# 如何預防 SQL Injection 的攻擊

撰稿：叡揚資訊資訊安全事業處 產品顧問 林柏齊

SQL Injection 資料隱碼攻擊的駭客攻擊手法，一直以來都高居 OWASP Top10 的前兩名，有關於如何有效防範其攻擊的相關文件與技術討論，在網路甚至資安論壇，討論都非常激烈。最近卻發現仍然有許多 programmer 還是不清楚其攻擊的原理，在安全性問題的管理控制方式也沒有抓到重點，許多網站應用系統在開發時仍然漏洞百出，其主要的原因不外乎是架構鬆散，程式人員偷懶或早期撰寫程式碼的習慣不改的緣故。

在這種攻擊方式中，攻擊者會將一些惡意資料庫查詢語法，輸入到開發者使用的程式碼中。然後透過各種方式將該字串傳遞到如 MS SQL Server 資料庫的查詢命列中進行分析和執行。只要這個惡意字元或語法符合 SQL 查詢語法的規則，在應用系統的編譯與執行階段時，就不會被編譯工具或執行階段工具發現。資料庫伺服器則會直接執行被竄改過的攻擊語法，對資料庫系統或儲存的資料，造成極大的威脅。因此，SQL 隱碼攻擊的危害是非常大的，那身為一個稱職的資料庫管理員或者開發人員該如何來防範呢？下面這些建議對相關人員預防 SQL 資料隱碼攻擊將非常有助益。

## 1．應用系統中存取資料庫時，應明確定義存取資料庫的使用者權限

假設一個普通用戶在 SQL 查詢語法中，嵌入一個 Drop Table 語句，那麼是否允許執行呢？由於 Drop 語法關係到資料庫的基本物件，因此操作這個語句用戶必須有相對應的操作權限。在允許的權限中，對於終端使用者，即應用系統的操作者，除非必要，不需要賦予資料庫物件的建立、刪除等相關權限。即使在使用 SQL 語句中，被植入帶有惡意的操作語法或程式碼。由於因為權限管控嚴謹，對使用者的操作限制，這些惡意的動作也將無法被執行。故應用程式在存取架構設計時，最好把系統管理員的使用者與普通使用者區分開來。如此，可以最大幅度降低 SQL Injection 資料隱碼攻擊對資料庫系統帶來的損害。

## 2．採用參數化（Parameterized）查詢語法

一般 SQL Injection 資料隱碼攻擊，是利用傳統習慣使用動態字串結合的方式，來組合成查詢語法，並將查詢語法結合程式碼，針對資料庫系統進行查詢或操作。因此，就給了駭客一個竄改資料並植入攻擊字串的機會。若能在撰寫 SQL 查詢語法時，使用者輸入的變數不是直接動態結合到 SQL 查詢語法，而是通過參數來傳遞這個變數的話，那麼就可以有效的避免 SQL Injection 資料隱碼攻擊。

換句話說，使用者的輸入絕對不能夠直接被結合到 SQL 查詢語法中。避免此類情形發生的作法，在針對使用者的輸入內容必須進行過濾，或者使用參數化的查詢方式，來傳遞使用者輸入的變數。參數化的查詢語法，在使用參數時，是把整個參數當成查詢資料，而不是將使用者輸入變數當成查詢的語法，因此就可以有效避免惡意



GSS 叡揚資訊 Galaxy Software Services 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787

使用者輸入攻擊語法。採用這種措施，可以杜絕大部分的 SQL Injection 資料隱碼的攻擊。不過可惜的是，現在支援參數化語句的資料庫系統並不多。不過，如果在資料庫系統支援的情況下，開發人員在開發應用系統時要儘量採用參數化查詢的方式來設計系統。

## 3．加強對用戶輸入資料的檢核與驗證

一般總體來說，防範 SQL Injection 資料隱碼攻擊可以採用兩種方法，一是加強對使用者輸入資料內容的檢核與驗證；二是強迫使用參數化語句來傳遞使用者輸入的內容。在 SQL Server 資料庫中，有許多的使用者輸入內容驗證工具，管理員可以使用來對付 SQL Injection 資料隱碼攻擊。例如對字串變數的內容進行測試：只接受所需的值、拒絕包含二進位資料、Escape 跳脫字元和注釋字元等一些容易造成攻擊的特殊字元過濾與驗證。這些動作有助於防止不當攻擊語法的植入，並且可以預防某些緩衝區溢位攻擊等相關手法。有效地測試使用者輸入內容的大小和資料類型，強制進行適當的限制與轉換，對於有效地防止攻擊手法有意造成的緩衝區溢位，以及資料隱碼攻擊有比較明顯的效果。

也可以使用一些過濾規則來驗證使用者的輸入，像是針對對使用者輸入的變數進行字元過濾，如拒絕一些特殊的符號。在某些惡意攻擊的程式碼中，只要還沒有進行查詢前，把特殊符號如單引號( ‘) 、分號(;)、注釋符號(--)過濾掉，那惡意攻擊的查詢語法，也就沒有用武之地了。在執行 SQL 語句之前，可以通過資料庫的驗證規則，來拒絕或允許一些特殊的符號的執行。

在不影響資料庫應用的前提下，應該讓資料庫拒絕包含以下字元的輸入，例如分號分隔符號(;)以及注釋分隔符號(-)，在 SQL Injection 資料隱碼攻擊手法中，經常使用這個符號將作為主要的幫兇。注釋符號只有在資料設計的時候，使用的機率才會比較高。一般使用者的查詢語句中，並沒有一定要使用注釋的內容，因此針對這個字元，直接進行過濾或拒絕輸入，通常使用這個方式，並不會發生重大的意外損失。把以上這些特殊符號拒絕掉，對於預防 SQL Injection 資料隱碼攻擊，將有非常大的助益。總而言之，透過測試資料的類型、長度、格式和範圍來驗證使用者輸入的資料，並且過濾使用者輸入的內容，這是防止 SQL Injection 資料隱碼攻擊的最常見且達到某些效果的防範措施之一。

## 4．盡量使用 SQL　Server 資料庫內建的安全參數

為了減少 SQL Injection 資料隱碼攻擊 對於 SQL Server 資料庫的不良影響，微軟在 SQL Server 資料庫中，專門設計一些相對安全的 SQL 參數提供給管理者使用。在資料庫設計過程中，開發人員要儘量採用這些參數來杜絕惡意的 SQL Injection 資料隱碼攻擊。

例如，在 SQL Server 資料庫中提供了 Parameters 集合。這個集合提供了資料型別檢查和長度驗證的功能。如果資料庫管理員採用了 Parameters 這個集合的話，則使用者輸入的內容將被視為資料如字元值，而不是資料庫執行的相關語法。即使使用者輸入的內容中含有可執行的程式碼，資料庫系統也會過濾掉。因為，資料庫只會



GSS 叡揚資訊 Galaxy Software Services 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787

把這個語法當作普通的字元來處理與過濾。使用 Parameters 集合的另外一個優點是可以強制執行資料型別和長度檢查，如果有不符合或者超出範圍以外的資料值將觸發例外錯誤。如果用戶輸入的值不符合指定的類型與長度約束，就會發生例外錯誤，並報告給管理員。如應用系統中，員工編號所定義的資料型別為字串，長度為 10 個字元。而使用者輸入的內容雖然也是字元型別的資料，但是其長度達到了 20 個字元。則此時就會引發系統例外錯誤，因為使用者輸入的內容長度超過了資料庫欄位長度的限制，資料庫管理者馬上可以針對這些例外狀況，進行對應的處理。

## 5．在 N-Tier 的架構下，如何有效預防 SQL Injection 資料隱碼攻擊

現今很多網際網路型的應用程式，大多採用 3-Tier 或者 N-Tier 的應用系統架構，在多層次應用架構中，使用者輸入的所有資料，都應該在驗證之後才能被允許進入到可以信任的資料區域。未通過資料驗證程序的資料應被在執行資料庫任何動作前被拒絕，並向上一層傳回錯誤資訊。

如何有效實現應用系統中多層的資料驗證，針對沒有目的的惡意使用者採取的被動預防措施，對有意且強大的惡意攻擊者防護性會較低。如此，更好的做法是在使用者介面和所有多層跨界面邊界上，對於資料輸入的驗證，就非常重要。如在用戶端應用程式中驗證資料可以防止簡單的攻擊語法輸入。但是，如果下一層認為其輸入已通過驗證，則任何可以繞過用戶端的惡意用戶就可以不受限制地存取下一層的系統資源。故對於多層次應用環境，在防止資料隱碼攻擊的時候，需要每一層都要重視，在用戶端與資料庫端的界面都要採用相應的措施來防範 SQL Injection 資料隱碼攻擊。

## 6．使用專業的程式碼弱點掃描工具來尋找應用系統所隱含的漏洞

使用專業的程式碼弱點掃描分析工具如白箱工具，可以快速且有效地協助應用系統開發人員來尋找所有可能造成 SQL Injection 資料隱碼攻擊的攻擊程式碼區域。開發人員發現弱點後，可以借助工具的修復建議對應用系統設計上的弱點，進行有效地修復，徹底改變不安全程式碼撰寫習慣，進而從根本下手，改進並加強應用系統的安全強度。這一類工具，雖然能有效地發現並找出攻擊弱點，而不能夠主動起到防禦 SQL 資料隱碼攻擊的作用，但是卻能使應用系統的開發人員，更重視因程式碼不夠安全，對整個系統所帶來的危害。

除此之外，還有相關弱點分析工具如黑箱工具，也可以協助使用者發現應用系統中的弱點，但不能很明確地指出弱點所在的程式碼，市場上已經有業者透過黑白箱工具的限制以及優點，進行弱點問題的整合與管理，可以大大地協助使用者發現弱點，並進行修復這一類工具也經常被駭客拿來使用。如駭客可以利用這個工具自動搜索攻擊目標並實施攻擊。因此在必要的情況下，企業應當投資於一些專業的弱點掃描工具。

一個完善的弱點掃描軟體工具不同於網路掃描程式，它可以專門挖掘資料庫中的 SQL 資料隱碼攻擊的漏洞。甚至，最新的弱點掃描程式可以查找最新發現的資料庫系統的相關漏洞。所以憑藉專業的工具，可以有效地幫助



GSS Galaxy Software Services 叡揚資訊 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787

資料庫管理員以及應用系統開發人員，發現 SQL 資料隱碼攻擊的漏洞，並提醒管理員採取積極的措施來預防 SQL 資料隱碼攻擊。如果攻擊者能夠發現的 SQL 資料隱碼攻擊，資料庫管理員、開發人員以及資安管控人員都能事先發現並採取積極的防範措施來堵住漏洞，那麼他們也就無從下手了。

## 結論

對於 SQL 資料隱碼攻擊對資料庫系統所造成的危害，大家應該都能很清楚地了解其嚴重程度。因此，對於 SQL 隱碼攻擊的防範措施，透過上面幾點的做法，對資料庫管理員、開發人員以及其他相關人員，在進行資料庫系統安全管理與防禦，是相當有效的，也是目前業界一些比較主流的作法。



GSS 叡揚資訊 Galaxy Software Services 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787