

網站應用程式弱點掃描— 修復學校網頁模組經驗分享

南投縣國姓國中 劉俊廷

Email : t18606@webmail.ntct.edu.tw

2013/09/27

有哪些修復方式？

彙整各種修復方式

1. 將單引號(')取代為\" : 'and'5'='5
2. 驗證輸入數字 : 789o不完全是數字
3. 驗證輸入數字或英文 : 234fdf@不完全是數字或英文
4. PHP5網管實驗室用PHP函數解決SQL injection :
'and'5'='5
5. 拒絕輸入特定符號(/.*[~`!@#%&||*()_+=|\\\\\\{[\\]:;'"<>.,\\.?\\V].*) :
 \$包含不允許的特殊符號

彙整各種修復方式

6. MySQL 可以使用 `mysql_real_escape_string()` 濾除跳脫字元：

`'and'5'='5`

`'\and\'5\'=\'5`

7. 檢查字元是否符合長度：(1) 輸入字元 `12345678`

(2) 字元長度 `9`

`12345678` 長度 `8` 未超過限定長度 `9`

有沒有簡單通用的方式？

如何開發夠安全的PHP網頁？ - IT邦幫忙::IT知識分享社群


- ▶ 我們建議採用資料庫提供的過濾函式，譬如MySQL可以使用`mysql_real_escape_string()`濾除跳脫字元，也免除了針對每個輸入都加上過濾函式的繁瑣工作。

SQL INJECTION修復實例

步驟一：查看弱點報告

網站結果		
網站名稱	檢測開始時間	狀態
南投縣立國姓國民中學	2013/8/30 下午 10:25:43	完成
南投縣立國姓國民中學	2013/8/30 下午 08:22:33	完成
南投縣立國姓國民中學	2013/8/29 下午 08:03:27	完成
南投縣立國姓國民中學學務系統	2013/8/2 下午 06:01:11	完成
南投縣立國姓國民中學	2013/8/2 下午 06:00:07	完成
南投縣立國姓國民中學學務系統	2013/8/31 下午 08:50:34	完成
南投縣立國姓國民中學	2013/8/31 下午 06:00:17	完成
南投縣立國姓國民中學學務系統	2013/1/10 下午 06:00:14	完成
南投縣立國姓國民中學(備用)	2013/1/10 下午 06:00:06	完成

步驟一：查看弱點報告

	弱點網址	弱點參數	XSS	SQL Injection	惡意檔案執行	不適當配置處理	目錄索引	備份檔案	檢測字串
1	http://www.khjh.ntct.edu.tw/school/discuss/perbasic.php	prgid		✓					檢視
2	http://www.khjh.ntct.edu.tw/school/pub/downfiles.php	relpath downfile		✓					檢視
3	http://www.khjh.ntct.edu.tw/school/schedule/show_calendar.php	id		✓					檢視
4	http://www.khjh.ntct.edu.tw/school/schedule/index.php	fm		✓					檢視
5	http://www.khjh.ntct.edu.tw/school/schedule/search_frm.php	show_kind		✓					檢視
6	http://www.khjh.ntct.edu.tw/school/discuss/search_frm.php	prgid		✓					檢視
7	http://www.khjh.ntct.edu.tw/school/schedule/month.php	year month		✓					檢視
8	http://www.khjh.ntct.edu.tw/school/netlink/index.php	parentid		✓					檢視
9	http://www.khjh.ntct.edu.tw/school/pub/rss.php	prgid		✓					檢視
10	http://www.khjh.ntct.edu.tw/school/discuss/index.php	prgid		✓					檢視


步驟一：查看弱點報告

▶ 判斷弱點畫面

問題網址列表					
項目	弱點網址	檢測字串	弱點類型	修補建議	判定弱點畫面
1	http://www.khjh.ntct.edu.tw/school/discuss/perbasi...	%27%61nd%275%27=%275	SQL Injection	檢視	檢視
2	http://www.khjh.ntct.edu.tw/school/discuss/perbasi...	%27%61nd%275%27=%275	SQL Injection	檢視	檢視

步驟一：查看弱點報告

▶ 複製弱點網址

弱點網址	http://www.khjh.ntct.edu.tw/school/discuss/perbasic.php?prgid=250 
網頁內容 [網頁預覽] [網頁原始碼]	檢測網址： http://www.khjh.ntct.edu.tw/school/discuss/perbasic.php?prgid=250%27%61nd%275%27=%275 <div style="text-align: center;"><input checked="" type="checkbox"/> 閱 ??</div> <p>?關 ?? ?餃 閱 ?? ? ? ? ?關餃? 露 ? 榮幹 ? ? 錫典? ?餃 蝟<?</p> <p>罷 ?? ??餃 閱 ??曝 ??臭誑?湔 ? 榮幹 ?曝?br>曉 銖 闖? ?亥?曉 ?? ?賴設 揮唾?</p> <p>撤 IV?餃 !</p>

步驟一：查看弱點報告

▶ 閱讀修補建議

問題網址列表					
項目	弱點網址	檢測字串	弱點類型	修補建議	判定弱點畫面
1	http://www.khjh.ntct.edu.tw/school/discuss/perbasi...	%27%61nd%275%27=%275	SQL Injection	檢視	檢視
2	http://www.khjh.ntct.edu.tw/school/discuss/perbasi...	%27%61nd%275%27=%275	SQL Injection	檢視	檢視

步驟一：查看弱點報告

▶ 修補建議

- ▶ 字元型參數注入點分析, 判斷是否存在SQL Injection漏洞, 直接從IE的URL網址列輸入資料, 如果加入'and'5'='5返回正常 (就是和原來沒有加'and'5'='5時頁面樣子的一樣), 而加入'and'5'='6返回錯誤 (和原來沒有加'and'5'='6時頁面的樣子不一樣), 就可以證明這個頁面存在SQL Injection漏洞。

步驟二：開啟網頁測試 ('AND'5'='5)

- ▶ 測試方式
 - ▶ 在網址變數後面加上 'and'5'='5
- ▶ 原始網址
 - ▶ <http://www.khjh.ntct.edu.tw/school/discuss/perbasic.php?prgid=250>
- ▶ 加上測試網址
 - ▶ <http://www.khjh.ntct.edu.tw/school/discuss/perbasic.php?prgid=250'and'5'='5>
- ▶ 加上測試網址
 - ▶ <http://www.khjh.ntct.edu.tw/school/discuss/perbasic.php?prgid=250'and'5'='6>

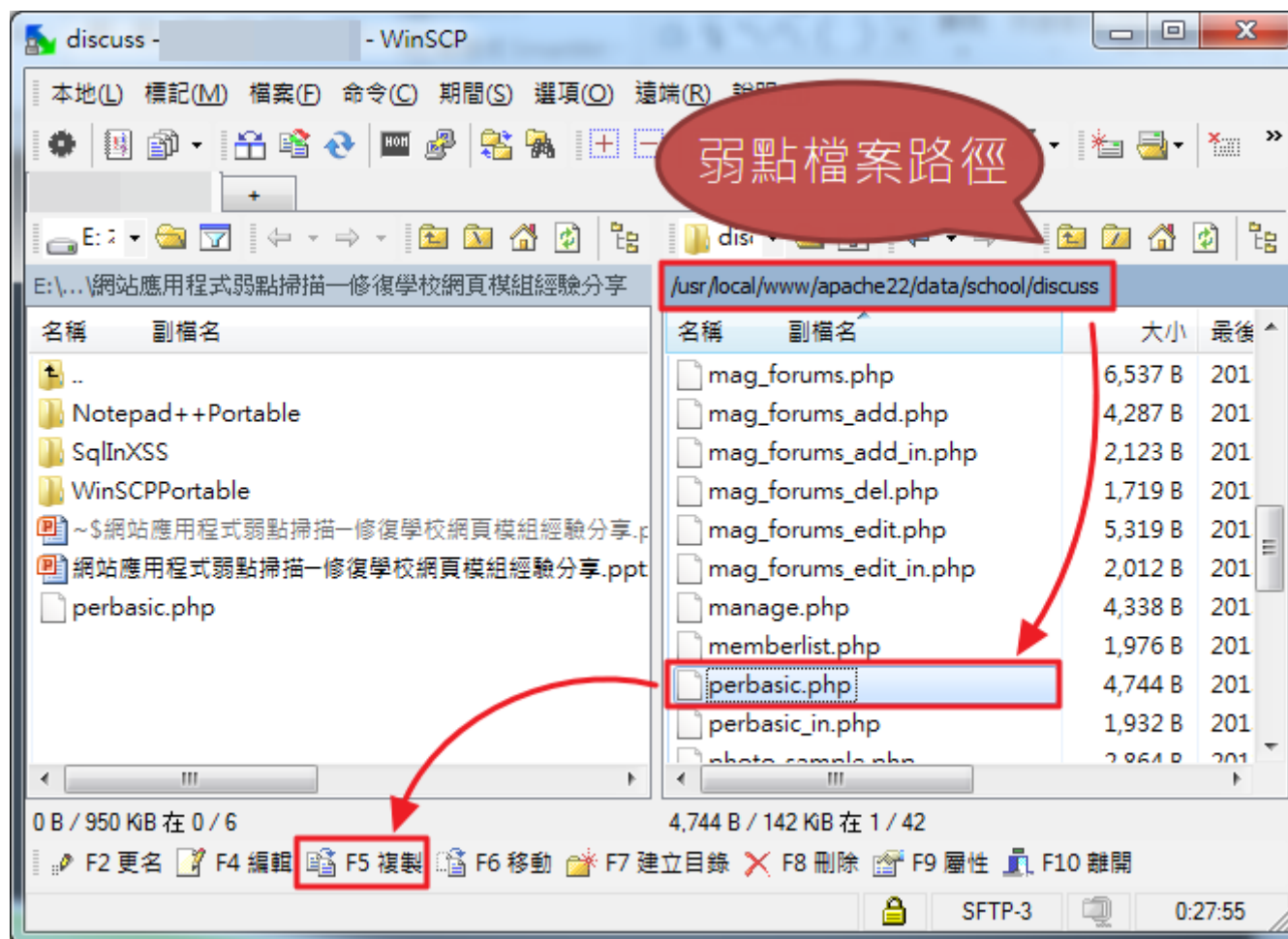
步驟三：下載要修復的網頁

► 3-1 根據弱點報告裡的弱點檔案路徑

弱點網址	http://www.khjh.ntct.edu.tw/school/discuss/perbasic.php?prgid=250 
網頁內容 [網頁預覽] [網頁原始碼]	檢測網址： http://www.khjh.ntct.edu.tw/school/discuss/perbasic.php?prgid=250%27%61nd%275%27=%275 <div style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <input checked="" type="checkbox"/> 閱 ?? </div> <p style="text-align: center;"> <input type="checkbox"/> 蟻 ?閩 ?? <input type="checkbox"/> ?餃 閩 ?? <input type="checkbox"/> ? ? <input type="checkbox"/> ? ?閩餃? <input type="checkbox"/> 露 ? 榮幹 ? <input type="checkbox"/> ? 錄典? <input type="checkbox"/> ?餃 蝟<? </p> <p style="text-align: center;"> 罷 ?? ??餃 閩 ??曝 ??臭誑?湔 ? 榮幹 ?曝?br>曉 銖 閩? ?亥?曉 ?? ?賴談 揮唾? 撤 IV?餃 ! </p>

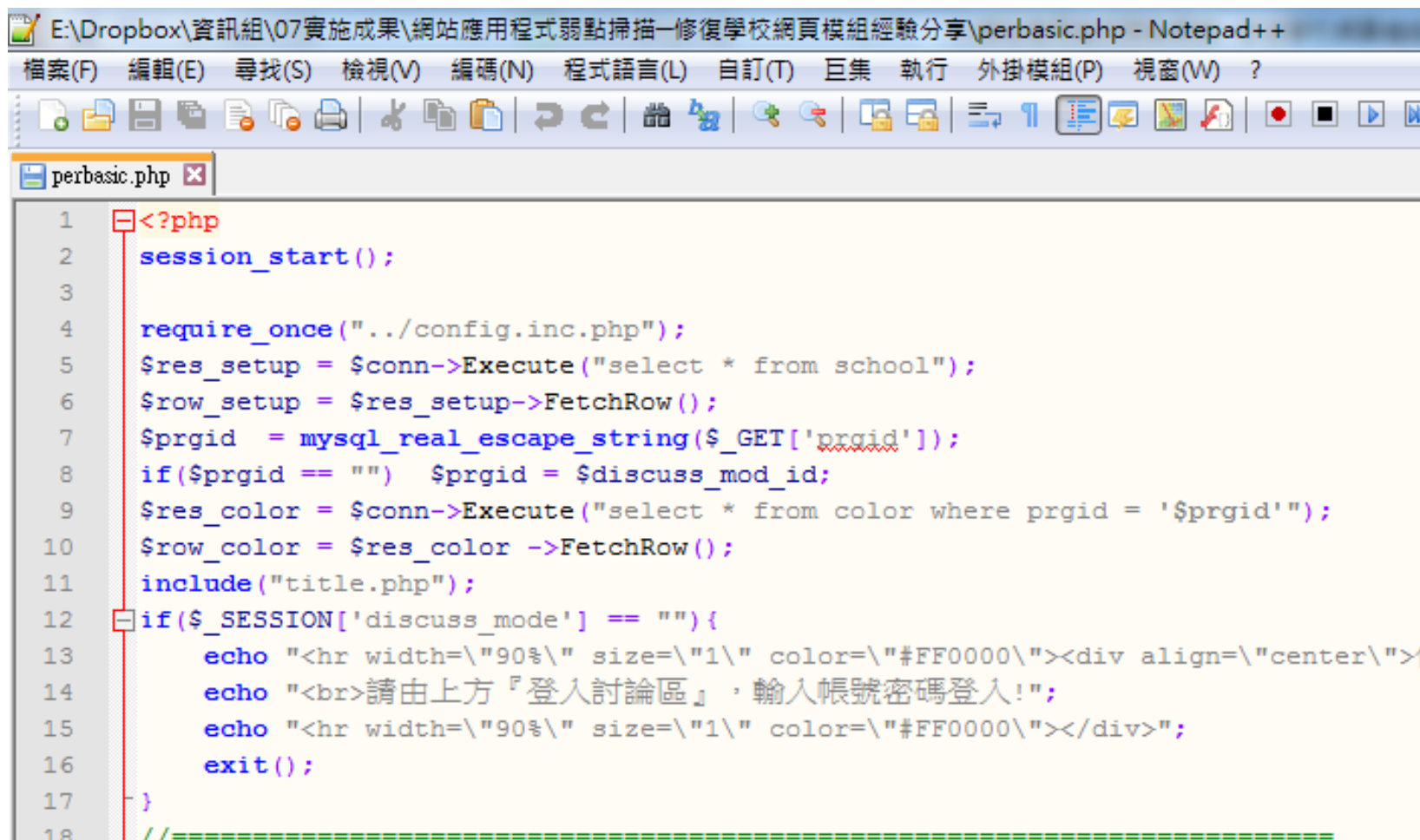
步驟三：下載要修復的網頁

▶ 3-2 使用WinSCP軟體下載弱點網頁



步驟四：開啟要修復的網頁

▶ 4-1 使用Notepad++軟體開啟弱點網頁



```
E:\Dropbox\資訊組\07實施成果\網站應用程式弱點掃描-修復學校網頁模組經驗分享\perbasic.php - Notepad++
檔案(F) 編輯(E) 尋找(S) 檢視(V) 編碼(N) 程式語言(L) 自訂(T) 巨集 執行 外掛模組(P) 視窗(W) ?

perbasic.php x
1  <?php
2  session_start();
3
4  require_once("../config.inc.php");
5  $res_setup = $conn->Execute("select * from school");
6  $row_setup = $res_setup->FetchRow();
7  $prgid = mysql_real_escape_string($_GET['prgid']);
8  if($prgid == "") $prgid = $discuss_mod_id;
9  $res_color = $conn->Execute("select * from color where prgid = '$prgid'");
10 $row_color = $res_color ->FetchRow();
11 include("title.php");
12 if($_SESSION['discuss_mode'] == ""){
13     echo "<hr width=\"90%\" size=\"1\" color=\"#FF0000\"><div align=\"center\">
14     echo "<br>請由上方『登入討論區』，輸入帳號密碼登入!";
15     echo "<hr width=\"90%\" size=\"1\" color=\"#FF0000\"></div>";
16     exit();
17 }
18 //=====
```

步驟四：開啟要修復的網頁

▶ 4-2 根據弱點報告查看【弱點參數】

	弱點網址	弱點參數	XSS	SQL Injection	惡意檔案執行	不適當配置處理	目錄索引	備份檔案	檢測字串
1	http://www.khjh.ntct.edu.tw/school/discuss/perbasic.php	prgid		✓					檢視
2	http://www.khjh.ntct.edu.tw/school/pub/downfiles.php	relpath downfile		✓					檢視
3	http://www.khjh.ntct.edu.tw/school/schedule/show_calendar.php	id		✓					檢視
4	http://www.khjh.ntct.edu.tw/school/schedule/index.php	fm		✓					檢視
5	http://www.khjh.ntct.edu.tw/school/schedule/search_fm.php	show_kind		✓					檢視
6	http://www.khjh.ntct.edu.tw/school/discuss/search_fm.php	prgid		✓					檢視
7	http://www.khjh.ntct.edu.tw/school/schedule/month.php	year month		✓					檢視
8	http://www.khjh.ntct.edu.tw/school/netlink/index.php	parentid		✓					檢視
9	http://www.khjh.ntct.edu.tw/school/pub/rss.php	prgid		✓					檢視
10	http://www.khjh.ntct.edu.tw/school/discuss/index.php	prgid		✓					檢視

◀ ▶ 1 2 3

步驟四：開啟要修復的網頁

▶4-3搜尋【弱點參數】



步驟四：開啟要修復的網頁

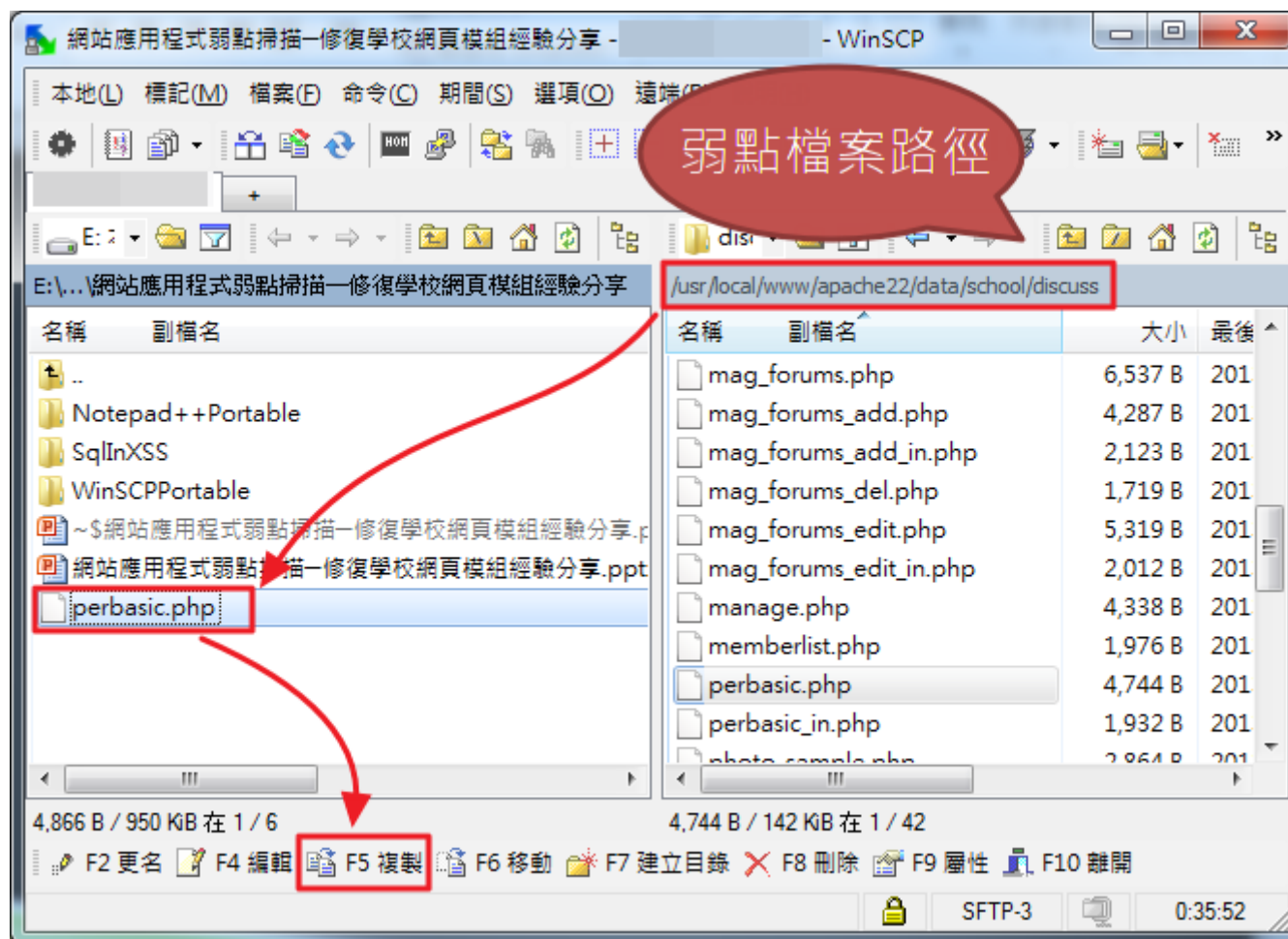
▶ 4-4 修補弱點並儲存

▶ 加上 `mysql_real_escape_string()` 參數

```
1 <?php
2 session_start();
3
4 require_once("../config.inc.php");
5 $res_setup = $conn->Execute("select * from school");
6 $row_setup = $res_setup->FetchRow();
7 $prgid = mysql_real_escape_string($_GET['prgid']);
8 if($prgid == "") $prgid = $discuss_mod_id;
9 $res_color = $conn->Execute("select * from color where mod_id = $prgid");
10 $row_color = $res_color->FetchRow();
```

步驟五：上傳修復好的網頁

- ▶ 使用WinSCP軟體上傳修復好的弱點網頁



步驟六：開啟網頁測試 ('AND'5'='5)

- ▶ 測試方式
 - ▶ 在網址變數後面加上 'and'5'='5
- ▶ 原始網址
 - ▶ <http://www.khjh.ntct.edu.tw/school/discuss/perbasic.php?prgid=250>
- ▶ 加上測試網址
 - ▶ <http://www.khjh.ntct.edu.tw/school/discuss/perbasic.php?prgid=250'and'5'='5>
- ▶ 加上測試網址
 - ▶ <http://www.khjh.ntct.edu.tw/school/discuss/perbasic.php?prgid=250'and'5'='6>

目前為止
已經可以修復

80%

的SQL Injection弱點

剩下的20%怎麼修復呢？

如何修復剩下的20%

- ▶ 設變數接受輸入
 - ▶ 不使用原始輸入資料
 - ▶ 輸入資料過濾檢查後再使用
- ▶ 限制輸入環境
 - ▶ 只能輸入英文、數字、男女等
- ▶ 修改程式

XSS修復實例

修復工具STRIP_TAG()

- ▶ 避免使用者的輸入中當有<IFRAME>、<SCRIPT>這些HTML標籤時會被瀏覽器當成網頁內容而執行。
- ▶ 如果資料輸入時本就不允許輸入HTML標籤，不如直接在輸入檢查時，以strip_tag()直接濾掉，免除後患。

修復範例

弱點類型：SQL Injection, XSS

弱點類型：parentid, level, selpage, prgid

弱點檔案：school=>files=>index.php

(1)第8行，增加以下的紅色部分。

```
=====
7 //取得相關顏色資料
8 $prgid =
strip_tags(mysql_real_escape_string($_GET['prgid']));
9 if($prgid == "")
=====
```

修復結果

日期	搜尋 總URL數	總檢測 網頁	XSS 弱點數	SQL Injection
2013年 08月02日	1340	720	0	25
08月12日	1347	249	1	11
08月21日	1622	262	0	6
08月22日	908	265	0	12
08月29日	824	256	0	2
2013年 08月30日	1514	257	0	0

修復紀錄

- ▶ 短網址：<http://goo.gl/8uMJQO>
- ▶ 原始網址：
<https://sites.google.com/site/altohornubuntnu/home/02-wang-zhan-tao-jian>

使用已修復檔案修復弱點

檔案說明

- ▶ 不包含《data》資料夾、《config.inc.php》檔案。
 - ▶ 《data》資料夾：裡面存的檔案是各校上傳的附加檔案、相片、影片等，所以各校的內容均不同。
 - ▶ 《config.inc.php》檔案：是各校網頁的設定檔，所以各校的內容均不同。

檔案說明

- ▶ 已經包含了下面的程式功能修改
 - ▶ 【行事曆】日期只到100年問題
 - ▶ 【行事曆】新增行事曆時看見其他人已建立的活動
 - ▶ 【最新公告】加上各處室名稱
 - ▶ 【最新公告】加上[特急件][急件]標示
 - ▶ 【最新公告】加上facebook的讚推文
 - ▶ 【最新公告】加上Google + 1 的推文
 - ▶ 【榮譽榜】加上得獎類別
 - ▶ 【教職員工簡介】不顯示帳號
 - ▶ 【密碼更新】增加密碼半年更新提醒密碼長度8字元以上

下載已修復檔案

▶ 短網址：<http://goo.gl/CfsoOR>

▶ 原始網址：

<https://sites.google.com/site/altohornubuntu/home/02-wang-zhan-tao-jian/cenglinfulaoshischoolmozuxiuzheng-shiyongyixiufudanganshengji>