2005.12.26

今天，接到市網中心及多所學校來電，得知多校被更換網頁。我在下午的時候，線上幫一所私立小學作各方面的檢測和修改，從該校網頁伺服器的系統紀錄檔著手，一一反向分析駭客入侵的手法和原理。詳細分析如下，敬請各位老師參考。

(其實，這裡所談到的，是 ASP 程式網頁伺服器都要注意的，並非只針對「行政公佈欄」這個程式)

# 1 緊急處理程序

## 1.1 修改網頁伺服器設定

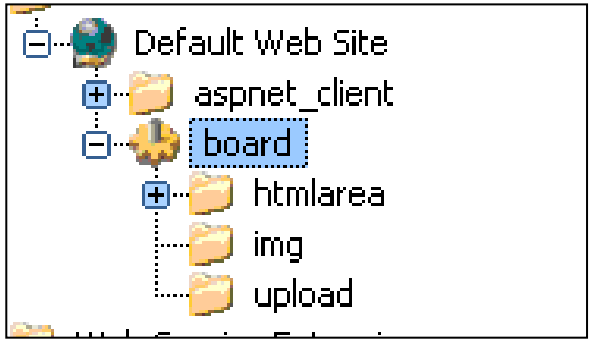
### 1.1.1 虛擬目錄「安全性」的設定

以前我的經驗不足，常常覺得乾脆把「完全控制」的權限加在「Everyone」這個帳號上，省得麻煩。

其實不然，最安全、也是最麻煩的設定步驟是把權限設定給「IUSR_xxxxxxx」

上述的「xxxxxxx」代表的是伺服器的電腦名稱

(以下設定以 board 行政公佈欄為例)：




1.1.1.1 網站放在 D 碟，則 D 碟設定給「IUSR_xxxxxx」帳戶有「讀取及執行」、「清單資料夾內容」、「讀取」的權限

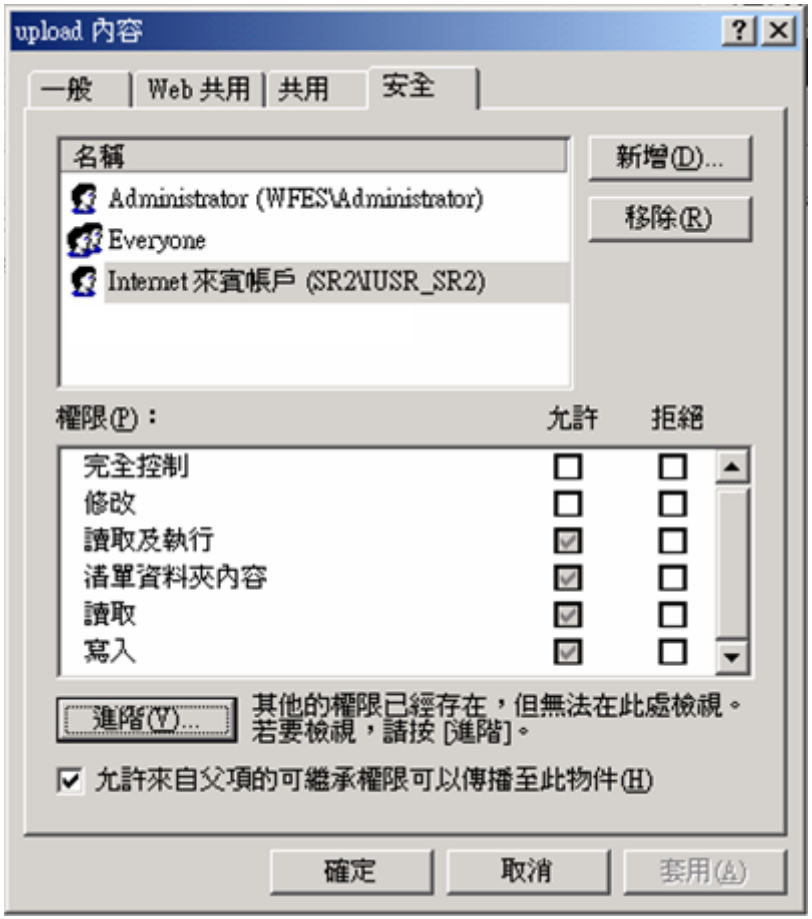
1.1.1.2 board 目錄裡面有 board.mdb，也就是 Access 的資料庫檔案，則「IUSR_xxxxxxx」帳戶對 board 資料夾要多加「寫入」權限

1.1.1.3 board.mdb 檔案本身不需作任何設定

1.1.1.4 upload 目錄因為向上繼承了 board 的「寫入」屬性，所以本身上傳檔案沒有問題

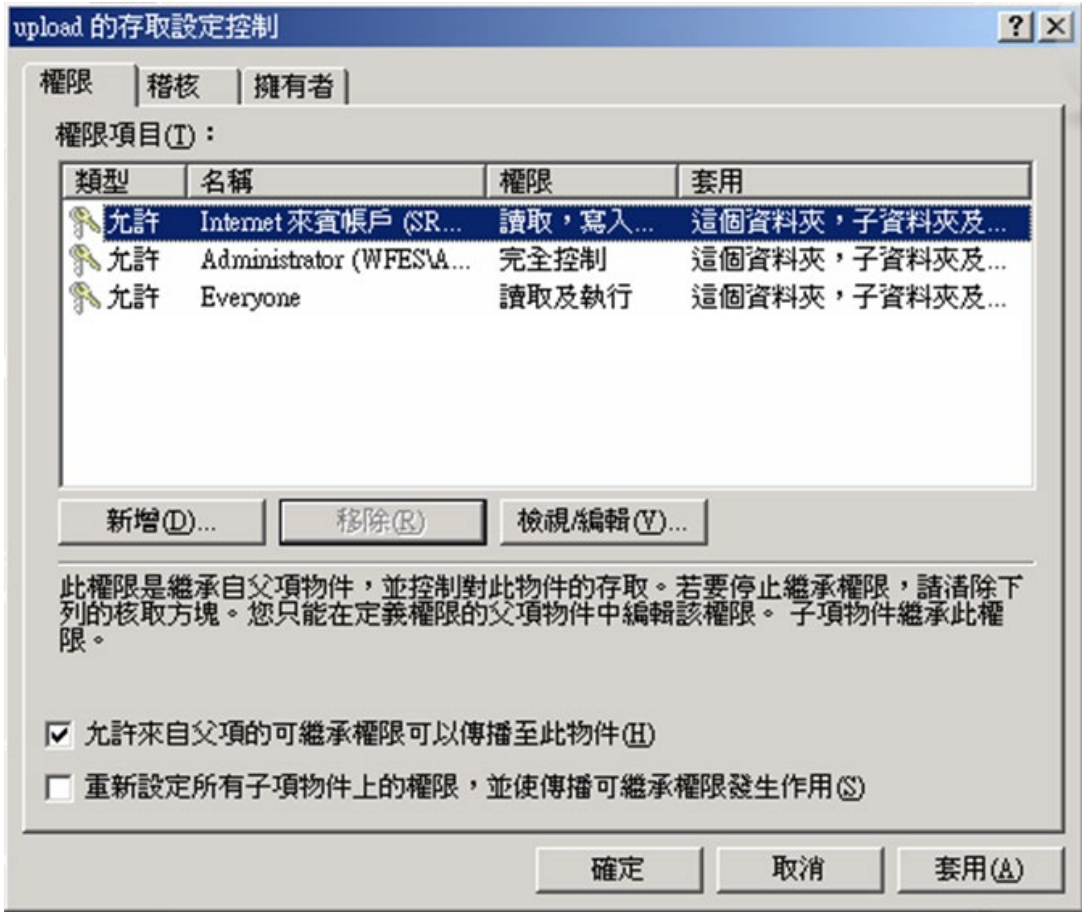
1.1.1.5 但是 upload 目錄會有刪除公告附件檔案的需要，所以需要進入「進階設定」，設定步驟如下：

1.1.1.5.1開啟 upload 資料夾的安全性設定

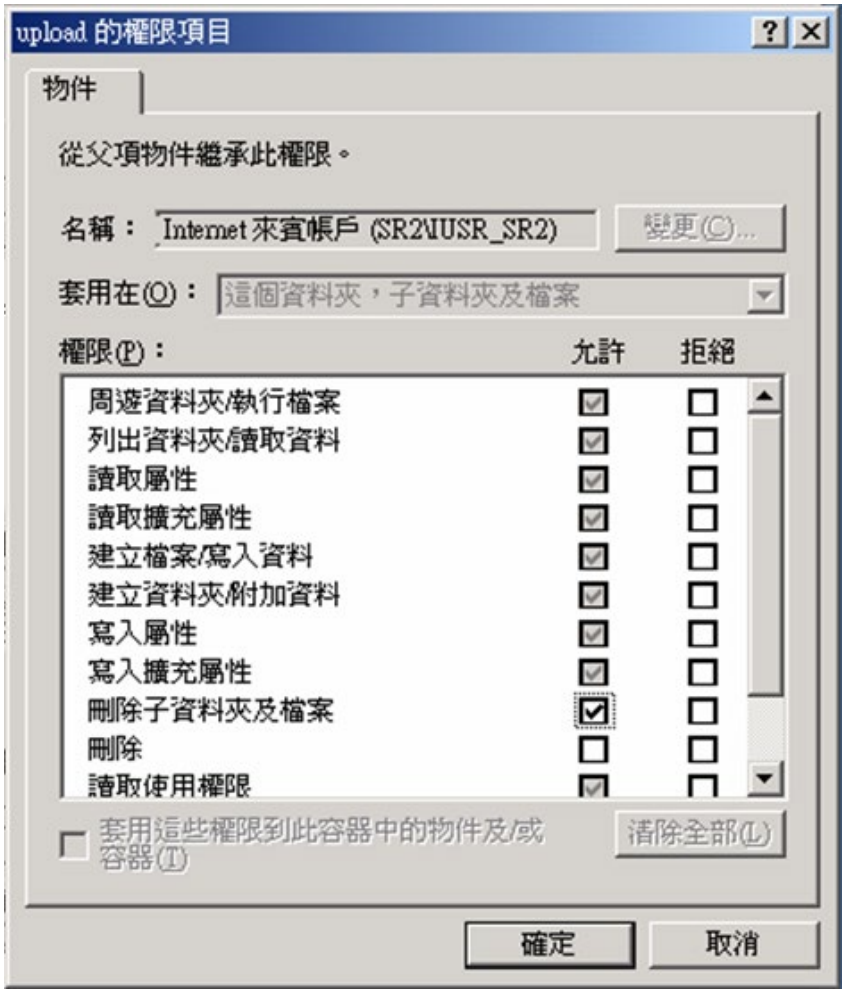



請按下「進階」

1.1.1.5.2選擇「Internet 來賓帳戶」(也就是 IUSR_xxxxxxx)，然後按下「檢視/編輯」



1.1.1.5.3將「刪除子資料夾及檔案」的權限打勾



1.1.2 關閉 WebDAV 服務

這項系統漏洞目前普遍出現在 Windows NT/2000，雖然微軟有修正程式，但是依據「台灣電腦網路危機處理暨協調中心」在「Buffer Overflow in Core Microsoft Windows DLL」這篇文章裡面所引用微軟的技術文件部份內容說到：『根據 MS03-007，微軟發覺有部分客戶安裝修正程式後重開機會遇到系統中止的錯誤。』。再加上根據我與幾位系管師和資訊組長相處的經驗，得知使用 WebDAV 在維護網站的人真的不多。

1.1.2.1 Windows NT

1.1.2.1.1「開始」「執行」，輸入 regedt32.exe

1.1.2.1.2從左邊的樹狀結構之中，用滑鼠點按並依序找到：

HKEY_LOCAL_MACHINE

SYSTEM

CurrentControlSet

Services

W3SVC ←這個名稱可能會有不同，譬如可能會是 WZCSVC

Parameters

1.1.2.1.3在右邊視窗空白處點一下滑鼠右鍵，新增一個型態為 DWORD 的值，取名為 DisableWebDAV。完成新增之後，按一下 Enter，就可以修改它的值。請輸入 1，然後按下「確定」。

1.1.2.1.4修改完畢之後，重新啟動網頁伺服器。(要重新開機也可以啦～只是比較狠一點。)

1.1.2.2 Windows 2000

1.1.2.2.1「開始」「執行」，輸入 regedit.exe

1.1.2.2.2其他步驟同 1.1.2.1.2 ~ 1.1.2.1.4

1.2 修改程式漏洞

1.2.1 密碼驗證

如果您的密碼程式是 pwd.asp，請您檢查您的驗證程序是不是這樣：

```
Set conn = Server.CreateObject("ADODB.Connection")
param = "driver={Microsoft Access Driver (*.mdb)}"
conn.Open param & ";dbq=" & Server.MapPath("/pwd/userspwd.mdb")
```

```
sql = "Select * From users Where pID='" & pID & "' And Pwd = '" & Pwd & "'"
Set rs = conn.Execute( sql )
    If rs.EOF Then
        CheckPwd = False
    Else
        CheckPwd = True
        pFrom = rs("pFrom")
        pName = rs("pName")
        pTag    = rs("pTag")
    End If
```

解決方法：

(一)修改密碼資料庫的存取位置：

將 userspwd.mdb 改名為 userspwd.asp，或是其他的名稱的.asp，例如：2g82jduhdlf.asp

然後記得把 conn.Open param & ";dbq=" & Server.MapPath("/pwd/userspwd.mdb")裡面

的 userspwd.mdb 改成您資料庫的新檔名

這樣一來，想要直接下載，大概會是一堆亂碼，但是至少不是那麼容易取得密碼的訊息。

不過，如果您想用 Microsoft Access 直接存取，就可能要把副檔名給回來讓 Access 可以存取。

(二)修改密碼驗證的語法：

驗證的主要語法在於：

```
    sql = "Select * From users Where pID='" & pID & "' And Pwd = '" & Pwd & "'"
    Set rs = conn.Execute( sql )
        If rs.EOF Then
            CheckPwd = False
        Else
            CheckPwd = True
            pFrom = rs("pFrom")
            pName = rs("pName")
```

```
            pTag    = rs("pTag")
        End If
```

請改為下列內容：

```
    sql="Select pID From users Where pID='" & Request("pID") & "'"
    Set Rs=conn.execute(sql)
    IF Rs.EOF<>True Then
      IF Rs("pID")=Request("pID") Then '檢查搜尋結果與 Request("ID")  再次驗證
        sql="Select * From users Where pID='" & Rs("pID") & "'" '以驗證的結果找密碼
        Set Rsp=conn.execute(sql)
        IF Rsp.EOF <>True Then
          IF Rsp("Pwd")=Request("Pwd") Then
            CheckPwd = True
            pFrom = Rsp("pFrom")
            pName = Rsp("pName")
            pTag    = Rsp("pTag")
            Session("pTag") = Rsp("pTag") '←將來其他的 ASP 程式可以透過這裡的 Session 來驗證
            Session("pName")= Rsp("pName")
            Session("pFrom")= Rsp("pFrom")
            rs.close:set rs=nothing
            conn.close:set conn=nothing
          Else
            CheckPwd = False
            Session("PwdHead1") = "<font color=#FF0000>密碼<font color=#0000FF>資料驗證有誤"
            Session("PwdHead2") = "<font color=#0000FF>Input Error in <font color=#FF0000>Password"
            Response.Write "<center><br><br><br><br>"
            Response.Write "<span style=font-size:20pt>" & Session("PwdHead1") & "</span><br>"
            Response.Write "<span style=font-size:16pt;font-family:arial>" & Session("PwdHead2") & "</span>"
            Response.End
```

```
            End IF
        Else
            CheckPwd = False
            Session("PwdHead1") = "<font color=#0000FF>找不到<font color=#FF0000>密碼<font color=#0000FF>,資料驗證有誤"
            Session("PwdHead2") = "<font color=#0000FF>Can Not Match The <font color=#FF0000>Password"
            Response.Write "<center><br><br><br><br>"
            Response.Write "<span style=font-size:20pt>" & Session("PwdHead1") & "</span><br>"
            Response.Write "<span style=font-size:16pt;font-family:arial>" & Session("PwdHead2") & "</span>"
            Response.End
        End IF
    Else
        CheckPwd = False
        Session("PwdHead1") = "<font color=#FF0000>使用者帳號<font color=#0000FF>資料驗證有誤"
        Session("PwdHead2") = "<font color=#0000FF>Input Error in <font color=#FF0000>Account"
        Response.Write "<center><br><br><br><br>"
        Response.Write "<span style=font-size:20pt>" & Session("PwdHead1") & "</span><br>"
        Response.Write "<span style=font-size:16pt;font-family:arial>" & Session("PwdHead2") & "</span>"
        Response.End
    End IF
Else
    CheckPwd = False
    Session("PwdHead1") = "<font color=#0000FF>找不到<font color=#FF0000>使用者帳號<font color=#0000FF>,資料驗證有誤"
    Session("PwdHead2") = "<font color=#0000FF>Can Not Find The <font color=#FF0000>Account"
    Response.Write "<center><br><br><br><br>"
    Response.Write "<span style=font-size:20pt>" & Session("PwdHead1") & "</span><br>"
    Response.Write "<span style=font-size:16pt;font-family:arial>" & Session("PwdHead2") & "</span>"
    Response.End
End IF
```

## 1.3 處理疑似駭客值入的後門程式檔案

### 1.3.1 刪除後門程式檔案

請利用「檔案搜尋功能」(請不要偷懶只尋找 board1 目錄，可能 upload 目錄裡面也會有)，尋找網頁伺服器裡面是否有下列檔案，如果有，請您刪除；如果想了解和分析，請搬移到安全的機器上。

asphelperb5.cer

ht_tw.asp

lndex.asp (←第一個字母是小寫的 L)

loader.asp

mm.asa

vnspass.asp (←值得研究)

webshell.asp

xd.asp (←經典，值得研究)

### 1.3.2 檢查原始程式是否被竄改

title.asp

index.asp

index.aspx

default.asp

default.aspx

2 按部就班的解析和處理程序

2.1 密碼驗證機制 pwd.asp 的引用方式

任何一個 ASP 的程式如果想要引用 pwd.asp 來驗證，語法是(請注意#include virtual 所引用的檔案位置，可能必須自行正確設定)：

```
<%If session("pTag")="" then%>
<!-- #include virtual="/pwd/pwd.asp" -->
<%end if%>

<%
If Right(pTag,1)<"k" Then
%>
<HTML><HEAD><TITLE></TITLE><meta http-equiv="Content-Type" content="text/html; charset=big5"></HEAD>
<BODY BACKGROUND='img/b01.jpg'>
<HR>
<center>敬愛的<font color='#FF0000'><%=pName%></font><BR>
您的權限無法張貼公告，所以不允許您進入。<BR>
如果真的有需要進入，請您與資訊小組聯繫。<BR><HR></center>
<CENTER>
<A HREF='Title.asp' class=9-font>返回公告欄主畫面</A>
</CENTER>
</BODY>
</HTML>
<%
  response.end
End If
%>
```

2.2 張貼機制

2.2.1 張貼的表單 titlefrm.asp

如果您的表單程式內容的驗證語法是

```
<!-- #include virtual="/pwd/pwd.asp" -->

<%
If Right(pTag,1)<"k" Then
    Response.Write "<HTML><HEAD><TITLE></TITLE></HEAD>"
    Response.Write "<BODY>"
    Response.Write "<HR>"
    Response.Write "<center>敬愛的<font color='#FF0000'>" & pName & "</font><BR>"
    Response.Write "您的權限無法張貼公告，所以不允許您進入。<BR>"
```

就必須改成

```
<%If session("pTag")="" then%>
<!-- #include virtual="/pwd/pwd.asp" -->
<%end if%>

<%
If Right(pTag,1)<"k" Then
    Response.Write "<HTML><HEAD><TITLE></TITLE></HEAD>"
    Response.Write "<BODY>"
    Response.Write "<HR>"
    Response.Write "<center>敬愛的<font color='#FF0000'>" & pName & "</font><BR>"
    Response.Write "您的權限無法張貼公告，所以不允許您進入。<BR>"
```

這樣修改的好處是，不必每次想要張貼，都必須重新輸入帳號和密碼。只要用戶沒有關掉瀏覽器，就可以一直張貼。當然，也要提醒大家，不用電腦的時候要關掉瀏覽器，同時登出網域，以免遭人利用。

### 2.2.2 接收表單資料並儲存的程式 titlenew.asp

這個程式的問題語法在於下面這一段：

```
Name=Request("Name")
Email=Request("Email")
```

```
Subject=Request("Subject")
Words=Request("Words")
Http=Request("Http")
StopYear=Request("StopYear")
StopMonth=Request("StopMonth")
StopDay=Request("StopDay")
```

要改為

```
Name=Request.Form("Name")
Email=Request.Form ("Email")
Subject=Request.Form ("Subject")
Words=Request.Form ("Words")
Http=Request.Form ("Http")
StopYear=Request.Form ("StopYear")
StopMonth=Request.Form ("StopMonth")
StopDay=Request.Form ("StopDay")
```

這樣將會強制接收資料的時候，一定要透過網頁裡的表單來填送。
否則駭客只要在他的瀏覽器下達下列這個網址，就不必通過表單，也能成功幫您張貼一篇公告。

http://xxx.xxxx.tp.edu.tw/board1/titlenew.asp?Name=駭客&Email=駭客俱樂部&Subject=駭客報到&Words=您的網站被我入侵了&StopYear=999&StopMonth=99&StopDay=99

因為這個程式也是「限定資格」的程式，所以最前面也要加上前面提過的驗證，會比較安全，也就是：

```
<%If session("pTag")="" then%>
<!-- #include virtual="/pwd/pwd.asp" -->
<%end if%>

<%
If Right(pTag,1)<"k" Then
    Response.Write "<HTML><HEAD><TITLE></TITLE></HEAD>"
```

```
Response.Write "<BODY>"
Response.Write "<HR>"
Response.Write "<center>敬愛的<font color='#FF0000'>" & pName & "</font><BR>"
Response.Write "您的權限無法張貼公告，所以不允許您進入。<BR>"
```

## 2.3 上傳機制

### 2.3.1 上傳附件的表單 upload.asp

這個程式的基本問題，也是在程式的開頭缺乏了驗證機制，請比照 2.2.1

### 2.3.2 接收上傳附件並儲存的程式 uploadok.asp

這個程式的基本問題，也是在程式的開頭缺乏了驗證機制，請比照 2.2.1

後記：我們都需要繼續成長(以下非技術文件，建議各位可以省略不看)

或許很多朋友認為我接下來要說的話是在放「馬後炮」，那麼我先向各位致歉。

「行政公佈欄」是我在 1989 年為了當年教育部「擴大內需方案」後續的「學校網頁製作比賽」而編寫的。那時候在「網站架設」、「網頁美工」、「程式設計」這三部份，我選擇擔任「程式設計」的工作。以一個「音樂教育學系」畢業的我來說，我非資訊科技相關科班出身，在自卑之餘，在最短的時間之中，儘速的吸取必要的知識，是我當時唯一的信念。

當時坊間的的書並不多，我東抄抄西抄抄，勉強拼湊出了個「行政公佈欄」。對於那些供我抄襲的網路資源和出電腦書的作者，至今我仍深懷感恩之心，從來不會因為他們提供的資源和經驗，導致我日後有修不完的程式漏洞，而耿耿於懷。也許您不相信，我似乎對駭客也抱著一絲絲的敬意和謝意，因為他們讓我有成長的機會。

對於提供我程式漏洞或是系統的朋友們，或許他們曾經寄望我會把這些程式或是系統的漏洞問題浮現出來跟大家分享。但是當時的我停下了我的腳步。因為我覺得凡事一體兩面，若是我公佈了漏洞，而不是每一位用我的程式的朋友都能夠收到這些訊息；那麼對於喜歡挑戰的駭客而言，我的分享也將成為他們學習的依據和入侵的參考，當然，僅僅只是被當作入門教材而已。

我雖然無法保證解決了百分之百的問題，也無法保證是不是百分之百收到每一位朋友的訊息、進而能夠提供我的經驗共同解決問題。不過，凡是透過電話、電子郵件或是透過論壇網站能夠與我聯繫得上的朋友們，還記得嗎？我們曾經透過 MSN 或是 VNC 共同解決了問題。我想我對他們無愧於心，我盡力了。畢竟我的正職只是一個普通的小學教師。請大家多參與網路論壇，因為別人發表的問題，也可能是您的問題、或是您將會遭遇到的問題。

最後要感謝市網中心的所有長官和業務相關人員，尤其是蔡政道先生，在他的眼中，我或許是微不足道的小系管，但是他總是熱心且誠懇的指導我，並且願意耐心聽完我的「火星話」，最後，協助我完成許多的業務。

臺北市萬芳國小 科任教師 李嘉澍 敬上

falcon@wfes.tp.edu.tw

p.s.除了市網的新討論板 http://web.tp.edu.tw/，我會在 http://itclub.wfes.tp.edu.tw/恭候各位的大駕光臨