WEB SERVER SECURITY ASSESSMENT

滲透測試報告

Penetration Testing Report

PREPARED FOR ・ 委託單位

苗栗縣特教科

SCAN TARGET ・ 掃描目標

https://spc.mlc.edu.tw/

SCANNER ・ 掃描工具

Nikto

標準掃描（HTTP/HTTPS 全面檢查 + CVE 比對）

SCAN DATE ・ 掃描日期

2026-07-21

SCAN TIME ・ 掃描時間

11:36 – 11:46

歷時 10m 16s

REPORT DATE ・ 報告產生日期

2026 年 07 月 21 日

存活主機：1 台 ・ 開放埠：0 個

掃描頁面：1 個

OVERALL RISK LEVEL ・ 整體風險等級

CRITICAL

共 7 筆 C 1 H 1 M 1 L 0 I 4

本報告由智新資通資安檢測系統（Nikto 2.1.5 (Docker)）產生，僅供資安評估參考。掃描結果可能包含誤報（False Positive），建議由資安人員進行人工驗證。本報告包含敏感安全資訊，請妥善保管，未經授權不得對外公開。

一、執行摘要

整體風險等級：CRITICAL

本次滲透測試發現 1 個嚴重風險，目標系統面臨極高度被入侵風險，建議立即停止對外服務並進行全面修補。

本次使用 **Nikto 2.1.5 (Docker)** 進行Web 伺服器安全檢測， 採用 **標準掃描** 模式，針對目標 **https://spc.mlc.edu.tw/** 進行自動化安全評估。 掃描作業於 2026年07月21日 11:36 開始，歷時 10m 16s 完成。 共掃描到 **1** 台存活主機，發現 **0** 個開放埠。 共掃描 **1** 個頁面。

1	1	1	0	4
CRITICAL 嚴重	HIGH 高風險	MEDIUM 中風險	LOW 低風險	INFO 資訊

二、風險等級說明

Critical	**嚴重漏洞**：可直接被遠端利用，無需授權即可取得系統控制權或存取敏感資料。常見如遠端程式碼執行（RCE）、遠端管理服務暴露等。**建議立即修復**（24 小時內）。
High	**高風險漏洞**：可能造成重大損害，如高風險服務暴露（RDP/FTP/Telnet）、資料洩漏、身分驗證繞過等。**建議 7 天內修復**。
Medium	**中等風險**：單獨利用危害有限，但可能與其他弱點組合使用。常見如不安全服務設定、HTTP 標頭缺失等。**建議 30 天內修復**。
Low	**低風險**：危害程度較低，通常為標準服務（SSH/HTTP/HTTPS）開放或一般設定觀察。**建議於例行維護時修復**。
Info	**資訊性**：非直接安全威脅，主要為服務探測、技術指紋識別，可輔助了解系統暴露面。

三、主要發現摘要（Top 3）

CRITICAL **No CGI Directories found (use '-C all' to force check all possible dirs)** → https://spc.mlc.edu.tw

No CGI Directories found (use '-C all' to force check all possible dirs)

HIGH **Uncommon header 'x-xss-protection' found, with contents: 1; mode=block** → https://spc.mlc.edu.tw

Uncommon header 'x-xss-protection' found, with contents: 1; mode=block

MEDIUM **Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN** → https://spc.mlc.edu.tw

Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN

四、OWASP Top 10 風險分佈

OWASP Top 10 是國際公認的十大 Web 應用程式安全風險清單，以下為本次掃描結果與 OWASP 分類的對應關係。

分類 ID	風險名稱	發現數	狀態
A01:2021	存取控制失效	—	✓未發現
A02:2021	加密機制失效	—	✓未發現
A03:2021	**注入式攻擊**	**1**	**⚠ 發現**
A04:2021	不安全設計	—	✓未發現
A05:2021	**安全設定錯誤**	**3**	**⚠ 發現**
A06:2021	易受攻擊的元件	—	✓未發現
A07:2021	身分驗證失效	—	✓未發現
A08:2021	軟體及資料完整性失效	—	✓未發現
A09:2021	安全記錄及監控失效	—	✓未發現
A10:2021	伺服器端請求偽造	—	✓未發現

五、修補建議優先順序

優先	嚴重度	問題名稱	建議修復措施
1	CRITICAL	**No CGI Directories found (use '-C all' to force check all possible dirs)**	請參閱相關 CVE 說明與廠商安全公告進行修補。
2	HIGH	**Uncommon header 'x-xss-protection' found, with contents: 1; mode=block**	請參閱相關 CVE 說明與廠商安全公告進行修補。
3	MEDIUM	**Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN**	設定 X-Frame-Options: DENY 或 SAMEORIGIN 防止 Clickjacking。

六、詳細發現清單（共 7 筆）

CRITICAL #001

No CGI Directories found (use '-C all' to force check all possible dirs)

nikto-8aae949dd97037daf941a5329fc66f1f

影響網址位置

https://spc.mlc.edu.tw

⚠ 對應風險分類

CRITICAL

可直接被遠端利用，無需授權即可取得系統控制權。建議立即（24H 內）修復。

i 問題說明

No CGI Directories found (use '-C all' to force check all possible dirs)

建議解法

請參閱相關 CVE 說明與廠商安全公告進行修補。

參考資料

—

技術資訊

ID：nikto-8aae949dd97037daf941a5329fc66f1f
埠/協定：443/http
服務：http

nikto web

HIGH #002

Uncommon header 'x-xss-protection' found, with contents: 1; mode=block

nikto-de0a9b09a3eca20b947dc10209131f2b A03:2021 A05:2021

影響網址位置

https://spc.mlc.edu.tw

⚠ 對應風險分類

HIGH

可能造成資料洩漏、身分驗證繞過等重大損害。建議 7 天內修復。

OWASP Top 10 2021

A03:2021 注入式攻擊
攻擊者向直譯器發送惡意資料，如 SQL、OS 命令、XSS。可能導致資料竊取或系統入侵。

A05:2021 安全設定錯誤
不安全的預設設定、不完整設定、錯誤的 HTTP 標頭、詳細的錯誤訊息等。

i 問題說明

Uncommon header 'x-xss-protection' found, with contents: 1; mode=block

建議解法

請參閱相關 CVE 說明與廠商安全公告進行修補。

參考資料

https://owasp.org/Top10/
https://owasp.org/Top10/

技術資訊

ID：nikto-de0a9b09a3eca20b947dc10209131f2b
埠/協定：443/http
服務：http

nikto web

MEDIUM #003

Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN

nikto-5563bc25e458d2854d79ac445ed791e7 A05:2021

影響網址位置

https://spc.mlc.edu.tw

⚠ 對應風險分類

MEDIUM

單獨利用危害有限，但可與其他漏洞組合使用。建議 30 天內修復。

OWASP Top 10 2021

A05:2021 安全設定錯誤
不安全的預設設定、不完整設定、錯誤的 HTTP 標頭、詳細的錯誤訊息等。

i 問題說明

Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN

建議解法

設定 X-Frame-Options: DENY 或 SAMEORIGIN 防止 Clickjacking。

參考資料

https://owasp.org/Top10/

技術資訊

ID：nikto-5563bc25e458d2854d79ac445ed791e7
埠/協定：443/http
服務：http

nikto web

INFO #004

Server: No banner retrieved

nikto-025be13ec1bf6e5f4460cbf1e1ee4ac3

影響網址位置

https://spc.mlc.edu.tw

⚠ 對應風險分類

INFO

非直接威脅，主要為技術指紋識別，可輔助了解系統暴露面。

i 問題說明

Server: No banner retrieved

建議解法

移除或隱藏 Server、X-Powered-By 等 Header 中的版本資訊。

參考資料

—

技術資訊

ID：nikto-025be13ec1bf6e5f4460cbf1e1ee4ac3
埠/協定：443/http
服務：http

nikto web

INFO #005

Uncommon header 'x-content-type-options' found, with contents: nosniff

nikto-dc21ba66386d2e97981a43f41174c69f A05:2021

影響網址位置

https://spc.mlc.edu.tw

⚠ 對應風險分類

INFO

非直接威脅，主要為技術指紋識別，可輔助了解系統暴露面。

OWASP Top 10 2021

A05:2021 安全設定錯誤
不安全的預設設定、不完整設定、錯誤的 HTTP 標頭、詳細的錯誤訊息等。

i 問題說明

Uncommon header 'x-content-type-options' found, with contents: nosniff

建議解法

設定 X-Content-Type-Options: nosniff 防止 MIME 嗅探。

參考資料

https://owasp.org/Top10/

技術資訊

ID：nikto-dc21ba66386d2e97981a43f41174c69f
埠/協定：443/http
服務：http

nikto web

INFO

#006

Server is using a wildcard certificate: '*.mlc.edu.tw'

nikto-76f4c59f9e0b62e45e8c193d659d7abe

影響網址位置

https://spc.mlc.edu.tw

⚠ 對應風險分類

INFO

非直接威脅，主要為技術指紋識別，可輔助了解系統暴露面。

i 問題說明

Server is using a wildcard certificate: '*.mlc.edu.tw'

建議解法

移除或隱藏 Server、X-Powered-By 等 Header 中的版本資訊。

參考資料

—

技術資訊

ID：nikto-76f4c59f9e0b62e45e8c193d659d7abe
埠/協定：443/http
服務：http

nikto web

INFO

#007

Scan terminated: 0 error(s) and 4 item(s) reported on remote host

nikto-ddc82008ce63c09eaf713607d9ef38e8

影響網址位置

https://spc.mlc.edu.tw

⚠ 對應風險分類

INFO

非直接威脅，主要為技術指紋識別，可輔助了解系統暴露面。

i 問題說明

Scan terminated: 0 error(s) and 4 item(s) reported on remote host

建議解法

請參閱相關 CVE 說明與廠商安全公告進行修補。

參考資料

—

技術資訊

ID：nikto-ddc82008ce63c09eaf713607d9ef38e8
埠/協定：443/http
服務：http

nikto web

本報告由智新資通資安檢測系統產生，結果僅供參考，建議由資安專業人員進行人工驗證。本文件含有敏感資訊，未經授權不得對外揭露。