|  |
| --- |
| **{{ company\_name }}**  **{{ project\_name }}**  **{{ report\_name }}** |

**文件編號：{{ file\_no }}**

**V1.0版**

**{{ date\_ch }}**

**安碁資訊股份有限公司**

**文件制／修訂記錄**

| **版次** | **日期** | **說明** | **作者** | **修訂中** | **定稿** |
| --- | --- | --- | --- | --- | --- |
| 1.0 | {{ date\_dot }} | Auto | 系統 |  | V |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**【目　　錄】**

[壹、 關於本報告 1](#_Toc192691780)

[一、 報告說明 1](#_Toc192691781)

[二、 盡責聲明 1](#_Toc192691782)

[貳、 檢測作業 2](#_Toc192691783)

[一、 檢測目標 2](#_Toc192691784)

[二、 檢測時間 2](#_Toc192691785)

[三、 檢測方式 3](#_Toc192691786)

[（一） 網頁攀爬 3](#_Toc192691787)

[（二） 網站架構深度分析 3](#_Toc192691788)

[（三） 產出弱點檢測報告與修正建議 3](#_Toc192691789)

[四、 檢測來源IP 3](#_Toc192691790)

[五、 檢測工具 4](#_Toc192691791)

[參、 檢測結果 5](#_Toc192691792)

[一、 弱點摘要 5](#_Toc192691793)

[二、 弱點手動檢核驗證 9](#_Toc192691794)

[（一） https://www.air-go.com.tw 9](#_Toc192691795)

[肆、 弱點說明與修正建議 10](#_Toc192691796)

[一、 10](#_Toc192691797)

[（一） 10](#_Toc192691798)

**【圖 目 錄】**

[圖1 Appscan檢測工具版本畫面 4](#_Toc167927118)

[圖2 jQuery相關弱點手動檢核 7](#_Toc167927119)

[圖3 Cookie屬性弱點手動檢核 8](#_Toc167927120)

[圖4 不安全的第三方鏈結弱點手動檢核 8](#_Toc167927121)

[圖5 SSL相關弱點手動檢核 9](#_Toc167927122)

[圖6 漏洞元件弱點手動檢核-1 10](#_Toc167927123)

[圖7 漏洞元件弱點手動檢核-2 10](#_Toc167927124)

[圖8 SRI（子資源完整性）支援弱點手動檢核 11](#_Toc167927125)

[圖9 Cookie屬性弱點手動檢核 12](#_Toc167927126)

[圖10 SSL相關弱點手動檢核 13](#_Toc167927127)

[圖11 SRI（子資源完整性）支援弱點手動檢核 13](#_Toc167927128)

[圖12 Cookie屬性弱點手動檢核 14](#_Toc167927129)

[圖13 SSL相關弱點手動檢核 15](#_Toc167927130)

[圖14 SRI（子資源完整性）支援弱點手動檢核 15](#_Toc167927131)

**【表 目 錄】**

[表1 檢測目標列表 2](#_Toc167927132)

[表2 弱點檢測分析報告 5](#_Toc167927133)

# 關於本報告

## 報告說明

網站弱點掃描（Web Vulnerability Assessment）是一種評估網站安全性的技術。本報告為安碁資訊股份有限公司承接{{ company\_name }}（下稱 貴公司）「{{ project\_name }}」（以下稱本案），依貴我雙方約定之作業範圍，透過自動化工具和手工驗證的方式執行網站弱點掃描，挖掘網站可能存在的漏洞後，就本次作業所見之項目進行說明陳述，提供相關優化、精進之資安防護機制之建議，供 貴公司做為後續防護規劃之依循參考。

## 盡責聲明

自動化工具可以快速發現大量網站漏洞，並透過手工驗證漏洞來提高準確度，減少誤報率。網站弱點掃描並無法找出全部的網站漏洞，當攻擊者試圖利用邏輯性漏洞進行攻擊、或是有了全新的攻擊手法出現，都會使得網站的安全性降低。唯有透過定期地進行網站弱點掃描，才能確保網站的安全性足夠抵禦外來的惡意攻擊。

本報告所使用之分析與檢測手法，為當前資訊安全產業所通用之技術與工具，本公司謹盡合理可能之最大努力，就所見所聞如實提出本報告，容或有不足之處，仍請考量當前科技所能達成之極限，予以諒解。

# 檢測作業

## 檢測目標

網站掃描範圍以 貴單位提供掃描的弱點目標為主，檢測網站如下表。

1. 檢測目標列表

| **編號** | **目標** | **掃描時間** |
| --- | --- | --- |
| {%tr for row in web\_goal\_lists %} | | |
| {{loop.index }} | {{ row.web\_url}} | {{ row.start\_time }} |
| {%tr endfor %} | | |

## 檢測時間

檢測時間自{{ date\_start }}至{{ date\_end }}止。在執行階段，在執行階段，除了 貴單位有提出特別排除的測試時間限制，否則原則上一天24小時任何時段均可進行。

## 檢測方式

由外部連線方式執行網站安全檢測程序，如為到府作業則由本公司工程師攜帶掃描機器至 貴單位，對 貴單位測試標的以內網方式連線進行檢測，檢測方式與流程說明如下：

### 網頁攀爬

將測試標的所屬網站目錄進行全面性的網頁攀爬與URL、路徑紀錄等。

### 網站架構深度分析

對網頁攀爬所記錄之網站程式與路徑，進行網站架構、網頁應用程式的安全測試及分析。

### 產出弱點檢測報告與修正建議

## 檢測來源IP

* {{ scanner\_ip }}

## 檢測工具

本次網站安全檢測將採用國際知名的Appscan檢測軟體進行掃描，透過掃描可檢測網站主機之各式安全性問題與弱點。為避免影響　貴單位網站服務正常，測試過程中不會採用任何植入性或破壞性測試。

Appscan檢測工具使用版本如下圖：

|  |
| --- |
| {{ appscan\_version\_image }} |

1. Appscan檢測工具版本畫面

主要檢測項目如下：

* 整體網站架構檢測。
* Web Application安全檢測，如：SQL Injection、Cross Site Scripting等弱點項目檢測。
* CGI程式存取權限檢查（如：GET、PUT、DELETE）。
* 網頁程式碼檢測與分析，依據不同程式碼PHP、JSP、ASP等，進行相對應的弱點測試與檢查。
* OWASP TOP 10 2021弱點檢核項目。

# 檢測結果

## 弱點摘要

本次網站弱點掃描結果共有 {{ number\_total\_web }} 個弱點總數，其中有 {{ count\_C\_web\_total }} 個嚴重風險弱點，{{ web\_summary }}弱點等級及數量如下圖。

|  |
| --- |
| {{ img\_web\_count\_image }} |

1. 風險等級弱點數目及總和

表列等級分為嚴重、高、中（Critical / High / Medium）等三級，建議立即安排修補與進一步確認。其餘低風險弱點請參閱附件說明。

1. 弱點檢測分析報告

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 編號 | 目標網站 | 弱點名稱 | 弱點描述 | 弱點等級 | 弱點總數 | 弱點數量 | | |
| **C** | **H** | **M** |
| {%tr for cause in web\_causes %} | | | | | | | | |
| {%tr for cc in cause.web\_causes\_need\_dict %} | | | | | | | | |
| {% vm %}{{ cause.num\_web }} | {% vm %}{{ cause.information\_web\_url}} | {{ cc.name }} | {{ cc.cause}} | {{ cc.severity }} | {{ cc. amount}} | {% vm %}{{ cause.count\_C\_web }} | {% vm %}{{ cause.count\_H\_web }} | {% vm %}{{ cause.count\_M\_web }} |
| {%tr endfor %} | | | | | | | | |
| {%tr endfor %} | | | | | | | | |
| **總計** | | | | | | **{{ count\_C\_web\_total }}** | **{{ count\_H\_web\_total }}** | **{{ count\_M\_web\_total }}** |

## 弱點手動檢核驗證

本次檢測針對網掃工具檢核出弱點等級嚴重、高、中以上分類的弱點進行手動驗證作業，以確認工具掃描出的弱點確實存在。

### https://www.air-go.com.tw

#### jQuery 上的跨網站 Scripting (CVE-2020-11022)

* 弱點等級：中

#### jQuery 上的跨網站 Scripting (CVE-2020-11023)

* 一張含有 文字, 螢幕擷取畫面 的圖片

  自動產生的描述弱點等級：中

1. jQuery相關弱點手動檢核

# 弱點說明與修正建議{% for row in web\_causes %}

## {{ row.information\_web\_url }}{% for cause in row.web\_causes\_explanation\_dict%}

### {{ cause.name }}

#### 弱點原因

{{ cause.risk | safe }}

#### 弱點說明

{{ cause.solution\_description | safe }}

#### 修補建議

{{ cause.solution\_suggest | safe }}

{%- endfor %}

{% endfor %}