

# Web 伺服器安全性調查

## 一、對象

Web Server 版本調查針對全台灣有登記 Domain Name 的六十萬台主機進行普查，運用程式連接 Port 80 (http)，紀錄各種不同廠牌之 Web 伺服器及其版本分布情形。

此外，由於不同的 Web 伺服器及其各版本有不同的系統安全漏洞，本次調查除了收集各 Web 版本資訊外，另外針對各版本的 Web Server 具有的系統安全漏洞進行資料收集。

## 二、方法

我們可以直接連接目標主機的 port 80( http )，送出要求頁面的請求，此時對方主機會回應版本訊息。

回應的訊息除了版本資訊以外，還包含了是否安裝其他的外掛模組，例如 SSL、PHP、Front Page Extension、SQL、mod\_perl 等等；運用這種方式可以有效探測對方伺服器的版本資訊。

## 三、伺服器版本及安全漏洞資料

對於全球 Web 伺服器的版本調查以及分布，NetCraft (<http://www.netcraft.com/>) 自 1995 年中起進行了持續性的調查，如圖 6-1 所示。

但是 NetCraft 對於 Web 伺服器的版本統計目的僅在於了解各廠牌伺服器的佔有比例，並未針對各版本 Web 伺服器的分布比例提出報告，加上該組織未能有效掌握台灣網路的詳細資料以及網路連線速度不理想，所提出的報告並不詳細。

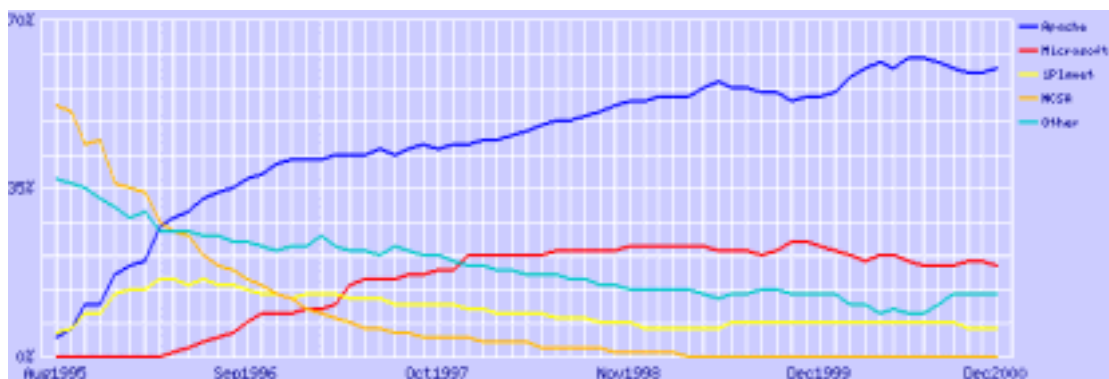


圖 1、Internet Web 伺服器佔有率分布趨勢 (1995-2000)

來源： NetCraft (<http://www.netcraft.com>)

Server	June 1999	Percent	July 2000	Percent	Change
Apache	3471051	56.19	11412233	62.81	6.62
Microsoft-IIS	1379370	22.33	3608415	19.86	-2.47
Netscape-Enterprise	349067	5.65	1255085	6.91	1.26
Rapidsite	107930	1.75	293957	1.62	-0.13
WebLogic	89591	1.45	291067	1.60	0.15
WebSitePro	84173	1.36	101174	0.56	-0.80
Stronghold	77796	1.26	91556	0.50	-0.76
Zeus	72061	1.17	227043	1.25	0.08
thttpd	69723	1.13	220937	1.22	0.09
WebSTAR	55962	0.91	88653	0.49	-0.42

表 1、Internet Web 伺服器佔有率 (1999/6~2000/7)

來源：NetCraft (<http://www.netcraft.com>)

由 NetCraft 的調查報告可以發現，Internet 上的 Web 伺服器以 Apache Web 伺服器佔最大宗，佔全部比例的 62.81%，並且 Microsoft IIS 伺服器近年來趨於負成長，到了 2000 年只剩下全球比例的 19.86%。由於 Apache Web 伺服器大多以 Unix 平台為基礎，而 IIS 僅有 Windows NT 以及 Windows 2000 的版本，所以我們可以得知 Internet 上的 Web Server 大多是 Unix-based 的機器。

從圖一來看，Netscape Web 伺服器也喪失了競爭力，佔有率不斷下滑。整個 Internet Web 伺服器由 Apache Web 伺服器以及 Microsoft IIS 伺服器兩者相互競爭。

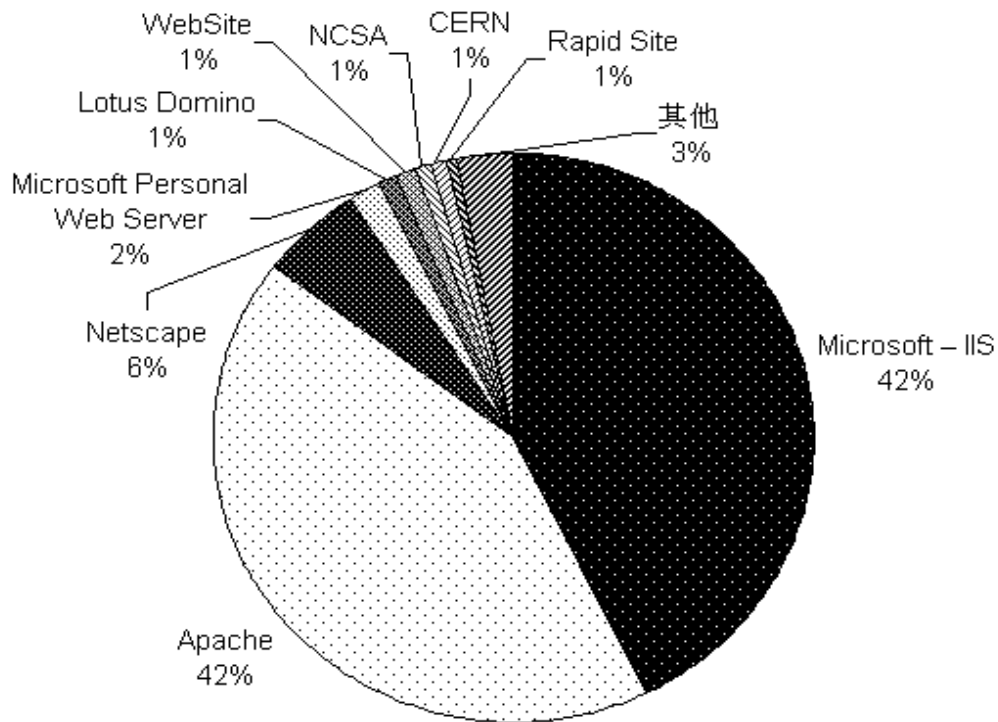


圖 2、台灣 Web 伺服器佔有率 (1999/6)

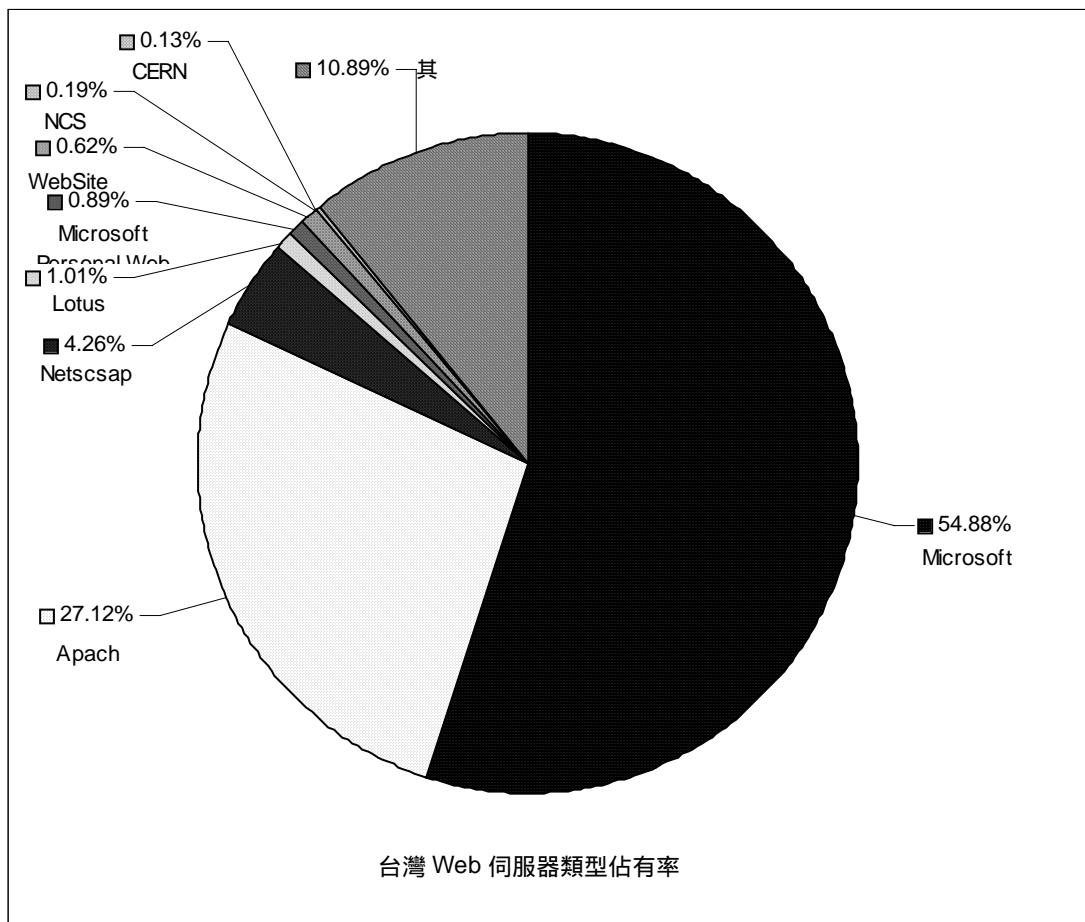


圖 3、台灣 Web 伺服器佔有率 (2000/12)

Server	June 1999	Percent	Dec 2000	Percent	Change
Microsoft – IIS	16334	42.71%	38409	54.88%	12.17%
Apache	16199	42.52%	18981	27.12%	-15.40%
Netscape	2159	5.67%	2978	4.26%	-1.41%
Microsoft Personal Web Server	592	1.55%	622	0.89%	-0.66%
Lotus Domino	460	1.21%	709	1.01%	-0.20%
WebSite	424	1.11%	436	0.62%	-0.49%
NCSA	337	0.88%	135	0.19%	-0.69%
CERN	297	0.78%	94	0.13%	-0.65%
其他	1356	3.56%	7621	10.89%	7.33%
總計	38158	100%	69985	100%	0.00%

表 2、台灣 Web 伺服器佔有率 (2000/12)

由本次調查台灣地區 Web 伺服器的分布與 NetCraft 調查所得的台灣 Web 伺服器版本的分布進行比對，發現兩者的趨勢剛好相反。與 NetCraft 調查所得的 Internet Web 伺服器市場佔有率趨勢相比對，台灣地區的 Web 伺服器版本分布與 Internet 環境有相當大的不同。台灣地區的 Apache Web 伺服器與 Microsoft IIS 的比例去年大約是 1：1，到了今年卻變成 1：2 剛剛好和 NetCraft 的調查完全相反，這也顯示了台灣地區的伺服器以 PC 平台為主，執行 Microsoft Windows NT 或者 Microsoft Windows 2000 作業系統。

從上述的資料我們可以發現國內與國外 web server 種類的分佈相差很大，雖然前兩大的伺服器種類不論國內外都是 Microsoft IIS 與 Apache Web 伺服器，在台灣前兩大伺服器相加所佔的比例就超過八成，國外的 Apache Web 伺服器大約是 Microsoft IIS 的兩倍，然而國內的 Microsoft IIS 比 Apache Web 伺服器數量多了將近一倍，配合著電子商務的盛行，台灣的網頁伺服器不似國外，為了快速的發展簡單的伺服器平台，大部分的公司選擇了安裝簡單卻安全漏洞較多的 Microsoft IIS，因此國內外的前兩大伺服器種類才会有這麼大的差別。

而在國內外都是第三大的 Netscape，從去年跟今年的資料可以看出他的佔有率正不斷下降中，這個產品將很有可能淡出這個市場，或者說因為在使用方便上 Microsoft IIS 展現了他的特色，而 Apache Web 伺服器又在安全性跟穩定性上

有突出的表現，相對來說，Netscape Web 伺服器產品並沒有相對於其他兩者之外有自己的特色，自然將不會成為一個成功的商品。

#### 四、Microsoft IIS 伺服器

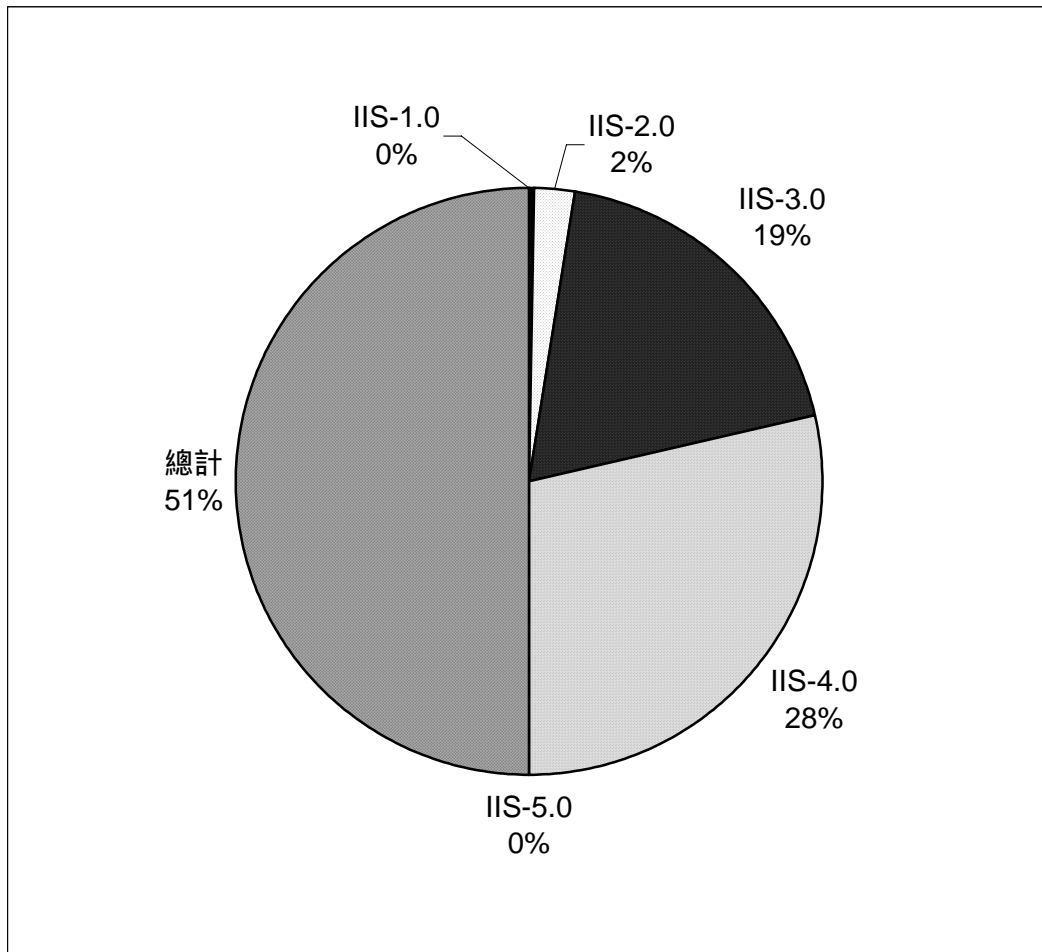


圖 4、Microsoft IIS Web 伺服器版本分布 (1999)

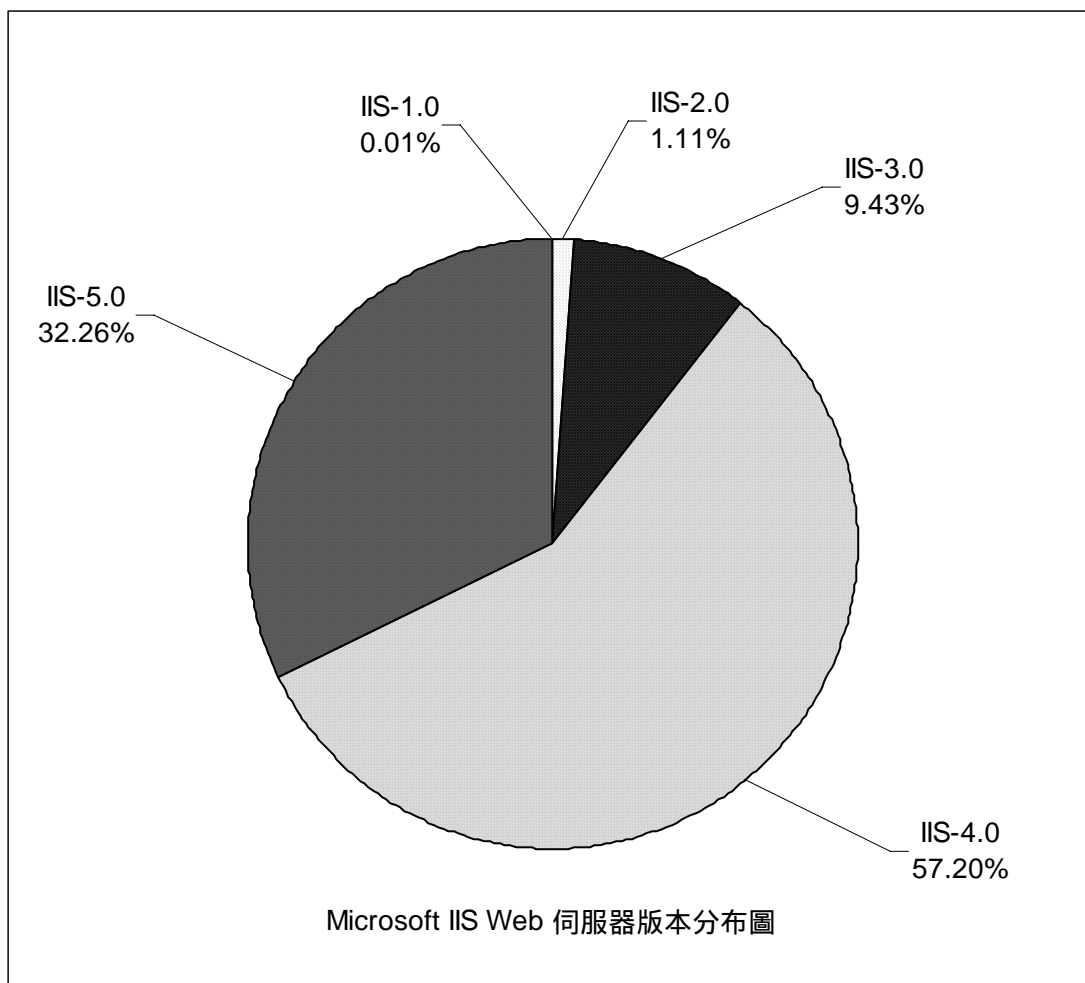


圖 5、Microsoft IIS Web 伺服器版本分布 (2000/2)

Server	June 1999	Percent	Dec 2000	Percent	Change
IIS-1.0	62	0.38 %	2	0.01%	-0.37%
IIS-2.0	790	4.84 %	427	1.11%	-3.73%
IIS-3.0	6179	37.83 %	3622	9.43%	-28.5%
IIS-4.0	9293	56.89 %	21969	57.20%	0.34%
IIS-5.0	10	0.06 %	12389	32.26%	32.2%
<b>總計</b>	<b>16334</b>	<b>100 %</b>	<b>38409</b>	<b>100%</b>	<b>0.00%</b>

表 3、IIS 佔有比率變化

Microsoft IIS Web 伺服器已知之安全漏洞：

版本	發表日期	名稱	影響
----	------	----	----

IIS 3.0/ IIS 4.0	1999/6/23	Double Byte Code Page	若將正在執行 IIS 的機器上，內定語系設定為 Double byte code page(如中文，日文，或是韓文)，而利用特定的 URL 結構來處理分散在虛擬目錄下的檔案需求，這種需求通常可以交由主機端進行處理。由於處理完的結果會以文字模式送回給瀏覽器，因此可能允許程式碼很輕易的被查閱。
IIS 4.0	1999/6/16	IIS Buffer Overflow	Microsoft IIS 4.0 有一個 buffer overflow 的安全性弱點，隱藏在針對 .HTR, .STM, .IDC 等類型檔案做處理的程式庫(library)裡面。這個漏洞可能引發 DoS 攻擊,並可能造成任意程式碼得以在 server 上被執行。
IIS 4.0	1999/6/15	Malformed HTR Request	這個漏洞可以導致對 Server 的 DoS 攻擊，或在特定情況下，允許任意的程式碼在 server 上執行。
IIS 4.0	1999/5/7	IIS File Viewers	IIS 跟 Site Server 上有一些檔案瀏覽的安全性弱點，使遠端使用者得以瀏覽任意檔案。
IIS 4.0	1999/5/7	IIS Showcode ASP	IIS 4.0 在安裝時放置了一些內定的 ASP 檔案,其中之一就是 showcode.asp ,由於這個 ASP 並未檢查對方的身分，遠端使用者可以透過此 ASP 檔，以 WWW 的權限瀏覽同一個 volume 中的任意檔案。
IIS 3.0 / IIS 4.0	1999/4/11	Using FSO and ASP to Read Server Files	遠端使用者可以透過 ASP，利用 './' 的方式瀏覽檔案。可以讀取系統任意檔案。例如： <a href="http://www.server.foo/showfile.asp?file=././global.asa">http://www.server.foo/showfile.asp?file=././global.asa</a>
IIS 1.0 / IIS 2.0 / IIS 3.0 / IIS 4.0	1998/7/8	IIS Multiple Data Streams	Microsoft NT 支援 Multiple data stream 功能，導致遠端使用者可以瀏覽在 NTFS 上的任何檔案
IIS 3.0/ IIS 4.0	1998/7/1	IIS \$DATA Error	遠端使用者可以藉由以下的方式 <code>http://xyz/myasp.asp::\$DATA</code> 瀏覽伺服器端的 ASP 檔原始碼。
IIS 4.0	1998/1/8	Back Door Access to Protected Files	由於系統設計時忽略了 Windows 相容 DOS 8+3 檔名的設計，遠端使用者可將長檔名轉換為 DOS 8+3 格式的檔名瀏覽，忽略原本的存取限制。
IIS 3.0	1997/6/25	Denial of Service	遠端使用者可以送出超過規定長度的 URL request，導致 IIS 伺服器當機。

		Attack	
IIS 3.0 及之前的版本	1996/3/5	.BAT CGI Script Hole	遠端使用者可以下載任何 CGI 檔案，並且可以透過 IIS Web Server 執行 NT 主機中 DOS 指令。
	1999/09/25	<a href="#">CVE-1999-0191</a>	IIS 中的 newdsn.exe CGI script 允許遠端使用者覆寫檔案。
	2000/01/18	<a href="#">CVE-1999-0233</a>	IIS 允許使用者利用.bat 或是.cmd 的檔案來任意的執行命令程式。
IIS 4.0 以及之前的版本	1999/09/11	<a href="#">CVE-1999-0278</a>	遠端的攻擊者可以在網址上的 ASP 檔案附加上 "::\$DATA" 就可以看到原始的程式碼。
	1999/09/29	<a href="#">CVE-1999-0281</a>	輸入長字串的 URL 可以阻斷 IIS 提供服務。
	1999/09/29	<a href="#">CVE-1999-0348</a>	在同一實體目錄下的兩個虛擬伺服器使用 ASP 會有暫存區釋放敏感資訊的問題。
IIS 3.0 以及 IIS 4.0	1999/09/25	<a href="#">CVE-1999-0349</a>	IIS 中的 FTP 存在可以使用 ls 命令來造成 buffer overflow, 這樣的功能可以允許遠端的攻擊者來阻斷服務的提供以及執行一些系統命令。
IIS 4.0	2000/06/02	<a href="#">CVE-1999-0407</a>	在預設的狀況下, IIS 4.0 下的虛擬目錄 /IISADMPWD 的檔案可以導致暴力法攻擊竊取密碼, 或是可以辨識系統特定的使用者。
	1999/09/29	<a href="#">CVE-1999-0412</a>	當伺服器正在系統模式下載入執行 ISAPI, 攻擊者可以在 IIS 以及其它網頁伺服器下使用系統命令。
IIS 4.0	1999/09/29	<a href="#">CVE-1999-0448</a>	IIS 4.0 以及 Apache 對於 HTTP 請求的方式, 並不管請求參數的長度, 這樣可以讓遠端的攻擊者可以隱藏他們真正想要進入的 URL。
	1999/09/29	<a href="#">CVE-1999-0449</a>	ExAir 網站可以使用 scripts 來阻斷 IIS 4 提供服務。
IIS 3.0 以及 IIS 4.0	2000/01/04	<a href="#">CVE-1999-0725</a>	又名 "Double Byte Code Page" 的漏洞, 允許遠端攻擊者可以看到 IIS 預設語言為中文, 韓文, 日文的原始檔案程式碼。
IIS 4.0	2000/01/04	<a href="#">CVE-1999-0777</a>	就算使用者沒有存取的權限, IIS FTP 伺服器可能允許遠端的攻擊者來讀取或是刪除檔案。
IIS 4.0	2000/01/04	<a href="#">CVE-1999-0861</a>	IIS 裡面的 SSL ISAPI 過濾器的競賽狀況可能導致加密原文的暴露。
IIS 4.0	2000/01/04	<a href="#">CVE-1999-</a>	在 IIS 4.0 的 HTTP 請求裡面使用特殊的標頭可

	1/04	<a href="#">0867</a>	以導致阻斷服務.
IIS 4.0	2000/06/02	<a href="#">CVE-1999-0874</a>	在 IIS 4.0 裡面經由執行 .HTR, .IDC, 或是 .STM 的請求, 可以造成緩衝區溢位, 導致阻斷服務.
IIS 4.0	2000/06/02	<a href="#">CVE-1999-1011</a>	IIS 3.x 以及 4.x 裡面的 The Remote Data Service (RDS) DataFactory component of Microsoft Data Access Components (MDAC) 有著漏洞, 可以讓遠端的使用者可以任意的執行命令.
IIS 4.0	2000/04/25	Escape Character Parsing	由於 IIS 沒有遵守 URLs, 所以遠端攻擊者可以使用特殊的字元來執行第三種程式.
IIS 4.0	2000/03/22	Virtual Directory Naming	IIS 4.0 以及 Site Server 3.0 允許遠端攻擊者讀取 ASP 的原始碼, 如果在虛擬目錄裡的名稱包含 .com, .exe, .sh, .cgi, or .dll.
	2000/03/22	Malformed Hit-Highlighting Argument	名叫 "Malformed Hit-Highlighting Argument" 的漏洞, 允許遠端攻擊者可以讀取非法的檔案在微軟的 Index Server 下的 ISAPI.
IIS 4.0	2000/06/02	Chunked Transfer Encoding Buffer Overflow Vulnerability	IIS 4.0 允許攻擊者使用 POST 以及 PUT 命令來要求大量的暫存區來耗盡記憶體導致阻斷服務.
IIS 4.0 以及 IIS 5.0	2000/06/02	Virtualized UNC Share	如果 IIS 4.0 以及 5.0 的虛擬目錄使用 UNC share, 將無法讓 IIS 使用 ISAPI 執行程序. 這樣會讓遠端的攻擊者可以讀取 ASP 的原始碼或是其他的檔案.
IIS 4.0 以及 IIS 5.0	2000/06/02	Myriad Escaped Characters	針對 IIS 4.0 以及 5.0 發送大量的 escaped 字串可以讓遠端攻擊者導致阻斷服務.
IIS 4.0 以及 IIS 5.0	2000/07/12	Undelimited .HTR Request	針對 IIS 4.0 以及 5.0 ISSADMPWD 虛擬目錄下的 inetinfo.exe 傳送特殊的要求, 可以讓遠端的攻擊者造成阻斷服務.

IIS 4.0 以及 IIS 5.0	2000/07/12	Malformed Extension Data in URL	IIS 4.05 以及 5.0 允許遠端攻擊者利用附加上大量檔案的複雜 URL 來造成阻斷服務。
IIS 4.0 以及 IIS 5.0	2000/10/13	File Fragment Reading via .HTR	IIS 4.0 以及 5.0 允許遠端的攻擊者在 URL 之後附加上.htr 就可以看到程式的原始碼片段。
IIS 4.0 以及 IIS 5.0	2000/10/13	Absent Directory Browser Argument	名叫"Absent Directory Browser Argument"的漏洞,一個 IIS 3.0 的管理權限的 script,被包含到 IIS 4.0 以及 IIS 5.0 裡面,允許遠端的攻擊者透過不正常的參數來造成阻斷服務。
IIS 4.0 以及 IIS 5.0	2000/10/13	File Permission Canonicalization	名叫"File Permission Canonicalization"的漏洞,可以讓遠端攻擊者在 IIS 4.0 以及 IIS 5.0 繞過檔案的控制權限而下載檔案。
IIS 5.0	2000/10/13	Specialized Header	名叫"Specialized Header"的漏洞,允許遠端攻擊者在 IIS 5.0 使用"Translate: f"這樣的 HTTP GET 請求來得到.ASP 程式的原始碼。

表 4、Microsoft IIS 伺服器安全漏洞

## 五、Apache Web 伺服器

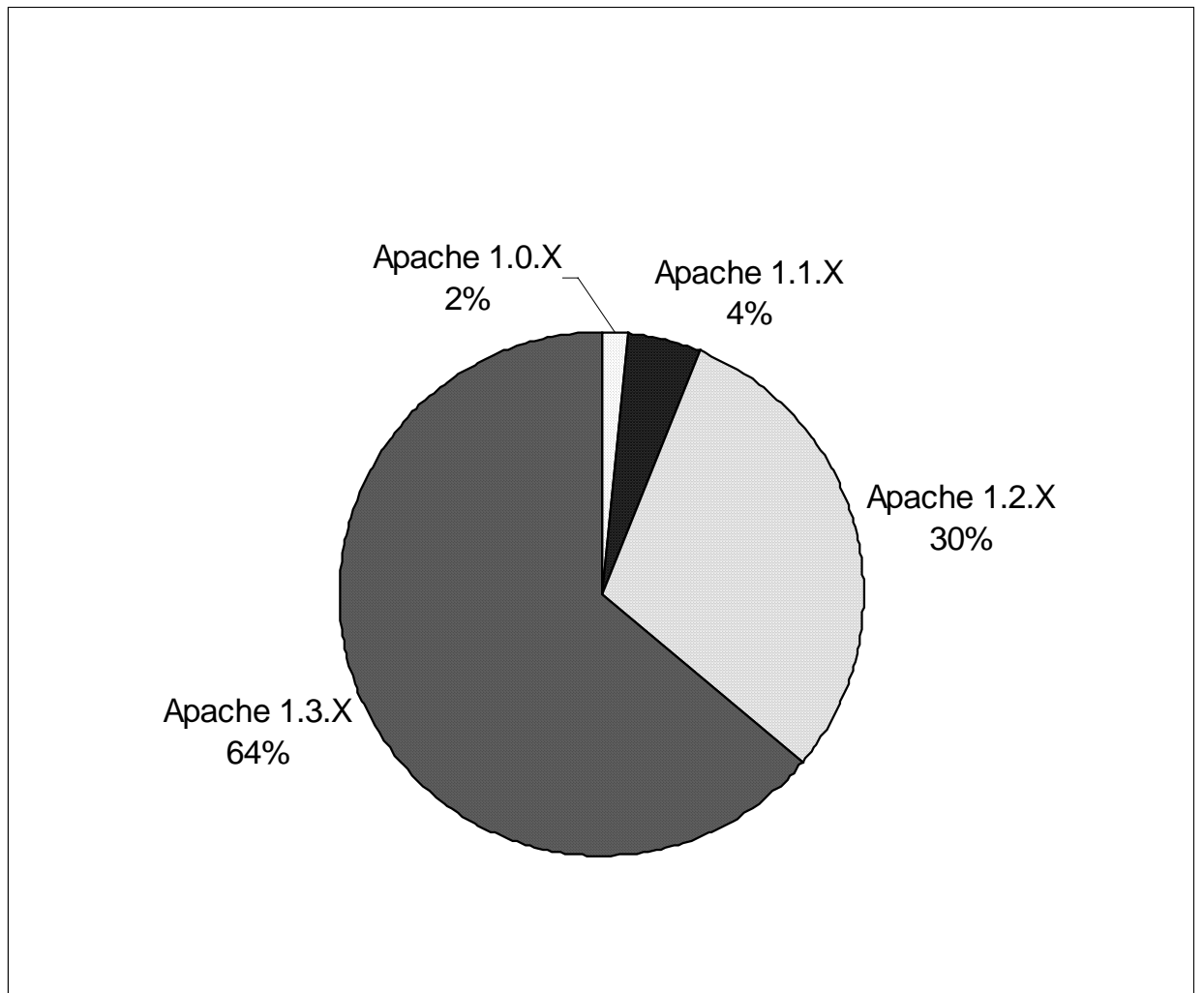


圖 6、Apache Web 伺服器版本分布 (1999/6)

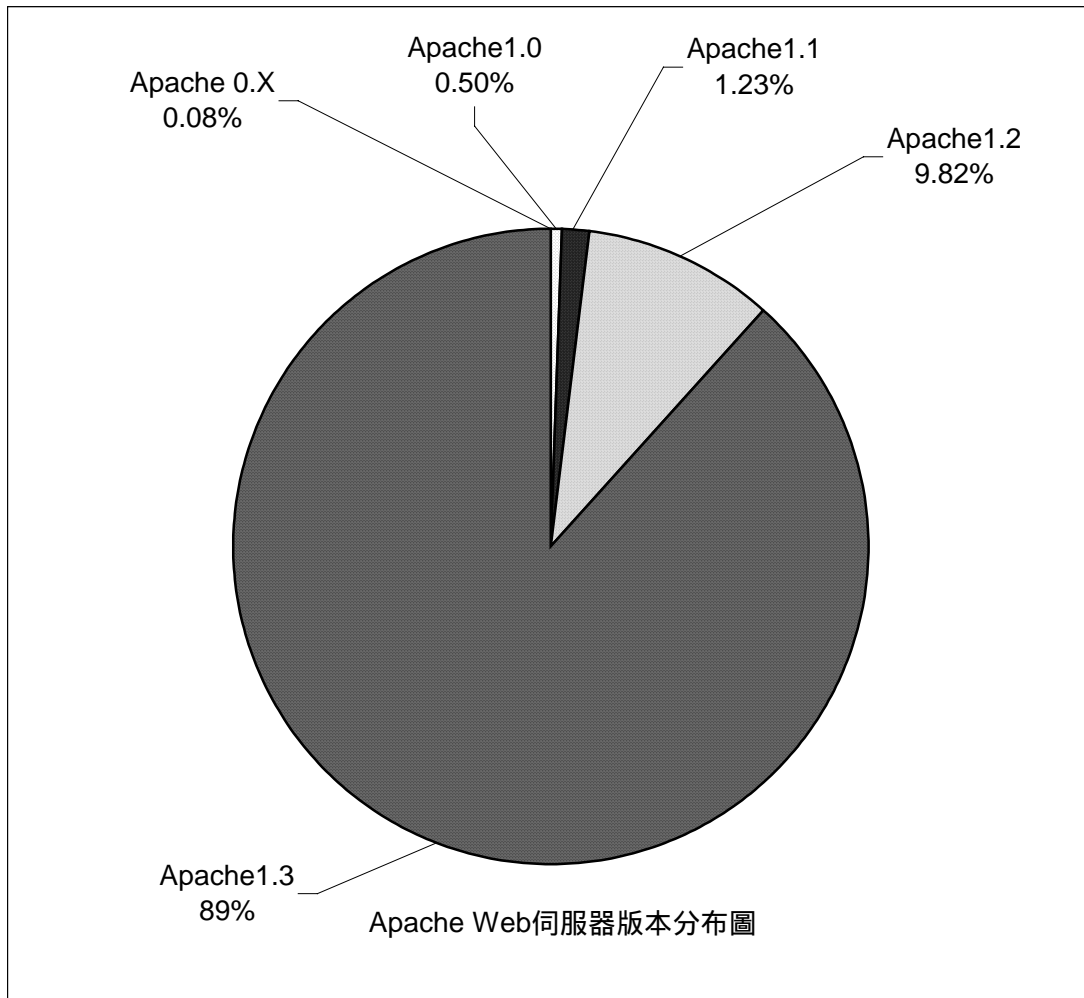


圖 7、Apache Web 伺服器版本分布 (2000/2)

Server	June 1999	Percent	Dec 2000	Percent	Change
Apache 0.X	9	0.05%	16	0.08%	0.03%
Apache 1.0.X	336	2.06%	94	0.5%	-1.46
Apache 1.1.X	866	5.34%	233	1.23%	-4.11
Apache 1.2.X	5960	36.8%	1863	9.82%	-26.98
Apache 1.3.X	12708	55.75	16775	89%	33.25

總計	16199	100 %	18981	100%	0.00%
----	-------	-------	-------	------	-------

表 5、Apache web server 佔有比率變化

Apache Web 伺服器已知之安全漏洞：

版本	發表日期	名稱	影響
Apache 1.2.4	1999/4/26	NTX Enhanced Server	遠端使用者可以藉由 NTX extension 的漏洞取得 root 權限。
Apache 1.2.5 之前的版本	1998/1/6	cfg_getline()	使用者可以造成 cfg_getline() 函式 buffer overflow，獲得遠端以 apache 身分讀取檔案的權限。
Apache 1.2.5 之前的版本	1998/1/6	mod_include()	使用者可以透過 mod_include() 的函式造成 apache 的 child process 進入無窮迴圈。
Apache 1.2.x/ Apache 1.3	1997/12/30	Apache DoS	遠端使用者可以在 URL request 中加入大量的 '/'，造成系統判斷路徑的錯誤，使得 CPU 負荷大量增加，造成 DoS 狀態。
Apache 1.1.3	1997/1/13	mod_cookie	遠端使用者可以造成 buffer overflow 的狀態，進而執行任何程式。
Apache 1.1.3	1997/1/11	Directory Index	遠端使用者可以利用假造的 URL 請求，獲得根目錄下所有的檔案清單。
Apache 1.0.3 之前的版本	1996/4/16	Escape Shell Command	遠端使用者可以利用此一漏洞執行任何程式，並且可以讀取所有擁有者為 WWW 的檔案；甚至可以利用 xterm 獲得完整的使用權限。
Apache 1.1.1 之前的版本	1997/9	http-apache-cookie	Apache httpd cookie 緩衝區溢位。
	1999/9/25		Apache httpd 的 ScriptAlias 目錄讓攻擊者讀取 CGI 程式。
Apache web server for Win32	1999/9/29		在 URL 中加入一個"點"(. )使得被限制的檔案被讀取。
Apache on Debian Linux	1999/4	apache-debian-usrdoc	Apache on Debian Linux 的預設值設定 ServerRoot to /usr/doc, 使遠端使用者可以讀取伺服器上所

			有的檔案。
Apache 1.3.x HTTP server for Windows platforms	2000/10/13	ibm-http-file-retrieve	The Apache 1.3.x HTTP server for Windows platforms 讓遠端攻擊者用包含很多"/"的 URL 來列出目錄內容。
Apache::ASP 1.93 以及之前的版本	2000/8	apache-source-asp-file-write	在 Apache ASP module 的 source.asp 範例 script 讓遠端攻擊者修改檔案。

表 6、Apache 伺服器安全漏洞

## 六、Netscape Web 伺服器

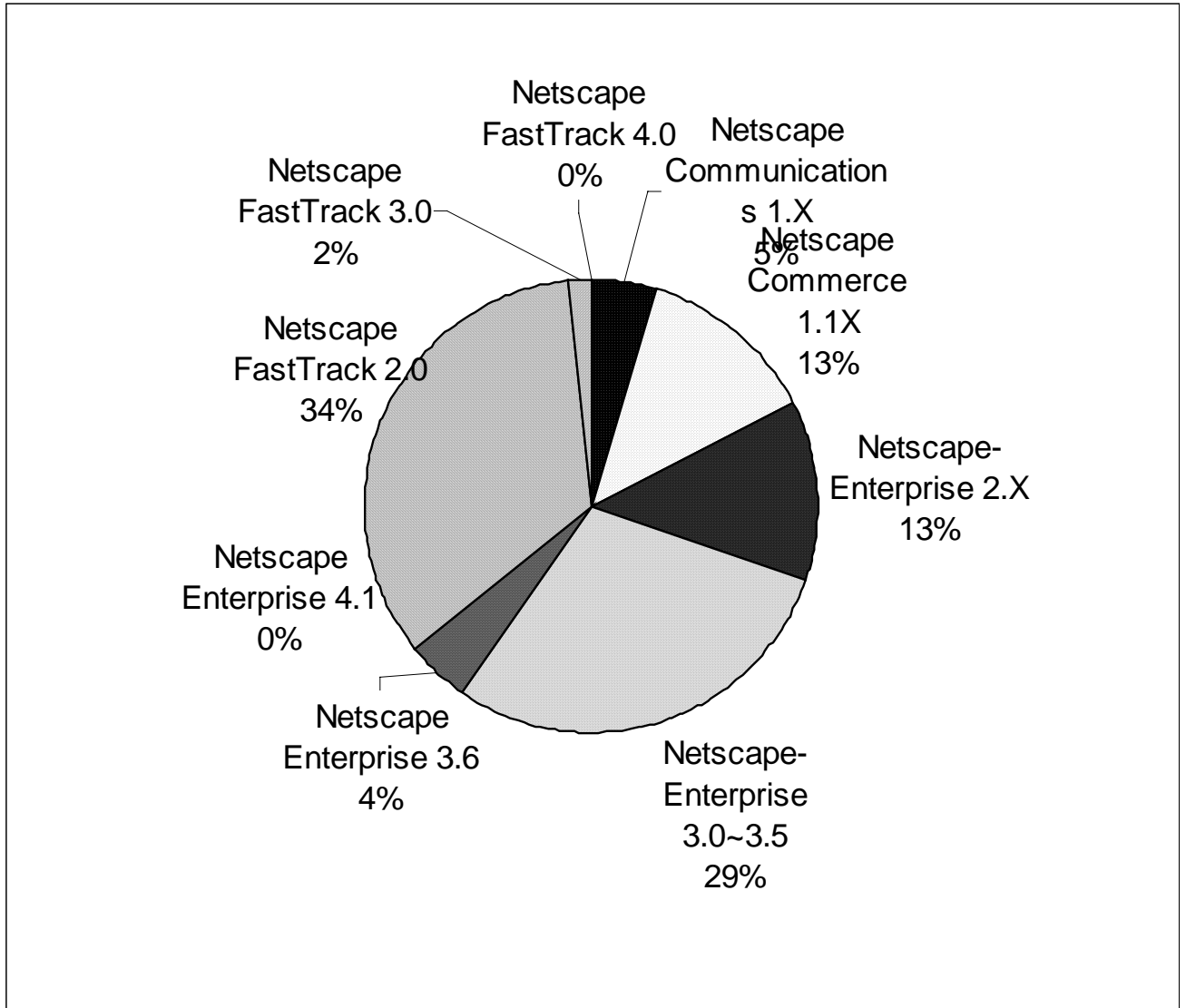


圖 8. Netscape Web 伺服器版本分布 (1999/6)

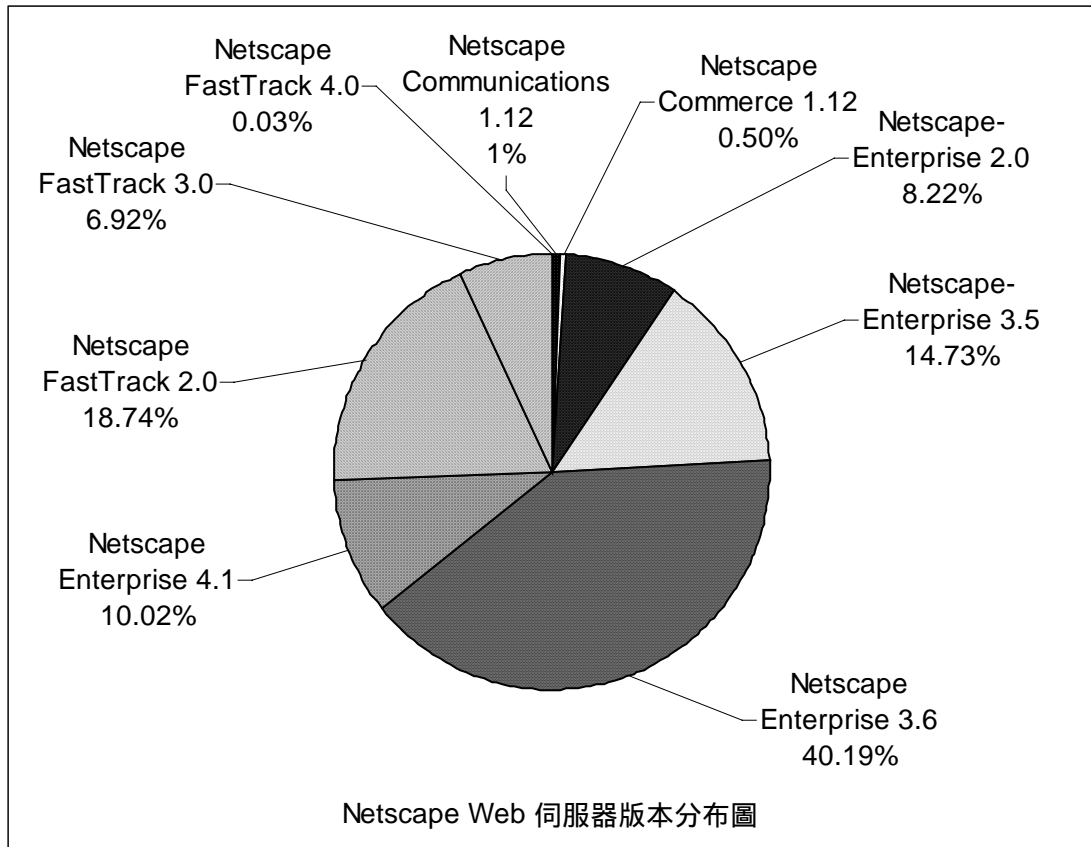


圖 9. Netscape Web 伺服器版本分布 (2000/12)

Netscape 公司所提供的 Web 伺服器主要分為幾個版本—Netscape Enterprise 佔最大宗，其次分別為 Netscape FastTrack、Netscape Communications 以及 Netscape Commerce。

Server	June 1999	Percent	Dec 2000	Percent	Change
Netscape Communications 1.X	106	4.68%	19	0.64%	-4.04%
Netscape Commerce 1.1X	288	12.72%	15	0.50%	-12.22%
Netscape-Enterprise 2.X	294	12.98%	246	8.26%	-4.72%
Netscape-Enterprise	663	29.27%	441	14.81%	-14.46%

3.0~3.5					
Netscape Enterprise 3.6	101	4.46%	1203	40.40%	35.94%
Netscape Enterprise 4.1	0	0.00%	300	10.07%	10.07%
Netscape FastTrack 2.0	775	34.21%	561	18.84%	-15.37%
Netscape FastTrack 3.0	38	1.68%	207	6.95%	5.27%
Netscape FastTrack 4.0	0	0.00%	1	0.03%	0.03%
總計	2265	100%	2978	100.00%	0.00%

表 7、netscape web server 佔有比率變化

版本	發表日期	名稱	影響
Communications	1998/6/25	Service-Side Include Source Code	遠端使用者可以利用此一漏洞下載 Server-Side Include 檔案之原始碼。
Communications 1.1	1996/1	DOS .bat files	遠端使用者在執行 .bat 格式的 CGI 時，可以使用 &<command> 的方式執行額外的程式。例如使用：“cgi-bin/test.bat&dir”，會在執行 test.bat 執行 dir，並將結果顯示在瀏覽器中。
Enterprise 3.51 / Enterprise 3.0	1999/5/19	Netscape %20 Filename	遠端使用者在 CGI 參數最後加入 ‘%20’ 時，伺服器會傳送 CGI 的原始碼，而非執行 CGI。
Enterprise 3.0	1998/1/8	Back Door Access to Protected Files	由於系統設計時忽略了 Windows 相容 DOS 8+3 檔名的設計，遠端使用者可將長檔名轉換為 DOS 8+3 格式的檔名瀏覽，忽略原本的存取限制。
FastTrack 3.01	1999/6/7	ROOT directory Listing	遠端使用者可以 telnet 至 httpd 的通訊埠，下 “GET /” 之命令獲得目錄下所有檔案的清單。
FastTrack 3.01	1999/5/19	Netscape %20	遠端使用者在 CGI 參數最後加入

		Filename	'%20' 時，伺服器會傳送 CGI 的原始碼，而非執行 CGI。
FastTrack 3.01	1998/1/8	Back Door Access to Protected Files	由於系統設計時忽略了 Windows 相容 DOS 8+3 檔名的設計，遠端使用者可將長檔名轉換為 DOS 8+3 格式的檔名瀏覽，忽略原本的存取限制。
Netscape 2.x, 3.x and 4.x	1997/7/15	Security Advisory in Netscape shipped with HP-UX	JavaScript 讓遠端攻擊者監視一個使用者的網路活動， aka the Bell Labs vulnerability.
Netscape FastTrack Web server	1998/7/16	Unauthorized directory listings with FastTrack v3.01 NT	Netscape FastTrack Web server 列出檔案當用小寫的"get"來取代大寫的"GET"。
Netscape Enterprise Server and FastTrask Server	1999/12/22	netscape-pa ssword-pref erences	緩衝區溢位讓遠端使用者利用一個很長的 URL request 來增加權限。
Netscape Enterprise Server	1999	netscape-ser ver-directory -indexing	開啟目錄索引的 Netscape Enterprise Server 使遠端攻擊者經由 web publishing tags 如 ?wp-ver-info 以及 ?wp-cs-dump 來列出伺服器上的目錄。
Netscape Enterprise Server with Web Publishing enabled	2000/3/23	netscape-we bpublisher-i nvalid-acces s	開啟 Web Publishing 功能的 Netscape Enterprise Server 讓遠端攻擊者列出任意目錄 經由 GET 指令(提供一個 Java applet 使攻擊者瀏覽這些目錄)取得/publisher 目錄。
Netscape Communicat or before version 4.73 and Navigator	2000/6/1	netscape-inv alid-ssl-sessi ons	沒有適當的驗證 SSL 認證，讓遠端攻擊者利用重導往合法網站的流量到自己的非法網站來竊取資訊， aka the "Acros-Suencksen SSL" vulnerability.

4.07			
Netscape 4.73 and earlier	2000/3/26	Inconsistent Warning Messages in Netscape Navigator	Netscape 4.73 and earlier does not properly warn users about a potentially invalid certificate if the user has previously accepted the certificate for a different web site, which could allow remote attackers to spoof a legitimate web site by compromising that site's DNS information.

表 8、Netscape Communications 伺服器安全漏洞

## 七、Lotus Domino Web 伺服器

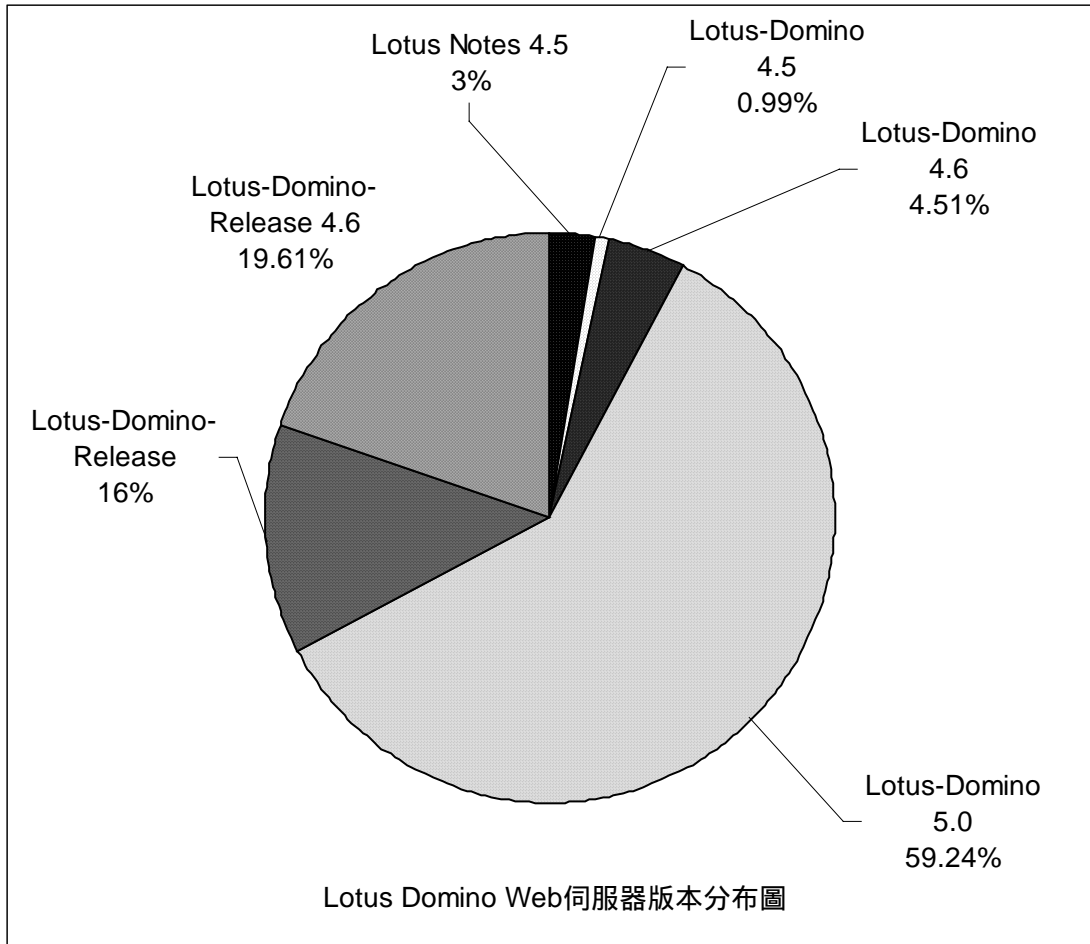


圖 10、Lotus Domino Web 伺服器版本分布(2000/2)

版本	發表日期	名稱	影響
Lotus Domino 4.6 之前的版本	1998/1/20	ACL designer access	遠端使用者可以不受 ACL 限制獲得檔案讀取權限。
Lotus Domino 4.6 之前的版本	1998/1/20	ACL parent template inheritance	遠端使用者可以不受 ACL 限制獲得檔案讀取權限。
Lotus Domino HTTP server	2000/3/22	serious Lotus Domino HTTP denial of service	Lotus Domino HTTP server does not properly disable anonymous access for the cgi-bin directory.
Lotus Domino HTTP server	2000/3/22	serious Lotus	藉由在 Lotus Domino HTTP server 的緩衝區溢位讓遠端攻

		Domino HTTP denial of service	擊者利用一個長的URL造成阻斷式攻擊。
Lotus Domino Server 5.0.1	2000/7/12	Lotus Domino ESMTP buffer overflow	Lotus Domino Server 5.0.1 的 ESMTP 服務的緩衝區溢位讓 遠端攻擊者利用一個長的 MAIL FROM 指令來造成阻斷式攻擊。

表9、Lotus Domino 伺服器安全漏洞

## 八、Microsoft Personal Web 伺服器

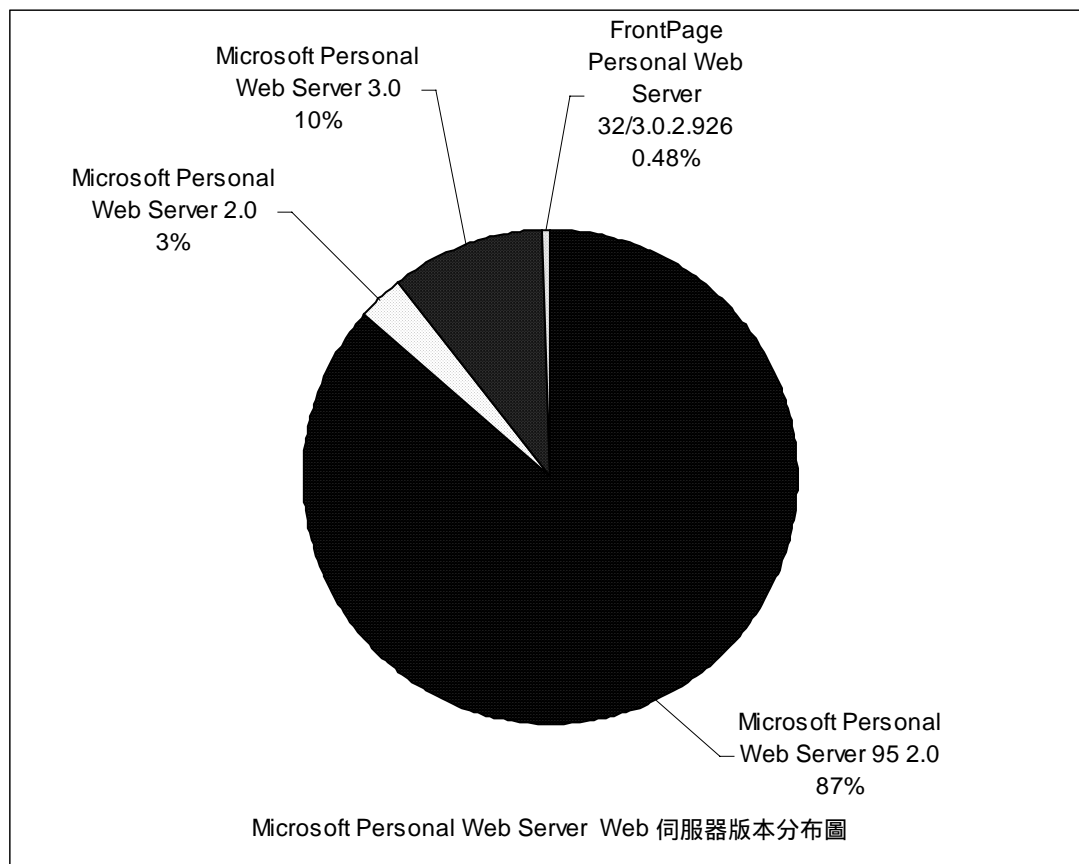


圖 11、Microsoft Personal Web Server 伺服器版本分布(2000/2)

版本	發表日期	名稱	影響
Window95 Window98	1999/3/26	File Access Vulnerability in Personal Web Server	利用非標準的 URL 使得遠端攻擊者 可以讀取伺服器上的檔案。

表 10、Microsoft Personal Web 伺服器安全漏洞

## 九、WebSite Web 伺服器

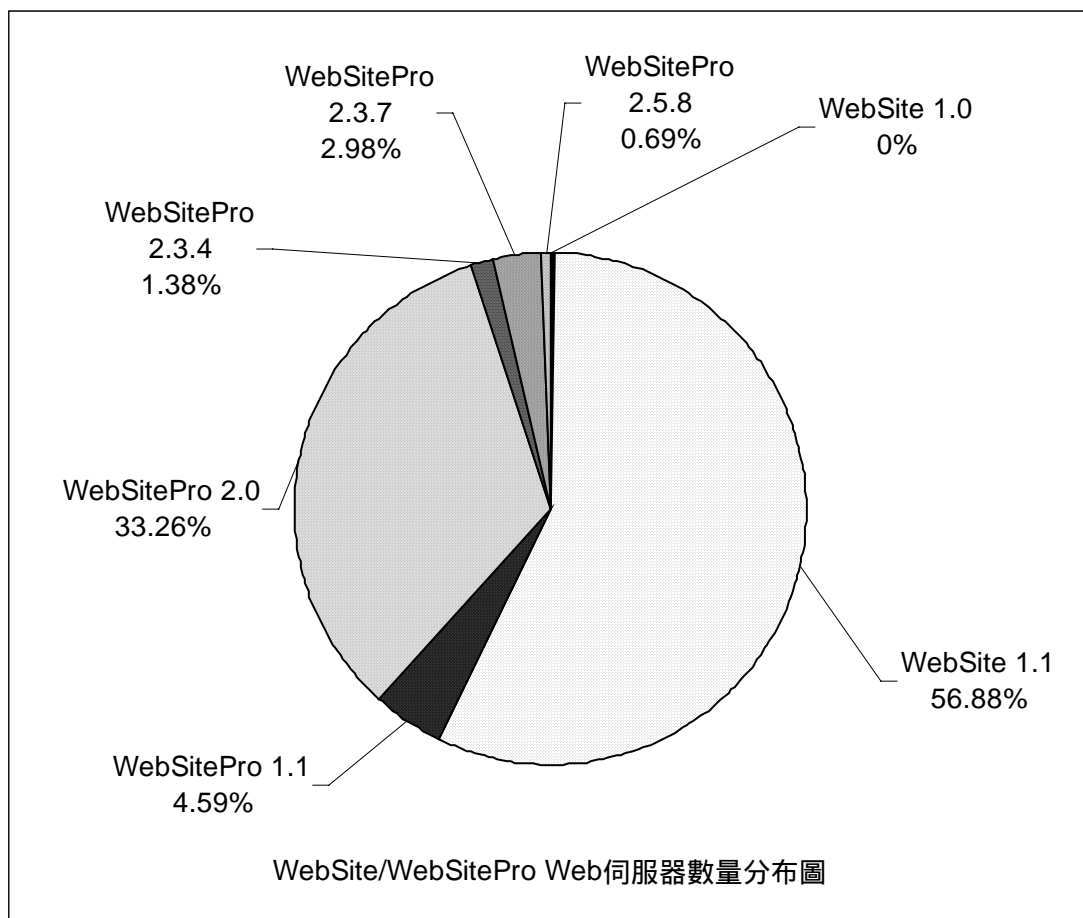


圖 12、WebSite 伺服器版本分布(2000/2)

版本	發表日期	名稱	影響
WebSite Pro 2.3 之前的版本	1998/6/25	Service-Side Include Source Code	遠端使用者可以利用此一漏洞下載 Server-Side Include 檔案之原始碼。
WebSite 1.1c 之前的版本	1996/3/5	DOS .bat files	遠端使用者在執行 .bat 格式的 CGI 時，可以使用 &<command> 的方式執行額外的程式。例如使用：“cgi-bin/test.bat&dir”，會在執行 test.bat 執行 dir，並將結果顯示在瀏覽器中。
WebSite 1.1	1999/9/25	WebSite 1.1 uploader allow remote attacker	WebSite web server 的上載程式讓遠端攻擊者執行任意程

		to upload and execute programs	式。
WebSite 1.1	1997/1	http-website-win sample	WebSite web server 的 win-c-sample 程式存在緩衝區溢位的問題導致遠端執行命令。
Allmanage Website administration software 2.6	2000/7/12	http-cgi-allmanage-account-access	在 Allmanage Website administration software 2.6 的 allmanageup.pl 檔上載 CGI 指令可以被遠端攻擊者執行，讓他們修改使用者帳號或者網頁。

表 11、WebSite 伺服器安全漏洞

## 十、NCSA Web 伺服器

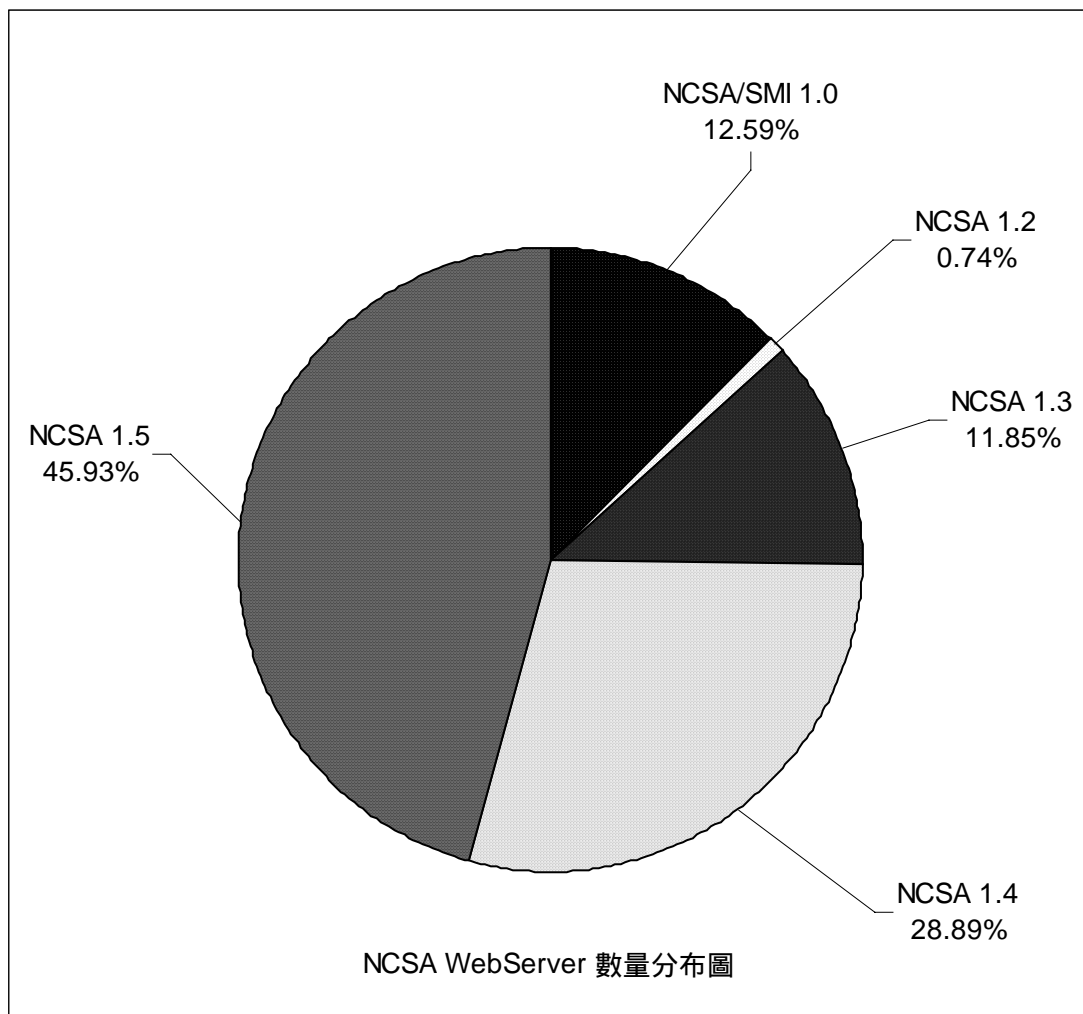


圖 13、NCSA 伺服器版本分布(2000/12)

版本	發表日期	名稱	影響
NCSA 1.5 之前的版本	1996/4/16	Escape Shell Command	遠端使用者可以利用此一漏洞執行任何程式，並且可以讀取所有擁有者為 WWW 的檔案；甚至可以利用 xterm 獲得完整的使用權限。
NCSA 1.4 之前的版本	Unknown	URL request overflow	遠端使用可以送出一個超長的 URL request，獲得 WWW 使用者完整權限。
NCSA 1.3 之前的版本	1995/4/17	Trick Executing Shell Command	遠端使用者可以利用此一漏洞獲得完整的 WWW 使用者權限。
NCSA Servers Old Common Gateway	1999/9/11	http-cgi-campas	一些有提供 campas CGI 程式的 NCSA web servers 讓攻擊者讀取任意檔案。

Interface (CGI)			
	1999/9/25	http-scriptalias	在 NCSA and Apache httpd 的 ScriptAlias 目錄讓攻擊者讀取 CGI 程式。
NCSA HTTP daemon v1.3	1999/7/20	Buffer overflow	在 NCSA HTTP daemon v1.3 緩衝區溢位使得可遠端執行指令。

表 12、NCSA 伺服器安全漏洞

### 十一、CERN Web 伺服器

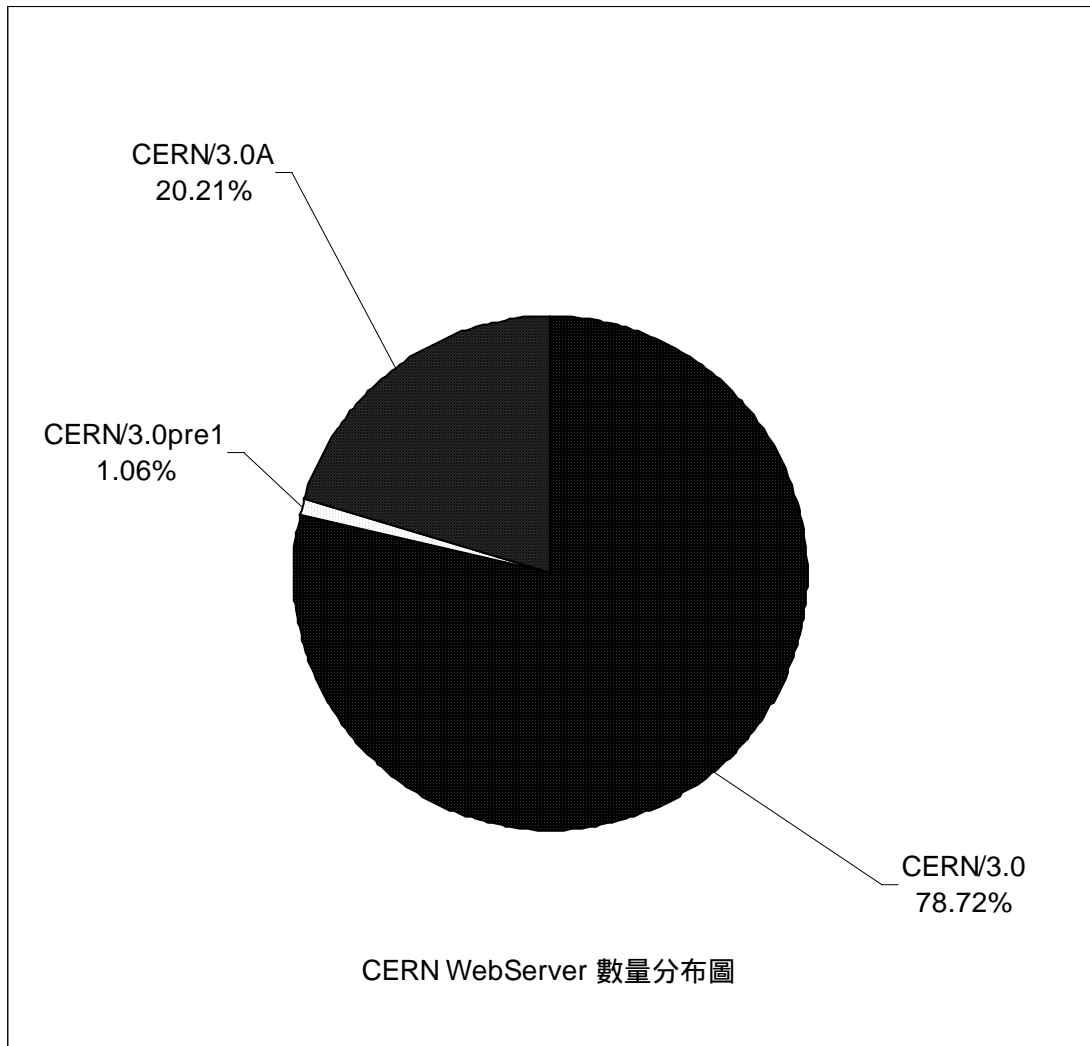


圖 14、CERN 伺服器版本分布(2000/12)

## 十二、網域名稱分布統計

Domain	.com	.net	.gov	.edu	.org	總計
數目	28711	764	744	3385	1449	35053
所佔比例	81.90%	2.17%	2.12%	9.65%	4.13%	100.00%

表 13、台灣地區網域名稱分布統計 (1999/12/01)

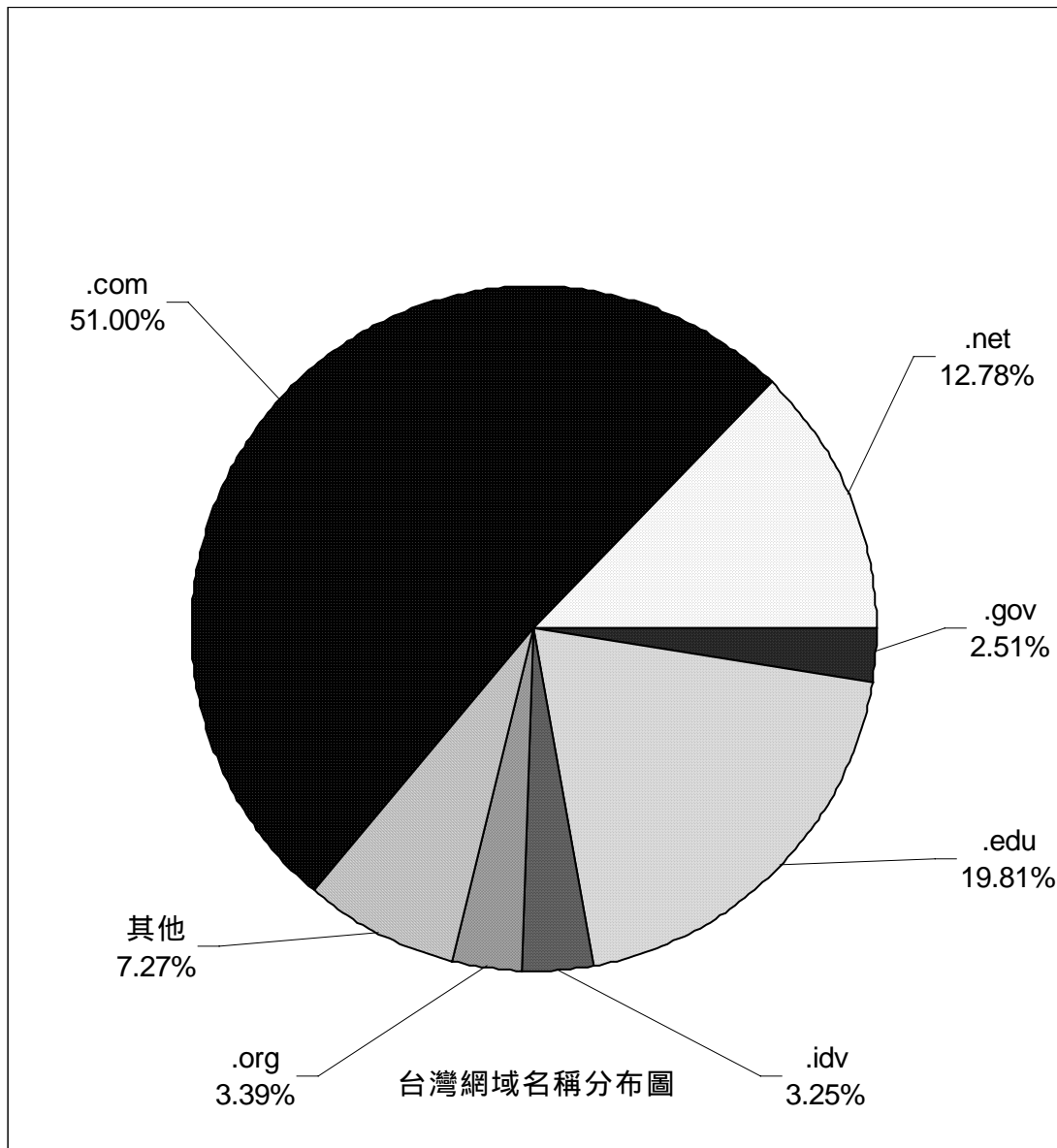


圖 15 台灣地區網域名稱分布統計 (2000/12)

Domain	.com	.net	.gov	.edu	.idv	.org	其他	總計
數目	35689	8943	1756	13865	2272	2371	5089	69985

所佔比例	51.00%	12.78%	2.51%	19.81%	3.25%	3.39%	7.27%	100.00%
------	--------	--------	-------	--------	-------	-------	-------	---------

表 14、 台灣地區網域名稱分布統計 (2000/12)

Domain	Dec 1999	Percent	Dec 2000	Percent	Change
.com	28711	81.90%	35689	51.00%	-30.9
.edu	3385	9.65%	13865	19.81%	10.16
.gov	744	2.12%	1756	2.51%	0.39
.net	764	2.17%	8943	12.78%	10.61
.org	1449	4.13%	2371	3.39%	-0.74
.idv	0	0%	2272	3.25%	3.25
其它	0	0%	5089	7.27%	7.27

因為 TWNIC 在 2000 年 5 月 1 日起正式開放 idv 之個人網域名稱註冊服務，以及 2000 年 11 月 17 日在美國洛杉磯開會時新增七個網域名稱，所以相較於在 2000 年 1 月 1 日所統計的五個網域名稱，2000 年 12 月的統計資料中多了 .idv 以及其它的網域名稱項目。

根據在 2000 年 12 月所完成的台灣網域名稱調查結果，我國的 Domain Name 總數約為 69985 座，其中以公司行號 (COM) 的 35689 做最多，佔總數 51.00%，但是公司行號的網域名稱卻是呈 30.9% 的負成長。第二位為教育機構 (EDU) 擁有 13865 佔總數的 19.81%。以網路組織 (NET) 則擁有 8943 座，佔總數的 12.78%，為第三多。

從 2000 年台灣地區網域名稱分布統計趨勢來看，.net 由去年的 764 成長到 8943 一共成長了 10.61%，說明了今年網路行公司所吹起的熱潮，網路公司急速的成長，相對的申請 .net 的公司也增加。由於中小學上網計劃的施行，也導致今年的 .edu 也成長了 10.16%，可見全國中小學上網的計劃推廣成效顯著。總觀來看，台灣地區各個網域名稱都有成長，可見台灣的電子商務也慢慢的穩定成長中。

## 十二、歸納與結論

根據版本收集的結果以及各伺服器漏洞的資料，我們可以得出台灣地區 Web 伺服器若遭遇惡意攻擊時的存活率。

由於 Web 伺服器本身並不需要管理者 (Unix 下為 root，NT 下為

Administrator)權限來執行，因此我們假設所有的伺服器都以正確的權限安裝，攻擊 Web 伺服器只能獲得 WWW 使用者的權限。

由於所有的伺服器都回傳了版本的訊息，所以版本訊息不列入 Information Leakage 的考慮之中，由於 CGI 程式碼內含有資料庫設定以及檔案位置等重要安全訊息，因此 Information Leakage 考慮否能瀏覽 CGI 原始碼以及獲得目錄下檔案列表之情形。

至於 Relay of Internet Attack 的攻擊方式與伺服器設定有關，無法由伺服器版本資訊獲得，在此不列入調查之內。

綜合之前收集到針對 Web 伺服器安全漏洞的資訊，我們可以歸納出四種不同的攻擊方式：伺服器設定資料洩漏(Information Leakage)、服務阻絕(Denial of Service)、遠端越權讀取(Remote File Read)、以及獲得管理者權限(Web Administrator's Shell)；我們可以依照不同的攻擊強度的進行評估。

表 6-25 為各攻擊強度下台灣 Web 伺服器的存活率。存活率的定義為：

$$(Total\ Hosts - Not\ Vulnerable\ Hosts) / Total\ Hosts$$

攻擊方式	Information Leakage	Denial of Service	Remote File READ	Web admin shell
存活率	20878/38158 (54.71 %)	14514/38158 (38.04 %)	15853/38158 (41.55 %)	20710/38158 (54.27 %)

表 15、各種不同攻擊強度下台灣 Web 伺服器存活率

