

第六堂 與程式間的合作

聯成電腦

張明泰 mtchang.tw@gmail.com





PHP與MySQL

- 複習：
- 確定自己的PHP及MySQL環境可以RUN。
- 講解複習預存程序。
- 工欲善其事必先利其器

<http://notepad-plus.sourceforge.net/uk/site.htm>



PHPMYADMIN

- 官方網站：
http://www.phpmyadmin.net/home_page/index.php
- 設定組態？ Config.default.php
- 操作...
- 教學文件：
<http://groups.google.com.tw/group/lccnetsql>
已有放置swf教學動畫檔



使用**PHP**讀取**MySQL**資料庫

```
<? # mysql_query.php檔案
# 設定mysql的連線ID
$conn = mysql_connect("localhost", "mtchang", "qw") or die("Could not connect");
# 設定再查詢mysql使用的字元編碼為UTF-8。很重要，沒設定出來會都是亂碼
mysql_query("SET NAMES 'utf8'");
# 選取資料庫
mysql_select_db("mtchang", $conn);
# 設定SQL敘述
$sql = "select * from students";
# 將SQL敘述傳給SQL server查詢，並節回傳結果放在變數$result
$result = mysql_query($sql);
# 計算此SQL表格有多少欄位
$numfields = mysql_num_fields($result);
# 迴圈，讀取$result裡面的內容，直到空為止
while ($row = mysql_fetch_row($result))
{
    # 迴圈，讀取列。依據欄位數顯示row值
    for($i = 0 ; $i < $numfields ; $i++)
    {
        echo $row[$i] . " ";
    }
    # html的斷行
    echo "<br />";
}
?>
```



練習：

- 請練習使用上頁範例程式，**改變SQL敘述及你的SQL server設定值**並輸出到網頁上。
- 請配合**SQL的limits**指令，限制輸出的row，並嘗試做到**分頁**的效果。



休息一下





改成表單**POST**傳值

(1)修改mysql_query.php最前面加入表單語法

```
<form enctype="multipart/form-data" action="mysql_inject.php"
method="post" name="mysql-test" target="_self">
<input name="query" type="text" value="" size="60" maxlength="300" />
<input type="submit" name="Submit" value="送出" />
</form>
```

(2)修改\$sql

將原本的 \$sql = "select * from students";

修改成爲 **\$sql=\$_POST['query'];**

接受來自於表單的值



一個**PHP**的例子**SQL- Injection**

- 我們修改一下剛剛表單輸入的程式，讓他成爲一個可以判斷學號是否正確的程式。

```
# 修改這行....設定SQL敘述
```

```
$sql='SELECT * FROM students WHERE 學號='.$_POST['query'].';';
```

```
# 在這行下面加入判斷式
```

```
$result = mysql_query($sql);
```

```
# 如果yes代表學號通過驗證，no代表不通過
```

```
if($result)
```

```
    echo "yes<br />";
```

```
else
```

```
    echo "no<br />";
```




SQL入侵練習與防範

- 上述範例如何讓他被SQL Injection ?
- 『資料隱碼』SQL Injection的源由與防範之道
- http://www.microsoft.com/taiwan/sql/SQL_Injection.htm
- SQL Injection (資料隱碼)– 駭客的 SQL填空遊戲
- http://www.microsoft.com/taiwan/sql/SQL_Injection_G1.htm



『資料隱碼』SQL Injection的源由與防範之道

- 利用特殊指令攻擊
- 駭客於任何要求輸入資料時打入特殊指令或程式碼，讓破壞性程式碼『隱藏』在標準的SQL程式中，達到其攻擊目的。
- 利用系統的錯誤訊息找出資料庫弱點
- 要對資料庫進行存取或修改，必需要對資料庫的結構有所瞭解，通常駭客很難瞭解資料庫結構，但未經掩飾的錯誤訊息反而容易造成問題。資料庫管理系統為能協助 程式開發與管理人員了解錯誤指令所造成的問題與根源，會在錯誤訊息上顯示完整的資訊，若電子商務系統未經防範而直接讓錯誤訊息顯示在網頁上，無異是給駭客 入侵留下線索。
- 為能有效的阻絕駭客利用『資料隱碼』方式入侵，微軟建議採取以下各項防範之道：
- 1. 加強程式上的安全檢查措施：在程式中加上輸入資料型態檢查、資料長度檢查與資料內容檢查，讓駭客無法利用隱藏於輸入資料的特殊指令或程式碼有機可乘。
- 2. 妥善使用權限管理：在程式中勿用較高權限來存取資料庫，比如說讓SQL程式使用資料庫管理員(System Administrator, SA)身份來存取資料庫。此外，若使用Windows 2000作業系統搭配SQL Server則建議使用Windows 2000認證機制。
- 3. 保持良好的程式開發習慣：撰寫資料庫存取或查詢程式時，利用兩個單引號『』來標註任何輸入的變數給SQL程式；利用單引號『』會讓駭客的隱碼易於得逞。
- 4. 將核心程式碼隱藏起來：勿讓網頁上程式直接存取或查詢資料庫，而是透過預存程式(Stored-procedure)來執行，而XML Web Service也是另一個提高安全性的好方法，保護核心程式邏輯與資料庫結構不至外洩，而Microsoft SQL Server 2000是目前唯一支援XML Web Service的資料庫管理系統。
- 5. 以標準的訊息回覆給客戶：電子商務網站對於任何回覆給客戶的訊息應有所規範，透過程式攔截下任何作業系統或資料庫管理系統所可能產生的錯誤訊息，改以統一且明確的訊息來指導客戶。
- 6. 刪除多餘的資料表(Table)：資料庫管理系統安裝後會有幾個既存的資料表，這些資料表是供程式開發、範例資料庫或暫存使用，如“pub”及“Northwind”等，請在電子商務網站上線後移除；因為這些公用的資料表架構是公開的，易為駭客所利用。



休息一下





變更欄位的結構

- 範例：**alter table test add writer varchar(30);**
- 說明：新增一個varchar(30)的欄位writer於test資料庫中
- 範例：**ALTER TABLE test ADD writer2 VARCHAR(30) DEFAULT 'ANK';**
- 說明：新增一個varchar(30)的欄位writer於test資料庫中並且設定其預設值為「ANK」



變更欄位的結構-2

- 範例：**ALTER TABLE `test` DROP `writer`**
- 說明：刪除write欄位



追加限制條件

- 範例：**ALTER TABLE `test` ADD PRIMARY KEY (學號);**
- 說明：在SQL中可以追加primary key, UNIQUE, check

結論：系統管理盡量用工具

127.0.0.1 / localhost / mtchang / test | phpMyAdmin 2.7.0-pl2 - Mozilla Firefox

檔案(F) 編輯(E) 檢視(V) 瀏覽(G) 書籤(B) 工具(T) 說明(H)

http://127.0.0.1/myweb/mysql_admin/index.php?lang=zh-tw-utf-8&server=1&collation_connecti





























































mtchang 常用文件網站 下載 最近焦點 快速搜尋 127.0.0.1 - /myweb/ Yahoo!奇摩 Google 電子化政府入口網

Google 吳佳諺 搜尋 PageRank ABC 檢查 選項 吳佳諺

127.0.0.1 - /myweb/sql/mt... Linux Company 127.0.0.1 / localhost / ... 博客來書籍館 SQL Injection (資料隱碼...)

localhost ▶ mtchang ▶ test "InnoDB free: 10240 kB"

結構 SQL 搜索 依範例查詢 (QBE) 輸出 Import 管理 權限 刪除

	資料表	執行	記錄	型態	校對	大小	多餘
<input type="checkbox"/>	conduct	    	479	InnoDB	utf8_general_ci	48.0 KB	-
<input type="checkbox"/>	customer	    	60	InnoDB	utf8_general_ci	16.0 KB	-
<input type="checkbox"/>	dept	    	17	InnoDB	utf8_general_ci	16.0 KB	-
<input type="checkbox"/>	employee	    	97	InnoDB	utf8_general_ci	16.0 KB	-
<input type="checkbox"/>	exp	    	97	InnoDB	utf8_general_ci	16.0 KB	-
<input type="checkbox"/>	leave	    	83	InnoDB	utf8_general_ci	16.0 KB	-
<input type="checkbox"/>	overtime	    	110	InnoDB	utf8_general_ci	16.0 KB	-
<input type="checkbox"/>	person	    	97	InnoDB	utf8_general_ci	16.0 KB	-
<input type="checkbox"/>	product	    	20	InnoDB	utf8_general_ci	16.0 KB	-
<input type="checkbox"/>	quota	    	16	InnoDB	utf8_general_ci	16.0 KB	-
<input type="checkbox"/>	quotat1	    	16	InnoDB	utf8_general_ci	16.0 KB	-
<input type="checkbox"/>	records	    	300	InnoDB	utf8_general_ci	48.0 KB	-

phpMyAdmin

資料庫

mtchang (19)

- conduct
- customer
- dept
- employee
- exp
- leave
- overtime
- person
- product
- quota
- quotat1
- records
- sales
- sales1
- sales2
- students
- test



感謝各位

<http://groups.google.com.tw/group/lccnetsql>

<msn/email:mtchang.tw@gmail.com>



參考

- <http://www.books.com.tw/exep/prod/booksfile.php?item=0010313014>
- <http://www.books.com.tw/exep/prod/booksfile.php?item=0010317524>
- <http://www.books.com.tw/exep/prod/booksfile.php?item=0010284070>

