**OOOO股份有限公司**

|  |
| --- |
| **網站弱點掃描報告 measurementUrl** |

**保 密 條 款**

本文件內容包含貴單位網站弱點掃描現況與精誠資訊業務營運技術等之機密資訊。依合約規定，視同為機密文件並採取必要之保密措施維持其機密性，雙方並同意，不得洩漏、告知、交付、移轉或以任何方式提供第三人或自行以非合約目的方式，加以使用或利用。

版本資訊

version\_info

**目錄**

壹、 測試目的 6

貳、 測試限制 6

參、 受測範圍與執行時程 7

肆、 測試結果彙整 8

伍、 測試方法說明 13

陸、 風險項目說明及修補建議 18

附錄一 網路安全控制檢測方法論 30

附錄二 風險程度定義說明 31

附錄三 OWASP TOP10 說明 32

附錄四 工具介紹Acunetix Version14 33

表目錄

[表 1受測範圍與執行時程 7](#_Toc113443797)

[表 2網站弱點掃描結果風險數量 8](#_Toc113443798)

[表 3 風險清單 10](#_Toc113443799)

[表 4 OWASP TOP10－2021年對照表 11](#_Toc113443800)

# 測試目的

本報告為OOOO股份有限公司 (以下簡稱　XXXX)委託精誠資訊股份有限公司(以下簡稱精誠資訊)執行之網站弱點掃描服務，精誠資訊初步完成測試後依據測試結果彙整並提出的弱點掃描報告，主要目的在於針對　XXXX指定之特定網站主機模擬外部駭客攻擊行為所進行的弱點掃描。並在測試之後，給予相對應的適當建議。

1. **測試限制**
2. 弱點掃描檢測服務是透過外部網際網路進行弱點揭露以及測試，受測標的可能因為防火牆、入侵偵測等資訊安全設備的保護，而無法完整揭露所有真實存在之風險弱點。
3. 弱點掃描服務過程中，為了不影響受測標的正常運行，在測試的過程中將不會執行任何具有攻擊性的攻擊行為。(例如：服務阻斷攻擊、壓力測試、暴力破解、木馬或後門程式植入)
4. 弱點掃描結果僅代表系統在某個時間點的安全狀態，如果檢測結果未發現任何弱點，也不代表未來在系統上不會有任何其他弱點遭到揭露及利用。
5. **受測範圍與執行時程**

本次受測範圍與執行時程如下表所示：

表 1受測範圍與執行時程

docMeasurementRange

1. **測試結果彙整**
2. 網站黑箱弱點掃描結果摘要

本次測試範圍為　XXXX所指定之網站名稱，在預定的時間內，由測試人員針對測試範圍所有主機，透過模擬駭客之攻擊手法完成網站弱點掃描。

本次測試過程中，所發現的風險數共有totalRiskCnt個。

其中包含高風險highRiskCnt個、中風險midRiskCnt個、低風險lowRiskCnt個以及資訊風險infoRiskCnt個，整體而言，主機對外網路安全性並無重大問題，建議落實持續改善即可。

表 2網站弱點掃描結果風險數量

docRiskCntList

1. 風險等級說明

**高風險( High Risk )**：弱點若被利用可能讓不具經驗的攻擊者直接取得管理者權限，導致系統中斷、拒絕服務攻擊、執行命令、敏感資訊的揭露…等。

**中風險( Medium Risk )** ：弱點若被利用可能讓稍有經驗的攻擊者直接取得非管理者層級權限，但攻擊者可利用進一步的Hacking技術來取得管理者權限。

**低風險( Low Risk )** ：弱點若被利用可能讓具有經驗的攻擊者間接取得一般等級使用者存取權。

**資訊風險( Information Risk )** ：此類弱點僅揭露不具價值的資訊，或是根本無法被利用來攻擊。

1. 風險清單

表 3 風險清單

docRiskList

1. OWASP Top 10 – 2021年版本對照表

此規範檢測是測試measurementUrl網站上可以被發現的測試結果，對照OWASP TOP 10 – 2021年版本所提供的合規性項目：

表 4 OWASP TOP10－2021年對照表

docOwaspList

1. **測試方法說明**

　　針對本次弱點掃描結果，在風險的部份以docOwaspRisk為主要問題，為OWASP所定義的十大風險範疇。建議應立即採取矯正及修補措施，相關修補方法可以參考本報告中的弱點修補建議。

1. 黑箱弱點掃描方法說明  
   　　利用搜集來的資訊集中測試，並透過特定的攻擊程式（Exploits）和攻擊手法驗證弱點有效性。建立可視之滲透成功證據。測試手法包含web弱點掃描、人工驗證結果。所有手法皆依循OWASP定義之網站十大風險之範疇。

* **Cross-Site Scripting：**中譯為跨站腳本攻擊。Web應用程式直接將來自使用者的執行請求送回瀏覽器執行，使得攻擊者可擷取使用者的Cookie或Session資料而能直接用使用者身分登入。
* **Injection Flaws：**中譯為注入弱點攻擊。Web應用程式執行來自外部包括資料庫在內的惡意指令，包含SQL Injection和 Command Injection等。
* **Insecure Direct Object Reference：**中譯為不安全的物件參考。攻擊者利用Web應用程式本身的檔案讀取功能，得任意存取檔案或重要資料。
* **Cross-Site Request Forgery (CSRF)：**中譯為跨網站的偽造請求。已登入Web應用程式的合法使用者執行到惡意的HTTP指令，但Web應用程式卻當成合法需求處理，使得惡意指令被正常執行。
* **Information Leakage and Improper Error Handling：**中譯為程式碼錯誤訊息外漏。當Web應用程式執行錯誤時，會將程式碼之錯誤訊息暴露在網頁上，使得有心人士可利用不同的錯誤訊息進行資料收集。
* **Broken Authentication and Session Management：**中譯為身分驗證功能缺失。Web應用程式中自行撰寫的身份驗證相關功能有缺陷。
* **Insecure Cryptographic Storage：**中譯為未加密的儲存設備。Web應用程式沒有對敏感性資料使用加密、使用較弱的加密演算法或將金鑰儲存於容易被取得之處。
* **Insecure Communication：**中譯為未加密的網路連線。沒有在傳送敏感性資料時使用HTTPS或其他加密方式。
* **Failure to Restrict URL Access：**中譯為無權限的控制。某些網頁因為沒有權限控制，使得攻擊者可透過網址直接存取。

1. 其他綜合攻擊  
   　　所有手法皆依循OWASP(Open Web Application Security Project, http://www.owasp.org)定義之網站十大風險之範疇，內容包含：

* **A1.** **權限控制失效(Broken Access Control)：**權限控制失效是指訪問控制策略未能將帳號限制設定為預期的權限，容易讓駭客透過這項漏洞，進入企業中查看、修改、洩露、刪除其他帳號和管理員的資料，或是修改帳號和權限，甚至將惡意軟體安裝到系統中。
* **A2. 加密機制失效(Cryptographic Failures) ：**問題核心定義在加密機制的失敗，並且因此而造成敏感性資料外洩或是系統被破壞。此外，它還表示為密碼保護不再足夠，並且預設情況下應該對所有包含敏感訊息的資料庫應用加密。
* **A3. 注入式攻擊(Injection)：**在注入式攻擊中，駭客將惡意程式碼注入系統以啟動未經授權的命令來取得敏感資料。注入式攻擊的列表很長，包括 SQL 注入、跨站點腳本 (XSS)、模板注入、XPath 注入、電子郵件標頭注入、shell 注入等。
* **A4. 不安全設計(Insecure Design)：**與應用程式設計缺陷相關的風險；不一定是設計錯誤，而只是有心人士可利用了能造成損害的漏洞。
* **A5. 安全設定缺陷(Security Misconfiguration)：**安全設定缺陷最常見原因是系統管理員沒有更改預設配置，或者他們在打開系統進行測試後忘記重新關閉系統。
* **A6.危險或過舊的元件(Vulnerable and Outdated Components)：**網路中的元件包含了未修補已知漏洞的情況，通常是過時且不受支援的作業系統、應用程式、Web 應用程式伺服器、API 和資料庫管理系統 (DBMS) 。
* **A7.認證及驗證機制失效(Identification and Authentication Failures)：**越來越多企業組織採用多因素身份驗證 (MFA) 以及行動 OTP 和生物識別等高級身份驗證技術，這些技術都有助防禦社交攻擊、憑證填充和暴力攻擊。
* **A8.軟體及資料完整性失效(Software and Data Integrity Failures)：**由於缺乏資料完整性驗證過程而使用篡改或損壞的資料做出某些決定的狀況。
* **A9.資安紀錄及監控失效(Security Logging and Monitoring Failures)：**之前名稱為記錄與監控不足風險，資安紀錄及監控失效描述了入侵監控和report系統未能捕獲和寫入駭客入侵的跡象。這可能是因為某些資安事件未記錄或日誌僅儲存在本地，或者警報值不足。如果沒有足夠的report報告，資料洩露可能會在數月或數年內未被發現。

1. **A10. 伺服器請求偽造(Server-Side Request Forgery, SSRF)：**當網頁應用程式正在取得遠端資源，卻未驗證由使用者提供的網址，此時就會發生偽造伺服端請求。即便有防火牆、VPN或其他網路ACL保護的情況下，攻擊者仍得以強迫網頁應用程式發送一個經過捏造的請求給一個非預期的目的端。這些損壞的請求可能會導致資料洩露。隨著雲端服務和雲端結構的複雜性，SSRF 攻擊的嚴重性將會愈來愈嚴峻。
2. 其他檢測項目包含：

* DNS檢測Zone Transfer的可能性
* FTP站測試連線、匿名登入及字典測試
* Windows主機測試簡單密碼及相關列舉
* 檔案分享檢測

1. **風險項目說明及修補建議**

* **docRiskDescribe**

**\*附註：此網站掃描細節可參閱網頁開發者報告.pdf**

# 附錄一 網路安全控制檢測方法論

網路安全評估方法主要是以概略性的掃描偵測方式，來發現網路及系統安全性弱點，不包含實際的滲透存取測試。

## Step 1：Scoping

第一步驟的目的是先釐清進行評估所受檢測的範圍，本專案選定將進行評估的範圍包括：內部網路環境、外部網路環境、網站服務應用伺服器、路由器及防火牆設備配置（包含異地備援環境）。

## Step 2：Fingerprinting

第二步驟的目的是要對網路上存在的伺服器及系統做初步的判定，由於不同的作業平台及應用系統會存在其個別的系統特性及安全性弱點，是以做系統初步判定以便支援進行。

## Step 3：Plug-in

這一步驟是根據前一步驟之結果來選擇適當的弱點掃描工具，以達到更有效率的弱點列舉掃描及避免造成系統的傷害。

## Step 4：Identify

根據所選擇的工具實地進行掃描，將產出的結果報告逐一分析比對，並整理出掃描報告的結果，並列舉個別存在的安全弱點。

## Step 5：Verify

延續前一步驟中整理出的弱點結果逐一實際人工比對驗證，以過濾掃描工具掃描產出結果是否誤判，以維持產出每一個結果的正確性。

# 附錄二 風險程度定義說明

為提供檢視報告時，對所發現的弱點能有具體的認知，將檢測中找到的弱點給予量化的危機等級，其中危機等級根據下列三個因素來劃分：

## 程度－程度與安全漏洞是相輔相成的。如果攻擊者可以取得完整的系統控制權，那危機評等就會比較高。

## 成果－成果是評量攻擊者嘗試利用漏洞攻擊所需要的知識（如技能程度、網路地點、目標系統的熟悉度等），越複雜的攻擊條件會降低危險性。但是遇到高手時，就算系統有著複雜的攻擊條件，危險性仍然很高。

## 影響－損壞程度是根據系統或網路受攻擊後的結果來判定。

風險＝程度＊（１／成果）＊影響

此評等定義是主觀的，主要依據弱點被攻擊者利用的程度，依照過往的經驗、知識和認知來定義。

# 附錄三 OWASP TOP10 說明

開放網路軟體安全計畫，簡稱 OWASP （Open Web Application Security Project）是一個開放社群、非營利性組織，其主要目標是研議協助解決網路軟體安全之標準、工具與技術文件，長期致力於協助政府或企業瞭解並改善應用程式的安全性。美國聯邦貿易委員會（FTC）更強烈建議所有企業務必遵循 OWASP 所發佈的十大網路弱點防護守則，美國國防部亦將此守則列為最佳實務，就連國際信用卡資料安全技術 PCI 標準更將其列為必要元件。

OWASP Top10 主要目的，是將最常見的網路應用系統安全弱點，教育開發者（Developers）、設計者（Designers）、架構師（Architects）和組織（Organizations），提供基本的方法保護防止這些弱點，是軟體開發安全計劃最好的開始。

# 附錄四 工具介紹Acunetix Version14

1. 自動化針對客戶端產生腳本分析程式，能夠對AJAX和Web2.0應用程式進行安全測試
2. SQL Injection和跨網站腳本測試
3. 使用Windows Defender或在Linux上使用ClamAV進行惡意軟件掃描(Web Application上發現腳本，下載腳本並在本地對其進行掃描)
4. 革命性的SmartScan引擎：在掃描的前20％中發現多達80％的漏洞；速度及準確度更佳
5. 證明DeepScan上關於Angular，Vue , React, 系統整合功能(包括GitLab，Bugzilla和Mantis)等等的漏洞。
6. 圖像化總體紀錄程式可輕鬆測試Web表單和受密碼保護的區域
7. 支援CAPTHCA的網頁，單方面指令和雙因素(Two Factor)驗證機制
8. 多樣化的報告功能，包括ISO27001、OWASP報告；且單擊漏洞時，漏洞警報詳細信息將在同一頁面的側面打開。這使您可以檢查漏洞警報詳細信息，而不會丟失Acunetix識別的其他漏洞。
9. 高速的多執行緒掃描程式，快速檢索成千上萬個網頁
10. 智慧抓取程式檢測Web伺服器類型和應用程式語言
11. Acunetix搜尋、分析網站，包括Flash內容、SOAP和AJAX
12. 匯出網站漏洞報告

==========文件結尾==========