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

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。

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。

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）


中華電信 會員中心 MemberCenter
使用您的帳號登入
HiNet企業資安服務
帳號
請輸入手機號碼、email或HN帳號
密碼
請輸入密碼
保持登入狀態
(公用電腦不建議使用)
登入
忘記帳號?
忘記密碼?
沒有帳號嗎? 立刻 加入會員

步驟四：請選擇畫面右方「Email 註冊」或「手機註冊」進行註冊。

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」。

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。

步驟三：請點選左方功能選單中的「下載專區」。

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。

步驟五：請點選「下載」按鈕，即可下載本服務之報表操作說明。

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」。

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。

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「帳號與連絡資訊設定」。

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。

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」。

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。

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」。

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。

4. 網站弱點掃描

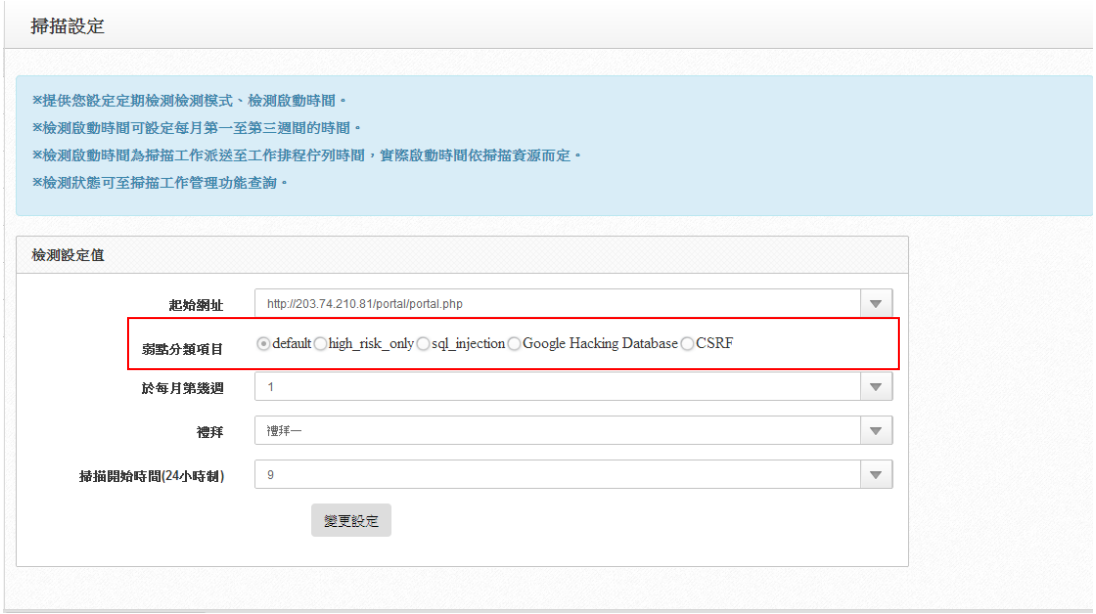
1. 服務簡介

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，並提供弱點掃瞄分析報表，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。

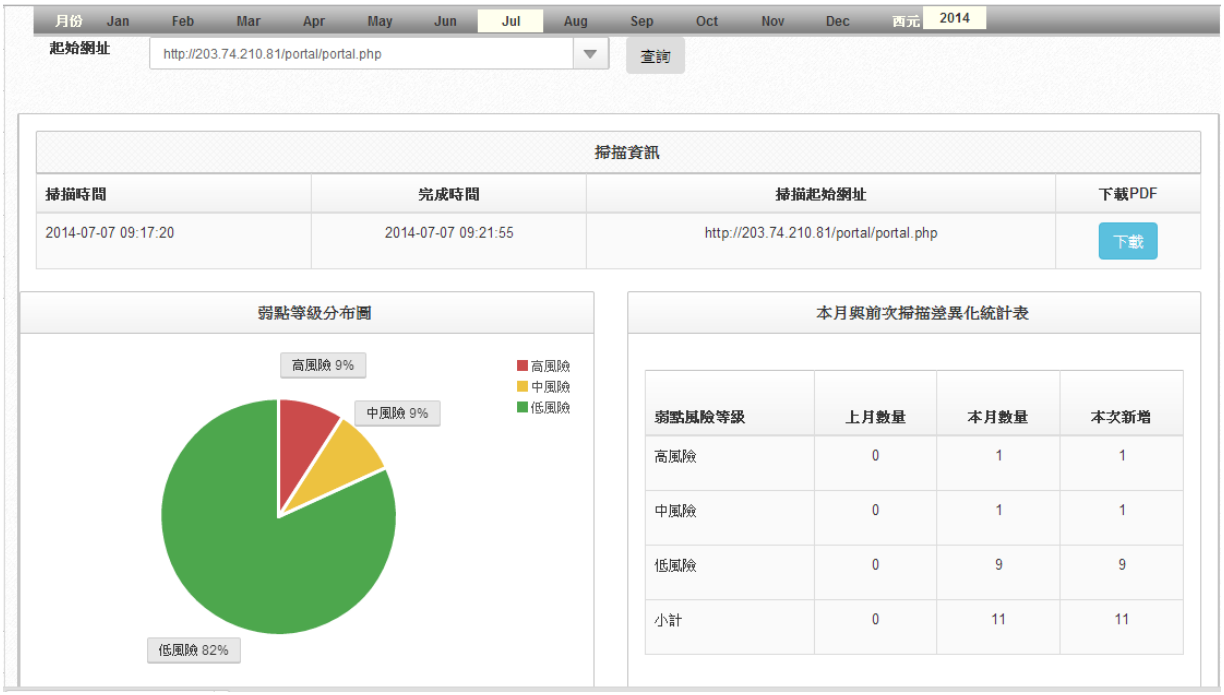


掃描時間設定則依用戶需要可選擇每月的第幾週，禮拜幾與指定小時啟動檢測，弱點分類與檢測時間選擇確定後，按下變更設定按鈕即完成設定。

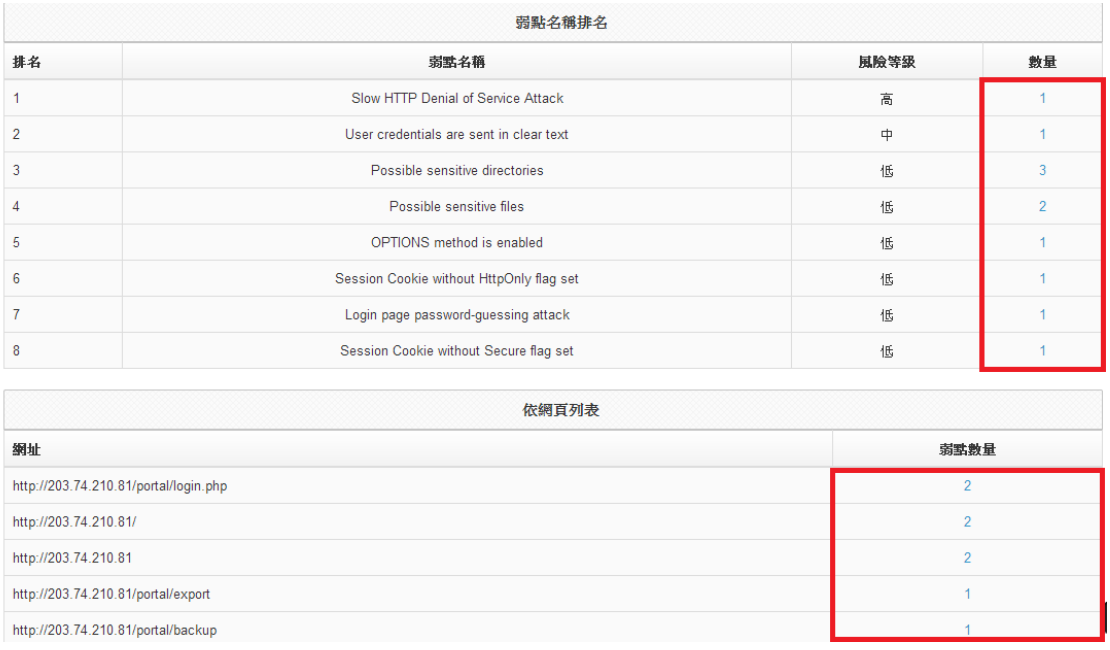
b. 定期檢測報表查詢

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。

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。



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。

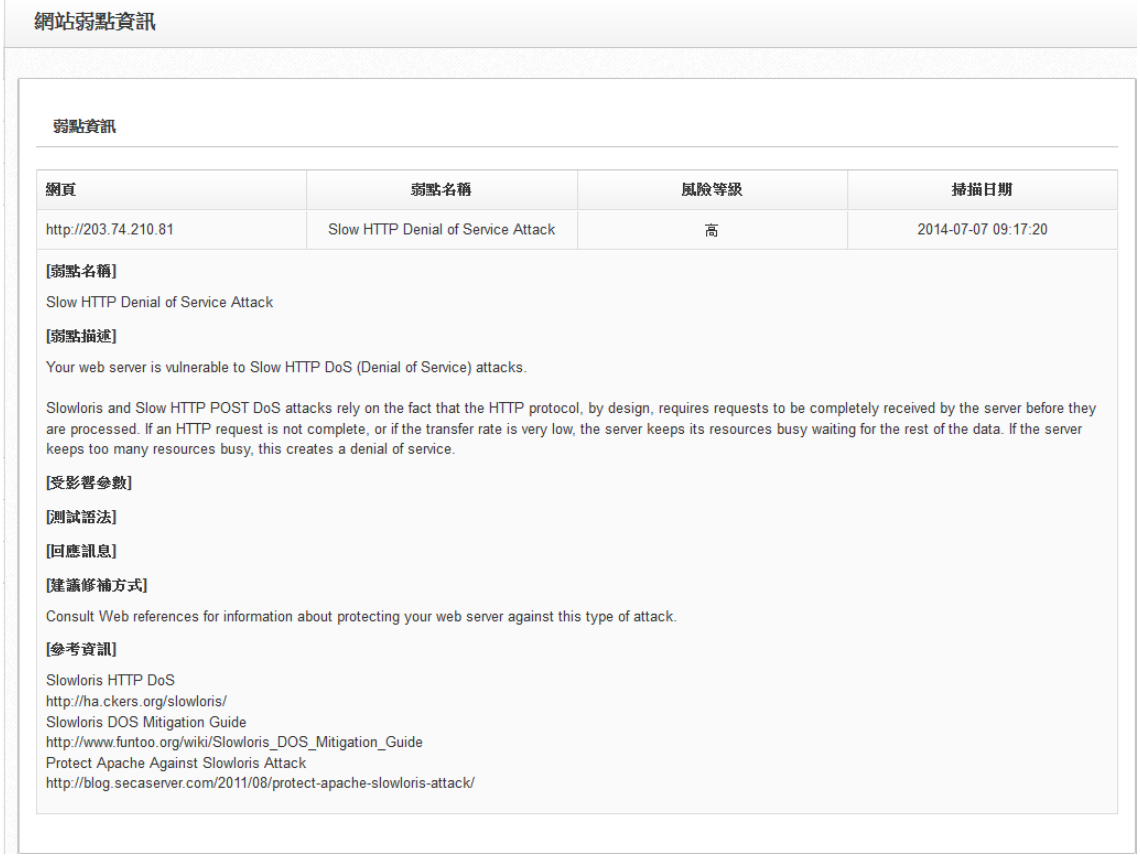


弱點名稱排名

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



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]

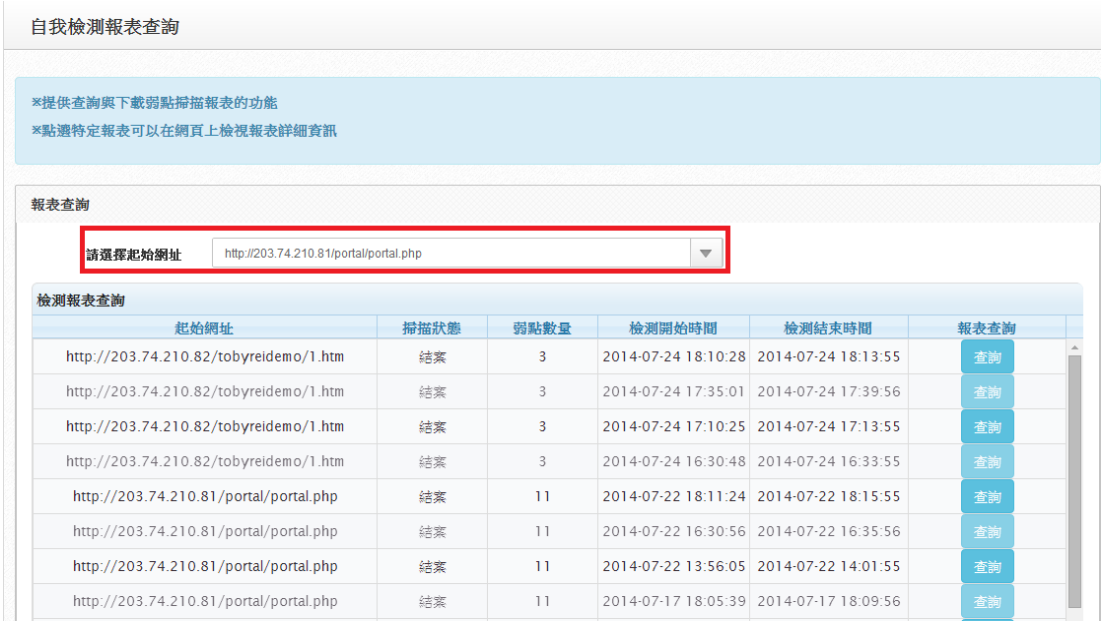
Consult Web references for information about protecting your web server against this type of attack.

[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
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。



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。

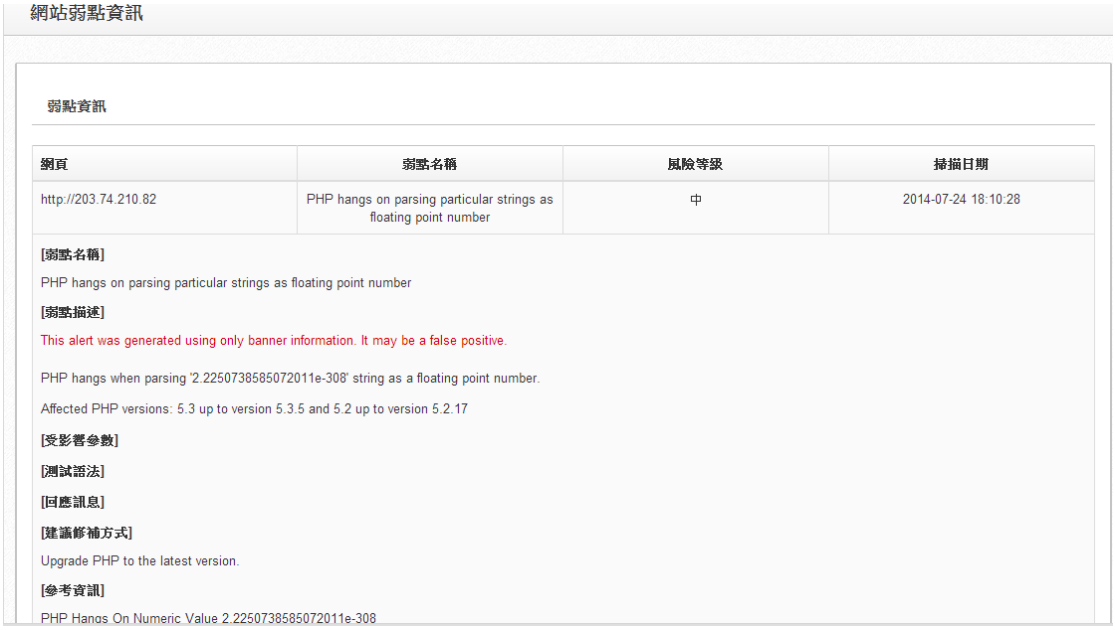
若欲查看弱點詳細資訊，可透過點選弱點排名或依網頁列表排序弱點數量圖表中的弱點數量連結，即可查看該弱點之弱點描述與修補建議。

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

[弱點名稱]

PHP hangs on parsing particular strings as floating point number

[弱點描述]

This alert was generated using only banner information. It may be a false positive.

PHP hangs when parsing '2.2250738585072011e-308' string as a floating point number.

Affected PHP versions: 5.3 up to version 5.3.5 and 5.2 up to version 5.2.17

[受影響參數]

[測試語法]

[回應訊息]

[建議修補方式]

Upgrade PHP to the latest version.

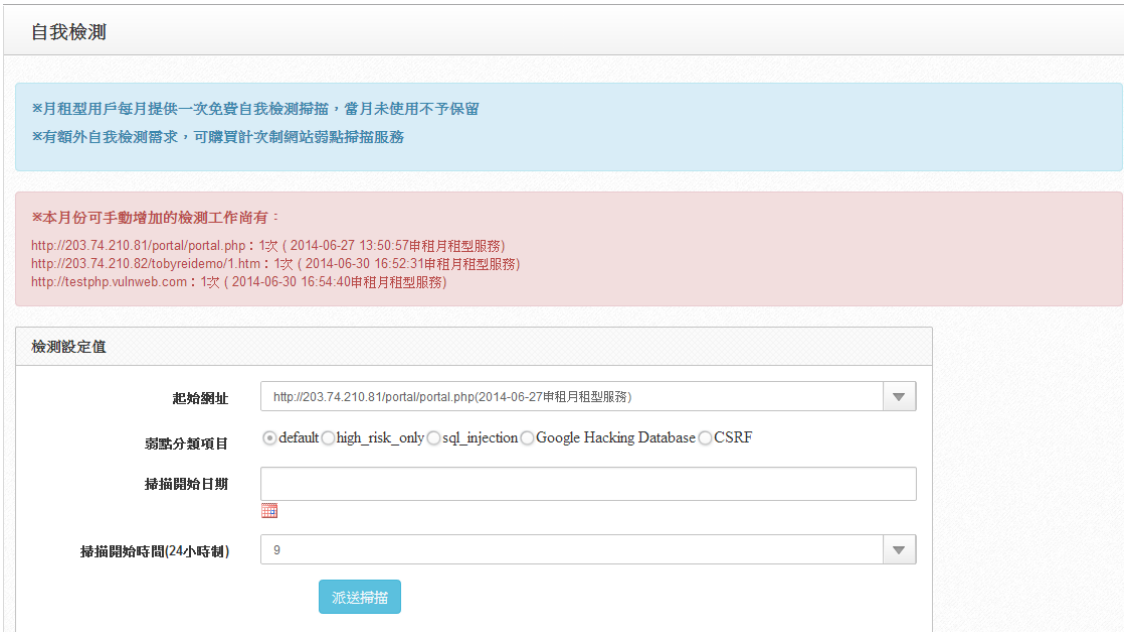
[參考資訊]

PHP Hangs On Numeric Value 2.2250738585072011e-308

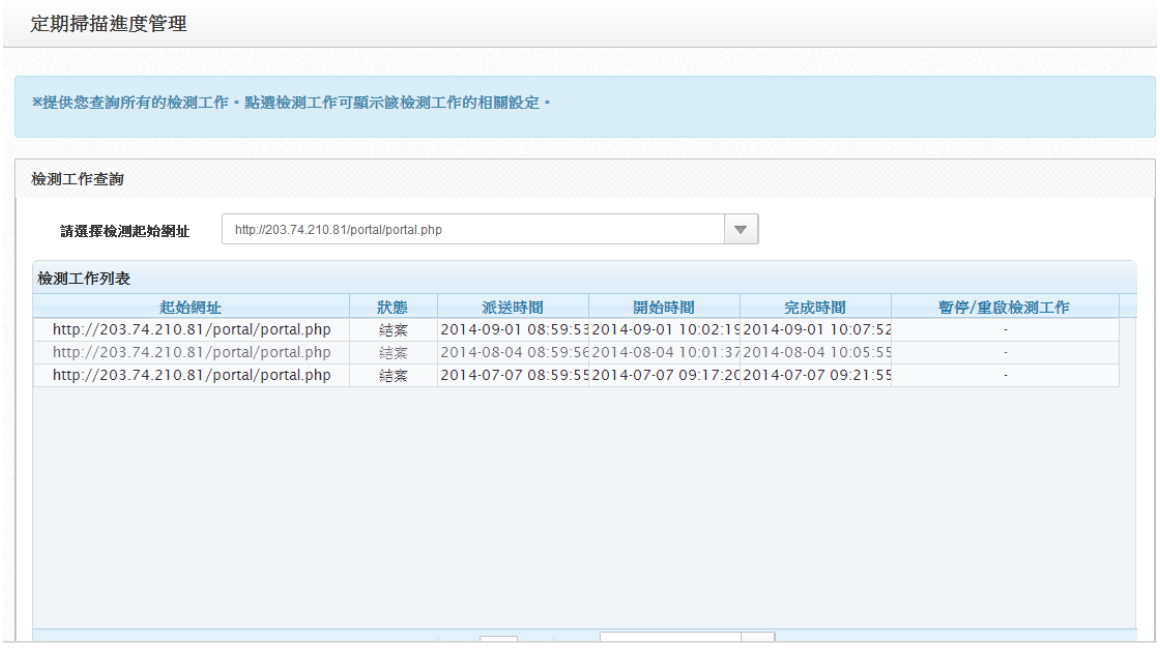
d. 自我檢測

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。



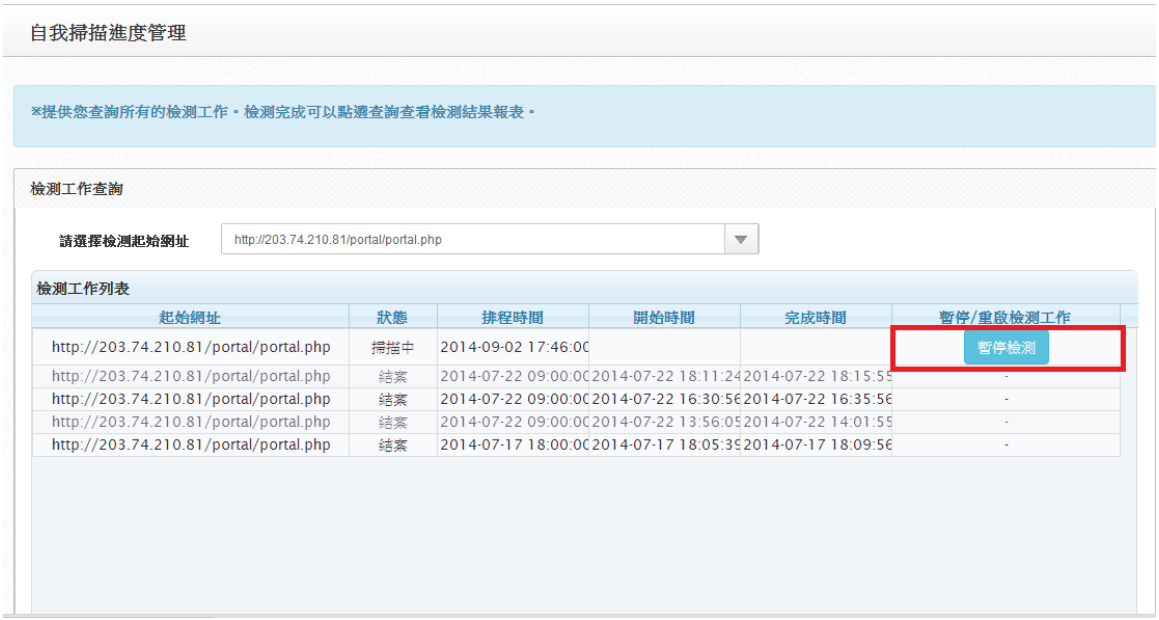
e. 定期掃描工作管理

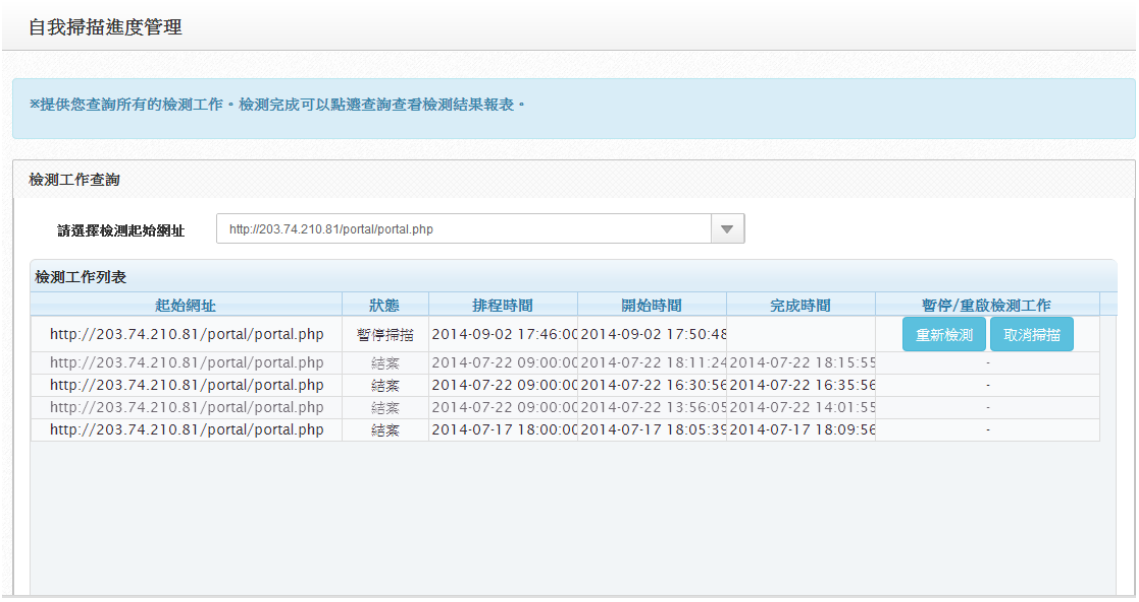


f. 自我掃描工作管理

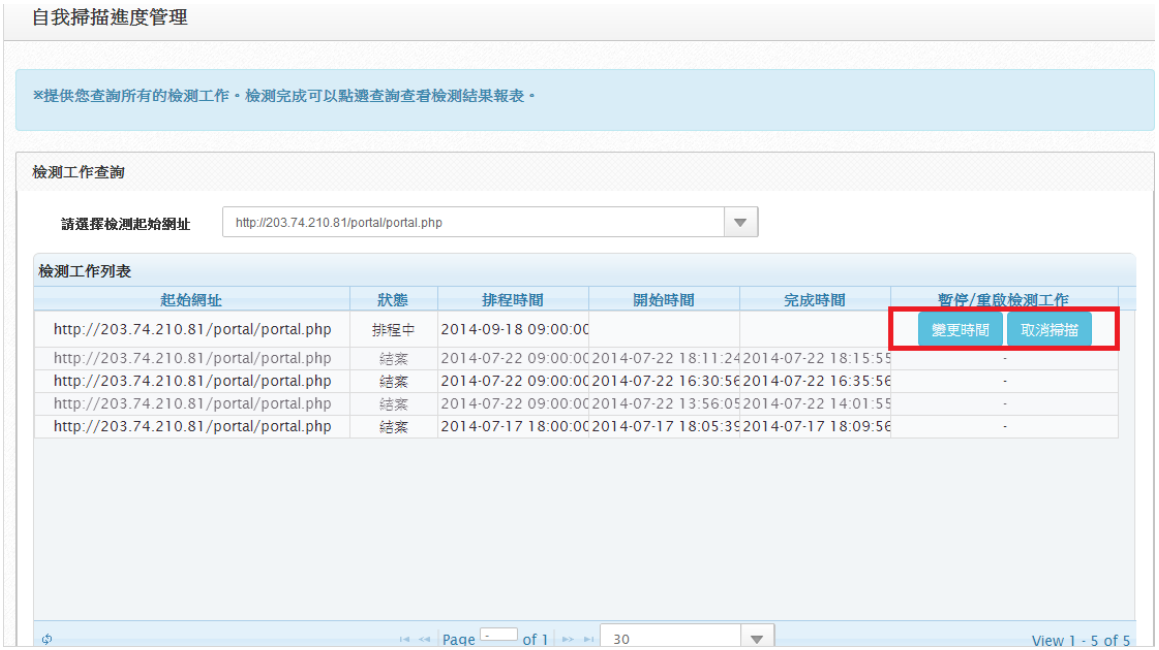
此功能是讓用戶可因其需要針對排程中或掃描中的網站進行暫停檢測或啟動檢測的管理。

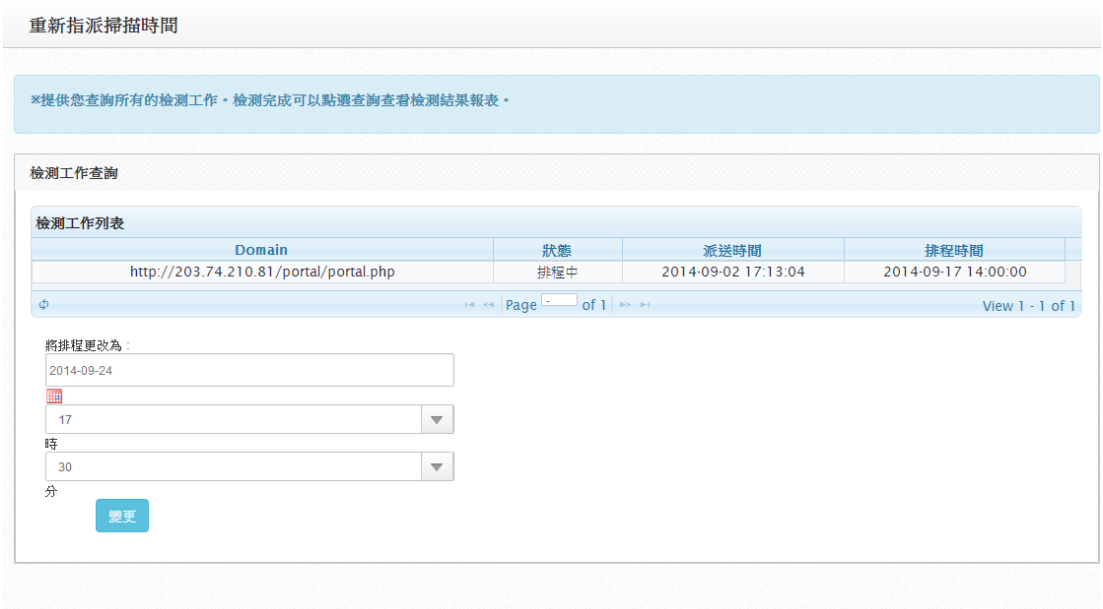
正在進行掃描中的工作，用戶可以點選暫停，但點選暫停後，若需要重新檢測，掃描將重新開始無法接續暫停前的狀態。





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。


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
http://203.74.210.81/portal/portal.php
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
變更時間
取消掃描
結案
Page
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
Page
of 1
View 1 - 1 of 1
將排程更改為：
2014-09-24
17
時
30
分
變更

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

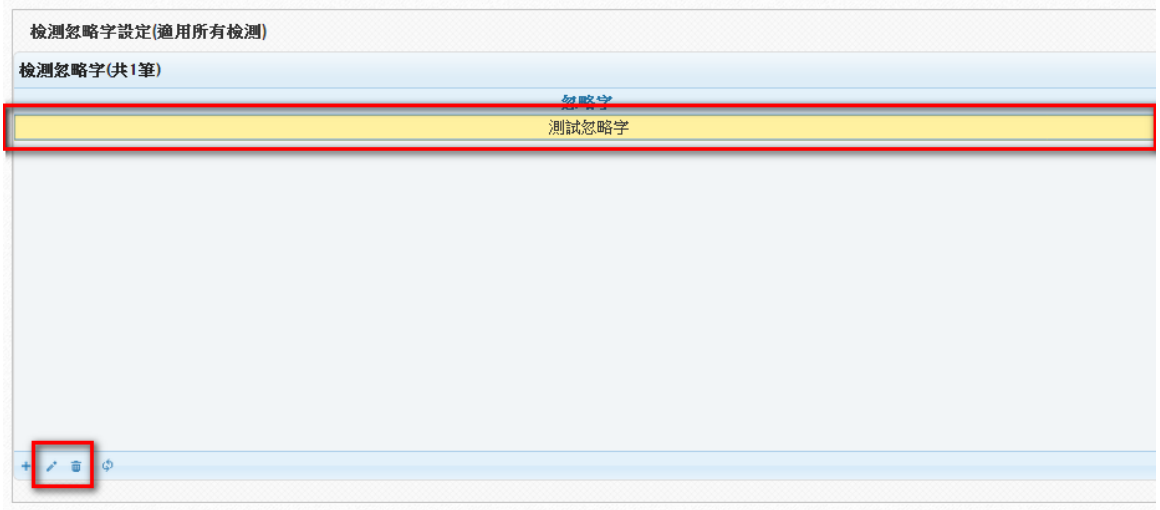
本功能提供用戶進行檢測項目設定、檢測忽略字設定、定期檢測啟動時間設定(預設於每月 1 號開始檢測)。

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。

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。

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。

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。

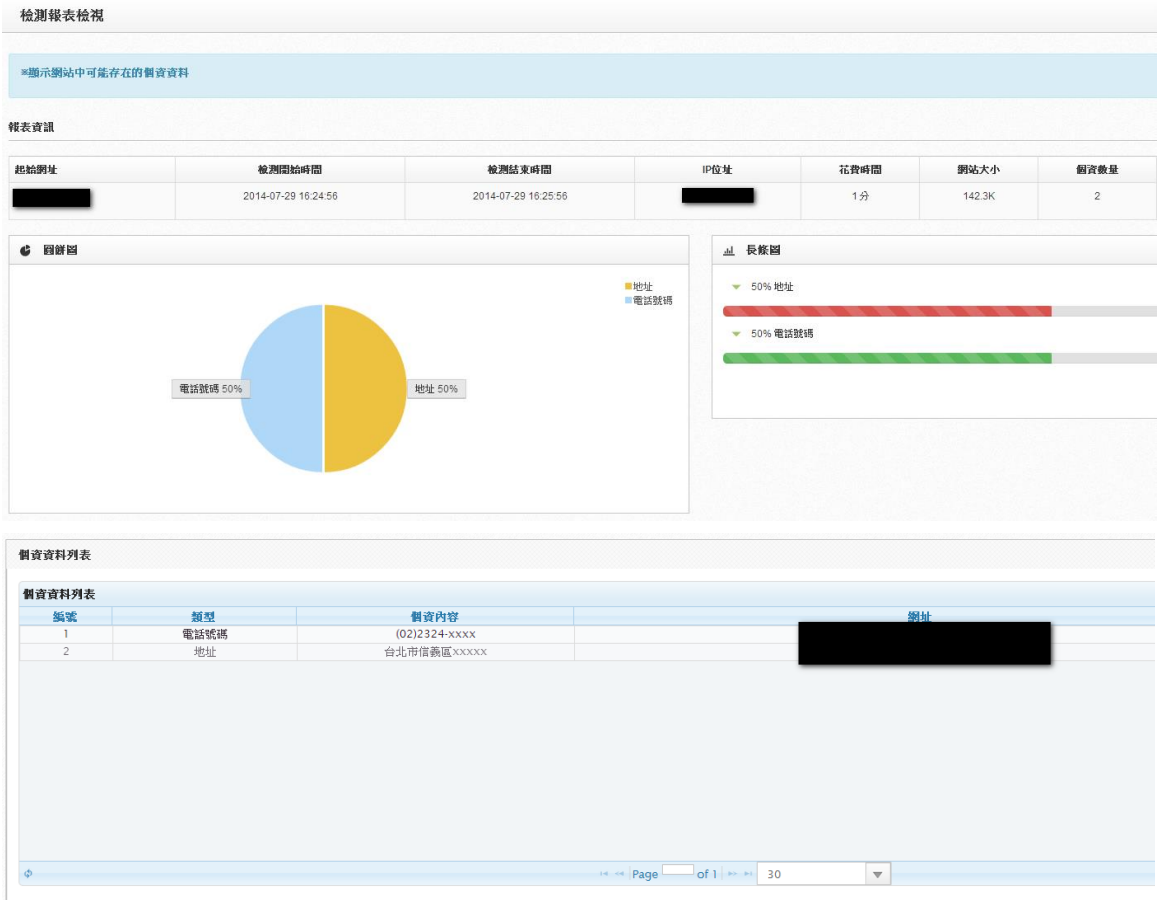


b. 定期檢測報表查詢

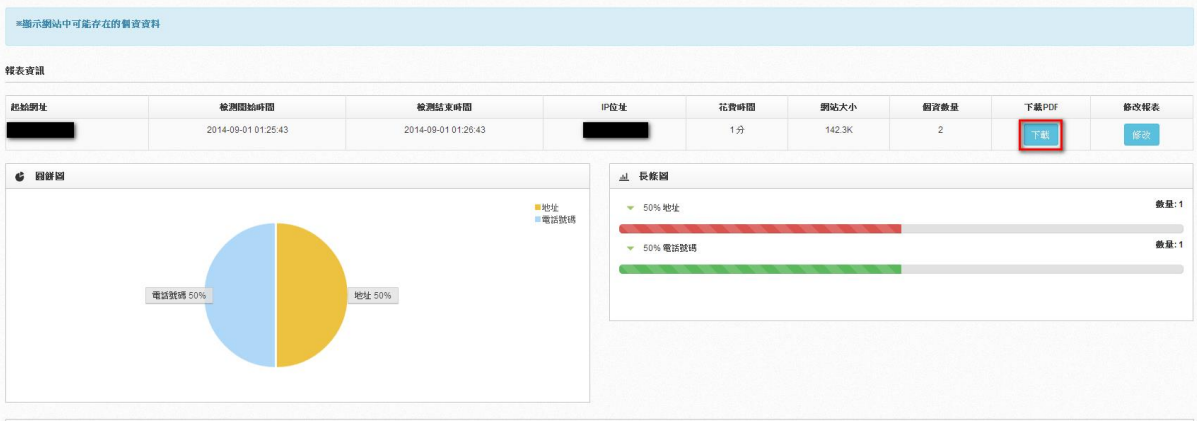
月租型客戶每月會固定派送定期檢測，掃描完成後的報表可在定期檢測報表查詢功能查詢。

點入此功能後可直接點選要下載的 PDF 報表：

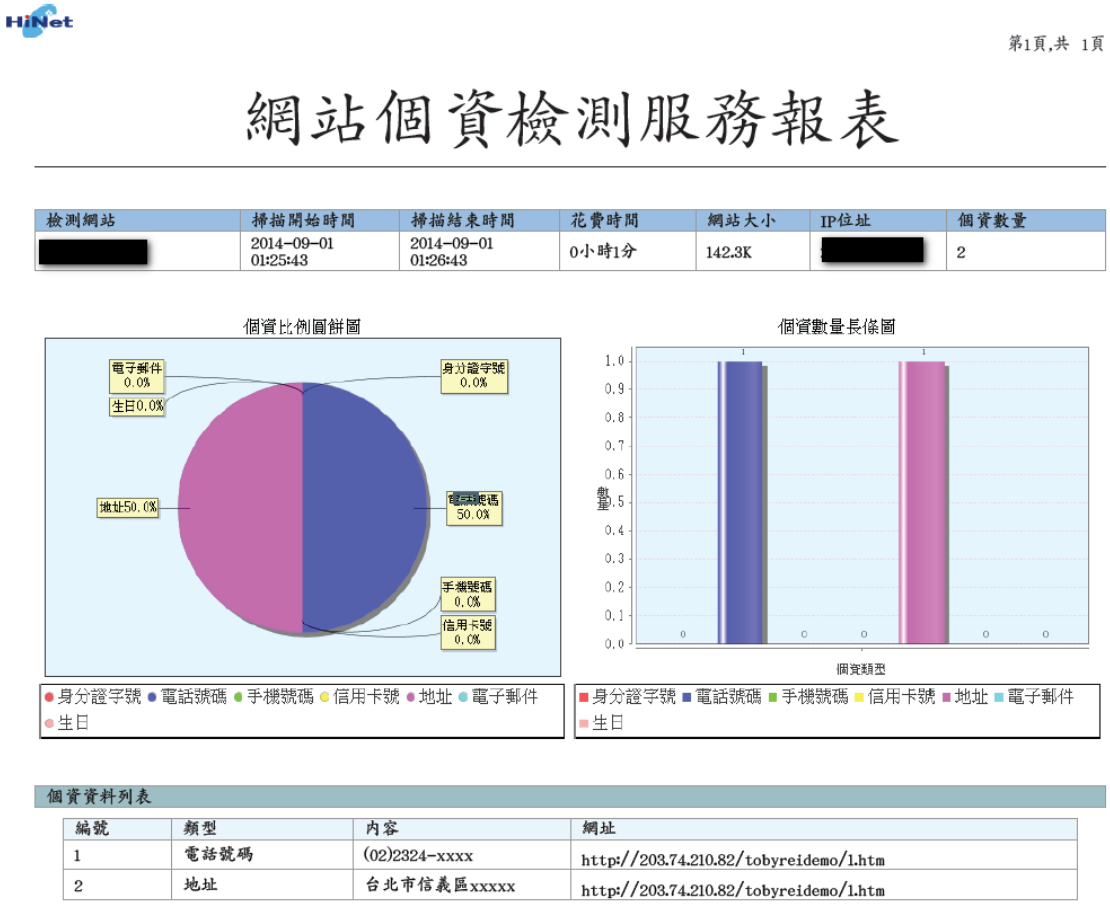
或是點選想要查看詳細資訊的月份後，在網頁上呈現當月報表：



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)。



PDF 格式的報告：



HiNet

第1頁,共 1頁

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

個資比例圖餅圖

個資數量長條圖

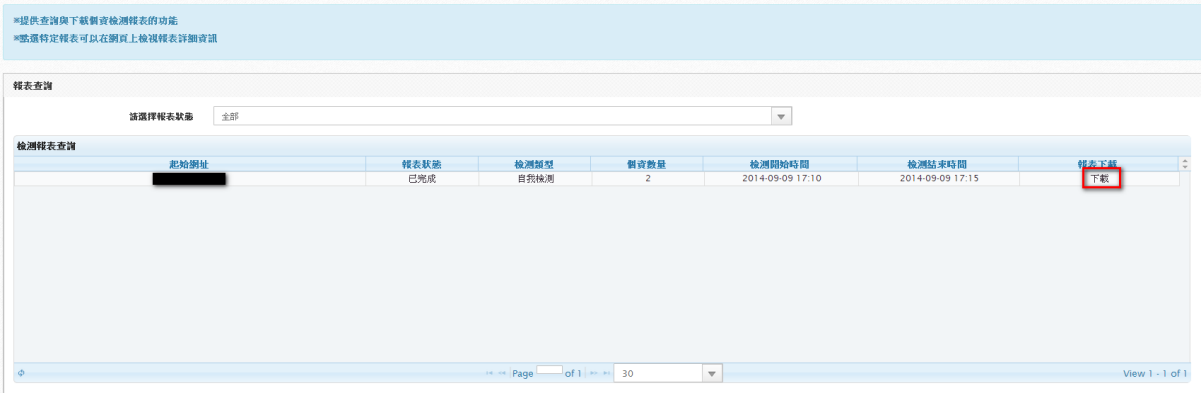
個資資料列表

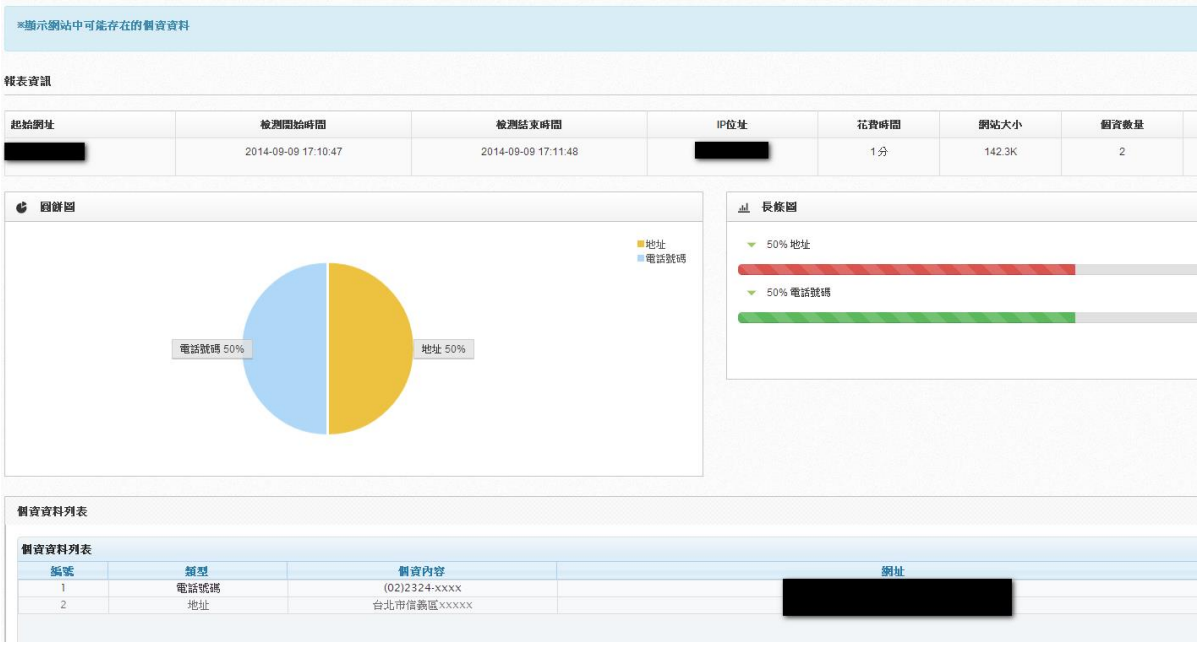
編號	類型	內容	網址
1	電話號碼	(02)2324-xxxx	http://203.74.210.82/tobyreidemo/1.htm
2	地址	台北市信義區xxxxx	http://203.74.210.82/tobyreidemo/1.htm

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。



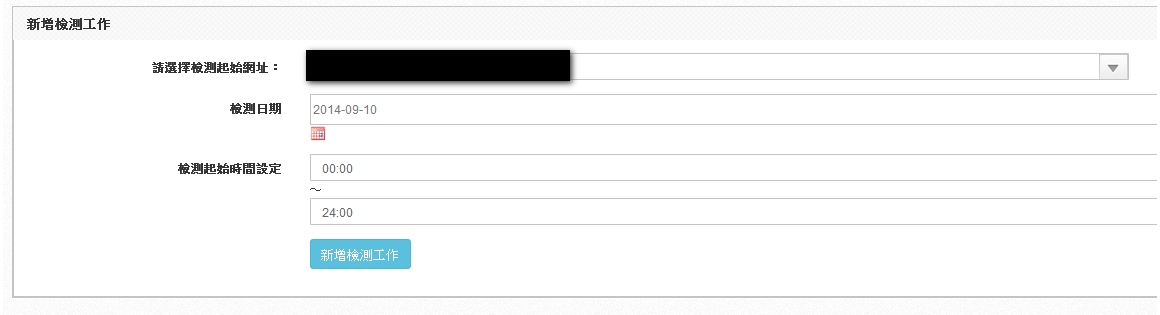


d. 新增檢測工作

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。

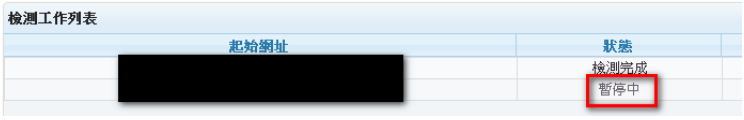
畫面中紅色的區塊會註明可新增檢測的次數。

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。

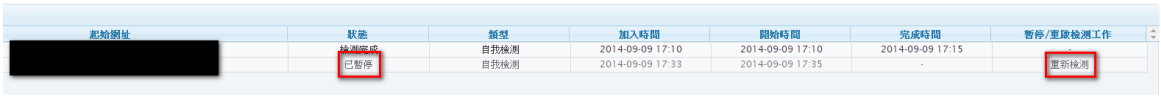


e. 定期檢測工作管理

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。

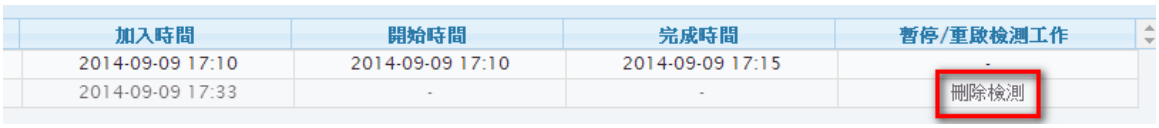


暫停檢測後，可重新啟動檢測：



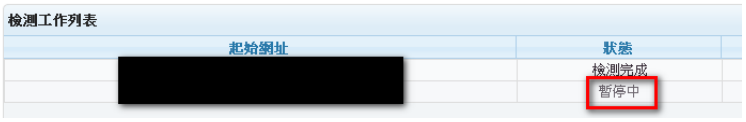
f. 自我檢測工作管理

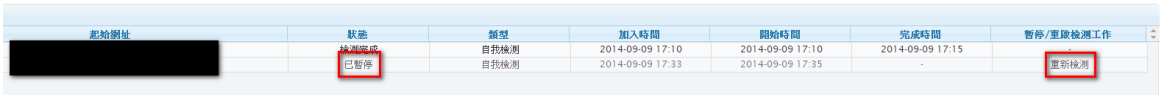
計次型客戶及月租型客戶每月自行新增的檢測工作可在此功能查看執行狀況。與定期檢測不同的是，若自我檢測尚未開始掃描，是可以刪除的。



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。





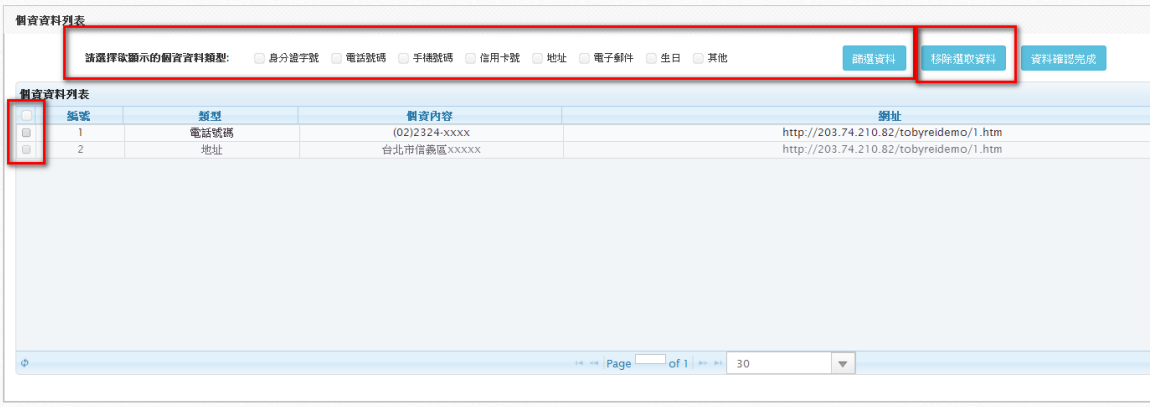
g. 檢測報表修改

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。

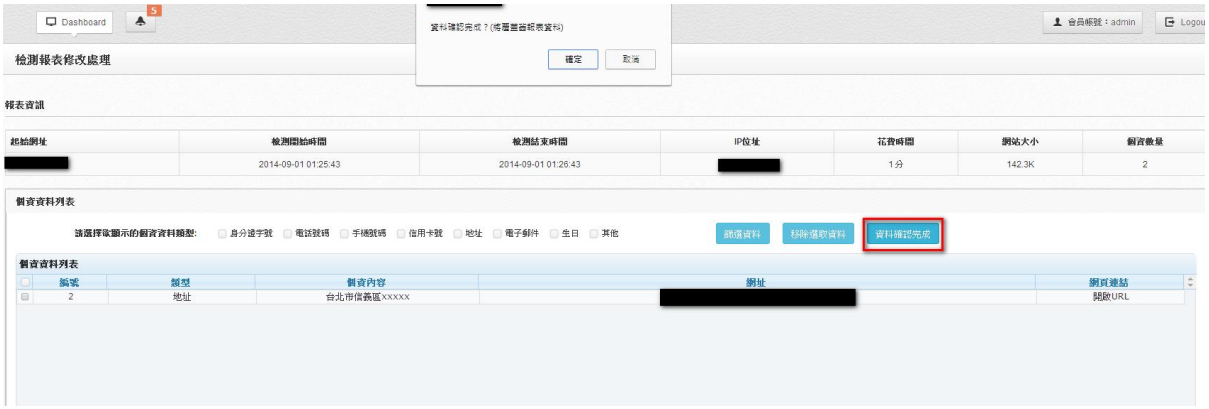
點選定期或自我檢測報表查詢，並按下要修改的報表：

接著點選畫面右上方的修改報表：

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。



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。



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

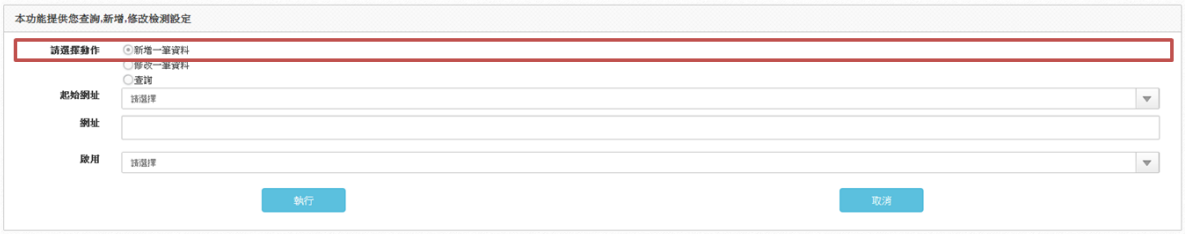
a. 檢測設定

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。

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



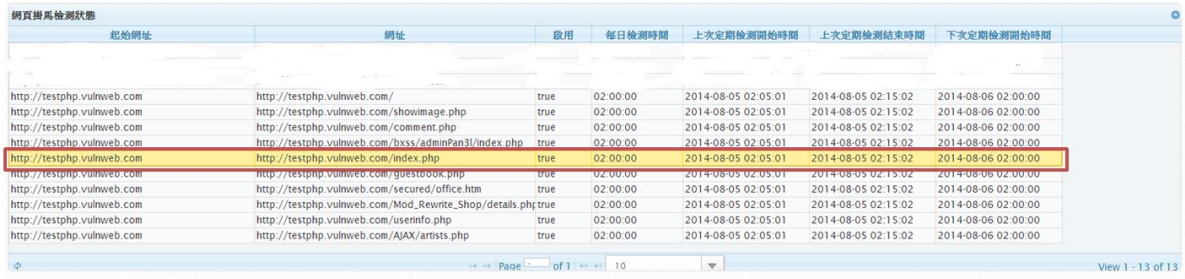
2nd.　選擇起始網址並填寫相關設定(各項設定說明請見下方備註一)

3rd.　按執行，即可完成

(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)

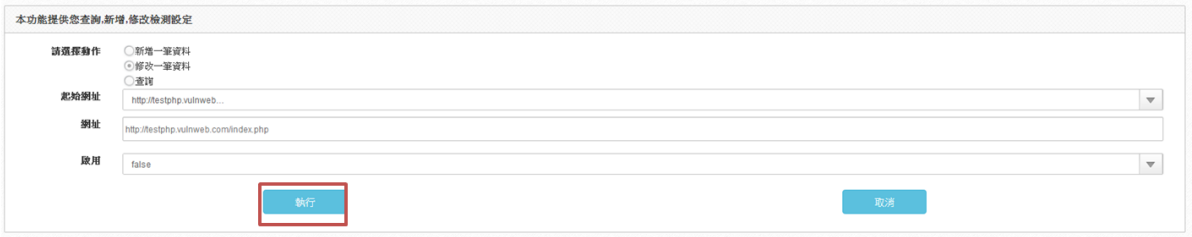
2nd.　在下方資料中選擇您要修改的那筆資料並點選



3rd.　此時上方輸入框會出現這筆資料的相關訊息

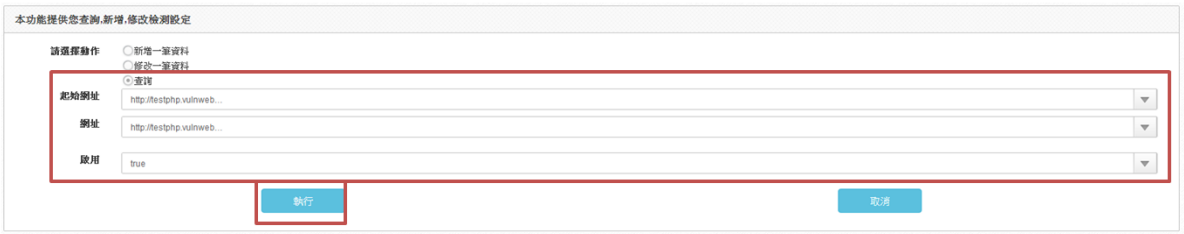
4th.　輸入要修改的值(在此範例我們把啟用改成 false)

5th.　按執行，即可完成



(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

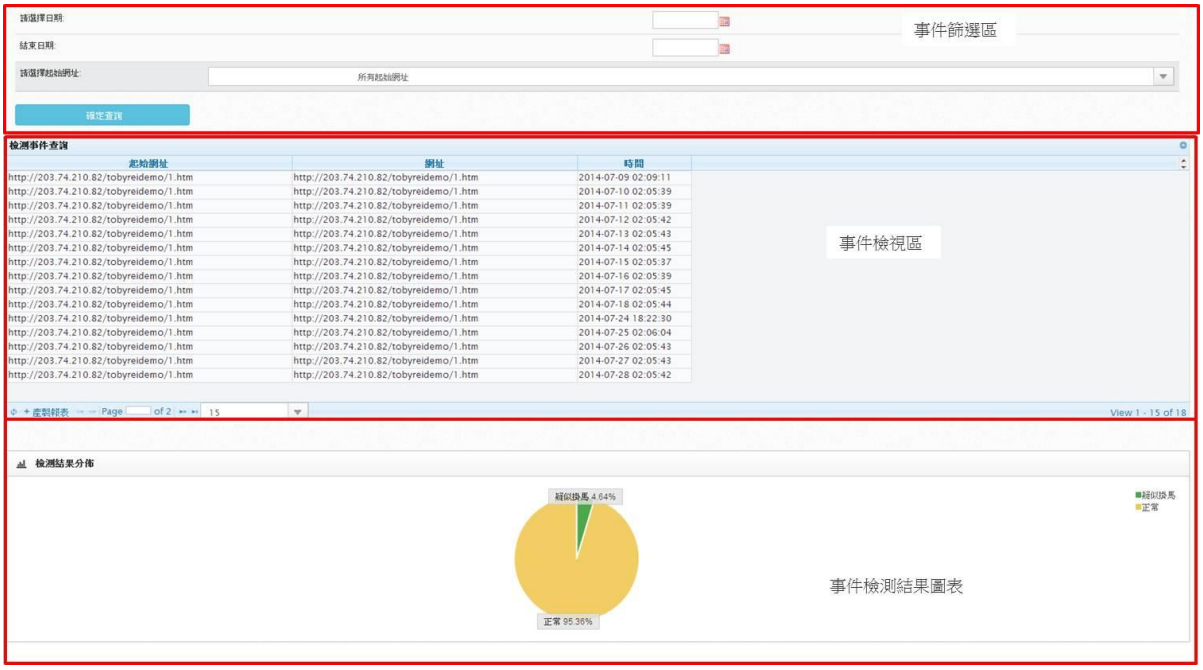
如果跳出”新增成功或修改成功”，表示新增資料或修改資料成功；如果跳出一些錯誤訊息，請按照錯誤訊息來修改輸入的資料。

(6) 備註三

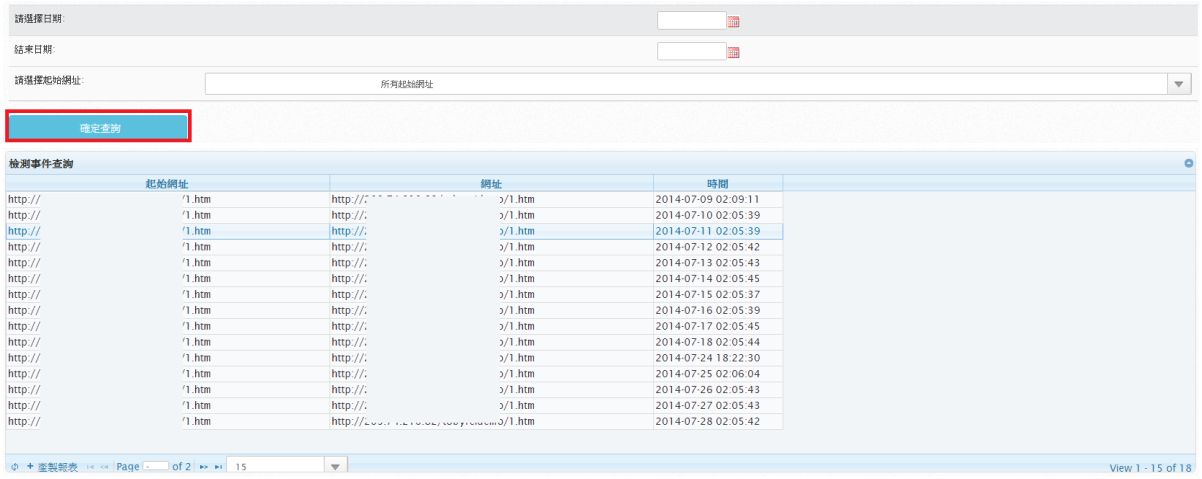
按取消紐可以把正在輸入的值清掉，此時就可以再重新輸入一遍。

b. 檢測報表查詢

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。

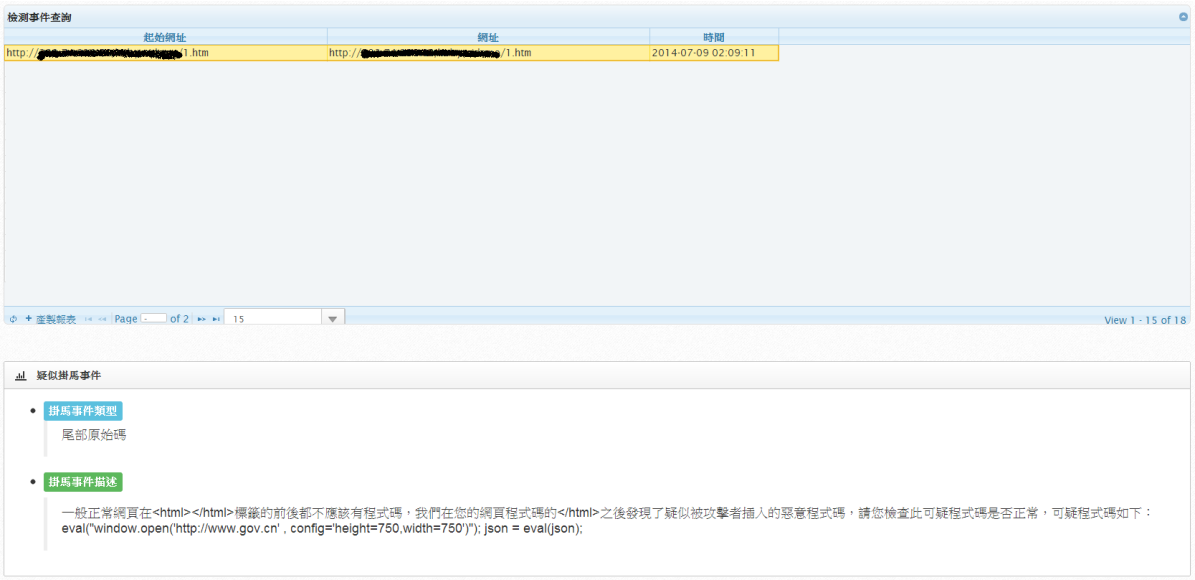


在事件篩選區，使用者可以篩選事件開始時間、結束時間以及起始網址。按下確定查詢後，篩選結果會立即顯示在事件檢視區。



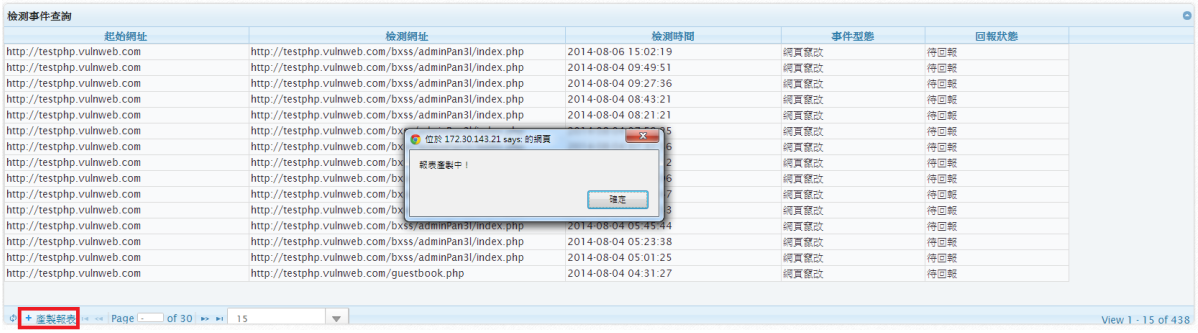
檢測事件檢視區可以查到每一筆疑似遭受掛碼事件的起始網址、檢測網址、檢測的時間，表格左下角處可以重新整理、依照目前篩選結果產生報表以及變更顯示筆數、翻頁。

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。



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。



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：

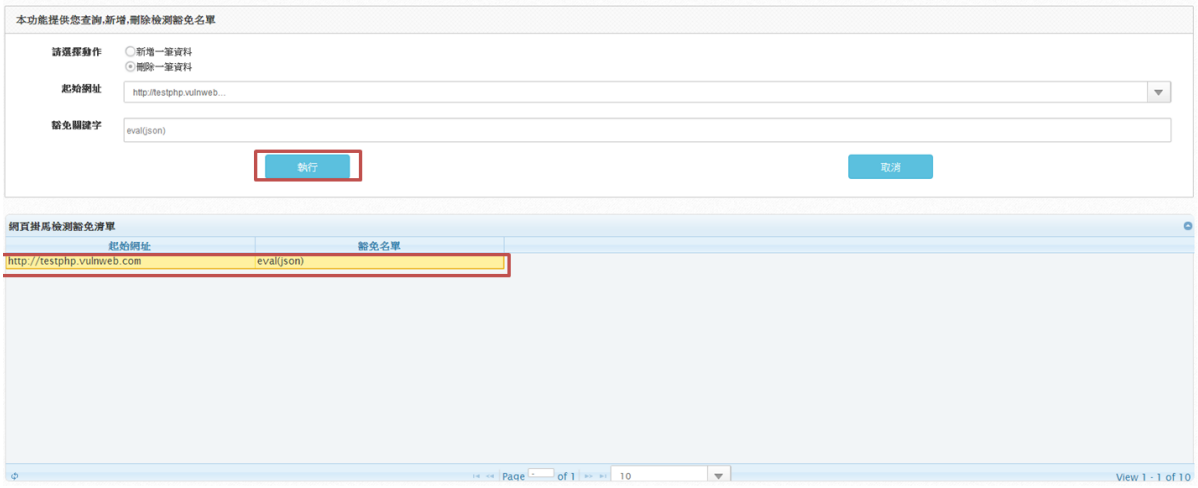
(1) 新增一筆資料

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**

(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**

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。



(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。

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

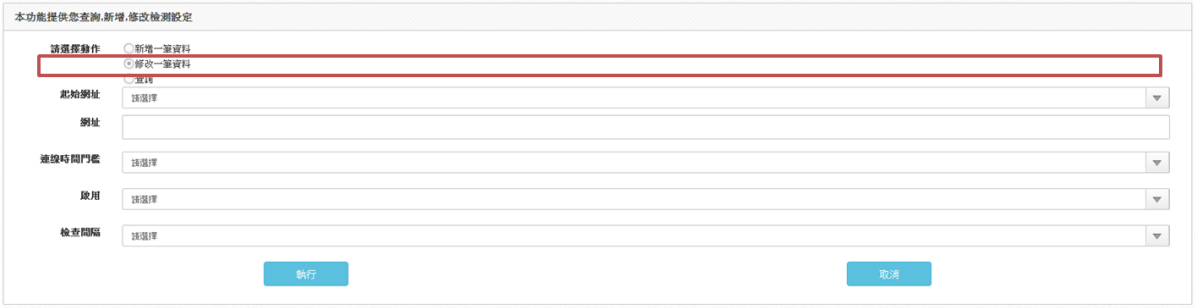
1st. 選擇新增一筆資料

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)

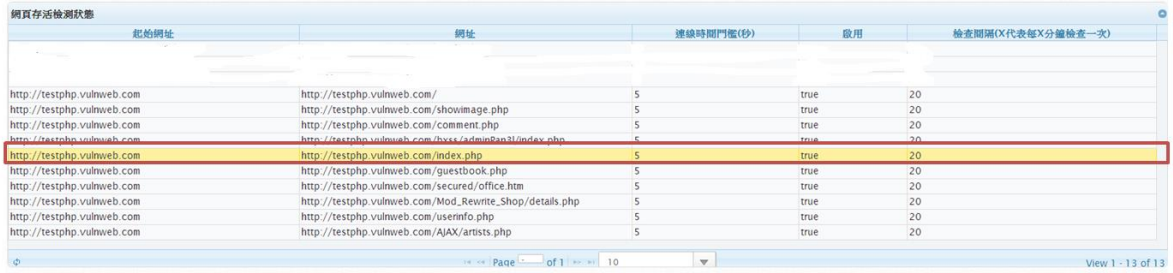
3rd.　按執行，即可完成

(2) 修改一筆資料

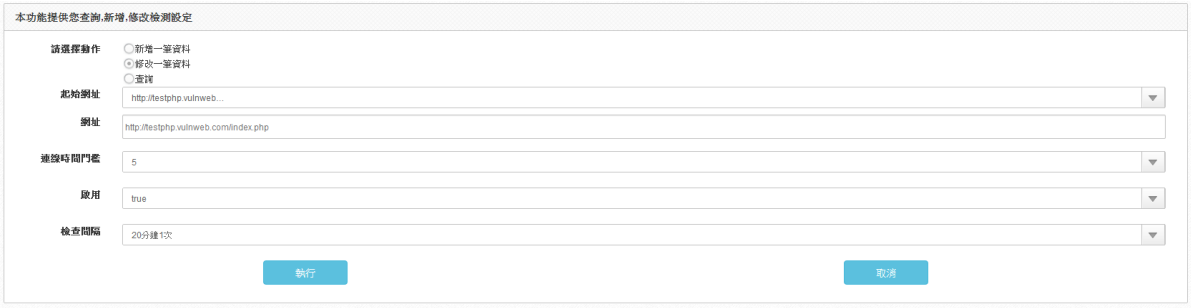
1st.　選擇修改一筆資料(這時會跳出提示訊息，按下確定即可)



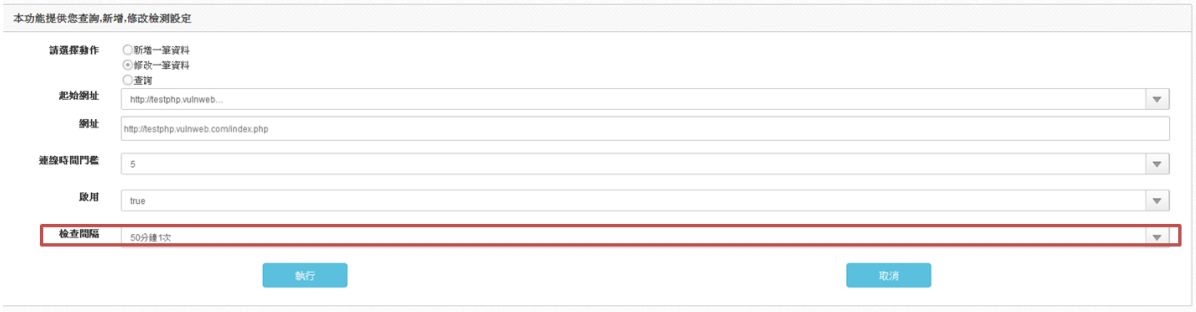
2nd.　在下方資料中選擇您要修改的那筆資料並點選



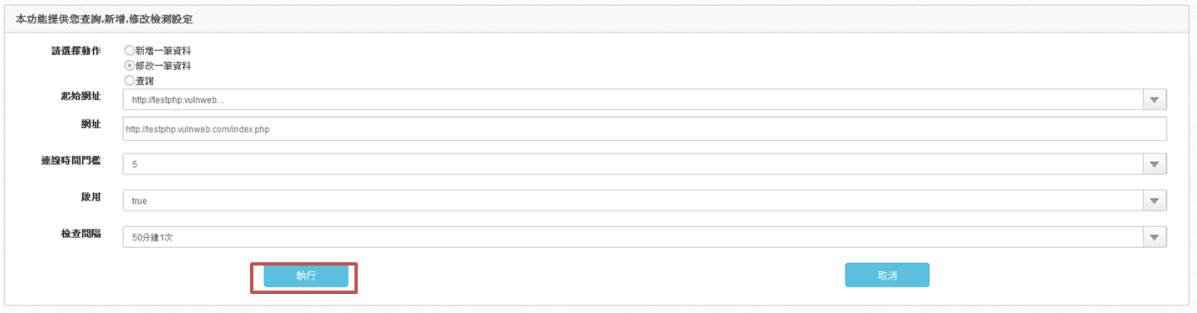
3rd.　此時上方輸入框會出現這筆資料的相關訊息



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)

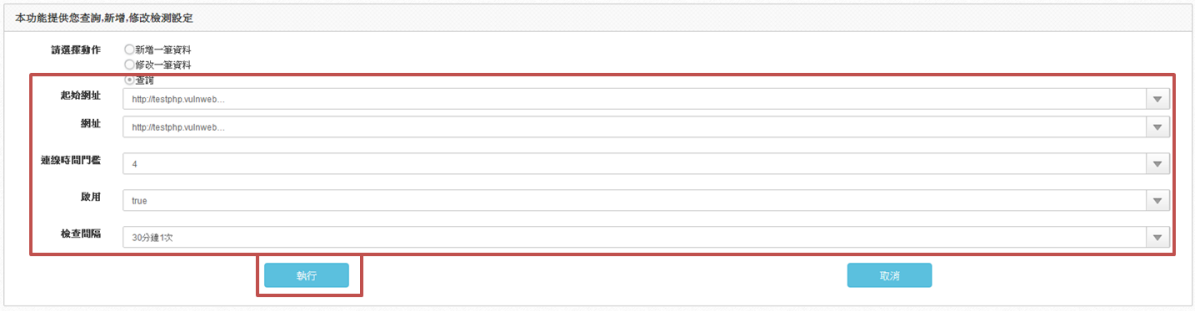


5th.　按執行，即可完成



(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

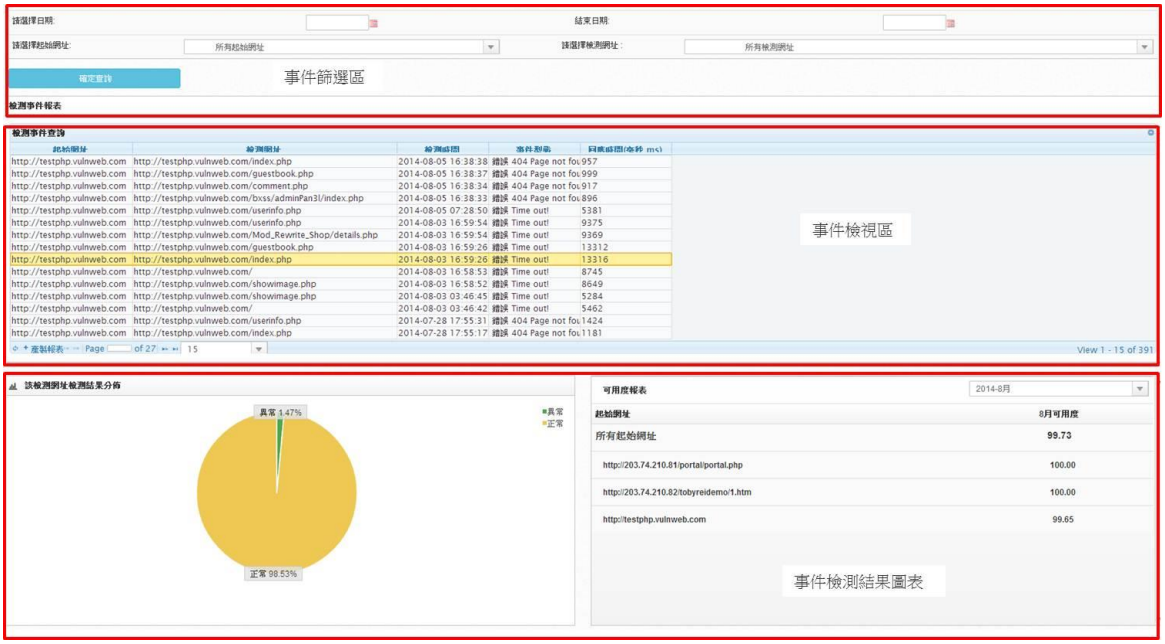
如果跳出”新增成功或修改成功”，表示新增資料或修改資料成功；如果跳出一些錯誤訊息，請按照錯誤訊息來修改輸入的資料。

(6) 備註三

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。

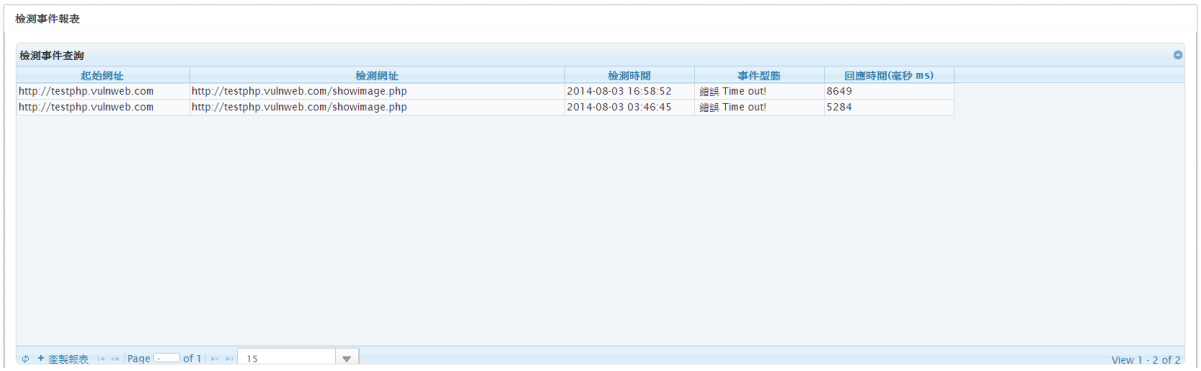
b. 檢測報表查詢

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。

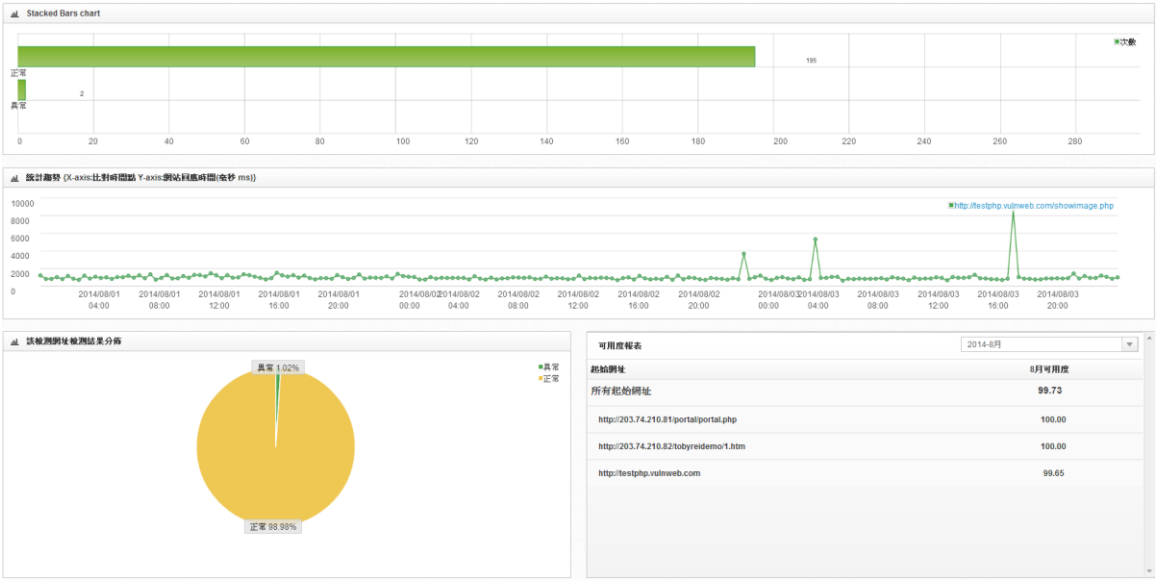


在事件篩選區，使用者可以篩選事件開始時間、結束時間、起始網址、監控網址。按下確定查詢後，篩選結果會立即顯示在事件檢視區。

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。



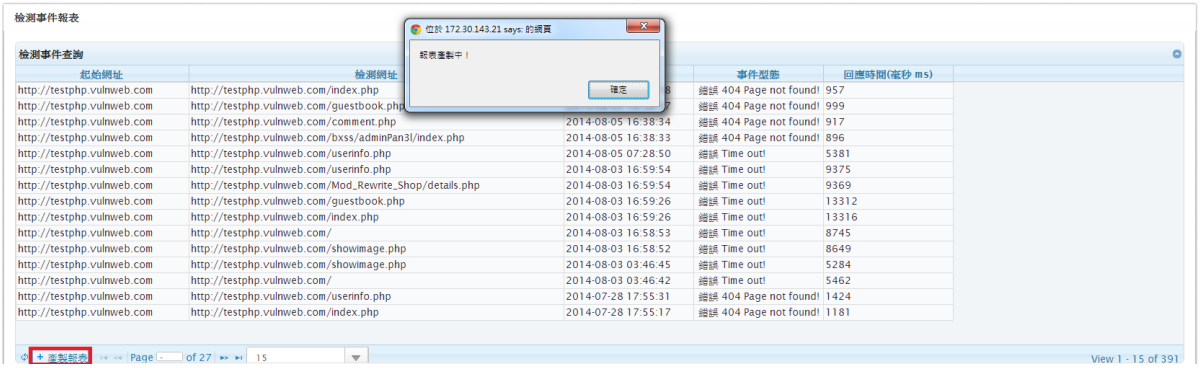
事件檢測結果分佈會依據篩選結果更動，若指定單一檢測網址會進一步顯示詳細的數據。



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

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。

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

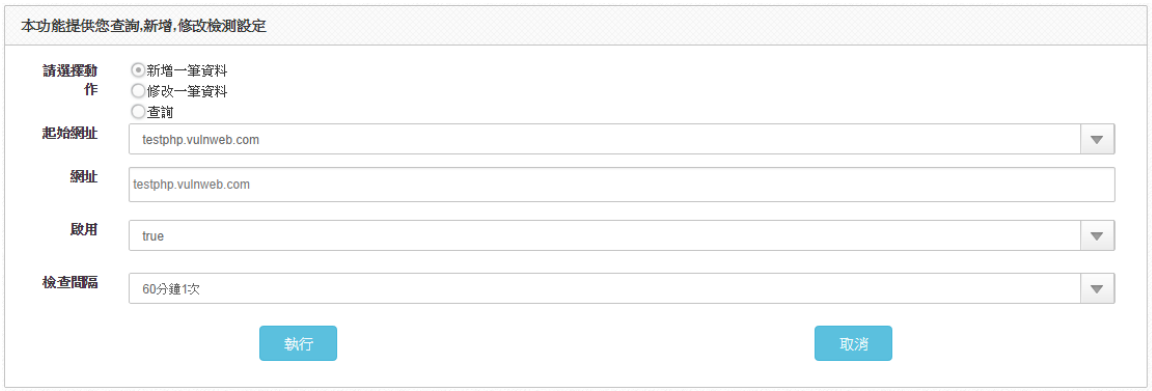
a. 檢測設定

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：

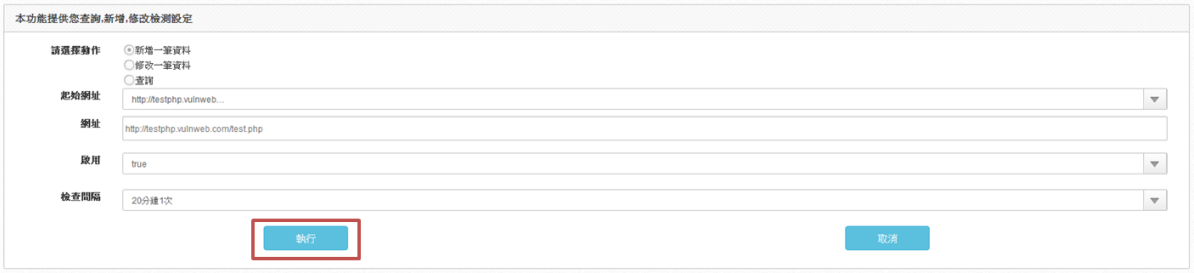
(1) 新增一筆資料

1st. 選擇新增一筆資料

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)



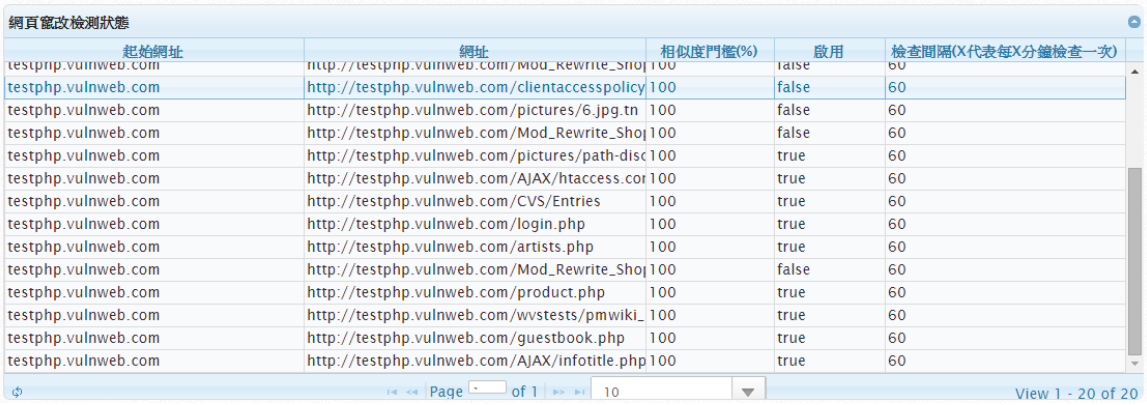
3rd.　按執行，即可完成



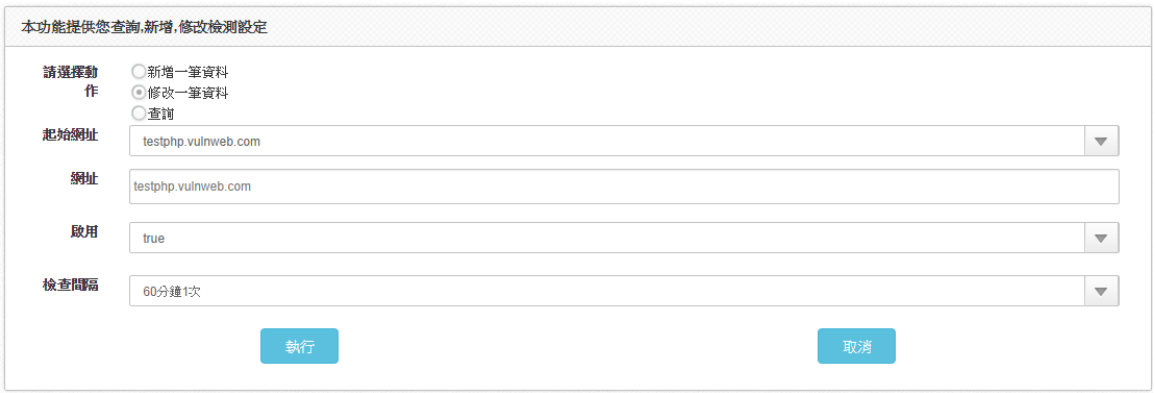
(2) 修改一筆資料

1st.　選擇修改一筆資料(這時會跳出提示訊息，按下確定即可)

2nd.　在下方資料中選擇您要修改的那筆資料並點選



3rd.　此時上方輸入框會出現這筆資料的相關訊息



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)

5th. 按執行，即可完成

(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。

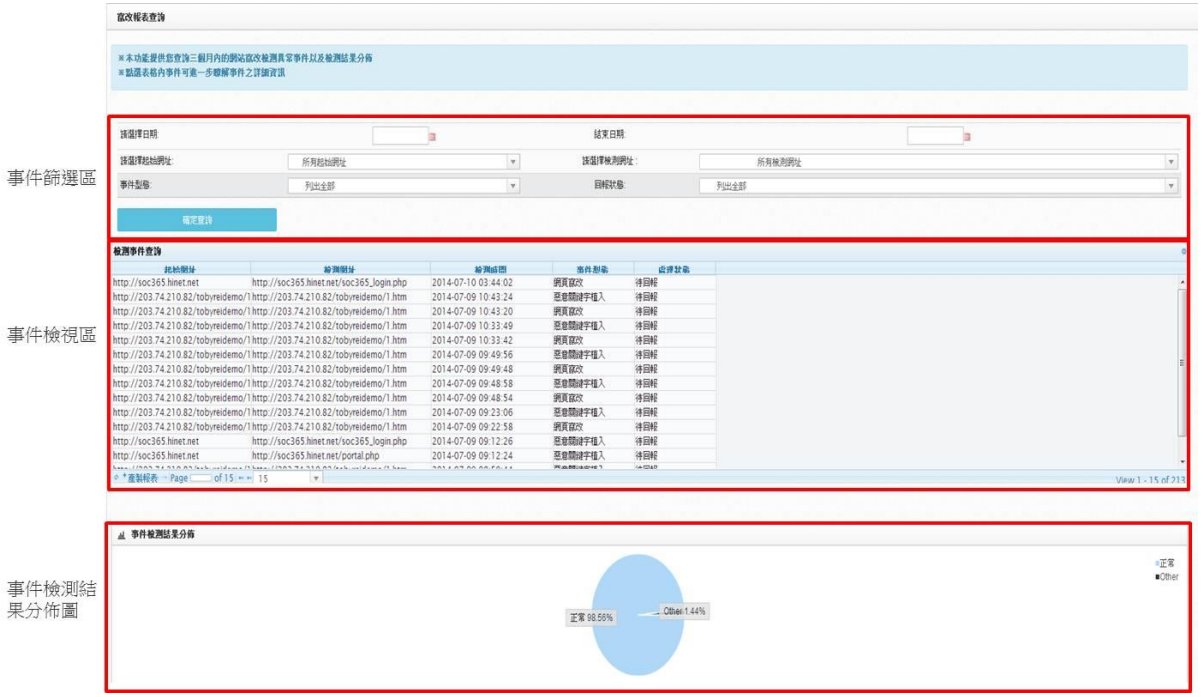
(6) 備註三

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

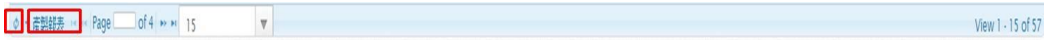
(1) 功能區塊說明

竄改報表查詢功能可提供使用者查詢三個月內的網站竄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。

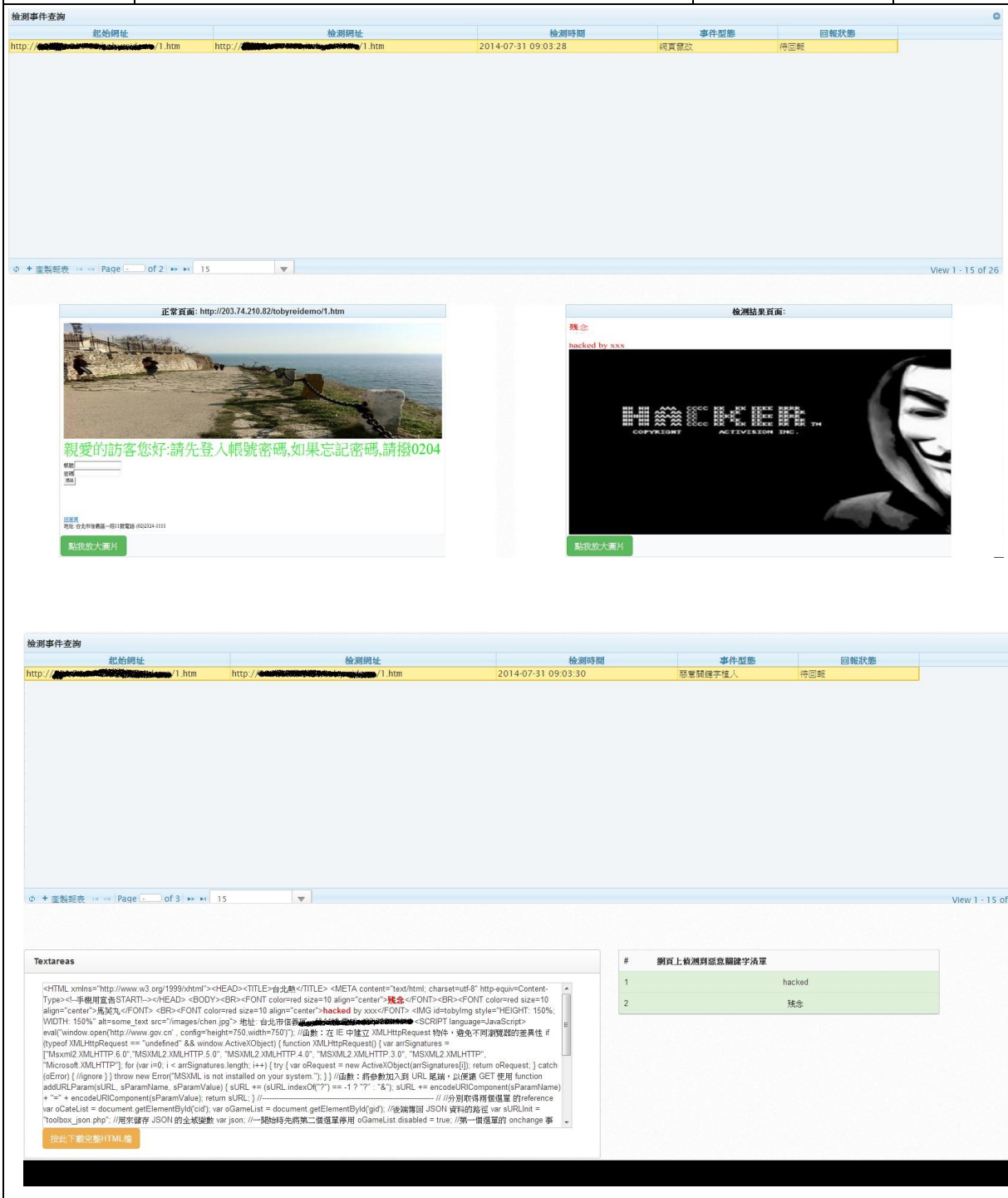


在事件篩選區，使用者可以篩選事件開始時間、結束時間、起始網址、監控網址、事件型態以及目前回報狀態。

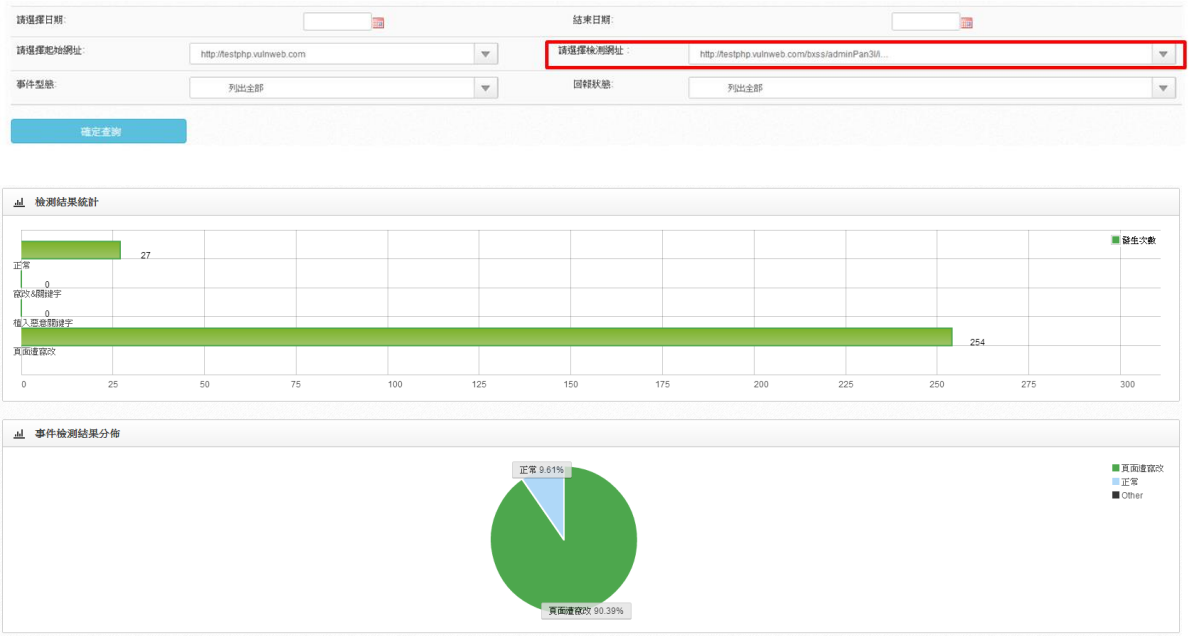
按下**確定查詢**後，篩選結果會立即顯示在事件檢視區，
檢測事件檢視區可以查到每一筆疑似遭受竄改事件的起始網址、檢測網址、檢測的時間、遭駭的事件類型以及回報的狀態，表格左下角處可以重新整理、依照目前篩選結果產生 PDF 報表以及變更顯示筆數、翻頁。



點選表格中其中一筆事件可在下方檢視更加詳細的資訊，如竄改事件則可以看到原先頁面以及遭受竄改頁面的比較，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。

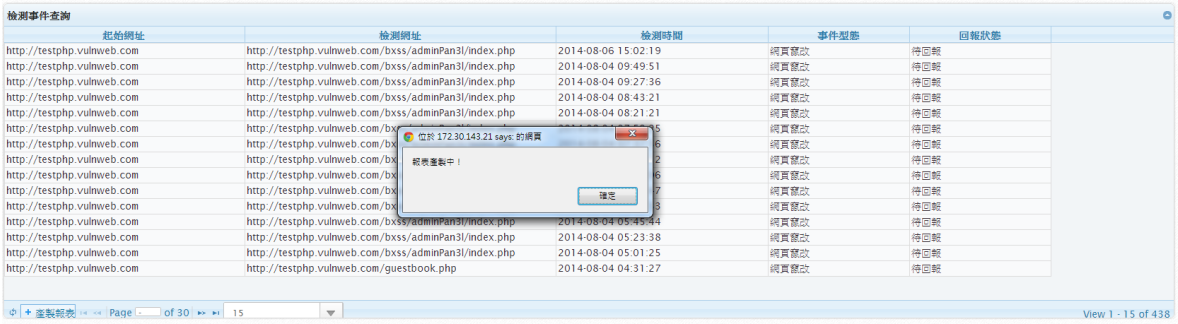


事件檢測結果分佈會依據篩選結果動態變動，若指定單一檢測網址會進一步顯示詳細的數據。



c. 檢測報表下載

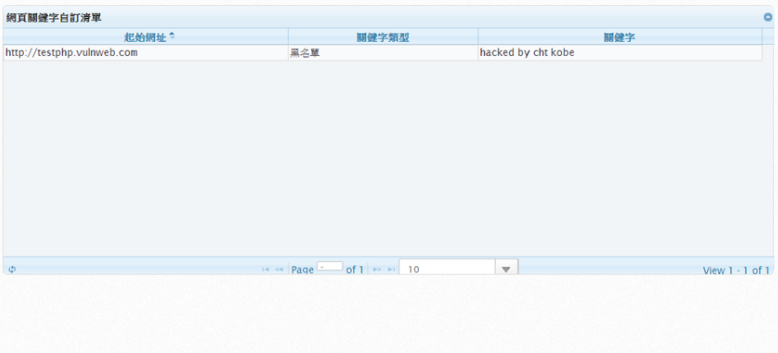
竄改報表下載功能可提供使用者下載在報表檢視頁面所產製的報表，如 Figure 4-16，按下產製報表後，您可至信箱或檢測報表下載頁面得到產製之報表。



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：



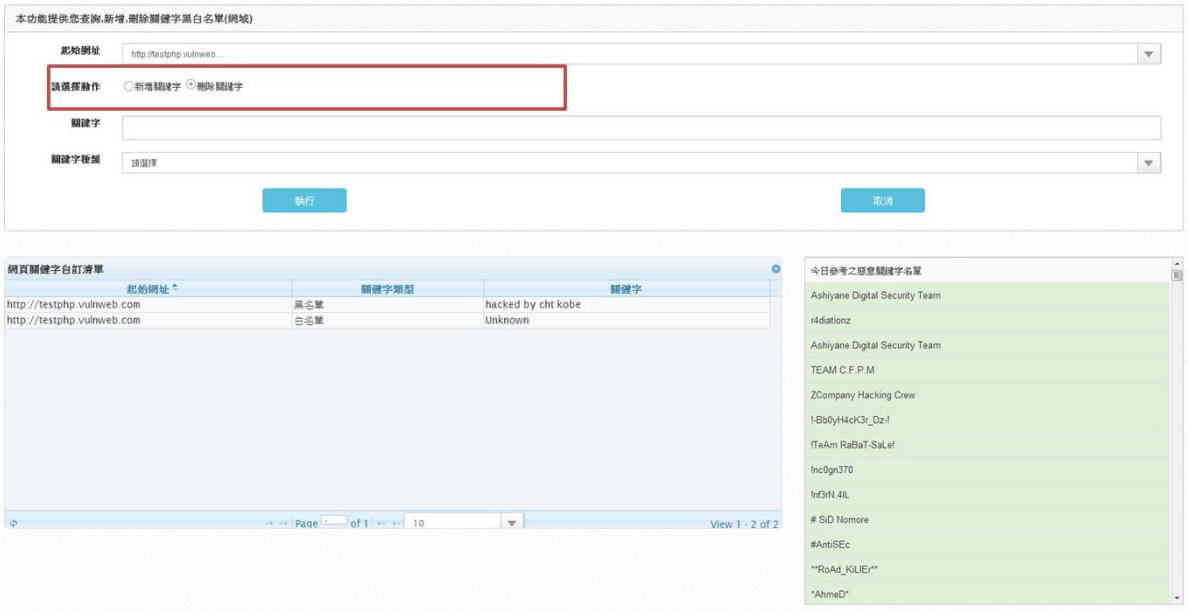
(1) 新增關鍵字

1st.　選擇起始網址以及新增關鍵字，並填妥相關資料(各項

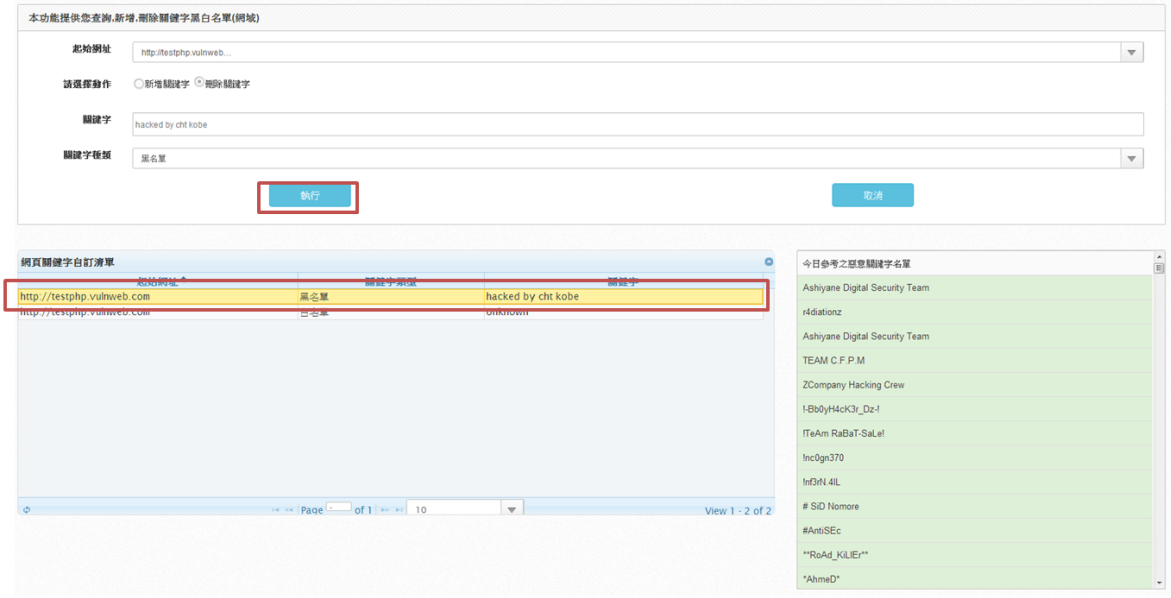
設定說明請參照下方備註)`，按執行後即可完成。

(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)



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。



(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

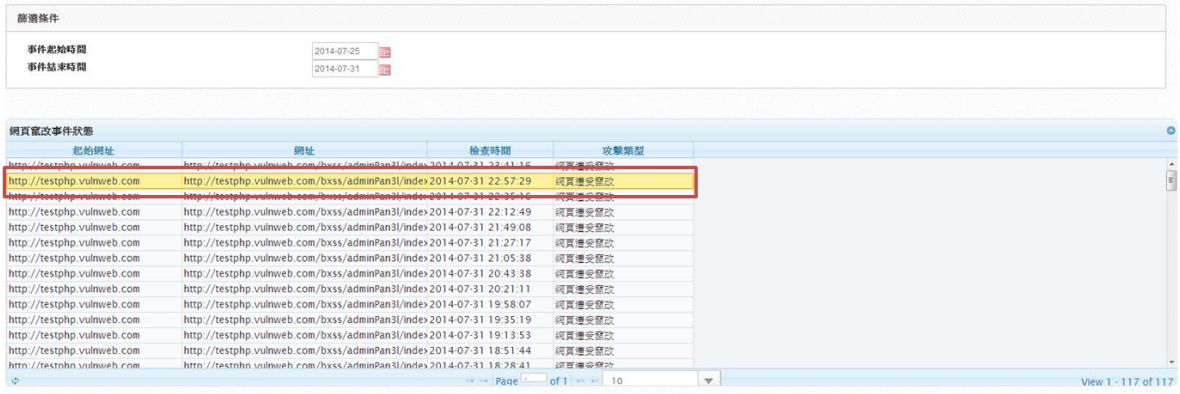
按取消紐可以把正在輸入的值清掉，此時就可以再重新輸入一遍。

e. 竄改事件處理回饋

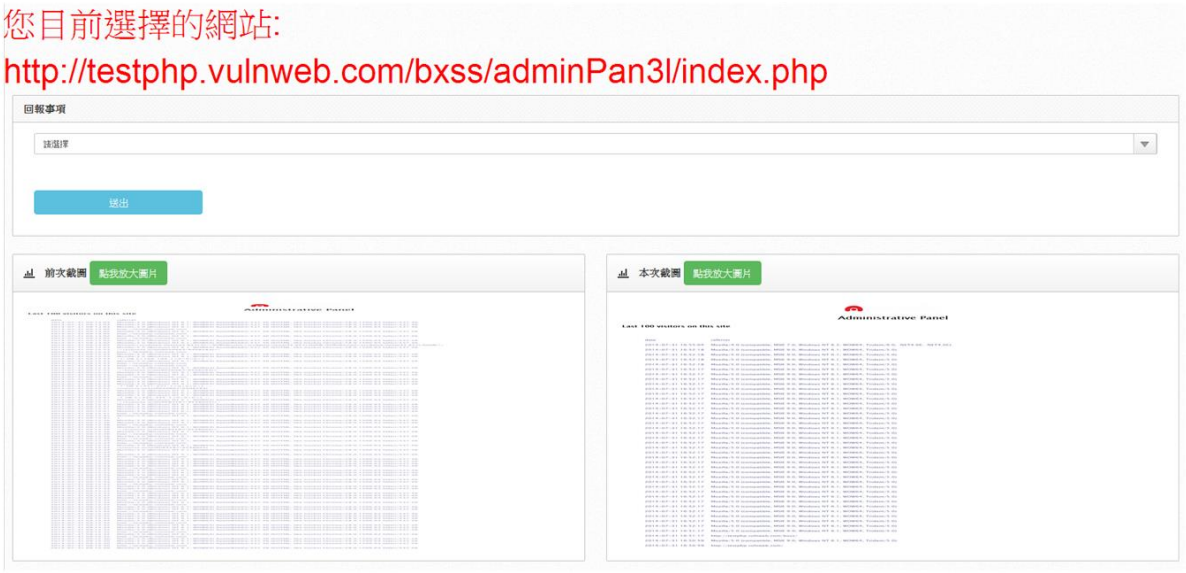
因為竄改和惡意關鍵字檢測有一定的機率會造成誤判的狀況(EX：網頁改版)，所以需要提供回饋機制讓使用者可以回報。本功能提供使用者回報竄改和惡意關鍵字事件的狀態。

(1) 網頁竄改回饋

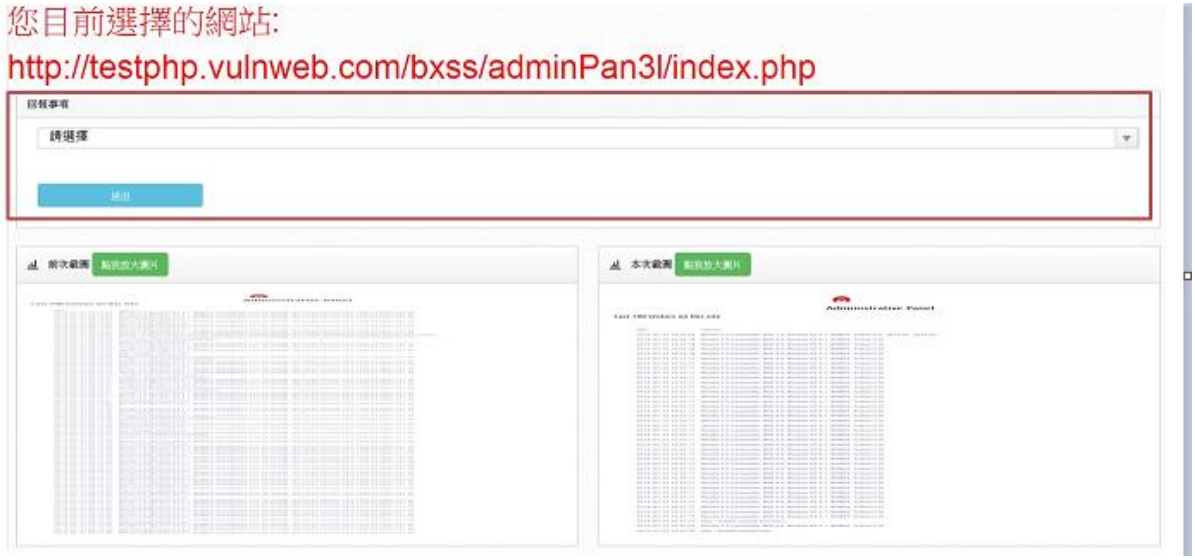
1st.　選擇一個事件並點選(上方可以用日期篩選)



2nd.　點選後，下方會出現比對的網頁截圖

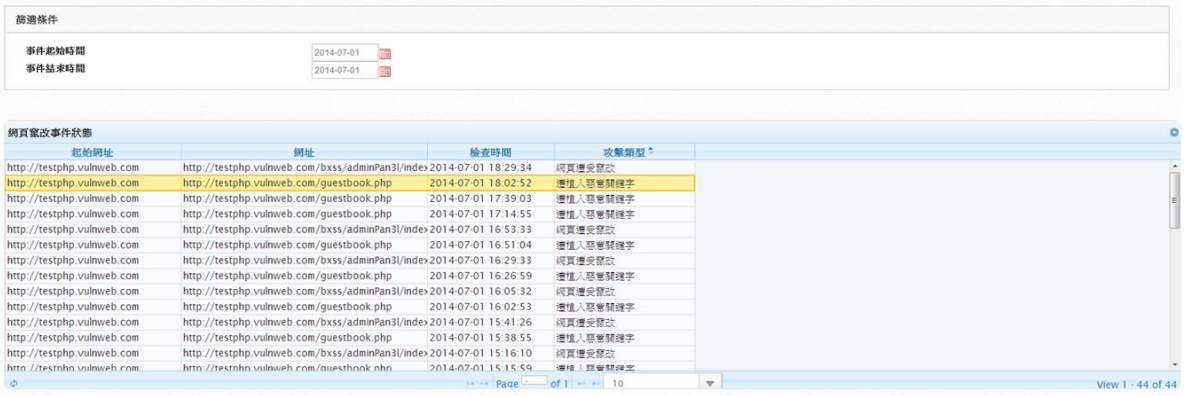


3rd.　在回報事項中選擇回饋訊息後按送出即可(請見備註一)

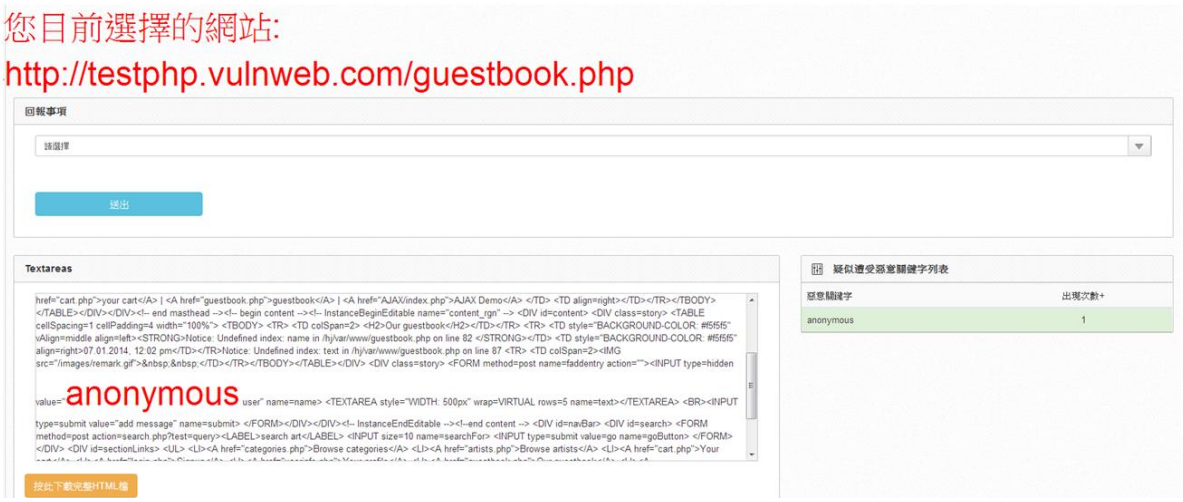


(2) 網頁惡意關鍵字回饋

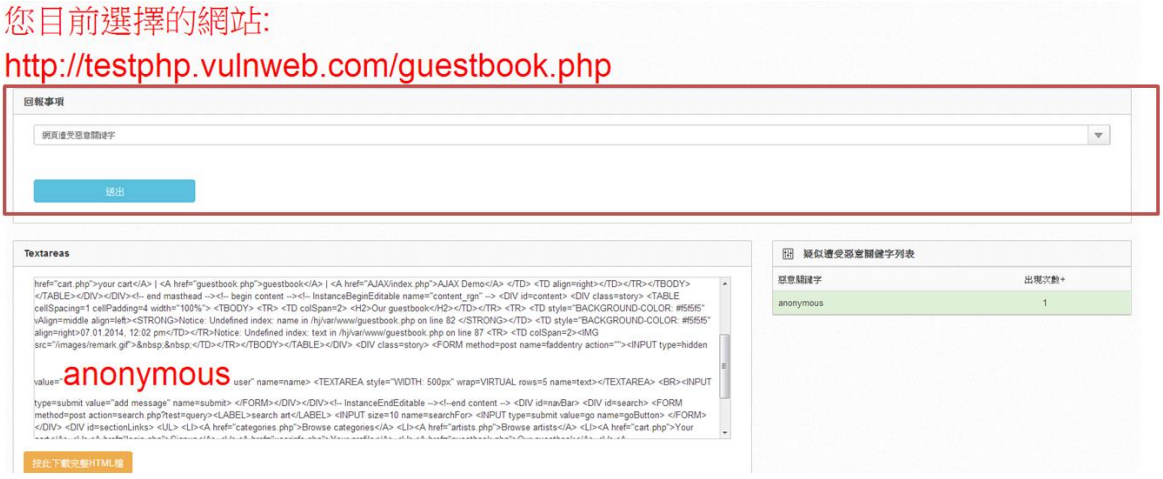
1st.　選擇一個事件並點選(上方可以用日期篩選)



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



3rd.　在回報事項中選擇回饋訊息後按送出即可(請見備註二)



(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

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

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，並提供弱點掃瞄分析報表，可依據建議改善措施，修補弱點，以降低遭受入侵的風險。

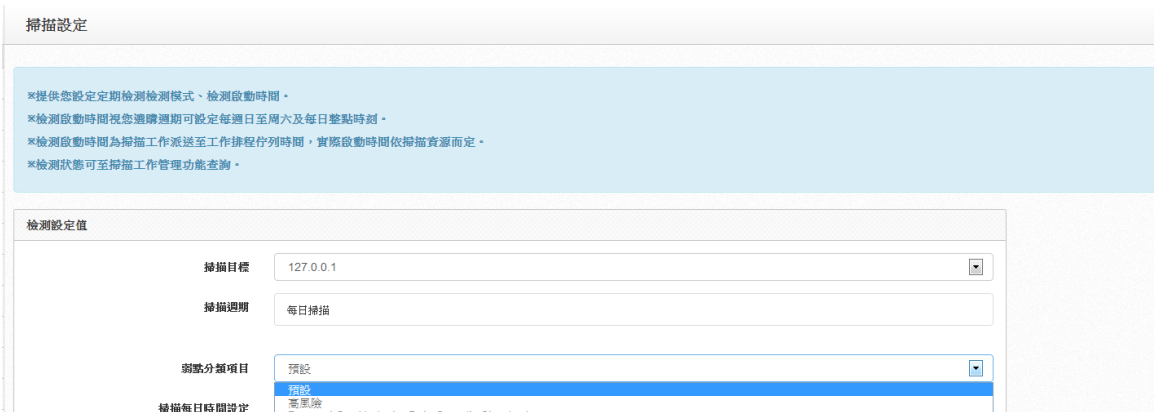
2. 服務功能操作說明

a. 掃描標的設定

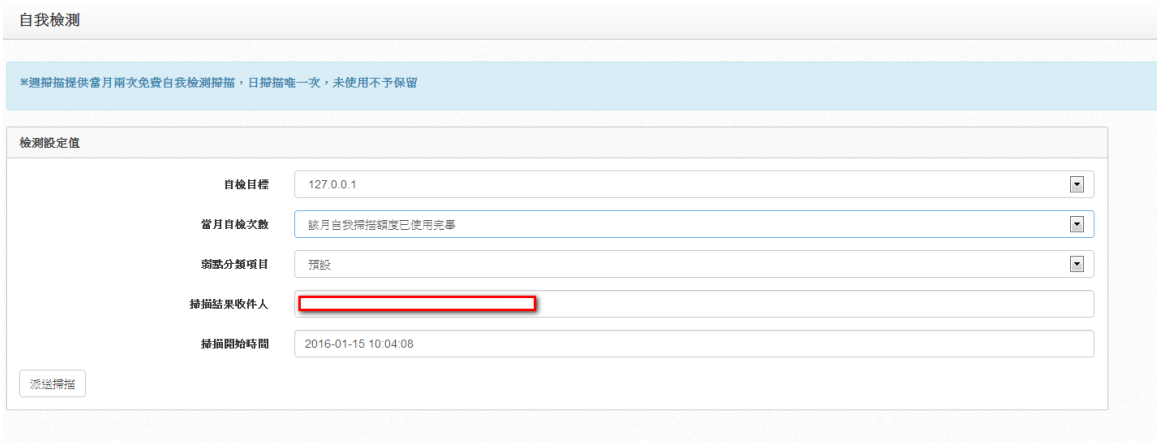
提供用戶更改掃描標的，目前為一個月可以任意更改一次。

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。



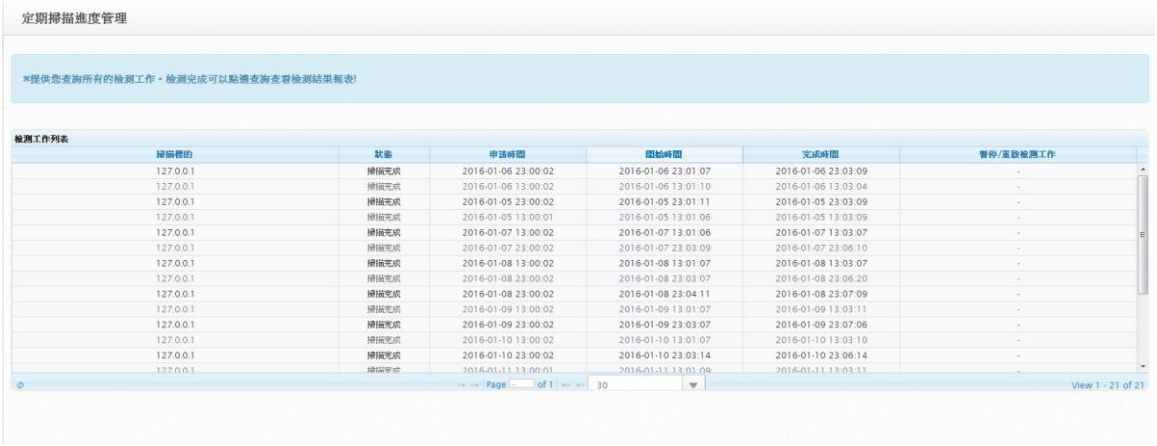
用戶進行掃描標的自我檢測功能，每月依照合約內容提供不同的自我檢測次數，如定期檢測可設定不同掃描分類，也可以設定掃描開始日期。



d. 定期(自我)掃描進度管理

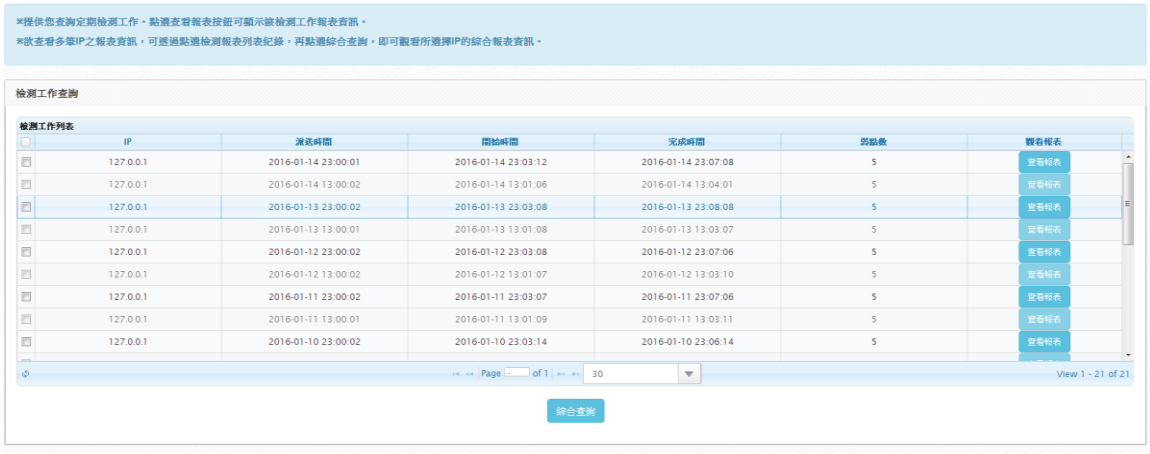
此功能是讓用戶可因其需要針對排程中或掃描中的工作進行暫停檢測或啟動檢測的管理。

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。



e. 定期(自檢)檢測報表查詢

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。



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