網站技術使用說明

系統環境+服務器配置和資訊安全

(一) 網站管理系統

PROADMIN 1.0

採用由威盛網路公司與日本 FOYOKO 工作室共同研發的網站管理系統作為核心架構，此系統最大的特點在於人性且友善地操作環境，並且具有無限的擴充性，降低服務器運作資源，提供管理者最簡便的操作方式.

ProAdmin 優勢特點

1. 容易學習，使用者易於熟悉，才可發揮系統的價值性.
2. 減省成本，公司人事的流動，在教育的工作時間縮短.
3. 降低資源，節省服務器資源，降低服務器的配置成本
4. 易於擴充，將來網站的升級，將不受模組的開發限制.

(二) 網站系統開發環境

1. 採用最具經濟和效率的 LAMP (Linux+Apache+Mysql+ PHP)進行網站系統開發工作;
2. LAMP 開發的獨有優勢 A. 低成本 B. 高效率 C. 好維護
3. Facebook 的全球用戶量、用戶訪問量、資料存儲量已可完全證明 LAMP 其強大效能

(三) 伺服器配置

1. 使用 Intel Xeon 四核服務器 4GB RAM 內存和 100Mbit / s 的連接，服務器配置 RAID 10
2. RAID 控制器時可靠性最高配置 4 個硬盤。
3. 即使發生 2 個驅動器在同一時間失效，我們的服務器將繼續運行，並且不會丟失網站資料
4. 配置提供了很大的效能，讓您的網站，任何時候都能迅速打開。
5. 伺服器工作中的所有服務每分鐘都在被監視，如果發生故障，我們就會接到警報，我們能快速的修復他。
6. 伺服器的檔案和資料庫以秒做為計算進行 7 天 24 的同步備份，你可以隨時要求恢復過去 7 天的某個檔案

(四) 資訊安全作業能力

(一) 品質水準

1、 本公司具有開發相關系統之經驗與專案能力，為確保系統之品質，在系統開發各階段均會進行系統品質與測試驗證。

2、 本公司充分了解本專案需求規格書所列之各項軟硬體規格需求，可利於後續之系統分析。

3、 因系統分析所需之使用者訪談，提供制式表格詳加記錄，並經接受訪談者與相關人員確認。

4、 系統各項功能之實作，於雛形完成時先行提供相關人員確認。各模組之完成，本公司先自行進行完整之測試，再交由使用者測試。

(二) 系統安全

1、 系統中不存在有後門或特洛伊木馬程式等非規劃內之額外功能並符合資訊安全相關規定。

2、 系統提供查詢個人資料所有紀錄，以維持資料保密機制。

3、 系統發展過程中所接觸之重要資料，皆有安全管控措施，防止資料被竊取、竄改、販售、洩漏及不當備份的情形。

(三) 帳號及密碼管理

1、 強式混合型要求原則：各使用者之帳號密碼長度至少需為 8 個字元(含)以上、且強迫為英、數字混合、英文字母大小寫均視為不同、密碼不可與帳號相同。

2、 密碼生命週期限制：各使用者之密碼可由系統管理者設定 6 個月為其生命周期 (Password aging，即該密碼使用 6 個月後必需被強迫更新，否則於到期日後必須更新密碼後始得進入系統中使用，並於到期之日 1 個月前開始提出修改密碼之警訊)，且不得沿用上次的密碼

3、 密碼輸入錯誤次數控制：可由系統管理者設定當使用者連續輸入密碼錯誤達 5 次時，系統自動將該帳號停權，並立即 e-mail 通知系統管理者該帳號資料、使用 IP、嘗試次數，待系統管理者處理後才可回復正常使用。

4、 密碼欄位使用不可還原型加密：資料庫中的密碼資料皆不以明文型態存放，使用 MD5 加密技術保護原始密碼不被顯示，如下圖所示：

5、

```
//寫入資料庫
$modSQL  = "UPDATE `member` SET ";
//視情況更新密碼
if(isset($userpswd)&&strlen($userpswd)>0)
{
  $modSQL .= "userpswd='".md5($userpswd)."',";
}
$modSQL .= "idnum='$idnum',";
$modSQL .= "cname='$cname',";
$modSQL .= "sex='$sex',";
$modSQL .= "tel='$tel',";
$modSQL .= "fax='$fax',";
```

密碼使用 MD5 加密示意圖

(四) 強化應用程式資料驗證程序

1、 資料一致性

系統確認所有關聯資料無誤才做寫入動作

本系統採用關聯式資料庫設計，在程式對資料庫做寫入動作前，會自動檢查所有與該筆資料關聯之其他資料表是否都有正確輸入值，才做寫入動作，避免資料庫錯亂的情況。

使用資料庫交易 Transaction 機制

在資料庫系統中，所有會更改到資料庫中資料內容的動作都以異動交易(Transaction)為主要的處理單位，而通常一個異動交易(Transaction)中包含了數個以上資料庫動作(Actions)。採用本機制可讓整個異動交易視為一個不可分割的單元，也就說整個異動交易的所有動作必須全部做完，若異動交易的中間過程中有任何錯誤產生時，會自動撤回(Rollback)到未執行異動交易前的原點，也就是整個異動都不做。如此便可以維護資料的:一致性(Consistency)、正確性(Correctness)與並行控制(Concurrency)。

寫入資料單一性確認

在建立新類別時，系統會自動產生具有唯一識別性的代碼資料，而在其他資料寫入時，則會先檢查資料庫中是否有同樣唯一性的識別資料存在(ex: 身分證字號)，保護同一筆資料不被重覆寫入。

2、 資料安全性

過濾特殊字元防止 SQL Injection、XSS 跨網域指令碼攻擊

應用系統對所有使用者輸入欄位都會進行字元檢查，排除不必要的特殊字元(如' "!$%^&*_|->;等)，防止應用系統被利用異常資料進行惡意攻擊。

```
/*==========接收參數處理-開始==========*/
$op = (isset($op)&&strlen($op)>0)?(addslashes(htmlspecialchars(trim($op)))):'';
$id = (isset($id)&&strlen($id)>0)?(addslashes(htmlspecialchars(trim($id)))):'';
$title = (isset($title)&&strlen($title)>0)?(addslashes(htmlspecialchars(trim($title)))):'';
$url = (isset($url)&&strlen($url)>0)?(addslashes(htmlspecialchars(trim($url)))):'';
$seq = (isset($seq)&&strlen($seq)>0)?(addslashes(htmlspecialchars(trim($seq)))):'';
$start_time = (isset($start_time)&&strlen($start_time)>0)?(addslashes(trim($start_time))):'';
$end_time = (isset($end_time)&&strlen($end_time)>0)?(addslashes(trim($end_time))):'';
$keep_YN = (isset($keep_YN)&&strlen($keep_YN)>0)?(addslashes(htmlspecialchars(trim($keep_YN)))):'';
$hide_YN = (isset($hide_YN)&&strlen($hide_YN)>0)?(addslashes(htmlspecialchars(trim($hide_YN)))):'N';
$op_id = $_SESSION[EMPLOY_id];
$op_ip = $_SESSION[client_ip];
/*==========接收參數處理-結束==========*/
```

程式過濾特殊字元示意圖

使用加密防範 Session 及 Cookie 竄改攻擊

下圖中之 add_key(base64_encode()," ")即為加密函數，確保存在 Session 及 Cookie 中的資料不被駭客竄改攻擊。

```
/*==========Session加密處理-開始==========*/
$_SESSION[USER_ID] = add_key(base64_encode($USER_ID),"aaXe3Dg466xs");
$_SESSION[USER_Name] = add_key(base64_encode($USER_Name),"aaXe3Dg466xs");
/*==========Session加密處理-結束==========*/
```

程式加密 Session 示意圖

3、 提供系統遭駭客入侵蝕之防護

SQL Injection 入侵方式檢測表

入侵方式	避免產生的資料或語法	檢 測
以 SQL 執行方式入侵	說明：避免直接利用使用者輸入的資料來組合 SQL 語法 如：strSQL="SELECT * FROM tblUser WHERE UserName='".$username."' AND Password='".$password."'"	Y□ N□
常用帳號入侵	說明：避免一般管理人員可能建立的使用者名稱 如：admin、administrator、supervisor、sa、root... 等等。	Y□ N□
讓 SQL 僅執行 UserName 的方式入侵	說明：阻擋欄位輸入「Admin' --」，讓原先的 AND 子句變成僅執行 UserName 如：SELECT * FROM tblUser WHERE UserName='admin'--' AND Password='abcde'	Y□ N□
用未知的使用者名稱登入	說明：阻擋欄位輸入「'or 1=1--」，則不管之前的條件為合，只要某個條件為真，整個判斷式就都為真，因此回傳的執行	Y□ N□

	結果包含了全部的會員記錄。 如：SELECT * FROM tblUser WHERE UserName='' or 1=1--' AND Password=' abcde '	
利用錯誤訊息獲取欄位數量與名稱	說明：阻擋利用錯誤訊息來判斷欄位的資料型態與會員的帳號密碼。 如：利用 VBScript 語法的 On Error Resume Next，並搭配 If Err.Number<>0 Then 的錯誤處理方式，自行將錯誤重導到適當的錯誤處理網頁。	Y□ N□
資料庫伺服器 停止執行	說明：阻擋直接輸入 Shutdown 命令，要求 資料庫伺服器停止執行。 如：「';SHUTDOWN--」	Y□ N□
破壞內容	說明：阻擋刪除某個資料庫、資料表的語法 如：「' ;DROP Database」、「' ;Truncate Table」、「' ;Truncate Table」、「' ;DELETE FROM」 <資料庫名稱>--	Y□ N□
規避前端檢測入侵	說明：在伺服器端檢查與限制輸入變數的型別與長度，過濾掉不需要的內容。要注意的是這些檢查不要放在前端。	Y□ N□
資料庫伺服器預設群組帳號入侵	說明：程式登入 資料庫伺服器 的帳號不要使用 root，避免有過大的權限。	Y□ N□
引用延伸預存程序	說明：將系統中用不到但功能權限過於強大的延伸預存程序刪除。	Y□ N□

一、 業務持續運作及障礙排除機制

(一) 系統效能及穩定度

1、 本公司規劃的系統架構均以達成系統最大效能及穩定度為目標，透過資料庫的穩定性架構及測試開發期間不斷地的調校，建構一更具有擴充性與系統穩定性的架構。

2、 本公司在開發測試系統運作的同時，會以透過監測 CPU、記憶體、網路的使用量來觀測系統的效能，同時也可以利用模擬壓力測試來檢測系統的穩定性，透過上述方法，可有效達成系統開發校能的最佳狀態。

(二) 系統測試及維運計畫

1、 系統測試

本專案軟體之測試環境將以下列的方式進行測試。每項功能測試至少包括以下測試項目：

(1) 正常資料測試：測試人員將合於規定的資料輸入時，系統是否產生正確的輸出。

(2) 異常資料測試：測試人員將不合於規定的資料輸入時，系統是否會拒絕錯誤資料且產生錯誤訊息。

(3) 系統整合測試：將相關設備依系統需求，並做整體性之整合測試，系統之各環節是否順暢且運作無誤。

測試內容主要包含如下：

i. 需求測試：需求測試係提早檢驗功能需求之重要步驟，於系統分析階段將先期完成雛型系統之使用者介面，模擬未來操作使用時境，向各使用者解說、介紹，達到雙方溝通效果，增加未來系統上線之實用性。

ii. 單元測試：程式設計師於程式設計完成，需進行單元測試，測試程式指令，各段邏輯之正確性，測試個案依各程式之功能進行設計，務使每段程式邏輯均驗證過，測試者可自行設定各種變數、條件再逐一檢查。

iii. 系統測試：本項所指系統測試係將經單元測試之程式模組，所組成之子系統進行測試，本項測試之重點在驗證各子系統之功能，尤其著重於程式連結上資料交換之正確性。

2、 維護計畫

針對此專案之維護事宜，本公司提供專人及專線以諮詢及排除系統各種問題。

(1) 本公司提供專線電話以供諮詢，服務時間為：
週一至週五 09：30 至 18：30，中午休息時間為 12：00 至 13：00。(例假日、國定假日、民俗節日及全國性選舉投票日及各級主管機關臨時公布放假日除外)

遇緊急情事而有礙本專案之執行時，立即提供服務或維護，不受上述時間限制。

(2) 維護專案小組：

i. 業務窗口：負責與貴司之溝通協調事宜。

ii. 專案技術人員：專案技術人員包含：技術諮詢工程師，負責系統報修單的處理、教育訓練、技術諮詢、檢測維護報告及程式的修正與更新。

iii. 電話客服專員：負責接報、紀錄貴司來電問題，並追蹤問題處理進度。

(3) 問題等級及處理時間：

接獲貴司提出之系統問題，本公司均於 4 個工作小時內回應，並於 14 個工作日內排除故障。

(4) 問題反應方式：

i. 客服專線負責接收貴司所提出之系統問題並追蹤問題後續處理進度。

ii. 電子郵件服務，提供專屬服務信箱，讓貴司的使用人員方便隨時提出問題。