Hacking from WEB

行政院 國家資通安全會報
技術服務中心
For HIT2005
Charmi Lin

July 19, 2005

前言

- 網站伺服器(Web Server)，幾乎是每一個組織單位在網際網路上都必須要提供的網路服務。
- WEB管理失當的危險

常見的WEB弱點

- 伺服器應用程式Buffer Overflow
- MISConfiguration(配置失當)
- 使用者輸入驗證上的錯誤
- 網頁程式邏輯上的錯誤
- 程式輸出錯誤
- 密碼管制失當

Buffer Overflow

- 常被使用也最容易修補、發現
- 修補方式僅需安裝廠商的修補程式即可

MISConfiguration

- 目錄權限失當
  - Windows 2000預設將inetpub\wwwroot目錄給於everyone完全的控制權限(可以執行、讀取、寫入)
  - User將Apache使用root權限執行

MISConfiguration

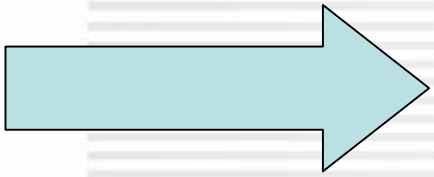
- 提供功能失當
  - WEBDAV的支援
  - 湯姆貓的8005 port

WebDAV

- WebDAV是什麼？
- "Web-based Distributed Authoring and Versioning".
- 它是一組由 HTTP/1.1 的功能延伸出來的通訊協定，讓用戶端發行(公佈資源讓他人使用)、鎖定、並管理 Web 上的資源，使得使用者們得以經由網頁來共同編輯、整理、管理檔案資料。

WebDAV的『好處』

- 啟用WebDAV的好處???
  - 具有權限的使用者就可以在 WebDAV 目錄中自由複製、尋找 、刪除並移動檔案。
  - 修改與某些資源相關的內容。 舉例來說，使用者可以寫入並取回檔案的內容資訊。
  - 將資源鎖定或解除鎖定，如此多位使用者可同時讀取檔案，但一次只有一個人可以修改檔案。
  - 搜尋 WebDAV 目錄中的檔案的要旨與內容。舉例來說，您可以搜尋所有含有 table 這個字的檔案，或是搜尋所有由 Fred 建立的檔案。



誰是有權限的使用者?
誰可以決定要不要用webdav功能?
好處真的是好處嗎?

WebDAV指令

- OPTIONS ？ **à** 可以查詢網站提不提供WebDAV指令

```
OPTIONS * HTTP/1.1
Host: localhost

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Fri, 11 Aug 2000 14:09:10 GMT
Content-Length: 0
Accept-Ranges: bytes
DASL: <DAV:sql>
DAV: 1, 2
Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE,
    MKCOL, PROPFIN
D, PROPPATCH, LOCK, UNLOCK, SEARCH

Allow: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE,
    MKCOL, PROPFIND
, PROPPATCH, LOCK, UNLOCK, SEARCH
Cache-Control: private
```

WebDAV指令

- HEAD？ à 查詢檔案存不存在

```
HEAD /dir/ HTTP/1.1
Host: iis-server
Content-Length: 0
```

WebDAV指令

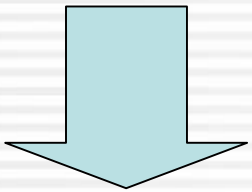
- PUT à 直接上傳檔案
- Delete à 刪除檔案
- Move à 搬移檔案

MISConfiguration

- 元件配置失當
  - FrontPage Server Extension元件

FrontPage Server Extension漏洞

- 什麼是FrontPage Server Extension
  - 一套功能強大的網站管理軟體，支援FrontPage 中的HTML 編輯製作；並擴充 Web 伺服器功能之程式及 Script 的集合，讓使用者可以快速地進行搬移檔案、檢查超連結等動作，管理整個網站



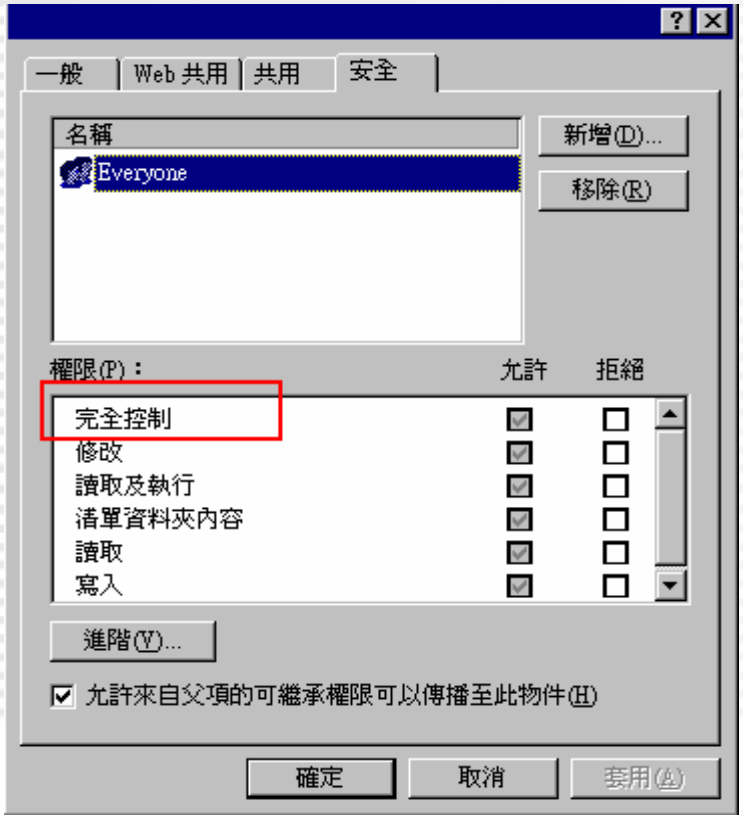
又是一樣的老問題：

誰有權利可以透過FrontPage來管理網站?

誰可以決定要不要啓用FrontPage Server Extension功能?

FrontPage Server Extension漏洞

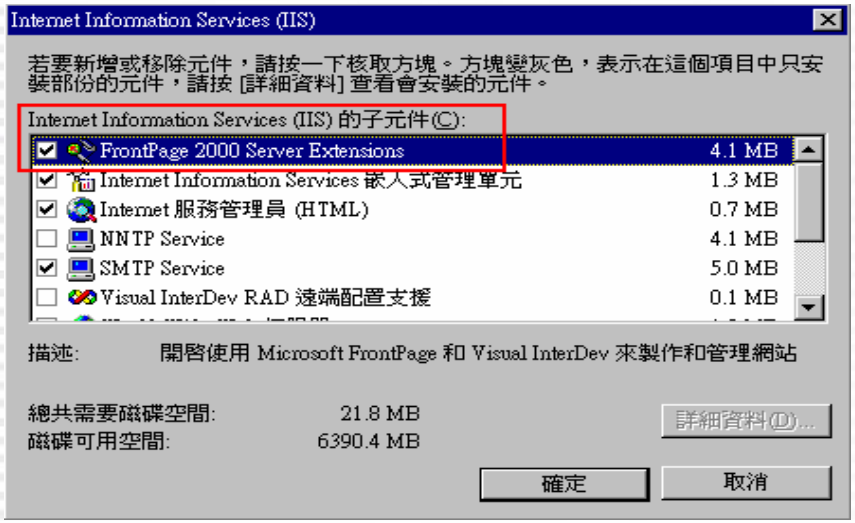
- 誰有權利可以透過FrontPage來管理網站？à Windows的存取控制
- !!!!!! à Windows預設Everyone擁有檔案的完全控制權



任何人都可以透過FrontPage來管理你的網站

FrontPage Server Extension漏洞

- 誰可以決定要不要啟用FrontPage Server Extension功能?



!!!!預設會安裝FrontPage Server Extension!!!!

MISConfiguration

- 範例檔配置失當
  - IIS showcode.asp
  - Php phpinfo.php
  - Tomcat pageInfo.jsp

MISConfiguration

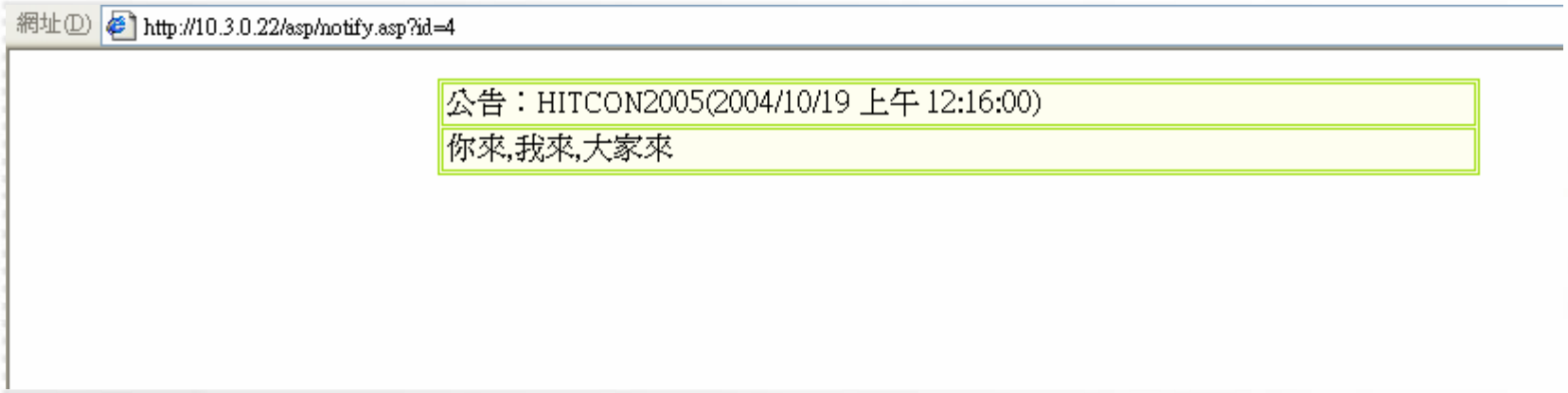
- 網頁編輯器失當
  - old
  - bak
  - ~

使用者輸入驗證上的錯誤

- SQL Injection
- XSS
- Code injection
- 路徑跳脫

XSS

- http://IP/<SCRIPT>foo</SCRIPT>



程式邏輯上的錯誤

- 僅對使用者是否有權限讀取檔案作管理
- 僅對登入畫面做權限控管
- 將重要的資料放在Form表單的隱藏欄位中
- 使用教科書上的檔名、目錄

程式輸出錯誤

密碼管制失當

案例說明－OfficeScan隱含弱點事件

- Trend Micro OfficeScan CGI Directory Insufficient Permissions Vulnerability
  - Trend Micro OfficeScan Corporate Edition 3.0
  - Trend Micro OfficeScan Corporate Edition 3.5
  - Trend Micro OfficeScan Corporate Edition 3.11
  - Trend Micro OfficeScan Corporate Edition 3.13
  - Trend Micro OfficeScan Corporate Edition 3.54
  - Trend Micro Virus Buster Corporate Edition 3.52
  - Trend Micro Virus Buster Corporate Edition 3.53
  - Trend Micro Virus Buster Corporate Edition 3.54
  - 皆有弱點

案例說明－OfficeScan隱含弱點事件

- 正常的登錄畫面
  - 擁有密碼的人才有權利進入系統 ???

案例說明－OfficeScan隱含弱點事件

- 只要知道檔案放在哪裡，就可以竄改密碼!!!!!!!

恭請指正