拓圖科技

(112 年度第一季初測)

版本號：V1.0

網頁弱點掃描

結果與建議報告

Web Vulnerability Assessment Report

中華資安國際
CHT Security

中華民國 112 年 02 月 21 日

機密等級： □公開 □一般 □敏感 ■機密

文件修訂紀錄

日期	版號	修訂者	覆核者	修訂紀錄
112-02-21	1.0	賴郁仁	林澤宇	正式交付

目錄

圖目錄

表目錄

第一章　執行計畫

第一節　目的

本服務係利用系統自動化工具，結合資訊安全專家（以下簡稱本團隊）之專業知識、資訊安全技術，對於雙方所約定之目標系統進行弱點掃描，並提供客戶專屬測試報告及系統補強建議。

本服務將由本團隊專業的資通安全專家，配合　貴單位需求，從外部或內部環境對受測目標系統進行非破壞性弱點掃描，找出系統潛在風險，並將於測試完成後提供專業之評估報告、改善建議及專業諮詢，協助　貴單位做好各種資通安全防護措施。

第二節　作業規範

(一)貴單位同意、授權且委託本團隊因執行本服務所需，須對貴單位之網際網路資訊系統環境進行測試安全檢測服務。

(二)於本服務中所獲得與蒐集之資訊，僅用來作為本服務執行之發現事項佐證資訊使用，不做其它用途之使用，且採取

適當及必要之保護措施，不得在未經書面授權下洩露予第三者，或供非職務目的加以使用、拷貝、隱藏，並得經貴單位同意及簽訂保密切結書辦理。

(三)其它保密事項之規範，遵循貴我雙方所簽訂之專案合約規範及保密合約。

第三節 執行期間

	作業項目	開始日期	結束日期
執行期間	專案啟動及需求確認	112-02-13	112-02-17
	執行弱點掃描	112-02-21	112-02-21
	提交弱掃結果分析報告	112-02-21	112-02-21
檢測時段	■ 上班時段：星期一至星期五 AM 9:00 開始作業。 非上班時段：星期一至星期五 PM 6:00 開始作業。 夜間時段：星期一至星期五 PM11:00 開始作業。 假日：包含國定假日及星期六、星期日 AM 9:00 開始作業。 特定時段：		

第四節 專案成員

姓名	職稱	聯絡方式

郭耿耀	專案經理	kengyao@chtsecurity.com
賴郁仁	檢測工程師	andylai@chtsecurity.com
以下空白		

第五節　網頁弱點掃描範圍

項次	Domain / URL	用途
1	https://www.esist.org.tw	能源統計專區網站

第二章　執行步驟與項目

第一節　執行方式與流程

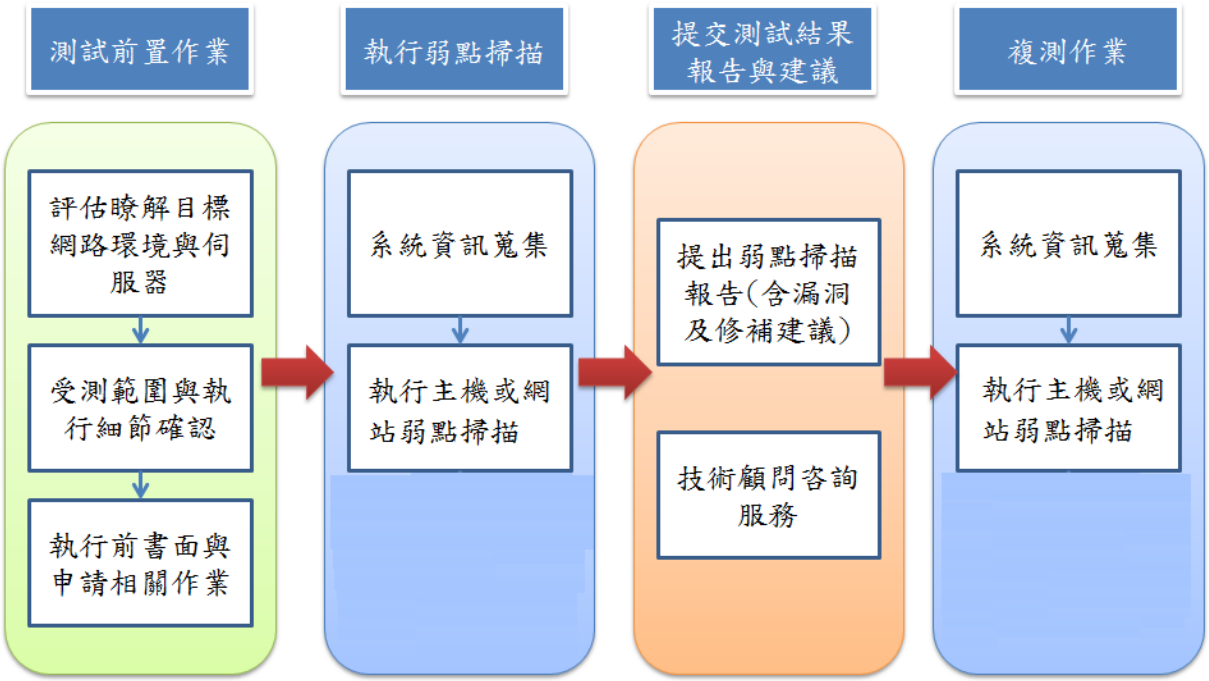

圖- 1 弱點掃描流程圖

一、前置作業

弱點掃描開始前，本團隊將事先與　貴單位承辦人員開會討論各項測試內容，說明整個作業流程，進行潛在風險溝通與需求訪談，以完成下方前置工作：

(1) 定義工作範圍及項目。

(2) 確認測試時程及執行時間。

(3) 參與測試之系統、伺服器及人員數量。

(4) 評估現有網路環境架構以及確認其他特殊需求。

(5) 溝通潛在風險項目，提供檢測前建議安控措施。

(6) 取得正式弱點掃描執行授權。

二、執行弱點掃描

(1) 系統資訊蒐集

透過搜尋引擎及資訊蒐集工具，蒐集客戶的公開資訊、開啟的通訊埠及服務、系統及軟體版本、網站架構等資訊，找出容易成為攻擊標靶的途徑所在。

(2) 執行弱點掃描

根據客戶需求及蒐集資訊進行分析及評估，選擇各種適當之弱點掃描工具進行安全檢測，瞭解系統以及網頁程式的脆弱點所在，尤其針對目前最常發生的網頁及應用程式弱點。

三、提交弱掃結果報告與建議

本團隊將在測試結束後二週內提交中文化「弱點掃描報告」，報告內容包含弱掃所發現之漏洞、風險統計、相關修補與建議措施等。另於　貴單位進行安全強化修補期間，視需求本團隊可協助提供相關技術諮詢服務。

四、**複測作業**

於　貴單位系統及網站管理人員完成安全強化與修補作業後，建議經需求評估後執行弱掃複測作業，以確保弱點及問題確實得到修補與改善。

第二節　檢測工具說明與設定

一、工具簡介

本服務採用 Acunetix 公司出品的 Acunetix Web Vulnerability Scanner，是一套自動化網路應用程式安全檢測商業級軟體，用來掃描 Web 應用程式，檢查駭客可能會利用的各種漏洞。資料庫中有超過 2,000 種駭客常用手法和應用程式弱點檢測規則，可自行訂定檢測項目且符合 OWASP TOP 10 最新版，能夠充分發掘網站的漏洞，具有自動偵測(包括但不限於)以下弱點：

(一)跨網站指令碼攻擊(Cross-site Scripting, XSS)。

(二)SQL 程式碼注入攻擊(SQL injection)。

(三)Google Hacking 資料庫模擬查詢。

(四)程式碼執行。

(五)目錄遍歷漏洞。

(六)檔案引入(Local/Remote File Inclusion)。

(七)網站程式原始碼洩露。

(八)CRLF 注入。

(九)跨頁框指令碼(Cross-Frame Scripting, Clickjacking)。

(十)自動搜尋備份檔或目錄功能。

(十一) 自動搜尋具有敏感性資料的檔案或目錄。

(十二) 自動搜尋常見檔案，如記錄檔、應用程式追蹤等。

(十三) 自動查詢目錄清單功能。

(十四) 搜尋弱點權限之目錄功能，如可新建、編輯或刪除檔案之目錄。

(十五) 具有自動搜尋可用的網站伺服器技術之功能。

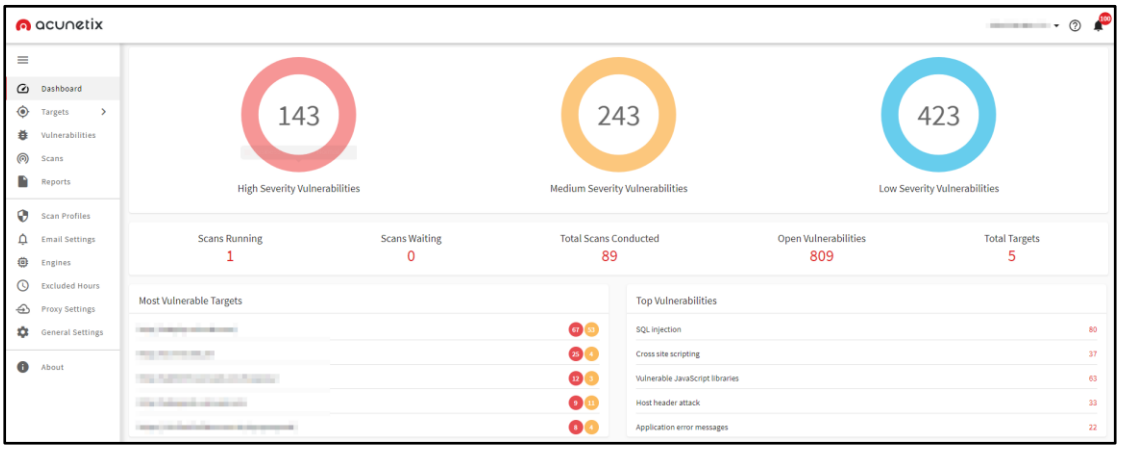

圖- 2 網站應用程式安全掃描軟體─Acunetix 主畫面

二、網站掃描政策設定

掃描政策的設定，結合本團隊資安專家相關檢測經驗，盡可能將掃描期間影響降至最低，下圖為該樣版的掃描政策設定。

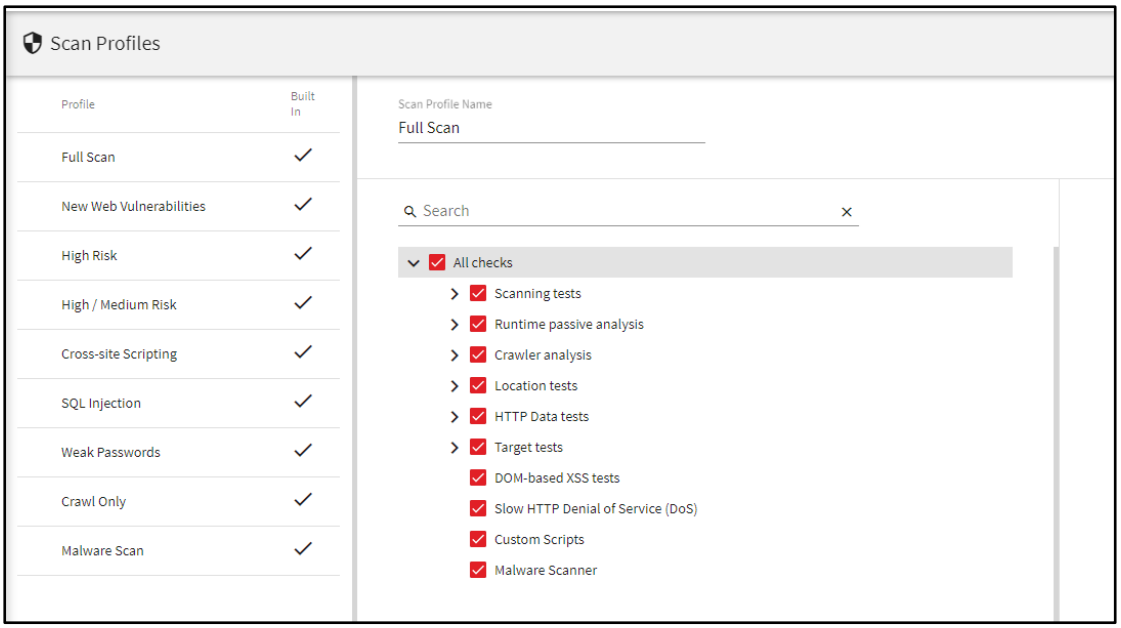

圖- 3 Acunetix Web Vulnerability Scanner 掃描政策設定截圖

三、弱點資料庫更新

為確保服務完整性，於每次初測進行弱點掃描軟體弱點資料庫更新，更新日期如下圖。

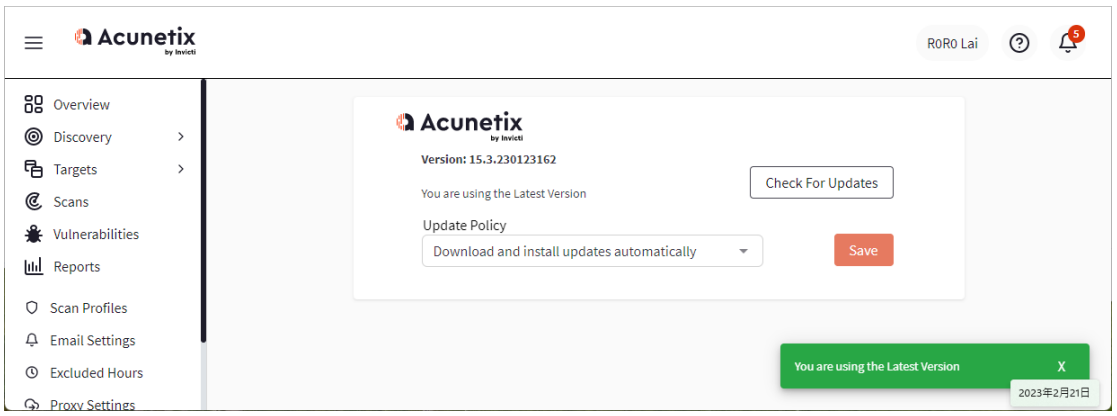

圖- 4 Acunetix Web Vulnerability Scanner 版本更新截圖

第三章　網站應用程式弱點掃描執行結果摘要說明

第一節　網站應用程式弱點分佈情況摘要

下列統計表將列示本次受測目標範圍中，各個受測系統的弱點總數，並分別列出各等級弱點數，使　貴單位主管及系統管理者可透由本表瞭解貴單位的脆弱系統為何。

表- 1 本次掃描結果各等級風險弱點總數量統計表

單位/科別	網站數量	弱點總數	高	中	低
拓圖科技	1	5	0	1	4

一、弱點數嚴重程度分佈狀況

本次檢測　貴單位由弱點數嚴重程度分佈狀況圖表可得知此次掃描弱點總數為 5 個。其中，高風險弱點數為 0 個；中風險弱點數為 1 個；低風險弱點數為 4 個。

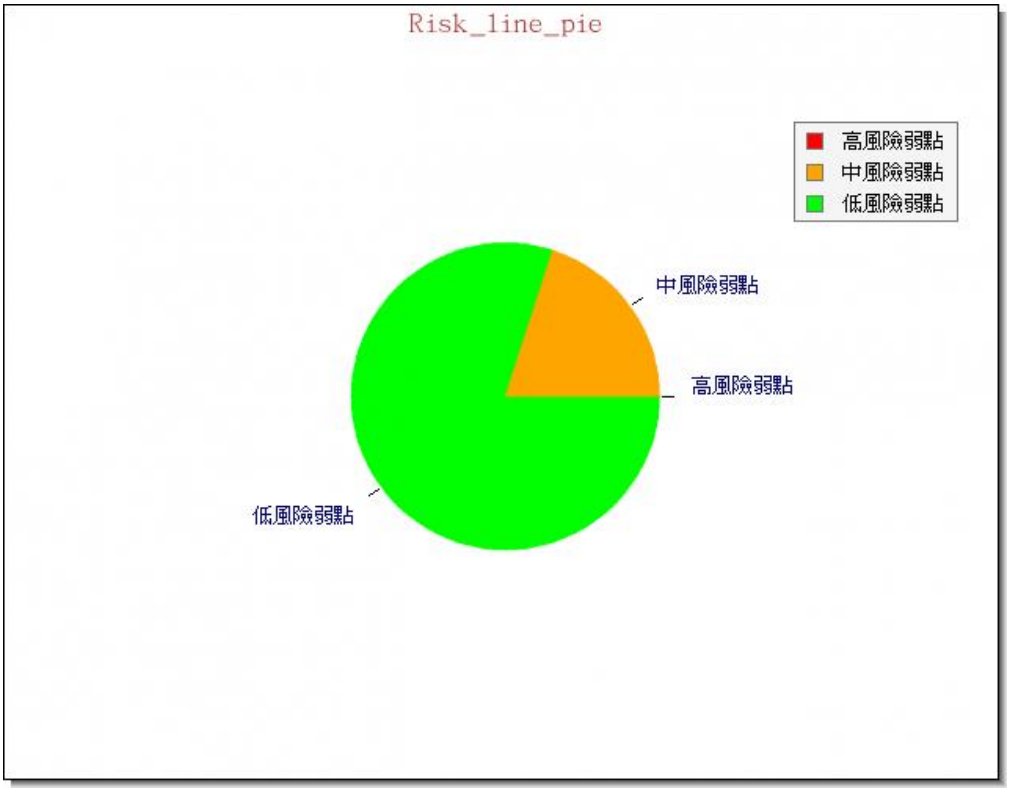

圖- 5 弱點數嚴重程度分佈狀況

表- 2 弱點數嚴重程度分佈狀況

受測範圍	高風險	中風險	低風險	弱點總數
拓圖科技	0	1	4	5

二、前 10 大中高風險弱點說明

貴單位所有網站中，前 10 大中高風險弱點數量統計列表如下，詳細弱點資訊及建議修補方式請參閱附件。

表- 3 前 10 大高風險弱點

高風險弱點名稱	弱點數量
無	無

表- 4 前 10 大中風險弱點

中風險弱點名稱	弱點數量
Vulnerable JavaScript libraries	1

三、網站應用程式風險等級分佈

本次檢測結果發現，本次受測標的中無高風險網站，分佈如下圖。

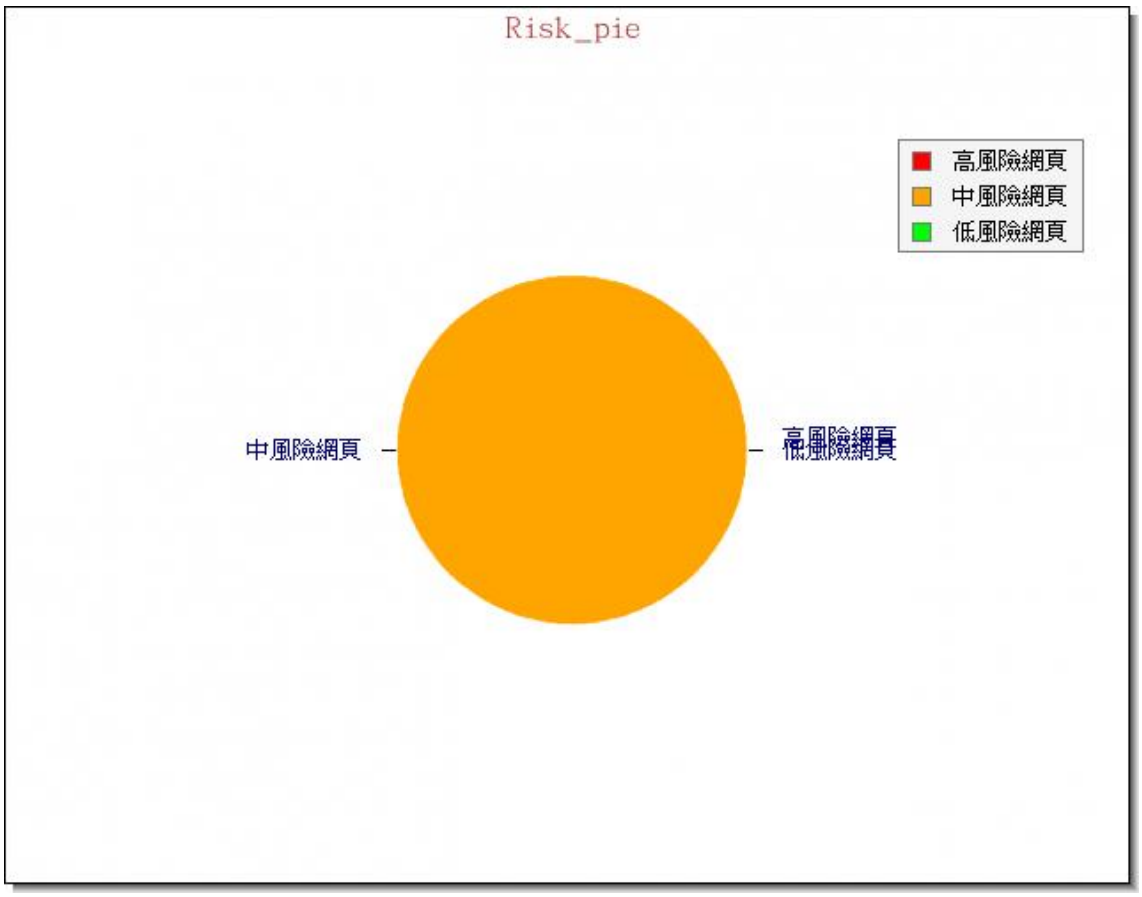

圖- 6 網站應用程式風險等級分佈

表- 5 網站應用程式風險等級分佈

受測範圍	高風險網站	中風險網站	低風險網站	風險網站總數
拓圖科技	0	1	0	1

四、前 10 大風險網站應用程式弱點數量統計

貴單位前 10 大風險網站應用程式弱點依照風險等級以及數量由高至低排序，結果如下表，貴單位可優先聲對該網站應用程式進行修補作業。

表- 6 前 10 大風險網站統計表

索引	主機	URL	伺服器	高	中	低	總計
1	210.65.88.31	www.esist.org.tw	Microsoft-IIS/8.0	0	1	4	5
總計				0	1	4	5

第四章　各網站應用程式與弱點類別詳細清單

第一節　網站應用程式風險等級清單

貴單位網站應用程式展開後依風險等級數量統計排序結果如下表，其中伺服器欄位請參考附錄之說明。

表- 7 風險等級統計表

索引	主機	URL	伺服器	高	中	低	總計
1	210.65.88.31	www.esist.org.tw	Microsoft-IIS/8.0	0	1	4	5
總計				0	1	4	5

第二節　弱點類別清單

貴單位網站應用程式所有弱點依照風險與數量進行統計，結果如下表。

表- 8 高風險弱點類別統計表

索引	高風險弱點名稱	弱點數量
總計		0

表- 9 中風險弱點類別統計表

索引	中風險弱點名稱	弱點數量
1	Vulnerable JavaScript libraries	1
總計		1

表- 10 低風險弱點類別統計表

索引	低風險弱點名稱	弱點數量
1	ASP.NET MVC version disclosure	1
2	HTTP Strict Transport Security (HSTS) not implemented	1
3	Cookies with missing, inconsistent or contradictory properties	1
4	Cookies without Secure flag set	1
總計		4

第三節　網站應用程式風險等級列表

依網站應用程式風險等級將貴單位網站歸類為高度風險、中度風險、低度風險網站並標示出對應部門，供貴單位了解個別網站的整體風險程度，其中伺服器欄位請參考附錄之說明。

表- 11 高風險之網站列表

索引	IP	URL	伺服器
-	-	-	-

表- 12 中風險之網站列表

索引	IP	URL	伺服器
1	210.65.88.31	www.esist.org.tw	Microsoft-IIS/8.0

表- 13 低風險之網站列表

索引	IP	URL	伺服器
-	-	-	-

第五章　結論

資訊安全可以經過系統化的檢測與專家經驗的輔助來降低風險指數，網頁弱點掃描係透過檢視網站/伺服器的回應狀況評估是否有已知的潛在安全性風險，但資訊安全漏洞層出不窮，近幾年惡意程式碼數量與變化更是大幅增加，駭客手法也日新月異，仍需定期執行才能有效地確保安全。

第六章　附件

一、網站弱點清單。

二、網站弱點誤判清單。

三、網站排除弱點清單。

四、網站個別修補建議。

第七章　附錄

網站伺服器判斷方式

本判斷方式係弱點掃描工具於爬站及掃描過程中，藉由伺服器的回應狀況，如回應的標頭、版本資訊、錯誤訊息、預設伺服器頁面以及其他特殊語法的回應方式，**推測**出網站可能性最高的伺服器，由於版本及回應資訊皆可以偽造，或透過資安設備改變內容，偵測結果僅供參考。

中華資安國際
CHT Security

服務據點

台北：100 台北市中正區杭州南路一段 26 號 8 樓
台中：408 台中市南屯區文心路一段 351 號 2 樓
高雄：813 高雄市左營區至聖路 200 號 5 樓 505 室

聯繫電話

02-2343-1628

客服信箱

Service@chtsecurity.com

官方網站

www.chtsecurity.com