網站應用程式弱點檢測報告說明

教育機構網站應用程式弱點監測平台-弱點檢測報告

教育機構網站應用程式弱點監測平台-弱點檢測報告

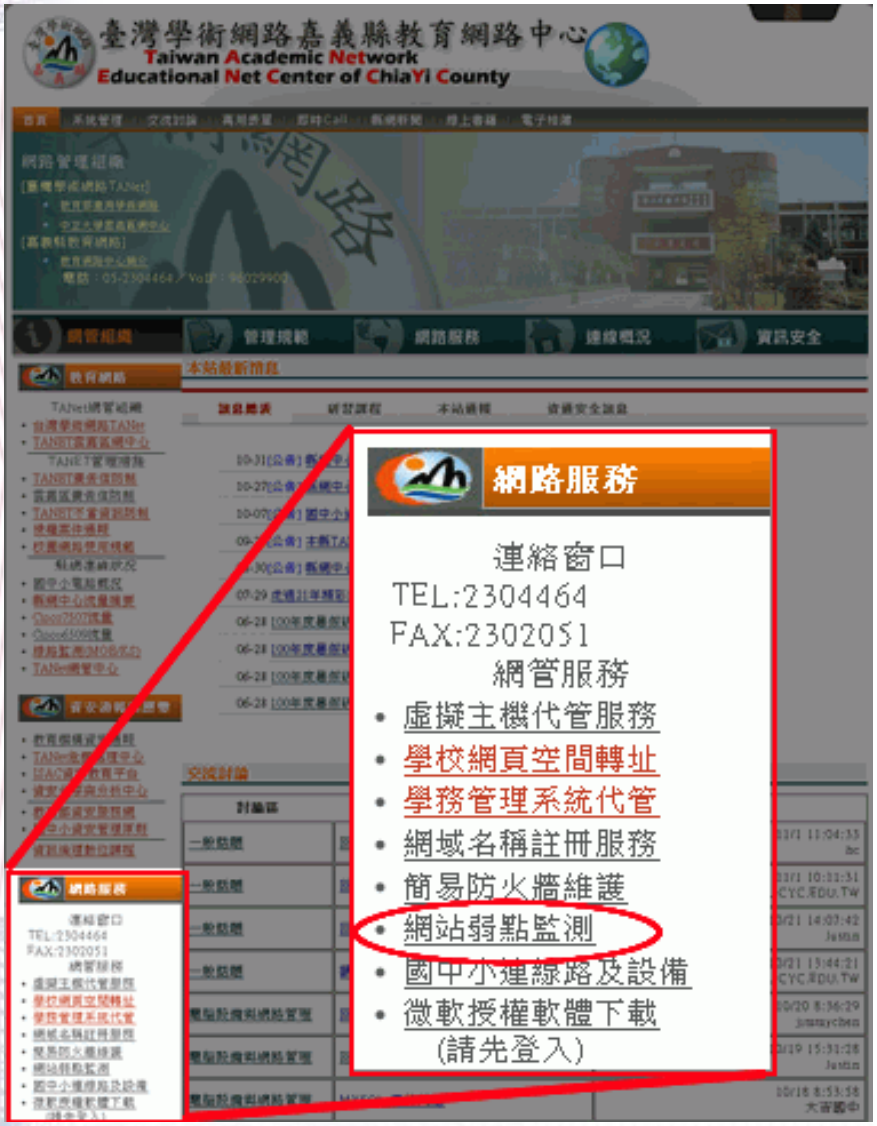
一、檢測資訊

- 受測帳號：
- 檢測網站名稱：
- 檢測網站網址：I
- 檢測開始時間：
- 檢測完成時間：
- 搜尋總URL數：　　筆　• 總檢測網頁：　筆　•疑似弱點：0筆
- 檢測類別：XSS、SQL Injection、惡意檔案執行、不適當配置處理、目錄索引
- POST設定：---
- 伺服器端資訊：

二、弱點資訊

教育部電算中心版權所有　© 2009

報告由網站應用程式弱點監測平台產生



- 此平台由教育部提供
- 網址
  http://ewavs.cyc.edu.tw
- 或從縣網中心網站左側「網路服務」的「網站弱點監測」進入

現在網站的弱點

- 現在只要使用瀏覽器，透過網站應用程式就可以把東西放上伺服器。
- 一個網站有成千上萬個應用程式，只要其中一個有弱點，就可能把整個網站送給別人。

網站應用程式的弱點造成的影響？

- 可能被拿來惡作劇
  - 如發佈假新聞明天全校放假一天
- 可能被利用來犯罪
  - 如發廣告信、放置惡意程式、釣魚網頁
- 可能洩漏個人資料
  - 一筆資料 NT500 ~ 20000 元
- 其他

有弱點的網站應用程式如何處理？

- 廠商做的：要求廠商修補或更換廠商
- 架站套件：更換修補後的版本
- 自己寫的：嘗試修補

- 無法修補的：從伺服器中刪除（注意，不是停用而已）

- 注意事項：最新的版本可能仍有弱點
  - 新版本沒有修補漏洞而是追加新功能，結果弱點更多

檢測報告中的各種弱點說明

- XSS（ Cross-site scripting ，跨站指令碼攻擊）
- SQL Injection（資料隱碼攻擊 /SQL 注入攻擊）
- 惡意檔案執行
- 不適當配置處理
- 目錄索引
- 備份檔案（本次未檢測）

- 將報告中的「檢測網址」輸入到瀏覽器網址列進行驗證

XSS（跨站指令碼攻擊）

教育機構網站應用程式弱點監測平台-弱點檢測報告

一、檢測資訊

・受測帳號：LYS	・搜尋總URL數：1418筆 ・總檢測網頁：128筆 ・疑似弱點：35筆
・檢測網站名稱： ・檢測網站網址： ・檢測開始時間： ・檢測完成時間：	・檢測類別：XSS、SQL Injection、惡意檔案執行、不適當配置處理、目錄索引 ・POST設定：--- ・伺服器端資訊：無法辨識

二、弱點資訊

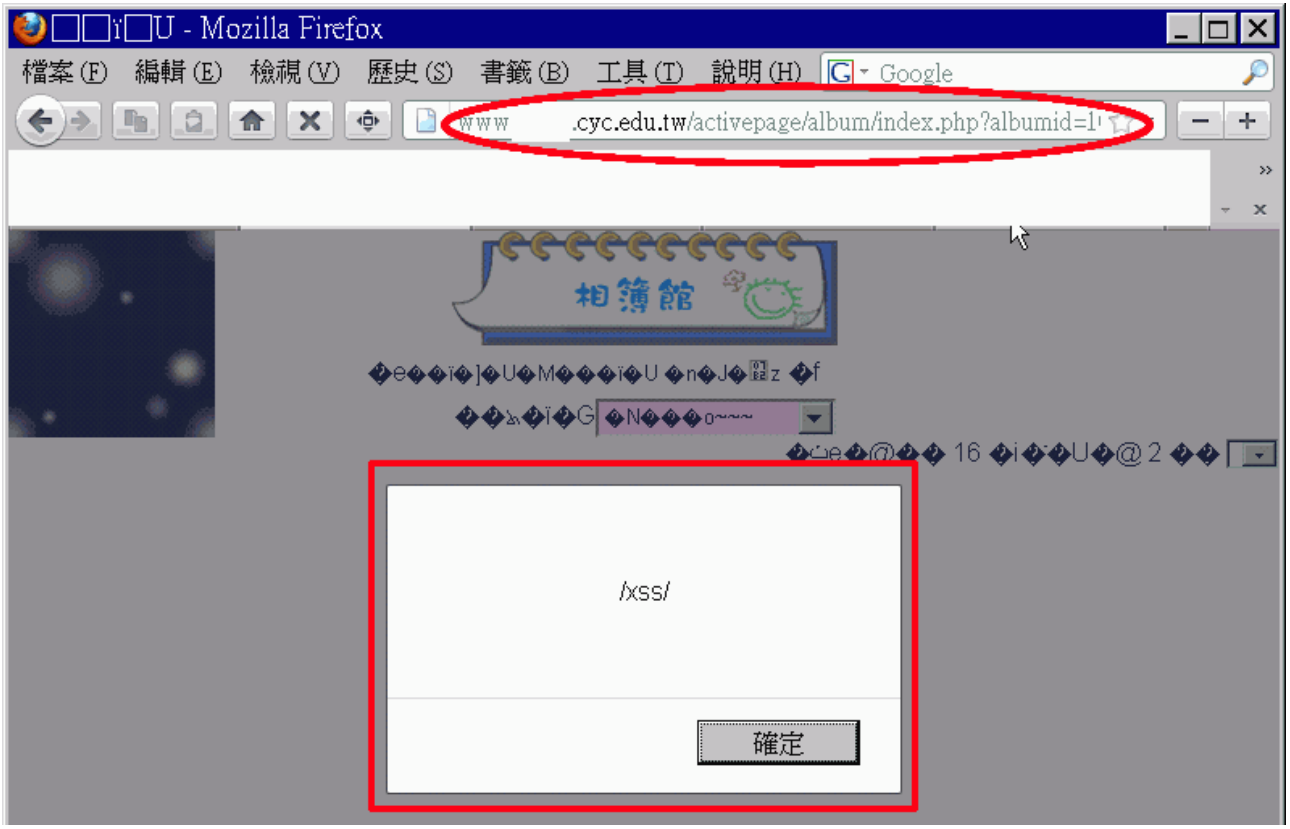
1. http://www. .cyc.edu.tw/activepage/album/index.php

弱點類型	弱點參數	檢測網址
XSS	albumid dup	http://www. cyc.edu.tw/activepage/album/index.php?albumid=10845%22%3e%3cs%63ript>%61lert%28/xss/%29%3c/s%63ript%3e&account=t14&dup=0
XSS	albumid dup	http://www. .cyc.edu.tw/activepage/album/index.php?albumid=10845%22%3e%3ciframe src=abcd%3e&account=t14&dup=0

XSS-修護建議	
範例介紹：	透過網頁上的 TextBox控制項輸入資料或直接從IE的URL網址列輸入攻擊字串

XSS（跨站指令碼攻擊）

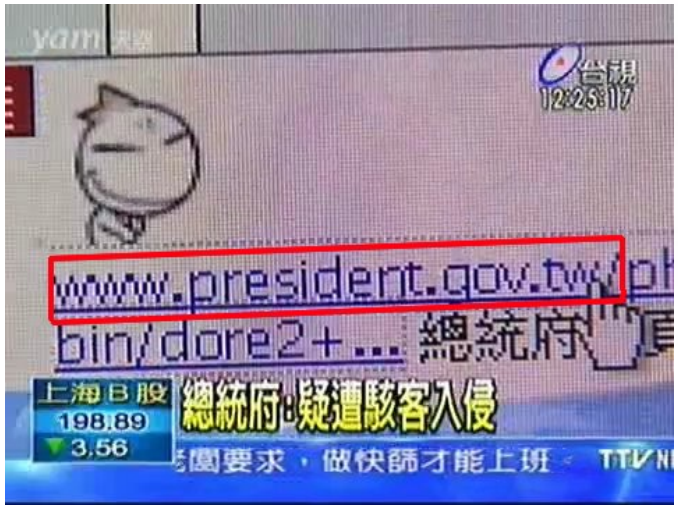
- 測試方法：將報告中的「檢測網址」內容貼到瀏覽器的網址列，如果跳出 XSS 視窗就表示有弱點。



XSS（跨站指令碼攻擊）

- 有名案例：總統府網站
  - 馬英九跟流行跳《 sorry sorry 》？　總統府網頁被惡搞
    - http://www.nownews.com/2009/08/28/91-2498144.htm
    - （ nownews 新聞 ）
  - 機會教育：從中華民國總統府網站被發現 XSS 漏洞講起
    - http://blog.miniasp.com/post/2009/08/28/Suggest-add-www-president-gov-tw-to-Restricted-sited.aspx
    - （ google 總統府 xss ）
  - 【莫拉克颱風】惡搞【臺灣之 Super 救命兒】在總統府網站新聞稿播放！
    - http://www.youtube.com/watch?v=sQ0fvNWihZY
    - （台視新聞片段）

XSS（跨站指令碼攻擊）



開頭網址是總統府網站

- 可能影響：
  - 惡作劇、社交工程、網路釣魚、嵌入惡意程式等
  - 影響主要在使用者這邊
  - 若網站管理者上當，取得權限後就可能對網站造成侵害。
- 修補方式：
  - 將網站應用程式更新到沒有弱點的版本
  - 從伺服器中刪除

SQL Injection（資料隱碼攻擊）

4. http://www. cyc.edu.tw/school/album/index.php

弱點類型	弱點參數	檢測網址
XSS	selpart selpage selwork	http://www. .cyc.edu.tw/school/album/index.php?selpart=0%22%3e%3cs%63ript>%61lert%28/xss/%29%3c/s%63ript%3e
XSS	selpart selpage selwork	http://www. .cyc.edu.tw/school/album/index.php?selpart=0%22%3e%3ciframe src=abcd%3e
SQL Injection	selpart selpage selwork	http://www. cyc.edu.tw/school/album/index.php?prgid=3&sgd=&selpage=1%25%27%20%61nd%203=3%20%61nd%20%27%25%27=%27&selwork=
SQL Injection	selpart selpage selwork	http://www. .cyc.edu.tw/school/album/index.php?prgid=3&sgd=&selpage=1&selwork=%20%61nd%205=5
SQL Injection	selpart selpage selwork	http://www .cyc.edu.tw/school/album/index.php?prgid=3&sgd=&selpage=1&selwork=%20%61nd%203>2

SQL Injection（資料隱碼攻擊）

- 測試方法：將報告中的「檢測網址」內容輸入到瀏覽器的網址列，如果兩邊內容有差異就判定為有弱點。
- 實際測試：分別將前一頁的兩個「檢測網址」內容貼到瀏覽器的網址列，發現兩個網頁呈現出來的內容是不同的。
- 網站應用程式若有 SQL Injection 的弱點，通常也會有 XSS 弱點，因為這兩個弱點都是未檢查輸入字串造成。

SQL Injection（資料隱碼攻擊）

SQL Injection（資料隱碼攻擊）

- 案例：
  - 示範影片：不用輸入密碼就以管理者身份登入
- 可能影響：
  - 攻破網站、竄改資料、撈取資料
  - 利用此弱點可以真的攻進網站

SQL Injection(資料隱碼攻擊)

- 誤判說明：
  - 跳出回覆頁面的網站應用程式會造成誤判
    - 跳出「所選模組不存在」並不是弱點（如東榮國中）
    - 跳出「沒有權限使用請先登入」並不是弱點（如新港國小）
  - 隨機變動的網頁（如隨機照片）會造成誤判
    - 在全部頁面顯示隨機變動的網頁區塊（如梅北國小）
  - 曾使用過、現在關閉的 XOOPS 模組都會造成誤判
- 修補方式：
  - 將網站應用程式更新到沒有弱點的版本
  - 從伺服器中刪除

惡意檔案執行

- 說明：
  - 至今尚未檢出此弱點
- 可能影響：
  - 這個弱點可以執行本機或遠端的檔案，可能造成系統損壞
- 檢測方法：
  - 直接在網址增加遠端的檔案連結，如果能執行就判定為有弱點

不適當配置處理

教育機構網站應用程式弱點監測平台-弱點檢測報告

一、檢測資訊

・受測帳號：LYS	・搜尋總URL數：1705筆 ・總檢測網頁：42筆 ・疑似弱點：1筆
・檢測網站名稱：[redacted] ・檢測網站網址： ・檢測開始時間： ・檢測完成時間：	・檢測類別：XSS、SQL Injection、惡意檔案執行、不適當配置處理、目錄索引 ・POST設定：--- ・伺服器端資訊：Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny13 with Suhosin-Patch

二、弱點資訊

*此為誤判

1. http://www.[redacted]cyc.edu.tw/backend.php/

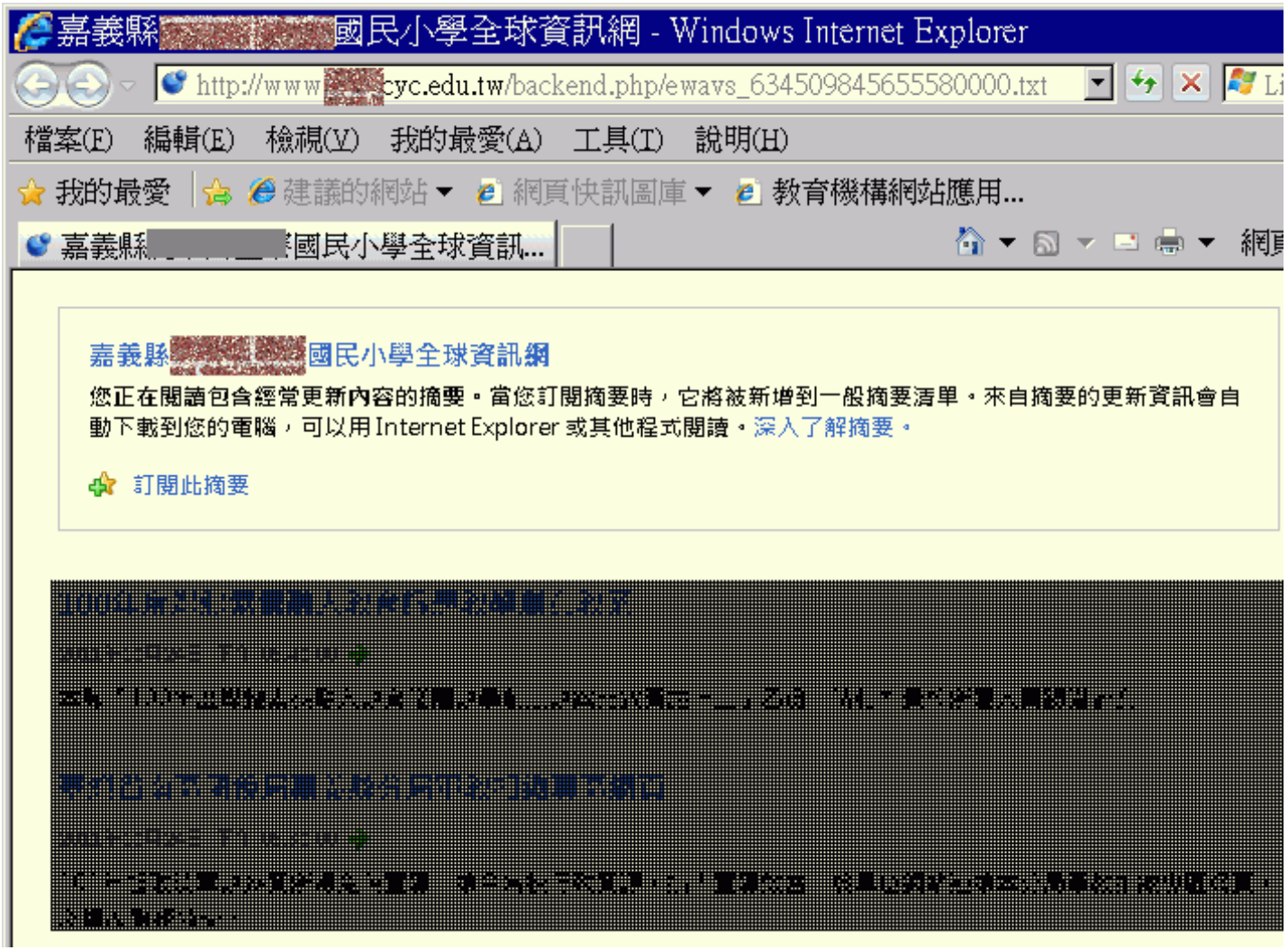
弱點類型	弱點參數	檢測網址
不適當配置處理	---	http://www[redacted]cyc.edu.tw/backend.php/ewavs_634509845655580000.txt

不適當配置處理-修護建議

不適當配置處理

- 說明：
  - 屬於伺服器設定問題
  - 系統可讓人直接送檔案到伺服器上
    - 如果送上去的是駭客工具那伺服器就送人了。
  - 目前檢出的應該都是誤判。
- 測試方法：
  - 將報告中的「檢測網址」內容貼到瀏覽器的網址列
  - 如果出現一串數字就判定為有弱點。
- 誤判說明：
  - XOOPS 的 backend.php 是 rss 即時新聞，不是弱點。

不適當配置處理



將檢測網址輸入瀏覽器的網址列之後出現 RSS 訂閱訊息，證明是誤判

目錄索引

教育機構網站應用程式弱點監測平台-弱點檢測報告

一、檢測資訊

・受測帳號：LYS	・搜尋總URL數：969筆 ・總檢測網頁：38筆 ・疑似弱點：3筆
・檢測網站名稱： ・檢測網站網址： ・檢測開始時間： ・檢測完成時間：	・檢測類別：XSS、SQL Injection、惡意檔案執行、不適當配置處理、目錄索引 ・POST設定：--- ・伺服器端資訊：無法辨識

二、弱點資訊

1. http://www. cyc.edu.tw/webadmin/

弱點類型	弱點參數	檢測網址
目錄索引	---	http://www. cyc.edu.tw/webadmin/

目錄索引-修護建議	
範例介紹：	伺服器網站設定未關閉瀏覽目錄索引。網頁伺服器若於該目錄不存在預設首頁時，將顯示該目錄中所有檔案內容，若該項目內存在重要資料，如Access資料庫(.dbm)或設定檔(config.inc)，則使用者即可下載取得該機敏內容。

目錄索引

- 測試方法：
  - 將報告中的「檢測網址」內容貼到瀏覽器的網址列，若看到檔案列表就判定為有弱點。
- 說明：
  - 某些新聞區 / 留言板的網站應用程式是把資料庫檔案放在網站外部可存取處，目錄索引功能沒關就可以直接找到檔案，將資料庫下載後可找到管理帳號密碼。
  - 目錄索引只是讓這個新聞區 / 留言板的弱點更顯著，就算關閉目錄索引，仍可用猜的把資料庫檔案抓回去

目錄索引

www.[redacted].cyc.edu.tw - /webadmin/

[To Parent Directory]

2011/5/27 上午 11:13	<dir>	admin
2011/5/30 下午 03:19	6847	admin_login.asp
2011/5/27 上午 11:13	<dir>	album
2011/5/27 上午 11:13	<dir>	authorise
2011/5/27 上午 11:13	<dir>	batchupload
2011/11/4 上午 09:16	<dir>	db
2011/5/27 上午 11:13	<dir>	editor
2011/5/27 上午 11:13	<dir>	ewebeditor
2011/6/15 下午 04:37	<dir>	eWebEditor6
2011/5/27 上午 11:13	<dir>	form
2011/5/27 上午 11:13	<dir>	forma
2011/5/27 上午 11:13	<dir>	forme
2011/2/25 上午 10:16	1571	frame.asp
2011/5/27 上午 11:13	<dir>	gif
2011/5/30 下午 03:18	<dir>	images
2011/5/27 上午 11:13	<dir>	include
2011/5/27 上午 11:13	<dir>	item
2011/5/27 上午 11:13	<dir>	link
2011/5/27 上午 11:13	<dir>	linkr
2011/5/27 上午 11:13	<dir>	links
2011/6/15 下午 05:22	<dir>	mem_folder
2011/5/27 上午 11:13	<dir>	news_post
2011/2/25 上午 10:16	679	redirection.asp
2011/5/27 上午 11:13	<dir>	upfile
2011/10/13 上午 09:06	<dir>	upload
2011/9/17 上午 10:48	<dir>	uploadfile
2011/5/27 上午 11:12	<dir>	welcome
2011/3/21 上午 10:31	213	writecookies.asp

www.[redacted].cyc.edu.tw - /webadmin/db/

[To Parent Directory]

2011/11/4 上午 09:16	4620288	db_[redacted].accdb
2011/4/13 上午 10:12	1626112	db_[redacted].mdb

目錄索引

tb_admin : 資料表

	a_id	a_class	a_unit	a_account	a_pwd
▶	1	0	管理者	[redacted]	[redacted]
	2	0	管理者2		
*	(自動編號)				

- 進入後發現 db 資料夾
- 再進去看到 mdb 檔
- 下載 mdb 檔
- 用 access 開啟發現管理者的帳號密碼

目錄索引

- 示範：
  - http://www.tlps.cyc.edu.tw/icons/ （非弱點）
- 說明：
  - 屬於伺服器設定問題
  - 當目錄沒有 index.html 、 default.asp 等索引檔案時，點到該位置就會把目錄中所有檔案全部秀出。
  - 不一定是弱點
  - 但他會讓其他弱點會死的更快更徹底

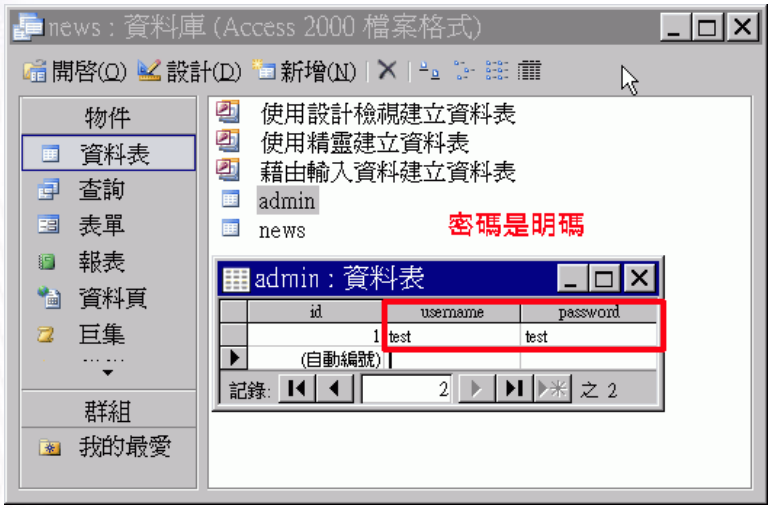
目錄索引

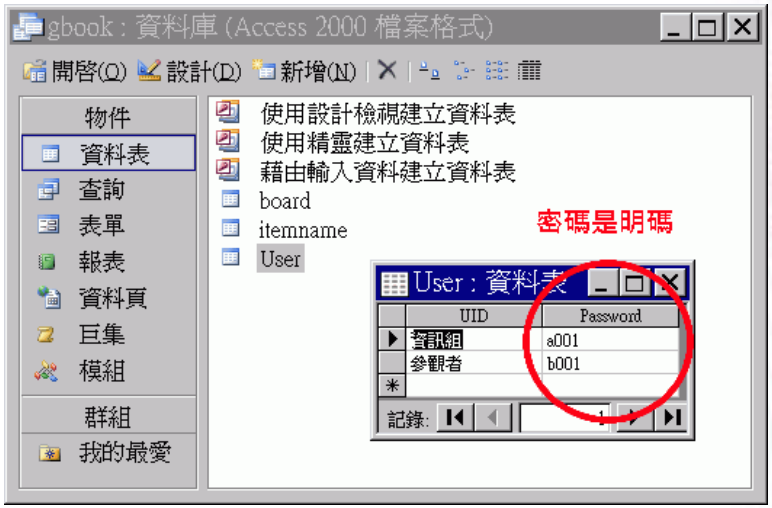
- 可能影響：
  - 可能暴露相當重要的資料。
- 修補方式：
  - 透過伺服器設定關閉
  - 在每個重要資料夾放入 index.html 或 default.asp 等檔案
    - xoops 的每個資料夾中都有 index.html / php 故無此弱點
  - 設定檔可能在不同的地方，像 debian/b2d 主機的 /home/[使用者]/public_html/ 的目錄索引設定是在 /etc/apache2/mods-available/userdir.conf 裡面。

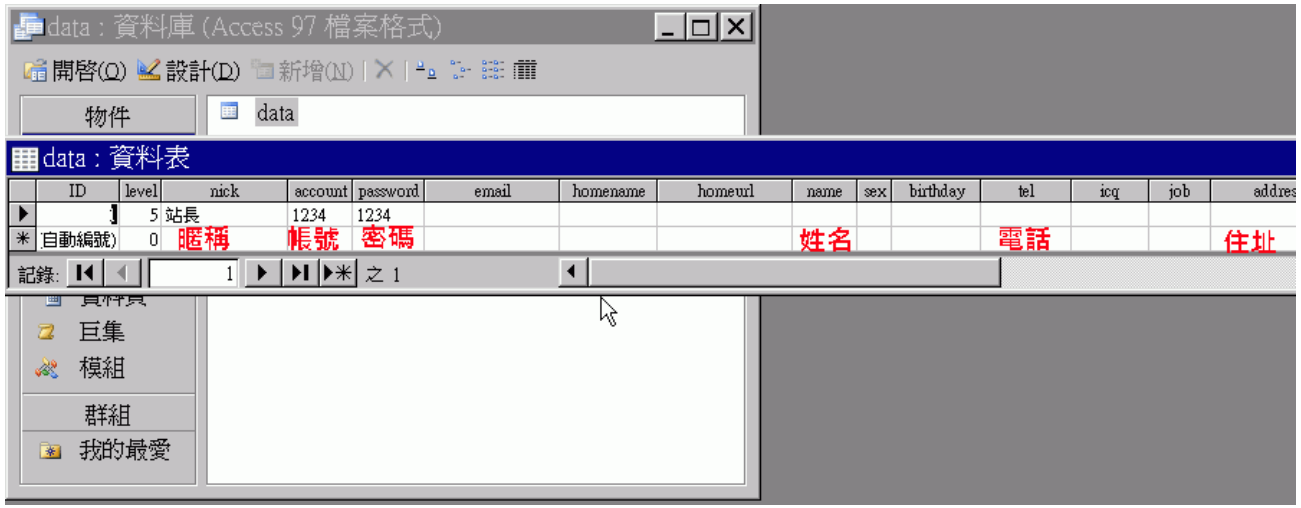
ASP+AccessMDB 簡易佈告欄問題

- 問題不是他有什麼弱點，而是他本身就是弱點
  - MDB 檔放在可以下載的位置
  - MDB 檔裡面有各種資料
  - 儲存密碼是明碼顯示
  - 有很多是上個世紀留下來的
  - 目錄索引功能讓弱點更容易被暴露出來
  - 即使目錄索引關掉也能猜得到
- 示範操作：帳號密碼個資全部抓下來

ASP+AccessMDB 簡易佈告欄問題







以上是在網路上找到的「免費」佈告欄、校園公告系統、會員管理系統的資料庫檔案

備份檔案


網站總弱點檢測報告
檢測類別：XSS、SQL Injection、惡意檔案執行、不適當配置處理、目錄索引、備份檔案
POST設定：---
Apache 安全漏點
總檢測弱點比例圖
無明顯弱點
疑似弱點
85.7%
各類別弱點比例圖
備份檔案
備份檔案
1 (100%)
100%
*此為誤判
檢測類別
風險等級
1 XSS 高
2 SQL Injection 高
3 惡意檔案執行 高
4 不適當配置處理 中高
5 目錄索引 中
6 備份檔案 中
弱點數長條圖
每頁顯示筆數: 10
檢測網址
檢測參數
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://www2.cyc.edu.tw/modules/piCal/
檢視

備份檔案

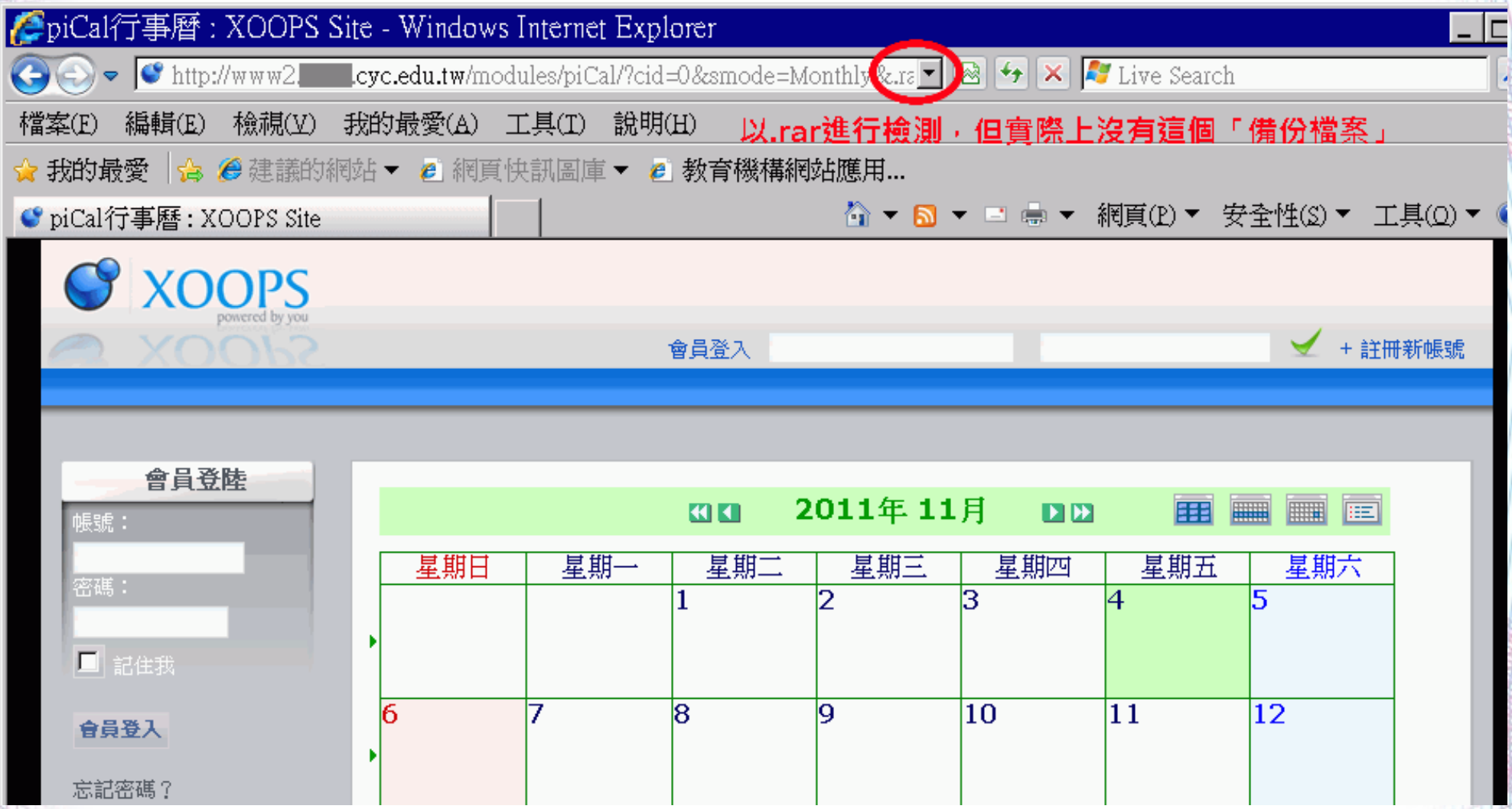
- 定義說明：
  - 此處「備份檔案」並不是指備份檔案的「動作」
    而是「把備份的檔案放在網路上可直接存取的位置」
- 範例說明：
  - 某些軟體在修改檔案時，會自動調整副檔名
  - 如修改 test.php 時自動生成 test.php.bak（←備份檔案）
  - 若管理者未移除 test.php.bak 就將整個資料夾直接上傳
    而 test.php 藏有機敏資料就可能被利用，如下面
    - http://hc.cyc.edu.tw/temp/test.php
    - http://hc.cyc.edu.tw/temp/test.php.bak

備份檔案

- 可能影響：
  - 洩漏重要資料，如管理帳號密碼、資料庫帳號密碼等
  - 如果有目錄索引弱點，此弱點會馬上現形。
- 檢測方法：

  加上 .rar .bak 等字串，如有回應就判斷為弱點。
- 誤判情形：
  - XOOPS 的 piCal 模組帶了字串會有回應讓系統誤判。
- 處理方式：刪除
- 本次並未檢測此一弱點。

備份檔案

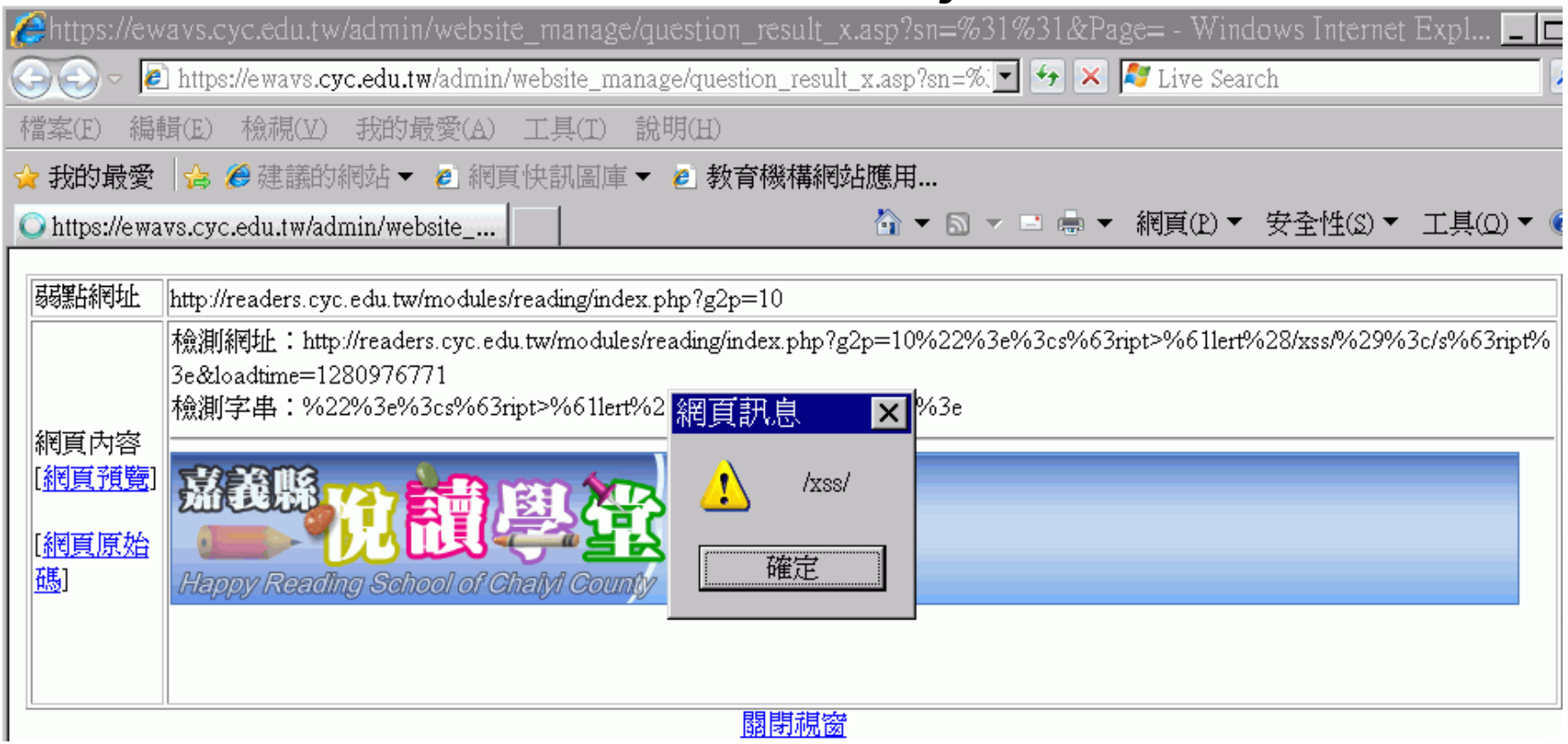

piCal行事曆 : XOOPS Site - Windows Internet Explorer
http://www2.[redacted].cyc.edu.tw/modules/piCal/?cid=0&smode=Monthly&.ra
Live Search
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
以.rar進行檢測，但實際上沒有這個「備份檔案」
我的最愛
建議的網站
網頁快訊圖庫
教育機構網站應用...
piCal行事曆 : XOOPS Site
網頁(P)
安全性(S)
工具(O)
XOOPS
powered by you
會員登入
+ 註冊新帳號
會員登陸
帳號：
密碼：
記住我
會員登入
忘記密碼？
2011年 11月
星期日 星期一 星期二 星期三 星期四 星期五 星期六
1 2 3 4 5
6 7 8 9 10 11 12

管理網站的注意事項

- 只把必要資料放到網站上
- 有的學校會將網站整個用 FTP 複製回去←這部份 OK
  然後又上傳到網頁空間的某處←這是沒有必要的
  - 舊資料可能沒有修補弱點
  - 舊資料可能藏有機敏資料
  - 雞蛋放在同一個籃子無助於分散風險

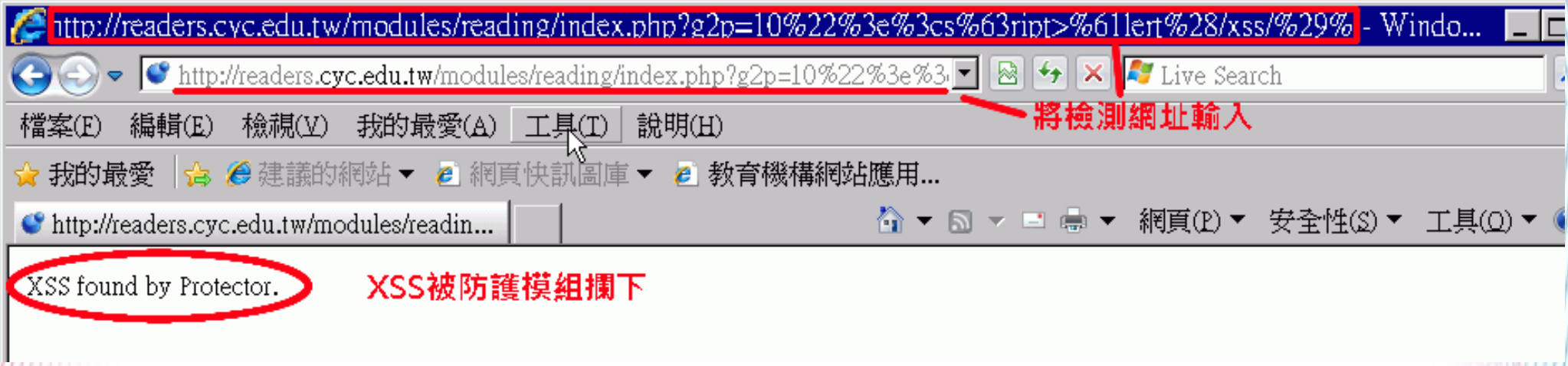
XOOPS 防護模組

- 使用 XOOPS 務必安裝、開啟防護模組
- 防護模組可攔阻 XSS 、 SQL Injection 攻擊



未安裝防護模組，以 XSS 攻擊測試成功

XOOPS 防護模組



安裝防護模組後再測試，將檢測網址輸入網址列，結果 XSS 攻擊被攔下

檢測原理與限制

- 檢測原理：
  - 上網用搜尋引擎搜尋網址，將這些存到資料庫中
  - 檢測搜尋到的網址是否有弱點
- 檢測限制：
  - 全新的網站很可能檢測不出弱點，需持續追蹤
    - 某校網站剛建置時未檢出弱點，這次掃描發現中毒已深
  - 轉址網站檢測不出弱點
    - 部份學校有兩份報告的原因
  - 若主網站由縣網託管，資料連結到其他主機，系統只能測到託管的部份
    - 此時檢測無弱點也只是託管的部份沒有弱點

報告完畢