# 資訊安全管理與數位鑑識論壇

講師 林俊賢
lin.jsian@gmail.com

105.04.19

# 關於我

- 學歷:
  2010.09-2012.06:虎尾科技大學資訊管理所碩士
  2006.09-2010.06:虎尾科技大學資訊管理系學士

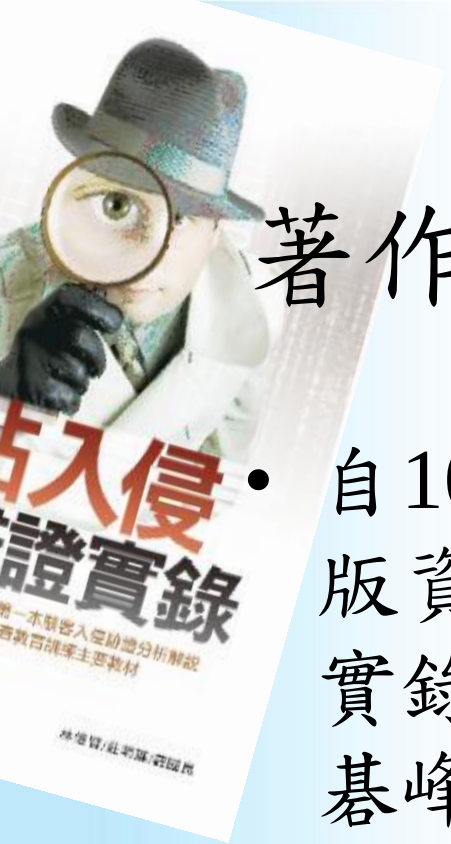
- 經歷:
  2016.04:資策會 資安所
  2015.11至2016.03:遠東銀行資安部 資深專員
  2013.01至2015.11 :刑事局研發替代役
  2014.04:賽門鐵克_網路安全攻防戰(War Game)
  2014:103年行政院國家資通安全網路攻防演練
  2013:102年行政院國家資通安全網路攻防演練

# 關於我

- 證照:
  2015.08:Network Security of Packet Analysis,NSPA
  2014.11:EC-Council Certified Ethical Hacker,CEH v8
  2012.03:TQC-行動裝置應用程式設計認證(Android APP)
- 2007.10:勞委會-軟體設計丙級
- 2006.03:勞委會-軟體應用乙級

# 研究領域

- 日誌檔分析
- 惡意程式分析(電腦/手機)
- 資安檢測
- 中繼站追查
- 駭客手法解析
- APP檢測




# 著作–網站入侵現場鑑證實錄

- 自104年11月退伍後，於105年1月出版資訊安全專書「網站入侵現場鑑證實錄(ISBN:9789863478812)，出版社:碁峰」，其書籍主要是幫助企業資安、網管人員了解駭客入侵後所遺留下的數位證據來輔助分析，以找出駭客入侵手法後修補網站漏洞。

# 著作–網站入侵現場鑑證實錄

- 出版著作迄今皆在各大網路書店(博客來、天瓏、金石堂等)有不錯的銷售成績(Top 10)。
- 目前更被國外應用軟體開發廠商(lizard-labs )，主動將本書封面更新至官方網站進一步推廣。

# 演講經驗

2013年至今，近20場的資安講課經驗

| 日期 | 演講主題 | 地點 |
|---|---|---|
| 2016.03 | 追查惡意程式分析實例-以gh0st為案例介紹 | 國立虎尾科技大學 資訊管理系 |
| 2015.12 | 大學時期求學經驗分享與資安宣導 | 國立虎尾科技大學 資訊管理系 |
| 2015.10 | 網路犯罪偵查技術及個案分享 | 憲兵隊幹部人員 |
| 2015.10 | 手機惡意APP解析 | 國立虎尾科技大學 資訊管理系 |
| 2015.10 | 瞭解駭客如何入侵您的網站與手法 | 國立虎尾科技大學 資訊管理系 |
| 2015.09 | Android手機鑑識 | 嘉義縣警察局 |
| 2015.08 | 網路攻擊入侵事件 -伺服器日誌檔案分析實務 | 104年度科技犯罪偵查教育訓練 |
| 2015.04 | 線上賭博網站追查 | 刑事局偵查科(保一總隊) |
| 2015.04 | APP通訊軟體解析 | 基隆市警察局刑事警察大隊 |
| 2015.04 | 駭客入侵攻擊手法解析 | 中央警察大學 |



更多: http://linjsian.bloagspot.tw/p/blog-page.html

# 企業現況如何判斷異常

- 等到網站整個掛了?
- 流量異常?
- 個資外洩?
- 無事即無異常?

# 人為分析與設備分析迷思

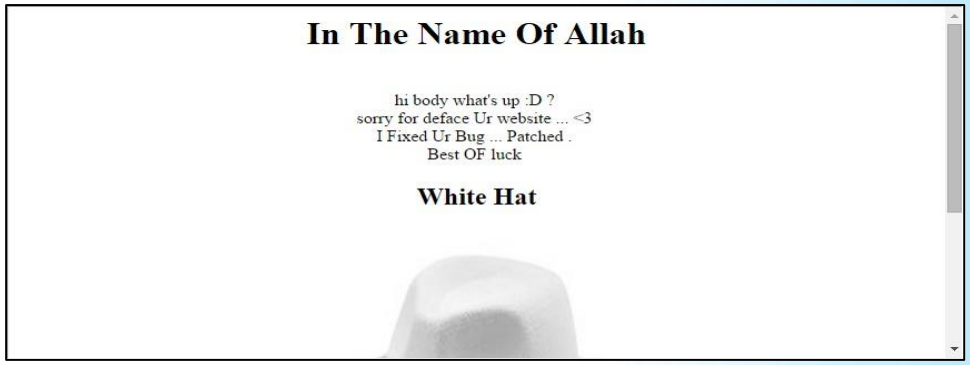
- 網站流量中，同時存在正常流量與異常行為並存的情況
- 人為分析
  經驗、專業、know how
- 設備分析
  設備說沒問題就沒問題

# 寫書目的

- 網站管理人員不知道網站為何被駭?
- 企業網站不知道本身漏洞為何?
- 駭客怎麼利用漏洞進來的?
- 怎麼修補資安面臨的漏洞?
- 宣導資安的重要性
- 工作經驗的分享

# 網路攻擊無所不在

- 下一個目標會不會就是你維護的網站呢?

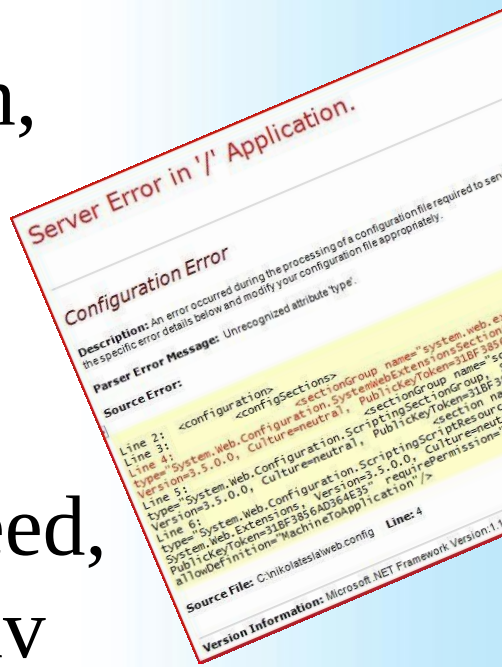


# 駭客入侵手法百百款

- 網站漏洞(XSS，SQL injection…)
- 程式出錯秀出敏感資料(404)
- 外掛程式漏洞(Fckeditor)
- 權限未設置完全(index of)
- 弱密碼(123456 、12345、p@ssw0rd)
- 認證邏輯問題(認證信件問題)
- Zero Day(零時差攻擊)
- APT(電子郵件)

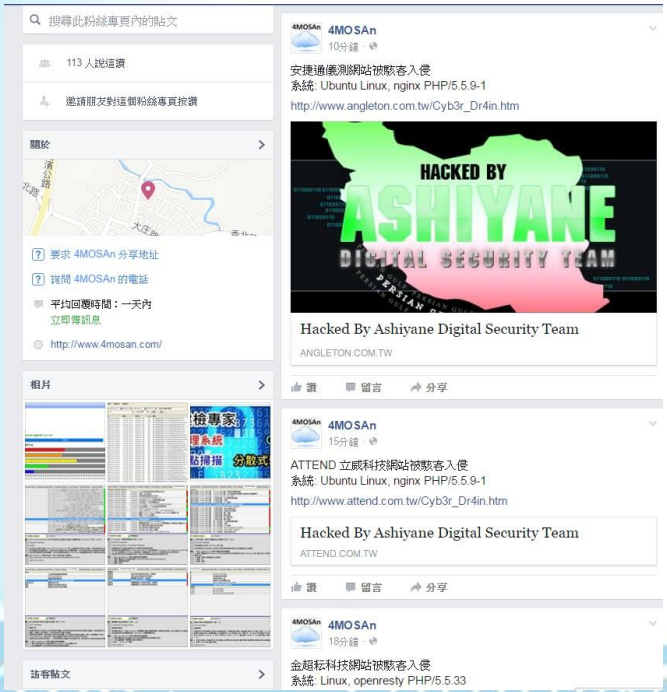
# 了解駭客如何進來您的網站

- 常見網站攻擊手法
- 網站前端(web)
  OWASP TOP 10 (SQL injection, XSS,webshell, index of, weak password…等)
- 系統漏洞(system)
  0-day(CVE-2014-0160 Heartbleed, CVE-2015-0235 Ghost),WebDav



# 網站遭入侵後，傳播之快

- Facebook,Twitter,plurk,etc.
- 全世界都知道，就您不知道!



# 網站遭駭所造成的影響?

- 個資外洩
- 隱私外洩
- 詐騙電話
- 金錢損失
- 工作不保

# 全球最大的偷情網站「Ashley Madison」遭駭客入侵

Ashley Madison (Avid Dating Life, Inc) [CA] https://www.ashleymadison.com

rt number

會員登入

ASHLEY MADISON®

2015年09月30日11:16 傳送 讚 1,202 G+1 0

全球知名偷情網站Ashley Madison日前被駭客公布會員電郵帳號，廉政署隨即接獲舉報，指國內共有104個政府單位及1396個教育單位的電郵，也在名單內。

今日出刊的《周刊王》報導，比對完整名單，發現帳號擁有者包括民進黨籍屏東縣長潘孟安、台大法醫研究所所長孫家棟，台北市政府也有11個高階人員入列。《周刊王》調查，偷情網遭駭客公布的電郵中，「ly11061c@ly.gov.tw」是潘孟安擔任立委時的國會研究室公用帳號。對此，屏東縣長室祕書黃建嘉表示，潘孟安個人或公務信箱，從不曾上過Ashley Madison網站。因事涉政府資安與個人操守，廉政署正釐清。（即時新聞中心／綜合報導）

號稱是「偷情專用Google」的全球最大偷情媒介網站ASHLEY MADISON今年7月遭駭後，美國媒體披露，逾3700萬名會員的姓名、信用卡資料、裸照等個資，已遭駭客全數公布。今天出刊的「周刊王」報導指出， 廉政署接獲舉報，指國內共有104個政府單位和1396個教育單位的電郵，也在偷情客名單之列。

**北市府11人入列**

「周刊王」指出，這個名單包括民進黨屏東縣長潘孟安、台大法醫研究所所長孫家棟，以及台北市政府也有11個高階人員名列其中。公布的電郵中，「ly11061c@ly.gov.tw」是潘孟安擔任立委時的國會研究室公用帳號。

屏東縣府發言人黃建嘉上午指出，名單裡面遭駭的是潘孟安擔任立委時的公務信箱，潘孟安未曾使用公務信箱或個人信箱上過這個網站。除了潘孟安信箱以外，國內共有104個政府單位及1396個教育單位的電郵也在名單內，縣長也是眾多受害者之一，希望中央政府能夠重視資安問題，建立阻止駭客機制，不能讓駭客予取予求。

# 歐悅旅館被駭萬筆個資外洩

iThome 新聞 產品評測 CIO DevOps 技術 專題 專欄 主題頻道 研討會 社群

## 歐悅連鎖精品汽車旅館傳遭駭，5000筆個資外流

駭客去年11月在Pastebin公佈了約5000筆歐悅會員住宿客資料，包括姓名、電話、訂房型式、帳號等，可能使不少男女私下交往的親密關係曝光。

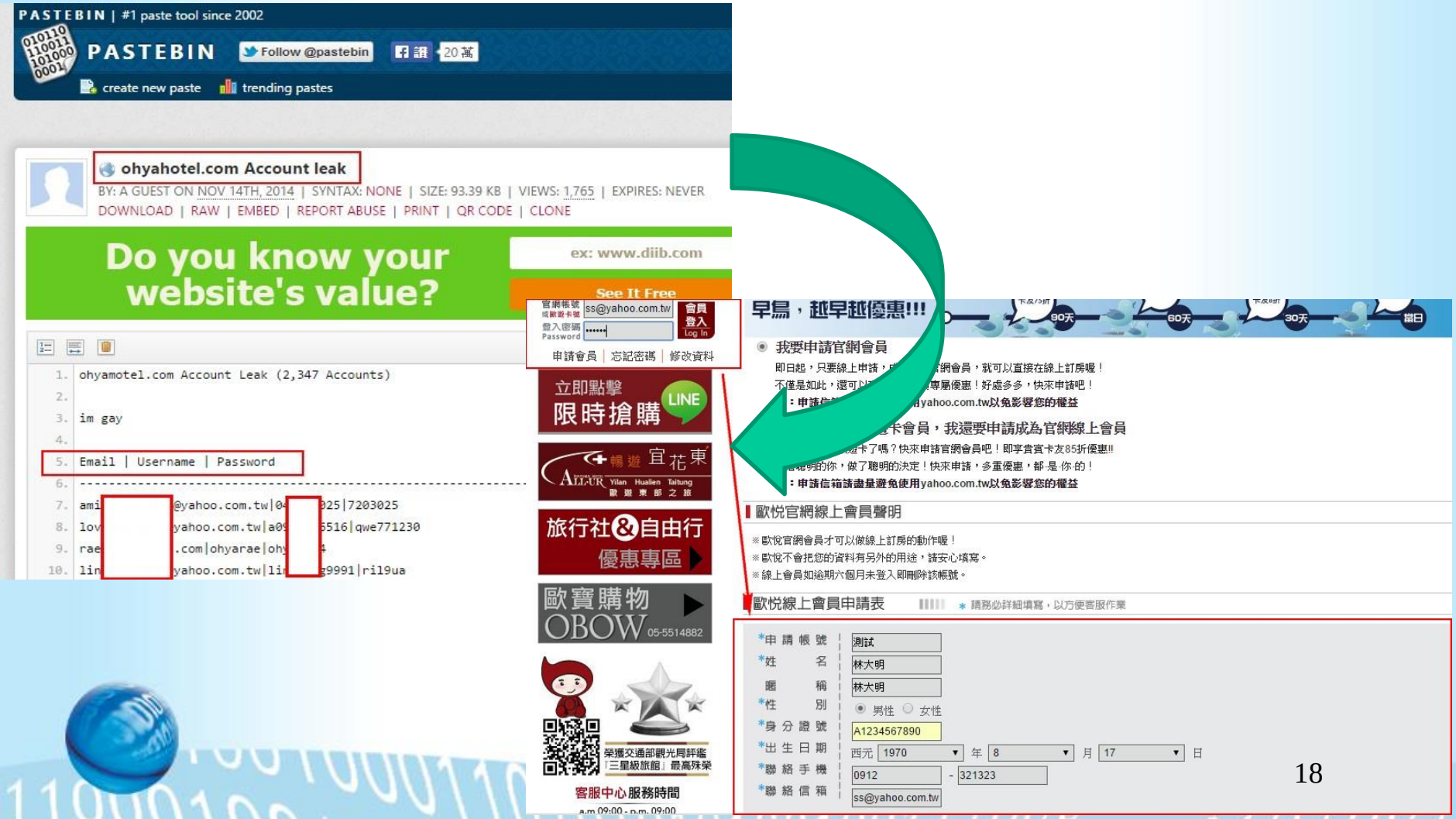
文/ 蘇文彬 | 2015-09-30 發表

讚 1.7萬 按讚加入iThome粉絲團 分享 16 G+1 2

全台有15家據點的歐悅國際連鎖精品旅館集團遭駭長達10個月，去年被發現有五千筆會員和住宿客戶個資，遭張貼在pastebin駭客網站上，客戶的姓名、電話，連訂房型式、房間都一覽無遺。

今日出版的《自由時報》報導，歐悅疑遭中國網軍或網路駭客攻擊，再將駭得的資料放到pastebin網站公布，可供任何人或其他駭客瀏覽。遭駭個資包括：姓名、帳號、電郵、生日、電話、行業別、訂房型式、註冊時間等。駭客只要以流出的帳號密碼登入，即可看到帳號持有人登記的個資。台北市警方資訊犯罪偵查人員昨認為，目前最緊張的，可能是有偷情紀錄怕被發現的人；至於對一般人，個資外洩難免會收到一些行銷電話，徒增困擾。（即時新聞中心／綜合報導）

# 隱私曝露

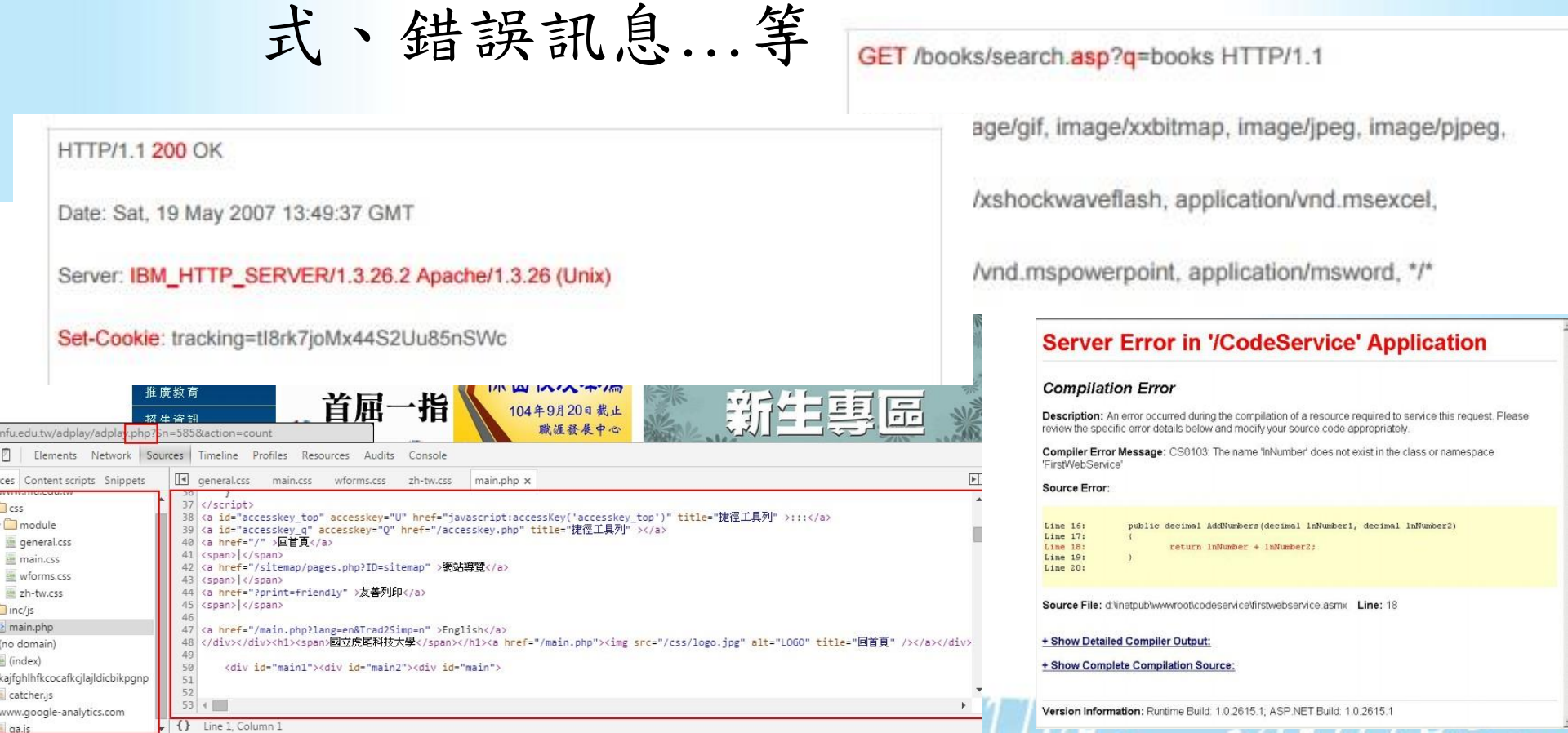

PASTEBIN | #1 paste tool since 2002
PASTEBIN
Follow @pastebin
create new paste
trending pastes
ohyahotel.com Account leak
BY: A GUEST ON NOV 14TH, 2014 | SYNTAX: NONE | SIZE: 93.39 KB | VIEWS: 1,765 | EXPIRES: NEVER
DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT | QR CODE | CLONE
Do you know your website's value?
ex: www.diib.com
See It Free
1. ohyamotel.com Account Leak (2,347 Accounts)
3. im gay
5. Email | Username | Password
7. ami @yahoo.com.tw|04 925|7203025
8. lov yahoo.com.tw|a09 5516|qwe771230
9. rae .com|ohyarae|ohy 4
10. lin yahoo.com.tw|lin 9991|ri19ua
會員登入
申請會員 | 忘記密碼 | 修改資料
立即點擊 限時搶購 LINE
暢遊 宜花東
旅行社&自由行 優惠專區
歐寶購物 OBOW 05-5514882
榮獲交通部觀光局評鑑「三星級旅館」最高殊榮
客服中心服務時間
早鳥，越早越優惠!!!
我要申請官網會員
歐悅官網線上會員聲明
※歐悅官網會員才可以做線上訂房的動作喔！
※歐悅不會把您的資料有另外的用途，請安心填寫。
※線上會員如逾期六個月未登入即刪除該帳號。
歐悅線上會員申請表
*申請帳號 測試
*姓名 林大明
暱稱 林大明
*性別 男性 女性
*身分證號 A1234567890
*出生日期 西元 1970 年 8 月 17 日
*聯絡手機 0912 - 321323
*聯絡信箱 ss@yahoo.com.tw

# 會員長相

- Facebook
- Google
- Mail(yahoo,hotmail)
- etc…

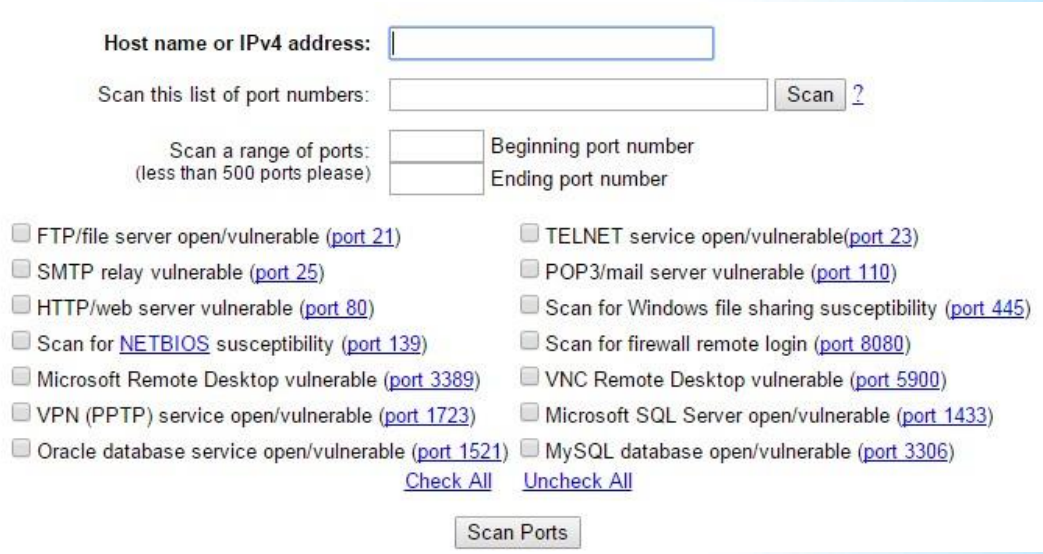
# 基本檢測網站手法

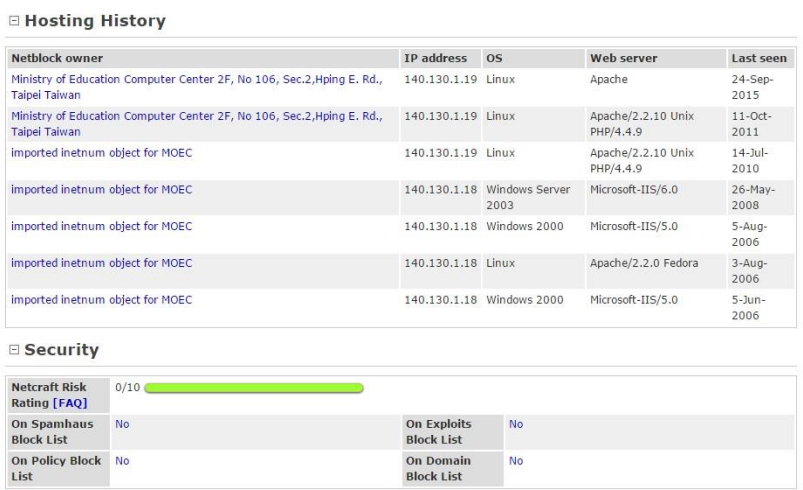
- HTTP Request、Response，開發者模式、錯誤訊息…等



# 線上掃瞄測試

- Port scan
- OS scan



Hosting History

| Netblock owner | IP address | OS | Web server | Last seen |
|---|---|---|---|---|
| Ministry of Education Computer Center 2F, No 106, Sec.2,Hping E. Rd., Taipei Taiwan | 140.130.1.19 | Linux | Apache | 24-Sep-2015 |
| Ministry of Education Computer Center 2F, No 106, Sec.2,Hping E. Rd., Taipei Taiwan | 140.130.1.19 | Linux | Apache/2.2.10 Unix PHP/4.4.9 | 11-Oct-2011 |
| imported inetnum object for MOEC | 140.130.1.19 | Linux | Apache/2.2.10 Unix PHP/4.4.9 | 14-Jul-2010 |
| imported inetnum object for MOEC | 140.130.1.18 | Windows Server 2003 | Microsoft-IIS/6.0 | 26-May-2008 |
| imported inetnum object for MOEC | 140.130.1.18 | Windows 2000 | Microsoft-IIS/5.0 | 5-Aug-2006 |
| imported inetnum object for MOEC | 140.130.1.18 | Linux | Apache/2.2.0 Fedora | 3-Aug-2006 |
| imported inetnum object for MOEC | 140.130.1.18 | Windows 2000 | Microsoft-IIS/5.0 | 5-Jun-2006 |

Security

| | | | |
|---|---|---|---|
| Netcraft Risk Rating [FAQ] | 0/10 | | |
| On Spamhaus Block List | No | On Exploits Block List | No |
| On Policy Block List | No | On Domain Block List | No |

http://www.t1shopper.com/tools/port-scan/
http://www.netcraft.com/

# 滲透(弱掃)工具

- SQLmap
- Acunetix Web Vulnerability Scanner, WVS
- Nmap
- Kail

# 網站管理人員/資安人員應具備的分析技術

- 了解駭客如何進來
- 網站本身的漏洞
- 如何進行修補動作
- 以防下次又遭到第2次攻擊

學會分析日誌檔案!

# 本次學習目標

- 學會怎麼看日誌檔案(Log)
- 好用網路工具分享
- 降低學習門檻
- 互相交流

# 需檢視什麼記錄呢?

- log檔(伺服器的web log、本機的event log[應用程式 log，安全性 log，系統 log])
- 網站程式碼
- 防火牆記錄(firewall log)
- 其他被駭證明記錄檔

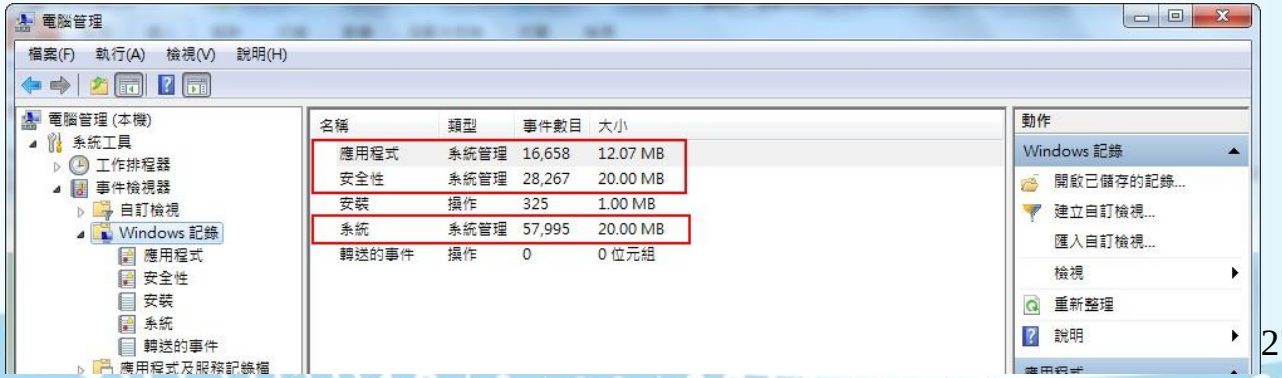
# 什麼是log檔?

- 俗稱「日誌檔」
- 分為本機日誌檔(event log)和伺服器日誌檔(server log)
- 本機日誌檔主要記錄主機本身所有的行為記錄(登入/出，異常，系統，安裝等)
- 伺服器日誌檔主要記錄網站伺服器所發生的行為(瀏覽、查詢、登入/出等)

# 本機日誌檔

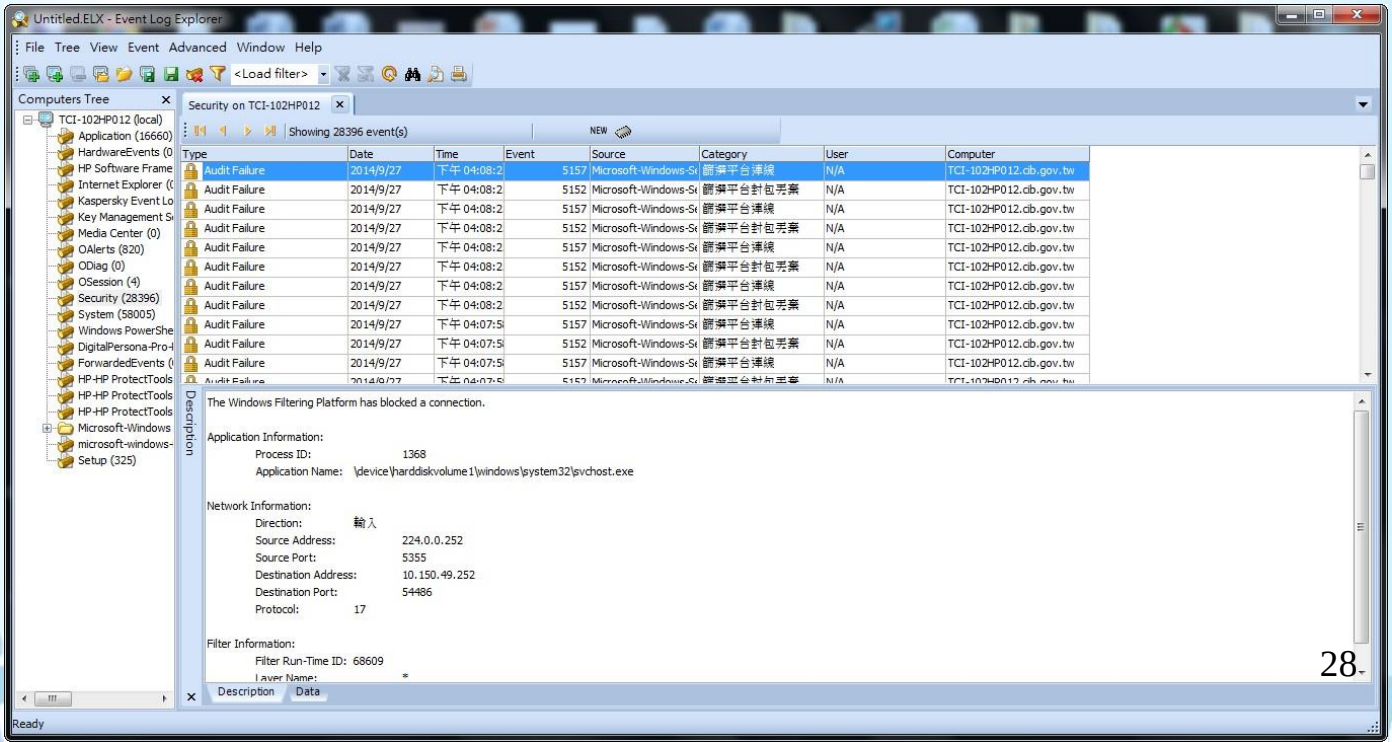
- 電腦>管理>系統工具>Windows記錄
- 應用程式(application)-主要記錄系統安裝的程式(惡意程式活動記錄)
- 系統(system)-系統活動記錄(是否有惡意程式服務)

★安全性(security)-系統本身登入/出資料(異常登入)。



# 本機日誌檔

- 推薦軟體「Event Log Explorer」
- 專門開啟event log的軟體，易用



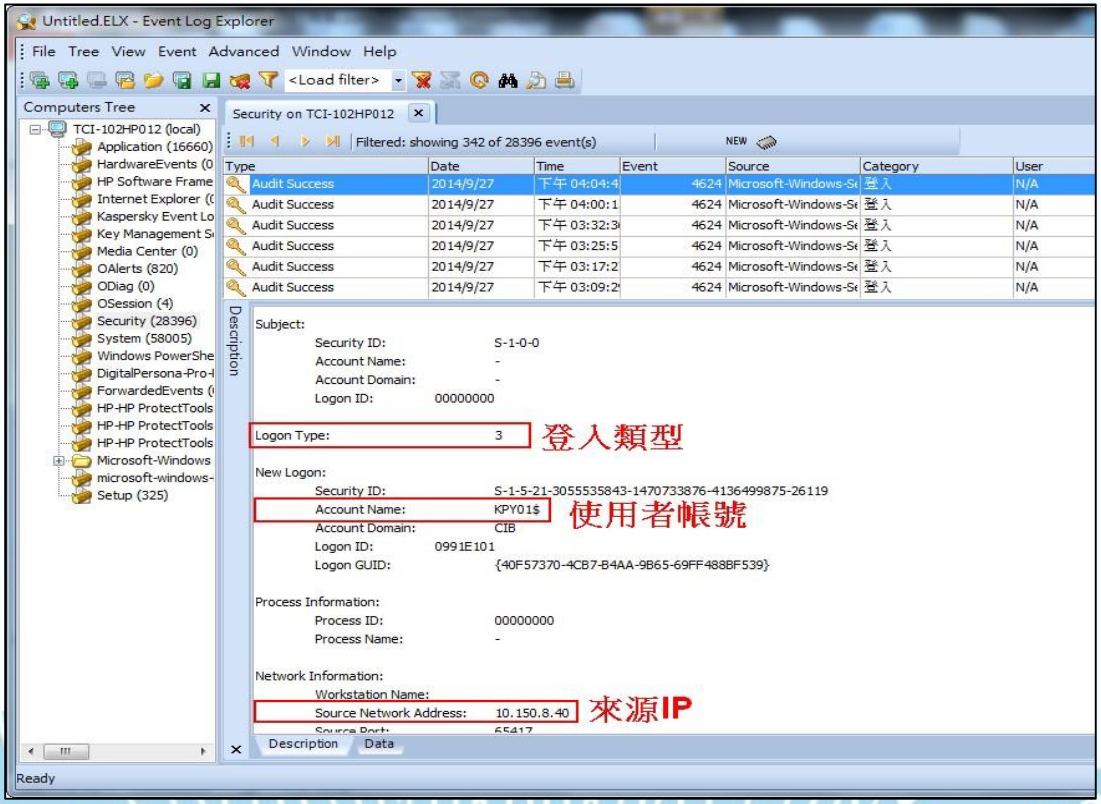
# 本機日誌檔

- security log
- windows的安全稽核記錄，可以查看登入的情況

| 事件代碼 (XP、server 2003) | 事件代碼 (w7、server 2008) | 事件說明 |
|---|---|---|
| 529、530、531、532、533、534、535、536、537、539 | 4625 | 登入失敗 |
| 528、540 | 4624 | 登入成功 |
| 538、551 | 4638、4647 | 登入成功 |

# 本機日誌檔

- security log
- 登入成功記錄分析



# 本機日誌檔

- security log
- 登入類型:使用者登入方式

| 登入類型 | 登入標題 | 描述 |
|---|---|---|
| 2 | 互動 | 使用者已登入這部電腦 |
| 3 | 網路 | 使用者或電腦從網路登入這部電腦 |
| 4 | 批次 | 批次登入類型是批次伺服器所使用，其中程序可代表使用者執行，而無須使用者的直接登入 |
| 5 | 服務 | 服務已由「服務控制管理員」啟動 |
| 7 | 解除鎖定 | 此工作站已解除鎖定 |
| 8 | NetworkCleartext | 使用者從網路登入這部電腦。使用者的密碼以非雜湊格式傳遞給驗證封裝。內建的驗證在傳送所有雜湊認證通過網路之前會先進行封裝 |
| 9 | NewCredentials | 呼叫者複製其目前的權杖，並指定輸出連線的新認證。新的登入工作階段擁有相同的本機識別。但對其他網路連線使用不同的認證 |
| 10 | RemoteInteractive | 使用者使用「終端機服務」或「遠端桌面」從遠端登入這部電腦 |
| 11 | CachedInteractive | 使用者使用存放在本機電腦上的網路認證登入這部電腦。未聯絡網域控制站以確認認證。 |

# 本機日誌檔

- security log
- 帳戶名稱:登入的使用者名稱，需檢查是否為經授權的合法使用者。
- 來源網路位址:若是遠端登入則會記錄登入者的來源IP，可利用此IP查實際登入來源。
- 來源工作站:在某部分網路環境中，使用者的IP並不固定，若無法使用IP判斷哪台電腦，則可利用來源工作站判斷。

# 本機日誌檔

- security log
- 其他重要的事件

| 事件代碼<br>(XP、server 2003) | 事件代碼<br>(w7、server 2008) | 事件說明 |
|---|---|---|
| 624、625、626、627、628、629、630、642、644 | 4720、4722、4723、4724、4725、4726、4738、4740 | 使用者帳號改變 |
| 631至641、643、645至666 | 4727至4737、4739至4762 | 使用者群組改變 |
| 612 | 4719 | 稽核政策改變 |

# 本機日誌檔

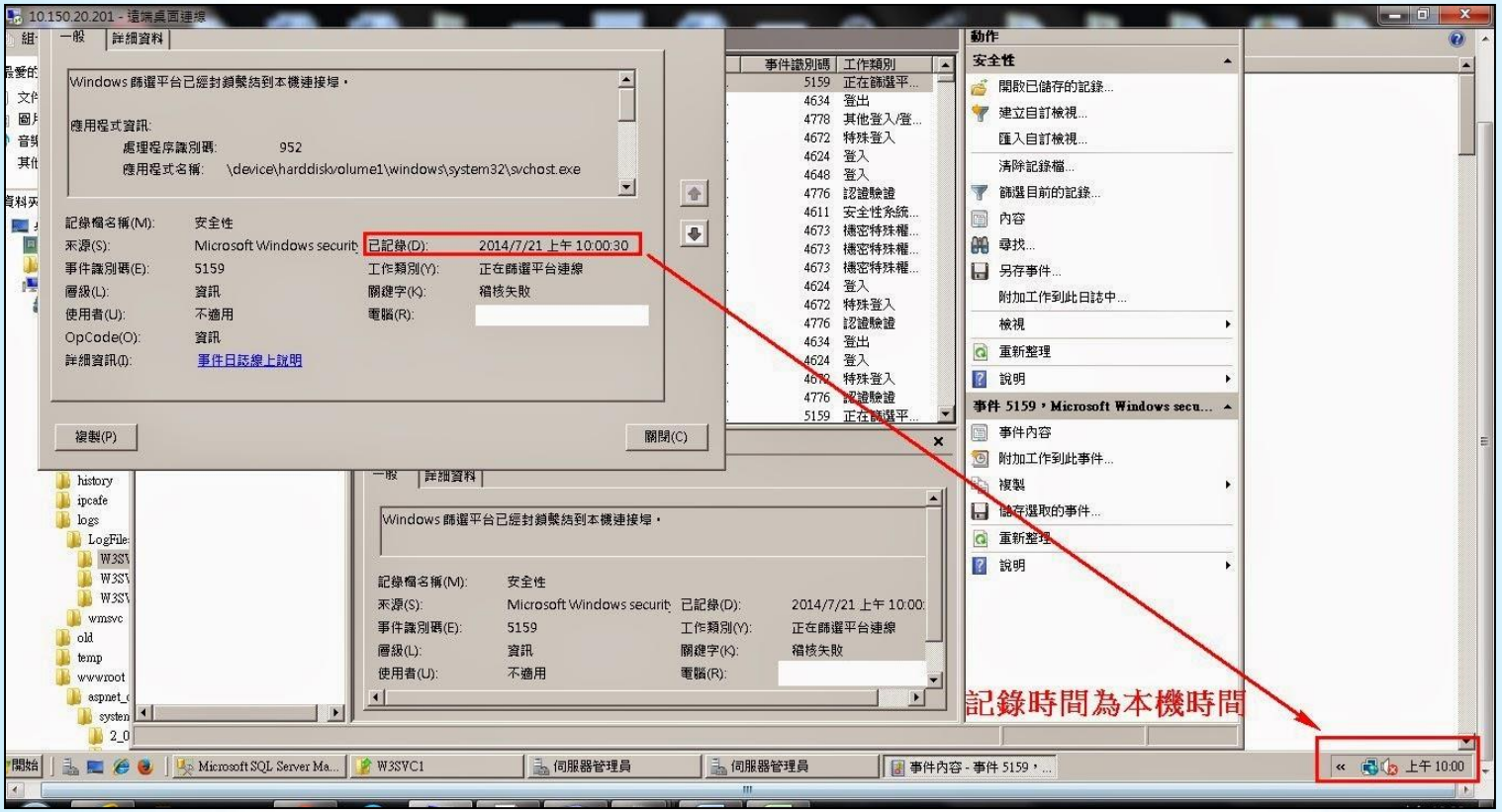
- security log
- 稽核原則改變
- +表示會記錄登入/登出的事件
- -表示不記錄登入/登出的事件

| 成功 | 失敗 | |
|---|---|---|
| + | – | 登入/登出 |
| – | – | 物件存取 |
| – | – | 特權使用 |
| + | – | 帳戶管理 |
| – | – | 原則變更 |
| – | – | 系統 |
| – | – | 詳細追蹤 |
| – | – | 目錄服務存取 |
| + | – | 帳戶登入 |

# event log時間區分

- 在event log上，主要紀錄伺服器的安全、登入事件、更新等情況，其中最重要的時間點紀錄方式
- 為抓取伺服器的時間，若伺服器的時間設定為何，則event log紀錄的時間就是伺服器設定的時間。

# event log時間區分

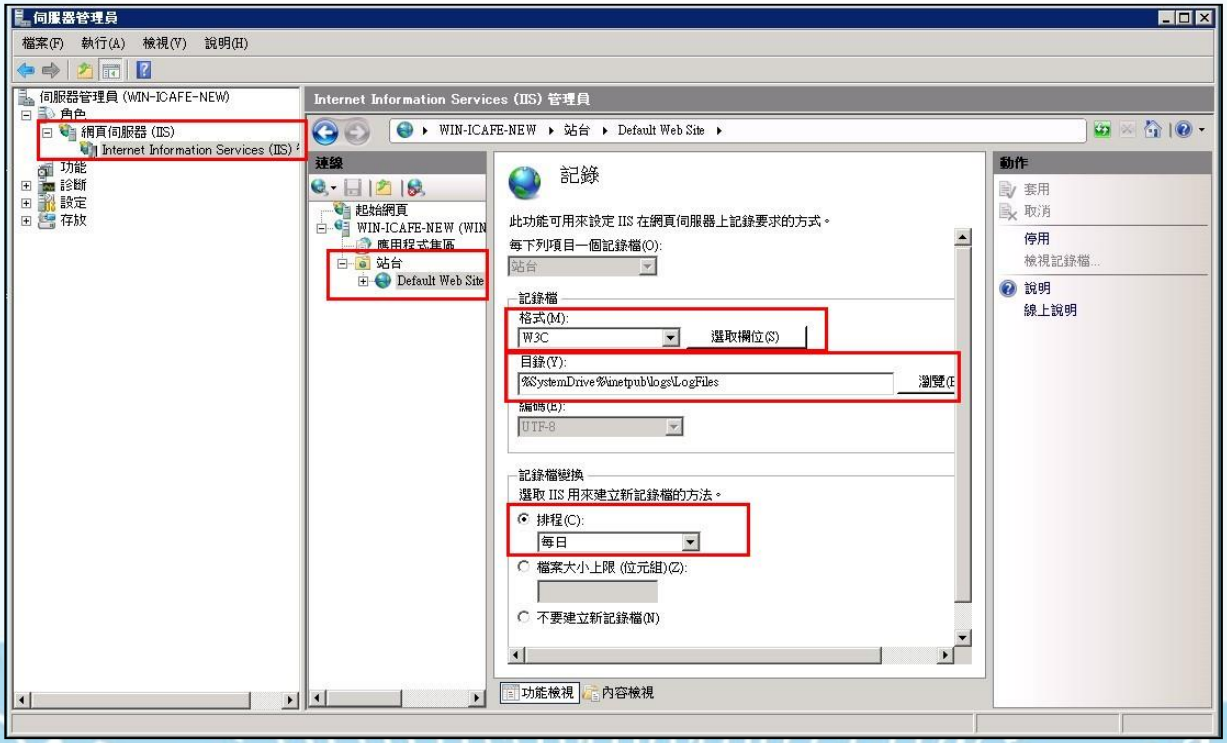


# 伺服器日誌檔

- 又稱為web log
- 網站伺服器會將所有的Web連線請求記錄在log中
- 常見的伺服器作業系統類型有windows和linux類型
- 因此web依據作業系統類型不同，分為IIS log格式和NCSA log格式

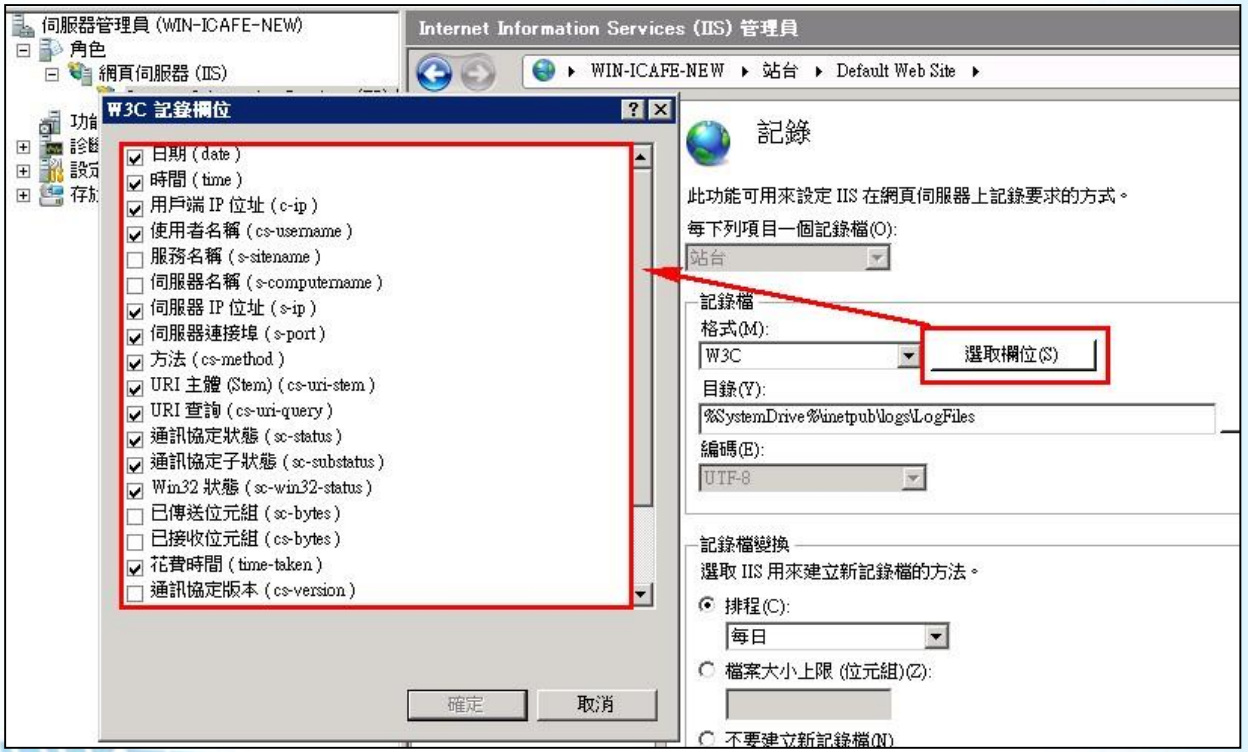
# windows server 2008

- log存放路徑:
- 角色＞網頁伺服器(iis)＞站台＞default web site＞紀錄



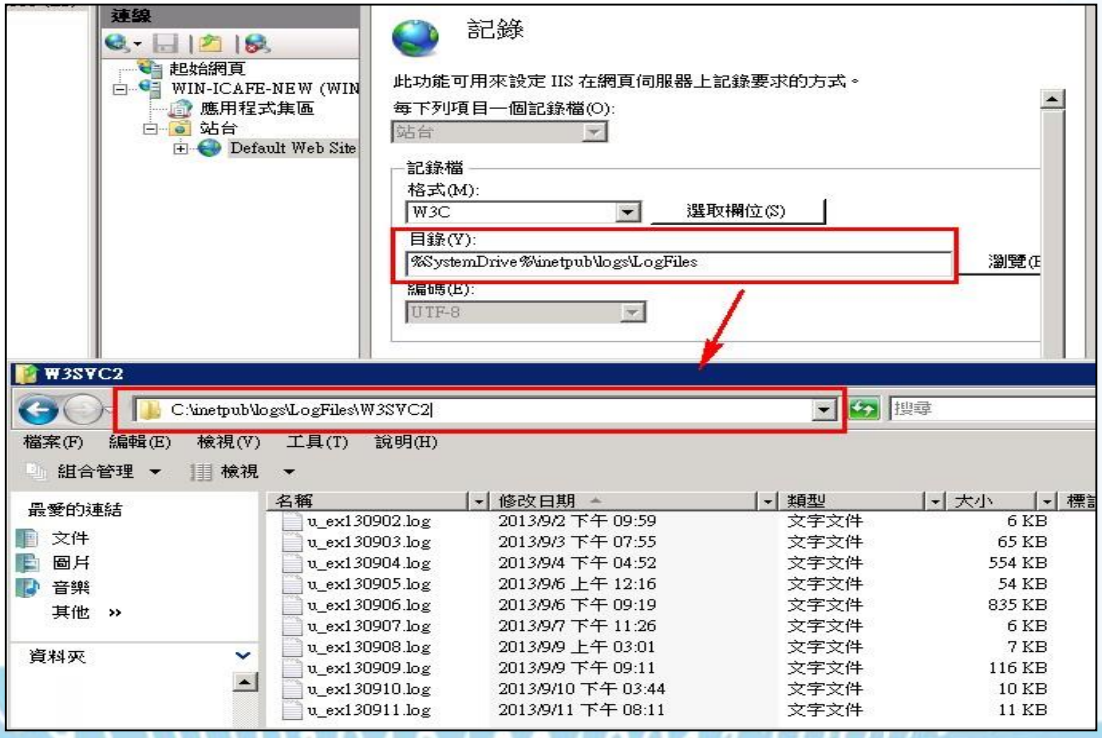
# windows server 2008

- log記錄的欄位資訊



# windows server 2008

- log存放路徑資料夾
- C:\inetpub\logs\LogFiles



# linux相關log路徑與解說

- /var/log/secure：記錄登入系統存取資料的檔案，例如 pop3, ssh, telnet, ftp 等都會記錄在此檔案中；
- /var/log/wtmp：記錄登入者的訊息資料，由於本檔案已經被編碼過，所以必須使用 last 這個指令來取出檔案的內容；
- /var/log/messages：這個檔案相當的重要，幾乎系統發生的錯誤訊息（或者是重要的資訊）都會記錄在這個檔案中；
- /var/log/boot.log：記錄開機或者是一些服務啟動的時候，所顯示的啟動或關閉訊息；
- /var/log/maillog 或 /var/log/mail/*：紀錄郵件存取或往來( sendmail 與 pop3 )的使用者記錄；
- /var/log/cron：這個是用來記錄 crontab 這個例行性服務的內容的！
- /var/log/httpd, /var/log/news, /var/log/mysqld.log, /var/log/samba, /var/log/procmail.log： 分別是幾個不同的網路服務的記錄檔啦！

# Web log格式

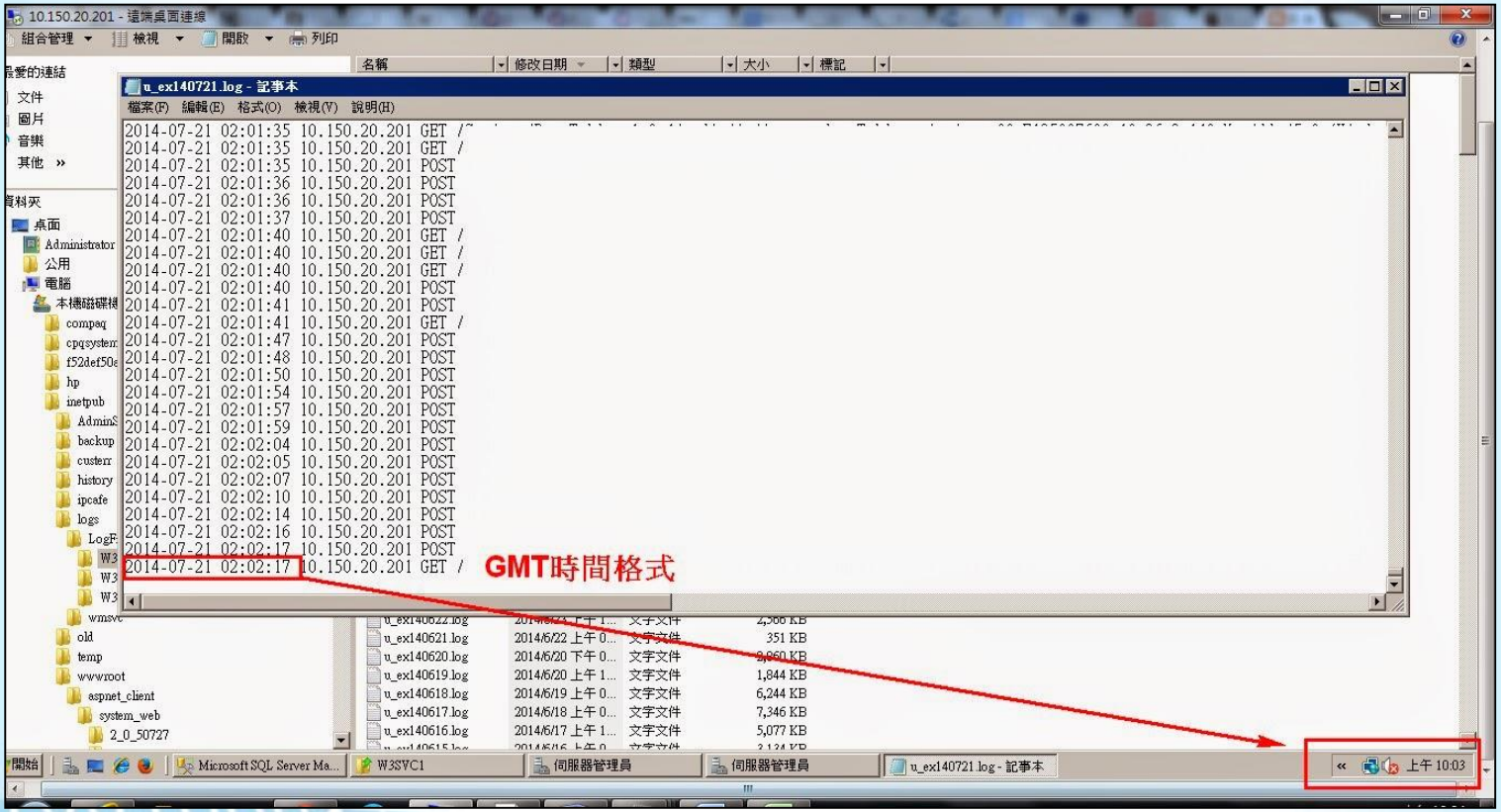
- Windows log格式與Linux log格式，記錄方式大同小異。
- IIS log-日期時間在前、IP在後
- NCSA log-IP記錄在前、日期時間在後

# web log時間區分(windows)

- 在web log上，主要是紀錄網站瀏覽的行為或網站的任何事件。其紀錄檔案放置在IIS的設定路徑下，時間紀錄的格式為GMT。若要還原為台灣時間，則需+8小時，變成GMT+8

# web log時間區分(windows)

換算成台灣時間需+8小時(GMT+8)



# 常見HTTP指令

| HTTP指令 | 解說 |
| --- | --- |
| GET | 存取網頁資源 |
| POST | 傳送用戶端資料到指定網頁 |
| HEAD | 測試主機是否提供某些網頁資源 |
| OPTIONS | 測試某些網頁指令是否能被執行 |
| TRACE | 測試HTTP指令傳送迴圈是否正常 |
| CONNECT | 進行安全HTTP連接資訊的指令 |
| PUT | 上傳資料到網站 |
| DELETE | 刪除網站中的檔案 |

# 常見HTTP伺服器回應代碼

- 1XX:一般資訊說明

  100:繼續通訊

  101:切換協定
- 2XX:指令執行成功

  200:指令執行完成

  201:新資料檔案建立完成

  202:指令已接受

# 常見HTTP伺服器回應代碼

- 3XX:需求忽略或通訊轉向

  301(302):通訊轉向

  304:網頁自上次瀏覽後未經修改
- 4XX:用戶端指令內容錯誤(client error)

  403:伺服器拒絕請求(Forbidden)

  404:伺服器找不到網頁

  408:伺服器逾時

# 常見HTTP伺服器回應代碼

- 5XX:主機端指令執行錯誤(server error)

  500:網站內部錯誤

  501:未提供的功能

  502:錯誤的閘道中繼主機

  503:無法使用此網路服務

  504:閘道中繼主機逾時

# Log Parser Lizard

- 由國外廠商開發，以微軟開發log parser的log分析工具為核心，並改良成視覺化軟體。。
- 免費版(無法匯出整理好的資料)
- 使用SQL語法進行Log資料篩選

安裝順序

- .Net 4.0
- Log Parser
- Log Parser Lizard

# Log Parser Lizard 安裝

| 安裝順序 | 安裝程式名稱 | 說明 | 備註 |
|---|---|---|---|
| 1 | Microsoft .NET Framework 4 | NET Framework4.0 以上的環境 | . NET環境 |
| | 下載點:http://www.microsoft.com/zh-TW/download/details.aspx?id=17718 | | |
| 2 | LogParser.msi | Log Parser 安裝 | LogParser核心程式 |
| | 下載點: http://www.microsoft.com/en-us/download/details.aspx?id=24659 | | |
| 3 | owc10.exe | 匯出圖表時需用到 | 非必要安裝 |
| | 下載點:http://www.microsoft.com/zh-tw/download/details.aspx?id=9468 | | |
| 4 | LogParserLizardSetup.msi | Log Parser Lizard 安裝 | 將LogParser圖形化介面 |
| | 下載點:http://www.lizard-labs.net/log_parser_lizard.aspx | | |

# 建議安裝3.5.0的版本

www.lizard-labs.net/log_parser_lizard.aspx

1 2 3 4 5 Share

## Log Parser Lizard GUI - FREE Query Software

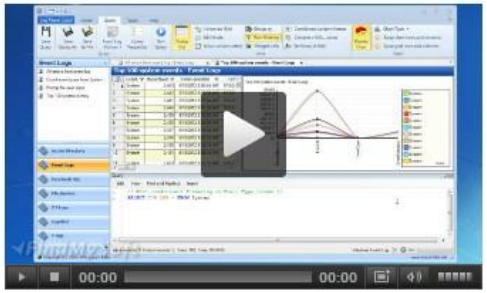
Log Parser is wonderful because it effectively lets you run **SQL** queries against text files:

*SELECT DISTINCT src-ip FROM pfirewall.log WHERE action='DROP'*

*SELECT cs-uri-stem FROM c:|InetPub|Logs|ex*.log*
*GROUP BY cs-uri-stem HAVING COUNT(*) > 50*

*SELECT to_lowercase(extract_extension(cs-uri-stem)) AS PageType, SUM(sc-bytes)*
*FROM ex131118.log, ex131119.log GROUP BY PageType*

### Short Introduction to Log Parser Lizard




**Log Parser Lizard** is a **GUI** for Microsoft Logparser, definitely the best one available on the market today. Log Parser is a very powerful and versatile query software tool that provides **universal query access (using SQL)** to text-based data, such as **log files**, **XML** files, and **TSV/CSV text files**, as well as key data sources on the Microsoft Windows operating system, such as the **Windows Event Log**, **IIS log**, the **registry**, the **File System**, the **Active Directory** services and much more.

**Microsoft Logparser is an enhanced query software that digs through information in log**

- Download Log Parser Lizard for FREE
- Version history and feature list
- Tutorials for Log Parser Lizard GUI
- BUY NOW the Full Version of Log Parser Lizard
- Download previous version of Log Parser Lizard 3.5

下載該版本

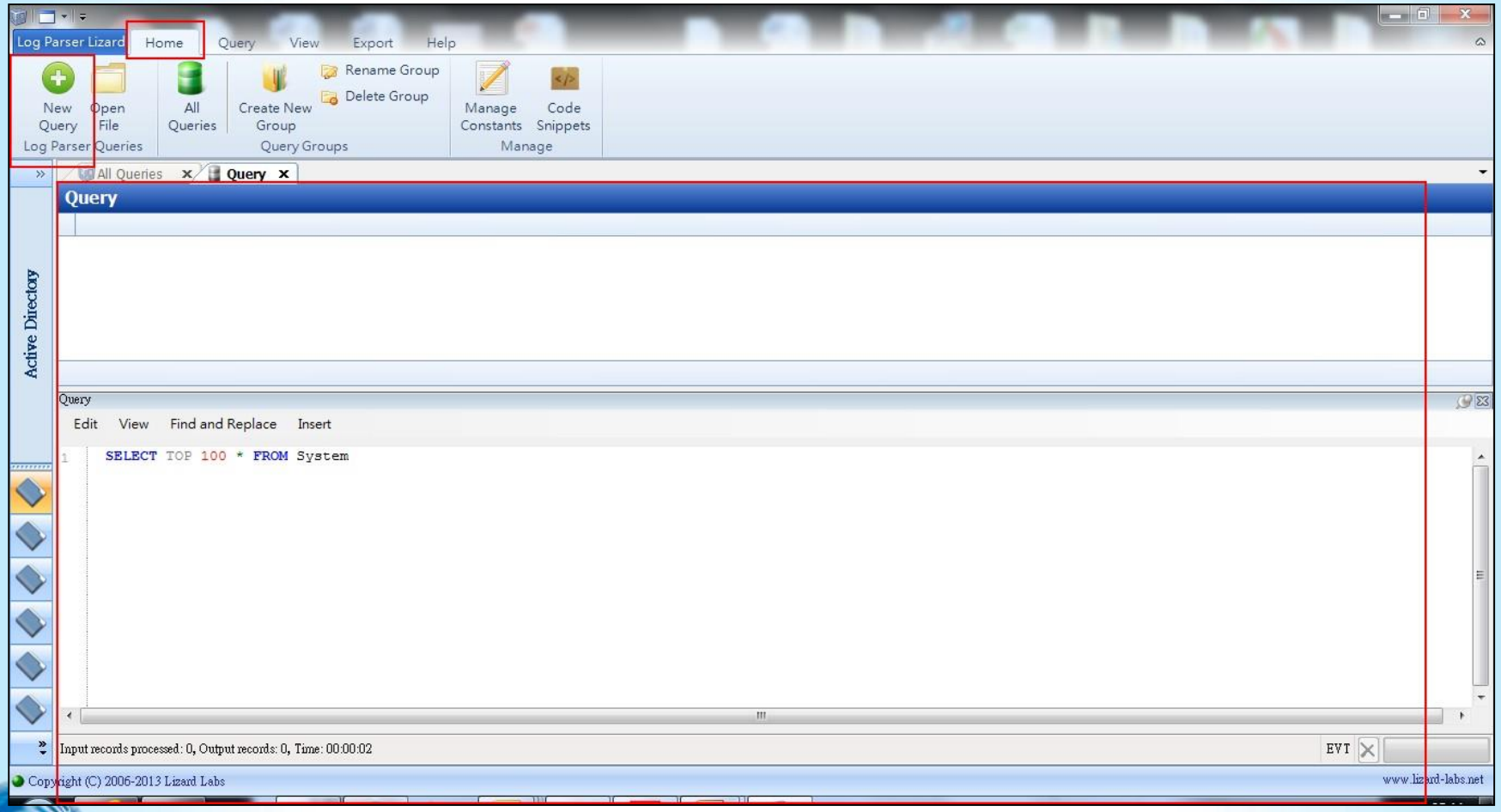
### RECENT AWARDS

Log Parser Lizard has been reviewed by software.informer.com editors and got "Editor's Pick Award"

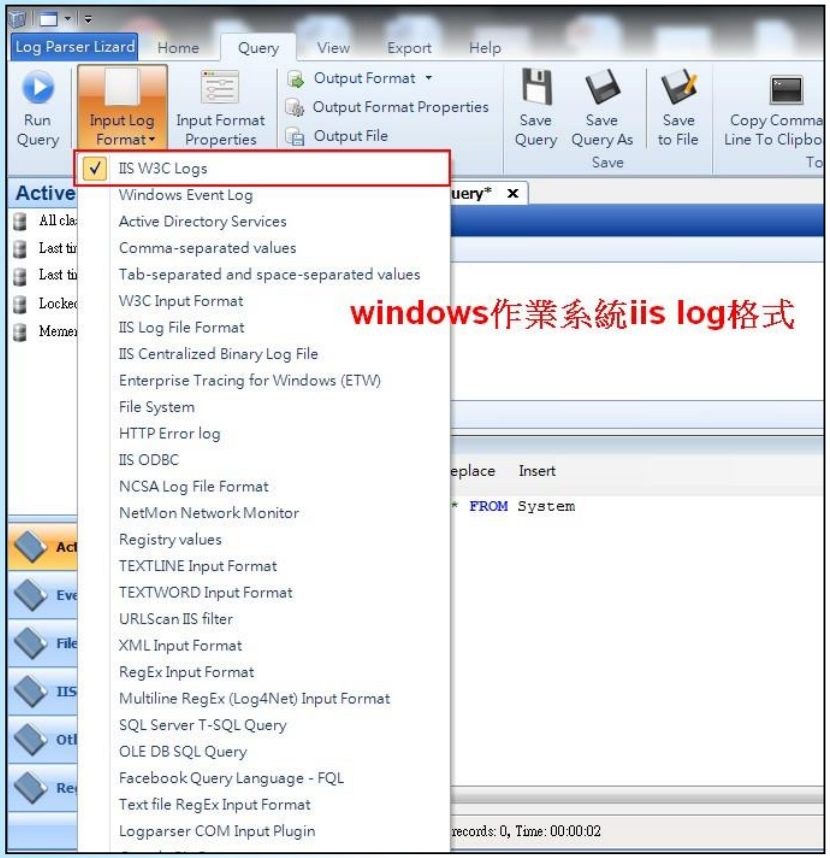
Editor's pick award
software.informer

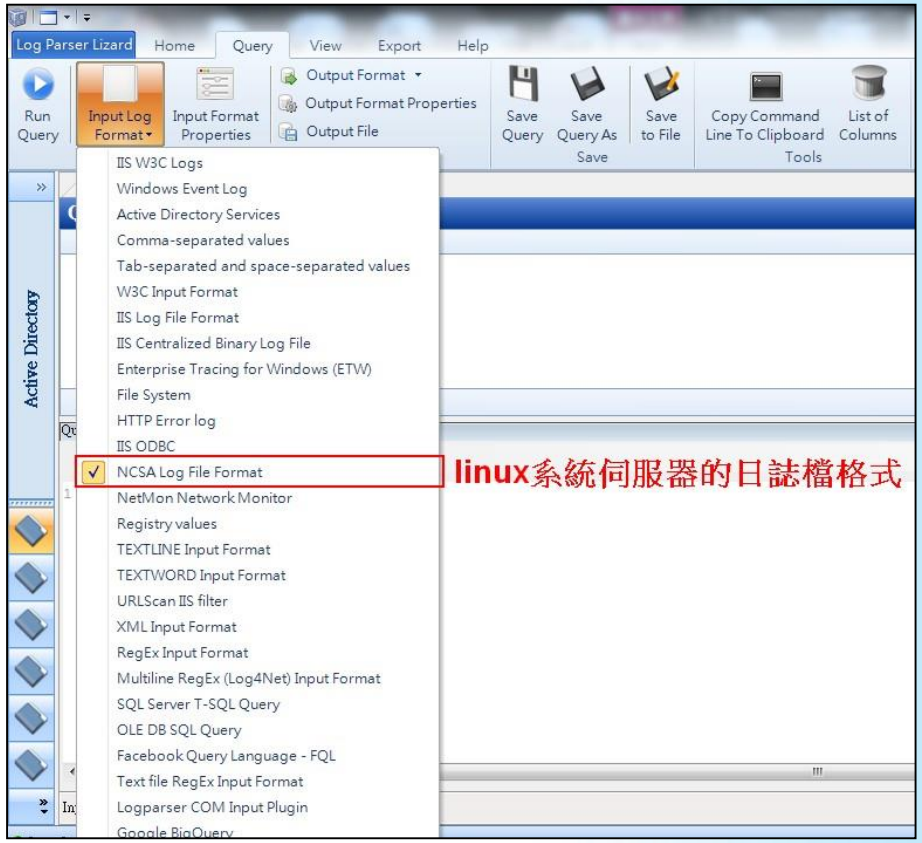
Log Parser Lizard has been reviewed by Frederick Barton on 20 Jun 2012. Based on the user interface, features and complexity, Findmysoft has rated Log Parser Lizard 5 out

# 新增一個查詢(home>new query)



# 選擇log格式

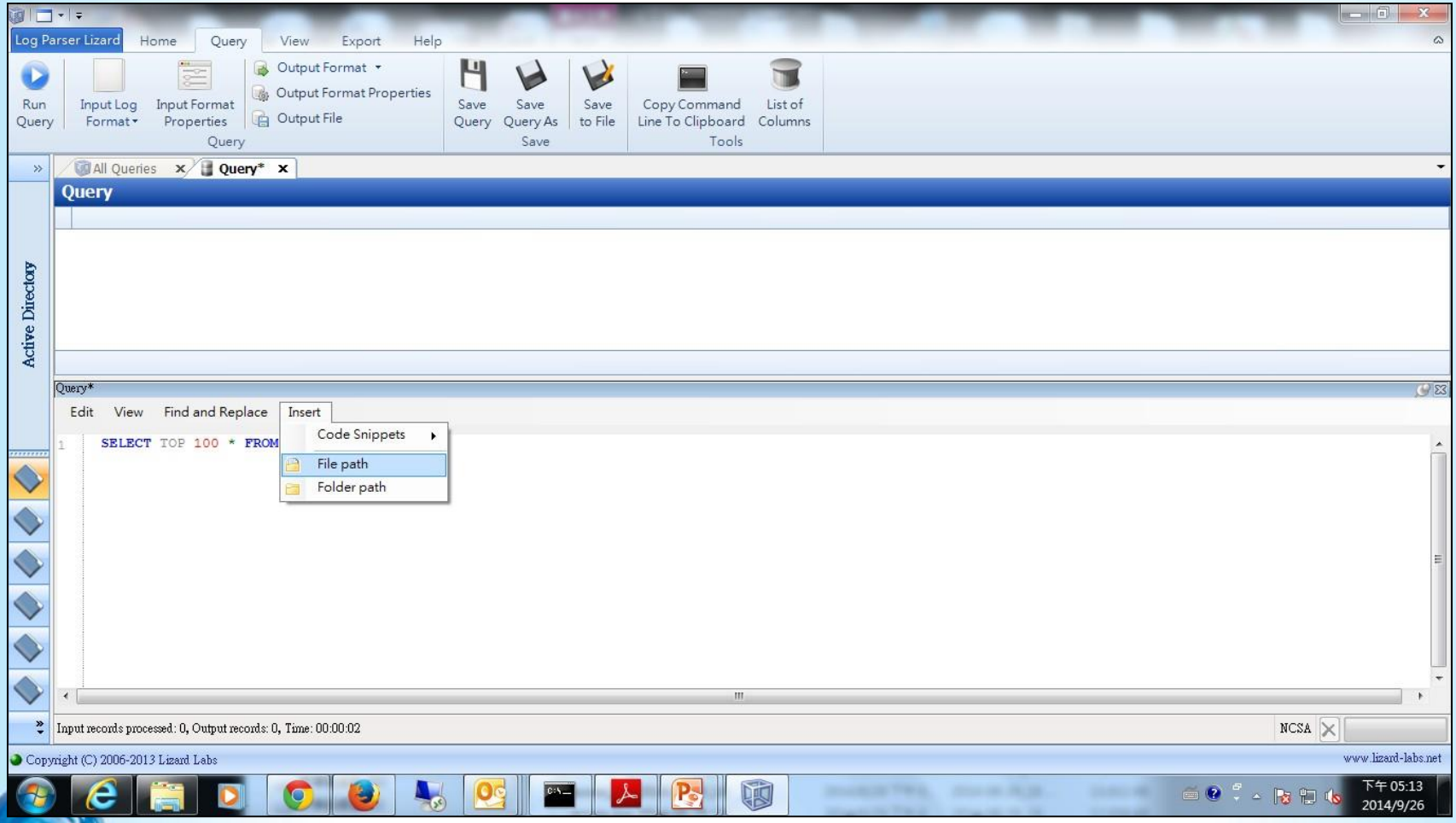


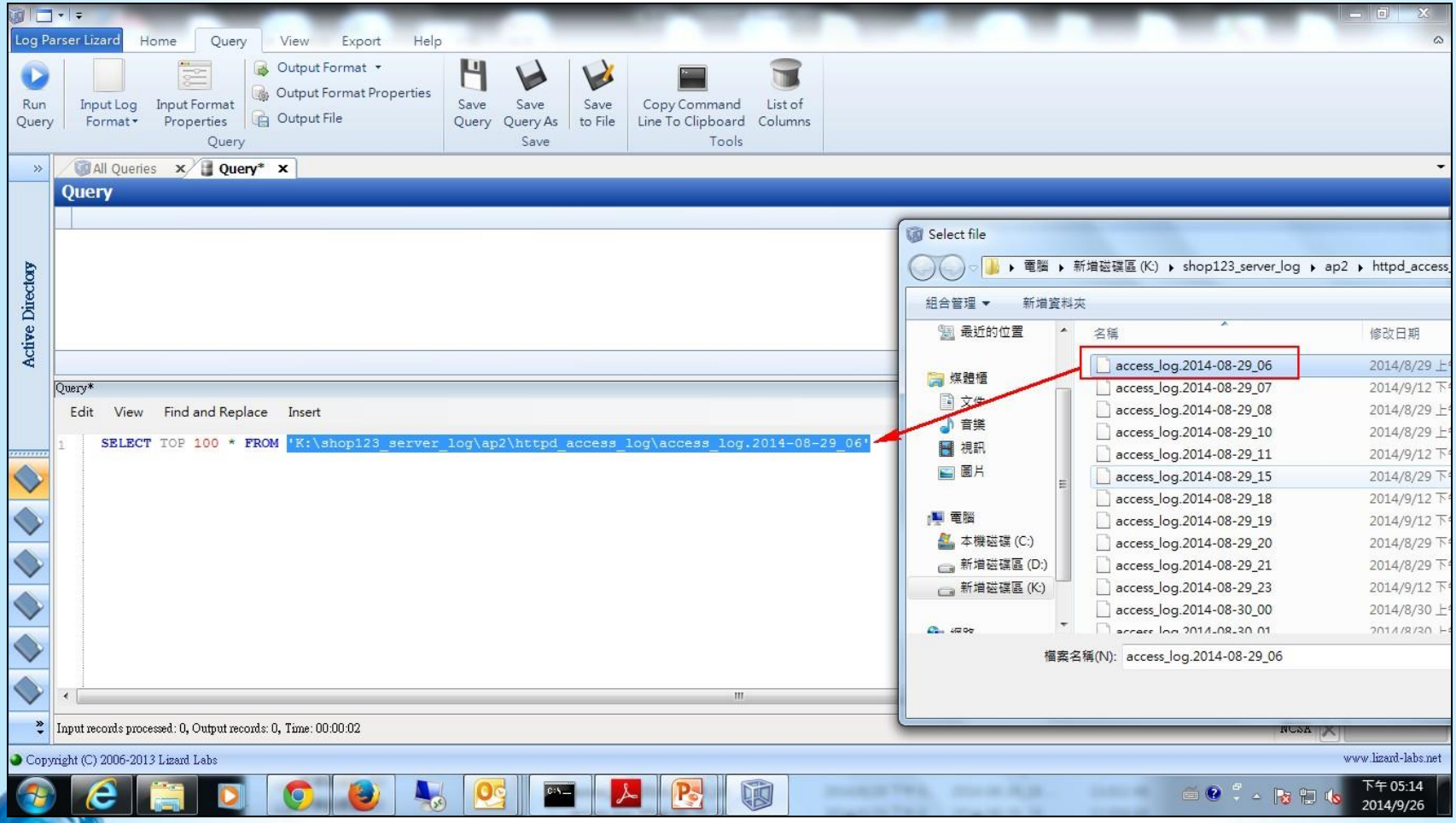

windows的iis格式

linux的ncsa格式

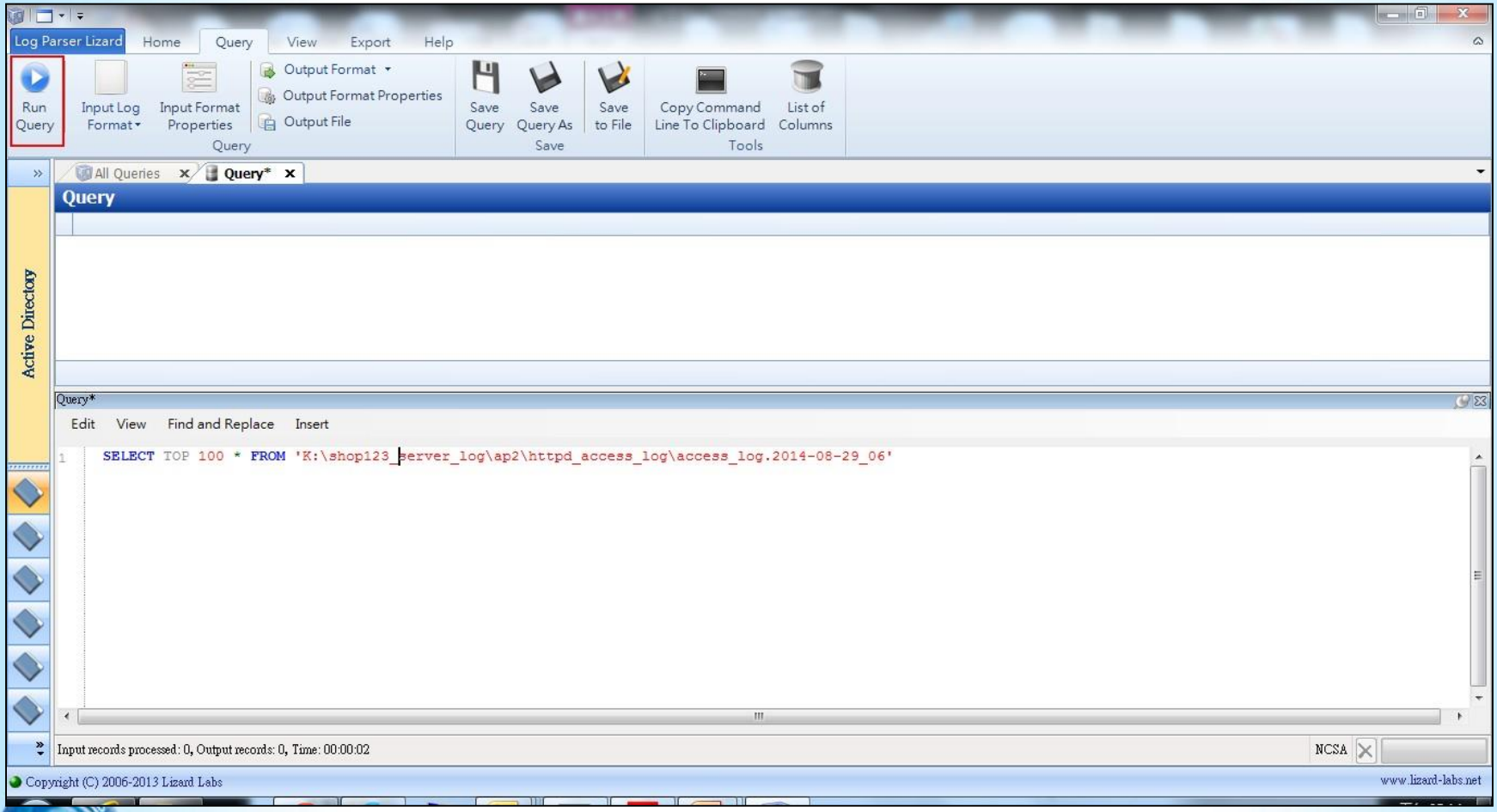
# 選擇log路徑(insert>file path)



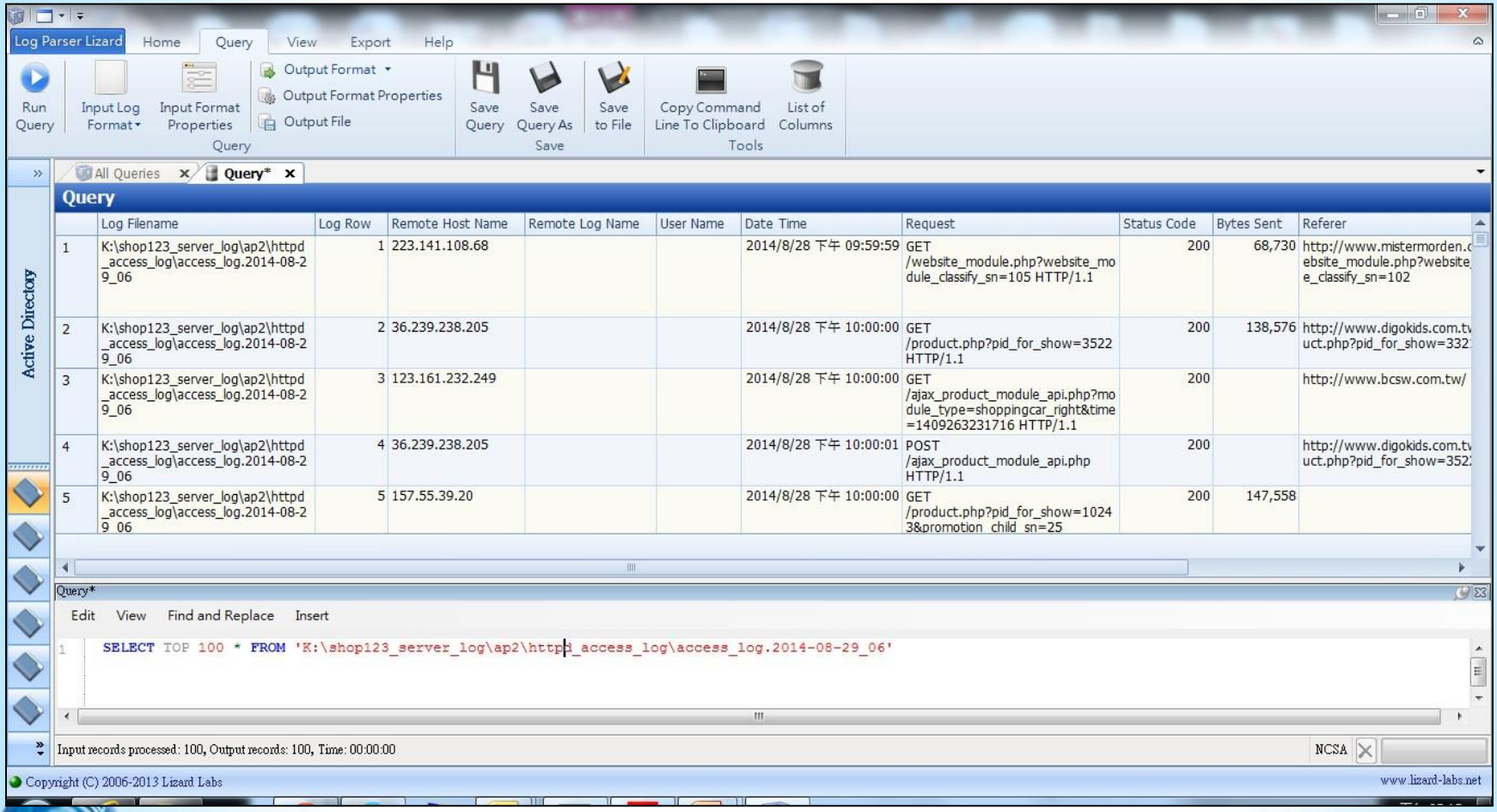
# 找到log檔案的位置


Log Parser Lizard
Home
Query
View
Export
Help
Run Query
Input Log Format
Input Format Properties
Output Format
Output Format Properties
Output File
Query
Save Query
Save Query As
Save to File
Save
Copy Command Line To Clipboard
List of Columns
Tools
All Queries
Query*
Query
Active Directory
Query*
Edit
View
Find and Replace
Insert
SELECT TOP 100 * FROM 'K:\shop123_server_log\ap2\httpd_access_log\access_log.2014-08-29_06'
Input records processed: 0, Output records: 0, Time: 00:00:02
Copyright (C) 2006-2013 Lizard Labs
www.lizard-labs.net
Select file
電腦 ▸ 新增磁碟區 (K:) ▸ shop123_server_log ▸ ap2 ▸ httpd_access_
組合管理
新增資料夾
最近的位置
媒體櫃
文件
音樂
視訊
圖片
電腦
本機磁碟 (C:)
新增磁碟區 (D:)
新增磁碟區 (K:)
名稱
修改日期
access_log.2014-08-29_06
access_log.2014-08-29_07
access_log.2014-08-29_08
access_log.2014-08-29_10
access_log.2014-08-29_11
access_log.2014-08-29_15
access_log.2014-08-29_18
access_log.2014-08-29_19
access_log.2014-08-29_20
access_log.2014-08-29_21
access_log.2014-08-29_23
access_log.2014-08-30_00
檔案名稱(N): access_log.2014-08-29_06
下午 05:14
2014/9/26

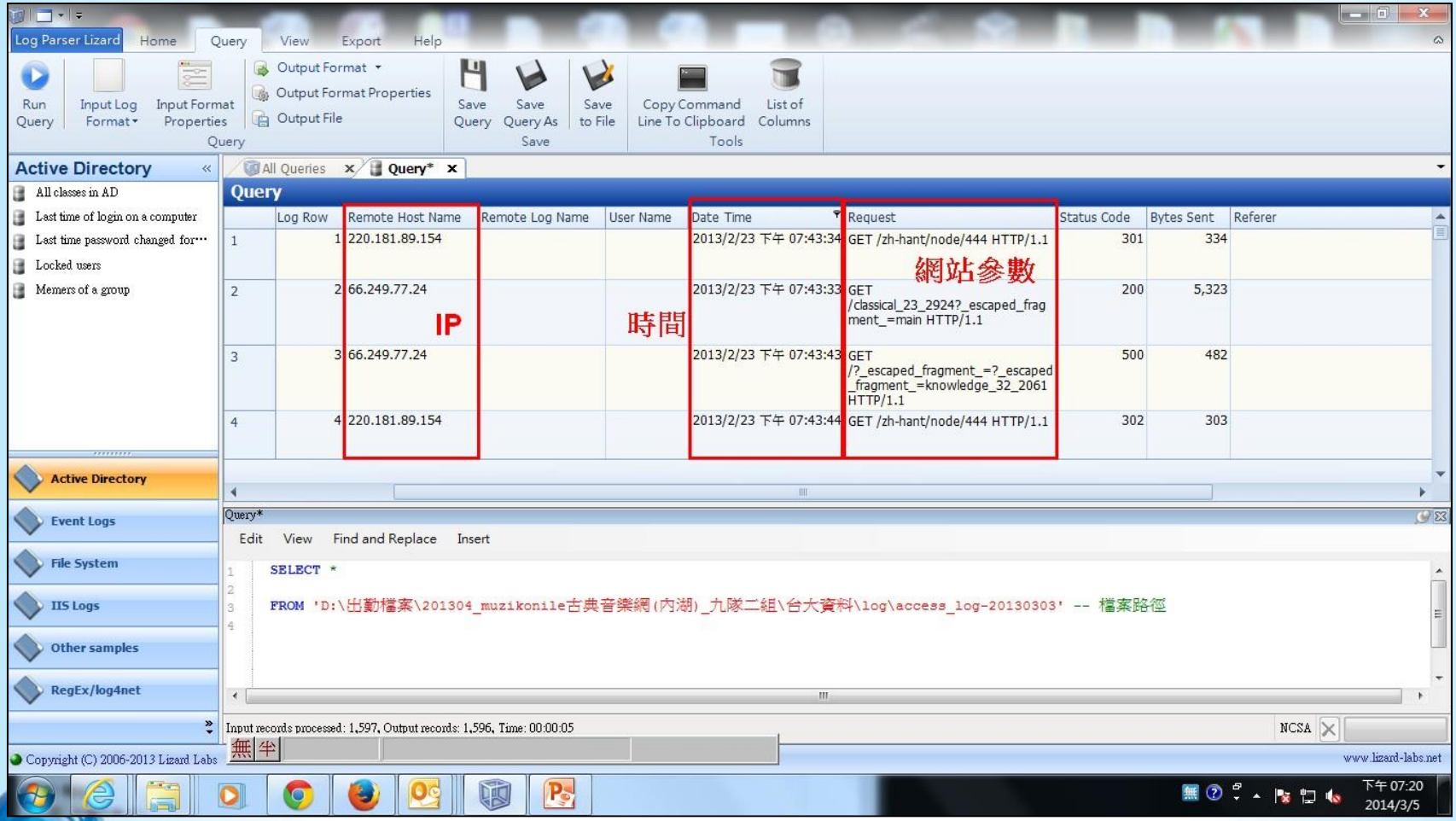
# 選擇前100筆測試，點選run query



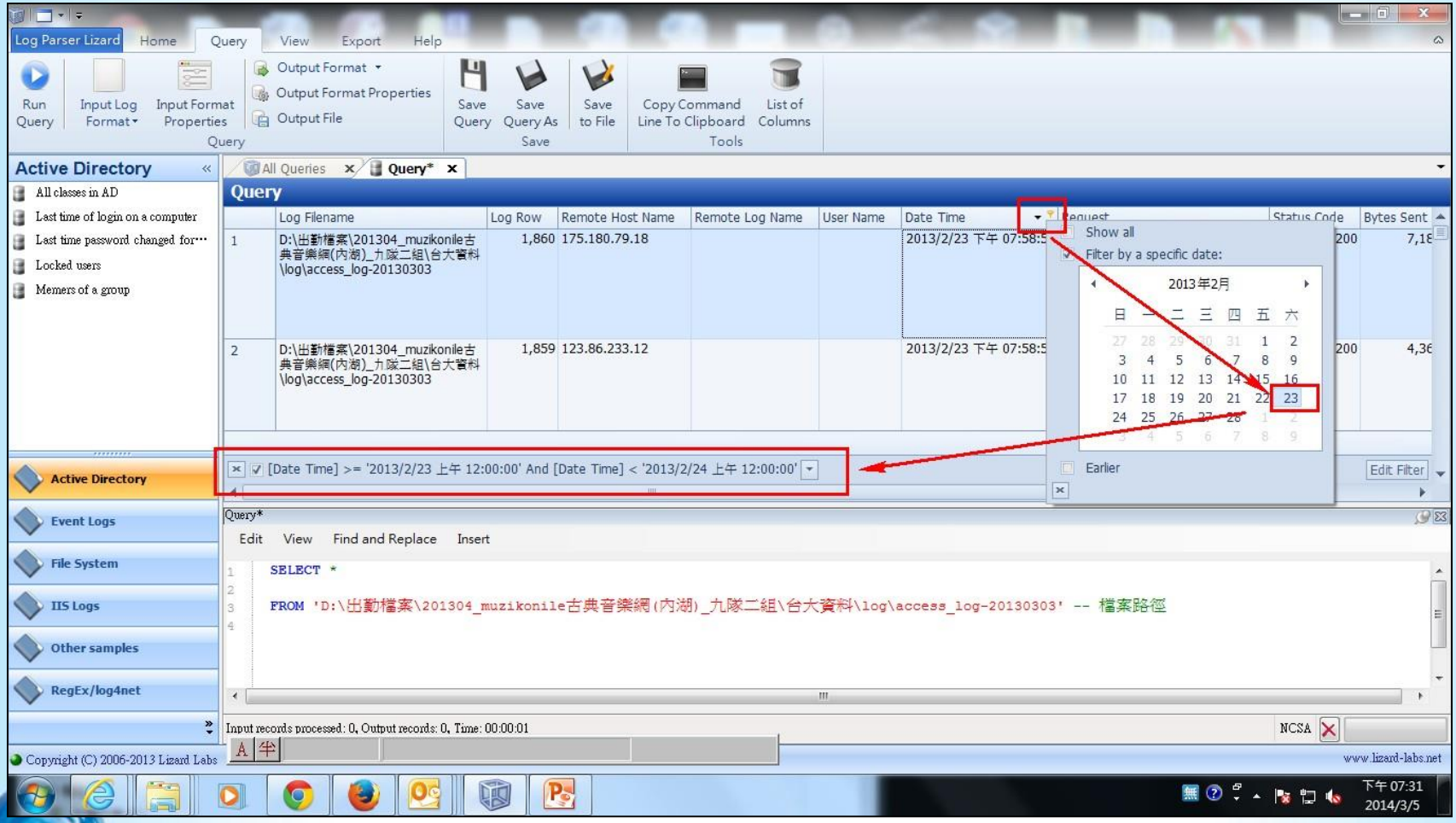
# 測試成功，前100筆資料



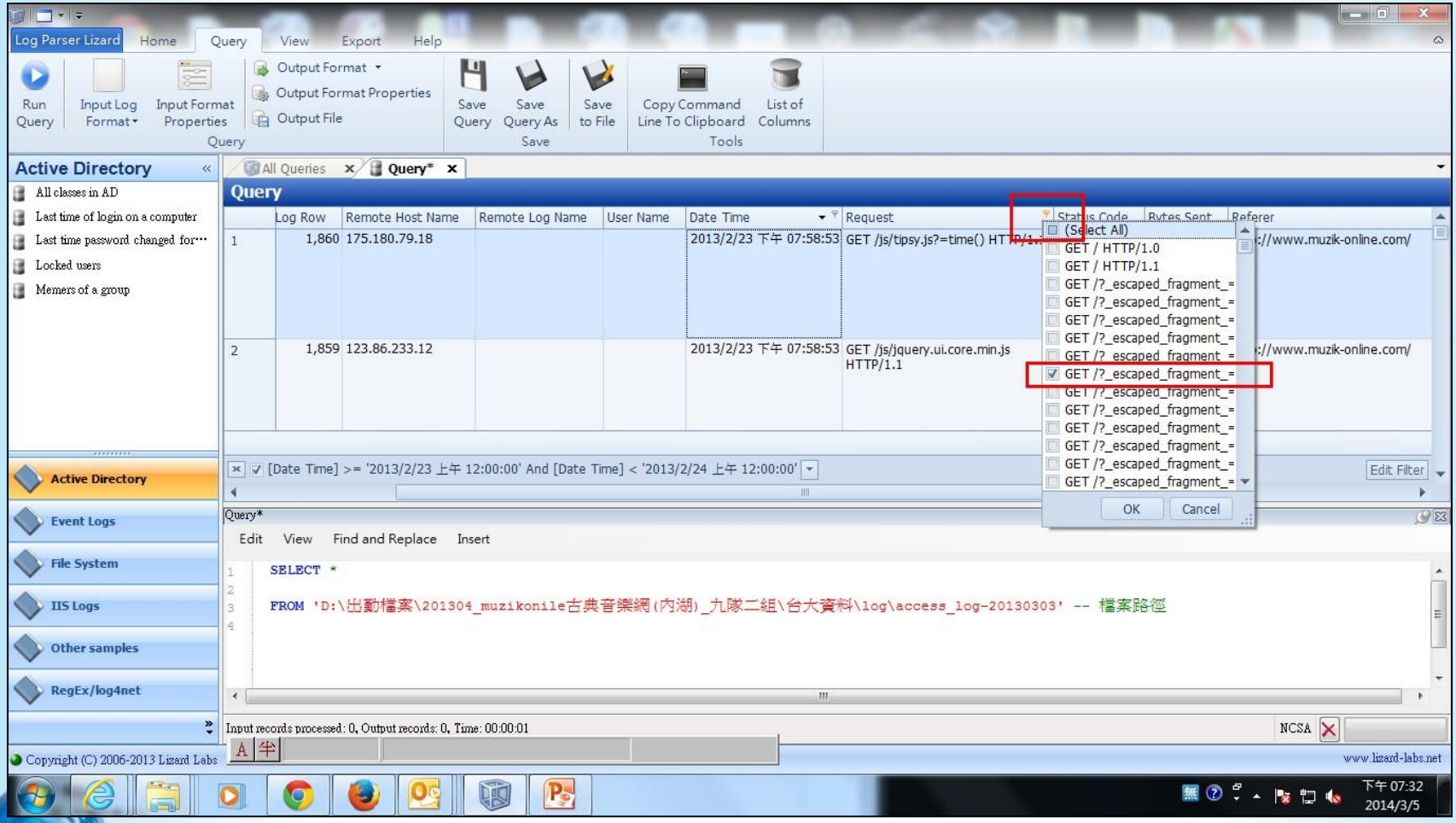
# 基本操作


Log Parser Lizard
Home
Query
View
Export
Help
Run Query
Input Log Format
Input Format Properties
Output Format
Output Format Properties
Output File
Query
Save Query
Save Query As
Save to File
Save
Copy Command Line To Clipboard
List of Columns
Tools
Active Directory
All classes in AD
Last time of login on a computer
Last time password changed for…
Locked users
Members of a group
All Queries
Query*
Query
Log Row
Remote Host Name
Remote Log Name
User Name
Date Time
Request
Status Code
Bytes Sent
Referer
1 1 220.181.89.154 2013/2/23 下午 07:43:34 GET /zh-hant/node/444 HTTP/1.1 301 334
2 2 66.249.77.24 2013/2/23 下午 07:43:33 GET /classical_23_2924?_escaped_fragment_=main HTTP/1.1 200 5,323
3 3 66.249.77.24 2013/2/23 下午 07:43:43 GET /?_escaped_fragment_=?_escaped_fragment_=knowledge_32_2061 HTTP/1.1 500 482
4 4 220.181.89.154 2013/2/23 下午 07:43:44 GET /zh-hant/node/444 HTTP/1.1 302 303
IP
時間
網站參數
Active Directory
Event Logs
File System
IIS Logs
Other samples
RegEx/log4net
Query*
Edit
View
Find and Replace
Insert
SELECT *
FROM 'D:\出勤檔案\201304_muzikonile古典音樂網(內湖)_九隊二組\台大資料\log\access_log-20130303' -- 檔案路徑
Input records processed: 1,597, Output records: 1,596, Time: 00:00:05
NCSA
Copyright (C) 2006-2013 Lizard Labs
www.lizard-labs.net
下午 07:20
2014/3/5

# 基本操作(快速找出日期)


Log Parser Lizard
Home
Query
View
Export
Help
Run Query
Input Log Format
Input Format Properties
Output Format
Output Format Properties
Output File
Save Query
Save Query As
Save to File
Copy Command Line To Clipboard
List of Columns
Active Directory
All classes in AD
Last time of login on a computer
Last time password changed for…
Locked users
Members of a group
All Queries
Query*
Log Filename
Log Row
Remote Host Name
Remote Log Name
User Name
Date Time
Request
Status Code
Bytes Sent
1
D:\出勤檔案\201304_muzikonile古典音樂網(內湖)_九隊二組\台大資料\log\access_log-20130303
1,860
175.180.79.18
2013/2/23 下午 07:58:5
200
7,18
2
D:\出勤檔案\201304_muzikonile古典音樂網(內湖)_九隊二組\台大資料\log\access_log-20130303
1,859
123.86.233.12
2013/2/23 下午 07:58:5
200
4,36
Show all
Filter by a specific date:
2013年2月
日 一 二 三 四 五 六
Earlier
Edit Filter
[Date Time] >= '2013/2/23 上午 12:00:00' And [Date Time] < '2013/2/24 上午 12:00:00'
Active Directory
Event Logs
File System
IIS Logs
Other samples
RegEx/log4net
Query*
Edit
View
Find and Replace
Insert
SELECT *
FROM 'D:\出勤檔案\201304_muzikonile古典音樂網(內湖)_九隊二組\台大資料\log\access_log-20130303' -- 檔案路徑
Input records processed: 0, Output records: 0, Time: 00:00:01
NCSA
Copyright (C) 2006-2013 Lizard Labs
www.lizard-labs.net
下午 07:31
2014/3/5

# 基本操作(快速找出網頁參數)



# Log分析要領

- 確認網站受害類型
- 確認Log格式
- 確認案發時間與Log記錄時間

# 基本SQL語法

SELECT　欄位

FROM　　路徑

WHERE　條件

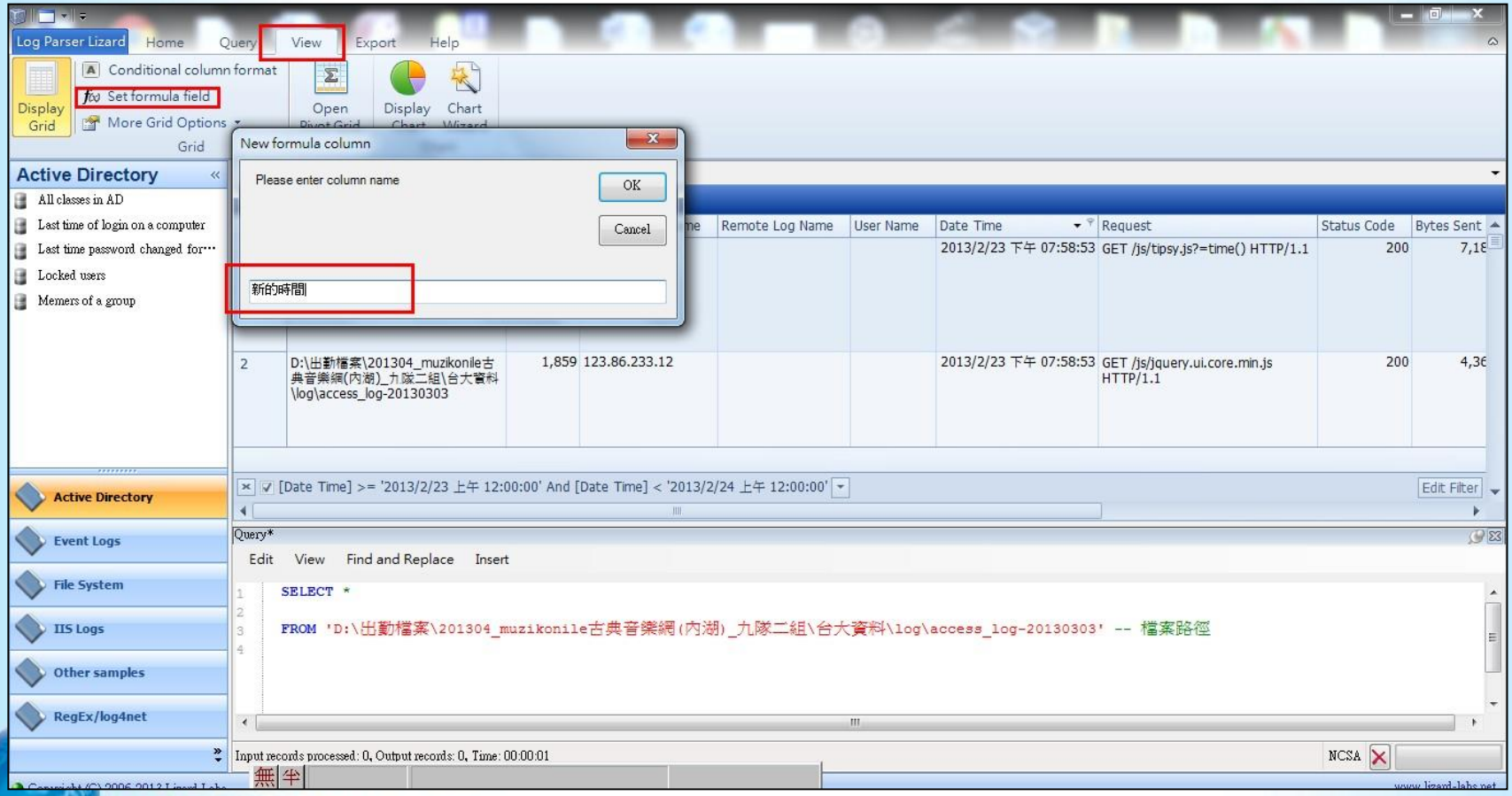
# Log Parser Lizard時間問題

- 使用Log Parser Lizard，不管是讀取IIS log 或 NCSA格式的log。一定都要再加+8小時才會正確。
- 因為IIS log是以GMT時間計算
- NCAS格式的log

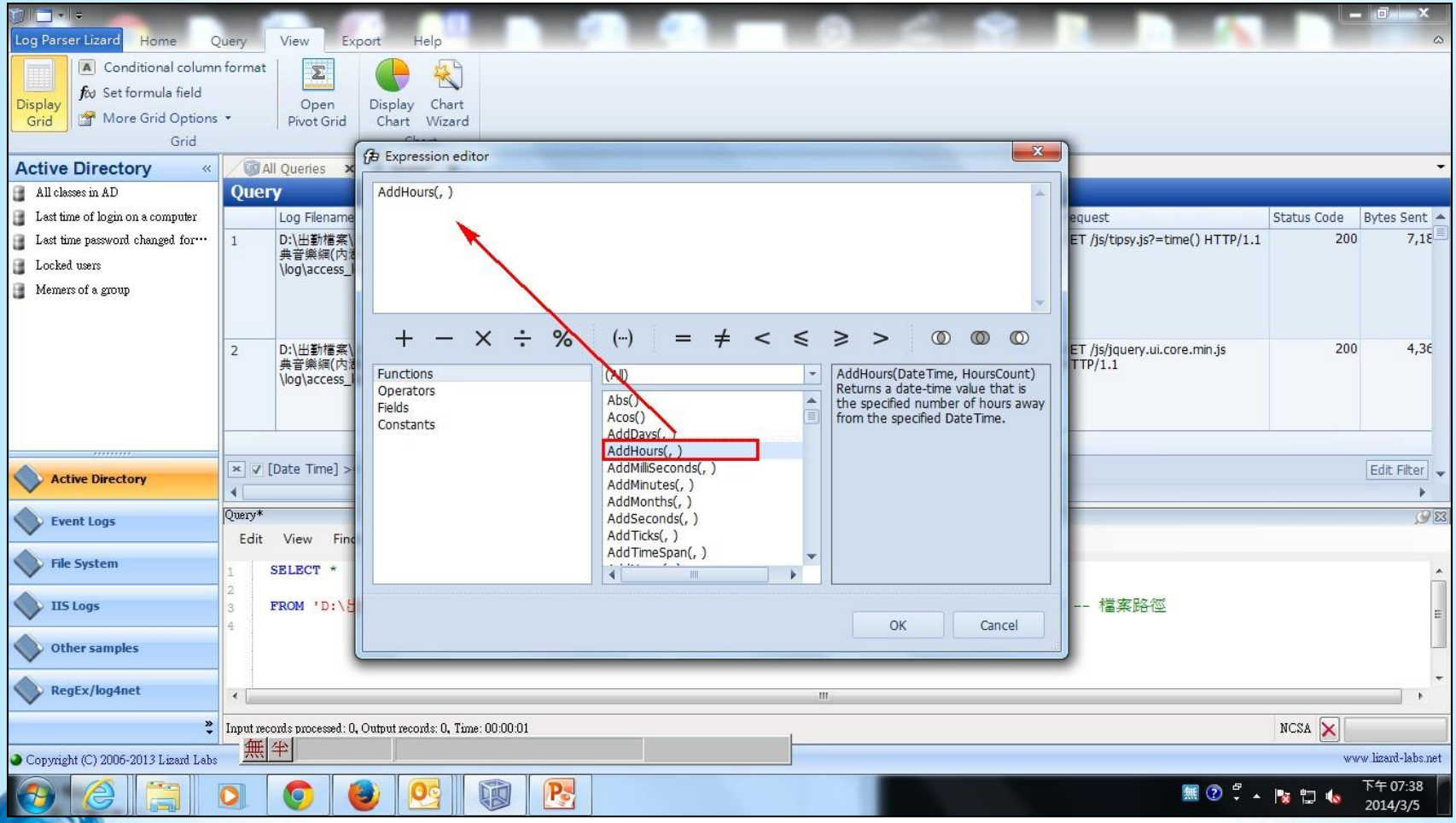
  log parser lizard會-8小時。

# 時間調整，若被自動調整+8:00 or -8:00的時間，可依下列方式調回來(限NCSA log)

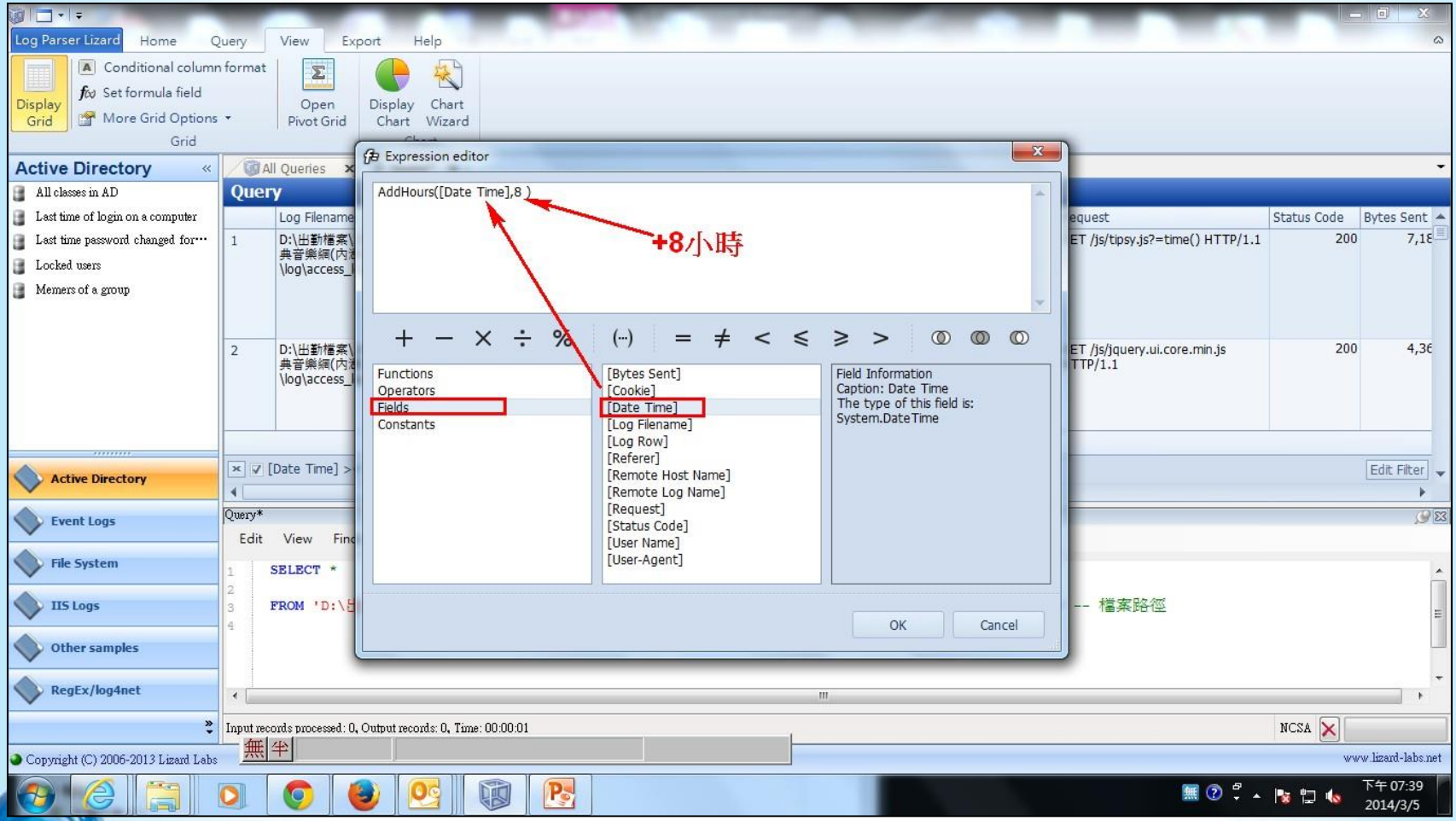
view>set formula field>新增欄位



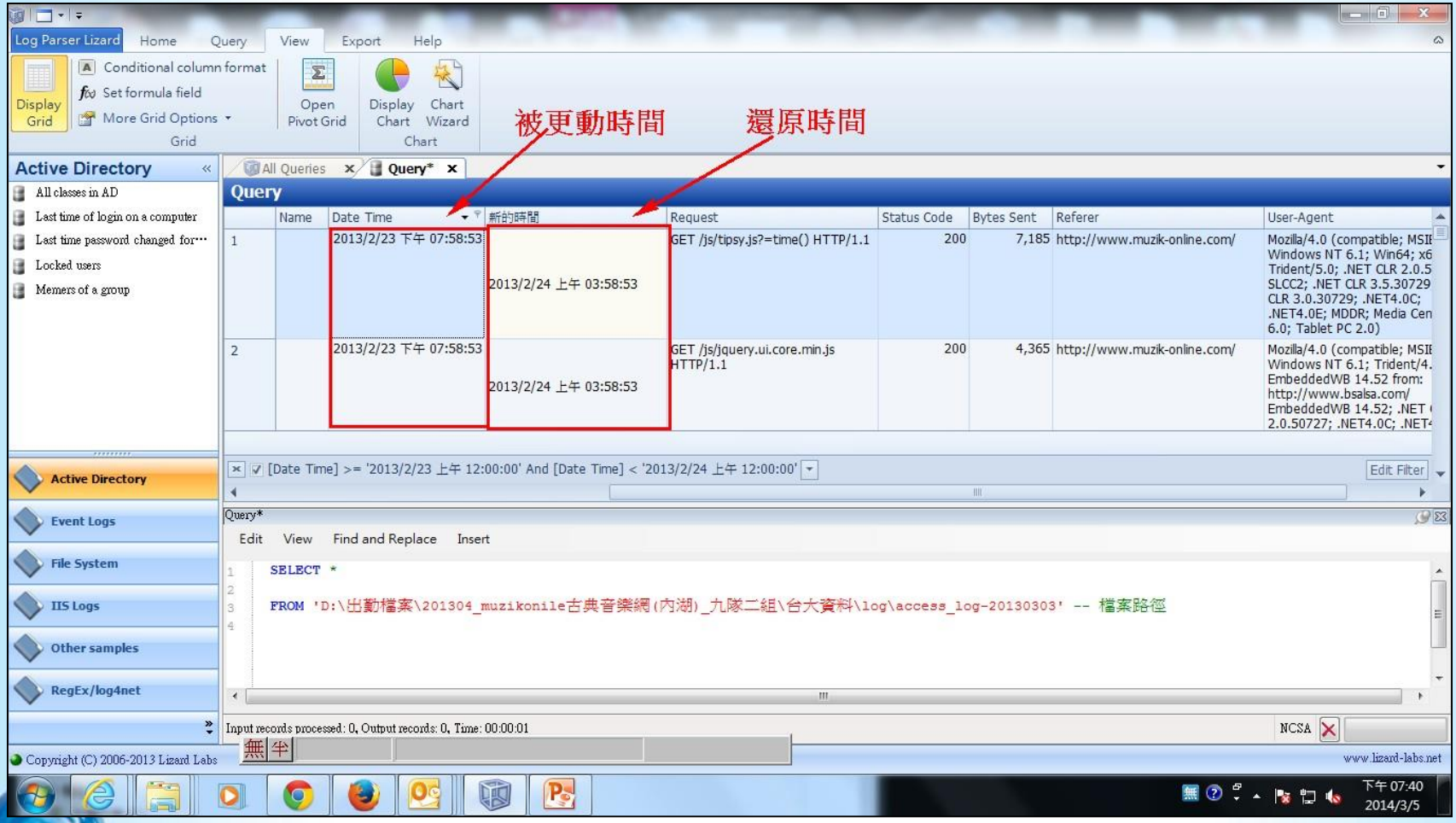
# Function>addhours(,)



# Addhours(欄位, 時間)



# 更動後的時間


被更動時間
還原時間
Log Parser Lizard
Home
Query
View
Export
Help
Display Grid
Conditional column format
Set formula field
More Grid Options
Grid
Open Pivot Grid
Display Chart
Chart Wizard
Chart
Active Directory
All classes in AD
Last time of login on a computer
Last time password changed for…
Locked users
Members of a group
All Queries
Query*
Query
Name
Date Time
新的時間
Request
Status Code
Bytes Sent
Referer
User-Agent
1
2013/2/23 下午 07:58:53
2013/2/24 上午 03:58:53
GET /js/tipsy.js?=time() HTTP/1.1
200
7,185
http://www.muzik-online.com/
2
2013/2/23 下午 07:58:53
2013/2/24 上午 03:58:53
GET /js/jquery.ui.core.min.js HTTP/1.1
200
4,365
http://www.muzik-online.com/
[Date Time] >= '2013/2/23 上午 12:00:00' And [Date Time] < '2013/2/24 上午 12:00:00'
Edit Filter
Active Directory
Event Logs
File System
IIS Logs
Other samples
RegEx/log4net
Query*
Edit
View
Find and Replace
Insert
SELECT *
FROM 'D:\出勤檔案\201304_muzikonile古典音樂網(內湖)_九隊二組\台大資料\log\access_log-20130303' -- 檔案路徑
Input records processed: 0, Output records: 0, Time: 00:00:01
NCSA
Copyright (C) 2006-2013 Lizard Labs
www.lizard-labs.net
下午 07:40
2014/3/5

# 網站常見攻擊手法與案例

- 網站首頁遭置換一案(Web shell)
- 網站遭植入xss攻擊一案(XSS)
- 網站資料庫遭攻擊一案(SQL injection)
- 網站遭目錄穿越攻擊一案(local file inclusion)

# Web shell

- 常見web shell上傳手法有:
- 利用系統本身服務的漏洞來上傳木馬

  例如:server2003的WebDAV服務
- 利用網站上傳服務漏洞上傳木馬

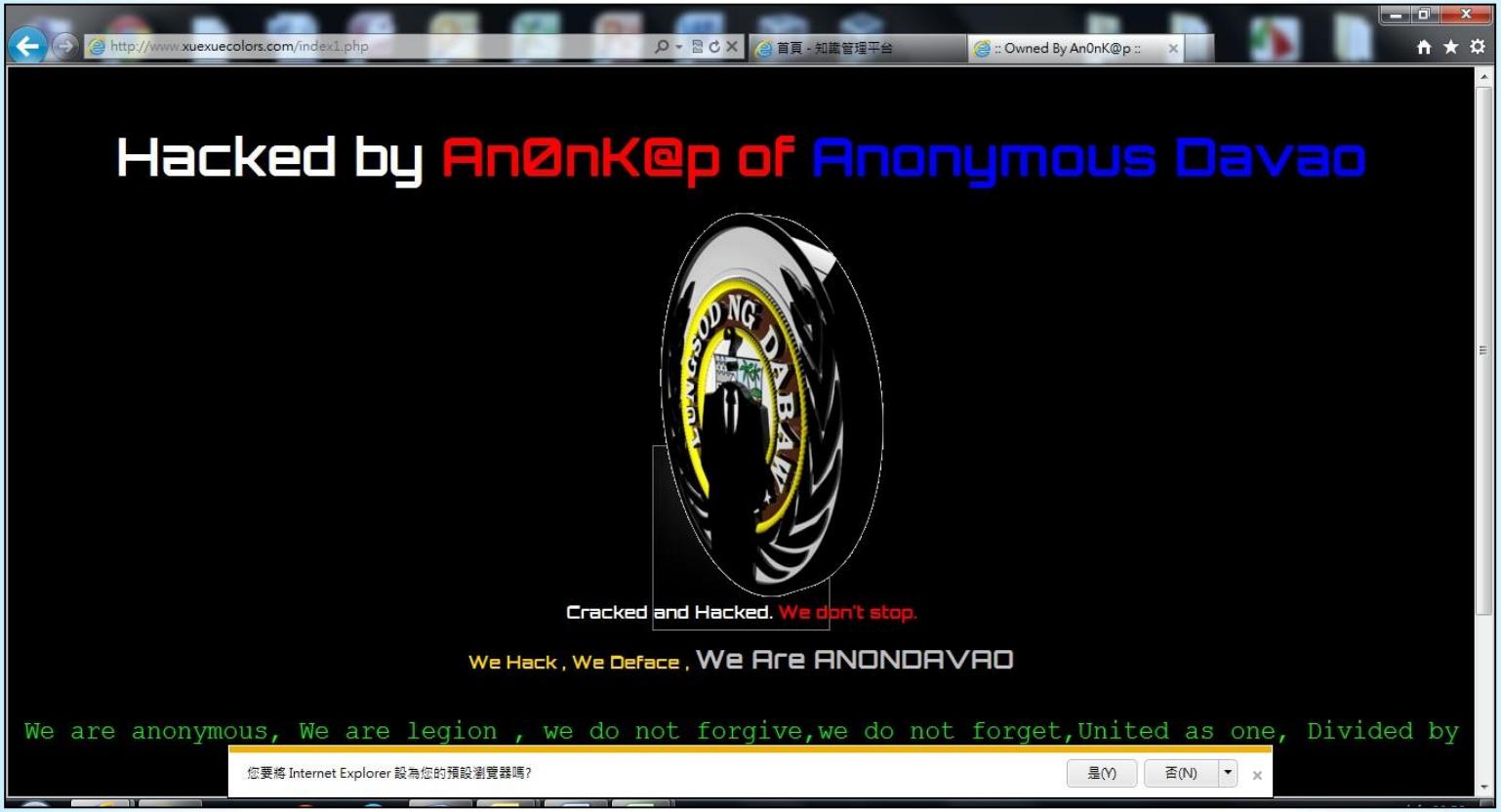
  例如:圖片、檔案上傳服務，fckeditor

  編輯器漏洞。

# 正常公司網站

xue xue COLORS
學 學 台 灣 文 化 色 彩
靈感圖庫 Collections
配色練習 Practice
色彩社群 Community
色彩活動 Events
色彩出版 Publications
靈感圖庫 | 王國禎
藝術創作 植物（牡丹）

# 被駭公司網頁


http://www.xuexuecolors.com/index1.php
首頁 - 知識管理平台
:: Owned By An0nK@p ::
Hacked by An0nK@p of Anonymous Davao
Cracked and Hacked. We don't stop.
We Hack , We Deface , We Are ANONDAVAO
We are anonymous, We are legion , we do not forgive,we do not forget,United as one, Divided by
您要將 Internet Explorer 設為您的預設瀏覽器嗎?
是(Y)
否(N)

# SERVER 2003與iis 6.0 漏洞

- WebDAV（Web-Based Distributed Authoring and Versioning）是一種可與遠端主機進行檔案或資料交換方式的標準，它讓在 Web 檔案變得可讀可寫，就像在本機上的檔案系統。
- 不過自windows2003與iis6.0，WebDAV被發現漏洞缺陷，且此漏洞已被利用在攻擊手法中，此漏洞的手法主要為利用微軟處理的Unicode token過程產生漏洞，如%c0和%af的16進位碼，代表在特定目錄(c:\\)中取得相當權限(administrator)後，利用dos特殊指令來控制網站的所有權，以達到新增、修改、刪除等權限內容。

# WebDAV入侵方式

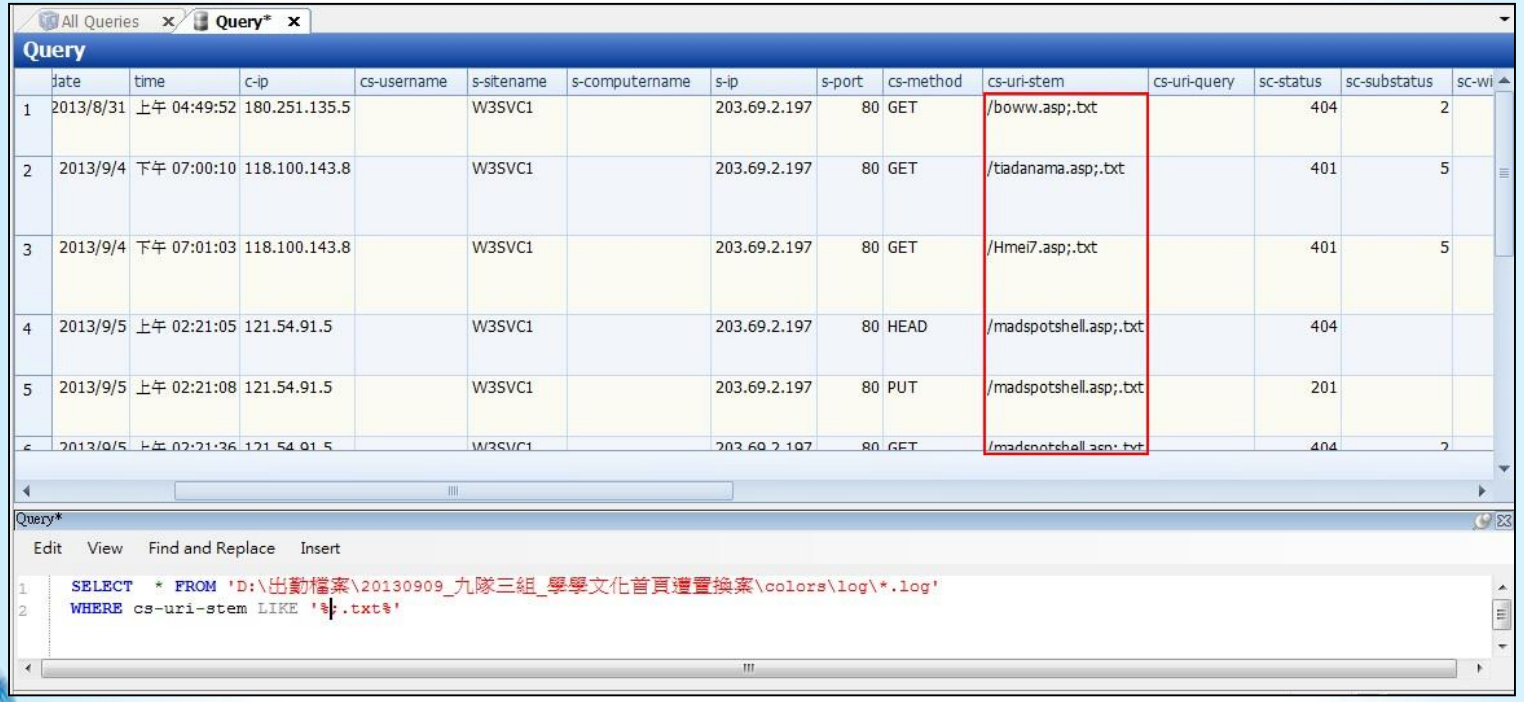
- 經由日誌檔的分析方式，得知下列IP在伺服器上是有異常存取(新增、修改)的動作，其主要攻擊的方式為下列五種方式:
- 1.鎖定使用IIS服務的主機，並且有開啟WebDAV的網站。
- 2.上傳文字檔格式(txt)的木馬程式(webshell)。
- 3.利用HTTP的MOVE、PUT等方法，上傳ASP、PHP格式的木馬程式。
- 4.修改網站原有的網頁檔，實現掛馬(放上木馬程式)。
- 5.結合IIS在文件名稱解析的漏洞，上傳.asp;.txt、.txt、.php等多種木馬程式。

# 異常增加檔案(.ASP;.txt)

| date | time | c-IP | s-port | cs-method | cs-uri-stem | sc-status |
|---|---|---|---|---|---|---|
| 2013/8/31 | 上午 04:49:52 | 180.251.135.5 | 80 | GET | /boww.asp;.txt | 404 |
| 2013/9/4 | 下午 07:00:10 | 118.100.143.8 | 80 | GET | /tiadanama.asp;.txt | 401 |
| 2013/9/4 | 下午 07:01:03 | 118.100.143.8 | 80 | GET | /Hmei7.asp;.txt | 401 |
| 2013/9/5 | 上午 02:21:05 | 121.54.91.5 | 80 | HEAD | /madspotshell.asp;.txt | 404 |
| 2013/9/5 | 上午 02:21:08 | 121.54.91.5 | 80 | PUT | /madspotshell.asp;.txt | 201 |
| 2013/9/5 | 上午 02:21:36 | 121.54.91.5 | 80 | GET | /madspotshell.asp;.txt | 404 |
| 2013/9/5 | 上午 02:21:50 | 121.54.91.5 | 80 | HEAD | /home.asp;.txt | 404 |
| 2013/9/5 | 上午 02:21:53 | 121.54.91.5 | 80 | PUT | /home.asp;.txt | 201 |
| 2013/9/5 | 上午 02:21:59 | 121.54.91.5 | 80 | GET | /home.asp;.txt | 401 |
| 2013/9/5 | 上午 02:22:04 | 121.54.91.5 | 80 | GET | /home.asp;.txt | 401 |

# log parser lizard軟體操作 (web shell)

找尋重點:HTTP PUT方法和*.txt(木馬)



# 跨站腳本攻擊
# Cross-Site Scripting，XSS

- 它指的是惡意攻擊者往Web頁面裏插入惡意html代碼，當用戶瀏覽該頁之時，嵌入其中Web裏面的html代碼會被執行，從而達到惡意用戶的特殊目的。(被植入成功後，只能從網頁程式碼找出有無被嵌入XSS惡意語法)
- 特徵:

受害網站的頁面，應會留下XSS的嘗試攻擊語法。

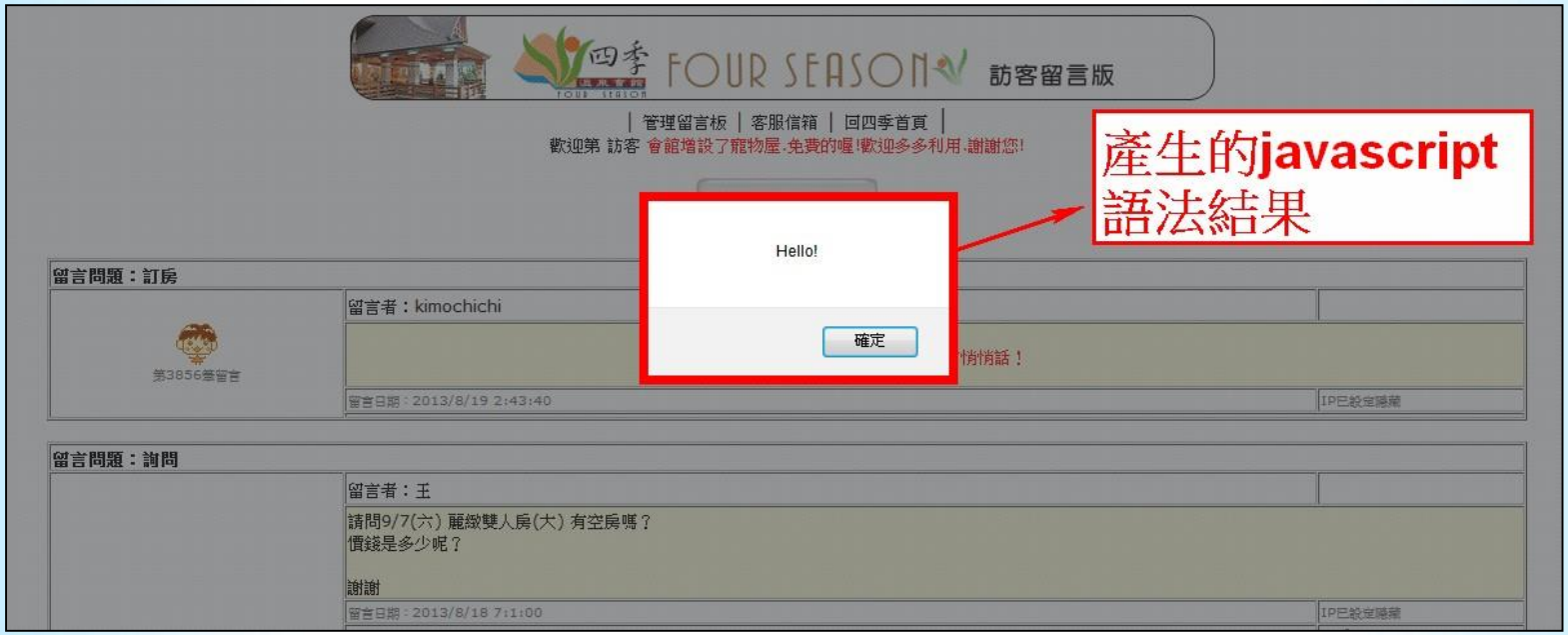
# XSS攻擊新聞事件

eBay出現跨站攻擊漏洞，用戶可能被導向釣魚網站
eBay 的XSS漏洞讓駭客得以在產品頁面上植入一段惡意程式碼，讓使用者點入後自動被導引到假冒eBay登入頁面的外部網頁。若一經取得帳密，可能讓駭客取得任何想要的用戶資訊。
文/ 林妍溱 | 2014-09-23 發表
7,485 按讚加入iThome粉絲團
分享 89
3
File Edit View Favorites Tools Help
ebay
Welco
Sign in
Email or user ID
Password

# demo-填寫留言加入 javascript語法-以hello world為例

```
<script type="text/javascript">
alert("Hello, world!");          // 開啟對話視窗顯示
</script>
```

# demo-產生hello視窗
# 成功!!!!



# 常見xss語法，可依照xss語法找關鍵字

script,alert,document,cookie,%3C,%3E...

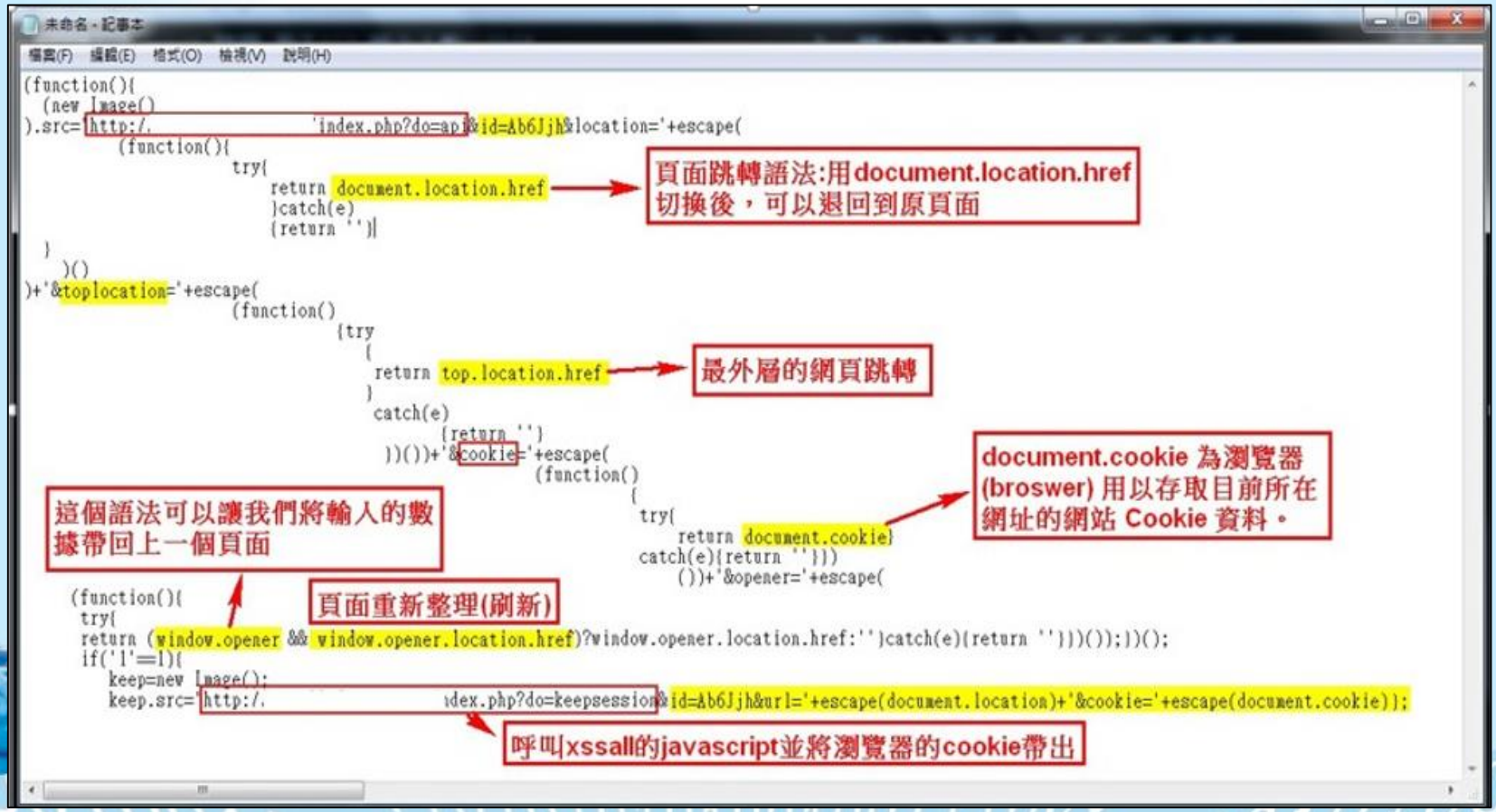
# log檔XSS攻擊的記錄

找尋重點:xss語法(script、document、cookie...)

```
/category.php?count&arem=114&arem1=2510&type=1'()&%<script >prompt(955716)</script>"
/category.php?count&arem=114&arem1=2510'()&%<script >prompt(965199)</script>&type=1"
/category.php?count&arem=114'()&%<script >prompt(973595)</script>&arem1=2510&type=1"
/category.php?count'()&%<script >prompt(904668)</script>&arem=114&arem1=2510&type=1"
/choose.php?choose_sn=202'()&%<script >prompt(902062)</script>"
/special_column.php?special_column_classify_sn=39&special_column_sn=66'()&%<script >prompt(985462)</script>"
/special_column.php?special_column_classify_sn=39'()&%<script >prompt(964471)</script>&special_column_sn=66"
/special_column.php?special_column_classify_sn=39'()&%<script >prompt(999015)</script>&special_column_sn=91"
/special_column.php?special_column_classify_sn=39'()&%<script >prompt(910607)</script>&special_column_sn=90"
/brand_info.php?brand_sn=9'()&%<script >prompt(909933)</script>"
/product.php?pid_for_show=3711'()&%<script >prompt(930076)</script>"
```

# 遭埋入的XSS語法

- 竊取使用者cookie



# 資料庫隱碼攻擊
# SQL injection

- 是在輸入的字串之中夾帶SQL指令，在設計不良的程式當中忽略了檢查，那麼這些夾帶進去的指令就會被資料庫伺服器誤認為是正常的SQL指令而執行，因此遭到破壞。
- 特徵:

日誌檔中可以看出SQL injection嘗試攻擊過程

資料庫發生異常，多半為SQL injection

# 資料庫隱碼攻擊新聞事件

## 警方偵破古典音樂網站Muzik Online駭客入侵案

Muzik Online在今年2月底遭駭客入侵，駭客透過網站漏洞以SQL Injection攻擊，導致會員資料被竄改無法正常登入使用各項服務，刑事局調查出為施姓休學研究生所為，目前以依妨害電腦使用罪章送辦。

文/ 蘇文彬 | 2013-05-07 發表

讚 7,495 按讚加入iThome粉絲團 分享 1 g+1 2

刑事警察局偵破古典音樂網站Muzik Online遭入侵案，施性駭客透過網站漏洞，以SQL Injection隱碼攻擊入侵，竄改該網站會員資料，駭客被依妨害電腦使用罪送辦。

Muzik Online以經營古典音樂社群為主，介紹古典樂迷國內外知名的演奏家、樂壇最新情報、知識及討論區，目前網站提供的服務均為免費性質，現在約有1.5萬會員。

2月底Muzik Online遭駭客入侵，駭客利用網站漏洞進行SQL Injection攻擊，竄改會員資料，因為已影響網站正常經營，經營Muzik Online的英屬維京群島商希幔數位向刑事局偵九隊請求偵辦。

# log檔SQLinjection攻擊的記錄

找尋重點:%20--、--、select

```
/category.php?count and sleep(4) &arem=114&arem1=2510&type=1
/search_result.php?&keyword=請輸入關鍵字&keyword_product_brand=10&search_by_product_money_end=1&search_by_product_money_start=1;select pg_sleep(4); -- &se
/category.php?count'+(select 1 from (select sleep(4))a)+&arem=114&arem1=2510&type=1
/search_result.php?&keyword=請輸入關鍵字&keyword_product_brand=10&search_by_product_money_end=1&search_by_product_money_start=1'+(select 1 from (select sle
/category.php?count=sleep(4)="&arem=114&arem1=2510&type=1"
/search_result.php?&keyword=請輸入關鍵字&keyword_product_brand=10&search_by_product_money_end=1&search_by_product_money_start=1=sleep(4)="&search_by_s
/category.php?count'=sleep(4)='&arem=114&arem1=2510&type=1
/search_result.php?&keyword=請輸入關鍵字&keyword_product_brand=10&search_by_product_money_end=1&search_by_product_money_start=1'=sleep(4)='&search_by_s
/category.php?count or (sleep(4)+1) limit 1 -- &arem=114&arem1=2510&type=1"
/category.php?count' or (sleep(4)+1) limit 1 -- &arem=114&arem1=2510&type=1
/search_result.php?&keyword=請輸入關鍵字&keyword_product_brand=10&search_by_product_money_end=1&search_by_product_money_start=1 or (sleep(4)+1) limit 1 -- &
/category.php?count and sleep(4)="&arem=114&arem1=2510&type=1"
/search_result.php?&keyword=請輸入關鍵字&keyword_product_brand=10&search_by_product_money_end=1&search_by_product_money_start=1' or (sleep(4)+1) limit 1 --
/search_result.php?&keyword=請輸入關鍵字&keyword_product_brand=10&search_by_product_money_end=1&search_by_product_money_start=1 and sleep(4)="&search_b
/category.php?count' and (sleep(4)+1) limit 1 -- &arem=114&arem1=2510&type=1
/category.php?count' and sleep(4)='&arem=114&arem1=2510&type=1
/search_result.php?&keyword=請輸入關鍵字&keyword_product_brand=10&search_by_product_money_end=1&search_by_product_money_start=1' and (sleep(4)+1) limit 1 -
/search_result.php?&keyword=請輸入關鍵字&keyword_product_brand=10&search_by_product_money_end=1&search_by_product_money_start=1' and sleep(4)='&search_b
/search_result.php?&keyword=請輸入關鍵字&keyword_product_brand=10&search_by_product_money_end=1&search_by_product_money_start=1 or (sleep(4)+1) limit 1 -- &
/search_result.php?&keyword=請輸入關鍵字&keyword_product_brand=10&search_by_product_money_end=1&search_by_product_money_start=1 and sleep(4) &search_by
```

# 目錄穿越攻擊
# local file inclusion

- 目錄穿越式攻擊漏洞,合法使用者可利用 ls 指令 , 配合 '../' 等字元, 存取 FTP 程式安裝所在目錄,或其他路徑; 而入侵者也常使用這個漏洞來竊取其他使用者目錄資訊, 並進一部對主機造成安全威脅。
- 特徵:

log中會出現大量../../../和../../etc/passwd的字串

# 目錄穿越攻擊新聞事件

iThome 新聞 產品評測 CIO 技術 專題 專欄 主題頻道 研討會 社群
遠通電收網站被駭，主機管理資訊在網路被公開
遠通電收網站主機遭到入侵，駭客將取得的主機帳號資料在網路上公告出來，遠通電收證實確實遭到不明攻擊，已修改密碼、改善網站安全，強調用戶資料並未被竊。
文/ 蘇文彬 | 2014-01-08 發表
7,495 按讚加入iThome粉絲團
分享 0
Untitled
Public Pastes
Related Results
1. Machinery and Tools
Find Mfrs of Machinery and Tools Find Products, Services & Resources
2. 64-Year-Old Mom Looks 27
Follow this 1 weird tip and remove 20 years of wrinkles in 20 days.
Related Results
1. Machinery and Tools
Find Manufacturers and Sellers of Industrial Equipment
2. 64-Year-Old Mom Looks 27
Follow this 1 weird tip and remove 20 years of wrinkles in 20 days

# log檔，目錄穿越攻擊記錄

找尋重點:../../、passwd、etc

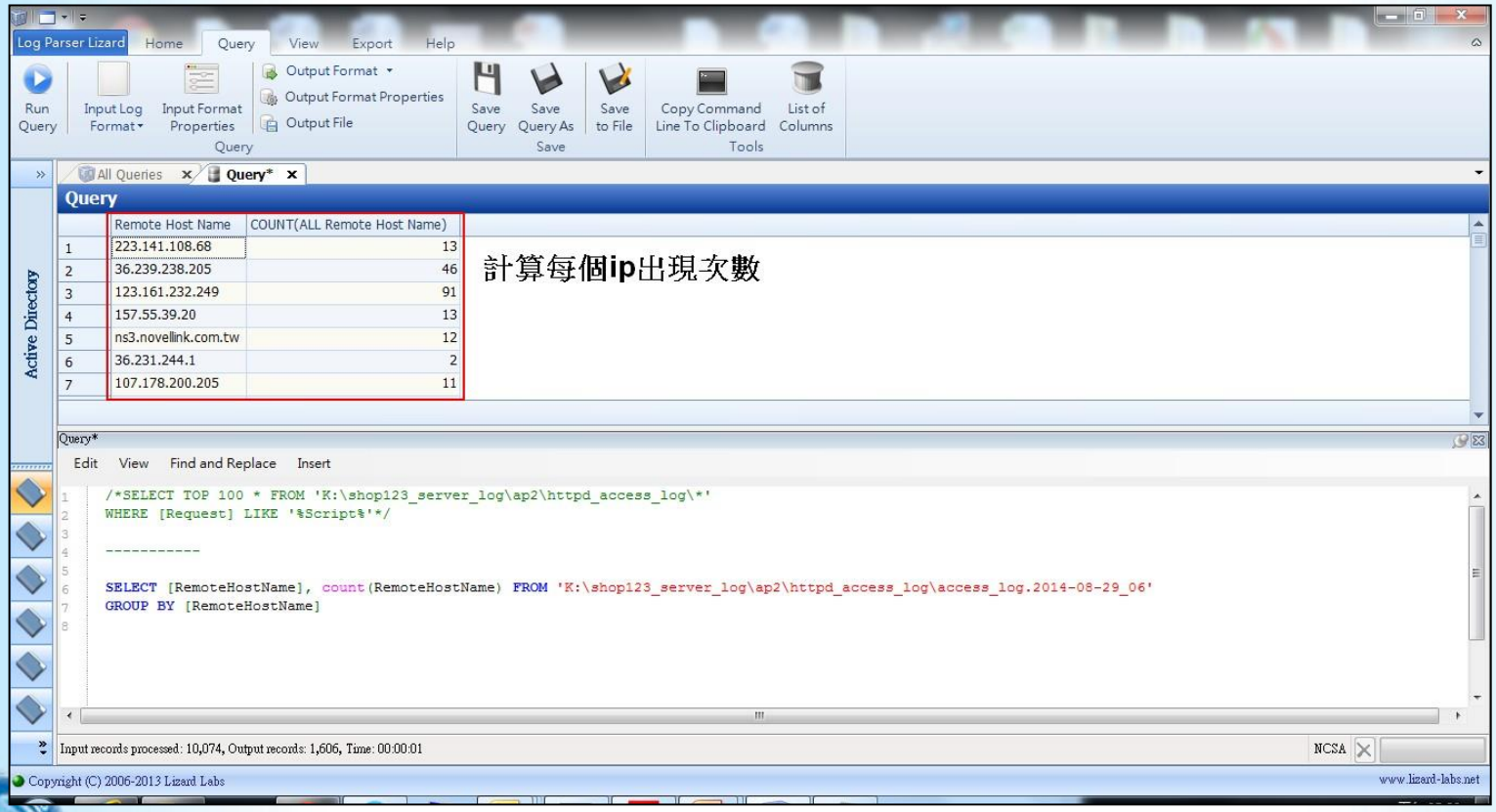
| |
|---|
| /400185/category.php?&type=../../../../../../../../../../../../../../../../../../etc/passwd |
| /400185/category.php?type=../../../../../../../../../../../../../../../../../../etc/passwd |
| /400185/category.php?&type=../../../../../../../../../../../../../../../../../../etc/passwd |
| /400185/category.php?type=../../../../../../../../../../../../../../../../../../etc/passwd |
| /400185/category.php?&type=../../../../../../../../../../../../../../../../../../etc/passwd |
| /400185/category.php?type=../../../../../../../../../../../../../../../../../../etc/passwd |
| /400185/category.php?&type=../../../../../../../../../../../../../../../../../../etc/passwd |
| /400185/category.php?type=../../../../../../../../../../../../../../../../../../etc/passwd |
| /product.php?&pid_for_show=../../../../../../../../../../../../../../../../../../etc/passwd |
| /product.php?pid_for_show=../../../../../../../../../../../../../../../../../../etc/passwd |
| /product.php?&pid_for_show=../../../../../../../../../../../../../../../../../../etc/passwd |
| /product.php?pid_for_show=../../../../../../../../../../../../../../../../../../etc/passwd |
| /product.php?&pid_for_show=../../../../../../../../../../../../../../../../../../etc/passwd |
| /product.php?pid_for_show=../../../../../../../../../../../../../../../../../../etc/passwd |
| /product.php?&pid_for_show=../../../../../../../../../../../../../../../../../../etc/passwd |
| /product.php?pid_for_show=../../../../../../../../../../../../../../../../../../etc/passwd |
| /product.php?&pid_for_show=../../../../../../../../../../../../../../../../../../etc/passwd |
| /product.php?pid_for_show=../../../../../../../../../../../../../../../../../../etc/passwd |
| /product.php?&pid_for_show=../../../../../../../../../../../../../../../../../../etc/passwd |
| /product.php?pid_for_show=../../../../../../../../../../../../../../../../../../etc/passwd |
| /product.php?&pid_for_show=../../../../../../../../../../../../../../../../../../etc/passwd |

# 若不知道攻擊手法呢?
# 怎麼分析LOG?

- 統計近期每個IP拜訪次數(找出異常高峰點後，再逐一分析每個IP行為模式)。
- 找尋大量404失敗的特徵，有沒有突然出現200成功。
- 找尋嘗試掃瞄網站後台記錄(admin、root、phpmyadmin等)。
- 案發時間點與網站受害情況。

# 計算異常IP出現次數

瞭解異常IP的存取情況，再逐一分析(土法煉鋼)




**SELECT** [RemoteHostName], count(RemoteHostName) **FROM** 路徑
**GROUP BY** [RemoteHostName]

# Q & A