109 年臺中教育大學
學生學習歷程暨知識管理資料庫系統
初測報告

文件編號：**202008C34032007029**
V1.0 版

2020 年 **08** 月 **14** 日

華電聯網股份有限公司 謹呈

文件制／修訂記錄

版次	日期	說明	作者	修訂中	定稿
1.0	2020.08.14	定稿	劉怡萱	V	

【目　　錄】

【表 目 錄】

【圖 目 錄】

壹、前言

一、 目的

目前網路犯罪越來越普遍，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，本公司將配合 貴單位時程，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。

二、 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 1 個 URL，弱點數量僅以嚴重風險（Critical）部分呈現，如表 1 所列。

表 1　URL / IP List

序號	URL/IP	弱點數量
1	https://mlckms.ntcu.edu.tw/　（前台）	1（Critical）
2	https://mlckms.ntcu.edu.tw/admin（後台）	1（Critical）

貳、檢測作業

一、 檢測時間

檢測期間由 109 年 08 月 05 日至 109 年 08 月 08 日。

二、 檢測方式

由本公司位於汐止之弱點檢測主機，對 貴單位測試標的（內部網址）以遠端方式執行網站安全檢測程序，檢測方式與流程說明如下：

（一） 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。

（二） 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。

（三） 產出弱點檢測報告與修正建議

三、 檢測工具

網站安全檢測將採用國際知名的 Micro Focus WebInspect 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 TOP10 2017 弱點檢核項目。

參、檢測結果

一、 弱點摘要說明

表 2、及下圖所列（呈現）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（此表僅列出 Critical 弱點部分，其他弱點項目請參閱附件檔），建議立即安排修補與進一步確認。

表 2　弱點檢測分析報告

URL / IP Address	弱點描述	弱點等級	弱點 AP（程式碼）	弱點總數
https://mlckms.ntcu.edu.tw/　（前台）	Insecure Transport: Weak SSL Cipher	Critical	https://mlckms.ntcu.edu.tw:443/js/controllers/common.js	1
https://mlckms.ntcu.edu.tw/admin（後台）	Insecure Transport: Weak SSL Cipher	Critical	https://mlckms.ntcu.edu.tw:443/js/models/base_model.js	1

Scan Name:	Site: https://mlckms.ntcu.edu.tw/		
Policy:	Standard	**Crawl Sessions:**	19
Scan Date:	8/6/2020 5:34:27 PM	**Vulnerabilities:**	25
Scan Version:	19.1.0.302	**Scan Duration:**	21 minutes : 37 seconds
Scan Type:	Site	**Client:**	FF

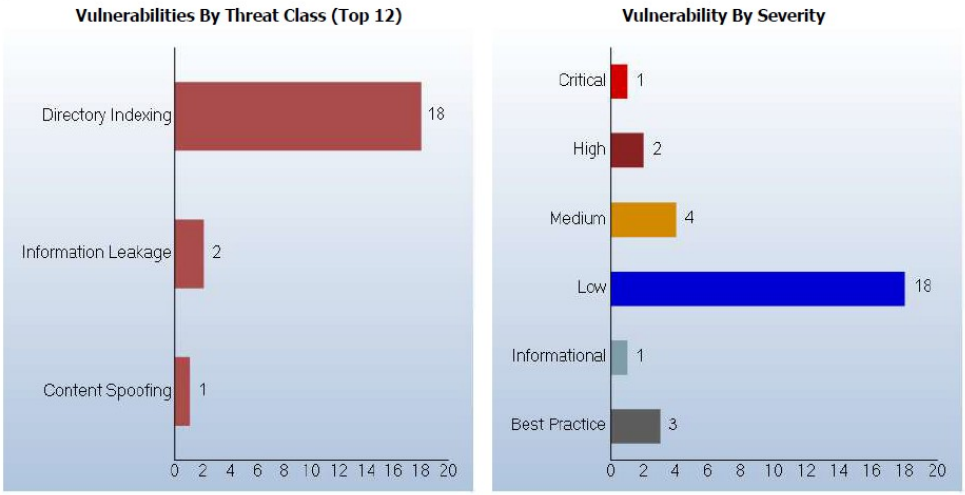

圖 1　檢測摘要

二、 Critical 弱點分析

（一） Insecure Transport: Weak SSL Cipher

傳輸層安全性（TLS）和安全通訊端層（SSL）通訊協定可提供 保護機制，以確保用戶端 Web 伺服器之間傳送資料的真確性、機密 性及完整性。此保護機制的強度由為傳送機密資訊（透過 TLS/SSL 通道）所選擇的驗證、加密及雜湊演算法（統稱為加密套件）決定。 大多數 Web 伺服器都支援各種強度的此類加密套件。

而當使用弱式加密或長度不足的加密金鑰可使攻擊者能夠攻擊保護機制，並竊取或修改機密資訊。

三、 高弱點分析參考

高弱點分析原始資料請參考附件檢測報告，本項屬於補充資料。

（一） Insecure Transport: Weak SSL Protocol（11395、11378） 傳輸層安全性（TLS）通訊協定和安全通訊端層（SSL）通訊協定可提供保護機制，以確保用戶端和 Web 伺服器之間傳送資料的真確性、機密性及完整性。TLS/SSL 通訊協定已經歷多次修訂，從而產生定期版本更新。每次新修訂都旨在解決較舊版本中發現的安全性弱點。

當使用不安全的通訊協定版本會降低傳輸保護強度，從而使得攻擊者能夠危害安全性，竊取或修改機密資訊。

四、 Critical 弱點檢核

（一） Insecure Transport: Weak SSL Cipher

Server: https://mlckms.ntcu.edu.tw:443

Critical Issues

Insecure Transport: Weak SSL Cipher (11285) View Description

CWE: 319,326,327

Kingdom: Security Features

Page: https://mlckms.ntcu.edu.tw:443/js/controllers/common.js

Request:

```
GET /js/controllers/common.js HTTP/1.1
Referer: https://mlckms.ntcu.edu.tw/
Host: mlckms.ntcu.edu.tw
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-AscRawUrl: /js/controllers/common.js
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:30.0) Gecko/20100101
Firefox/30.0
Connection: Keep-Alive
X-WIPP: AscVersion=19.1.0.302
X-Scan-Memo: ScriptEngine="Gecko"; Category="Crawl";
SID="E96558A3A9A8F3AFBB2CC45A2E4A3FAA";
PSID="9EF54E172FA964E00242670D3B32117F"; SessionType="Crawl";
CrawlType="ScriptInclude"; AttackType="None"; OriginatingEngineID="00000000-
0000-0000-0000-000000000000"; ThreadId="54"; ThreadType="JScriptEvent";
X-RequestManager-Memo: sid="59"; smi="0"; sc="1"; ID="cfee5c6d-9b27-4a34-
a1f0-bcf9a660053d";
X-Request-Memo: ID="1364235a-6f98-4160-a474-cf9cce0faf09"; sc="1"; tid="54";
Cookie: CustomCookie=WebInspect153040ZX1555F194D0EC485DA108F9E66FEDE80BY455F
```

圖 2 前台檢核畫面

Server: https://mlckms.ntcu.edu.tw:443

Critical Issues

Insecure Transport: Weak SSL Cipher (11285) View Description

CWE: 319,326,327

Kingdom: Security Features

Page: https://mlckms.ntcu.edu.tw:443/js/models/base_model.js

Request:

```
GET /js/models/base_model.js HTTP/1.1
Accept: */*
Referer: https://mlckms.ntcu.edu.tw/admin
Accept-Language: zh-TW
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like
Gecko
Accept-Encoding: gzip, deflate
Host: mlckms.ntcu.edu.tw
Connection: Keep-Alive
Pragma: no-cache
Cookie: CustomCookie=WebInspect153040ZX1555F194D0EC485DA108F9E66FEDE80BY455F
```

圖 3 後台檢核畫面

肆、安全強化建議

Insecure Transport: Weak SSL Cipher 及 Insecure Transport: Weak SSL Protocol 修補建議

（一） Windows IIS

1. 使用 IISCrypto 排除不安全的 Protocols、Ciphers

- 工具下載連結 https://www.nartac.com/Products/IISCrypto
- 將不必要的 Protocols、Ciphers 取消勾選

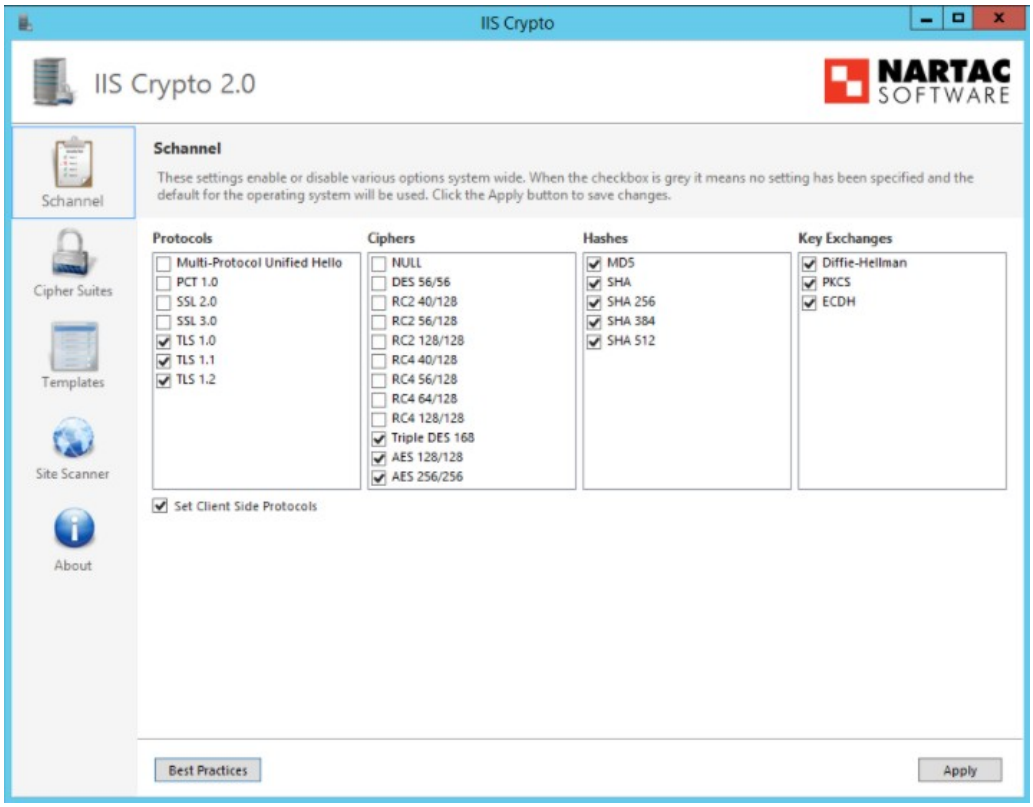

圖 4　不必要的 Protocols、Ciphers 取消勾選

2. 使用 IISCrypto 排除不安全的 Cipher Suites

- 將檢測出有問題的 Cipher Suites 取消勾選

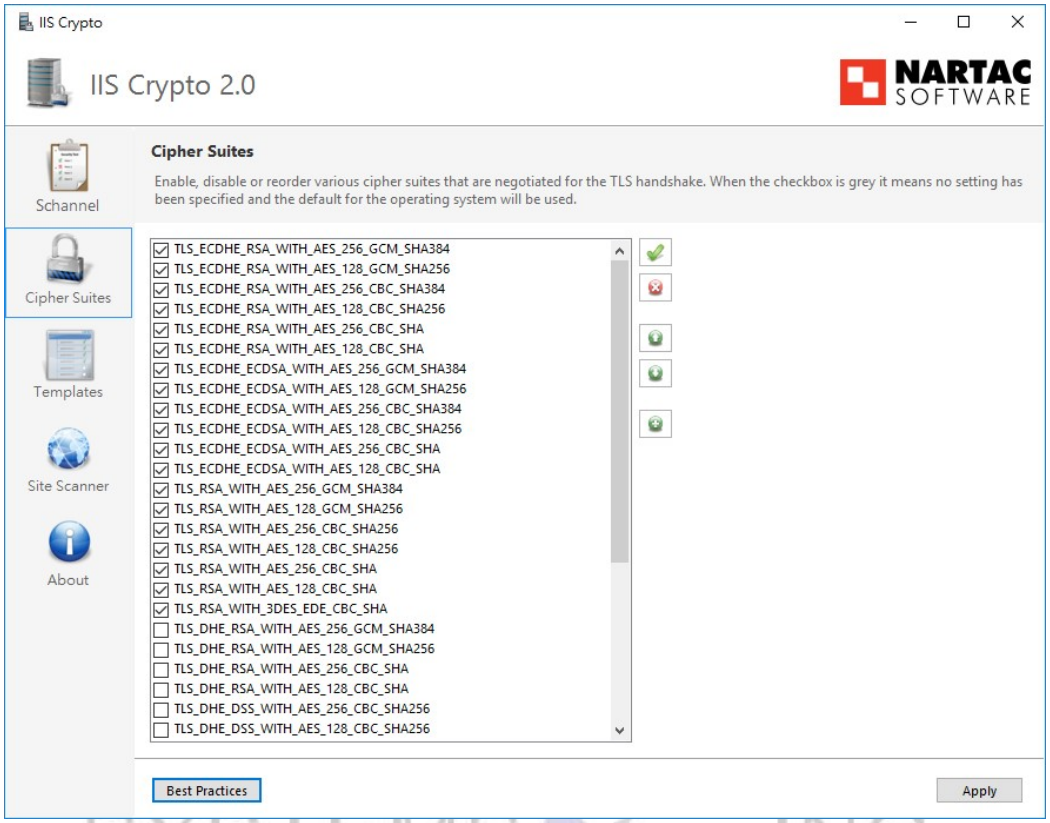

圖 5　排除不安全的 Cipher Suites

3. 重啟服務

- 完成後按下Apply確認設定
- 重啟IIS服務