**關貿網路第50期電子報**

《哈燒話題》

**「雲端有大師服務」讓您輕鬆駕馭大數據**

****

巨量資料分析(大數據)正夯，不要說對資訊科技一竅不通的門外漢來說是霧裡看花，就算是專業的資訊人員來說，也還是探索的階段。想嘗試所謂的大數據分析，光考慮從前端的硬體建置一直到後端的專業分析技術培養，連專業的資訊人員都感到一個頭N個大。

關貿網路Yodass有大師平台的成立，便是看到了從門外漢到資訊專業人員、從企業到個人都希望有一個簡單且高度硬軟體整合的巨量資料分析平台需求。現在你可以不用萬丈高樓平地起，只需要一步步跟隨大師的腳步，就能輕鬆解決大數據分析的工作。

立即申請您將馬上擁有30天完整體驗大數據分析服務，10G Hadoop資料倉儲，迅速套用模板展現資料價值，自在遨遊於資料美麗新世界。

立即申請體驗[http://www.yodass.com](http://www.yodass.com/eDM)

若您對Yodass有任何問題，歡迎您撥打24小時服務專線與我們聯絡。

Yodass服務中心

服務專線:+886-2-26551188

專人服務時間: 09:00 – 18:00

24小時服務信箱: [support@yodass.com](mailto:support@yodass.com)



《關貿新聞》

## 本公司配合食品藥物管理署輔導食品業者落實登錄制度

近日來台灣食安事件層出不窮，不僅相關產業受創影響台灣美食王國的聲譽，廣大消費者更深受其害，食品安全堪為當前最重要的議題。

為有效監督管理我國食品業者，衛生福利部食品藥物管理署(以下簡稱食藥署)積極推動我國食品業者落實登錄制度，由本公司建構「食品業者登錄平台」(<https://fadenbook.fda.gov.tw/>)，並於本(9)月25日配合食藥署辦理「落實食品業者登錄種子人員教育訓練」，培訓27位資訊種子人員，自今年10月1日起

於各縣市衛生局協助食品業者於食品業者登錄平台完成登錄，俾利我國食品業者配合政府政策，並提升食品衛生管理效率，使民眾重拾對食品業的信心與安心。

新聞引述自衛生福利部食品藥物管理署：【[種子人員起步走，輔導食品業者落實登錄制度！](http://www.fda.gov.tw/TC/newsContent.aspx?id=11601&chk=1c3189cd-fecd-47d8-9e26-bd1af5853c63&param=pn%3d1%26cid%3d4%26cchk%3df11420b2-cf8e-4d3a-beb5-66521b800453)】



《關貿CSR》

回饋鄉里，貫徹永續經營理念，本期關貿CSR要分享的是我們榮獲台北市政府頒發之「103年度鄰里公園績優認養人獎項」。

我們自三年前即認養南港火車站前的南興公園，我們更成立愛心志工社號召同仁加入南興公園巡查行列，每天安排志工針對公園整潔、設施狀況做巡查，並將巡查狀況回報南港區公所。同時，我們也不定時配合區公所來個公園大掃除與整理。

在盡力維護南興公園之外，我們還曾邀請各位民眾一起來發掘南興公園的美景，在認養期間我們舉辦過「我愛南港桂花香寫生比賽」及「我愛南興公園攝影比賽」。

在此，我們要感謝台北市政府及南港區公所的肯定，更要感謝本公司所有參與志工同仁，因為有你們的辛勞，公司才能得到這份殊榮。



《資安小常識》

**Shellshock漏洞，再度在各大伺服器中掀起一陣腥風血雨**

近日，資訊界發佈一個比4月份的OpenSSL Heartbleed還要令資訊人員日以繼夜忙碌的嚴重漏洞：Shellshock。這是一個藏在Bash內長達20年以上的安全漏洞，嚴重程度超過今年4月份的Heartbleed漏洞(<http://www.trade-van.com/index.do?act=edmArticle&articleId=7>)。

Shellshock漏洞的影響範圍包括了絕大部份的Unix-like系統，若系統預設shell是以Bash執行，利用特殊的字串，讓伺服器在讀取使用者輸入的字串時造成解析錯誤，便可在特殊字串後直接執行任意指令。許多常見的Unix-like系統預設shell就是Bash，例如Redhat、CentOS…等，只要Bash的版本並未更新至最新，就可能被駭客利用。

作業系統預設shell：

|  |  |
| --- | --- |
| 作業系統 | 預設shell |
| CentOS | bash |
| RHEL | bash |
| Fedora | bash |
| MAC OS X | bash |
| SUSE | bash |
| Android | sh |
| FreeBSD | tcsh |
| Ubuntu | dash |

本次的漏洞利用Bash對環境變數上的解析，在環境變數中塞入惡意的程式碼後，讓Bash讀取，造成解析錯誤，則系統就會執行駭客所塞入的程式碼或指令，駭客就可以有作業系統的基本操作權限。駭客在攻擊前只有兩個重點，一是找到地方寫入環境變數，二是找到地方呼叫Bash，使其執行指令，只要達成這兩個條件，就可以攻擊成功。

　　但這次的漏洞也不需要特別的恐慌，只要注意幾個重點，就可以降低被攻擊的風險。

一、升級Bash版本至最新版本。

二、利用IPS、WAF設定阻擋攻擊行為。

三、利用防火牆或作業系統內建的防火牆如IPTable設定只允許信任的來源存取。

四、強化系統安全，例如啟用SELinux、AppArmor。

五、評估停止使用mod\_cgi、mod\_fastcgi。

六、注意網路設備及儲存設備是否有更新。

　　最後，除了以上幾點以外，同時要持續關注是否有新的更新檔或是新的攻擊手法，才能夠避免自己的系統遭受入侵，造成損失。

《關貿新聞》

本公司連前總經理鯤菁已於今年8月26日榮退，由原副總經理魏垚德接任總經理乙職，原副總經理職務，則暫由本公司通關服務群張陸生協理代理。

另本公司前何董事長鴻榮亦於今年9月23日因法人董事改派，由行政院政務顧問施明豪先生接任本公司董事長。

《關貿新聞》

本公司最新官方網站改版囉！

為提供更完善的服務，本公司官網於今年5月改版完成，歡迎大家多多利用！如有任何建議歡迎指教！



本公司官網網址為<http://www.trade-van.com>

提醒您：為獲得最佳瀏覽效果，建議使用Google Chrome、Fire Fox瀏覽器，如使用IE瀏覽器，請升級至9.0以上，謝謝您！