|  |
| --- |
| **p\_userName**  **p\_projectName**  **p\_reportName\_p\_period** |

**文件編號：p\_reportCode\_p\_period**

**V1.0版**

**109年10月09日**

**安碁資訊股份有限公司 謹呈**

**文件制／修訂記錄**

| **版次** | **日期** | **說明** | **作者** | **修訂中** | **定稿** |
| --- | --- | --- | --- | --- | --- |
| 1.0 | 109.10.09 | 定稿 | 黃騰澔 |  | V |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**【目　　錄】**

[壹、 前言 5](#_Toc53503497)

[一、 目的 5](#_Toc53503498)

[二、 範圍 5](#_Toc53503499)

[貳、 檢測作業 7](#_Toc53503500)

[一、 檢測時間 7](#_Toc53503501)

[二、 檢測方式 7](#_Toc53503502)

[（一） 網頁攀爬 7](#_Toc53503503)

[（二） 網站架構深度分析 7](#_Toc53503504)

[（三） 產出弱點檢測報告與修正建議 7](#_Toc53503505)

[三、 檢測工具 7](#_Toc53503506)

[參、 檢測結果 9](#_Toc53503507)

[一、 弱點摘要說明 9](#_Toc53503508)

[二、 弱點分析（弱點描述） 10](#_Toc53503509)

[（一） SQL注入 10](#_Toc53503510)

[三、 弱點手動檢核 10](#_Toc53503511)

[（一） SQL注入 10](#_Toc53503512)

[肆、 安全強化建議（修補方式） 13](#_Toc53503513)

[一、 SQL 注入弱點修補建議 13](#_Toc53503514)

[（一） 防止SQL Injection的原則 13](#_Toc53503515)

**【表 目 錄】**

[表1 URL / IP List 5](#_Toc53503516)

[表2 弱點檢測分析報告 9](#_Toc53503517)

**【圖 目 錄】**

[圖1 SQL注入弱點手動檢核之一 10](#_Toc53503518)

[圖2 SQL注入弱點手動檢核之二 11](#_Toc53503519)

[圖3 SQL注入弱點手動檢核之三 12](#_Toc53503520)

[圖4 SQL注入弱點手動檢核之四 12](#_Toc53503521)

# 前言

## 目的

目前網路犯罪越來越普遍，政府機關防制駭客入侵、防止機密資料外洩及機關網頁竄改是刻不容緩工作。網站系統（Web Server）的弱點攻擊是目前最常見及最容易成功的攻擊手法，除網站系統本身的安全弱點之外，因應網站需求而開發的AP應用程式及網頁程式碼如PHP、ASP、JSP…等，都是被攻擊的主要目標之一，使用的攻擊手法不外乎SQL Injection、Cross Site Scripting（XSS）..等，電腦駭客往往都能透過網頁程式碼設計上的缺陷，進行破壞性的入侵行為，如刪除破壞資料、植入木馬、竄改檔案及網頁、竊取機密資料等，往往造成企業主及機關單位的重大損失。

為提高 貴單位重要網站系統（Web Server）的安全防護，本公司將定期配合 貴單位弱點掃描時程，協同進行網站系統弱點檢測服務並提供檢測報告，以協助評估 貴單位網站系統的風險層級，以及早發現弱點及早處理。本文件即在說明本次，本公司對 貴單位執行網站弱點檢測之成果及相關說明。

## 範圍

網站掃描範圍以 貴單位提供掃描的弱點主機為主，檢測網站總數為147個URL，弱點數量僅以高/中風險（High/Medium）部分呈現，如表1所列。

1. URL / IP List

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序號 | URL/IP | 網站名稱 | 弱點數量 | |
| **H** | **M** |
| 1 | https://fido.moi.gov.tw:443/ | FIDO-行動身分識別系統（東七） | 0 | 0 |
| 2 | https://www.cpu.edu.tw | 中央警察大學全球資訊網 | 0 | 0 |

# 檢測作業

## 檢測時間

檢測期間為109年08月17日至09月18日。

## 檢測方式

由本公司位於龍潭SOC之弱點檢測主機，對 貴單位測試標的發起遠端（Remote）網站安全檢測程序，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

## 檢測工具

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 貴單位正常網站服務，測試過程中不會採用任何植入性或破壞性測試。

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 2017弱點檢核項目。

# 檢測結果

## 弱點摘要說明

表2所列為本次檢測發現之弱點項目，為 貴單位疑似存在網站相關安全弱點，建議立即安排修補與進一步確認。

1. 弱點檢測分析報告

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| URL / IP Address | 網站名稱 | 弱點類別 | 風險等級 | 弱點AP（程式碼） | 弱點總數 |
| https://lmsw.lceb.gov.tw/ | 土地開發工程管理系統網站平台 | 偵測到RC4 密碼組合 | Medium | https://lmsw.lceb.gov.tw/ | 2 |
| 支援已淘汰的SSL 版本 | Medium | https://lmsw.lceb.gov.tw/ |
| https://www.lceb.gov.tw/index.aspx | 土地重劃工程處全球資訊網 | 發現不存在網域的鏈結 | High | https://www.lceb.gov.tw/banner/index.aspx?Parser=99,10,70 | 1 |
| https://www.lceb.gov.tw/site1/index.aspx | 農村社區土地重劃資訊平台 | 發現不存在網域的鏈結 | High | https://www.lceb.gov.tw/banner/index.aspx?Parser=99,10,70 | 1 |

## 弱點分析（弱點描述）

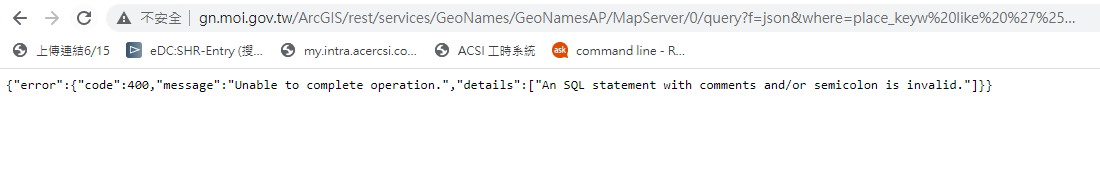
### SQL注入

SQL Injection是一種未做好輸入查驗（Input Validation）的問題，即在撰寫應用程式時，沒有對使用者的輸入做妥善的過濾與處理，便將其組合成 SQL 指令，傳送給 SQL server 執行。若使用者輸入之資料中含有某些對資料庫系統有特殊意義的符號或命令時，便可能讓使用者有機會對資料庫系統下達指令，而造成入侵所帶來的損失。事實上，這樣的疏漏並不是資料庫系統的錯誤，而是程式設計師或軟體開發者的疏忽所產生的。SQL Injection 弱點與威脅主要是因為未作輸入檢查，所以讓攻擊者有機會可以將 SQL 指令送至後端資料庫執行，進一步竊取資料或造成系統破壞。但如果程式於資料驗證部分沒有加以檢查，也可能導致網站執行錯誤，而直接顯示Database Error Message於網頁上。

## 弱點手動檢核

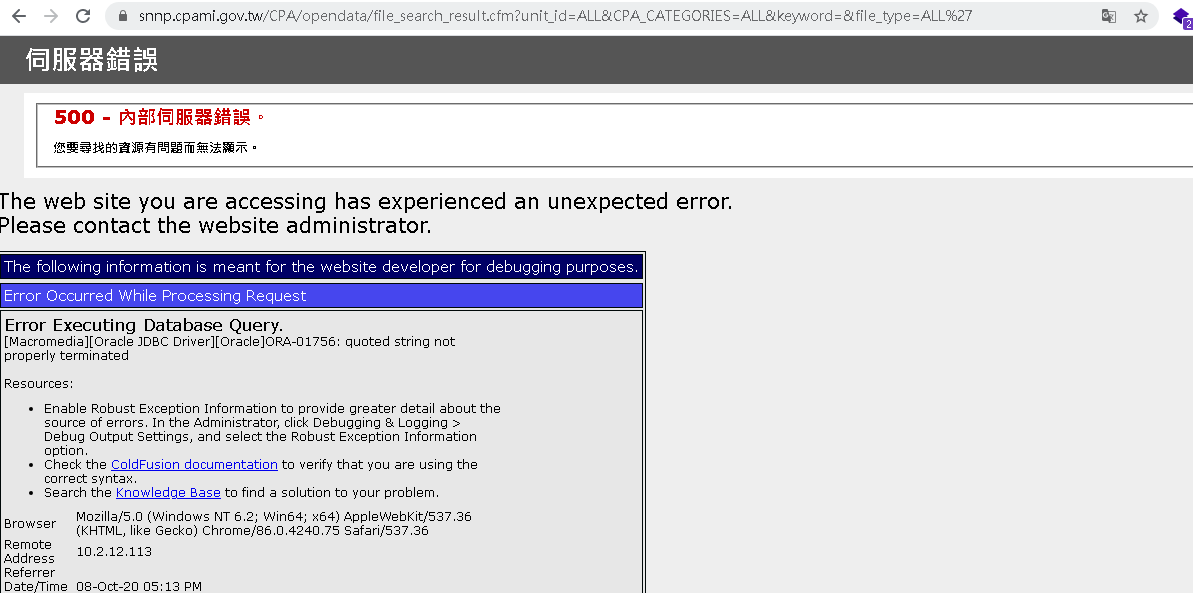
### SQL注入

#### 地名資訊服務網

http://gn.moi.gov.tw/ArcGIS/rest/services/GeoNames/GeoNamesAP/MapServer/0/query，此URL使用POST方式執行，可執行SQL語法，建議與AP廠商確認與修補。

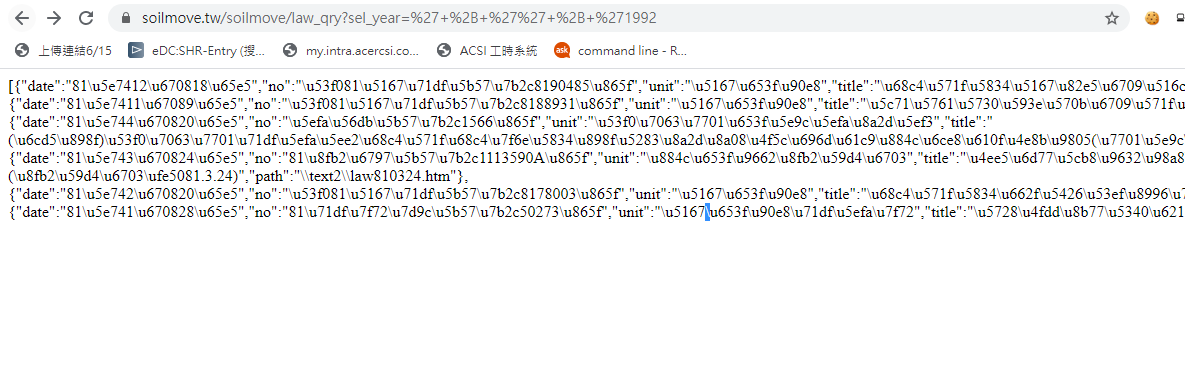
1. SQL注入弱點手動檢核之一

#### 國家自然公園

https://snnp.cpami.gov.tw/CPA/opendata/file\_search\_result.cfm，此URL使用POST方式執行，可執行SQL語法，建議與AP廠商確認與修補。

1. SQL注入弱點手動檢核之二

#### 營建剩餘土石方資訊服務中心

http://www.soilmove.tw/soilmove/law\_qry，此URL使用GET方式執行，可執行SQL語法，建議與AP廠商確認與修補。

1. SQL注入弱點手動檢核之三

#### 社會經濟統計地理資訊網

https://moisagis.moi.gov.tw/moiap/gis2010/content/user/figure/help/metadata.cfm，此URL使用GET方式執行，可執行SQL語法，建議與AP廠商確認與修補。

1. SQL注入弱點手動檢核之四

# 安全強化建議（修補方式）

## SQL 注入弱點修補建議

有關SQL Injection弱點強化建議，說明如下：

### 防止SQL Injection的原則

#### 輸入資料

##### 限定輸入集合

對於有特定輸入值，如性別、月份，可以採用限定輸入集合，僅允許使用者點擇等定值，並且檢查輸入值是否屬於輸入集合中。對於有特定範圍的輸入值，如年齡（雖然不明確，但仍可以設定最大值），則可以檢查輸入的值的範圍。

##### 檢查資料格式

有些資料，字串長度固定而且有特定的格式，例如身份證字號、手機號碼等；有些資料，雖然字串長度可變但仍有特定的格式，例如電子郵件帳號。若有固定長度可先針對字串長度檢查，對於資料格式則可以用正規表示式（Regular Expression）檢查是否符合格式。

##### 過濾特殊字元

對於沒有特定範圍、特定格式的資料，如密碼、個人描述等，即無法限定輸入集合，也無法檢查資料格式，此時將特殊字元過濾、編碼，可以避免SQL Injection的攻擊。特殊字元最主要的有「/ \ | ’ ” ` ; , < > $ @ % & ! # \* ^ ~」。

#### 查詢資料庫

在查詢資料庫時使用的SQL指令，若是將變數值及填入成完整的指令，再進行查詢，此時變數值若包含特殊字元，將造成解譯的錯誤。比較安全的方式為，預先編好查詢指令，並轉成資料庫內部表示方式，僅留下參數欄在取得後填入，因此即使變數值中包含有特殊字元，仍只被視為變數值，而不會解譯錯誤。