如何防範資料庫遭隱碼攻擊

一個美國男子把自己的姓改為Null，就可以免費租車、免費住旅館，這麼「好」的事情，是電腦誤判，還是人為疏失？

（資料來源：法務部調查局清流雙月刊 2016 年 5 月號）

◎科技大學資訊管理系講師 魯明德

最近有一則新聞曝光度很高，一直在Facebook 上被人轉貼，話說一位美國男子，把自己的姓改成Null，不但可以免費租了2 次車，還免費住了7 次旅館，甚至於去治療牙齒也不用付錢，因為他的姓會讓電腦誤判，而通過驗證。

科技新貴小潘也看到了這則新聞，想到自己的公司最近正在投入跨境電商的業務，如果使用者能把自己的名字改成特定字，就可以進入資料庫，對於未來自己的電商系統的資料安全，豈不是一大風險。於是，小潘決定利用清明假期中的師生下午茶約會，把這個問題提出來，看看有沒有什麼方法解決。司馬特老師喝口咖啡，先針對這個事件發生的可能性進行剖析。

一般的管理資訊系統一定會有資料庫來儲存資料， 資料庫都有結構化的查詢語言(Structural Query Language, SQL)，提供程式開發人員運用它的指令做資料查詢之用，當資料庫設計有缺陷時，就可能會有安全漏洞發生在應用程式的資料庫內層，如果漏洞在系統做弱點偵側時沒有被發現，就有可能在未來系統上線後，遭到有心人士的入侵。

除了國外的這個案例之外，無獨有偶地， 國內近期也有相關的報導發生， 像2015年底就有傳出戶政事務所的系

統有4 處SQL Injection 漏洞，2016 年4 月日盛證券的網站系統也發現SQL Injection 漏洞，導致數億筆資料可能洩漏。

這些事件都是有心人士利用資料庫的安全漏洞，在輸入的字串中夾帶SQL 指令，當系統的程式疏忽沒有檢查時，這些被夾帶的指令就會被資料庫伺服器誤認為是正常的SQL指令而被執行，系統就遭到入侵或破壞，也就是大家所習稱的SQL Injection，中文又稱為隱碼攻擊。

小潘趁著司馬特老師喝咖啡的空檔，抓到機會趕快問：一旦系統遭到隱碼攻擊，會有什麼後果？司馬特老師接著解釋，系統遭到隱碼攻擊，輕者可能會造成資料表中的資料外洩，像客戶資料、密碼…等。也可能會在攻擊中取得資料庫結構或管理員的帳號，足以日後再對資料庫做下一波的攻擊。嚴重者，駭客在取得較高的系統權限後，可以在網頁中加入惡意連結，也可以修改或控制作業系統，甚至於破壞硬碟、癱瘓整個系統。

小潘聽到這裏，對隱碼攻擊已經有了個初步的概念，但是應該要怎麼防範呢？司馬特老師說一般人會以為隱碼攻擊只會針對微軟的SQL Server 做攻擊，其實不然，只要是支援SQL 指令的資料庫伺服器，都有可能會遭到隱碼攻擊。

因此，為防範系統遭到隱碼攻擊，首先在應用程式要存取資料庫時，就要設下第一道防線，把系統的使用者與管理者的權限分開,對於應用系統的使用者,不要賦予可以建立、修改、刪除資料庫的權限，以減少隱碼攻擊帶來的損害。

其次，要加強對使用者輸入資料的內容做檢核、驗證，

可以利用現有的內容驗證工具或建立一些驗證規則，針對使用者輸入一些特殊的字元，先行過濾掉，讓那些惡意攻擊的SQL 語法無法執行。

除了對使用者設限外，系統設計時也要配合隱碼攻擊做防護，以往程式設計都習慣使用動態字串結合的方式，來組成查詢語法，無形中提供了駭客一個舞台，如果使用者輸入的查詢變數，不要直接放到SQL 查詢語法中，而是改成參數來傳遞，或者是使用SQL Server 內建的安全參數，也可以避免駭客輸入攻擊語法。

目前很多網站的架設，都是採用3-tier 或N-tier 的架構，因此，在每一tier 上的驗證就很重要，系統的設計不能只在最外層驗證成功，就讓使用者可以長驅直入，為了避免隱碼攻擊，每一tier 都應該要做驗證，驗證不通過就要立刻採取行動，才不會讓駭客輕易的入侵。

最後，要運用弱點掃描工具來協助系統開發人員，有效的發掘可能造成隱碼攻擊的漏洞，適時的加以修復，如果系統開發人員、資料庫管理人員及資安人員能夠對資安漏洞事前防範，駭客就不易侵入。

這個月的師生下午茶約會，就在華燈初上伴隨著濃濃的焦糖瑪琪朵香味中，漸漸進入尾聲，小潘聽了司馬特老師的說明，心想著等上班後，一定要對自己的系統先做個弱點掃描，了解那裏有漏洞，趕快來補強，以免日後不知不覺中遭到隱碼攻擊，造成不可彌補的損害。

法務部矯正署臺南監獄政風室提醒您