

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

# 中華電信數據通信分公司

## 網站偵防隊服務使用手冊

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

## 目 錄

|                                 |    |
|---------------------------------|----|
| 1. 網站偵防隊服務概述 .....              | 4  |
| 2. 申請網站偵防隊服務 .....              | 4  |
| 1. 如何登入企業資安服務網站 .....           | 4  |
| 2. 如何納管我的線路 .....               | 8  |
| 3. 如何修改資安通報聯絡資料 .....           | 12 |
| 1. 中華電信/HiNet 會員通報信箱查詢與修改 ..... | 12 |
| 2. 電路資安聯絡人查詢與設定 .....           | 14 |
| 3. 全球預警情報發送信箱查詢與修改 .....        | 15 |
| 4. 網站弱點掃描 .....                 | 15 |
| 1. 服務簡介 .....                   | 15 |
| 2. 服務功能操作說明 .....               | 16 |
| 5. 網站個資檢測 .....                 | 25 |
| 1. 服務簡介 .....                   | 25 |
| 2. 服務功能操作說明 .....               | 25 |
| 6. 網站掛馬檢測 .....                 | 33 |
| 1. 服務簡介 .....                   | 33 |
| 2. 服務功能操作說明 .....               | 33 |
| 7. 網站存活檢測 .....                 | 41 |
| 1. 服務簡介 .....                   | 41 |
| 2. 服務功能操作說明 .....               | 41 |
| 8. 網站竄改、惡意關鍵字檢測 .....           | 47 |
| 1. 服務簡介 .....                   | 47 |
| 2. 服務功能操作說明 .....               | 48 |

|   |             |      |      |
|---|-------------|------|------|
| 名稱  | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號  |             | 版次   | V1.0 |
| <p>9. 主機弱點掃描 ..... 63</p> <p>    1. 服務簡介 ..... 63</p> <p>    2. 服務功能操作說明 ..... 63</p> |             |      |      |

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

## 1. 網站偵防隊服務概述

中華電信為提出全方位的網站防護措施，推出「網站偵防隊」服務，服務含括：(1) 網站弱點掃描。(2) 網站個資檢測。(3) 網站掛馬檢測。(4) 網站存活檢測。(5) 網站竄改、惡意關鍵字檢測。以下各章節依序詳述各服務使用說明。

## 2. 申請網站偵防隊服務

### 1. 如何登入企業資安服務網站

步驟一：請先連至 HiNet 首頁：<http://www.hinet.net>，將畫面拉到網站最下方，點選畫面中企業資安服務的「網站偵防隊」選項。

|   |  |   |  |   |  |
|---|--|---|--|---|--|
| <b>寬頻上網</b><br>光世代<br>ADSL<br>Wi-Fi無線上網<br>IPv6申請<br>連線速率測試 | <b>網路安全</b><br>色情守門員<br>上網時間管理<br>行動健康上網<br>防毒防駭 / 線上掃毒  | <b>智慧家庭</b><br>經濟型<br>實用型<br>豪華型                              | <b>HiNet用戶專屬</b><br>信箱(網頁郵件服務)<br>我的網頁<br>歡樂點<br>會員中心<br>個人雲                     | <b>生活情報</b><br>新聞<br>氣象<br>股市<br>命理<br>3D地圖 / 實價登錄<br>中華首頁(網路電話簿)<br>科技樂生活<br>妞時尚 | <b>購物訂票</b><br>數位商城<br>歡樂點商城<br>鐵路訂票<br>點數卡<br>中華支付(小額付款)<br>動態密碼鎖                         |
| <b>影音娛樂</b><br>中華影視<br>hichannel廣播<br>卡拉OK(KOD)<br>遊戲       | <b>部落格/粉絲團</b><br>Xuite隨意窩<br>相簿 / 日誌 / Mlog<br>hichannel粉絲團<br>HiNet say Hi粉絲團<br>光世代粉絲團<br>卡拉OK(KOD)粉絲團<br>PO新聞粉絲團 | <b>便民服務</b><br>鐵路訂票<br>地政<br>航港<br>公路監理<br>政府採購<br>票據<br>政府網路 | <b>客服/繳費</b><br>障礙櫃台<br>客服Q博士<br>客服APP<br>常用客戶服務<br>線上繳費<br>電子帳單<br>電子發票<br>服務據點 | <b>企業網路</b><br>企業上網<br>VPN企業內部網路  | <b>雲端hicloud</b><br>CaaS雲運算<br>VPC虛擬私雲<br>Box(e)資料櫃<br>S3雲儲存<br>PaaS雲創平台<br>Mall雲市集<br>微軟雲 |
| <b>IDC網路資料中心</b><br>基本服務<br>加值服務<br>專案服務                    | <b>企業資安</b><br>郵件守門員<br>安全評估<br>網站偵防隊<br>入侵防護<br>企業防駭防駭<br>DDoS進障防護<br>上網內容過濾<br>動態密碼鎖                               | <b>物聯網</b><br>千里眼(雲端監錄)<br>eHome智慧家庭<br>iEN智慧節能<br>ITS智慧運輸    | <b>企業架站</b><br>hi-Hosting企業架站<br>網域註冊(買網址)                                       | <b>整合通信</b><br>hiBox全能信箱<br>hiMail企業郵件<br>企業簡訊<br>數據語音<br>網際傳真                    | <b>企業影音</b><br>hievent雲端影音<br>視訊會議<br>企業學習<br>放心播(公播音樂)                                    |

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

步驟二：請點選畫面右上方的「會員登入」，以便連結至會員登入專區。

**HiNet 企業資安服務**

產品訊息 | 最新消息 | 成功案例 | 媒體報導 | 下載專區 | FAQ

首頁 > 檢測 (工具) > 網站偵防隊 > 網站偵防隊介紹

網站偵防隊介紹

### 服務簡介

「網站偵防隊」是以雲端掃描的方式，從中華電信機房端掃描客戶網站的資安服務。不論是使用哪一家ISP、或是網站放在何處，都不需要額外安裝軟體或是更動網路架構，只要提供URL，即可使用「網站偵防隊」服務。

「網站偵防隊」並提供簡單友善的使用者介面，方便您進行各項功能設定（詳見下方「使用方式」）。

### 服務內容

**定期檢測，每月提供報表**

**1.網頁弱點掃描:**  
利用高效率網頁弱點掃描工具協助企業發現網站管理的設定不當或網頁應用程式的漏洞，對發現的網頁應用程式的安全弱點進行交叉比對分析，並且提供改善建議及統計報表資訊。

**2.網站個資檢測:**  
檢測客戶網站上，是否存在個資，如：身份證字號、手機號碼、信用卡號、住址、電子郵件、出生年月日等。可支援一般網頁、及可下載文件檔（RAR壓縮檔、MS Office、PDF...等文件）。

**網頁監控，即時異常告警**

**3.網頁掛馬檢測:**  
以HiNet SOC資安團隊自行開發之技術，模擬真實網頁瀏覽行為，透過程式碼與異常行為分析模型，並結合龐大HiNet網路惡意行為資料庫，有效發現隱藏於網頁中的惡意程式及木馬。

步驟三：請先登入中華電信會員中心。（若您已擁有會員中心的帳號，則請跳過以下步驟；若您無會員中心的帳號，則請您點選畫面下方的「加入會員」按鈕，即可免費註冊一組新的中華電信會員中心帳號）

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |



|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

步驟四：請選擇畫面右方「Email 註冊」或「手機註冊」進行註冊。



### 加入會員

一個帳號，隨意通行

歡迎您加入中華電信，  
請選擇您想使用的會員帳號。  
只要一個帳號，  
您可以盡享各項中華電信優質服務。



Email註冊      手機註冊

手機號碼

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

## 2. 如何納管我的線路

步驟一：登入中華電信會員後，請點選左方功能選單中的「群組電路」。

中華電信 | HiNet首頁  
會員 [ ] 您好

HiNet 企業資安服務

我的產品 會員登出 我要申租

產品訊息 最新消息 成功案例 媒體報導 下載專區 FAQ

產品監看中心  
 ■ 資安防護概表  
 ■ 資安事件告警紀錄  
 ■ 下載專區  
 ■ 全球預警情報

設定  
 ■ **群組電路**  
 ■ 擷取聯絡資料  
 ■ 電路資料修改

首頁 > 設定 > 群組電路

群組電路

新增電路

請輸入用戶號碼與密碼以新增至我的產品，做群組管理。

用戶號碼:

用戶密碼:

新增至我的產品

我的產品

| 未分群組 |      |      |      |
|------|------|------|------|
| [ ]  | 1007 | 自訂名稱 | 自訂群組 |
| [ ]  | 599  | 自訂名稱 | 自訂群組 |
| [ ]  | [ ]  | 自訂名稱 | 自訂群組 |

移出我的產品



|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

步驟二：請輸入使用網站偵防隊服務的用戶號碼及密碼（若您不清楚用戶號碼及密碼之使用方式，請點選畫面中「用戶號碼與密碼說明」按鈕），再點選「新增至我的產品」按鈕，即可將線路帳號匯入所屬的中華電信會員中心帳號以便觀看報表。

新增至我的產品成功後，畫面下方「我的產品」欄位將出現您所新增的記錄。

The screenshot shows the HiNet Enterprise Security Service portal. The main content area is titled '群組電路' (Group Circuit). A form titled '新增電路' (Add Circuit) prompts the user to '請輸入用戶號碼與密碼以新增至我的產品，做群組管理。' (Please enter user ID and password to add to my products for group management). The form has two input fields: '用戶號碼:' (User ID) and '用戶密碼:' (User Password). Below the form is a blue button labeled '新增至我的產品' (Add to My Products). To the left is a navigation menu with '設定' (Settings) expanded to show '群組電路' (Group Circuit) selected. Below the form is a table titled '我的產品' (My Products) with the following data:

| 未分群組       |      |      |      |
|------------|------|------|------|
| [Redacted] | 1007 | 自訂名稱 | 自訂群組 |
| [Redacted] | 599  | 自訂名稱 | 自訂群組 |

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

步驟三：請點選左方功能選單中的「下載專區」。

HiNet 企業資安服務

我的產品 會員登出 我要申租

產品訊息 最新消息 成功案例 媒體報導 下載專區 FAQ

產品監看中心

- 資安防護報表
- 資安事件告警紀錄
- 下載專區**
- 全球預警情報

設定

- 群組電路
- 通報聯絡資料
- 電路資料修改

首頁 > 產品監看中心 > 下載專區

下載專區

| 項次 | 方案名稱                                       | HN   | 公司名稱              | 資安服務名稱      | 起租日期       | 下載 |
|----|--|------|-------------------|-------------|------------|----|
| 1  | HiNet UTM代管服務超值旗艦方案(UTM設備租用+現場安裝維護+防護代管方案) | 1007 |                   | UTM代管服務     | 2008-09-01 | 下載 |
| 2  | 是方IDC入侵防護服務                                | 599  |                   | 入侵防護服務(施工中) | 2011-12-27 | 下載 |
| 3  | HiNet入侵防護服務(多機型), 前三個月免收費, 第四個月起每月499元     | 710  | 中華電信股份有限公司數據通信分公司 | 入侵防護服務      | 2007-03-26 | 下載 |
| 4  | HiNet資安艦隊2009方案(內含HiNet UTM代管服務, 需綁約兩年)    | 710  | 中華電信股份有限公司數據通信分公司 | UTM代管服務     | 2009-02-17 | 下載 |

步驟四：您可於畫面下方瀏覽已申請的資安服務，您可點選資安服務類別的服務進入管理介面，例如要進入「網站偵防隊」管理介面，請點選「網站偵防隊」，即可進入管理介面。

產品監看中心

- 資安防護報表
- 資安事件告警紀錄
- 下載專區**
- 全球預警情報

設定

- 群組電路
- 通報聯絡資料
- 電路資料修改

首頁 > 產品監看中心 > 下載專區

下載專區

| 項次 | 方案名稱       | HN | 公司名稱 | 資安服務名稱       | 起租日期       | 下載 |
|----|------------|----|------|--------------|------------|----|
| 1  |            |    |      | 網站個資檢測服務     | 2012-08-14 | 下載 |
| 2  |            |    |      | 入侵防護服務       | 2014-04-16 | 下載 |
| 3  |            |    |      | DDoS防護服務     | 2014-12-18 | 下載 |
| 4  |            |    |      | 入侵防護服務       | 2012-11-12 | 下載 |
| 5  | 網站偵防隊(月租型) |    |      | <b>網站偵防隊</b> | 2014-10-21 | 下載 |
| 6  | 網站偵防隊(月租型) |    |      | 網站偵防隊        | 2014-10-24 | 下載 |
| 7  | 網站偵防隊(月租型) |    |      | 網站偵防隊        | 2014-10-24 | 下載 |

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

步驟五：請點選「下載」按鈕，即可下載本服務之報表操作說明。

產品監看中心 > 產品監看中心 > 下載專區

下載專區

| 項次 | 方案名稱       | HN         | 公司名稱       | 資安服務名稱   | 起租日期       | 下載 |
|----|------------|------------|------------|----------|------------|----|
| 1  | [Redacted] | [Redacted] | [Redacted] | 網站個資檢測服務 | 2012-08-14 | 下載 |
| 2  | [Redacted] | [Redacted] | [Redacted] | 入侵防護服務   | 2014-04-16 | 下載 |
| 3  | [Redacted] | [Redacted] | [Redacted] | DDoS防護服務 | 2014-12-18 | 下載 |
| 4  | [Redacted] | [Redacted] | [Redacted] | 入侵防護服務   | 2012-11-12 | 下載 |
| 5  | 網站偵防隊(月租型) | [Redacted] | [Redacted] | 網站偵防隊    | 2014-10-21 | 下載 |
| 6  | 網站偵防隊(月租型) | [Redacted] | [Redacted] | 網站偵防隊    | 2014-10-24 | 下載 |
| 7  | 網站偵防隊(月租型) | [Redacted] | [Redacted] | 網站偵防隊    | 2014-10-24 | 下載 |

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

### 3. 如何修改資安通報聯絡資料

當用戶租用企業上網內容過濾服務之後，系統會提供定期報表寄送及事件通報等服務，客戶可依下列說明查詢或修改接收資安通報的聯絡資料。

#### 1. 中華電信/HiNet 會員通報信箱查詢與修改

步驟一：請登入企業資安服務網站（詳細步驟請參考本說明手冊「二、申請企業上網內容過濾服務」→「1. 如何登入企業資安服務網站」）。

步驟二：欲查詢中華電信/HiNet 會員聯絡資料請點選左方功能選單中的「通報聯絡資料」。

**HiNet 企業資安服務**

我的產品 | 會員登出 | 我要申租

產品訊息 | 最新消息 | 成功案例 | 媒體報導 | 下載專區 | FAQ

首頁 > 設定 > 通報聯絡資料

通報聯絡資料

電路資安聯絡人

| 通報項目       | 說明         | 適用服務   | 通報形式        | 通報人員  |
|------------|------------|--|-------------|---|
| 企業資安服務週報摘要 | 提供每週防護摘要報表 | <ul style="list-style-type: none"> <li>入侵防護服務</li> <li>DDoS進階防護服務</li> <li>企業上網內容過濾服務</li> <li>APT狙擊手</li> </ul> | 電子郵件 (每週定期) | 中華電信/HiNet會員  |
| 入侵防護服務週報   | 提供每週防護完整報表 | 入侵防護服務   | 電子郵件 (每週定期) | <ul style="list-style-type: none"> <li>中華電信/HiNet會員</li> <li>電路資安聯絡人</li> </ul> |
| 資安事件通報     | 發現資安事件立即通報 | 入侵防護服務週報   | 電子郵件 (24hr) | <ul style="list-style-type: none"> <li>中華電信/HiNet會員</li> <li>電路資安聯絡人</li> </ul> |

中華電信 / HiNet會員

聯絡人 | 電子郵件信箱

步驟三：畫面中第二項「中華電信/HiNet 會員」的聯絡人資訊，即為入侵防護服務之通報聯絡資訊。

中華電信 / HiNet會員

聯絡人 | 電子郵件信箱

HiNet防毒防駭 | [Redacted Email Address]

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

步驟四：如欲新增或修改通報聯絡資訊，請先登入中華電信會員中心：  
<http://member.hinet.net/MemberCenter/index.jsp>，並點選畫面左方選單的「帳號與聯絡資訊設定」。



步驟五：於「連絡信箱」項目，點選「立即設定」按鍵，即可修改通報聯絡信箱。



|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

## 2. 電路資安聯絡人查詢與設定

步驟一：請登入企業資安服務網站（詳細步驟請參考本說明手冊「二、申請 HiNet 入侵防護服務」→「1. 如何登入企業資安服務網站」）。

步驟二：欲查詢電路資料請點選左方功能選單中的「電路資料修改」。

HiNet 企業資安服務

產品訊息 | 最新消息 | 成功案例 | 媒體報導 | 下載專區 | FAQ

產品監看中心

- 資安防護報表
- 資安事件告警紀錄
- 下載專區
- 全球預警情報

設定

- 群組電路
- 通報聯絡資料
- 電路資料修改**

首頁 > 設定 > 電路資料修改

電路資料修改

- 點選[用戶號碼]：固定IP之服務，用戶可查詢電路的MRTG流量圖。
- 點選[用戶名稱]：固定IP之服務，用戶可查詢或修改用戶CPE資料。
- 點選[用戶IP]：固定IP8個月以上之服務，用戶可查詢TWNIC whois database所登記之IP資料。

| 產品名稱 | 用戶號碼 | 用戶名稱 | 連線速度  | 使用狀態 | 用戶IP  |
|------|------|------|-------|------|-------|
| N/A  | 1007 |      | /100M | 使用中  | 203.7 |
|      | 898  |      | /未知   | 使用中  |       |
|      | 899  | 測試產品 | /未知   | 使用中  |       |
|      | 899  |      | /未知   | 使用中  |       |
|      | 899  |      | /未知   | 使用中  |       |

步驟三：畫面中點選「用戶名稱」即可查詢或修改電路連絡資料。

HiNet 企業資安服務

產品訊息 | 最新消息 | 成功案例 | 媒體報導 | 下載專區 | FAQ

產品監看中心

- 資安防護報表
- 資安事件告警紀錄
- 下載專區
- 全球預警情報

設定

- 群組電路
- 通報聯絡資料
- 電路資料修改**

首頁 > 設定 > 電路資料修改

電路資料修改

- 點選[用戶號碼]：固定IP之服務，用戶可查詢電路的MRTG流量圖。
- 點選[用戶名稱]：固定IP之服務，用戶可查詢或修改用戶CPE資料。
- 點選[用戶IP]：固定IP8個月以上之服務，用戶可查詢TWNIC whois database所登記之IP資料。

| 產品名稱 | 用戶號碼 | 用戶名稱 | 連線速度  | 使用狀態 | 用戶IP  |
|------|------|------|-------|------|-------|
| N/A  | 1007 |      | /100M | 使用中  | 203.7 |
|      | 898  |      | /未知   | 使用中  |       |
|      | 899  | 測試產品 | /未知   | 使用中  |       |
|      | 899  |      | /未知   | 使用中  |       |
|      | 899  |      | /未知   | 使用中  |       |

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

### 3. 全球預警情報發送信箱查詢與修改

步驟一：請登入企業資安服務網站（詳細步驟請參考本說明手冊「二、申請 HiNet 入侵防護服務」→「1. 如何登入企業資安服務網站」）。

步驟二：欲查詢全球預警情報發送信箱請點選左方功能選單中的「全球預警情報」。

The screenshot shows the HiNet Enterprise Security Service interface. The left sidebar has a menu with 'Global Alert Information' highlighted. The main content area is titled 'Global Alert Information' and contains a 'Modify Notification Settings' form. The form includes a 'Notification Conditions' section with checkboxes for Windows, Linux/Unix, Solaris, xBSD, 應用軟體, 網路設備, and 其他. Below this is a 'Risk Level' section with radio buttons for 高, 中以上, and 低以上. At the bottom, there is a 'Send E-Mail' checkbox and a text input field containing 'XXX@gmail.com'. A '確定' (Confirm) button is at the bottom right.

步驟三：畫面中「發送 E-Mail」即為全球預警情報發送信箱，可勾選或進行修改。

This screenshot is similar to the previous one but highlights the 'Send E-Mail' checkbox and the email address input field with a red box. The 'Send E-Mail' checkbox is currently unchecked, and the email address is 'XXX@gmail.com'. The '確定' (Confirm) button remains at the bottom right.

## 4. 網站弱點掃描

### 1. 服務簡介

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

網頁弱點掃描主要是協助企業發現網站管理的設定不當或網頁應用程式的漏洞，並且提供改善建議及統計摘要報表資訊。網頁弱點掃描服務是利用高效率網頁弱點掃描工具，針對目前已經發現的網頁應用程式安全弱點，將所得到的結果進行交叉比對分析，並提供弱點掃描分析報表，可依據建議改善措施，修補弱點，以降低遭受入侵的風險。

## 2. 服務功能操作說明

### a. 掃描設定

本功能提供用戶進行掃描 pattern 與定期檢測掃描時間設定。掃描模式依用戶需要可選擇 default、high\_risk\_only、sql\_injection、Google Hacking Database 與 CSRF。

**掃描設定**

※提供您設定定期檢測檢測模式、檢測啟動時間。  
 ※檢測啟動時間可設定每月第一至第三週間的時間。  
 ※檢測啟動時間為掃描工作派送至工作排程佇列時間，實際啟動時間依掃描資源而定。  
 ※檢測狀態可至掃描工作管理功能查詢。

**檢測設定值**

起始網址:

弱點分類項目:  default  high\_risk\_only  sql\_injection  Google Hacking Database  CSRF

於每月第幾週:

禮拜:

掃描開始時間(24小時制):

掃描時間設定則依用戶需要可選擇每月的第幾週，禮拜幾與指定小時啟動檢測，弱點分類與檢測時間選擇確定後，按下變更設定按鈕即完成設定。



|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

掃描設定

※提供您設定定期檢測檢測模式、檢測啟動時間。  
 ※檢測啟動時間可設定每月第一至第三週間的時間。  
 ※檢測啟動時間為掃描工作派送至工作排程佇列時間，實際啟動時間依掃描資源而定。  
 ※檢測狀態可至掃描工作管理功能查詢。

檢測設定值

起始網址

弱點分類項目  default  high\_risk\_only  sql\_injection  Google Hacking Database  CSRF

於每月第幾週

禮拜

掃描開始時間(24小時制)

### b. 定期檢測報表查詢

網站弱點服務每月會依用戶設定之檢測時間與 pattern 設定進行派送掃描，用戶可於掃描結束之後點選欲瀏覽的報表月份，再點選查詢按鈕進行查看掃描結果，如下圖所示月份選擇為七月，點選查詢則可查看該月份定期檢測報告。

定期檢測報表查詢

月份 Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 西元 2014

起始網址

依據選擇之月份，月報表將會呈現掃描資訊、弱點等級分布圖、本月與上個月分掃描差異統計、依弱點名稱與網頁列表進行弱點數量排序等內容，若欲下載報告離線瀏覽，可透過點選下載按鈕即可下載 PDF 格式之報告。

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

月份 Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 西元 2014

起始網址  查詢

**掃描資訊**

| 掃描時間                | 完成時間                | 掃描起始網址                                 | 下載PDF              |
|---------------------|---------------------|--|--------------------|
| 2014-07-07 09:17:20 | 2014-07-07 09:21:55 | http://203.74.210.81/portal/portal.php | <a href="#">下載</a> |

**弱點等級分布圖**

高風險 9%  
中風險 9%  
低風險 82%

**本月與前次掃描差異化統計表**

| 弱點風險等級 | 上月數量 | 本月數量 | 本次新增 |
|--------|------|------|------|
| 高風險    | 0    | 1    | 1    |
| 中風險    | 0    | 1    | 1    |
| 低風險    | 0    | 9    | 9    |
| 小計     | 0    | 11   | 11   |

若欲查看弱點名稱排名或依網頁列表排序之弱點詳細資料，可點選弱點數量上之連結，即可查看該弱點之弱點描述與修補建議，點選連結位置如下圖紅色方框所示。

**弱點名稱排名**

| 排名 | 弱點名稱                                     | 風險等級 | 數量 |
|----|--|------|----|
| 1  | Slow HTTP Denial of Service Attack       | 高    | 1  |
| 2  | User credentials are sent in clear text  | 中    | 1  |
| 3  | Possible sensitive directories           | 低    | 3  |
| 4  | Possible sensitive files                 | 低    | 2  |
| 5  | OPTIONS method is enabled                | 低    | 1  |
| 6  | Session Cookie without HttpOnly flag set | 低    | 1  |
| 7  | Login page password-guessing attack      | 低    | 1  |
| 8  | Session Cookie without Secure flag set   | 低    | 1  |

**依網頁列表**

| 網址                                    | 弱點數量 |
|---------------------------------------|------|
| http://203.74.210.81/portal/login.php | 2    |
| http://203.74.210.81/                 | 2    |
| http://203.74.210.81                  | 2    |
| http://203.74.210.81/portal/export    | 1    |
| http://203.74.210.81/portal/backup    | 1    |

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

## 網站弱點資訊

## 弱點資訊

| 網頁                   | 弱點名稱                               | 風險等級 | 掃描日期                |
|----------------------|------------------------------------|------|---------------------|
| http://203.74.210.81 | Slow HTTP Denial of Service Attack | 高    | 2014-07-07 09:17:20 |

**[弱點名稱]**

Slow HTTP Denial of Service Attack

**[弱點描述]**

Your web server is vulnerable to Slow HTTP DoS (Denial of Service) attacks.

Slowloris and Slow HTTP POST DoS attacks rely on the fact that the HTTP protocol, by design, requires requests to be completely received by the server before they are processed. If an HTTP request is not complete, or if the transfer rate is very low, the server keeps its resources busy waiting for the rest of the data. If the server keeps too many resources busy, this creates a denial of service.

**[受影響參數]**
**[測試語法]**
**[回應訊息]**
**[建議修補方式]**

Consult Web references for information about protecting your web server against this type of attack.

**[參考資訊]**

Slowloris HTTP DoS  
<http://ha.ckers.org/slowloris/>  
 Slowloris DOS Mitigation Guide  
[http://www.funtoo.org/wiki/Slowloris\\_DOS\\_Mitigation\\_Guide](http://www.funtoo.org/wiki/Slowloris_DOS_Mitigation_Guide)  
 Protect Apache Against Slowloris Attack  
<http://blog.secaserver.com/2011/08/protect-apache-slowloris-attack/>

### c. 自我檢測報表查詢

自我檢測報表查詢提供用戶查詢自檢結果，用戶可從選擇起始網址的下拉選單選擇受檢測之網站，並選擇欲查看之自簡報表點選查詢按鈕即可查看詳細資訊。

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

自我檢測報表查詢

\*提供查詢與下載弱點掃描報表的功能  
\*點選特定報表可以在網頁上檢視報表詳細資訊

報表查詢

請選擇起始網址

檢測報表查詢

| 起始網址                                   | 掃描狀態 | 弱點數量 | 檢測開始時間              | 檢測結束時間              | 報表查詢 |
|--|------|------|---------------------|---------------------|------|
| http://203.74.210.82/tobyreidemo/1.htm | 結束   | 3    | 2014-07-24 18:10:28 | 2014-07-24 18:13:55 | 查詢   |
| http://203.74.210.82/tobyreidemo/1.htm | 結束   | 3    | 2014-07-24 17:35:01 | 2014-07-24 17:39:56 | 查詢   |
| http://203.74.210.82/tobyreidemo/1.htm | 結束   | 3    | 2014-07-24 17:10:25 | 2014-07-24 17:13:55 | 查詢   |
| http://203.74.210.82/tobyreidemo/1.htm | 結束   | 3    | 2014-07-24 16:30:48 | 2014-07-24 16:33:55 | 查詢   |
| http://203.74.210.81/portal/portal.php | 結束   | 11   | 2014-07-22 18:11:24 | 2014-07-22 18:15:55 | 查詢   |
| http://203.74.210.81/portal/portal.php | 結束   | 11   | 2014-07-22 16:30:56 | 2014-07-22 16:35:56 | 查詢   |
| http://203.74.210.81/portal/portal.php | 結束   | 11   | 2014-07-22 13:56:05 | 2014-07-22 14:01:55 | 查詢   |
| http://203.74.210.81/portal/portal.php | 結束   | 11   | 2014-07-17 18:05:39 | 2014-07-17 18:09:56 | 查詢   |

報告資訊中含有掃描資訊、弱點風險等級分布圖與弱點排名等資訊，若用戶欲下載報告離線瀏覽，可點選線上報告中的下載按鈕，即可下載 PDF 格式報告，如下圖所示。

自我檢測報表查詢

報表查詢

掃描資訊

| 掃描時間                | 完成時間                | 掃描網站網址                                 | 下載PDF |
|---------------------|---------------------|--|-------|
| 2014-07-24 18:10:28 | 2014-07-24 18:13:55 | http://203.74.210.82/tobyreidemo/1.htm | 下載    |

弱點等級分布圖

■ 高風險  
■ 中風險  
■ 低風險

中風險 33%

低風險 67%

若欲查看弱點詳細資訊，可透過點選弱點排名或依網頁列表排序弱點數量圖表中的弱點數量連結，即可查看該弱點之弱點描述與修補建議。

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

| 弱點排名 |  |      |    |
|------|--|------|----|
| 排名   | 弱點名稱   | 風險等級 | 數量 |
| 1    | PHP hangs on parsing particular strings as floating point number | 中    | 1  |
| 2    | TRACE method is enabled  | 低    | 1  |
| 3    | OPTIONS method is enabled  | 低    | 1  |

| 依網頁列表                |      |
|----------------------|------|
| 網址                   | 弱點數量 |
| http://203.74.210.82 | 3    |

| 網站弱點資訊   |  |      |                     |
|--|--|------|---------------------|
| 弱點資訊   |  |      |                     |
| 網頁   | 弱點名稱   | 風險等級 | 掃描日期                |
| http://203.74.210.82   | PHP hangs on parsing particular strings as floating point number | 中    | 2014-07-24 18:10:28 |
| <p><b>[弱點名稱]</b><br/>PHP hangs on parsing particular strings as floating point number</p> <p><b>[弱點描述]</b><br/>This alert was generated using only banner information. It may be a false positive.<br/>PHP hangs when parsing '2.2250738585072011e-308' string as a floating point number.<br/>Affected PHP versions: 5.3 up to version 5.3.5 and 5.2 up to version 5.2.17</p> <p><b>[受影響參數]</b></p> <p><b>[測試語法]</b></p> <p><b>[回應訊息]</b></p> <p><b>[建議修補方式]</b><br/>Upgrade PHP to the latest version.</p> <p><b>[參考資訊]</b><br/>PHP Hangs On Numeric Value 2.2250738585072011e-308</p> |  |      |                     |

#### d. 自我檢測

此功能提供用戶在定期檢測之外，每月可再依其需要進行一次自我檢測，用戶可在定期檢測執行完畢後，依據弱點修補描述完成修補之後，啟動自我檢測驗證是否將弱點完成修補。

在功能頁面將註明尚可使用自我檢測的起始網址與次數，如下圖紅色區塊所顯示，在自檢執行前，用戶可以其需求選擇掃描弱點分類，以及指定掃描時間。

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

### 自我檢測

※月租型用戶每月提供一次免費自我檢測掃描，當月未使用不予保留  
 ※有額外自我檢測需求，可購買計次制網站弱點掃描服務

※本月份可手動增加的檢測工作尚有：

http://203.74.210.81/portal/portal.php：1次 (2014-06-27 13:50:57申租月租型服務)  
 http://203.74.210.82/tobyreidemo/1.htm：1次 (2014-06-30 16:52:31申租月租型服務)  
 http://testphp.vulnweb.com：1次 (2014-06-30 16:54:40申租月租型服務)

#### 檢測設定值

起始網址

弱點分類項目  default  high\_risk\_only  sql\_injection  Google Hacking Database  CSRF

掃描開始日期

掃描開始時間(24小時制)

### e. 定期掃描工作管理

### 定期掃描進度管理

※提供您查詢所有的檢測工作・點選檢測工作可顯示該檢測工作的相關設定・

#### 檢測工作查詢

請選擇檢測起始網址

| 檢測工作列表 | 起始網址                                   | 狀態 | 派送時間                | 開始時間                | 完成時間                | 暫停/重啟檢測工作 |
|--------|--|----|---------------------|---------------------|---------------------|-----------|
|        | http://203.74.210.81/portal/portal.php | 結束 | 2014-09-01 08:59:53 | 2014-09-01 10:02:15 | 2014-09-01 10:07:52 | -         |
|        | http://203.74.210.81/portal/portal.php | 結束 | 2014-08-04 08:59:56 | 2014-08-04 10:01:37 | 2014-08-04 10:05:55 | -         |
|        | http://203.74.210.81/portal/portal.php | 結束 | 2014-07-07 08:59:55 | 2014-07-07 09:17:20 | 2014-07-07 09:21:55 | -         |

### f. 自我掃描工作管理

此功能是讓用戶可因其需要針對排程中或掃描中的網站進行暫停檢測或啟動檢測的管理。

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

正在進行掃描中的工作，用戶可以點選暫停，但點選暫停後，若需要重新檢測，掃描將重新開始無法接續暫停前的狀態。

自我掃描進度管理

※提供您查詢所有的檢測工作・檢測完成可以點選查詢查看檢測結果報表・

檢測工作查詢

請選擇檢測起始網址

檢測工作列表

| 起始網址                                   | 狀態  | 排程時間                | 開始時間                | 完成時間                | 暫停/重啟檢測工作 |
|--|-----|---------------------|---------------------|---------------------|-----------|
| http://203.74.210.81/portal/portal.php | 掃描中 | 2014-09-02 17:46:00 |                     |                     | 暫停檢測      |
| http://203.74.210.81/portal/portal.php | 結案  | 2014-07-22 09:00:00 | 2014-07-22 18:11:24 | 2014-07-22 18:15:59 | -         |
| http://203.74.210.81/portal/portal.php | 結案  | 2014-07-22 09:00:00 | 2014-07-22 16:30:56 | 2014-07-22 16:35:56 | -         |
| http://203.74.210.81/portal/portal.php | 結案  | 2014-07-22 09:00:00 | 2014-07-22 13:56:05 | 2014-07-22 14:01:55 | -         |
| http://203.74.210.81/portal/portal.php | 結案  | 2014-07-17 18:00:00 | 2014-07-17 18:05:35 | 2014-07-17 18:09:56 | -         |

自我掃描進度管理

※提供您查詢所有的檢測工作・檢測完成可以點選查詢查看檢測結果報表・

檢測工作查詢

請選擇檢測起始網址

檢測工作列表

| 起始網址                                   | 狀態   | 排程時間                | 開始時間                | 完成時間                | 暫停/重啟檢測工作 |
|--|------|---------------------|---------------------|---------------------|-----------|
| http://203.74.210.81/portal/portal.php | 暫停掃描 | 2014-09-02 17:46:00 | 2014-09-02 17:50:46 |                     | 重新檢測 取消掃描 |
| http://203.74.210.81/portal/portal.php | 結案   | 2014-07-22 09:00:00 | 2014-07-22 18:11:24 | 2014-07-22 18:15:59 | -         |
| http://203.74.210.81/portal/portal.php | 結案   | 2014-07-22 09:00:00 | 2014-07-22 16:30:56 | 2014-07-22 16:35:56 | -         |
| http://203.74.210.81/portal/portal.php | 結案   | 2014-07-22 09:00:00 | 2014-07-22 13:56:05 | 2014-07-22 14:01:55 | -         |
| http://203.74.210.81/portal/portal.php | 結案   | 2014-07-17 18:00:00 | 2014-07-17 18:05:35 | 2014-07-17 18:09:56 | -         |

對於尚在排程中的檢測工作則可變更檢測排程時間，畫面如下圖所示，點選變更時間將帶出設定排程時間畫面，原先排定 9/18 上午九點進行檢測派送，可透過網站功能修改為 9/24 下午五點三十分。

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

自我掃描進度管理

\*提供您查詢所有的檢測工作・檢測完成可以點選查詢查看檢測結果報表・

檢測工作查詢

請選擇檢測起始網址

檢測工作列表

| 起始網址                                   | 狀態  | 排程時間                | 開始時間                | 完成時間                | 暫停/重啟檢測工作   |
|--|-----|---------------------|---------------------|---------------------|---|
| http://203.74.210.81/portal/portal.php | 排程中 | 2014-09-18 09:00:00 |                     |                     | <input type="button" value="變更時間"/> <input type="button" value="取消掃描"/> |
| http://203.74.210.81/portal/portal.php | 結案  | 2014-07-22 09:00:00 | 2014-07-22 18:11:24 | 2014-07-22 18:15:55 | -   |
| http://203.74.210.81/portal/portal.php | 結案  | 2014-07-22 09:00:00 | 2014-07-22 16:30:56 | 2014-07-22 16:35:56 | -   |
| http://203.74.210.81/portal/portal.php | 結案  | 2014-07-22 09:00:00 | 2014-07-22 13:56:05 | 2014-07-22 14:01:55 | -   |
| http://203.74.210.81/portal/portal.php | 結案  | 2014-07-17 18:00:00 | 2014-07-17 18:05:35 | 2014-07-17 18:09:56 | -   |

Page 1 of 1 30 View 1 - 5 of 5

重新指派掃描時間

\*提供您查詢所有的檢測工作・檢測完成可以點選查詢查看檢測結果報表・

檢測工作查詢

檢測工作列表

| Domain                                 | 狀態  | 派送時間                | 排程時間                |
|--|-----|---------------------|---------------------|
| http://203.74.210.81/portal/portal.php | 排程中 | 2014-09-02 17:13:04 | 2014-09-17 14:00:00 |

將排程更改為：

時  
  
 分



|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

## 5. 網站個資檢測

### 1. 服務簡介

因應新版個資法公告生效，企業需對個資進行盤點。針對此需求網站偵防隊提供網站個資檢測服務，於遠端模擬使用者瀏覽網頁的行為對客戶網站進行個資盤點。檢測的個資項目包含：身分證字號、電話號碼、手機號碼、信用卡號、住址(目前僅支援台灣地區中文地址)、電子郵件、生日。檢測完成後並提供詳盡的報表，讓客戶可以清楚了解網站中個資的分佈。

### 2. 服務功能操作說明

#### a. 掃描設定

本功能提供用戶進行檢測項目設定、檢測忽略字設定、定期檢測啟動時間設定(預設於每月1號開始檢測)。

設定前請先選擇要設定哪一個起始網址。檢測項目共有：身分證字號、電話號碼、手機號碼、信用卡號、住址可供選擇。

**檢測參數設定**

※編輯檢測設定將會套用到所有新的檢測工作  
 ※定期檢測啟動時間設定適用定期檢測(預設每月的第一週星期一開始派送)  
 ※已被加入行列的檢測工作無法套用新的檢測設定  
 ※檢測忽略字最多可設定20筆  
 ※忽略字請勿輸入逗號

請選擇要設定的起始網址:

http://[redacted] (1970-01-01 申租月租型服務)

**檢測項目設定(適用所有檢測工作)**

身分證字號
  電話號碼
  手機號碼
  信用卡號
  地址
  電子郵件
  生日

定期檢測啟動時間設定可依用戶需要選擇每月的第幾週，禮拜幾與指定小時啟動檢測，各項目填寫完成後按下儲存設定即可完成。

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

定期檢測啟動時間設定

於每月第幾週

禮拜

檢測起始時間設定

~

檢測忽略字設定讓使用者設定欲忽略的個資，至多可設定 20 筆，設定好的忽略字在掃描時將不會被視為個資。新增忽略字請按下左下角的“+”號，輸入資料後按下確定即可新增。

檢測忽略字設定(適用所有檢測)

檢測忽略字(共0筆)

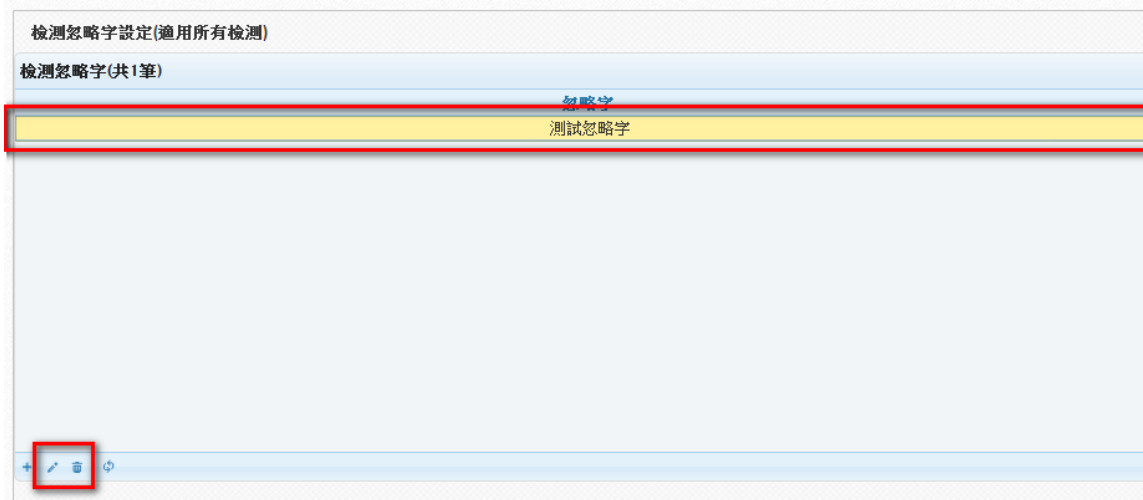
忽略字

資料新增

忽略字

欲修改、刪除忽略字請先點選要修改、刪除的資料後按下左下角的鉛筆、垃圾桶圖示。

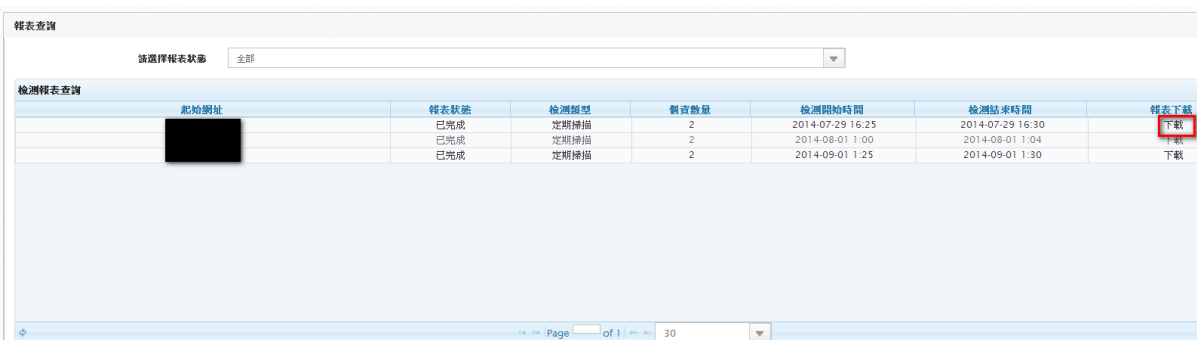
|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |



b. 定期檢測報表查詢

月租型客戶每月會固定派送定期檢測，掃描完成後的報表可在定期檢測報表查詢功能查詢。

點入此功能後可直接點選要下載的 PDF 報表：



或是點選想要查看詳細資訊的月份後，在網頁上呈現當月報表：

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

檢測報表檢視

顯示網站中可能存在的個資資料

報表資訊

| 起始網址       | 檢測開始時間              | 檢測結束時間              | IP位址       | 花費時間 | 網站大小   | 個資數量 |
|------------|---------------------|---------------------|------------|------|--------|------|
| [Redacted] | 2014-07-29 16:24:56 | 2014-07-29 16:25:56 | [Redacted] | 1分   | 142.3K | 2    |

圖餅圖

長條圖

- 50% 地址
- 50% 電話號碼

個資資料列表

| 編號 | 類型   | 個資內容          | 網址         |
|----|------|---------------|------------|
| 1  | 電話號碼 | (02)2324-XXXX | [Redacted] |
| 2  | 地址   | 台北市信義區XXXXX   | [Redacted] |

Page 1 of 1 30

同一個畫面也可以下載 PDF 或是修改報表(將在本章最後一個章節介紹)。

顯示網站中可能存在的個資資料

報表資訊

| 起始網址       | 檢測開始時間              | 檢測結束時間              | IP位址       | 花費時間 | 網站大小   | 個資數量 | 下載PDF              | 修改報表               |
|------------|---------------------|---------------------|------------|------|--------|------|--------------------|--------------------|
| [Redacted] | 2014-09-01 01:25:43 | 2014-09-01 01:26:43 | [Redacted] | 1分   | 142.3K | 2    | <a href="#">下載</a> | <a href="#">修改</a> |

圖餅圖

長條圖

- 50% 地址 數量: 1
- 50% 電話號碼 數量: 1

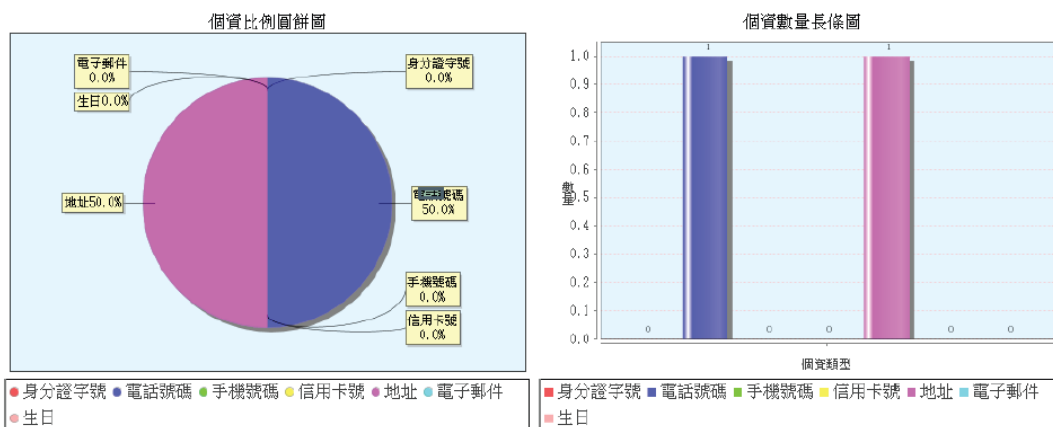
PDF 格式的報告：

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |



## 網站個資檢測服務報表

| 檢測網站       | 掃描開始時間              | 掃描結束時間              | 花費時間  | 網站大小   | IP位址       | 個資數量 |
|------------|---------------------|---------------------|-------|--------|------------|------|
| [REDACTED] | 2014-09-01 01:25:43 | 2014-09-01 01:26:43 | 0小時1分 | 142.3K | [REDACTED] | 2    |



個資資料列表

| 編號 | 類型   | 內容            | 網址                                     |
|----|------|---------------|--|
| 1  | 電話號碼 | (02)2324-xxxx | http://203.74.210.82/tobyreidemo/1.htm |
| 2  | 地址   | 台北市信義區xxxxx   | http://203.74.210.82/tobyreidemo/1.htm |

### c. 自我檢測報表查詢

計次型客戶及月租型客戶每月自行新增的檢測工作可在此功能查詢報表。

點入此功能後，與定期檢測相同，可直接下載 PDF 報表或是點擊想要查看詳細資訊的報表。

\*提供查詢與下載個資檢測報表的功能。  
\*點選特定報表可以在網頁上檢視報表詳細資訊

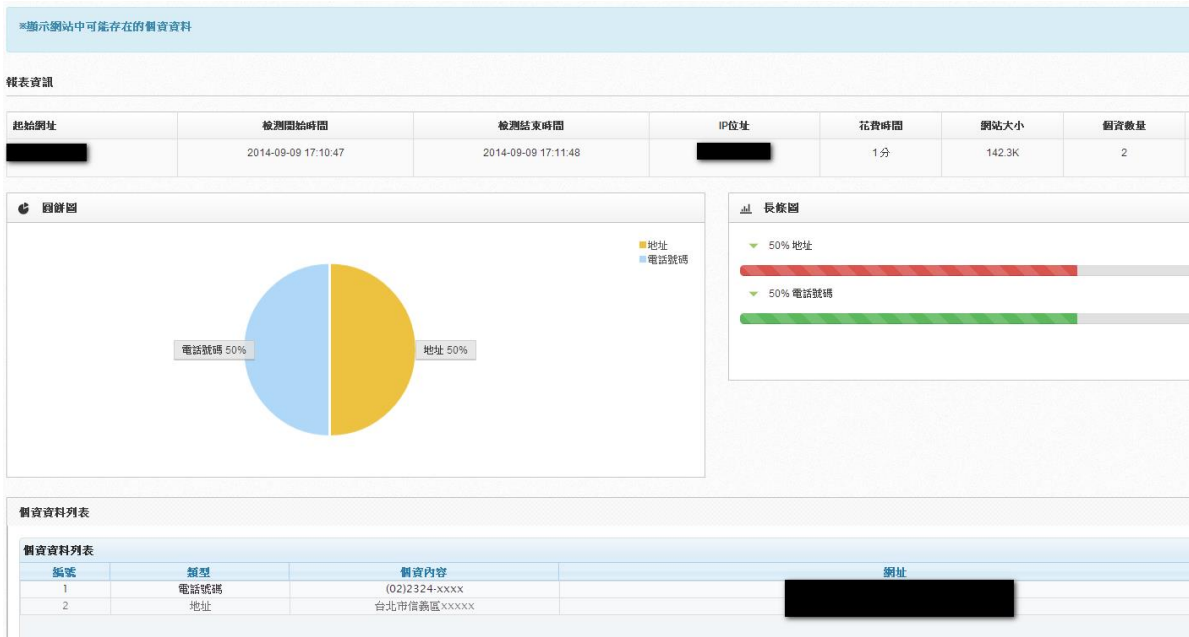
報表查詢

請選擇報表狀態: 全部

| 檢測報表查詢 | 起始網址       | 報表狀態 | 檢測類型 | 個資數量 | 檢測開始時間           | 檢測結束時間           | 報表下載  |
|--------|------------|------|------|------|------------------|------------------|---|
|        | [REDACTED] | 已完成  | 自我檢測 | 2    | 2014-09-09 17:10 | 2014-09-09 17:15 | <span style="border: 1px solid #ccc; padding: 2px;">下載</span> |

Page 1 of 1 | 30 | View 1 - 1 of 1

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |



#### d. 新增檢測工作

新增檢測工作規則：(1) 月租型服務之客戶，每月可免費新增 1 次檢測工作。(2) 計次型服務之客戶，可不限時間新增 1 次檢測工作。(3) 自行新增的檢測工作，請在自我檢測報表查詢功能查詢報表。

畫面中紅色的區塊會註明可新增檢測的次數。

※月租型服務之客戶，每月可免費新增1次檢測工作

※計次型服務之客戶，可不限時間新增1次檢測工作

※請您先在左方選單的「網站個資檢測」->「掃描設定」，確認您的檢測參數之後再新增檢測工作

※本月份可手動增加的檢測工作尚有：

|            |    |                     |
|------------|----|---------------------|
| ██████████ | 0次 | (1970-01-01申租月租型服務) |
| ██████████ | 1次 | (申租計次型服務)           |

選擇起始網址、檢測日期、啟動時間區間後，按下新增檢測工作即可完成新增。

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

新增檢測工作

請選擇檢測起始網址：

檢測日期：2014-09-10

檢測起始時間設定：00:00 ~ 24:00

e. 定期檢測工作管理

此功能提供月租客戶查詢每月定期檢測的執行狀況，若需暫停檢測、重新啟動檢測也可於此功能進行操作。

| 開始時間             | 完成時間             | 暫停/重啟檢測工作                           |
|------------------|------------------|-------------------------------------|
| 2014-09-09 17:10 | 2014-09-09 17:15 |                                     |
| 2014-09-09 17:35 | -                | <input type="button" value="暫停檢測"/> |

檢測工作列表

| 起始網址                 | 狀態                                  |
|----------------------|-------------------------------------|
| <input type="text"/> | <input type="button" value="檢測完成"/> |
| <input type="text"/> | <input type="button" value="暫停中"/>  |

暫停檢測後，可重新啟動檢測：

| 起始網址                 | 狀態                                 | 類型   | 加入時間             | 開始時間             | 完成時間             | 暫停/重啟檢測工作                           |
|----------------------|------------------------------------|------|------------------|------------------|------------------|-------------------------------------|
| <input type="text"/> | <input type="button" value="已暫停"/> | 自我檢測 | 2014-09-09 17:10 | 2014-09-09 17:10 | 2014-09-09 17:15 |                                     |
| <input type="text"/> |                                    | 自我檢測 | 2014-09-09 17:33 | 2014-09-09 17:35 | -                | <input type="button" value="重新檢測"/> |

f. 自我檢測工作管理

計次型客戶及月租型客戶每月自行新增的檢測工作可在此功能查看執行狀況。與定期檢測不同的是，若自我檢測尚未開始掃描，是可以刪除的。

| 加入時間             | 開始時間             | 完成時間             | 暫停/重啟檢測工作                           |
|------------------|------------------|------------------|-------------------------------------|
| 2014-09-09 17:10 | 2014-09-09 17:10 | 2014-09-09 17:15 |                                     |
| 2014-09-09 17:33 | -                | -                | <input type="button" value="刪除檢測"/> |

刪除掃描後，自檢使用的權力會還原到未使用的狀況。與定期檢測相同，自檢工作也可以暫停、重新啟動。

| 開始時間             | 完成時間             | 暫停/重啟檢測工作                           |
|------------------|------------------|-------------------------------------|
| 2014-09-09 17:10 | 2014-09-09 17:15 |                                     |
| 2014-09-09 17:35 | -                | <input type="button" value="暫停檢測"/> |

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

檢測工作列表

| 起始網址       | 狀態   |
|------------|------|
| [Redacted] | 檢測完成 |
|            | 暫停中  |

| 起始網址       | 狀態  | 類型   | 加入時間             | 開始時間             | 完成時間             | 暫停/重啟檢測工作 |
|------------|-----|------|------------------|------------------|------------------|-----------|
| [Redacted] | 已暫停 | 自我檢測 | 2014-09-09 17:10 | 2014-09-09 17:10 | 2014-09-09 17:15 |           |
|            |     | 自我檢測 | 2014-09-09 17:33 | 2014-09-09 17:35 |                  | 重新檢測      |

### g. 檢測報表修改

為增加產製報表的彈性，若客戶認為系統檢測出的個資是可以合法存在的個資，如網站常有的聯絡我們(電話、E-Mail)，客戶就可以利用此功能移除此類資料，並重新產製報表。

點選定期或自我檢測報表查詢，並按下要修改的報表：

定期檢測報表查詢

※提供查詢與下載個資檢測報表的功能  
 ※點選特定報表可以在網頁上檢視報表詳細資訊

報表查詢

請選擇報表狀態

檢測報表查詢

| 起始網址       | 報表狀態 | 檢測類型 |
|------------|------|------|
| [Redacted] | 已完成  | 定期掃描 |
|            | 已完成  | 定期掃描 |
|            | 已完成  | 定期掃描 |

Page 1 of 1

接著點選畫面右上方的修改報表：

| 檢測開始時間              | 檢測結束時間              | IP位址       | 花費時間 | 網站大小   | 個資數量 | 下載PDF                             | 修改報表                              |
|---------------------|---------------------|------------|------|--------|------|-----------------------------------|-----------------------------------|
| 2014-09-01 01:25:43 | 2014-09-01 01:26:43 | [Redacted] | 1分   | 142.3K | 2    | <input type="button" value="下載"/> | <input type="button" value="修改"/> |

畫面上方可依個資類型篩選資料、欲移除的資料請先點選表格左方的小方框後按下右上方的移除選取資料。



|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

請選擇欲顯示的個人資料類型:  身分證字號  電話號碼  手機號碼  信用卡號  地址  電子郵件  生日  其他

| 編號 | 類型   | 資料內容          | 網址                                     |
|----|------|---------------|--|
| 1  | 電話號碼 | (02)2324-XXXX | http://203.74.210.82/tobyreidemo/1.htm |
| 2  | 地址   | 台北市信義區XXXXX   | http://203.74.210.82/tobyreidemo/1.htm |

資料皆移除成功後，按下資料確認完成，報表即會以新資料重新產製。

資料確認完成? (需重新生成報表資料)

| 起始網址     | 檢測開始時間              | 檢測結束時間              | IP位址     | 花費時間 | 網站大小   | 網頁數量 |
|----------|---------------------|---------------------|----------|------|--------|------|
| ████████ | 2014-09-01 01:25:43 | 2014-09-01 01:26:43 | ████████ | 1分   | 142.3K | 2    |

## 6. 網站掛馬檢測

### 1. 服務簡介

網站掛馬為駭客一種流行的攻擊方式，當使用者瀏覽您的網站時，遭受惡意程式攻擊，植入使用者的電腦中，駭客可利用使用者的系統資源當作跳板產生更多的資安攻擊或是盜取使用者機敏資訊。

網頁掛馬檢測服務每日針對網站進行模擬測試，並於發現網站遭受掛馬時立刻告警，讓管理人員立即採取補救或防範措施，復原網站運作，避免造成使用者瀏覽您的網站時遭受入侵或是資料被竊取等資安風險。

### 2. 服務功能操作說明

#### a. 檢測設定

本功能提供您新增修改查詢受檢測的目標網址以及一些設定。

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

本系統預設幫用戶找出十個隨機的網址來做檢測。如果您覺得想要新增受測網址或是想更改網址的一些設定，皆可以利用此功能來達成。具體步驟如下：

### (1) 新增一筆資料

#### 1st. 選擇新增一筆資料

本功能提供您查詢、新增、修改檢測設定

請選擇動作  新增一筆資料  
 修改一筆資料  
 查詢

起始網址

網址

啟用

#### 2nd. 選擇起始網址並填寫相關設定(各項設定說明請見下方備註一)

本功能提供您查詢、新增、修改檢測設定

請選擇動作  新增一筆資料  
 修改一筆資料  
 查詢

起始網址

網址

啟用

#### 3rd. 按執行，即可完成

本功能提供您查詢、新增、修改檢測設定

請選擇動作  新增一筆資料  
 修改一筆資料  
 查詢

起始網址

網址

啟用

### (2) 修改一筆資料

#### 1st. 選擇修改一筆資料(這時會跳出提示訊息，按下確定即可)

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

本功能提供您查詢、新增、修改檢測設定

請選擇動作  新增一筆資料  
 修改一筆資料  
 查詢

起始網址

網址

啟用

2nd. 在下方資料中選擇您要修改的那筆資料並點選

網頁掛馬檢測狀態

| 起始網址                       | 網址  | 啟用   | 每日檢測時間   | 上次定期檢測開始時間          | 上次定期檢測結束時間          | 下次定期檢測開始時間          |
|----------------------------|---|------|----------|---------------------|---------------------|---------------------|
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/                             | true | 02:00:00 | 2014-08-05 02:05:01 | 2014-08-05 02:15:02 | 2014-08-06 02:00:00 |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/showimage.php                | true | 02:00:00 | 2014-08-05 02:05:01 | 2014-08-05 02:15:02 | 2014-08-06 02:00:00 |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/comment.php                  | true | 02:00:00 | 2014-08-05 02:05:01 | 2014-08-05 02:15:02 | 2014-08-06 02:00:00 |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bss/adminPanel/index.php     | true | 02:00:00 | 2014-08-05 02:05:01 | 2014-08-05 02:15:02 | 2014-08-06 02:00:00 |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/index.php                    | true | 02:00:00 | 2014-08-05 02:05:01 | 2014-08-05 02:15:02 | 2014-08-06 02:00:00 |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/guestbook.php                | true | 02:00:00 | 2014-08-05 02:05:01 | 2014-08-05 02:15:02 | 2014-08-06 02:00:00 |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/secured/office.htm           | true | 02:00:00 | 2014-08-05 02:05:01 | 2014-08-05 02:15:02 | 2014-08-06 02:00:00 |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/Mod_Revrite_Shop/details.php | true | 02:00:00 | 2014-08-05 02:05:01 | 2014-08-05 02:15:02 | 2014-08-06 02:00:00 |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/userinfo.php                 | true | 02:00:00 | 2014-08-05 02:05:01 | 2014-08-05 02:15:02 | 2014-08-06 02:00:00 |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/AJAX/artists.php             | true | 02:00:00 | 2014-08-05 02:05:01 | 2014-08-05 02:15:02 | 2014-08-06 02:00:00 |

Page 1 of 10 View 1 - 13 of 13

3rd. 此時上方輸入框會出現這筆資料的相關訊息

本功能提供您查詢、新增、修改檢測設定

請選擇動作  新增一筆資料  
 修改一筆資料  
 查詢

起始網址

網址

啟用

4th. 輸入要修改的值(在此範例我們把啟用改成 false)

本功能提供您查詢、新增、修改檢測設定

請選擇動作  新增一筆資料  
 修改一筆資料  
 查詢

起始網址

網址

啟用

5th. 按執行，即可完成

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

### (3) 查詢

1st. 選擇查詢，輸入搜尋條件後按送出，即可看到相關的資料

### (4) 備註一

起始網址代表用戶網站的起始網址，網址代表想要新增的目標網址，啟用代表這個網址目前是否要被檢測。

### (5) 備註二

如果跳出”新增成功或修改成功”，表示新增資料或修改資料成功；如果跳出一些錯誤訊息，請按照錯誤訊息來修改輸入的資料。

### (6) 備註三

按取消鈕可以把正在輸入的值清掉，此時就可以再重新輸入一遍。

### b. 檢測報表查詢

掛馬檢測報表查詢功能可提供使用者查詢三個月內的網站存活檢測異常事件以及檢測結果分佈，使用者一進入可看到事件篩選區、事件檢視區、事件檢測結果分佈圓餅圖及三個月內網站可用度資訊，一開始進入時會顯示使用者所有監控的網址。

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

The screenshot shows a web-based interface for monitoring website security. At the top, there is a search area with fields for '請選擇日期' (Select Date), '結束日期' (End Date), and '請選擇起始網址' (Select Start URL). A '確定查詢' (Confirm Search) button is located below these fields. Below the search area is a table titled '檢測事件查詢' (Detection Event Query) with columns for '起始網址' (Start URL), '網址' (URL), and '時間' (Time). The table contains 18 rows of data, all showing the same start and end URLs and various timestamps. To the right of the table is a '事件檢視區' (Event View Area). Below the table is a '產製報表' (Generate Report) button and a page indicator 'Page 1 of 2'.

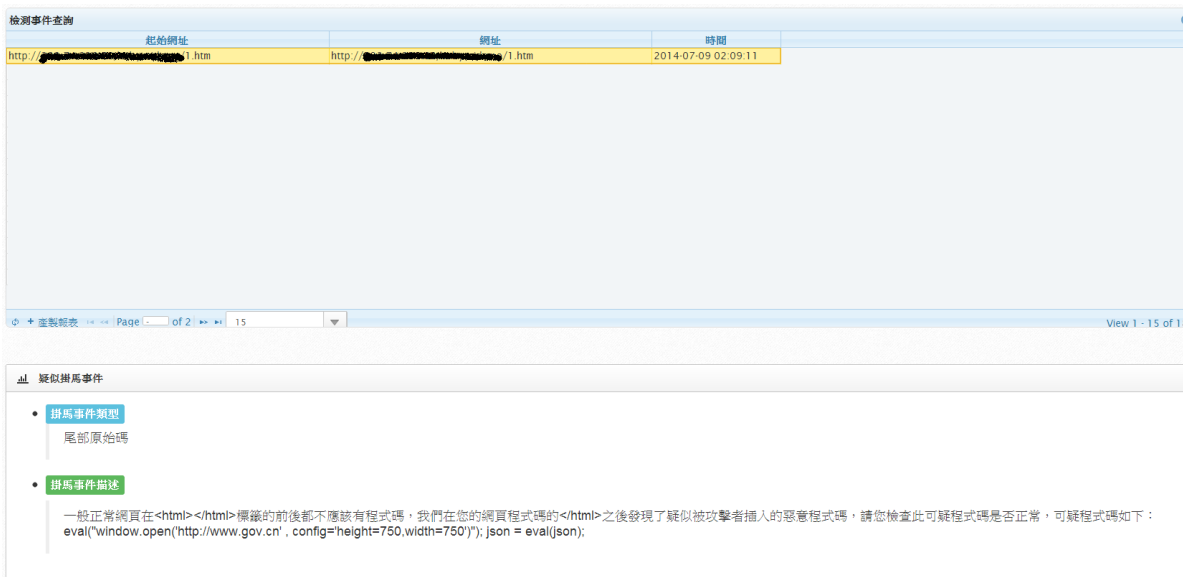
在事件篩選區，使用者可以篩選事件開始時間、結束時間以及起始網址。按下確定查詢後，篩選結果會立即顯示在事件檢視區。

The screenshot shows the '檢測結果分佈' (Detection Results Distribution) section. It features a pie chart with two segments: a large yellow segment representing '正常' (Normal) at 95.36% and a small green segment representing '疑似掛馬' (Suspected Malware) at 4.64%. To the right of the chart is a legend with a green square for '疑似掛馬' and a yellow square for '正常'. Below the chart is a '事件檢測結果圖表' (Event Detection Results Chart) label. The interface also includes a '確定查詢' (Confirm Search) button and a table with columns for '起始網址' (Start URL), '網址' (URL), and '時間' (Time).

檢測事件檢視區可以查到每一筆疑似遭受掛碼事件的起始網址、檢測網址、檢測的時間，表格左下角處可以重新整理、依照目前篩選結果產生報表以及變更顯示筆數、翻頁。

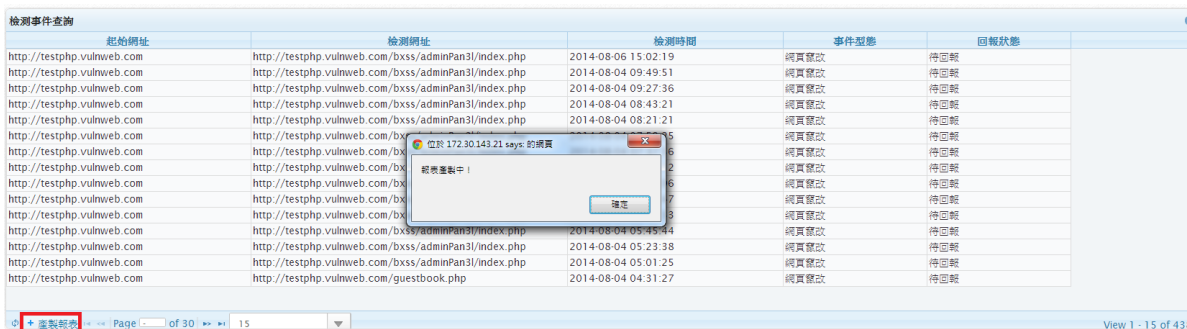
點選表格中其中一筆事件可在下方檢視更加詳細的資訊，如 Figure 4-12 可看到掛碼事件類型以及詳細描述。

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |



### c. 檢測報表下載

掛碼報表下載功能可提供使用者下載在報表檢視頁面所產製的報表，如 Figure 4-13，按下產製報表後，您可至信箱或檢測報表下載頁面得到產製之報表。



|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

| 編號 | 報表名稱                               | 產製時間                | 狀態 | 下載   |
|----|------------------------------------|---------------------|----|------|
| 1  | WAD_9999_R_2014_06_23_17_27_04.pdf | 2014/06/23 17:27:04 | 完成 | 報表下載 |

#### d. 檢測豁免名單設定

本功能提供您自訂專屬於自己網頁的掛馬檢測豁免名單。本系統只要檢測到疑似被掛馬的網頁都會發送告警信件通知用戶。如果您覺得這些檢測結果是可以豁免的，都可以在這裡設定。設定了之後就不會收到這種掛馬類型的告警信件。步驟為：

##### (1) 新增一筆資料

- 1st. 選擇新增一筆資料以及起始網址(此時會顯示這個起始網址目前已經存在的豁免名單)，填寫相關設定(各項設定說明請見下方備註一)後按執行即可

本功能提供您查詢、新增、刪除檢測豁免名單

請選擇動作:  新增一筆資料  刪除一筆資料

起始網址: http://testphp.vulnweb...

豁免關鍵字: eval(json)

執行 取消

##### (2) 刪除一筆資料

- 1st. 選擇刪除一筆資料以及起始網址(此時會顯示這個起始網址目前已經存在的豁免名單)，這時會跳出提示訊息，按下確定即可

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

本功能提供您查詢、新增、刪除檢測豁免名單

請選擇動作  新增一筆資料  刪除一筆資料

起始網址

豁免關鍵字

2nd. 在下方資料中選擇您要刪除的資料並點選，按執行後即可完成。

本功能提供您查詢、新增、刪除檢測豁免名單

請選擇動作  新增一筆資料  刪除一筆資料

起始網址

豁免關鍵字

| 起始網址                       | 豁免名單       |
|----------------------------|------------|
| http://testphp.vulnweb.com | eval(json) |

Page 1 of 10 View 1 - 1 of 10

### (3) 備註一

起始網址代表用戶網站的起始網址，豁免關鍵字代表想要豁免的關鍵字。

### (4) 備註二

如果跳出”新增成功或刪除成功”，表示新增豁免關鍵字或刪除豁免關鍵字成功；如果跳出一些錯誤訊息，請按照錯誤訊息來修改輸入的資料。

### (5) 備註三

按取消紐可以把正在輸入的值清掉，此時就可以再重新輸入一遍。



|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

## 7. 網站存活檢測

### 1. 服務簡介

網站首要目的便是讓任何瀏覽者隨時皆可存取網站正常內容，若是網站因故斷線造成無法存取，可能造成各種嚴重的後果，損害網站所屬單位之形象或實質收益。

網頁存活檢測服務針對網站進行即時監控，並於發現網站連線逾時或運作異常時立刻告警，讓管理人員立即採取補救或防範措施，復原網站運作，避免造成更多損失。

### 2. 服務功能操作說明

#### a. 檢測設定

本功能提供您新增修改查詢受檢測的目標網址以及一些設定。

本系統預設幫用戶找出十個隨機的網址來做檢測。如果您覺得想要新增受測網址或是想更改網址的一些設定，皆可以利用此功能來達成。具體步驟如下：

#### (1) 新增一筆資料

##### 1st. 選擇新增一筆資料

本功能提供您查詢,新增,修改檢測設定

請選擇動作

新增一筆資料

修改一筆資料

查詢

起始網址

網址

連線時間門檻

費用

檢查間隔

##### 2nd. 選擇起始網址並填寫相關設定(各項設定說明請見下方備註一)

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

本功能提供您查詢、新增、修改檢測設定

請選擇動作  新增一筆資料  
 修改一筆資料  
 查詢

起始網址 http://testphp.vulnweb...  
 網址 http://testphp.vulnweb.com/test.php  
 連線時間門檻 5  
 啟用 true  
 檢查間隔 20分鐘 1次

執行 取消

3rd. 按執行，即可完成

本功能提供您查詢、新增、修改檢測設定

請選擇動作  新增一筆資料  
 修改一筆資料  
 查詢

起始網址 http://testphp.vulnweb...  
 網址 http://testphp.vulnweb.com/test.php  
 連線時間門檻 5  
 啟用 true  
 檢查間隔 20分鐘 1次

執行 取消

## (2) 修改一筆資料

1st. 選擇修改一筆資料(這時會跳出提示訊息，按下確定即可)

本功能提供您查詢、新增、修改檢測設定

請選擇動作  新增一筆資料  
 修改一筆資料  
 查詢

起始網址 請選擇  
 網址  
 連線時間門檻 請選擇  
 啟用 請選擇  
 檢查間隔 請選擇

執行 取消

2nd. 在下方資料中選擇您要修改的那筆資料並點選

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

網頁存活檢測狀態

| 起始網址                       | 網址  | 連線時間門檻(秒) | 啟用   | 檢查間隔(X代表每X分鐘檢查一次) |
|----------------------------|---|-----------|------|-------------------|
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/                             | 5         | true | 20                |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/showimage.php                | 5         | true | 20                |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/comment.php                  | 5         | true | 20                |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/index.php                    | 5         | true | 20                |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/index.php                    | 5         | true | 20                |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/guestbook.php                | 5         | true | 20                |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/secured/office.htm           | 5         | true | 20                |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/Mod_Rewrite_Shop/details.php | 5         | true | 20                |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/userinfo.php                 | 5         | true | 20                |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/AJAX/artists.php             | 5         | true | 20                |

Page 1 of 10 View 1 - 13 of 13

3rd. 此時上方輸入框會出現這筆資料的相關訊息

本功能提供您查詢、新增、修改檢測設定

請選擇動作

新增一筆資料

修改一筆資料

查詢

起始網址: http://testphp.vulnweb.com

網址: http://testphp.vulnweb.com/index.php

連線時間門檻: 5

啟用: true

檢查間隔: 20分鐘 1次

執行 取消

4th. 輸入要修改的值(在此範例我們把檢測間隔改成 50 分鐘一次)

本功能提供您查詢、新增、修改檢測設定

請選擇動作

新增一筆資料

修改一筆資料

查詢

起始網址: http://testphp.vulnweb.com

網址: http://testphp.vulnweb.com/index.php

連線時間門檻: 5

啟用: true

檢查間隔: 50分鐘 1次

執行 取消

5th. 按執行，即可完成

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

本功能提供您查詢,新增,修改檢測設定

請選擇動作  新增一筆資料  
 修改一筆資料  
 查詢

起始網址

網址

連線時間門檻

啟用

檢查間隔

### (3) 查詢

- 1st. 選擇查詢，輸入搜尋條件後按送出，即可看到相關的資料

本功能提供您查詢,新增,修改檢測設定

請選擇動作  新增一筆資料  
 修改一筆資料  
 查詢

起始網址

網址

連線時間門檻

啟用

檢查間隔

### (4) 備註一

起始網址代表用戶網站的起始網址，網址代表想要新增或修改的目標網址，連線時間門檻代表檢測時間超過這個時間即判斷為網站有連線問題，啟用代表這個網址目前是否要被檢測，檢查間隔代表幾分鐘檢測一次。

### (5) 備註二

如果跳出”新增成功或修改成功”，表示新增資料或修改資料成功；如果跳出一些錯誤訊息，請按照錯誤訊息來修改輸入的資料。

### (6) 備註三

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

按取消鈕可以把正在輸入的值清掉，此時就可以再重新輸入一遍。

### b. 檢測報表查詢

存活檢測報表查詢功能可提供使用者查詢三個月內的網站存活檢測異常事件以及檢測結果分佈，使用者一進入可看到事件篩選區、事件檢視區、事件檢測結果分佈圖餅圖及三個月內網站可用度資訊，一開始進入時會顯示使用者所有監控的網址。

The screenshot displays the 'Event Selection' (事件篩選區) interface. At the top, there are input fields for 'Start Date' (選擇日期) and 'End Date' (結束日期), and dropdown menus for 'Start Site' (選擇起始網址) and 'Detection Site' (選擇檢測網址). A 'Confirm Search' (確定查詢) button is visible. Below this is the 'Event Selection Table' (檢測事件列表), which contains a table with columns for 'Start Site', 'Detection Site', 'Detection Time', 'Status', and 'Response Time (ms)'. The table lists various events, including '404 Page not found' and 'Time out'. To the right of the table is the 'Event View Area' (事件檢視區). Below the table is a 'Detection Results Distribution' (該檢測網址檢測結果分佈) section, which includes a pie chart showing 'Abnormal' (異常) at 1.47% and 'Normal' (正常) at 98.53%. To the right of the pie chart is a 'Availability Table' (可用度報表) showing 'Start Site' (起始網址) and '8-month Availability' (8月可用度) for various sites.

在事件篩選區，使用者可以篩選事件開始時間、結束時間、起始網址、監控網址。按下確定查詢後，篩選結果會立即顯示在事件檢視區。

This screenshot shows the search filter section of the interface. It includes 'Start Date' (選擇日期) set to 2014-08-01 and 'End Date' (結束日期) set to 2014-08-03. The 'Start Site' (選擇起始網址) is set to http://testphp.vulnweb.com and the 'Detection Site' (選擇檢測網址) is set to http://testphp.vulnweb.com/showimage.php. A 'Confirm Search' (確定查詢) button is highlighted with a red box.

檢測事件檢視區可以查到每一筆存活檢測事件的起始網址、檢測網址、檢測的時間、回應的 HTTP 代碼及回應時間，表格左下角處可以重新整理、依照目前篩選結果產生 PDF 報表以及變更顯示筆數、翻頁。

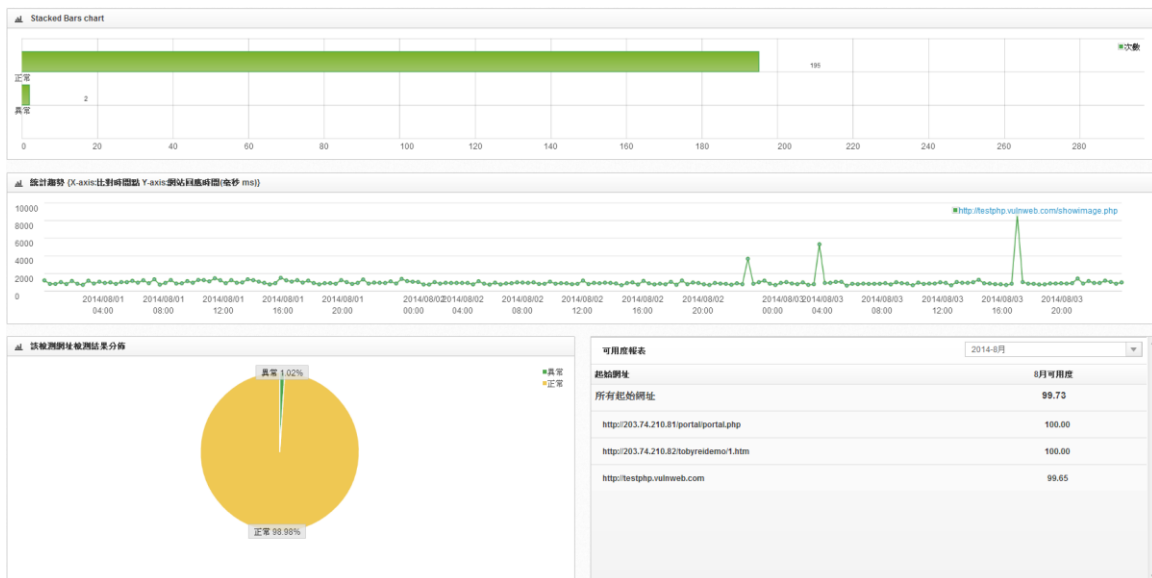
|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

檢測事件列表

| 起始網址                       | 檢測網址                                     | 檢測時間                | 事件類型         | 回應時間(毫秒 ms) |
|----------------------------|--|---------------------|--------------|-------------|
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/showimage.php | 2014-08-03 16:58:52 | 錯誤 Time out! | 8649        |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/showimage.php | 2014-08-03 03:46:45 | 錯誤 Time out! | 5284        |

Page 1 of 1 | 15 | View 1 - 2 of 2

事件檢測結果分佈會依據篩選結果更動，若指定單一檢測網址會進一步顯示詳細的數據。

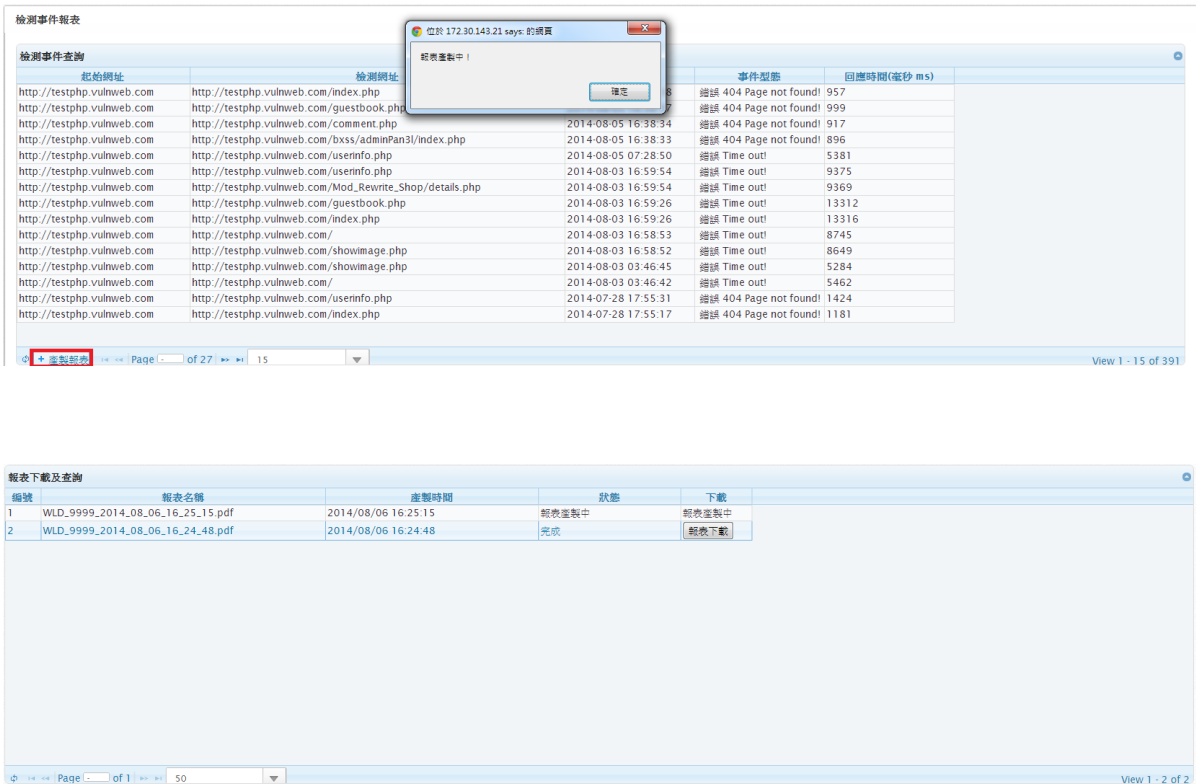


可在事件檢測結果中檢視結果長條圖、網址回應時間(預設為 12 小時內)、結果分佈圓餅圖、以及所有網址可用度。

### c. 檢測報表下載

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

竄改報表下載功能可提供使用者下載在報表檢視頁面所產製的報表，如 Figure 5-14，按下產製報表後，您可至信箱或檢測報表下載頁面取得產製之報表。



## 8. 網站竄改、惡意關鍵字檢測

### 1. 服務簡介

網站首要目的便是讓任何瀏覽者隨時皆可存取網站正常內容，若是網站因故斷線造成無法存取，或者遭到駭客入侵而置換網頁，可能造成各種嚴重的後果，損害網站所屬單位之形象或實質收益。

網頁竄改及關鍵字檢測服務針對網站進行即時監控，並於發現網站遭受竄改時立刻告警，讓管理人員立即採取補救或防範措施，復原網站運作，避免造成更多損失。

駭客入侵網站時，通常會將網站首頁全部或部份置換成該名駭客或駭客組織的專屬畫面，或於網頁內容某處留下特定標語或化名，如「Hacked by X」或「Owned by X」，以之彰顯功力、提昇知名度或宣揚理念，如 Figure 6-1。

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |



本服務模擬一般使用者瀏覽受測目標網站，藉由多次瀏覽獲得的網頁畫面，分析其變動趨勢，自動推論出合理的變化程度，並由網頁原始碼中尋找是否含有惡意關鍵字（如：駭客化名）。

## 2. 服務功能操作說明

### a. 檢測設定

本功能提供您新增修改查詢受檢測的目標網址以及一些設定。

本系統預設幫用戶找出十個隨機的網址來做檢測。如果您覺得想要新增受測網址或是想更改網址的一些設定，皆可以利用此功能來達成。具體步驟如下：

#### (1) 新增一筆資料

##### 1st. 選擇新增一筆資料

本功能提供您查詢、新增、修改檢測設定

請選擇動作  新增一筆資料  修改一筆資料  查詢

起始網址

網址

網址

類似度門檻

採用

檢查間隔



|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

**2nd. 選擇起始網址並填寫相關設定(各項設定說明請見下方備註一)**

本功能提供您查詢,新增,修改檢測設定

請選擇動作

新增一筆資料  
 修改一筆資料  
 查詢

起始網址

網址

啟用

檢查間隔

**3rd. 按執行，即可完成**

本功能提供您查詢,新增,修改檢測設定

請選擇動作

新增一筆資料  
 修改一筆資料  
 查詢

起始網址

網址

啟用

檢查間隔

**(2) 修改一筆資料**

**1st. 選擇修改一筆資料(這時會跳出提示訊息，按下確定即可)**

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

本功能提供您查詢、新增、修改檢測設定

請選擇動作

新增一筆資料

修改一筆資料

查詢

起始網址

網址

網址

相似度門檻

啟用

檢查間隔

2nd. 在下方資料中選擇您要修改的那筆資料並點選

網頁窺改檢測狀態

| 起始網址                | 網址  | 相似度門檻(%) | 啟用    | 檢查間隔(X代表每X分鐘檢查一次) |
|---------------------|---|----------|-------|-------------------|
| testphp.vulnweb.com | http://testphp.vulnweb.com/mod_rewrite_sho    | 100      | raise | 60                |
| testphp.vulnweb.com | http://testphp.vulnweb.com/clientaccesspolicy | 100      | false | 60                |
| testphp.vulnweb.com | http://testphp.vulnweb.com/pictures/6.jpg.tn  | 100      | false | 60                |
| testphp.vulnweb.com | http://testphp.vulnweb.com/Mod_Rewrite_Shoj   | 100      | false | 60                |
| testphp.vulnweb.com | http://testphp.vulnweb.com/pictures/path-disc | 100      | true  | 60                |
| testphp.vulnweb.com | http://testphp.vulnweb.com/AJAX/htaccess.cor  | 100      | true  | 60                |
| testphp.vulnweb.com | http://testphp.vulnweb.com/CVS/Entries        | 100      | true  | 60                |
| testphp.vulnweb.com | http://testphp.vulnweb.com/login.php          | 100      | true  | 60                |
| testphp.vulnweb.com | http://testphp.vulnweb.com/artists.php        | 100      | true  | 60                |
| testphp.vulnweb.com | http://testphp.vulnweb.com/Mod_Rewrite_Shoj   | 100      | false | 60                |
| testphp.vulnweb.com | http://testphp.vulnweb.com/product.php        | 100      | true  | 60                |
| testphp.vulnweb.com | http://testphp.vulnweb.com/vvstests/pmwiki    | 100      | true  | 60                |
| testphp.vulnweb.com | http://testphp.vulnweb.com/guestbook.php      | 100      | true  | 60                |
| testphp.vulnweb.com | http://testphp.vulnweb.com/AJAX/infotitle.php | 100      | true  | 60                |

Page 1 of 10 View 1 - 20 of 20

3rd. 此時上方輸入框會出現這筆資料的相關訊息

本功能提供您查詢、新增、修改檢測設定

請選擇動作

新增一筆資料

修改一筆資料

查詢

起始網址

網址

啟用

檢查間隔

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

**4th. 輸入要修改的值(在此範例我們把檢測間隔改成 90 分鐘一次)**

本功能提供您查詢,新增,修改檢測設定

請選擇動作  
 新增一筆資料  
 修改一筆資料  
 查詢

起始網址: testphp.vulnweb.com

網址: testphp.vulnweb.com

啟用: true

**檢查間隔: 90分鐘1次**

執行 取消

**5th. 按執行，即可完成**

本功能提供您查詢,新增,修改檢測設定

請選擇動作  
 新增一筆資料  
 修改一筆資料  
 查詢

起始網址: http://testphp.vulnweb...

網址: http://testphp.vulnweb.com/bass/index.php

啟用: true

檢查間隔: 50分鐘1次

**執行** 取消

**(3) 查詢**

**1st. 選擇查詢，輸入搜尋條件後按送出，即可看到相關的資料**

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

#### (4) 備註一

起始網址代表用戶網站的起始網址，網址代表想要新增或修改的目標網址，啟用代表這個網址目前是否要被檢測，檢查間隔代表幾分鐘檢測一次。

#### (5) 備註二

如果跳出”新增成功或修改成功”，表示新增資料或修改資料成功；如果跳出一些錯誤訊息，請按照錯誤訊息來修改輸入的資料。

#### (6) 備註三

按取消紐可以把正在輸入的值清掉，此時就可以再重新輸入一遍。

### b. 檢測報表查詢

#### (1) 功能區塊說明

竊改報表查詢功能可提供使用者查詢三個月內的網站竊改檢測異常事件以及檢測結果分佈，點選表格內事件可進一步瞭解事件之詳細資訊。使用者一進入可看到事件篩選區、事件檢視區、事件檢測結果分佈圓餅圖如 Figure 4-10，一開始進入時會顯示使用者所有監控的網址。

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

竊改報表查詢

※本功能提供查詢三個月內的網站竊改報表異常事件以及被測結果分析  
 ※點選表格內事件可進一步瞭解事件之詳細資訊

事件篩選區

請選擇日期: [日期選擇器] 結束日期: [日期選擇器]  
 請選擇起始網址: [所有起始網址] 請選擇檢測網址: [所有檢測網址]  
 事件型態: [列出全部] 回報狀態: [列出全部]  
 [確定查詢]

事件檢視區

| 起始網址                               | 檢測網址                                     | 檢測時間                | 事件型態    | 處理狀態 |
|------------------------------------|--|---------------------|---------|------|
| http://soc365.hinet.net            | http://soc365.hinet.net/soc365_login.php | 2014-07-10 03:44:02 | 網頁竊改    | 待回報  |
| http://203.74.210.82/hobyreidemo/1 | http://203.74.210.82/hobyreidemo/1.htm   | 2014-07-09 10:43:24 | 惡意關鍵字植入 | 待回報  |
| http://203.74.210.82/hobyreidemo/1 | http://203.74.210.82/hobyreidemo/1.htm   | 2014-07-09 10:43:20 | 網頁竊改    | 待回報  |
| http://203.74.210.82/hobyreidemo/1 | http://203.74.210.82/hobyreidemo/1.htm   | 2014-07-09 10:33:49 | 惡意關鍵字植入 | 待回報  |
| http://203.74.210.82/hobyreidemo/1 | http://203.74.210.82/hobyreidemo/1.htm   | 2014-07-09 10:33:42 | 網頁竊改    | 待回報  |
| http://203.74.210.82/hobyreidemo/1 | http://203.74.210.82/hobyreidemo/1.htm   | 2014-07-09 09:49:56 | 惡意關鍵字植入 | 待回報  |
| http://203.74.210.82/hobyreidemo/1 | http://203.74.210.82/hobyreidemo/1.htm   | 2014-07-09 09:49:48 | 網頁竊改    | 待回報  |
| http://203.74.210.82/hobyreidemo/1 | http://203.74.210.82/hobyreidemo/1.htm   | 2014-07-09 09:48:58 | 惡意關鍵字植入 | 待回報  |
| http://203.74.210.82/hobyreidemo/1 | http://203.74.210.82/hobyreidemo/1.htm   | 2014-07-09 09:48:54 | 網頁竊改    | 待回報  |
| http://203.74.210.82/hobyreidemo/1 | http://203.74.210.82/hobyreidemo/1.htm   | 2014-07-09 09:23:06 | 惡意關鍵字植入 | 待回報  |
| http://203.74.210.82/hobyreidemo/1 | http://203.74.210.82/hobyreidemo/1.htm   | 2014-07-09 09:22:58 | 網頁竊改    | 待回報  |
| http://soc365.hinet.net            | http://soc365.hinet.net/soc365_login.php | 2014-07-09 09:12:26 | 惡意關鍵字植入 | 待回報  |
| http://soc365.hinet.net            | http://soc365.hinet.net/portal.php       | 2014-07-09 09:12:24 | 惡意關鍵字植入 | 待回報  |

事件檢測結果分佈圖

在事件篩選區，使用者可以篩選事件開始時間、結束時間、起始網址、監控網址、事件型態以及目前回報狀態。

請選擇日期: 2014-08-01 結束日期: 2014-08-06  
 請選擇起始網址: http://testphp.vulnweb.com 請選擇檢測網址: http://testphp.vulnweb.com/bss/admin/Pan3M...  
 事件型態: 網頁竊改 回報狀態: 待回報  
 [確定查詢]

按下**確定查詢**後，篩選結果會立即顯示在事件檢視區，檢測事件檢視區可以查到每一筆疑似遭受竊改事件的起始網址、檢測網址、檢測的時間、遭駭的事件類型以及回報的狀態，表格左下角處可以重新整理、依照目前篩選結果產生 PDF 報表以及變更顯示筆數、翻頁。

[重新整理] Page 1 of 4 of 15 View 1 - 15 of 57

點選表格中其中一筆事件可在下方檢視更加詳細的資訊，如竊改事件則可以看到原先頁面以及遭受竊改頁面的比較，關鍵字植入則會列出該網址中所被偵測到的惡意關鍵字如 Figure 6-13、Figure 6-14。

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

| 檢測事件查詢 | 起始網址                    | 檢測網址                    | 檢測時間                | 事件型態 | 回報狀態 |
|--------|-------------------------|-------------------------|---------------------|------|------|
|        | http://[redacted]/1.htm | http://[redacted]/1.htm | 2014-07-31 09:03:28 | 網頁篡改 | 待回報  |



| 檢測事件查詢 | 起始網址                    | 檢測網址                    | 檢測時間                | 事件型態    | 回報狀態 |
|--------|-------------------------|-------------------------|---------------------|---------|------|
|        | http://[redacted]/1.htm | http://[redacted]/1.htm | 2014-07-31 09:03:30 | 惡意關鍵字植入 | 待回報  |

```

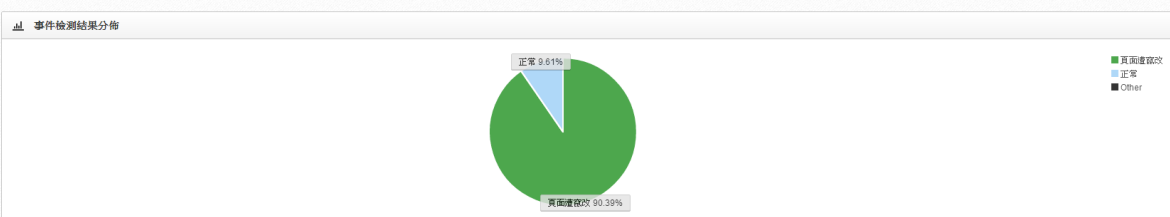
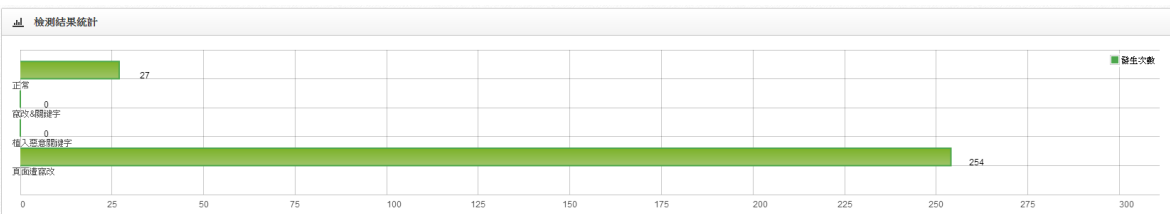
Textareas
<HTML xmlns="http://www.w3.org/1999/xhtml"><HEAD><TITLE>台北熱</TITLE> <META content="text/html; charset=utf-8" http-equiv=Content-Type><!--手機用宣告START!--></HEAD> <BODY><BR><FONT color=red size=10 align="center">残念</FONT><BR><FONT color=red size=10 align="center">馬英九</FONT> <BR><FONT color=red size=10 align="center">hacked by xxx</FONT> <IMG id=tobyimg style="HEIGHT: 150%; WIDTH: 150%" alt=some_text src="/images/chen.jpg">地址 台北市信義區[redacted] <SCRIPT language=JavaScript>
e=all"window.open("http://www.gov.taipei", "config","height=150,width=150"); //函數：在 IE 中建立 XMLHttpRequest 物件，避免不同瀏覽器的差異性
if (typeof XMLHttpRequest != "undefined" && window.ActiveXObject) { function XMLHttpRequest() { var arSignatures = ["Microsoft.XMLHTTP 6.0", "MSXML2.XMLHTTP 5.0", "MSXML2.XMLHTTP 4.0", "MSXML2.XMLHTTP 3.0", "MSXML2.XMLHTTP"];
for (var i=0; i < arSignatures.length; i++) { try { var oRequest = new ActiveXObject(arSignatures[i]); return oRequest; } catch (oError) { //ignore } } throw new Error("MSXML is not installed on your system."); } } //函數：將參數加入到 URL 尾端，以確保 GET 使用 function
addURLParam(sURL, sParamName, sParamValue) { sURL += (sURL.indexOf("?") == -1 ? "?" : "&"); sURL += encodeURIComponent(sParamName) + "=" + encodeURIComponent(sParamValue); return sURL; } //分別取得每個元素的reference
var oCateList = document.getElementById(cid); var oGameList = document.getElementById(gid); //後端返回 JSON 資料的路徑 var sURLInt = "toolbox_json.php"; //用來儲存 JSON 的全域變數 var json; //一開始時先將第二個清單停用 oGameList.disabled = true; //第一個清單的 onchange 事
    
```

| # | 網頁上檢測到惡意關鍵字清單 |
|---|---------------|
| 1 | hacked        |
| 2 | 残念            |

事件檢測結果分佈會依據篩選結果動態變動，若指定單一檢測網址會進一步顯示詳細的數據。

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

請選擇日期:  結束日期:   
 請選擇起始網址:  請選擇檢測網址:   
 事件型態:  回報狀態:



### c. 檢測報表下載

竄改報表下載功能可提供使用者下載在報表檢視頁面所產製的報表，如 Figure 4-16，按下產製報表後，您可至信箱或檢測報表下載頁面得到產製之報表。

檢測事件查詢

| 起始網址                       | 檢測網址   | 檢測時間                | 事件型態 | 回報狀態 |
|----------------------------|--|---------------------|------|------|
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bxss/adminPan3l/index.php | 2014-08-06 15:02:19 | 網頁竄改 | 待回報  |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bxss/adminPan3l/index.php | 2014-08-04 09:49:51 | 網頁竄改 | 待回報  |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bxss/adminPan3l/index.php | 2014-08-04 09:27:36 | 網頁竄改 | 待回報  |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bxss/adminPan3l/index.php | 2014-08-04 08:43:21 | 網頁竄改 | 待回報  |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bxss/adminPan3l/index.php | 2014-08-04 08:21:21 | 網頁竄改 | 待回報  |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bx                        |                     | 網頁竄改 | 待回報  |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bx                        |                     | 網頁竄改 | 待回報  |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bx                        |                     | 網頁竄改 | 待回報  |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bx                        |                     | 網頁竄改 | 待回報  |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bx                        |                     | 網頁竄改 | 待回報  |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bx                        |                     | 網頁竄改 | 待回報  |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bxss/adminPan3l/index.php | 2014-08-04 05:45:44 | 網頁竄改 | 待回報  |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bxss/adminPan3l/index.php | 2014-08-04 05:23:38 | 網頁竄改 | 待回報  |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bxss/adminPan3l/index.php | 2014-08-04 05:01:25 | 網頁竄改 | 待回報  |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/guestbook.php             | 2014-08-04 04:31:27 | 網頁竄改 | 待回報  |

Page 15 of 30 View: 1 - 15 of 438

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

| 編號 | 檔案名稱                             | 產製時間                | 狀態 | 下載                                  |
|----|----------------------------------|---------------------|----|-------------------------------------|
| 1  | WTD_9999_2014_08_06_15_10_50.pdf | 2014/08/06 15:10:50 | 完成 | <input type="button" value="檔案下載"/> |
| 2  | WTD_9999_2014_07_31_18_46_04.pdf | 2014/07/31 18:46:04 | 完成 | <input type="button" value="檔案下載"/> |
| 3  | WTD_9999_2014_07_31_18_42_00.pdf | 2014/07/31 18:42:00 | 完成 | <input type="button" value="檔案下載"/> |

#### d. 自訂惡意關鍵字

本功能提供您自訂專屬於自己網頁的惡意關鍵字以及豁免關鍵字。本系統每天都會收集世界各地最新的駭客關鍵字當作比對惡意關鍵字的資料庫。如果您覺得這些惡意關鍵字不足以用於檢測，或是有關鍵字想要豁免的，都可以在這裡設定。

首先，先選擇起始網址(如下圖)，選完後會顯示這個起始網址的關鍵字。右方則是本日最新的惡意關鍵字資料庫。之後的步驟為：

本功能提供您查詢,新增,刪除關鍵字黑白名單(網址)

起始網址:

請選擇動作:  新增關鍵字  刪除關鍵字

關鍵字:

關鍵字種類:

| 起始網址                       | 關鍵字類型 | 關鍵字                |
|----------------------------|-------|--------------------|
| http://testphp.vulnweb.com | 黑名单   | hacked by cht kobe |

今日參考之惡意關鍵字名單

- Ashiyane Digital Security Team
- r4diationz
- Ashiyane Digital Security Team
- TEAM C.F.P.M
- ZCompany Hacking Crew
- !Bb0yH4ck3r\_Dz-1
- ITeAm RaBaT-SaLe!
- Inc0gn370
- Inf3r1 4L
- # SID Nomore
- #AntiSEc
- \*\*RoAd\_KiLEr\*\*
- \*AhmeD\*

#### (1) 新增關鍵字

1st. 選擇起始網址以及新增關鍵字，並填妥相關資料(各項



|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

設定說明請參照下方備註)，按執行後即可完成。

## (2) 刪除關鍵字

1st. 選擇起始網址以及刪除關鍵字，(這時會跳出提示訊息，按下確定即可)

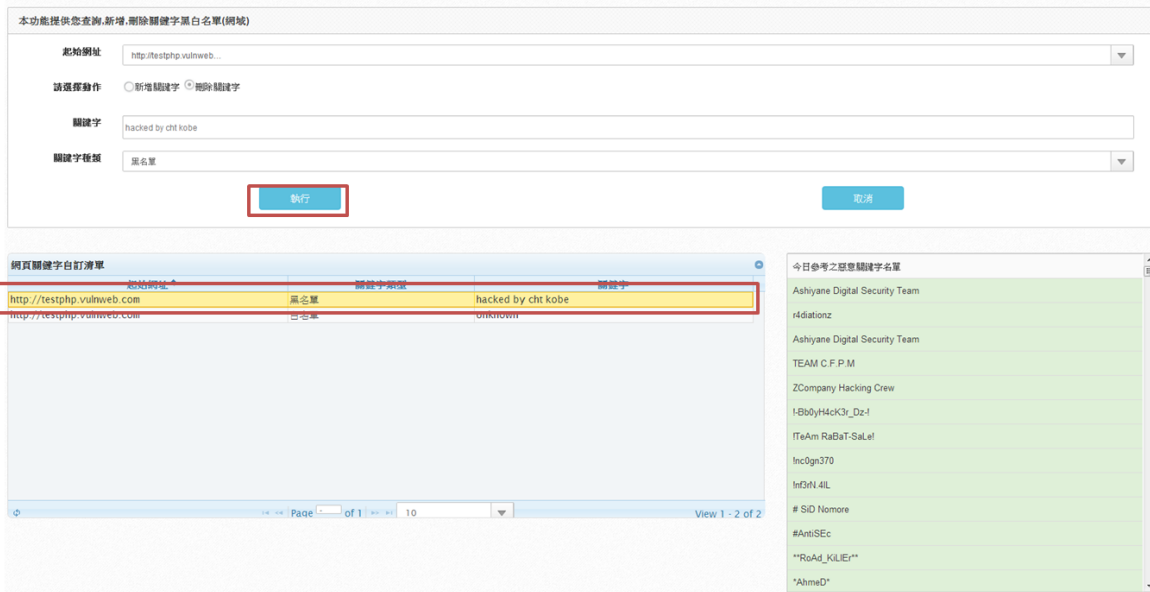
| 起始網址                       | 關鍵字類型 | 關鍵字                |
|----------------------------|-------|--------------------|
| http://testphp.vulnweb.com | 高名單   | hacked by cht kobe |
| http://testphp.vulnweb.com | 白名單   | Unknown            |

| 今日參考之惡意關鍵字名單                   |
|--------------------------------|
| Ashiyane Digital Security Team |
| r4diationz                     |
| Ashiyane Digital Security Team |
| TEAM C.F.P.M                   |
| ZCompany Hacking Crew          |
| I-Bb0yH4cK3r_Dz-I              |
| ITeAm RaBaT-SaLeI              |
| Inc0gn370                      |
| Inf3rn 4IL                     |
| # SID Nomore                   |
| #AntiSEc                       |
| **RoAd_KiLEr**                 |
| *AhmeD*                        |

2nd. 在下方資料中選擇您要刪除的關鍵字並點選，按執行後即可完成。

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |



### (3) 備註一

起始網址代表用戶網站的起始網址，關鍵字代表想要新增或刪除的關鍵字，關鍵字種類代表這個關鍵字屬於惡意或是豁免的關鍵字。

### (4) 備註二

如果跳出”新增成功或刪除成功”，表示新增關鍵字或刪除關鍵字成功；如果跳出一些錯誤訊息，請按照錯誤訊息來修改輸入的資料。

### (5) 備註三

按取消紐可以把正在輸入的值清掉，此時就可以再重新輸入一遍。

## e. 竄改事件處理回饋

因為竄改和惡意關鍵字檢測有一定的機率會造成誤判的狀況 (EX：網頁改版)，所以需要提供回饋機制讓使用者可以回報。本功能提供使用者回報竄改和惡意關鍵字事件的狀態。

### (1) 網頁竄改回饋

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

**1st. 選擇一個事件並點選(上方可以用日期篩選)**

篩選條件

事件起始時間: 2014-07-25  
事件結束時間: 2014-07-31

| 起始網址                       | 網址   | 檢查時間                | 攻擊類型   |
|----------------------------|--|---------------------|--------|
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bxss/adminPan3l/index | 2014-07-31 22:41:16 | 網頁遭受篡改 |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bxss/adminPan3l/index | 2014-07-31 22:57:29 | 網頁遭受篡改 |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bxss/adminPan3l/index | 2014-07-31 22:36:16 | 網頁遭受篡改 |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bxss/adminPan3l/index | 2014-07-31 22:12:49 | 網頁遭受篡改 |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bxss/adminPan3l/index | 2014-07-31 21:49:08 | 網頁遭受篡改 |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bxss/adminPan3l/index | 2014-07-31 21:27:17 | 網頁遭受篡改 |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bxss/adminPan3l/index | 2014-07-31 21:05:38 | 網頁遭受篡改 |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bxss/adminPan3l/index | 2014-07-31 20:43:38 | 網頁遭受篡改 |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bxss/adminPan3l/index | 2014-07-31 20:21:11 | 網頁遭受篡改 |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bxss/adminPan3l/index | 2014-07-31 19:58:07 | 網頁遭受篡改 |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bxss/adminPan3l/index | 2014-07-31 19:35:19 | 網頁遭受篡改 |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bxss/adminPan3l/index | 2014-07-31 19:13:53 | 網頁遭受篡改 |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bxss/adminPan3l/index | 2014-07-31 18:51:44 | 網頁遭受篡改 |
| http://testphp.vulnweb.com | http://testphp.vulnweb.com/bxss/adminPan3l/index | 2014-07-31 18:28:41 | 網頁遭受篡改 |

**2nd. 點選後，下方會出現比對的網頁截圖**

您目前選擇的網站:

<http://testphp.vulnweb.com/bxss/adminPan3l/index.php>

回報事項

請選擇

送出

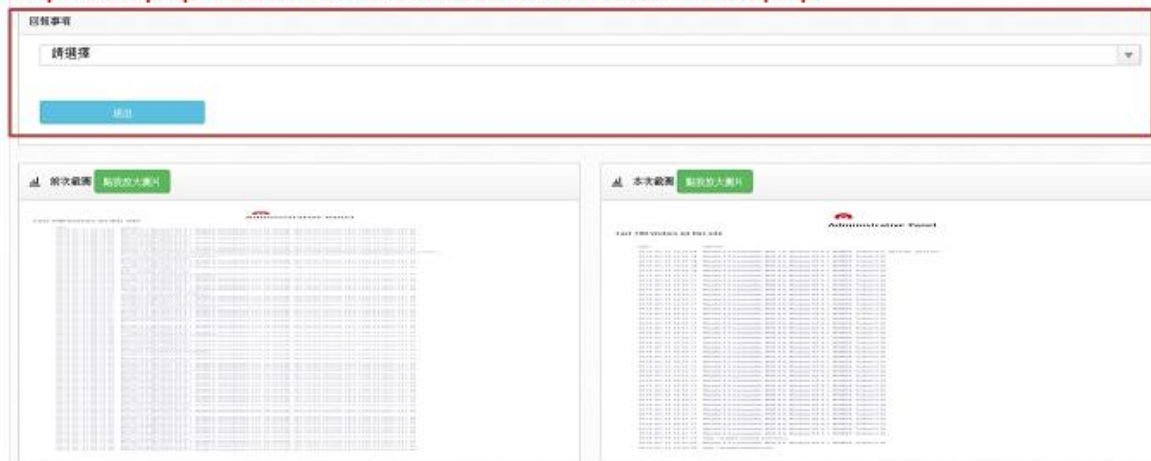
前次截圖 點我放大圖片

本次截圖 點我放大圖片

**3rd. 在回報事項中選擇回饋訊息後按送出即可(請見備註一)**

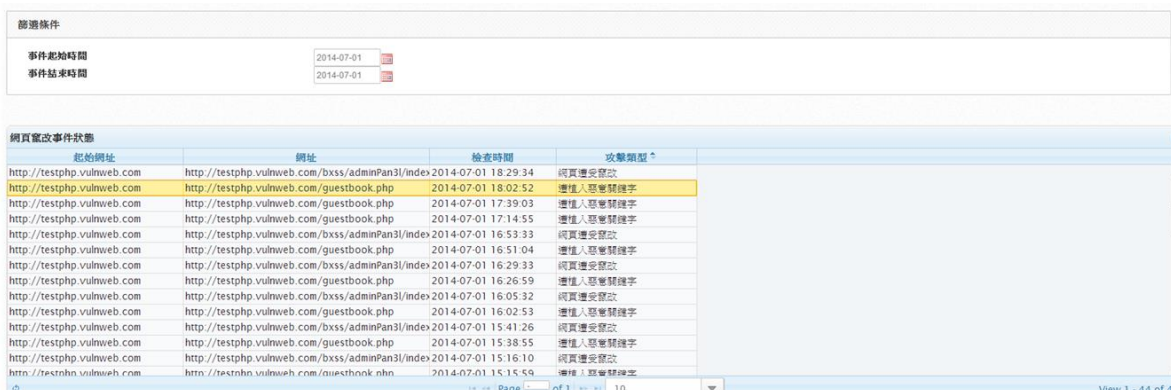
|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

您目前選擇的網站：  
<http://testphp.vulnweb.com/bxss/adminPan3l/index.php>



## (2) 網頁惡意關鍵字回饋

1st. 選擇一個事件並點選(上方可以用日期篩選)



2nd. 點選後，下方會出現網頁 HTML 原始碼以及比對到的惡意關鍵字截圖

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

您目前選擇的網站：  
<http://testphp.vulnweb.com/guestbook.php>

**3rd. 在回報事項中選擇回饋訊息後按送出即可(請見備註二)**

您目前選擇的網站：  
<http://testphp.vulnweb.com/guestbook.php>

**(3) 備註一**

在網頁竄改回報事項中，有四個選項

**1st. 網頁遭受竄改**

網頁真的遭受竄改攻擊，回報後請盡快檢查網站

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

狀況。

**2nd.** 網頁靜態改版

- 網站頁面靜態改版
- 此變動屬於靜態變動(每次進網頁看都一樣)
- 若同時屬於靜態改版或動態變動，以靜態改版優先
- EX:網頁更版

**3rd.** 網頁動態變動

- 網站頁面動態變動
- 此變動屬於動態變動(每次進網頁都有一些不一樣)
- 若同時屬於靜態改版或動態變動，以靜態改版優先
- EX:圖片或 FLASH 動畫

**4th.** 誤判

並非遭受網頁竄改且不是上述理由 2 或 3。

**(4) 備註二**

在網頁惡意關鍵字回饋中，有兩個選項

**1st.** 網頁遭受惡意關鍵字

網頁的確遭受惡意關鍵字。請回報後盡快檢查網頁狀態

**2nd.** 誤判

並非遭受惡意關鍵攻擊。回報後請到自訂惡意關鍵字功能新增豁免名單。

**(5) 備註三**

如果不做相關回報的話，有可能會一直收到檢測告警

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

信件。

## 9. 主機弱點掃描

### 1. 服務簡介

主機弱點掃描主要是協助企業發現主機管理的設定不當或主機的漏洞，並且提供改善建議及統計摘要報表資訊。主機弱點掃描服務是利用高效率主機弱點掃描工具，針對目前已經發現的主機應用程式安全弱點，將所得到的結果進行交叉比對分析，並提供弱點掃描分析報表，可依據建議改善措施，修補弱點，以降低遭受入侵的風險。

### 2. 服務功能操作說明

#### a. 掃描標的設定

掃描目標設定

\*提供主機弱點掃描用戶更新掃描標的  
 \*一般用戶一筆租約可設一組IP，貴安能隊最多三組可設3組IP  
 \*點選表格即可修改用戶IP

檢測目標設定

| # | HN       | 租約ID | 狀態 | 類型         | 掃描標的清單    | 租約開始時間              | 更新次數 | 上次更新時間 |
|---|----------|------|----|------------|-----------|---------------------|------|--------|
| 0 | 20151230 | 86   | 正常 | 一般用戶(每日掃描) | 127.0.0.1 | 2015-12-28 16:02:29 | 0    |        |
| 1 | 20151230 | 87   | 正常 | 一般用戶(每日掃描) | 127.0.0.1 | 2015-12-28 16:08:33 | 0    |        |
| 2 | 20151230 | 88   | 正常 | 一般用戶(每週掃描) | 127.0.0.1 | 2015-12-28 16:08:46 | 0    |        |

掃描目標設定 86 IP:0

提供用戶更改掃描標的，目前為一個月可以任意更改一次。

#### b. 掃描設定

本功能提供用戶進行掃描 pattern 與定期檢測掃描時間設定。掃描模式依用戶需要可選擇預設、高風險、PCI、DoS、其它規範。

掃描設定

\*提供您設定定期檢測檢測模式、檢測啟動時間。  
 \*檢測啟動時間視您選擇週期可設定每週日至周六及每日整點時刻。  
 \*檢測啟動時間為掃描工作派送至工作排程佇列時間，實際啟動時間依掃描資源而定。  
 \*檢測狀態可至掃描工作管理功能查詢。

檢測設定值

掃描目標

掃描週期

弱點分類項目

掃描每日時間設定

|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

用戶進行掃描標的自我檢測功能，每月依照合約內容提供不同的自我檢測次數，如定期檢測可設定不同掃描分類，也可以設定掃描開始日期。

自我檢測

\*週掃描提供每月兩次免費自我檢測掃描，日掃描僅一次，未使用不予保留

檢測設定值

自檢目標: 127.0.0.1

當月自檢次數: 該月自我掃描額度已使用完畢

掃描分類項目: 預設

掃描結果收件人: [Redacted]

掃描開始時間: 2016-01-15 10:04:08

添加掃描

#### d. 定期(自我)掃描進度管理

此功能是讓用戶可因其需要針對排程中或掃描中的工作進行暫停檢測或啟動檢測的管理。

掃描中的工作，用戶可以點選暫停，然後可以重啟或是停止該次掃描。

定期掃描進度管理

\*提供您查詢所有的檢測工作，檢測完成可以點選查詢查看檢測結果報表！

| 掃描標的      | 狀態   | 申請時間                | 開始時間                | 完成時間                | 暫停/重啟檢測工作 |
|-----------|------|---------------------|---------------------|---------------------|-----------|
| 127.0.0.1 | 掃描完成 | 2016-01-06 23:00:02 | 2016-01-06 23:01:07 | 2016-01-06 23:03:09 | -         |
| 127.0.0.1 | 掃描完成 | 2016-01-06 13:00:02 | 2016-01-06 13:01:10 | 2016-01-06 13:03:04 | -         |
| 127.0.0.1 | 掃描完成 | 2016-01-05 23:00:02 | 2016-01-05 23:01:11 | 2016-01-05 23:03:09 | -         |
| 127.0.0.1 | 掃描完成 | 2016-01-05 13:00:01 | 2016-01-05 13:01:06 | 2016-01-05 13:03:09 | -         |
| 127.0.0.1 | 掃描完成 | 2016-01-07 13:00:02 | 2016-01-07 13:01:06 | 2016-01-07 13:03:07 | -         |
| 127.0.0.1 | 掃描完成 | 2016-01-07 23:00:02 | 2016-01-07 23:03:09 | 2016-01-07 23:06:10 | -         |
| 127.0.0.1 | 掃描完成 | 2016-01-08 13:00:02 | 2016-01-08 13:01:07 | 2016-01-08 13:03:07 | -         |
| 127.0.0.1 | 掃描完成 | 2016-01-08 23:00:02 | 2016-01-08 23:03:07 | 2016-01-08 23:06:20 | -         |
| 127.0.0.1 | 掃描完成 | 2016-01-08 23:00:02 | 2016-01-08 23:04:11 | 2016-01-08 23:07:09 | -         |
| 127.0.0.1 | 掃描完成 | 2016-01-09 13:00:02 | 2016-01-09 13:01:07 | 2016-01-09 13:03:11 | -         |
| 127.0.0.1 | 掃描完成 | 2016-01-09 23:00:02 | 2016-01-09 23:03:07 | 2016-01-09 23:07:06 | -         |
| 127.0.0.1 | 掃描完成 | 2016-01-10 13:00:02 | 2016-01-10 13:01:07 | 2016-01-10 13:03:10 | -         |
| 127.0.0.1 | 掃描完成 | 2016-01-10 23:00:02 | 2016-01-10 23:03:14 | 2016-01-10 23:06:14 | -         |
| 127.0.0.1 | 掃描完成 | 2016-01-11 13:00:01 | 2016-01-11 13:01:06 | 2016-01-11 13:03:11 | -         |

Page 1 of 1 30 View 1 - 21 of 21

#### e. 定期(自檢)檢測報表查詢



|    |             |      |      |
|----|-------------|------|------|
| 名稱 | 網站偵防隊服務使用手冊 | 安全等級 | 公開   |
| 編號 |             | 版次   | V1.0 |

主機弱點服務每月或自檢會依用戶設定之檢測時間與 pattern 設定進行派送掃描，用戶可於掃描結束之後點選欲瀏覽的報表，再點選查詢按鈕進行查看掃描結果。

\*提供您查詢定期檢測工作，點選查看報表按鈕可顯示該檢測工作報表資訊。  
\*欲查看多個IP之報表資訊，可透過點選檢測報表列表紀錄，再點選綜合查詢，即可觀看所選擇IP的綜合報表資訊。

檢測工作查詢

| IP        | 派兵時間                | 開始時間                | 完成時間                | 弱點數 | 查看報表 |
|-----------|---------------------|---------------------|---------------------|-----|------|
| 127.0.0.1 | 2016-01-14 23:00:01 | 2016-01-14 23:03:12 | 2016-01-14 23:07:08 | 5   | 查看報表 |
| 127.0.0.1 | 2016-01-14 13:00:02 | 2016-01-14 13:01:06 | 2016-01-14 13:04:01 | 5   | 查看報表 |
| 127.0.0.1 | 2016-01-13 23:00:02 | 2016-01-13 23:03:08 | 2016-01-13 23:08:08 | 5   | 查看報表 |
| 127.0.0.1 | 2016-01-13 13:00:01 | 2016-01-13 13:01:08 | 2016-01-13 13:03:07 | 5   | 查看報表 |
| 127.0.0.1 | 2016-01-12 23:00:02 | 2016-01-12 23:03:08 | 2016-01-12 23:07:06 | 5   | 查看報表 |
| 127.0.0.1 | 2016-01-12 13:00:02 | 2016-01-12 13:01:07 | 2016-01-12 13:03:10 | 5   | 查看報表 |
| 127.0.0.1 | 2016-01-11 23:00:02 | 2016-01-11 23:03:07 | 2016-01-11 23:07:06 | 5   | 查看報表 |
| 127.0.0.1 | 2016-01-11 13:00:01 | 2016-01-11 13:01:09 | 2016-01-11 13:03:11 | 5   | 查看報表 |
| 127.0.0.1 | 2016-01-10 23:00:02 | 2016-01-10 23:03:14 | 2016-01-10 23:06:14 | 5   | 查看報表 |

Page 1 of 1 30 View 1 - 21 of 21

綜合查詢

點進去時可看到如例圖所示報表格式，也可以點選下載成 pdf

主機弱點掃描報表

報表查詢

掃描資訊

| 掃描IP      | 掃描Pattern | 掃描時間                | 完成時間                | 下載PDF |
|-----------|-----------|---------------------|---------------------|-------|
| 127.0.0.1 | default   | 2016-01-14 23:03:12 | 2016-01-14 23:07:08 | 下載    |

弱點等級分布圖

| 弱點等級 | 百分比 |
|------|-----|
| 中風險  | 60% |
| 低風險  | 40% |

弱點列表