臺大區網雲端服務

Deployment and Management of Cloud Services through NTU Network Regional Center

臺灣大學 計算機及資訊網路中心
曾保彰

背景簡介

- 國外案例
  - 美國國家科學基金會(NSF)
  - 於2014年8月花了2千萬美金，在全國各大學，
  - 成立"Chameleon"及"CloudLab"二個雲端測試平台
  - 650個nodes(含5PB的儲存空間)及
  - 15000 processing cores(1PB的儲存空間)
  - 分別作不同的雲端服務測試，其中包括100G及SDN等最先進的網路架構。

台大區網

臺大區網架構圖
TANET
ISP
1 Gb
臺大區網中心
10 Gb
NTU
GE-T
4 Gb
大專院校
30所
高中職
21所
台北市教育網
國中小學
1131所

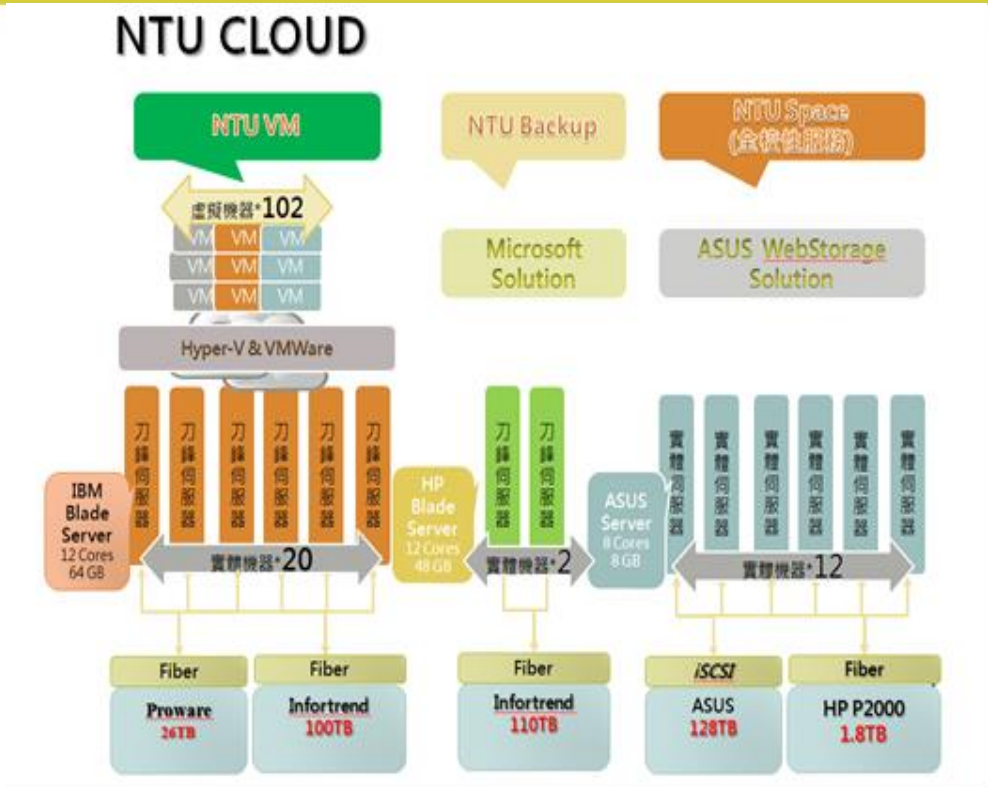
計畫目標

- 藉由臺大計中在推廣校內雲端服務的成功經驗，吸引臺大區網下各校主機虛擬化到臺大區網中心的雲端機房，達到校園節能的目標。

第一年目標:

- 預計建置一個容納120個虛擬主機的環境。
- 服務15個以上的學校、單位或計畫。
- 達成100 台以上虛擬主機在此環境實際運作，減少實體主機數量，以達節能之效。

臺大觔斗雲 (2010 ~)

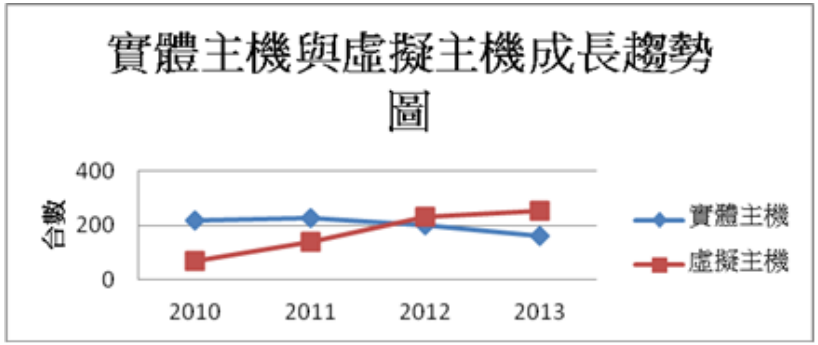


57 Servers、 485 TB 、 275 VM

臺大: 實體主機 vs. 虛擬主機

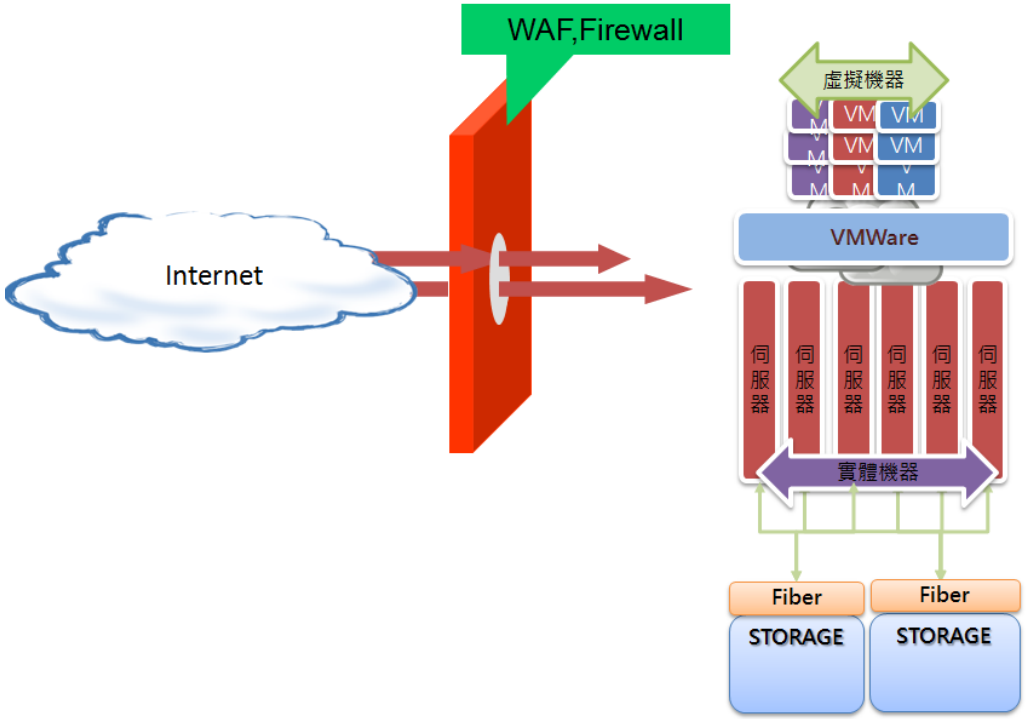
年度	計資中心採購伺服器量	其他單位採購伺服器量	全校總計
2010	19	199	218
2011	17	208	225
2012	15	185	200
2013	11	149	160
2014 上半年	11	57	68

年份	虛擬主機數目(累進)
2011 年 1 月-2012 年 12 月	140
2013 年 1 月-2013 年 12 月	231
2014 年 1 月-2014 年 8 月	251



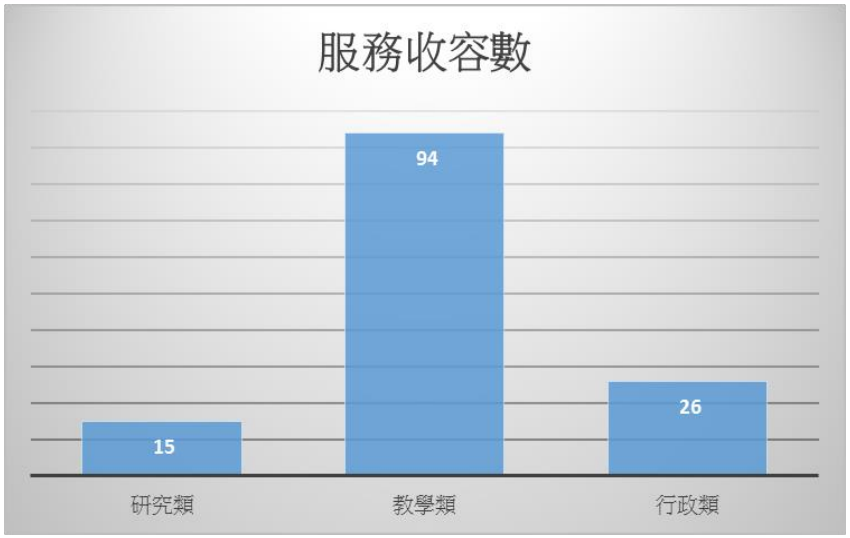
2010至2013年臺大實體主機與虛擬主機成長趨勢圖

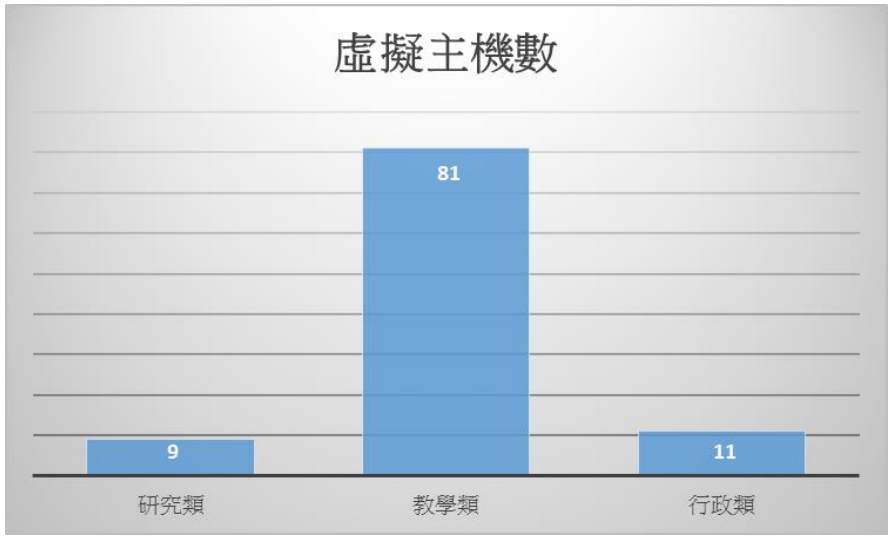
本計畫之雲端環境建置



6 Servers、 180 TB 、 101 VM、19學校

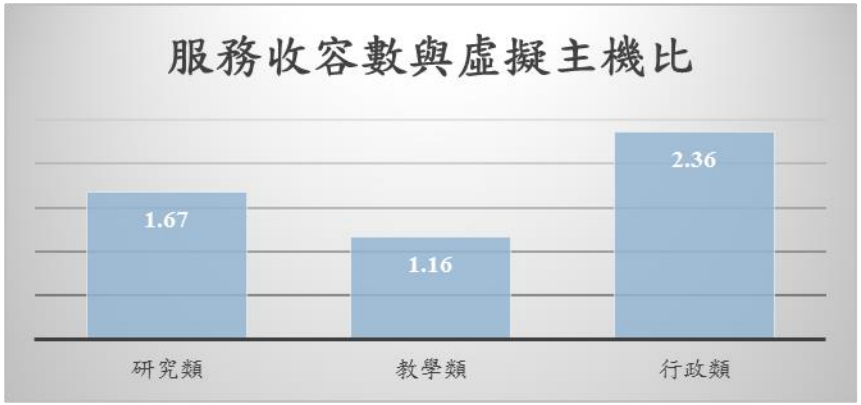
主要績效





服務收容數與
實體主機數比

22.5

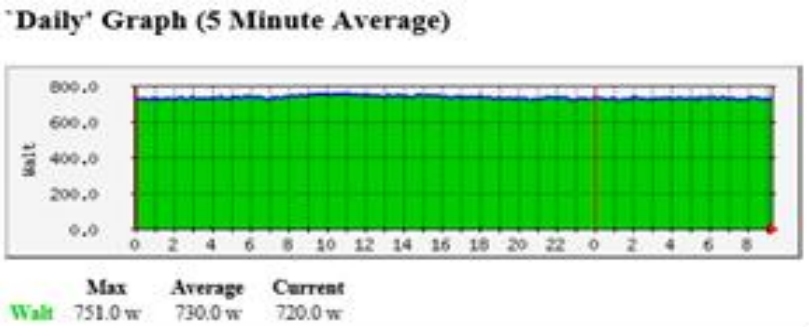


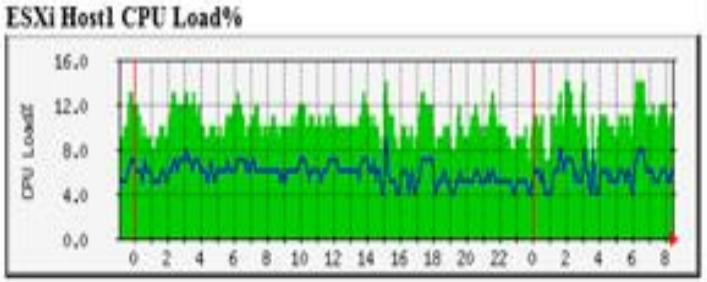
虛擬主機數與
實體主機數比

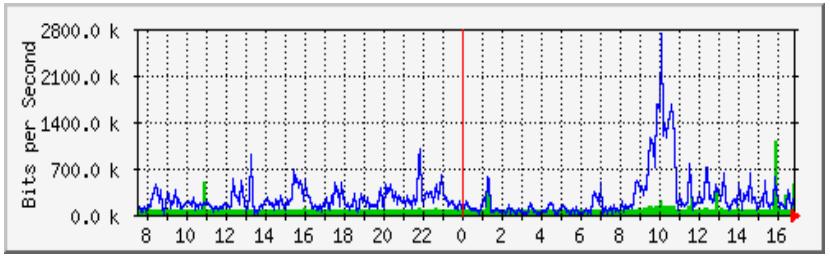
16.83

技術創新

- 計畫管理網頁 http://nepcloud.tp1rc.edu.tw
  - 虛擬主機總數
  - 即時電力量測
  - 即時網路流量
  - VM效能監控







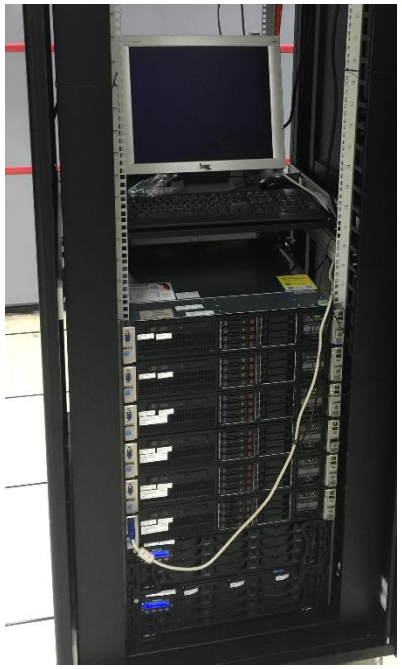
計畫亮點(酷課雲在臺大區網雲端)

- 2015-07-28 14:33:06 聯合新聞網 綜合報導
  - 台北市教育局籌備已久的「台北酷課雲」正式上線，（7/25）於建國中學舉辦第一階段成果發表會。
  - 酷課雲目前已使用臺大區網雲端 61個VM，持續增加中 。

經濟效益與社會影響

某國小機房
（約十台實體主機）

透過虛擬化轉化為

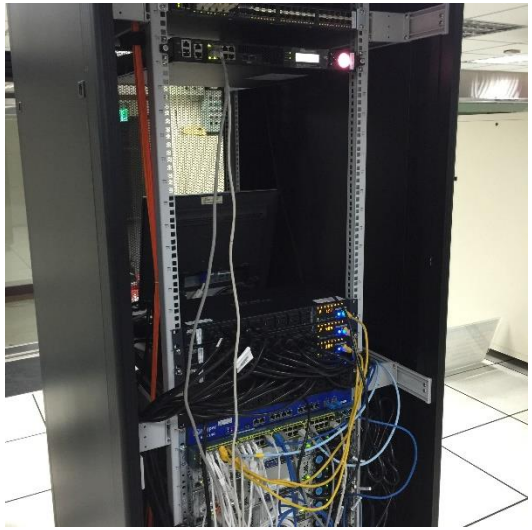


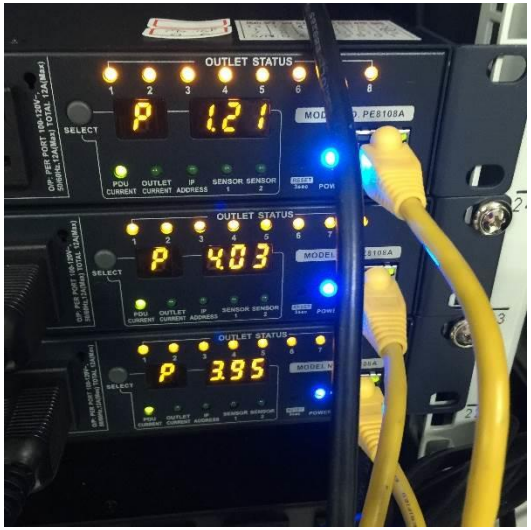
區網雲虛擬主機

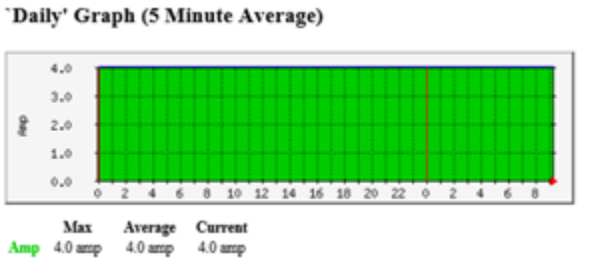
雲端研討會
目前已辦四場

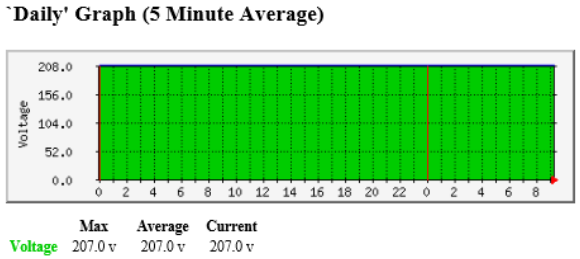
臺大機房機櫃耗能量測

可量測總耗能
及各別插座的耗能

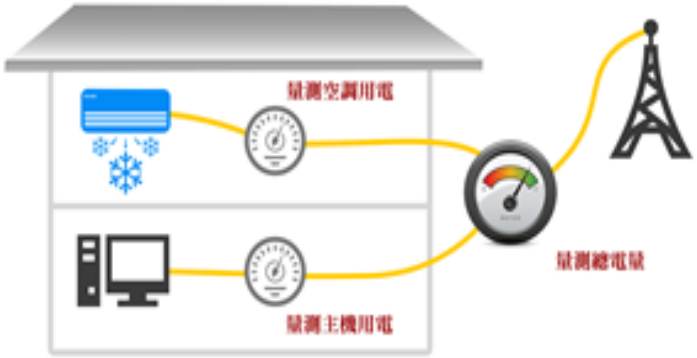


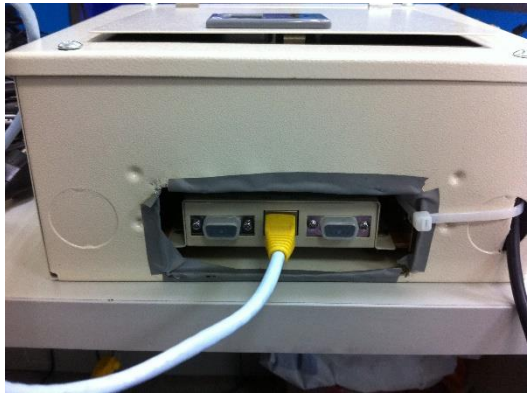






中小學機房耗能量測





各單位的VM及服務數

教學類: 高中高職

某高中1:VMx5,服務收容數5x2=10
某高中2:VMx1服務收容數1
某高中3:VMx3服務收容數3
某高中4:VMx4服務收容數8
某高中5:VMx1服務收容數1

教學類: 國小

某國小1:VMx1服務收容數2
某國小2:VMx3服務收容數3
某國小3:VMx4服務收容數4x2=8
某國小4:VMx1服務收容數1

行政類: 國小

某國小1:VMx1服務收容數1
某國小2:VMx1服務收容數1
某國小3:VMx1服務收容數1

行政類: 高中高職

某高中1:VMx1,服務收容數2
某高中2:VMx5,服務收容數5x2=10
某高中3:VMx1服務收容數1
某高中4:VMx1服務收容數5
某高中5:VMx1服務收容數2

行政類: 國小

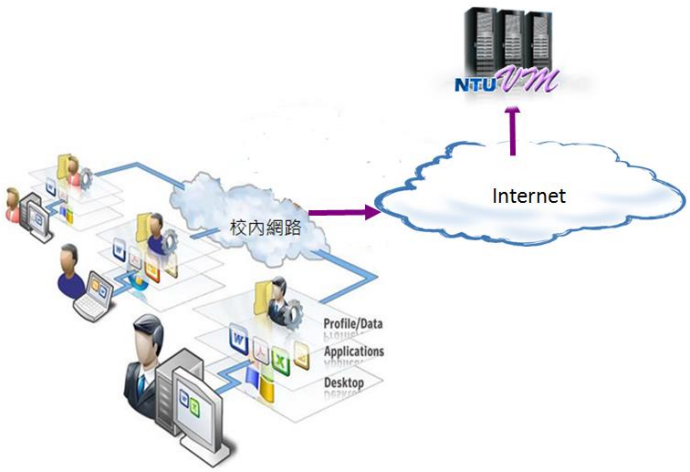
某國小1:VMx1服務收容數1
某國小2:VMx1服務收容數1
某國小3:VMx1服務收容數1

其他機構

某教育局: VMx61服務收容數61

未來展望

- 目前加入的有10所高中、7個國小、臺大7個系所及北市教育局共十九個單位。下一階段將積極推廣到臺大區網與台北市教育網之下的各級學校(國中小學及高中職共272所)
- 高國中小面臨:
  - 機房耗能
  - 缺主機管理人員
  - 資安問題



WAF 能幫什麼?

SQL INJECTION example from speed.ntu.edu.tw

id	IP	SelectCity	SelectZone	speed	satisfied	suggestions	daytime
2947	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:04:41
2948	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:04:48
2949	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:04:49
2950	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:04:49
2951	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:04:50
2952	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:04:50
2953	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:04:54
2954	218.65.12.200	???..	???..	??	???	test' and '1'='1	2015-05-25 13:05:03
2955	218.65.12.200	???..	???..	??	???	test' and '11'='11	2015-05-25 13:05:04
2956	218.65.12.200	???..	???..	??	???	test' and '1'='11	2015-05-25 13:05:04
2957	218.65.12.200	???..	???..	??	???	test' and '%'='	2015-05-25 13:05:04
2958	218.65.12.200	???..	???..	??	???	test' and '11%'='11	2015-05-25 13:05:08
2959	218.65.12.200	???..	???..	??	???	test' and '1%'='11	2015-05-25 13:05:08
2960	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:08
2961	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:09
2962	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:09
2963	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:09
2964	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:13
2965	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:16
2966	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:40
2967	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:41
2968	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:50
2969	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:51
2970	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:51
2971	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:52
2972	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:59
2973	218.65.12.200	???..	???..	??' and '1'='1	???	test	2015-05-25 13:06:04
2974	218.65.12.200	???..	???..	??' and '11'='11	???	test	2015-05-25 13:06:07
2975	218.65.12.200	???..	???..	??' and '1'='11	???	test	2015-05-25 13:06:11
2976	218.65.12.200	???..	???..	??' and '%'='	???	test	2015-05-25 13:06:11

The Open Web Application Security Project OWASP top 10

- A1 Injection (高中就在改成績)
- A2 Broken Authentication and Session Management (was formerly 2010-A3)
- A3 Cross-Site Scripting (XSS) (was formerly 2010-A2) 留言版最常發生
- A4 Insecure Direct Object References
- A5 Security Misconfiguration (was formerly 2010-A6)
- A6 Sensitive Data Exposure (2010-A7 Insecure Cryptographic Storage and 2010-A9 Insufficient Transport Layer Protection were merged to form 2013-A6)
- A7 Missing Function Level Access Control (renamed/broadened from 2010-A8 Failure to Restrict URL Access)
- A8 Cross-Site Request Forgery (CSRF) (was formerly 2010-A5)
- A9 Using Components with Known Vulnerabilities (new but was part of 2010-A6 – Security Misconfiguration)
- A10 Unvalidated Redirects and Forwards

資安工具

- Web Application Firewall ：A1,A3..
  - 誤判,調整POLICY
- CA:A2 PHISHING
- IBM Security AppScan
- HP FORTIFY STATIC CODE ANALYZER

敬請指教