



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

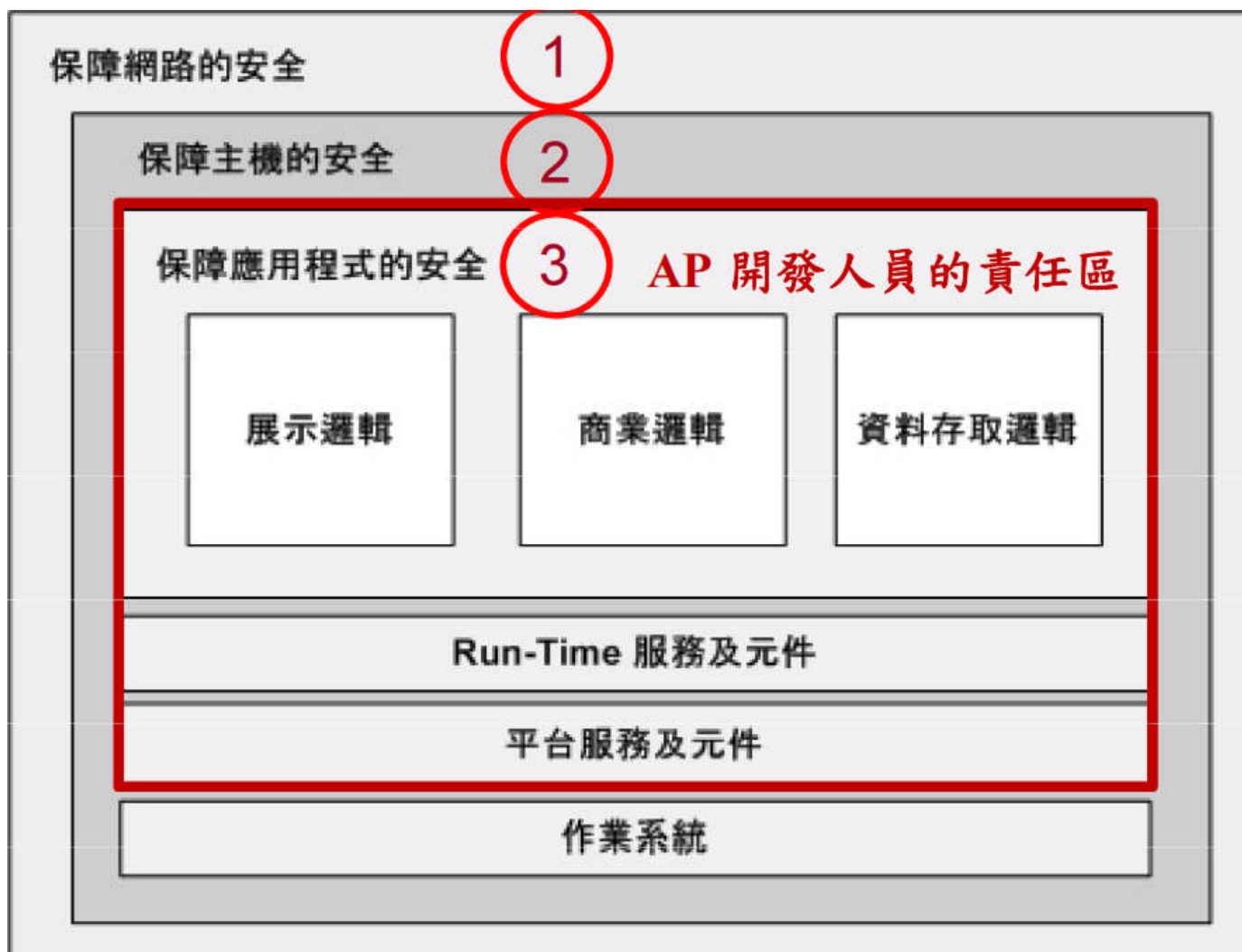
Open Web Application Security Project

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



English Japanese Korean Simplified Chinese Traditional Chinese

Expand All | Close All

A Taxonomy of Coding Errors that Affect Security

- ColdFusion
- C/C++
- C#/VB.NET/ASP.NET
- HTML
- Java/JSP
- Javascript
- PHP
- Python
- PLSQL/TSQL
- VisualBasic/VBScript/ASP
- Webservices
- XML

Fortify Taxonomy: Software Security Errors

This site presents a taxonomy of software security errors developed by the Fortify Software Security Research Group together with Dr. Gary McGraw. Each vulnerability category is accompanied by a detailed description of the issue with references to original sources, and code excerpts, where applicable, to better illustrate the problem.

The organization of the classification scheme is described with the help of terminology borrowed from Biology: vulnerability categories are referred to as *phyla*, while collections of vulnerability categories that share the same theme are referred to as *kingdoms*. Vulnerability phyla are classified into "seven plus one" pernicious kingdoms presented in the order of importance to software security:

1. Input Validation and Representation
2. API Abuse
3. Security Features
4. Time and State
5. Errors
6. Code Quality
7. Encapsulation
- *. Environment

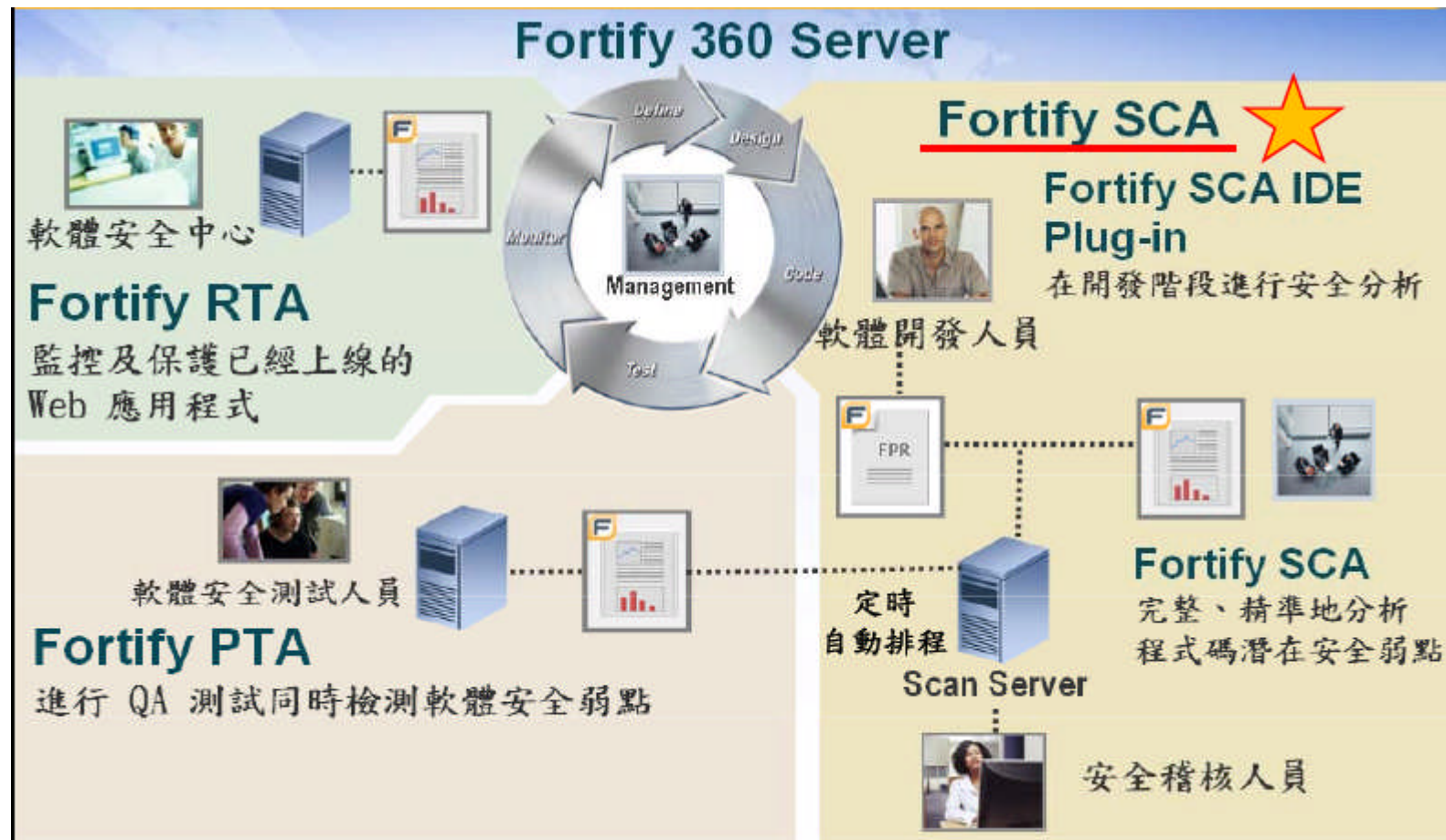
The first seven kingdoms are associated with security defects in source code, while the last one describes security issues outside the actual code. To browse the kingdom and phylum descriptions, simply navigate the taxonomy tree on the left.

The primary goal of defining this taxonomy is to organize sets of security rules that can be used to help software developers understand the kinds of errors that have an impact on security. By better understanding how systems fail, developers will better analyze the systems they create, more readily identify and address security problems when they see them, and generally avoid repeating the same mistakes in the future.

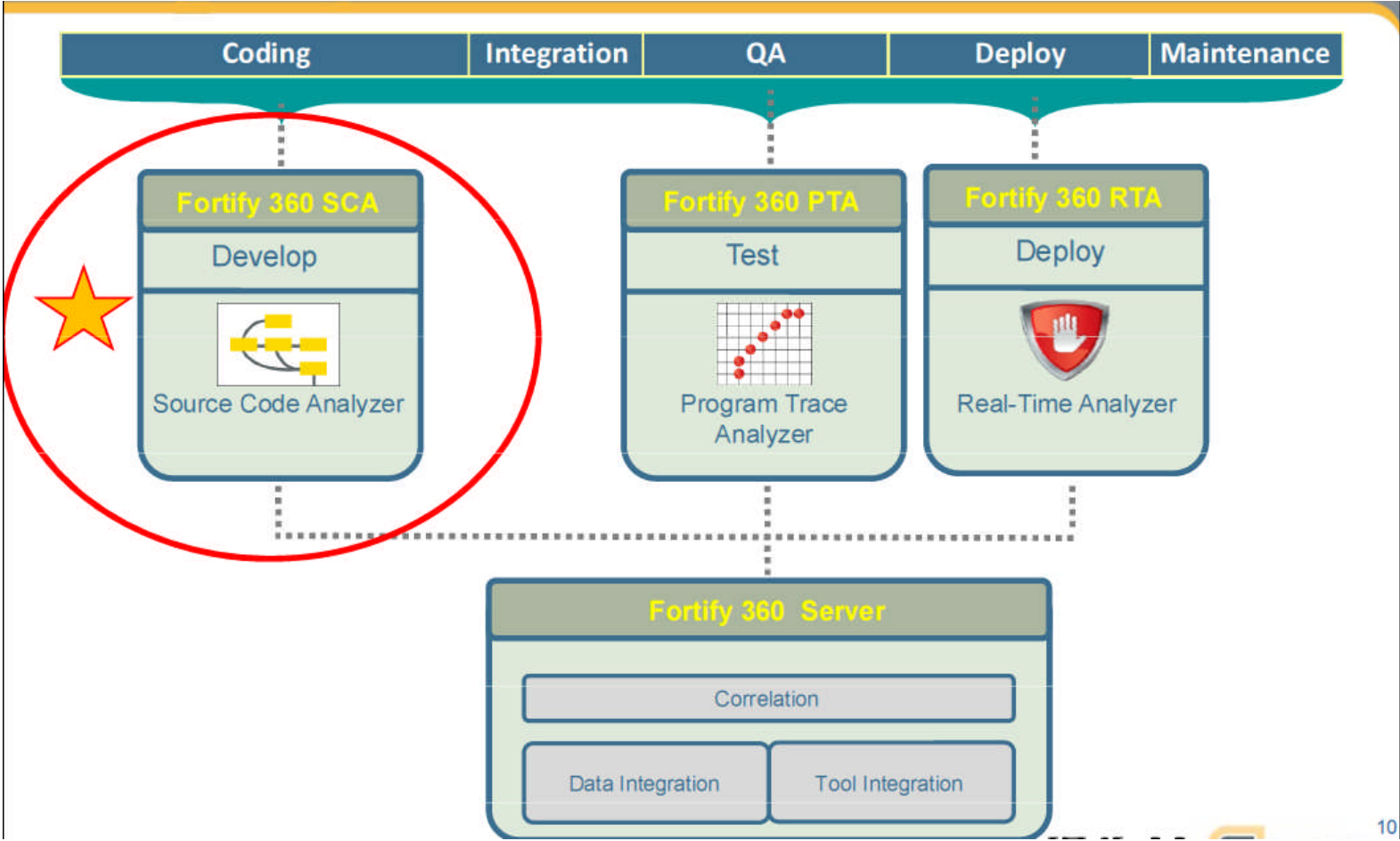
When put to work in an analysis tool, a set of security rules organized according to this taxonomy is a powerful teaching mechanism. Because developers today are by and large unaware of the myriad ways they can introduce security problems into their work, making a taxonomy like this available should provide tangible benefits to the software security community.

FORTIFY

- Fortify 360 軟體安全開發週期的完整解決方案



FORTIFY



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)

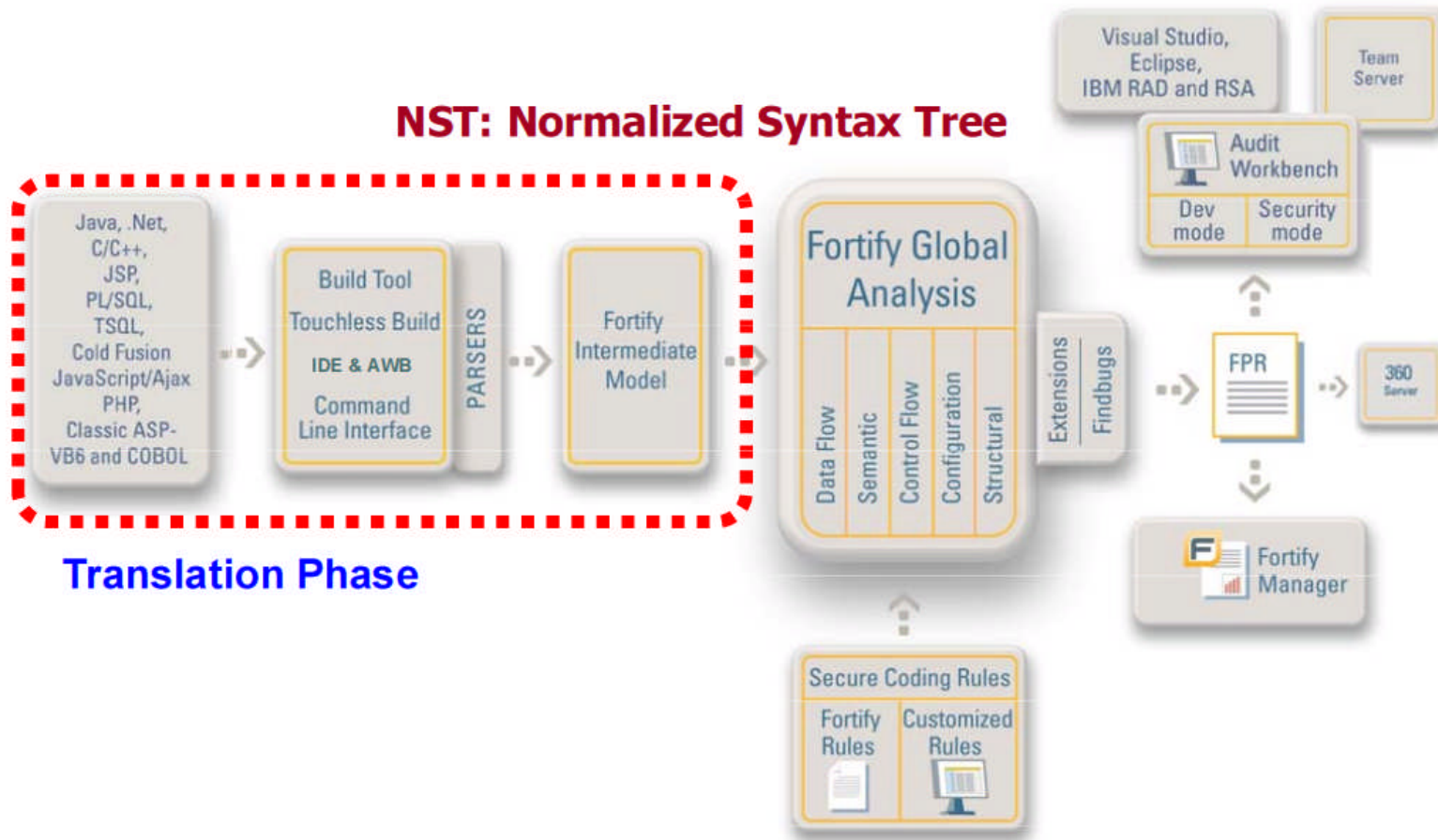


FORTIFY

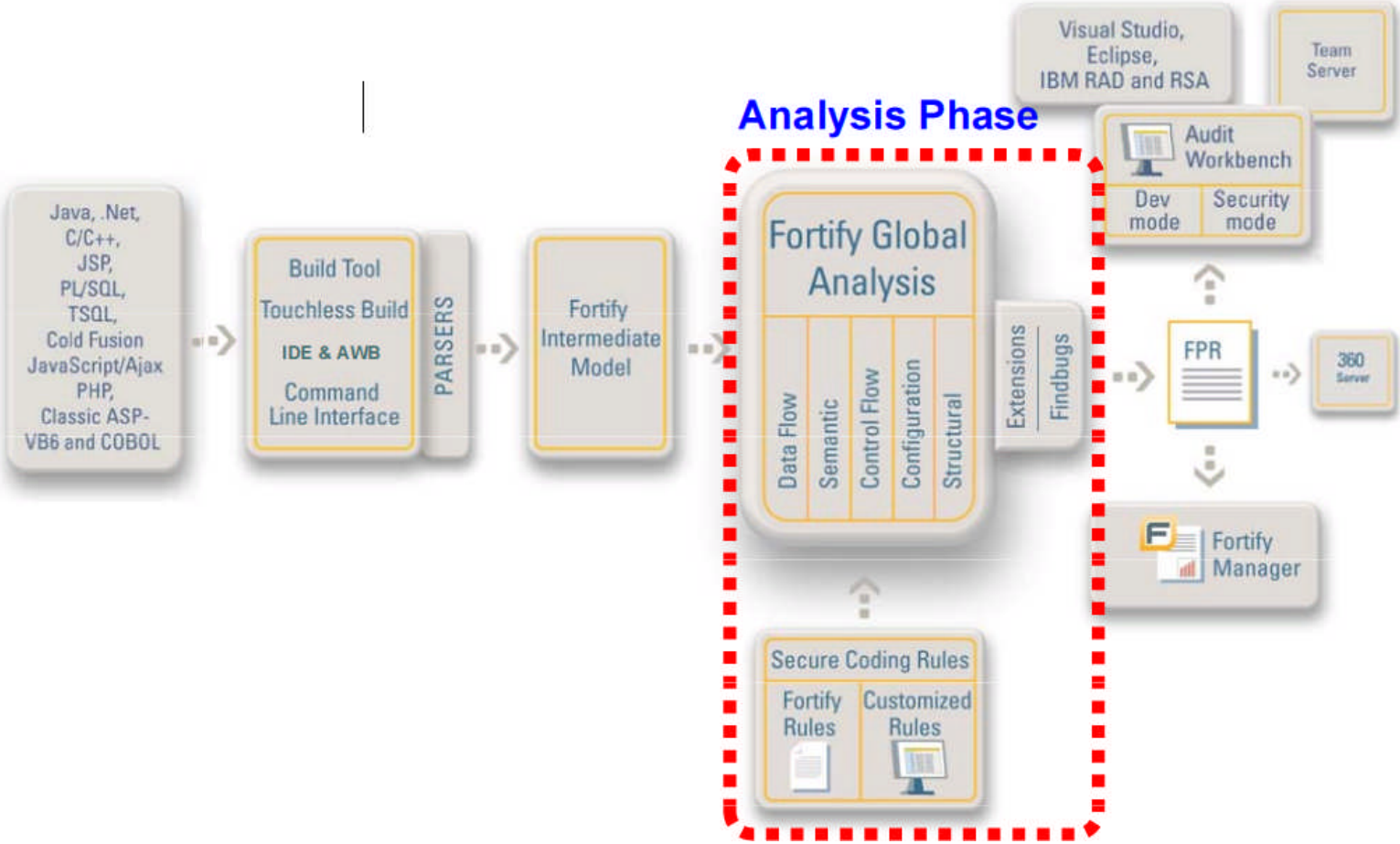
- Fortify 360 SCA 檢測程式碼安全的程序
- 轉譯階段 Translation Phase
- 分析階段 Analysis Phase
- 稽核階段 Audit Phase



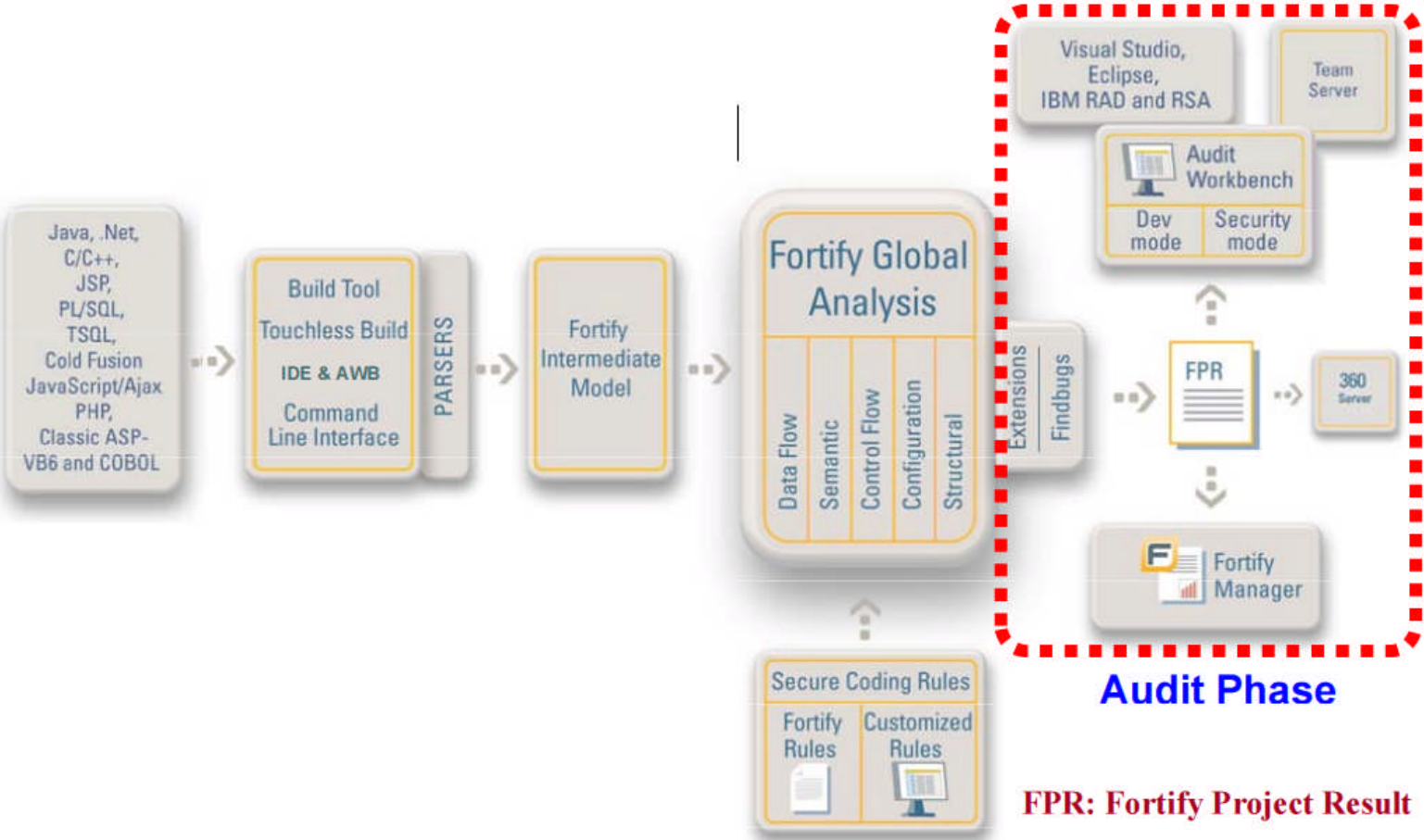
FORTIFY TRANSLATION PHASE



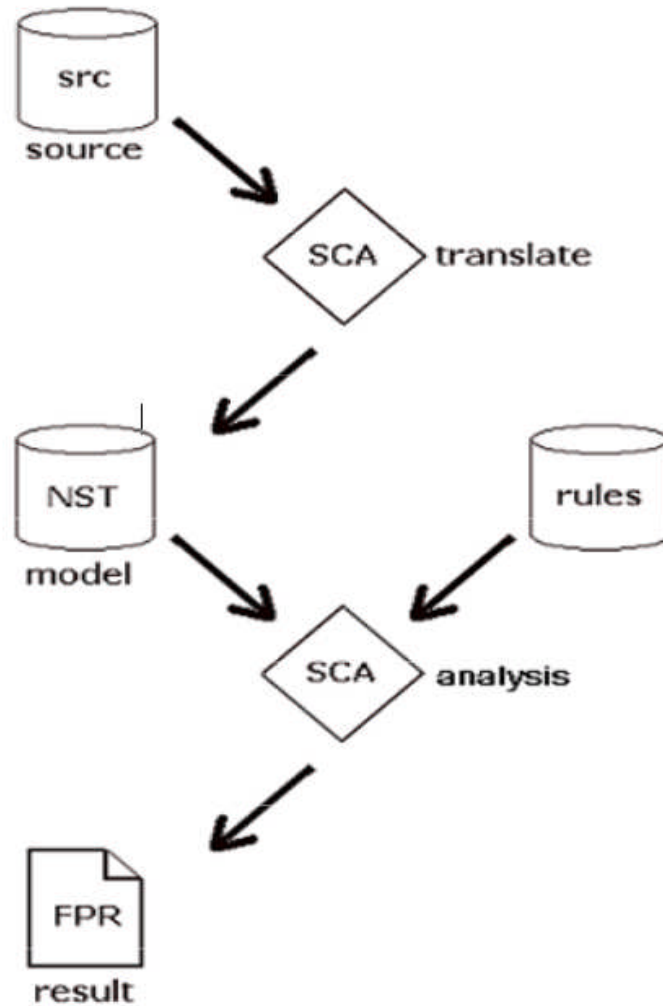
FORTIFY ANALYSIS PHASE



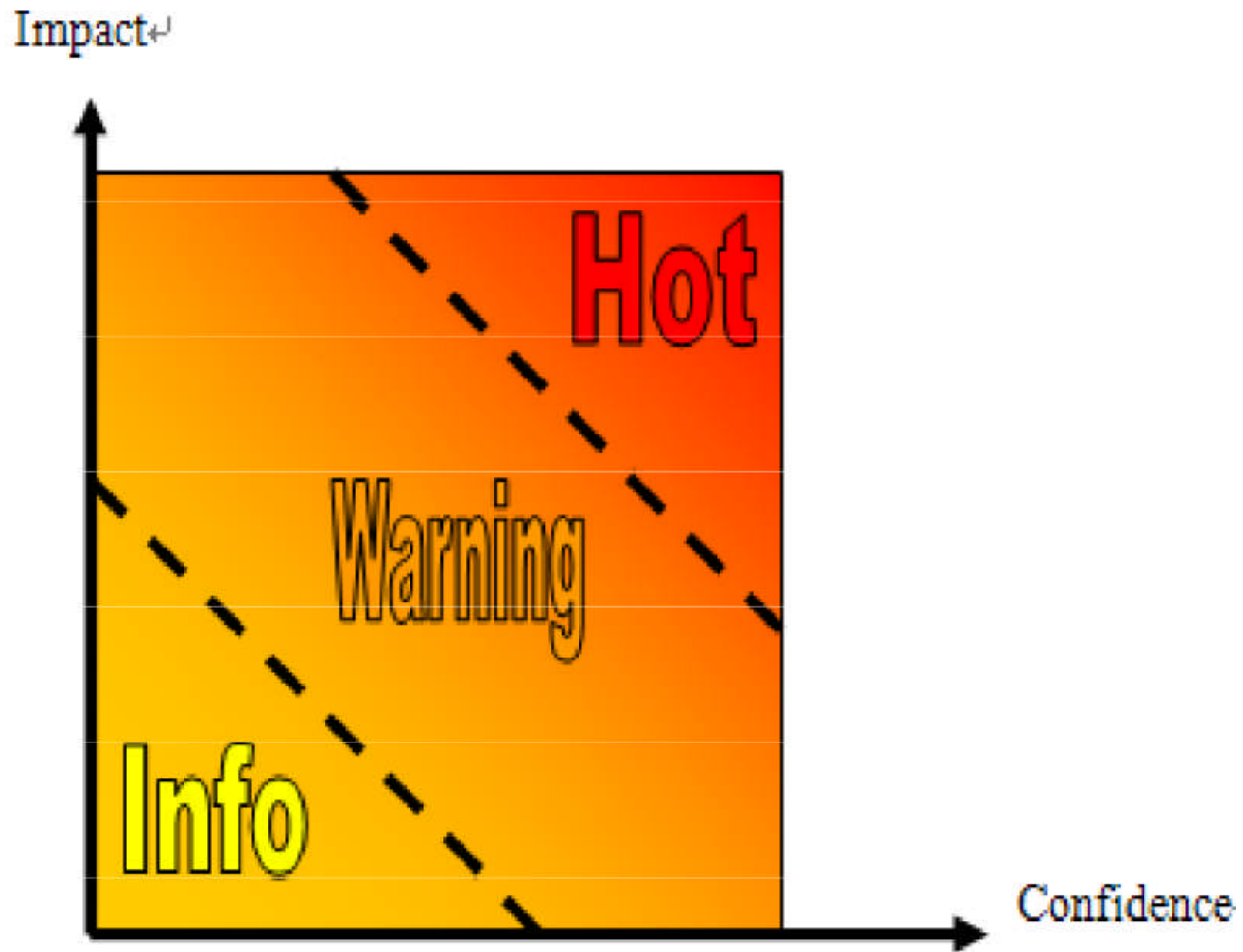
FORTIFY AUDIT PHASE



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

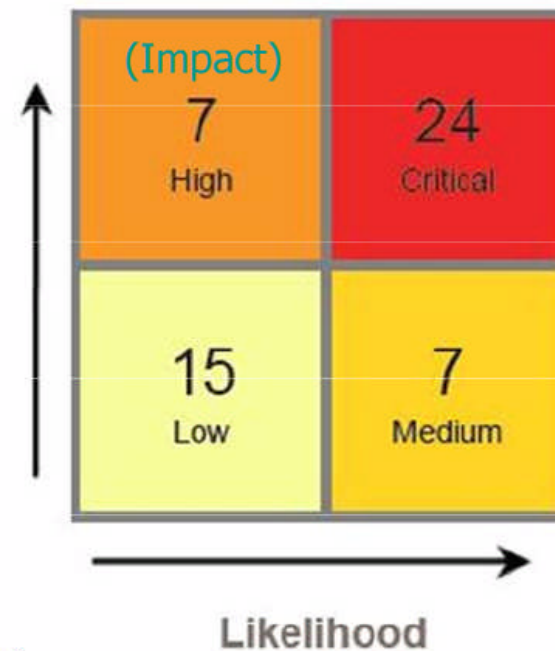
(一旦發生對部門或企業的影響衝擊性)

■ 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

Issues by Priority



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 - [0 / 1]
- + Log Forging - [0 / 3]
- + Null Dereference - [0 / 8]
- + Password Management: Empty Password - [0 / 2]
- + Password Management: Password in Configuration File - [0 / 1]
- + 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

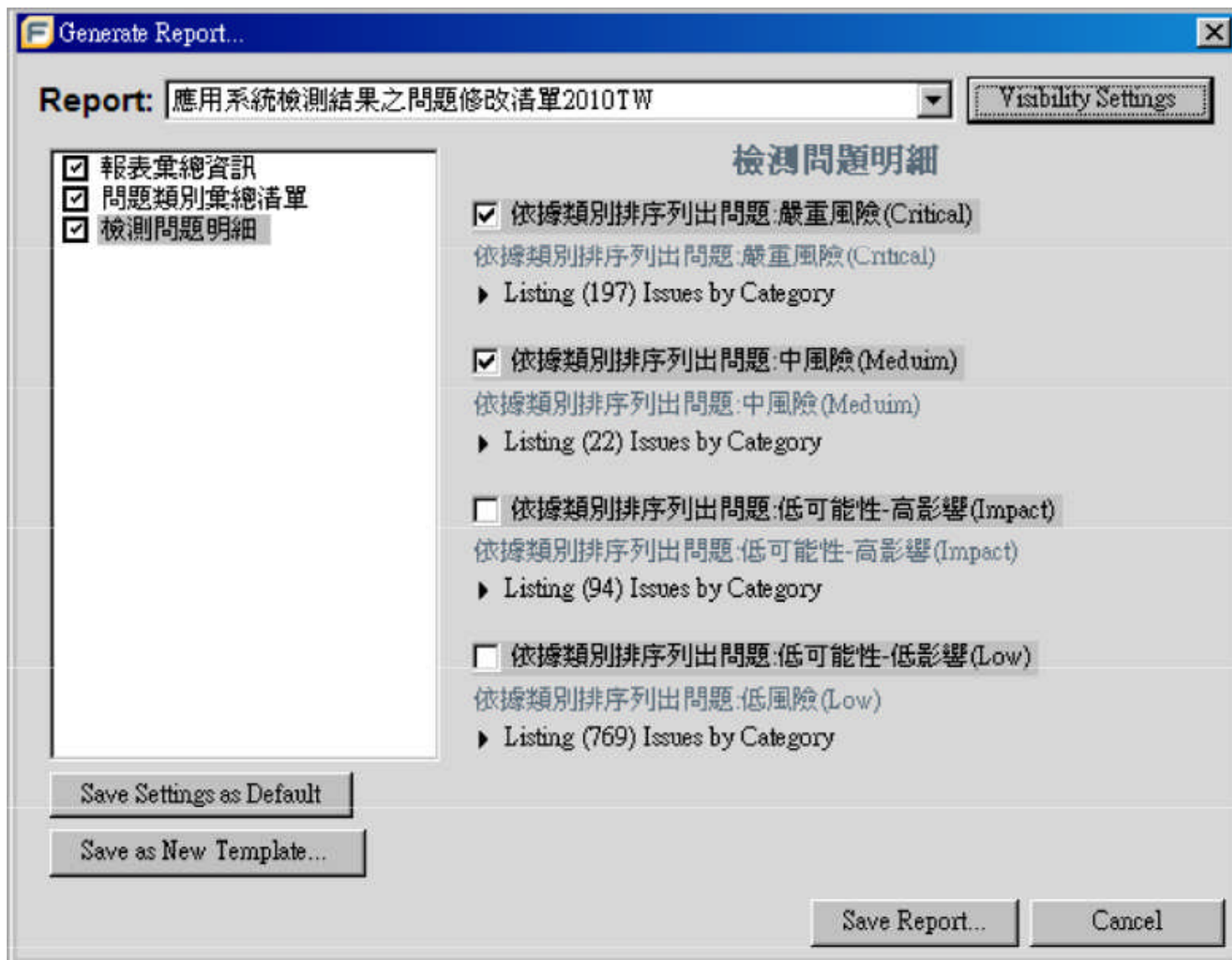
197 22 94 769 1082

Medium (22)

Group By: Category

- + Axis 2 Misconfiguration: Debug Information - [0 / 6]
- + Password Management: Hardcoded Password - [0 / 16]





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

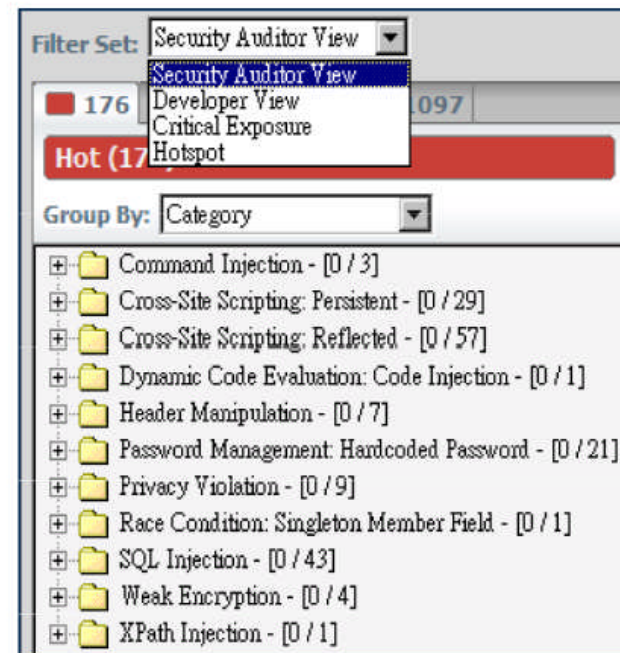
- AWB - Developer View Policy

- 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

The screenshot displays the Audit Workbench interface. The title bar reads "Sample1 - C:\Documents and Settings\willy\桌面\Merage0319\Sample1_Q4_T2.fpr - Audit Workbench". The menu bar includes "File", "Edit", "Tools", "Options", and "Help". The "Tools" menu is open, with "Merge Audit Projects..." highlighted. Other menu items include "Project Summary", "Audit Guide...", "Generate Report...", "Calculate Hotspot Ranking", "Upload Audit Project", "Configure Source Path...", and "Project Configuration...".

The main window shows the "Project Summary" tab. The summary includes:

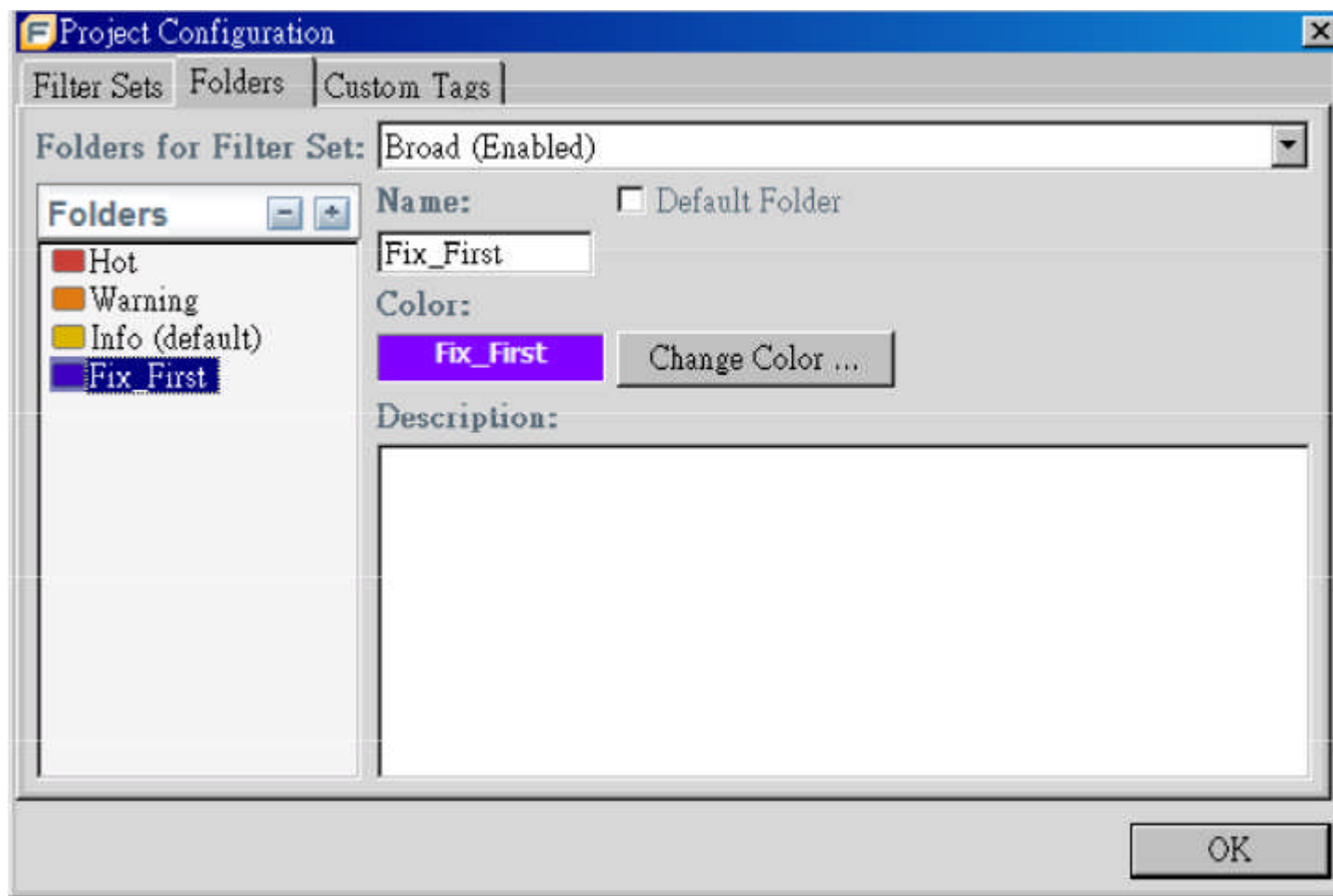
Build ID:	Sample1	Scanned:	1 files, 12 lines of code
Code Scanned:	Mar 19, 2009	Total Issues:	4
Warnings:	None	Certification:	Results Certification Valid

Below the summary is a section titled "All issues by Folder" with a horizontal bar chart. The chart shows a single bar for "Info (1)" with a value of 1.



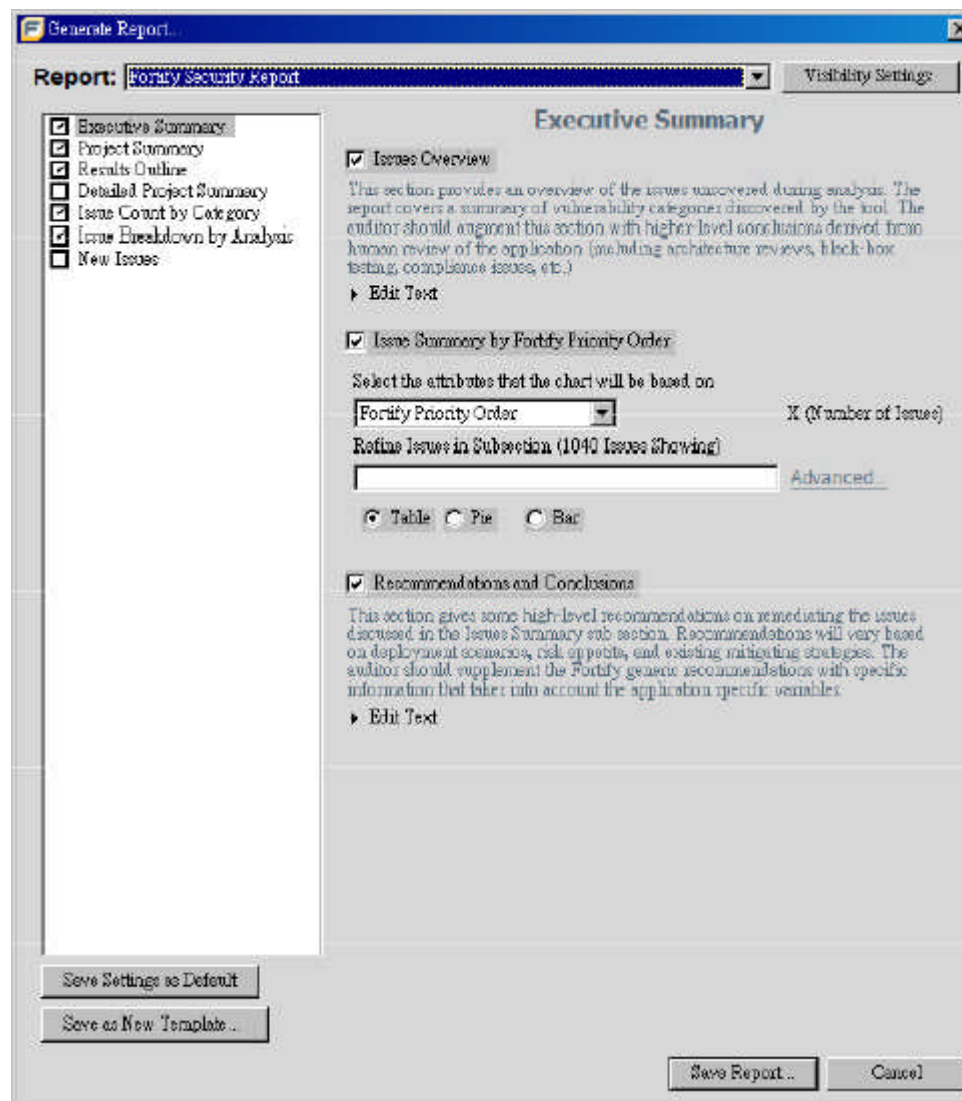
客製化程式碼安全政策

- SQL Injection and Cross Site Script



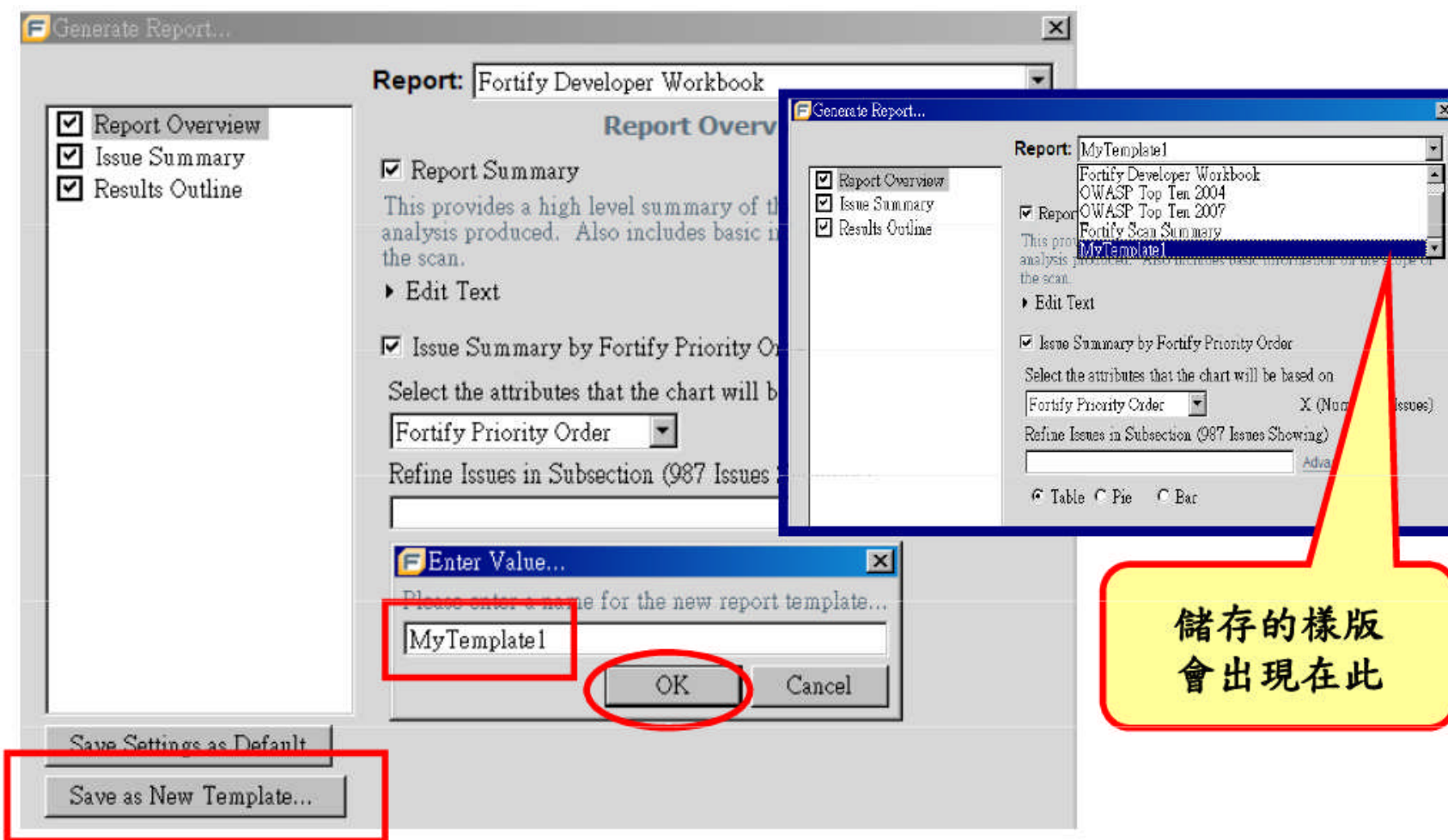
報表功能

- 使用報表精靈
- 預設樣板



自訂報表樣版

- 可供下次直接挑選



儲存的樣版
會出現在此

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？

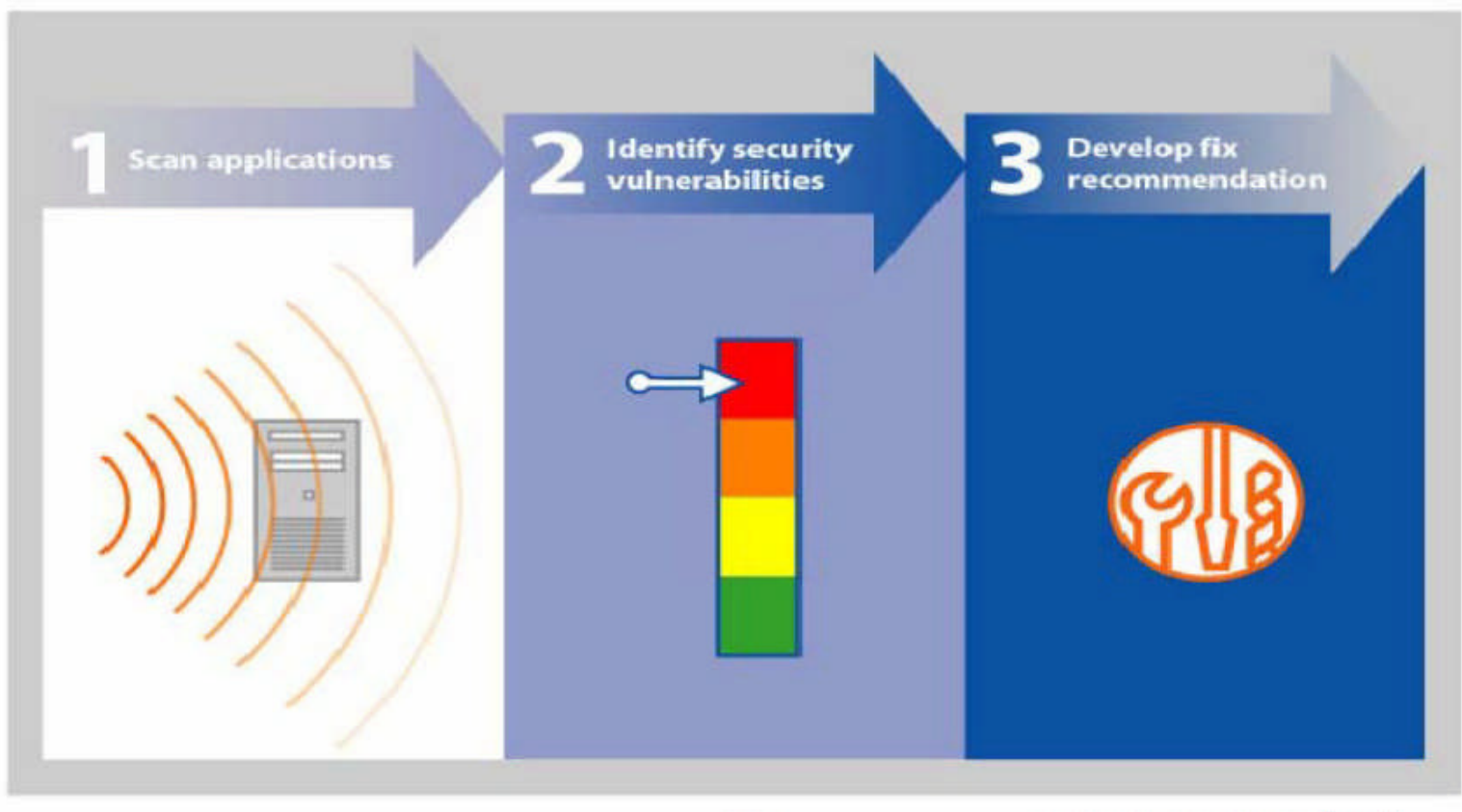
– 簡化發現與修復Web應用程式安全性問題的工作,降低維護資訊安全的成本。

○ 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



龐大的攻擊手法資料庫

The screenshot displays a software interface for security testing. On the left is a navigation pane with options like 'URL 與伺服器', '登入管理', and '掃描選項'. The main area is titled 'WASC 威脅分類' and contains a table with columns for 'WASC 威脅分類', '嚴重性', '應用 CVEs', and '類型'. Below the table, there are sections for '檢閱' and '常例', and a '修正錯誤' button. A red starburst callout is overlaid on the interface, containing the text: '高達1450項目且持續更新中!!!'. The right side of the interface shows a list of WASC threat categories, each with a checkbox and a plus icon, including '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：目錄搜索', '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', and '邏輯攻擊：阻斷服務'.

WASC 威脅分類	嚴重性	應用 CVEs	類型
<input checked="" type="checkbox"/> 用戶端攻擊：內容盜用			
<input checked="" type="checkbox"/> 用戶端攻擊：跨網站 Scripting			
<input checked="" type="checkbox"/> 指令執行：LDAP 注入			
<input checked="" type="checkbox"/> 指令執行：OS 接管			
<input checked="" type="checkbox"/> 指令執行：SQL 注入			
<input checked="" type="checkbox"/> 指令執行：SSI 注入			
<input checked="" type="checkbox"/> Misc: (Wright: Guestbook.pl 伺服器漏洞)	高	是	高級漏洞
<input checked="" type="checkbox"/> 駭取伺服器認證檔案	高	是	應用程序
<input checked="" type="checkbox"/> 指令執行：XPath 注入			
<input checked="" type="checkbox"/> 指令執行：格式字串攻擊			
<input checked="" type="checkbox"/> 指令執行：緩衝區溢位			
<input checked="" type="checkbox"/> 授權：未充分設定階段作業有效期			
<input checked="" type="checkbox"/> 授權：授權不足			
<input checked="" type="checkbox"/> 授權：階段作業固定			

檢閱 當前掃描的記錄

常例 修正錯誤

嚴重性: 高
類型: 基礎架構測試
WASC 威脅分類: 指令執行 SSI 注入
CVE 參照: CAN-2009-1053
安全風險: 有可能

可能原因
網站上安裝了...

詳細說明

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：目錄搜索
- 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

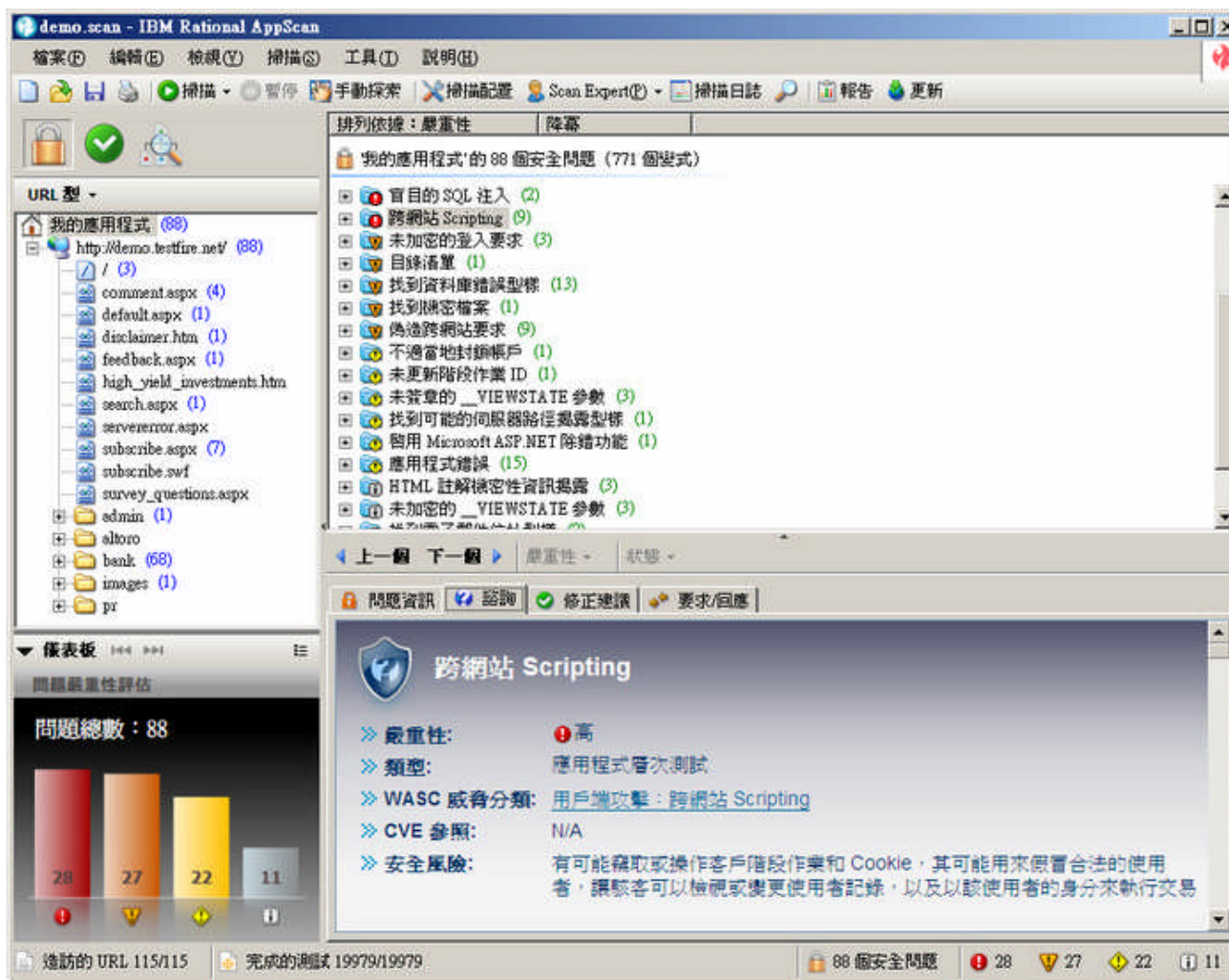


SCAN EXPERT

- 根據網站特性建議調整掃描設定



簡單明瞭的使用者介面



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



The screenshot shows a web application security tool interface with a navigation bar at the top containing icons for '問題資訊' (Problem Information), '諮詢' (Consultation), '修正建議' (Correction Advice), and '要求/回應' (Request/Response). The main content area is titled '跨網站 Scripting' (Cross-site Scripting) and features a '修正建議' (Correction Advice) section. Under this section, there are expandable categories: '一般' (General), 'Asp.Net', 'J2EE', and 'PHP'. The 'PHP' category is expanded, showing a sub-section '驗證輸入資料' (Validate Input Data). The text in this section states that while client-side validation is convenient, server-side validation is essential for security, as client-side validation can be easily bypassed (e.g., by disabling JavaScript). It then lists items that a good design should verify on the server side:

- 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 降

我的應用程式'的 53 個安全

- 跨網站 Scripting (7)
 - http://demo.testfire.net
 - customize.aspx
 - lang
 - uid
 - http://demo.testfire.net
 - 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

問題資訊 諮詢

顯示在瀏覽器中 報告誤

變式： 顯示在瀏覽器中

POST /bank/login.aspx HTTP/1.1
Content-Length: 67
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0)
Host: demo.testfire.net

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 的離現式畫面，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」，看看是否會出現離現式畫面。請注意，某些 Script 語法是瀏覽器專屬的，因此如果未離現注入的警示，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

ONLINE BANKING LOGIN PERSONAL CREDIT REPORTING INVESTMENT AND RETIREMENT

SEARCH

11595

模擬當這個頁面在瀏覽器中開啓時，會顯示的離現式畫面



報告產出

詳細安全問題

有漏洞的 URL : <http://demo.testfire.r>
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：

```
• <p><b><span id="_ctl0_Content_lblSt  
="</span></b></p>  
</span></b></p>  
• <p><span id="_ctl0_Content_lblDetails">System.Data.OleDb.OleDbException: Syntax error in string in query  
expression 'userid = '.
```

建立報告

安全報告 業界標準 法規相符性 差異分析 範本型

報告類型 版面設計

範本: 執行摘要

最低嚴重性: 參考資訊

測試類型: 全部

每一問題的變式數限制
變式數上限: 1

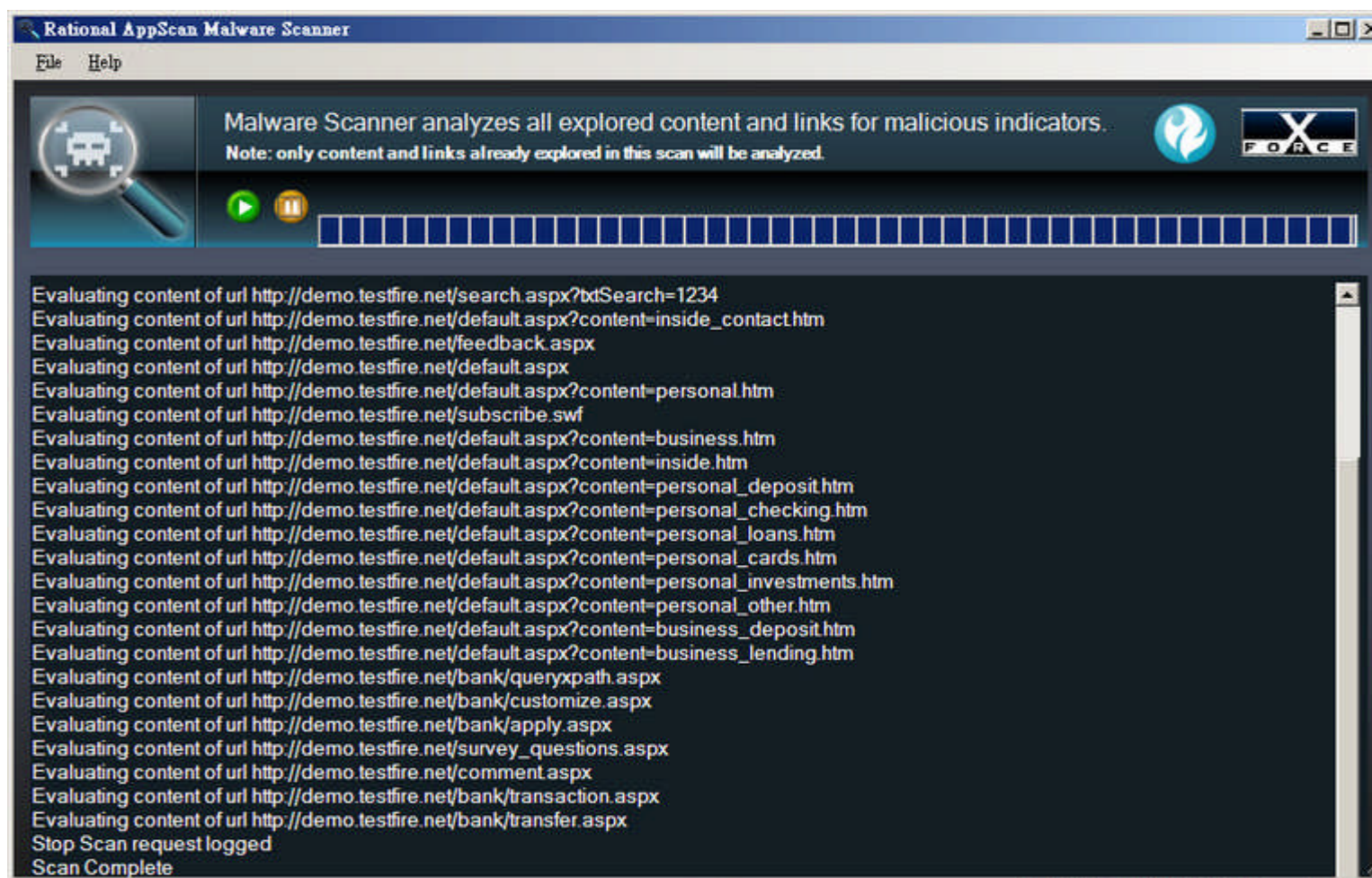
在每一個「問題 URL」之後加入分頁

報告內容

- 執行摘要 (整個掃描)
- 安全問題
 - 變式
 - 要求/回應
 - 使用者註解
 - 在回應中顯示驗證
 - 畫面
 - 諮詢和修正建議
 - .NET
 - J2EE
 - PHP
- 補救作業
- 應用程式資料
 - 應用程式 URL
 - Script 參數
 - 毀損鏈結
 - 註解
 - JavaScript
 - Cookie

惡意程式(MALWARE)掃描器

- 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

Thank
YOU

