



# 如何快速尋找有問題的入侵記錄

Microsoft MVP 黃建笙

Microsoft® Most Valuable Professional

CISSP® Certified Information Systems Security Professional


ISSMP® Management



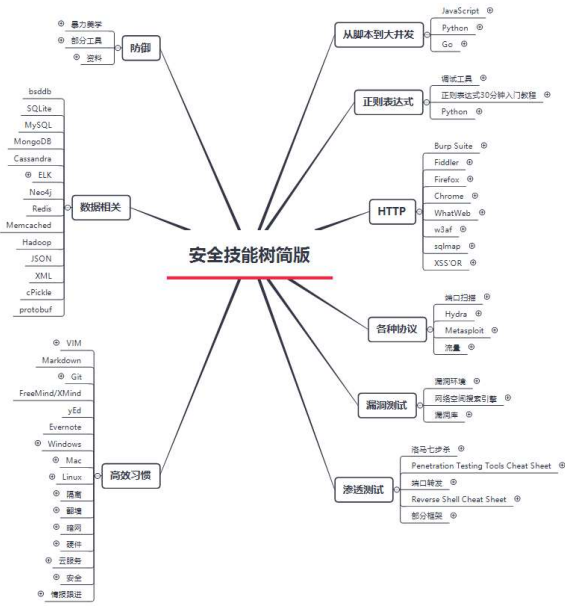
山女人王竹第一!



fpt.com





# 資訊安全職能領域



**安全技能树简版**

- 防壁
  - 暴力脚本
  - 部分工具
  - 资料
- 数据相关
  - Isidb
  - SQLee
  - MySQL
  - MongoDB
  - Cassandra
  - ELK
  - Neo4j
  - Redis
  - Memcached
  - Hadoop
  - JSON
  - XML
  - cPickle
  - protobuf
- 开发习惯
  - VIM
  - Markdown
  - Git
  - FreeMind/XMind
  - yEd
  - Evernote
  - Windows
  - Mac
  - Linux
  - 搭建
  - 部署
  - 维护
  - 设计
  - 云架构
  - 安全
  - 编程规范
- 从脚本到大开发
  - JavaScript
  - Python
  - Go
- 正则表达式
  - 测试工具
  - 正则表达式30分钟入门教程
  - Python
- HTTP
  - Burp Suite
  - Fiddler
  - Firefox
  - Chrome
  - WhatWeb
  - w3af
  - sqlmap
  - XSS'OR
- 各种协议
  - 端口扫描
  - Hydra
  - Metasploit
  - 流量
- 漏洞测试
  - 漏洞环境
  - 网络空间搜索引擎
  - 漏洞库
- 渗透测试
  - 渗透七步法
  - Penetration Testing Tools Cheat Sheet
  - 端口转发
  - Reverse Shell Cheat Sheet
  - 部分框架

[http://evilcos.me/security\\_skill\\_tree\\_basic/index.html](http://evilcos.me/security_skill_tree_basic/index.html)

fpt.com

這幾年下來  
Web Security已然成為資安顯學!

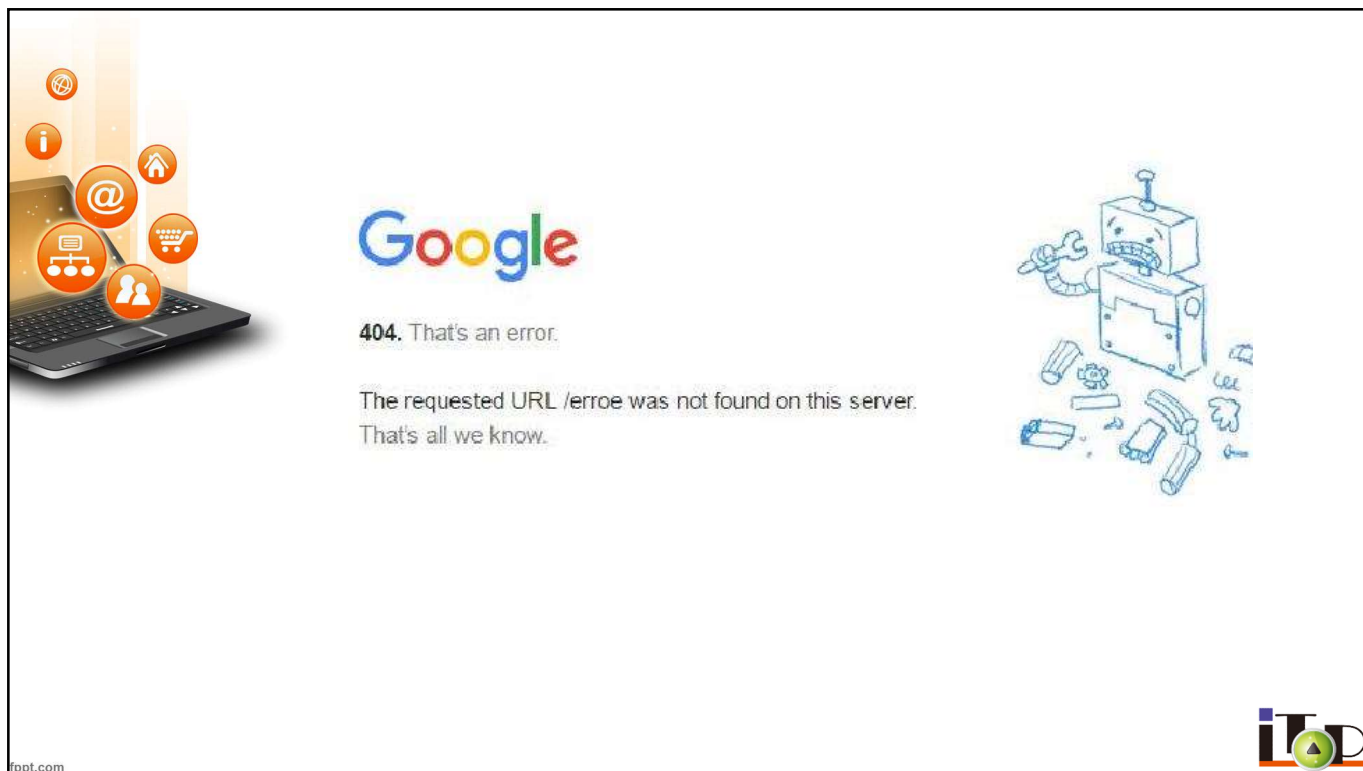


因為，再小的公司  
都有網站  
都有電子郵件服務!



讓我們來認識一下  
重要的錯誤訊息吧!

404, Oops! Not found!





## HTTP Error 404

### 404 Not Found

The Web server cannot find the file or script you asked for. Please check the URL to ensure that the path is correct.

Please contact the server's administrator if this problem persists.



上面這些都叫做

404 找不到!!



維基百科 http協定的狀態代碼如下：

**HTTP狀態碼**（英語：HTTP Status Code）是用以表示網頁伺服器超文字傳輸協定回應狀態的3位數字代碼。它由 [RFC 2616](#) 規範定義的，並得到 [RFC 2518](#)、[RFC 2817](#)、[RFC 2295](#)、[RFC 2774](#) 與 [RFC 4918](#) 等規範擴充功能。所有狀態碼的第一個數字代表了回應的五種狀態之一。所示的訊息短語是典型的，但是可以提供任何可讀取的替代方案。除非另有說明，狀態碼是HTTP / 1.1標準（[RFC 7231](#)）的一部分。<sup>[1]</sup>



# 404只是http Error code之一

1xx訊息

2xx成功

3xx重新導向

4xx用戶端錯誤

5xx伺服器錯誤



哦！來聊聊入侵的程序

現在開始大家切換到惡魔模式!!

當你看到一棟房子  
裡面有你極度想要的東西





你會先上下打量一下  
要怎麼進去!!





嘗試著開鎖!!



# 無聲的破窗!!



找到寶物!!

開始解開結界、開箱、貼粉專!!



榮登高富帥!!

迎娶白富美!!

成為人人稱羨的神仙伴侶!!



聽老衲一句話!!!

作夢爽一下就好，別當真啊!!



但事實相去不遠!!

一樣的行為!

應用在網站安全上是相同的!



## 典型的入侵程序



### 爬蛛

- 先找找網頁上有連結的，有那一些!!

### 憑經驗猜

- 多數用常見的名稱進行猜測(會出現大量的404)

### 開鎖

- 猜中後，可以開始針對你想隱藏的目錄會檔案進行存取(猜中了302、304、403、405)



fpt.com

## 我們可以這麼解釋



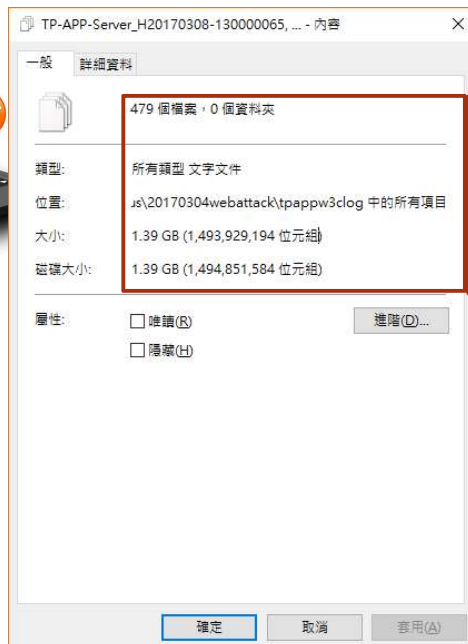
1. 某個入侵者會先大量的爬取，出現大量的200。
2. 接下來開始要猜猜看資源在那裡，出現大量的404
3. 當資源被猜中時，最常出現的是302、304、403、405
4. 最後就開始使用奇淫技巧，出現大量的500。
  - ◆ 檔案下載模組下載
  - ◆ 利用弱點或程式邏輯漏洞
  - ◆ 有外掛模組可上傳檔案，污染主機。
5. 得手資源



fpt.com



## 肉搜網友不強，肉搜log才強!



479 個檔案，0 個資料夾

所有類型 文字文件

js\20170304webattack\tpappw3clog 中的所有項目

1.39 GB (1,493,929,194 位元組)

1.39 GB (1,494,851,584 位元組)



## 這樣的log量才多少行?

```
c:\Program Files (x86)\Log Parser 2.2>LogParser.exe "select count (*) from  
C:\Users\Jason\OneDrive\LOG\20170304webattack\tpappw3clog\*.log" -i:w3c  
COUNT (ALL *)
```

6391922

Statistics:

```
Elements processed: 6391922  
Elements output: 1  
Execution time: 96.24 seconds (00:01:36.24)
```

Statistics:

```
-----  
Elements processed: 6391922  
Elements output: 1  
Execution time: 96.24 seconds (00:01:36.24)
```



## 找出有問題的記錄

統計狀態碼

以IP為基礎  
統計狀態碼

以狀態碼統計URI

統計該IP  
詢問的內容

針對特定的URI過濾

過濾每個URI  
連線內容



fppt.com

## IIS LOG的格式說明

[日期 (date)]：發生要求的日期。

[時間 (time)]：發生要求的時間，使用國際標準時間 (UTC)。

[用戶端 IP 位址 (c-ip)]：提出要求之用戶端的 IP 位址。

[使用者名稱 (cs-username)]：存取您的伺服器之已驗證使用者的名稱。匿名使用者會以連字號指示。



fppt.com



## IIS LOG的格式說明

[服務名稱 (s-sitename)]：完成要求的網站執行個體編號。

[伺服器名稱 (s-computername)]：產生記錄檔項目之伺服器的名稱。

[伺服器 IP 位址 (s-ip)]：產生記錄檔項目之伺服器的 IP 位址。

[伺服器連接埠 (s-port)]：針對服務設定的伺服器連接埠號碼。



fppt.com



## IIS LOG的格式說明

[方法 (cs-mothod)]：要求的動作，例如 GET 方法。

[URI Stem (cs-uri-stem)]：動作的「通用資源識別元」或目標。

[URI 查詢 (cs-rui-query)]：用戶端嘗試執行的查詢 (如果有的話)。只有針對動態頁面才需要執行通用資源識別元 (URI) 查詢。

[通訊協定狀態 (sc-status)]：HTTP 或 FTP 狀態代碼。



fppt.com



## IIS LOG的格式說明

[通訊協定子狀態 (sc-substatus)]：HTTP 或 FTP 子狀態代碼。

[Win32 狀態 ](sc-win32-status)：Windows 狀態代碼。

[已傳送位元組 (sc-bytes)]：伺服器傳送的位元組數。

[已接收位元組 (cs-bytes)]：伺服器接收的位元組數。



fppt.com



## IIS LOG的格式說明

[花費時間 (time-taken)]：動作所花費的時間長度 (毫秒)。

[通訊協定版本 (cs-version)]：用戶端使用的通訊協定版本，可為 HTTP 或 FTP。

[主機 (cs-host)]：主機名稱 (如果有的話)。

[使用者代理程式 (cs(UserAgent))]: 用戶端使用的瀏覽器類型。



fppt.com



## IIS LOG的格式說明

[Cookie (cs(Cookie))]: 已傳送或已接收的 Cookie 內容 (如果有的話)。

[推薦者 (cs(Referer))]: 使用者上次造訪的網站。此網站提供目前網站的連結。



ppt.com

# DEMO

實際統計

# 首先統計一下IP與狀態的關係吧

```
c:\Program Files (x86)\Log Parser 2.2>LogParser.exe "select c-ip,sc-status
, count(*) into f:\IPstatus.csv from C:\Users\Jason\OneDrive\LOG\20170304w
ebattack\tpappw3clog\*.log group by c-ip,sc-status" -i:w3c -o:csv
Task completed with parse errors.
```

Parse errors:

7931 parse errors occurred during processing (To see details about the parse

error(s), execute the command again with a non-zero value for the "-e" argument)

Statistics:

Elements processed: 6391372

Elements output: 175996

Execution time: 100.33 seconds (00:01:40.33)



		加總 - COUNT(ALL *)															欄標籤		
		列標籤		200	301	302	304	400	403	404	405	406	500	501 (空白)	總計				
		66.249.77.31		86632	271	229	231		1	143						87507			
		91.209.196.35		56681	221	11896		244	23	11633	549		3417	21	5	84690			
		210.242.157.166		40970		30490	2040		37	70						73607			
		66.249.77.28		139		43954	1						3			44097			
		66.249.79.173		29406	90	19	78			44						29637			
		68.180.228.34		14870	311	10246	89			81	2					25599			
		66.249.77.1		17858	99	69	78			46					1	18151			
		119.176.134.95		7505		7400	4			4						14913			
		66.249.79.149		54		14716							3			14773			
		91.209.196.35		12480	359	16				48						12903			
		68.180.228.34		7963	62	9	54			29					2	8119			
		119.176.134.95		3965		3713	107			14						7799			
		66.249.77.29		4737		252	1812			53						6854			
		61.216.146.174		40		6272	1			1			4		2	6320			
		91.209.196.35		4676		92	1418			26						6212			
		66.249.77.30		4691		77	1365			51						6184			
		66.249.79.153		5977	41	9	38			19						6084			
		210.242.157.166		4649	48	1252				28						5977			
		220.134.40.219		2894		334	2525		117	99						5969			
		54.219.188.185		3709	1	357	1320			53						5440			
		220.134.69.59		3971	43	1146				17						5177			
		66.249.82.92		4396	3	230	78			357						5064			
		61.220.222.25		4441		364	184			37						5026			
		211.22.104.189		2549		1513				833	4		17	1		4917			
		54.219.188.185		3113	3	454	1318			6						4894			
		123.193.117.210		2700	1	57	822			7						3587			
		66.249.82.93		2829	133	456	5			63						3486			
		110.75.145.1		2359		272	787			6						3424			
		123.194.96.130		1884		123	1278			12						3297			
		110.75.145.2		2506		88	587			8						3190			
		66.249.79.157			1														





# 再來統計一下IP、狀態及URI

```
c:\Program Files (x86)\Log Parser 2.2>LogParser.exe "select c-ip,sc-status,cs-uri-stem, count(*) into f:\IPstatusuri-91.209.196.35.csv from C:\Users\Jason\OneDrive\LOG\20170304webattack\tpappw3clog\*.log where c-ip='91.209.196.35' group by c-ip,sc-status,cs-uri-stem" -i:w3c -o:csv
Task completed with parse errors.
```

Parse errors:

7931 parse errors occurred during processing (To see details about the parse

error(s), execute the command again with a non-zero value for the "-e" argument)

Statistics:

Elements processed: 6391372

Elements output: 16142

Execution time: 93.50 seconds (00:01:33.50)



	A	B	C	D
1	c-ip	sc-status	cs-uri-stem	COUNT(ALL *)
2	91.209.196.35	501	/upload/toIdz9O0.htm	1
3	91.209.196.35	501	/tools/Btk7gpDQ.htm	1
4	91.209.196.35	501	/Nessus409045921.html	1
5	91.209.196.35	501	/common/appServer/jvmReport.jsf	1
6	91.209.196.35	501	/blog/index.php	13
7	91.209.196.35	501	/3HFwKp0r.htm	1
8	91.209.196.35	501	/2012layout/Z01nN4cT.htm	1
9	91.209.196.35	501	/2012layout/img/Zr7nTfdJ.htm	1
10	91.209.196.35	501	/2012layout/css/tGDmgulr.htm	1
11	91.209.196.35	500	/wordpress/	4
12	91.209.196.35	500	/UYmTXdvH.rem	1
13	91.209.196.35	500	/UserVerify_1.aspx	11
14	91.209.196.35	500	/UoRm8Vcf.	1
15	91.209.196.35	500	/u4b0qqzk.aspx	4
16	91.209.196.35	500	/status.xsl.	2
17	91.209.196.35	500	/ShoppingCartTW-tcb.aspx	1
18	91.209.196.35	500	/ShoppingCartOversea.aspx	1
19	91.209.196.35	500	/ShoppingCart.aspx	9
20	91.209.196.35	500	/Shoppingcart.aspx	8
21	91.209.196.35	500	/search=<script>alert("XSS")</script>	2
22	91.209.196.35	500	/scripts/u4b0qqzk.aspx	2
23	91.209.196.35	500	/scripts/search=<script>alert("XSS")</script>	1
24	91.209.196.35	500	/scripts/pleprt5n.aspx	2
25	91.209.196.35	500	/scripts/nessus"><script>alert('django_admin_xss.nasl')</script>/	1

其實最不安全的是政府網站!!



## 常見的網站問題

直播限定



Q&A



Thank you

