# 教育機構網站應用程式弱點監測平台

# 使用手冊(精簡版v 1.0)

委託機關（單位）：教育部

成大資通安全研發中心 製

服務專線：06-2761204

中華民國 100 年 2 月

# 版本修訂記錄

| 日　　期 | 修訂說明 | 版　　次 |
| --- | --- | --- |
| | | |
| | | |

# 目　次

# 圖　目　次



# 表　目　次

# 1. 前言

## 1.1. 平台簡介

在網站入侵事件層出不窮，自動化攻擊工具輩出的時代，身為網站管理者該如何即時監控所轄網站是否無弱點，以避免駭客入侵。

本系統由教育部補助成大資通安全研發中心團隊，藉由檢測地方政府網站之經驗，開發出網站應用程式弱點之自動化檢測平台，檢測平台可自動化的執行網站應用程式弱點檢測，並提供網站管理者發現弱點後之修復建議報告與網站弱點趨勢圖等分析報表作為未來網站安全決策之參考。

教育部推動之網站應用程式弱點監測平台除了成大資通安全研發中心團隊主站外，各區縣(市)網路中心也建立分區平台(網址請參考本手冊 Q&A 第 3.12 條)，各連線學校可至已設立之所屬區域網路中心或縣(市)教育網路中心申請使用。


圖1　弱點監測平台畫面

## 1.2. 教育機構資安責任分級

依據行政院國家資通安全會報 98 年 6 月 1 日資安發字第 0980100328 號函「資訊安全責任等級分級作業施行計畫」，針對各級單位皆規定每年需進行至少 1 次以上網站安全弱點檢測，並配合參與相關的教育訓練，以滿足規定之時數；因此，各教育單位僅需定期向所屬區網/縣市網路中心申請檢測服務，即可滿足行政院的要求，更能提升網站防護安全。各類資安系統等級應執行之工作事項如下：

表 1 資訊安全責任分級表

| 作業名稱 / 等級 | 防護縱深 | ISMS 推動作業(註一) | 稽核方式 | 資安教育訓練(一般主管、資訊人員、資安人員、一般使用者(註二)) | 專業證照(註四) | 檢測機關網站安全弱點 |
|---|---|---|---|---|---|---|
| A 級 | NSOC 直接防護/ SOC 自建或委外、IDS、防火牆、防毒、郵件過濾裝置 | 通過第三者驗証 | 每年至少 2 次內稽 | 1. 每年至少(3、6、18、3 小時)<br>2. 資訊人員、資安人員需通過資安職能鑑定(註三) | 維持至少 2 張資安專業證照 | 每年2次 |
| B 級 | SOC(選項)、IDS、防火牆、防毒、郵件過濾裝置 | 通過第三者驗証 | 每年至少 1 次內稽 | 1. 每年至少(3、6、16、3 小時)<br>2. 資訊人員、資安人員需通過資安職能鑑定(註三) | 維持至少 1 張資安專業證照 | 每年1次 |
| C 級 | 防火牆、防毒、郵件過濾裝置 | 自行成立推動小組規劃作業 | 自我檢視 | 每年至少(2、6、12、3 小時) | 資安專業訓練 | 每年1次 |
| D 級 | 防火牆、防毒、郵件過濾裝置 | 推動 ISMS 觀念宣導 | 自我檢視 | 每年至少(1、4、8、2 小時) | 資安專業訓練 | 每年1次 |

註一：驗證範圍應涵蓋機關（構）之核心業務資訊系統，並逐步擴大至全單位。

註二：

1、一般主管：擔任主管職務相關人員，如機關(副)首長、部門主管(含資訊主管)等。

2、資訊人員：負責資訊作業相關人員，如系統分析設計人員、系統設計人員、系統管理人員及系統操作人員等。

3、資安人員：負責資通安全業務相關人員，如資安管理人員、資安稽核人員等。

4、一般使用者：一般業務、行政、會計、總務人員等單位內資訊系統的使用者。

註三：資安職能鑑定科目包括：資通安全管理制度、資訊系統風險評鑑、資通安全稽核、政府資訊作業委外安全、資安事件應變作業、電子資料保護、電子郵件安全及 WEB 應用程式安全等，A、B 級機關(構)之資訊人員、資安人員需參加行政院研考會規劃辦理之資安訓練並通過鑑定。

註四：由國內外獨立認驗證機構所核發之資安專業證照(非針對特定廠牌產品之證照)，例如資安管理類之 ISO27001 主導稽核員（Lead Auditor, LA）、資訊安全經理人（Certified Information Security Manager, CISM）、系統安全從業人員（Systems Security Certified Practitioner, SSCP）、資訊安全管理師（Certification for Information System Security Professional, CISSP）等及資安技術類之道德駭客（Certified Ethical Hacker, CEH）、全方位資訊安全專家（Global Information Assurance Certification, GIAC）等。

## 2. 會員系統

包含會員帳號申請、使用者登入、修改個人資料與檢測網站申請等功能。

### 2.1.1. 會員申請

- 在平台中，點選「會員專區」選項後，點選「加入會員」按鈕。


圖2　點選加入會員畫面

- 使用者請閱讀校園網站弱點檢測服務條款，並勾選「□我已充分閱讀並了解且接受以上之服務條款」，然後點擊「我接受」按鈕就可進到下一頁。
- 使用者請閱讀校園網站弱點檢測服務條款，並勾選「□我已詳細閱讀並清楚貴營運點願承擔的保密責任」，然後點擊「同意」按鈕就可進到下一頁。
- 進入會員申請頁面，使用者必須填寫[會員申請]與[網站檢測]申請資

訊，方可完成帳號申請手續。

■[會員申請]

- [會員申請]需填項目有：業務連絡人姓名、申請單位、申請單位的種類、帳號、密碼、E-Mail、業務連絡所在地、業務連絡電話與傳真資訊。
- 此部份皆為必填欄位(*號)。

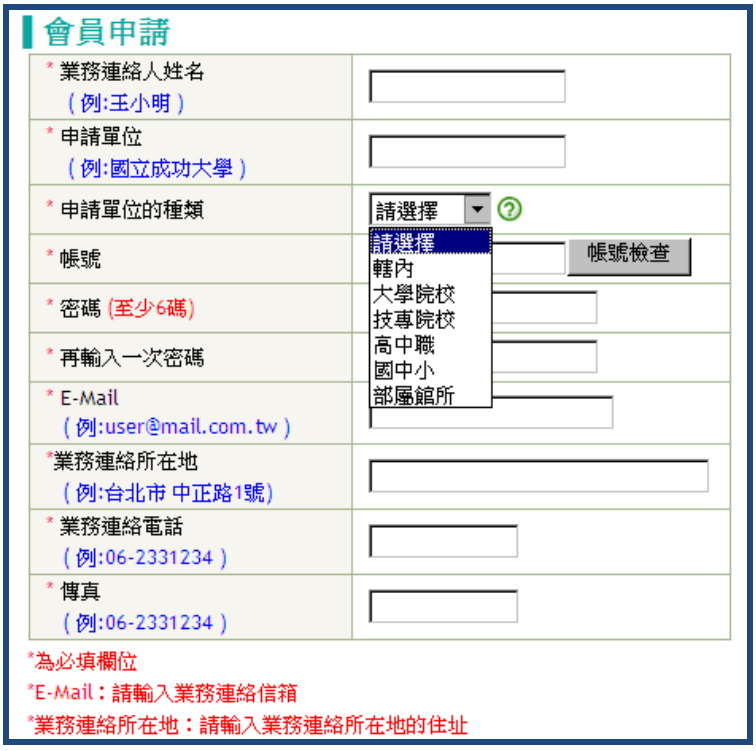



圖3　會員申請表格頁面

- 使用者輸入帳號後，可按「帳號檢查」按鈕查看此帳號是否重覆。

■[檢測網站申請]

- 檢測網站申請需填寫項目包含檢測網址與檢測網站名稱。
- 目前平台僅提供五組檢測網站申請欄位，欄位若不敷使用時，請於帳號申請通過後，再至【網站維護】選項頁面中新增其餘檢測網站。
- 會員申請和檢測網站申請填完後，點擊「申請」按鈕即可完成申請手續。

2.1.2. 會員資料修改

使用者進入平台後，可點選【會員修改】選項，以修改會員資料。

- 使用者登入後，點選「修改」按鈕。
- 進入會員資料修改頁面，即可修改欲更新之欄位。
- 除**帳號**與 **E-Mail** 無法變更之外，其餘欄位資料均可變更。
- 若欲修改 E-Mail，請點擊「聯絡我們」，於信件中輸入相關資訊，即可與系統管理者聯絡。
- 點選會員修改右下方的「修改」按鈕即修改完成。

## 2.2. 網站維護

- 使用者進入平台後，可點選【網站維護】選項，以進行檢測網站管理。
- 維護清單均為尚未排入檢測服務時程清單。
- 新增均需要再經由人工審核後，才可列入檢測服務。

### 2.2.1. 新增檢測網站

1. 填寫網站名稱。
2. 填寫網址。
3. 點擊新增後即可完成。

### 2.2.2. 刪除檢測網站

1. 在欲刪除的網站右邊點擊「刪除」按鈕。
2. 在刪除確認方塊點選「確定」即可完成。

## 2.3. 網站排程

- 使用者進入平台後，可點選【網站排程】選項，以進行網站排程設定管理。

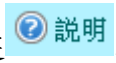
- 包含網站排程設定、已中斷排程設計與排程取消設定功能。


圖4　網站排程管理頁面

### 2.3.1. 網站排程

- 在檢測網址中下拉選擇欲檢測之網站。
- 選擇 XSS 檢測、SQL Injection 檢測時，可選擇是否使用「POST 檢測」。
- 點選 說明 連結，可檢視檢測類別的說明及注意事項。

- 選擇排程日期
- 點擊「後台頁面設定-開啟」連結後，可設定網站登入頁面資料、cookie 資料。

  點選 

連結，可檢視後台頁面登入設定教學。
- 點擊「送出」按鈕後，檢視排程確認，點擊「確定」後完成排程設定。

2.3.2. 設定已中斷排程

- 網站若未完成檢測動作，系統自動將之列為「已中斷排程」。
- 使用者需於【網站排程】/[設定已中斷排程]項目中，重新設定檢測時段，方可重新進行檢測工作。

2.3.3. 取消排程

- 在檢測網址中下拉選擇欲取消排程之檢測網站。
- 點選「取消排程按鈕」即可完成。
- 點選「繼續」就可回到網站排程畫面。

## 2.4. 網站結果

- 使用者進入平台後，可點選【網站結果】選項，查詢網站狀態。
- 使用者可瀏覽所有網站之檢測時間與檢測狀態。
- 檢測狀態分為：
  - 完成：受測網站已檢測完成，並完成分析報表。使用者直接點擊「完成」，即可瀏覽檢測報表。
  - 報表產生中：受測網站已檢測完成，尚等待平台報表產出。

– 進行中：受測網站正在進行檢測。

– 等待中：受測網站排程尚未到達檢測時間。

– 已中斷：受測網站未於設定的檢測時段內執行完弱點檢測或 Agent 中斷時，均無法進行網站檢測工作，系統將會自動發中斷通知信通知使用者。

## 2.5. 列印檢測同意書

- 使用者帳號申請審核通過後，即可登入平台。
- 登入後，可點選【列印檢測同意書】選項，以顯示列印頁面。
- 點選「請列印檢測同意書」，即可列印檢測同意書。
- 列印後，郵寄或傳真予所屬營運點之系統管理者(依各別網站管理作業不同，採線上申請或紙本作業，請洽本手冊 Q&A 第 3.11 條之各區縣(市)網路中心網站營運點管理者)。

## 3. 系統問與答(Q&A)

### 【教育機構網站應用程式弱點監測平台相關問題】

### 3.1. 教育機構網站應用程式弱點監測平台的功用？

Ans：

教育機構網站應用程式弱點監測平台主要提供 TANet 連線單位申請網站檢測服務，針對 SQL Injection、XSS、目錄索引、備份檔案、不適當配置處理、惡意檔案執行弱點，以自動化方式檢測申請單位轄下之網站，並產生掃瞄結果與修補建議報告，期能兼顧時效性與準確性，提升 TANet 資安防護水準。另外，監測平台（ 僅成大資通安全研發中心營運點 ）會主動蒐集各網站淪陷資訊，即時將 .edu.tw 淪陷網站清單傳送給教育部，以利於後續通知、修補之工作，後續將持續開發各項弱點及個人資料檢測服務。

### 3.2. 教育機構網站應用程式弱點監測平台服務對象？

Ans：

教育機構網站應用程式弱點監測平台主要之服務對象為 TANet 連線單位，只要各單位網站隸屬 TANet 連線單位皆可使用本監測平台之服務。

### 3.3. 教機構網站應用程式弱點監測平台有哪些檢測上之限制？

Ans：

(a). 只允許 TANet 連線單位申請使用服務。

(b). 僅提供申請單位進行所屬（ 管轄 ）網域內之網站檢測申請。

(c). 針對 XSS、SQL Injection、目錄索引、備份檔案、不適當配置處理、惡意檔案執行 弱點進行檢測。

(d). 需指定時段(早 06:00~18:00；晚 18:00~06:00)以進行檢測，若檢測時程超過指定時段，則系統將自行中斷。 (解決方式請參考檢測網站相關問題之

5) 。

(e). 監測平台對受測網站有設定時間限制(Request Timeout)，若超過時限 (30 分鐘)，則跳過該筆 URL 檢測，以掌控檢測時程。

(f). 受測網站之應用程式中，若含有 Flash 架構之 URL，可能無法順利進行弱點檢測(僅對於該筆 URL)。

(g). 監測平台檢測結果僅能作為單位 ( 校 ) 評估網站安全性之參考，不應為唯一依據，建議仍須使用其他檢測工具，以提升網站安全。

## 【申請使用相關問題】

### 3.4. 申請單位應由何種人員進行服務申請？

Ans：

由於本服務主要針對網站應用程式弱點進行檢測，因此建議各 TANet 連線單位應由負責網站維運或網站資訊安全之人員進行申請，而申請過程中所填寫之使用者資訊，應限於業務相關資訊，以便於日後負責人員承接之作業。

### 3.5. 使用者是否能變更個人資訊？

Ans：

使用者可以登入平台自行變更修改(帳號無法變更；E-Mail 則需向平台管理者聯繫，由管理者協助修改)。

## 【網站檢測相關問題】

### 3.6. 為何帳號申請未通過？

Ans：

貴單位帳號審核未通過可能原因如下：

(a). 貴單位已申請帳號。(目前單位僅開放申請一個帳號)。

(b). 使用者帳號聯絡資訊(業務聯絡所在地或聯絡電話)有誤。

需至監測平台重新申請，或與管理者聯絡。

### 3.7. 為何檢測網站申請未通過？

Ans：

貴單位受測網站審核未通過可能原因如下：

(a). 受測網址不在貴單位管轄範圍內。

(b). 受測網址填寫有誤。

需再次登入監測平台網站修改受測網站資訊，或與管理者聯絡。

### 3.8. 檢測網站資料是否可以變更？

Ans：

使用者可以登入監測平台，進入「網站維護」頁面，自行「新增」、「修改」及「刪除」檢測網站資訊。

### 3.9. 可否取消檢測排程？

Ans：

監測平台排程系統目前可接受取消距離現在時間 2 日後之排程。

### 3.10. 檢測過程中，為何會發生中斷？該如何處置？

Ans ：

監測平台檢測網站過程發生中斷，可能原因如下：

(a). 網站檢測工作無法在預定時程內完成檢測。

(b). 連線受測網站時，發生問題(請檢查貴單位網站是否正常運作)。

(c). 監測平台運作發生問題。

請再次登入監測平台設定網站檢測排程時間。若您重複遇到此問題，請與管理者聯絡。

### 3.11. 請問是否有詳細的操作手冊？

Ans ：

詳細操作手冊可至各營運點或總站（**http://ewavs.twisc.ncku.edu.tw/**）下載專區下載。

### 3.12. 各區網中心、縣市網中心與教育部所指定之教育機構營運點網址、聯絡人與聯絡方式為何?

Ans ：

以下資訊更新日期為 100 年 02 月 24 日，請以各營運點所提供資訊為主。

| 成大資安研發中心、教育部、中研院與全國十三區網中心資訊 | | | | |
|---|---|---|---|---|
| 區網名稱 | 聯絡人 | 聯絡電話 | E-mail | 各區網監測平台檢測申請網址 |
| 成大資安研發中心 | 林先生 | 06-2761204 | huisc@crypto.ee.ncku.edu.tw | http://ewavs.twisc.ncku.edu.tw/ |
| 教育部電算中心 | 余先生 | 02-77129088 | zongyan@mail.moe.gov.tw | http://ewavs.moe.edu.tw |
| 中央研究院 | 林先生 | 02-27899953 | arba@gate.sinica.edu.tw | http://waps.ascc.sinica.edu.tw |
| 高屏澎區網中心 | 周小姐 | 07-5252000 #2519 | kobejoy@staff.nsysu.edu.tw | http://ewavs.kpprc.edu.tw |
| 台南區網中心 | 陳先生 | 06-2757575 #61031 | jay24@mail.ncku.edu.tw | http://wavs.cc.ncku.edu.tw |
| 雲嘉區網中心 | 蕭先生 | 05-2720411 #14008 | vchsiao@ccu.edu.tw | http://ewavs.ccu.edu.tw |

| | | | | |
|---|---|---|---|---|
| 台中區網中心 | 鄭先生 | 04-22840306#765 | alancheng@nchu.edu.tw | http://waps.tcrc.edu.tw |
| 南投區網中心 | 李小姐 | 049-2910960#4045 | nyli@ncnu.edu.tw | http://ewavs.ntrc.edu.tw |
| 竹苗區網中心 2 | 李先生 | 03-5715131#80068 | tingchao@mx.nthu.edu.tw | http://ewavs.net.nthu.edu.tw |
| 竹苗區網中心 1 | 曾先生 | 03-5712121#52885 | ay529@mail.nctu.edu.tw | http://ewavs.hcrc.edu.tw |
| 桃園區網中心 | 邱先生 | 03-4227151#57516 | center38@cc.ncu.edu.tw | http://ewavs.tyc.edu.tw |
| 台北區網中心 1 | 李先生 | 02-33665012 | edward@ntu.edu.tw | http://mozart.cc.ntu.edu.tw |
| 台北區網中心 2 | 蔣先生 | 02-29393091#63315 | chieh@nccu.edu.tw | http://ewavs.nccu.edu.tw/ |
| 宜蘭區網中心 | 江先生 | 03-9357400#366 | ewavs@niu.edu.tw | http://ewavs.ilrc.edu.tw |
| 花蓮區網中心 | 楊先生 | 03-8632730 | moplay@mail.ndhu.edu.tw | http://ewavs.ndhu.edu.tw |
| 台東區網中心 | 林小姐 | 089-318855#2110 | show@nttu.edu.tw | http://ewavs.nttu.edu.tw |
| 縣市網路教育中心資訊 | | | | |
| 縣市網名稱 | 聯絡人 | 聯絡電話 | E-mail | 各區網監測平台檢測申請網址 |
| 基隆市網 | 王先生 | 02-24591311#304 | aa4220@mail.kl.edu.tw | http://webx.kl.edu.tw |
| 台北市網 | 蔡先生 | 02-27223004 | jdtsai@tp.edu.tw | http://webscan.tp.edu.tw |

| | | | | |
|---|---|---|---|---|
| 新北市網 | 林先生 | 02-80723456#542 | cangeroo@ntpc.edu.tw | http://ewavs.tpc.edu.tw |
| 新竹縣網 | 劉先生 | 03-5962103#308 | Hs3294@nc.hcc.edu.tw | https://ewavs.nc.hcc.edu.tw/ |
| 台中市網 | 劉先生 | 04-25295014 | brucelyc@tc.edu.tw | http://wscan.tcc.edu.tw |
| 嘉義市網 | 黃先生 | 05-2715325#15 | shanchin@mail.cy.edu.tw | http://ewavs.cy.edu.tw |
| 南投縣網 | 王先生 | 049-2241043#18 | admin@ntct.edu.tw | http://ewavs.ntct.edu.tw |
| 台南市網 | 張先生 | (06)213-0669#26 | hsinan@tn.edu.tw | http://webscan.tn.edu.tw |
| 高雄市網 | 張先生 | 07-7136536#52 | paar@mail.kh.edu.tw | http://websec.kh.edu.tw/ |
| 花蓮縣網 | 劉先生 | 03-846-2860#509 | an.feng@hlc.edu.tw | http://webscan.hlc.edu.tw/ |
| 嘉義縣網 | 吳先生 | 05-230-4464 | hirokofan@mail.cyc.edu.tw | http://ewavs.cyc.edu.tw/ |
| 新竹市網 | 林先生 | 03-524-9617#202 | tclin@hc.edu.tw | http://webscan.hc.edu.tw/ |
| 苗栗縣網 | 王先生 | 037-265087#11 | wloog@webmail.mlc.edu.tw | http://ewavs.mlc.edu.tw/ |
| 雲林縣網 | 陳先生 | 05-534-8221#004 | vcrvcr@ylc.edu.tw | http://security.ylc.edu.tw |
| 屏東縣網 | 楊先生 | 08-7364563 | minca@ptc.edu.tw | http://ewavs.ptc.edu.tw |