使用 NoSQL 資料庫
就可避免 SQL 資料隱碼攻擊了嗎？

撰稿/翻譯整理：叡揚資訊資訊安全事業處 產品顧問 卓立民

引用/參考資料：

Web App Security: http://www.idontplaydarts.com/2010/07/mongodb-is-vulnerable-to-sql-injection-in-php-at-least/

Fortify blog: http://blog.fortify.com/blog/2011/04/27/NoSQL-no-SQL-injections

每一家企業或多或少會使用資料庫來管理不同的資料，小規模資料量可能使用 Microsoft Excel、Access 這類的檔案格式，大量資料則可能採用以結構化查詢語言(SQL Structure Query Language)為基礎的關聯式資料庫管理系統(RDBMS Relational Database Management System)。

隨著時間的流逝，資料庫的資料量與日遽增，為了解決資料庫在進行大量資料存取時，所衍生出效能、後續擴充與維護…等問題，於是 Google 自行研發 BigTable，Facebook 開發出 Cassandra 資料庫，微軟 Windows 雲端平臺使用 NoSQL（No Only SQL，翻譯成「不只是 SQL」）技術來存取資料。為什麼這些國外大型網站紛紛捨棄存在已久的關聯式資料庫，而改用 NoSQL 資料庫呢？其原因，不外乎為了提升查詢效能、增加擴充彈性與備援(Redundancy)、降低建置成本。

維基百科(Wikipedia)對 NoSQL 的解釋是：NoSQL 資料庫是一個廣泛的資料庫管理系統(Database Management System)統稱，在某些方面與傳統的關聯式資料庫管理系統有顯著的不同，例如：可能不需要固定的資料表與結構描述(Schema)，經常會避免連結(Join)操作以及水平延展。一言以蔽之，NoSQL 資料庫泛指哪些非關聯式資料庫、不採用標準 SQL 語法的資料庫技術，這包括了數十多種不同類型的資料庫系統，例如 MongoDB 資料庫。NoSQL 資料庫大致上可以分成 8 種，請見表 1。

GSS 叡揚資訊 Galaxy Software Services
台北總公司：台北市 10461 中山區德惠街 9 號 5 樓 TEL：(02)2586-7890 FAX：(02)2586-8787
高雄辦公室：高雄市明華路 315 號 13 樓之 3 TEL:(07)586-6195
海外據點：上海、北京、東京

表 1

分類	產品名稱
文件 (Document)	Lotus Notes MongoDB
圖形 (Graph)	AllegroGraph DEX
鍵值儲存 (Key-value store)	Cassandra GT.M
託管服務 (Hosted services)	BigTable Oracle Coherence
多值 (Multivalue)	OpenQM OpenInsight
物件 (Object)	db4o GemStone/S
排序鍵值儲存 (Ordered key-value store)	Berkeley DB IBM Informix C-ISAM
表格 (Tabular)	BigTable Hadoop
原組儲存 (Tuple store)	Apache River

針對 NoSQL 資料庫是否容易受到類似 SQL 資料隱碼攻擊的課題，有些迷思出現。畢竟，我們要怎麼在那些不使用 SQL 的資料庫，進行資料隱碼攻擊呢？以 MongoDB 為例，沒有採用 SQL 風格的 SELECT 語法進行資料庫查詢操作，雖然在該資料庫的常見問題中，也一直強調：「一般來說，於使用 MongoDB 時，我們並不是用字串來組出查詢指令，所以**傳統**的 SQL 資料隱碼攻擊不會是一個問題。」這樣的說法，就技術的角度來說，是對的，但會有些誤導。很多人會曲解其原意為，就所有其他類型的隱碼攻擊而言，這樣是安全的，但卻沒有注意到那句話的關鍵字：**「傳統」**。

讓我們來看看 SQL 資料隱碼攻擊的手法。SQL 結構化查詢語法會包含資料（例如，欄位名稱）以及指令碼（比方說，查詢操作、篩選條件）。而 SQL 資料隱碼攻擊發生在沒有轉換逸出的中繼(Meta)字元，常見的字元是單引號，駭客即可讓解析器把內涵逸出字元的資料視為指令碼。簡單地說，資料隱碼攻擊是因為語法中，包含了要操作資料庫所需的指令碼，而這些指令碼卻沒有適當地處理逸出的中繼字元。由此我們可以理解為什麼 NoSQL 資料庫也會有受到此類攻擊的問題。NoSQL 資料庫的查詢語言，不論如何，勢必會包含資料與指令碼。只要駭客可以在資料字串中，強制切換資料與邏輯的內容，即會有隱碼攻擊。

GSS 叡揚資訊 Galaxy Software Services
台北總公司：台北市 10461 中山區德惠街 9 號 5 樓　TEL：(02)2586-7890　FAX：(02)2586-8787
高雄辦公室：高雄市明華路 315 號 13 樓之 3　TEL:(07)586-6195
海外據點：上海、北京、東京

換句話說，明確地不使用 SQL，並不能讓 NoSQL 資料庫免於其他來自於本身的查詢語言所引發的隱碼攻擊，而確保其資料庫的安全

來看一下 Amazon Web Service 的 SimpleDB 服務，系採用 SQL 風格的 SELECT 語法。以下面的程式碼片段為例，應用程式會讓已經通過驗證的客戶，根據他們所指定的產品類別來查詢相關的發票資料：

```
AmazonSimpleDBClient sdbc =
    new AmazonSimpleDBClient(appAWSCredentials);
String query = "select * from invoices where productCategory = '"
    + productCategory + "' and customerID = '"
    + customerID + "' order by '"
    + sortColumn + "' asc";
SelectResult sdbResult = sdbc.select(new SelectRequest(query));
```

應用程式執行時，會把相關的字串填入，例如要查詢客戶編號是 12345 所採購的筆記型電腦產品之發票資料，並依照價格進行升冪排序，所以上面那段的 query 程式碼會變成（換行是為了便於閱讀）：

```
select * from invoices
where productCategory = 'Notebook'
and customerID = '12345'
order by 'price' asc
```

假設駭客在產品類別的字串，送出 Notebook' or productCategory = \"，並且在排序方式中，填入\" order by 'price，此時程式碼會變成什麼樣的結果呢？SimpleDB 會把他們解釋成這樣（換行是為了便於閱讀）：

```
select * from invoices
where productCategory = 'Notebook'
or productCategory = "' and customerID = '12345' order by '"
order by 'price' asc
```

請注意，此時 customerID = '12345'子句會完全被忽略掉，因此駭客便得以查詢到所有訂購筆記型電腦的客戶發票資料。

GSS 叡揚資訊 Galaxy Software Services
台北總公司：台北市 10461 中山區德惠街 9 號 5 樓 TEL：(02)2586-7890 FAX：(02)2586-8787
高雄辦公室：高雄市明華路 315 號 13 樓之 3 TEL:(07)586-6195
海外據點：上海、北京、東京

使用類似 SQL SELECT 語法的資料庫，並不是唯一會遭受隱碼攻擊的資料庫。回到先前提到的 MongoDB，在 Phil 的 Web App Security 部落格 Mongodb is vulnerable to SQL injection in PHP at least (http://www.idontplaydarts.com/2010/07/mongodb-is-vulnerable-to-sql-injection-in-php-at-least/) 一文，提到如下的 MongoDB 查詢範例：

```
$collection->find(array(
    "username" => $_GET['username'],
    "passwd" => $_GET['passwd']
));
```

如果駭客在網址列，輸入 login.php?username=admin&passwd[$ne]=1 這樣的 URL，會發生什麼事情？在這個例子中，PHP 會自動將傳入的 passwd[$ne]=1 轉換成關聯陣列(Associative Array)，因此組出如下的查詢：

```
$collection->find(array(
    "username" => "admin",
    "passwd" => array("$ne" => 1)
));
```

換句話說，該查詢將傳回每一位密碼不是 1 的 admin 使用者，由於 admin 的密碼不可能是設定為 1，因此這個查詢會顯示所有 admin 的相關資料。

本文所要傳達的重點在於，千萬不要假設軟體是安全的，因為似乎沒有任何軟體會包含我們所熟知的全部攻擊弱點。不論這樣的建議已經被提出多少次，但總還是值得一提再提，那就是：不要相信使用者所輸入的任何資料，永遠要驗證使用者的輸入！

GSS 叡揚資訊 Galaxy Software Services
台北總公司：台北市 10461 中山區德惠街 9 號 5 樓 TEL：(02)2586-7890 FAX：(02)2586-8787
高雄辦公室：高雄市明華路 315 號 13 樓之 3 TEL:(07)586-6195
海外據點：上海、北京、東京