
IBM
Rational. software
【2009 IBM開發者大會】
開發，不只玩真的！
Real Teams. Real Insights.
Real Results.
REC

IBM

Rational. software

【2009 IBM開發者大會】

開發，不只玩真的！

蕭明清

淡江大學資訊中心 網路管理組組長

Real Teams. Real Insights. Real Results.

IBM

Rational. software

【2009 IBM開發者大會】

開發，不只玩真的！

校園資安重要新環節
-Web應用程式零漏洞

Real Teams. Real Insights.
Real Results.
REC

淡江大學資安發展經驗分享

- 淡江大學資安發展歷程
- 校園資安重要新環節 – 資訊安全零漏洞

淡江大學資安發展歷程

- 90年8月建置Internet Data Center (IDC)機房
  - 環境安全
    - 防火、防水、恆濕、恆溫、不斷電、網路線上監視、門禁
    - 集中管理校級伺服器，增加穩定性、安全性以及可靠性
  - 資料實體安全
    - 異地備份

淡江大學資安發展歷程

- 91年建置防火牆及入侵偵測系統（IDS）
  - 阻絕惡意攻擊、入侵行為
  - 校級伺服器防護
- 92年建置整合式威脅威脅管理系統（UTM）
  - 防火牆
  - 防毒牆（AntiVirus）
  - 入侵防禦系統（IPS）
- 93年建置垃圾信過濾及掃毒系統

淡江大學資安發展歷程

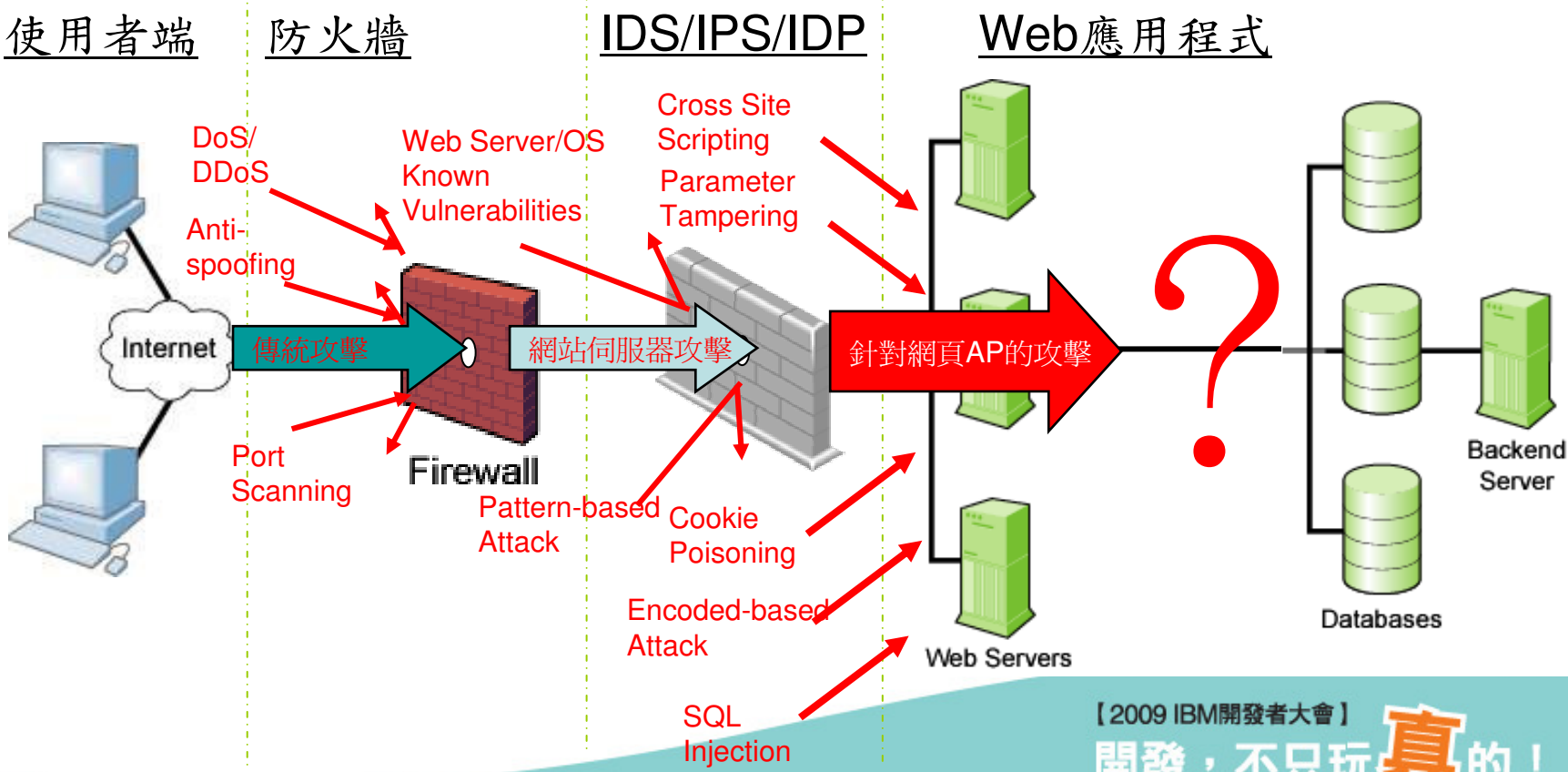
- 93年8月取得英國國際資訊安全稽核規範證書（BS 7799-2），為國內第一個通過此認證的學術研究單位。
- 95年5月5日通過BSI新版資訊安全管理系統（ISMS）審查，成為國內第一個取得ISO27001新版認證之學術單位。
- 97年建置Security Operations Center (SOC)
- 97年10月取得ISO 20000資訊服務管理（ITSMS）認證。

校園資安重要新環節

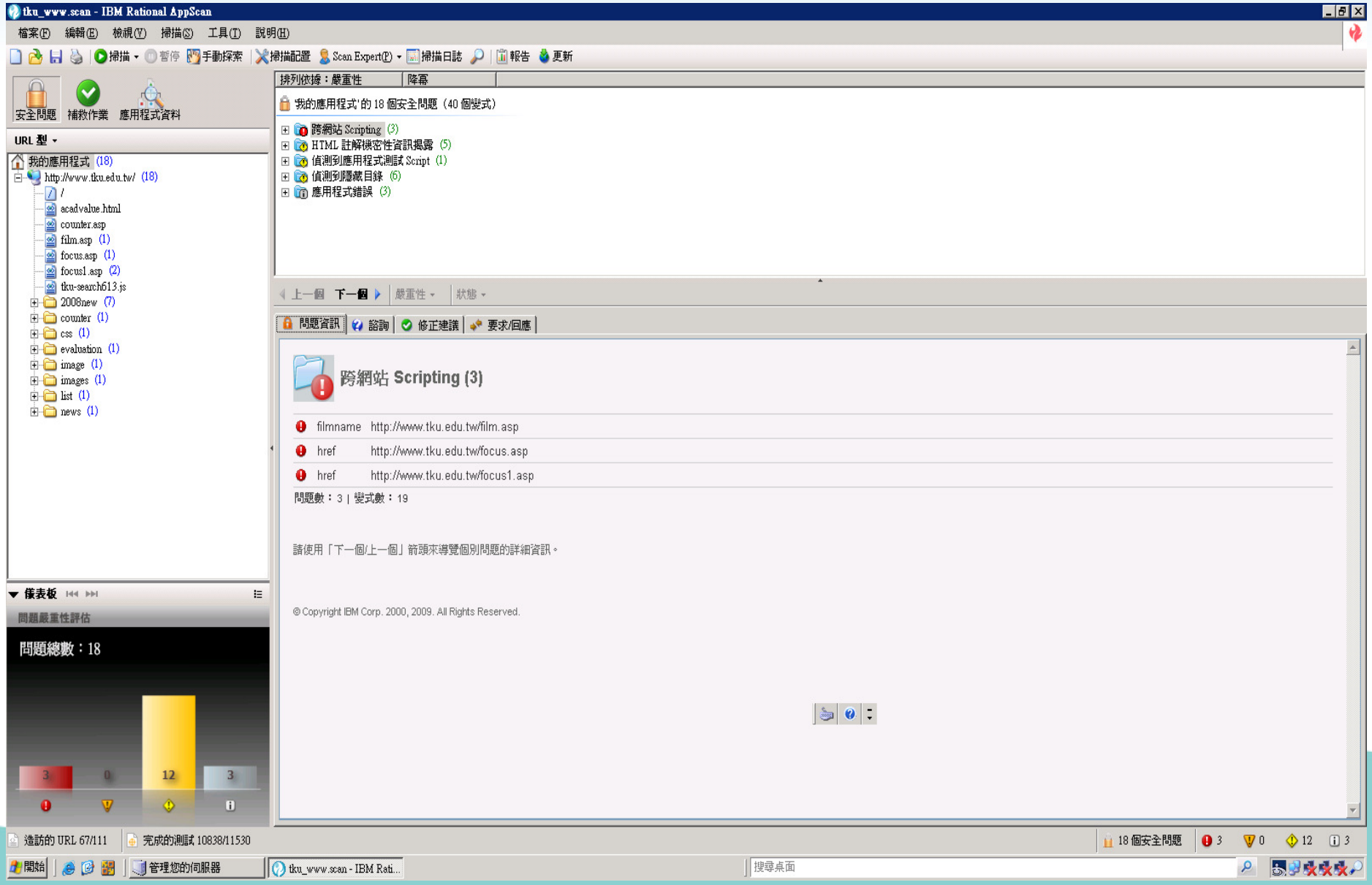
- 資訊安全零漏洞
  - 程式碼弱點分析
  - 網站弱點偵測（AppScan網站應用程式漏洞掃描工具）
- 成立資訊安全服務隊（98學年度計畫）
  - 協助各單位程式碼弱點分析及弱點矯正
  - 協助網站弱點偵測及安全漏洞修補
  - 監控網路安全(SOC運作)及協助木馬、病毒、...清除

網站弱點偵測

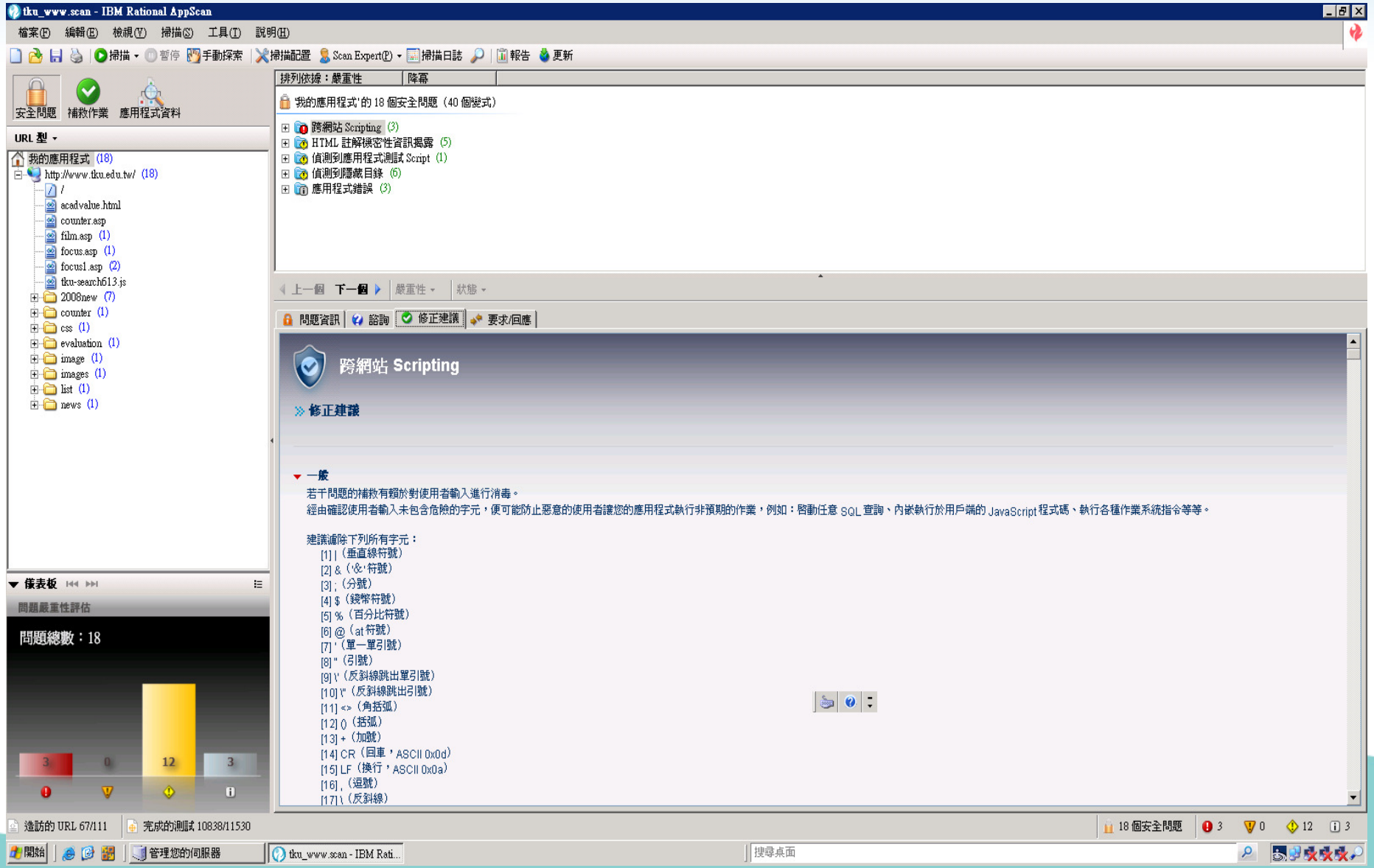
- 導入IBM Rational AppScan 網站應用程式漏洞掃描工具



網站弱點偵測

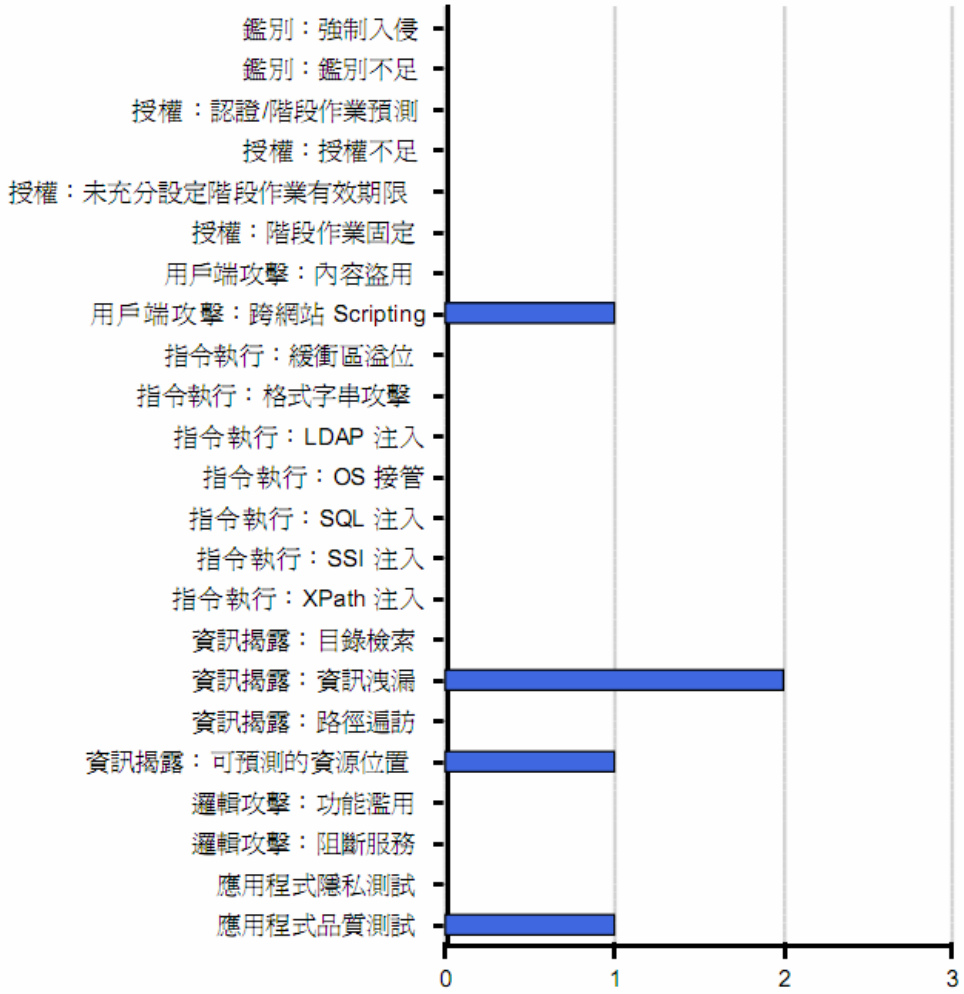

tku_www.scan - IBM Rational AppScan
檔案(F) 編輯(E) 檢視(V) 掃描(S) 工具(T) 說明(H)
掃描 暫停 手動探索 掃描配置 Scan Expert(P) 掃描日誌 報告 更新
安全問題 補救作業 應用程式資料
URL 型
我的應用程式 (18)
http://www.tku.edu.tw/ (18)
/
acadvalue.html
counter.asp
film.asp (1)
focus.asp (1)
focus1.asp (2)
tku-search613.js
2008new (7)
counter (1)
css (1)
evaluation (1)
image (1)
images (1)
list (1)
news (1)
儀表板
問題嚴重性評估
問題總數：18
3
0
12
3
排列依據：嚴重性
降冪
我的應用程式'的 18 個安全問題（40 個變式）
跨網站 Scripting (3)
HTML 註解機密性資訊揭露 (5)
偵測到應用程式測試 Script (1)
偵測到隱藏目錄 (6)
應用程式錯誤 (3)
上一個 下一個 嚴重性 狀態
問題資訊 諮詢 修正建議 要求/回應
跨網站 Scripting (3)
filmname http://www.tku.edu.tw/film.asp
href http://www.tku.edu.tw/focus.asp
href http://www.tku.edu.tw/focus1.asp
問題數：3 | 變式數：19
請使用「下一個/上一個」箭頭來導覽個別問題的詳細資訊。
© Copyright IBM Corp. 2000, 2009. All Rights Reserved.
造訪的 URL 67/111
完成的測試 10838/11530
18 個安全問題
3
0
12
3
開始
管理您的伺服器
tku_www.scan - IBM Rati...
搜尋桌面

網站弱點偵測


tku_www.scan - IBM Rational AppScan
檔案(F) 編輯(E) 檢視(V) 掃描(S) 工具(T) 說明(H)
掃描 暫停 手動探索 掃描配置 Scan Expert(P) 掃描日誌 報告 更新
安全問題 補救作業 應用程式資料
URL 型
我的應用程式 (18)
http://www.tku.edu.tw/ (18)
/
acadvalue.html
counter.asp
film.asp (1)
focus.asp (1)
focus1.asp (2)
tku-search613.js
2008new (7)
counter (1)
css (1)
evaluation (1)
image (1)
images (1)
list (1)
news (1)
儀表板
問題嚴重性評估
問題總數：18
3
0
12
3
排列依據：嚴重性
降冪
我的應用程式'的 18 個安全問題（40 個變式）
跨網站 Scripting (3)
HTML 註解機密性資訊揭露 (5)
偵測到應用程式測試 Script (1)
偵測到隱藏目錄 (6)
應用程式錯誤 (3)
上一個 下一個
嚴重性
狀態
問題資訊 諮詢 修正建議 要求/回應
跨網站 Scripting
修正建議
一般
若干問題的補救有賴於對使用者輸入進行消毒。
經由確認使用者輸入未包含危險的字元，便可能防止惡意的使用者讓您的應用程式執行非預期的作業，例如：啓動任意 SQL 查詢、內嵌執行於用戶端的 JavaScript 程式碼、執行各種作業系統指令等等。
建議濾除下列所有字元：
[1] | （垂直線符號）
[2] & （'&'符號）
[3] ; （分號）
[4] $ （錢幣符號）
[5] % （百分比符號）
[6] @ （at 符號）
[7] ' （單一單引號）
[8] " （引號）
[9] \' （反斜線跳出單引號）
[10] \" （反斜線跳出引號）
[11] <> （角括弧）
[12] () （括弧）
[13] + （加號）
[14] CR （回車，ASCII 0x0d）
[15] LF （換行，ASCII 0x0a）
[16] , （逗號）
[17] \ （反斜線）
造訪的 URL 67/111
完成的測試 10838/11530
18 個安全問題 3 0 12 3
開始
管理您的伺服器
tku_www.scan - IBM Rati...
搜尋桌面

網站弱點偵測

以下是依「威脅等級」分佈的安全問題清單。



導入 AppScan的成效

- 網站重大漏洞追蹤修改
- 持續密集檢測Web應用程式新的漏洞
- 協助程式人員於開發階段即可得知程式安全度，及早補正程式安全問題，降低開發時程影響
- 範例程式提供程式人員迅速正確處理資安問題，Web應用程式安全問題不再是上線的瓶頸

IBM

Rational. software

【2009 IBM開發者大會】

開發，不只玩真的！