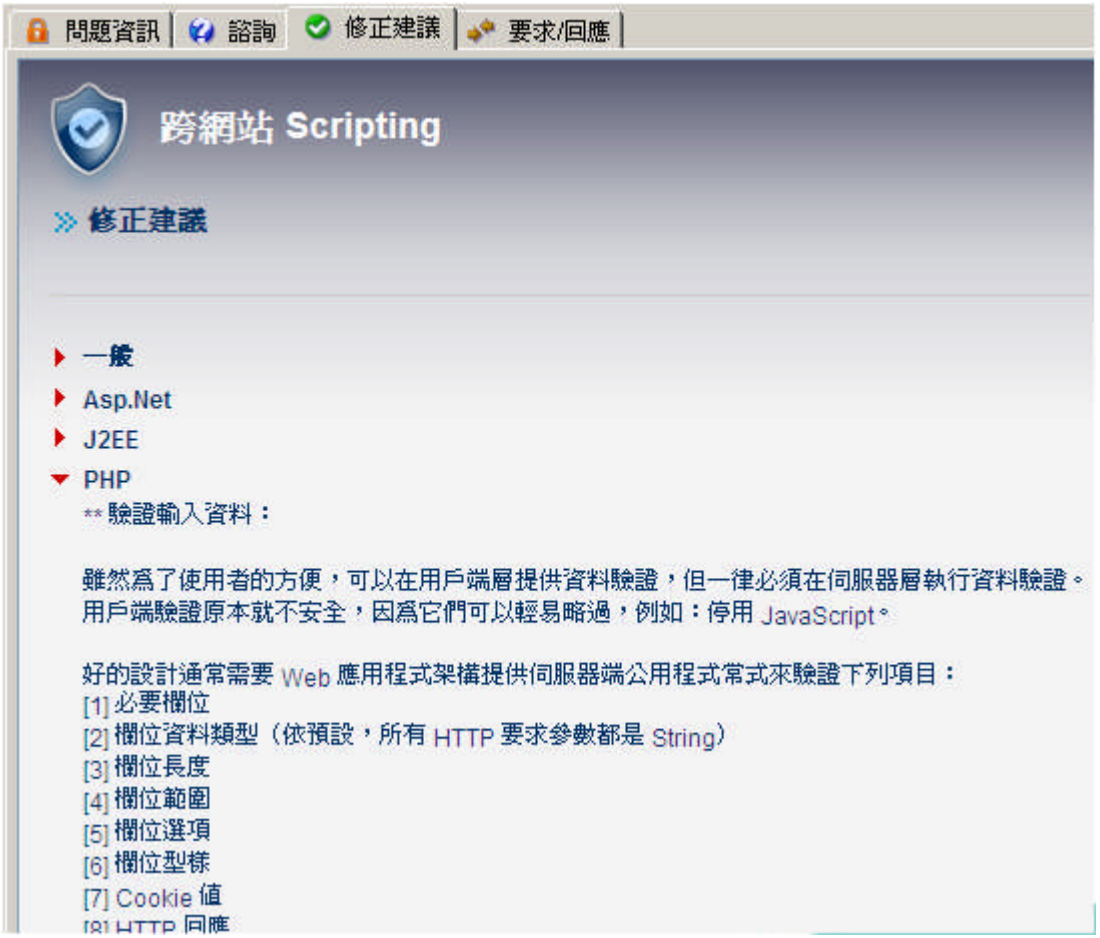
簡單明瞭的使用者介面


demo.scan - IBM Rational AppScan
檔案(F) 編輯(E) 檢視(V) 掃描(S) 工具(T) 說明(H)
掃描 手動探索 掃描配置 Scan Expert(P) 掃描日誌 報告 更新
排列依據：嚴重性
降幕
'我的應用程式'的 88 個安全問題（771 個變式）
盲目的 SQL 注入 (2)
跨網站 Scripting (9)
未加密的登入要求 (3)
目錄遍置 (1)
找到資料庫錯誤型樣 (13)
找到機密檔案 (1)
偽造跨網站要求 (9)
不適當地封鎖帳戶 (1)
未更新階段作業 ID (1)
未簽章的 __VIEWSTATE 參數 (3)
找到可能的伺服器路徑揭露型樣 (1)
啓用 Microsoft ASP.NET 除錯功能 (1)
應用程式錯誤 (15)
HTML 註解機密性資訊揭露 (3)
未加密的 __VIEWSTATE 參數 (3)
URL 型
我的應用程式 (88)
http://demo.testfire.net/ (88)
/ (3)
comment.aspx (4)
default.aspx (1)
disclaimer.htm (1)
feedback.aspx (1)
high_yield_investments.htm
search.aspx (1)
servererror.aspx
subscribe.aspx (7)
subscribe.swf
survey_questions.aspx
admin (1)
altoro
bank (68)
images (1)
pr
儀表板
問題嚴重性評估
問題總數：88
28
27
22
11
上一個 下一個
問題資訊 說明 修正建議 要求/回應
跨網站 Scripting
最重性: 高
類型: 應用程式層次測試
WASC 威脅分類: 用戶端攻擊：跨網站 Scripting
CVE 參照: N/A
安全風險: 有可能竊取或操作客戶階段作業和 Cookie，其可能用來假冒合法的使用者，讓駭客可以檢視或變更使用者記錄，以及以該使用者的身分來執行交易
造訪的 URL 115/115
完成的測試 19979/19979
88 個安全問題
28
27
22
11

檢測結果


排列依據：嚴重性
降幕
'我的應用程式'的 88 個安全問題（771 個變式）
盲目的 SQL 注入 (2)
跨網站 Scripting (9)
http://demo.testfire.net/bank/customize.aspx (2)
http://demo.testfire.net/bank/login.aspx (1)
http://demo.testfire.net/bank/transfer.aspx (2)
http://demo.testfire.net/comment.aspx (2)
http://demo.testfire.net/search.aspx (1)
txtSearch
http://demo.testfire.net/subscribe.aspx (1)
未加密的登入要求 (3)
目錄清單 (1)
找到資料庫錯誤型樣 (13)
找到機密檔案 (1)
偽造跨網站要求 (9)
不適當地封鎖帳戶 (1)

詳盡完整的補強建議


問題資訊
諮詢
修正建議
要求/回應
跨網站 Scripting
修正建議
一般
Asp.Net
J2EE
PHP
** 驗證輸入資料：
雖然爲了使用者的方便，可以在用戶端層提供資料驗證，但一律必須在伺服器層執行資料驗證。用戶端驗證原本就不安全，因爲它們可以輕易略過，例如：停用 JavaScript。
好的設計通常需要 Web 應用程式架構提供伺服器端公用程式常式來驗證下列項目：
[1] 必要欄位
[2] 欄位資料類型（依預設，所有 HTTP 要求參數都是 String）
[3] 欄位長度
[4] 欄位範圍
[5] 欄位選項
[6] 欄位型樣
[7] Cookie 值
[8] HTTP 回應

資安漏洞的測試回應


排列依據：嚴重性
我的應用程式'的 53 個安全
跨網站 Scripting (7)
http://demo.testfire.net
customize.aspx
lang
http://demo.testfire.net
uid
http://demo.testfire.net
http://demo.testfire.net
http://demo.testfire.net
HTTP 回應分割 (1)
未加密的登入要求 (2)
目錄清單 (2)
偽造跨網站要求 (4)
HTML 註解機密性資訊
未加密的 __VIEWSTAT
上一個 下一個
問題資訊
諮詢
顯示在瀏覽器中
變式：
顯示在瀏覽器中
POST /bank/login.aspx HTT
Content-Length: 67
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6
注入的 Script AppScan 似乎會包含在回應中。如果以下畫面顯示模擬產生注入 Script 的蹦現式畫面，即證明應用程式容易遭受「跨網站編寫 Script」的侵害。否則，如果要驗證這個漏洞：1) 開啓「要求/回應」標籤，然後按一下「顯示在瀏覽器中」，看看是否會出現蹦現式畫面。請注意，某些 Script 語法是瀏覽器專屬的，因此如果未蹦現注入的警示，請嘗試不同的瀏覽器（用滑鼠右鍵按一下瀏覽器 > 檢視來源 > 另存新檔...）。2) 檢查原始測試回應中警示 Script 的有效性。
呈現的測試回應
新視窗
AltoroMutual
DEMO SITE ONLY
ONLINE BANKING LOGIN
11595
OK
模擬當這個頁面在瀏覽器中開啓時，會顯示的蹦現式畫面
dback | Search

報告產出

詳細安全問題

有漏洞的 URL：http://demo.testfire.n

此 URL 總計有 3 個安全問題

[1/3] SQL 注入

嚴重性： 高

測試類型： 應用程式

有漏洞的 URL： http://demo.te

補救作業： 從使用者輸入

變式 1/6 [ID=7238]

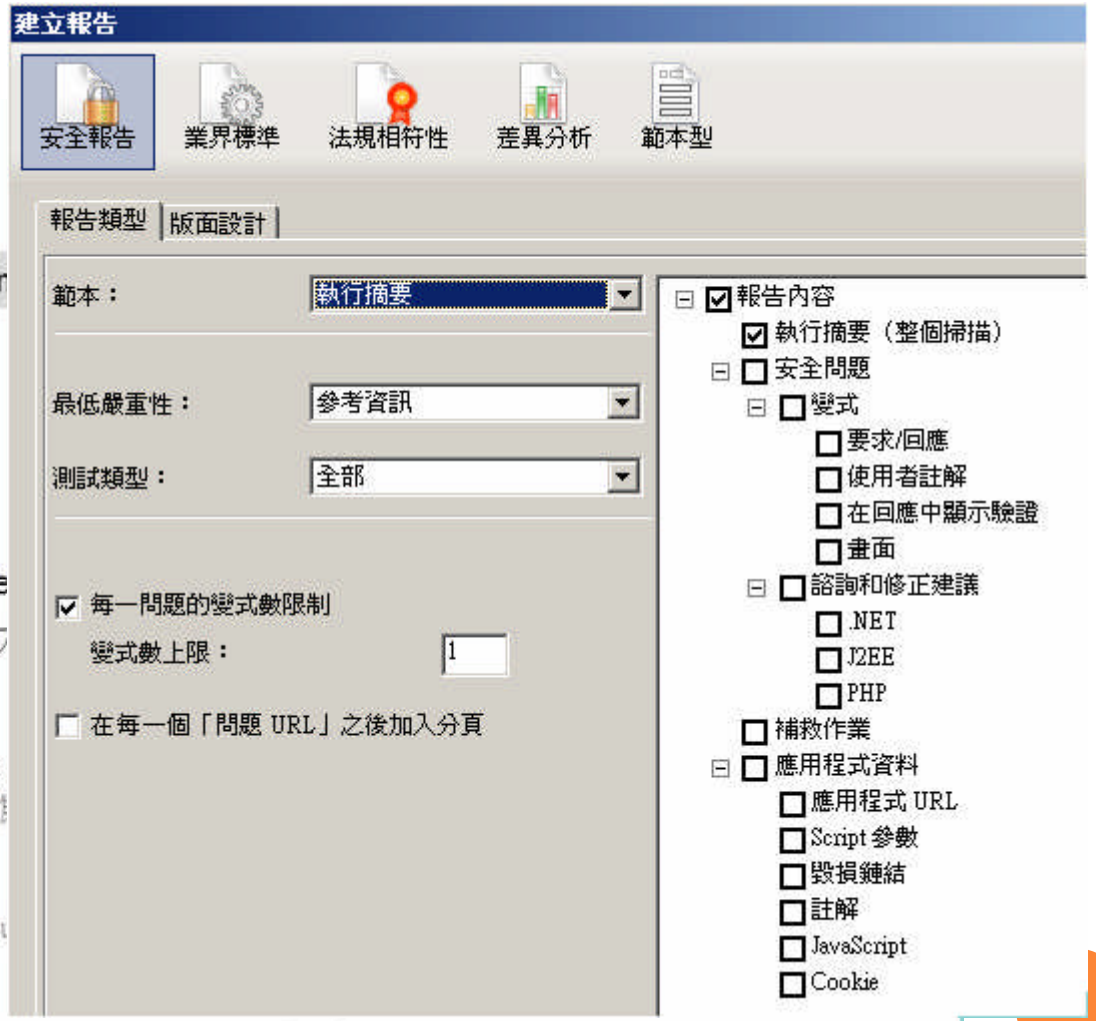
下列變更已套用到原始要求：

• 將 Cookie 'amUserId' 的值設

回應中的驗證：

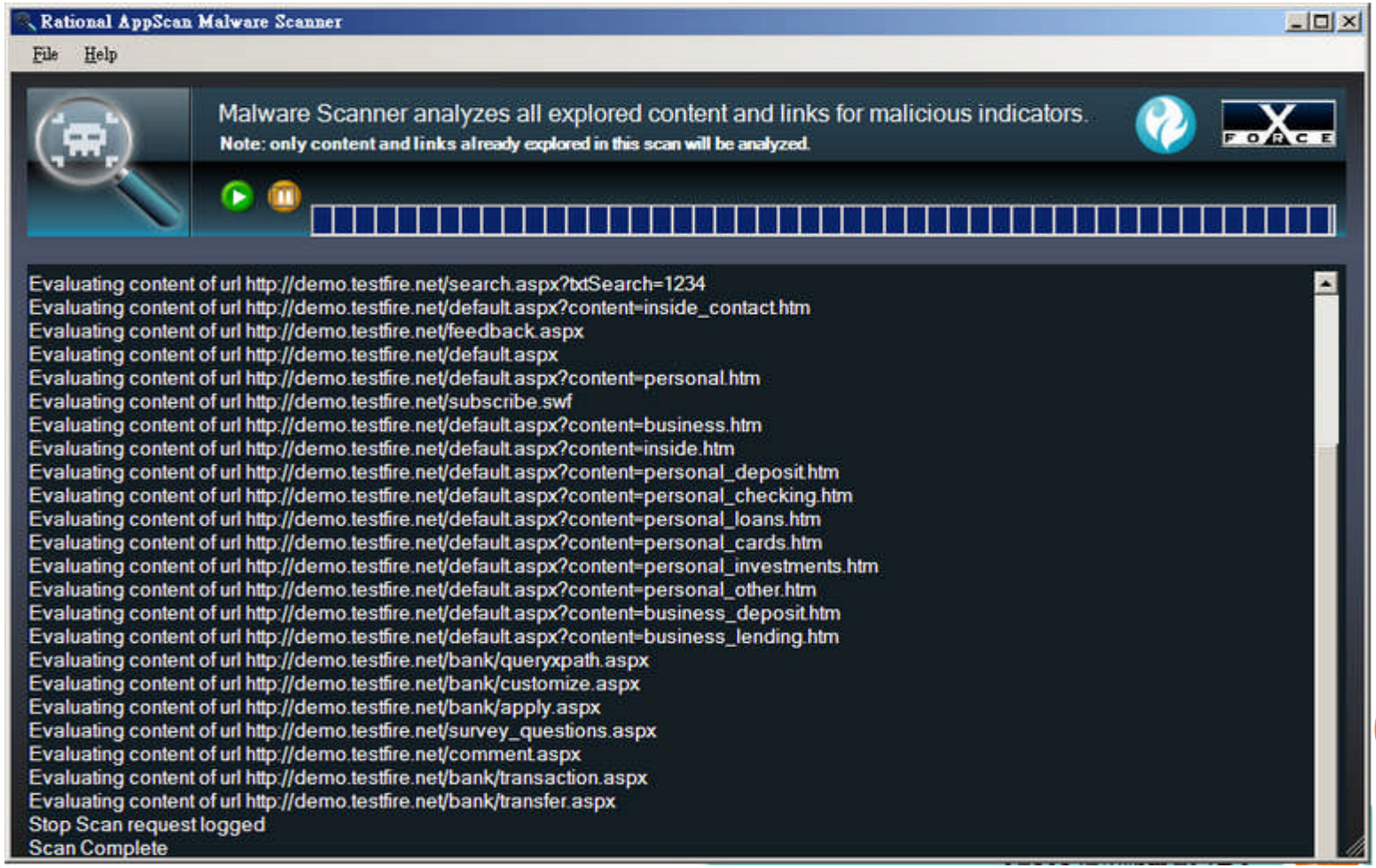
• <span id="_ctl0_Content_lblSu
= ".

• System.Data.OleDb.**OleDbException**: Syntax error in string in query expression 'userid = ".



惡意程式(Malware)掃瞄器

- 可檢測網站是否已遭植入惡意程式或連結



Feature Summary

1	網站弱點類型超過1450項且持續更新，掃描可靠度高
2	加強支援 AJAX, Flash, Web Services (最早支援Web 2.0 App)
3	高品質的中文化介面與內容
4	豐富的報表範本與格式 (純文字, HTML, PDF, WORD)
5	多執行緒式(Multi-thread)掃描 + 調適型(Adaptive)測試流程 更進一步提升效能與精確度
6	人工探索與多步驟作業錄製，讓測試涵蓋面更完整
7	AppScan SDK & AppScan eXtensions Framework 元件擴充與客製化測試彈性高

簡報結束