



WEB APPLICATION SECURITY ASSESSMENT

弱點掃描報告

Vulnerability Assessment Report

PREPARED FOR · 委託單位

| 苗栗縣網

TARGET WEBSITE · 掃描目標網站

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

PROJECT · 所屬專案

苗栗縣特殊教育網

SCAN DATE · 掃描日期

2026-07-29

SCAN TIME · 掃描時間

16:51 – 16:54

歷時 3m 6s

REPORT DATE · 報告產生日期

2026 年 07 月 29 日

掃描模式：ZAP Baseline（快速被動掃描）

OVERALL RISK LEVEL · 整體風險等級

MEDIUM

共 72 筆 C 0 H 0 M 25 L 42 I 5

7,363 個頁面 / URL

本報告由 智新資通 資安檢測系統（OWASP ZAP vstable）產生，僅供資安檢測參考。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：MEDIUM

本次掃描發現 25 個中等等級（Medium）漏洞，系統存在一定安全風險。建議於 30 天內評估並完成修補，避免漏洞被惡意組合利用。

本次使用 OWASP ZAP vstable 弱點掃描引擎，採用 ZAP Baseline（快速被動掃描）模式，針對目標 <https://spc.mlc.edu.tw> 進行自動化安全檢測。掃描作業於 2026年07月29日 16:51 開始，歷時 3m 6s 完成，涵蓋 OWASP Top 10 等主流弱點類型。本次共掃描 7,363 個頁面／URL。



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）、SQL Injection（資料庫注入）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，如資料洩漏、身分驗證繞過、未授權操作等。需要一定條件才能被利用。建議 7 天內修復。
Medium	中等風險：單獨利用危害有限，但可能與其他漏洞組合使用造成更大影響。常見如跨站腳本（XSS）、CSRF、資訊洩漏等。建議 30 天內修復。
Low	低風險：危害程度較低，通常為設定不當或資訊暴露問題。建議於例行維護時修復。
Info	資訊性：非直接安全威脅，主要為技術指紋識別、服務探測結果，可輔助了解系統暴露面。

三、主要發現摘要（Top 10）

MEDIUM	Vulnerable JS Library → https://spc.mlc.edu.tw/wp-includes/js/jquery/ui/core.min.js?ver=1.13.1
MEDIUM	Vulnerable JS Library → https://spc.mlc.edu.tw/wp-content/plugins/wpdatables/assets/js/bootstrap/bootstrap-select/bootstrap-select.min.js?ver=2.2.3
MEDIUM	Vulnerable JS Library → https://spc.mlc.edu.tw/wp-content/plugins/wpdatables/assets/js/bootstrap/bootstrap.min.js?ver=2.2.3
MEDIUM	Vulnerable JS Library → https://spc.mlc.edu.tw/wp-content/plugins/wpdatables/assets/js/moment/moment.js?ver=2.2.3
MEDIUM	Vulnerable JS Library → https://spc.mlc.edu.tw/wp-content/plugins/wpdatables/assets/js/wpdatables/wdt.frontend.min.js?ver=2.2.3
MEDIUM	Content Security Policy (CSP) Header Not Set → https://spc.mlc.edu.tw/wp-json/wp/v2/users/189
MEDIUM	Content Security Policy (CSP) Header Not Set → https://spc.mlc.edu.tw/wp-json/wp/v2/users/1054
MEDIUM	Content Security Policy (CSP) Header Not Set → https://spc.mlc.edu.tw/wp-json/wp/v2/users/433
MEDIUM	Content Security Policy (CSP) Header Not Set → https://spc.mlc.edu.tw/wp-json/wp/v2/users/179
MEDIUM	Content Security Policy (CSP) Header Not Set → https://spc.mlc.edu.tw/wp-json/wp/v2/users/1177

四、OWASP Top 10 風險分佈

OWASP（Open Web Application Security Project）Top 10 是國際公認的 Web 應用程式十大安全風險清單，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	5	⚠ 發現
A03:2021	注入式攻擊	10	⚠ 發現
A04:2021	不安全設計	—	✓ 未發現
A05:2021	安全設定錯誤	45	⚠ 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	漏洞名稱	建議修復措施
1	MEDIUM	Vulnerable JS Library	更新至最新穩定版本的 JS 函式庫，定期使用 Snyk 或 npm audit 檢查元件安全性。
2	MEDIUM	Vulnerable JS Library	更新至最新穩定版本的 JS 函式庫，定期使用 Snyk 或 npm audit 檢查元件安全性。
3	MEDIUM	Vulnerable JS Library	更新至最新穩定版本的 JS 函式庫，定期使用 Snyk 或 npm audit 檢查元件安全性。
4	MEDIUM	Vulnerable JS Library	更新至最新穩定版本的 JS 函式庫，定期使用 Snyk 或 npm audit 檢查元件安全性。
5	MEDIUM	Vulnerable JS Library	更新至最新穩定版本的 JS 函式庫，定期使用 Snyk 或 npm audit 檢查元件安全性。
6	MEDIUM	Content Security Policy (CSP) Header Not Set	實作嚴格的 CSP 標頭，限制可載入腳本、樣式和其他資源的來源。
7	MEDIUM	Content Security Policy (CSP) Header Not Set	實作嚴格的 CSP 標頭，限制可載入腳本、樣式和其他資源的來源。
8	MEDIUM	Content Security Policy (CSP) Header Not Set	實作嚴格的 CSP 標頭，限制可載入腳本、樣式和其他資源的來源。
9	MEDIUM	Content Security Policy (CSP) Header Not Set	實作嚴格的 CSP 標頭，限制可載入腳本、樣式和其他資源的來源。
10	MEDIUM	Content Security Policy (CSP) Header Not Set	實作嚴格的 CSP 標頭，限制可載入腳本、樣式和其他資源的來源。
11	MEDIUM	CSP: script-src unsafe-inline	部署強健的 Content Security Policy，定義允許的資源來源。
12	MEDIUM	CSP: script-src unsafe-inline	部署強健的 Content Security Policy，定義允許的資源來源。
13	MEDIUM	CSP: script-src unsafe-inline	部署強健的 Content Security Policy，定義允許的資源來源。
14	MEDIUM	CSP: script-src unsafe-inline	部署強健的 Content Security Policy，定義允許的資源來源。
15	MEDIUM	CSP: script-src unsafe-inline	部署強健的 Content Security Policy，定義允許的資源來源。
16	LOW	Cookie No HttpOnly Flag	為所有敏感 Cookie（特別是 Session Cookie）設定 HttpOnly 屬性。
17	LOW	Cookie No HttpOnly Flag	為所有敏感 Cookie（特別是 Session Cookie）設定 HttpOnly 屬性。
18	LOW	Cookie No HttpOnly Flag	為所有敏感 Cookie（特別是 Session Cookie）設定 HttpOnly 屬性。
19	LOW	Cookie No HttpOnly Flag	為所有敏感 Cookie（特別是 Session Cookie）設定 HttpOnly 屬性。
20	LOW	Cookie No HttpOnly Flag	為所有敏感 Cookie（特別是 Session Cookie）設定 HttpOnly 屬性。
21	LOW	Cookie Without Secure Flag	為所有 Cookie 設定 Secure 屬性，確保只透過 HTTPS 傳送。
22	LOW	Cookie Without Secure Flag	為所有 Cookie 設定 Secure 屬性，確保只透過 HTTPS 傳送。
23	LOW	Cookie Without Secure Flag	為所有 Cookie 設定 Secure 屬性，確保只透過 HTTPS 傳送。
24	LOW	Cookie Without Secure Flag	為所有 Cookie 設定 Secure 屬性，確保只透過 HTTPS 傳送。
25	LOW	Cookie Without Secure Flag	為所有 Cookie 設定 Secure 屬性，確保只透過 HTTPS 傳送。
26	LOW	Cross-Origin-Resource-Policy Header Missing or Invalid	設定 Cross-Origin-Embedder-Policy: require-corp 標頭，強制跨來源資源必須明確允許共享。
27	LOW	Cross-Origin-Resource-Policy Header Missing or Invalid	設定 Cross-Origin-Embedder-Policy: require-corp 標頭，強制跨來源資源必須明確允許共享。
28	LOW	Cross-Origin-Resource-Policy Header Missing or Invalid	設定 Cross-Origin-Embedder-Policy: require-corp 標頭，強制跨來源資源必須明確允許共享。
29	LOW	Cross-Origin-Resource-Policy Header Missing or Invalid	設定 Cross-Origin-Embedder-Policy: require-corp 標頭，強制跨來源資源必須明確允許共享。
30	LOW	Cross-Origin-Resource-Policy Header Missing or Invalid	設定 Cross-Origin-Embedder-Policy: require-corp 標頭，強制跨來源資源必須明確允許共享。

五、詳細發現清單 (共 72 筆)

MEDIUMVulnerable JS Library		
#001	zap-10003	
📍 影響網址位置 https://spc.mlc.edu.tw/wp-includes/js/jquery/ui/core.min.js?ver=1.13.1		
⚠ 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。	i 漏洞說明 偵測到已知存在安全漏洞的 JavaScript 函式庫版本，攻擊者可利用已公開漏洞攻擊使用者瀏覽器。 建議解法 更新至最新穩定版本的 JS 函式庫，定期使用 Snyk 或 npm audit 檢查元件安全性。	參考資料 https://www.zaproxy.org/docs/alerts/10003/ 技術資訊 ID：zap-10003 類型：HTTP 發現次數：8 處 zapplugin-10003

MEDIUM

Vulnerable JS Library

#002

zap-10003

📍 影響網址位置

https://spc.mlc.edu.tw/wp-content/plugins/wpdatables/assets/js/bootstrap/bootstrap-select/bootstrap-select.min.js?ver=2.2.3

△ 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。

i 漏洞說明

偵測到已知存在安全漏洞的 JavaScript 函式庫版本，攻擊者可利用已公開漏洞攻擊使用者瀏覽器。

建議解法

更新至最新穩定版本的 JS 函式庫，定期使用 Snyk 或 npm audit 檢查元件安全性。

參考資料

https://www.zaproxy.org/docs/alerts/10003/

技術資訊

ID：zap-10003

類型：HTTP

發現次數：8 處

zap

plugin-10003

MEDIUMVulnerable JS Library	
#003	zap-10003
📍 影響網址位置 https://spc.mlc.edu.tw/wp-content/plugins/wpdatatables/assets/js/bootstrap/bootstrap.min.js?ver=2.2.3	
⚠ 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。	i 漏洞說明 偵測到已知存在安全漏洞的 JavaScript 函式庫版本，攻擊者可利用已公開漏洞攻擊使用者瀏覽器。 建議解法 更新至最新穩定版本的 JS 函式庫，定期使用 Snyk 或 npm audit 檢查元件安全性。
參考資料 https://www.zaproxy.org/docs/alerts/10003/ 技術資訊 ID：zap-10003 類型：HTTP 發現次數：8 處 zapplugin-10003	

MEDIUMVulnerable JS Library	
#004	zap-10003
📍 影響網址位置 https://spc.mlc.edu.tw/wp-content/plugins/wpdatatables/assets/js/moment/moment.js?ver=2.2.3	
⚠ 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。	i 漏洞說明 偵測到已知存在安全漏洞的 JavaScript 函式庫版本，攻擊者可利用已公開漏洞攻擊使用者瀏覽器。 建議解法 更新至最新穩定版本的 JS 函式庫，定期使用 Snyk 或 npm audit 檢查元件安全性。
參考資料 https://www.zaproxy.org/docs/alerts/10003/ 技術資訊 ID：zap-10003 類型：HTTP 發現次數：8 處 zapplugin-10003	

MEDIUM

Vulnerable JS Library

#005zap-10003

📍 影響網址位置

https://spc.mlc.edu.tw/wp-content/plugins/wpdatatables/assets/js/wpdatatables/wdt.frontend.min.js?ver=2.2.3

△ 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。

i 漏洞說明

偵測到已知存在安全漏洞的 JavaScript 函式庫版本，攻擊者可利用已公開漏洞攻擊使用者瀏覽器。

建議解法

更新至最新穩定版本的 JS 函式庫，定期使用 Snyk 或 npm audit 檢查元件安全性。

參考資料

https://www.zaproxy.org/docs/alerts/10003/

技術資訊

ID：zap-10003
類型：HTTP
發現次數：8 處

zapplugin-10003

MEDIUM

Content Security Policy (CSP) Header Not Set

#006zap-10038A05:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/wp-json/wp/v2/users/189

⚠️ 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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

Content Security Policy (CSP) 標頭遺失或設定不當，可能允許惡意腳本在網頁中執行。

建議解法

實作嚴格的 CSP 標頭，限制可載入腳本、樣式和其他資源的來源。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10038/

技術資訊

ID：zap-10038

類型：HTTP

發現次數：12 處

zapplugin-10038

MEDIUM

Content Security Policy (CSP) Header Not Set

#007zap-10038A05:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/wp-json/wp/v2/users/1054

⚠️ 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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

Content Security Policy (CSP) 標頭遺失或設定不當，可能允許惡意腳本在網頁中執行。

建議解法

實作嚴格的 CSP 標頭，限制可載入腳本、樣式和其他資源的來源。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10038/

技術資訊

ID：zap-10038

類型：HTTP

發現次數：12 處

zapplugin-10038

MEDIUM

Content Security Policy (CSP) Header Not Set

#008zap-10038A05:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/wp-json/wp/v2/users/433

⚠️ 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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

Content Security Policy (CSP) 標頭遺失或設定不當，可能允許惡意腳本在網頁中執行。

建議解法

實作嚴格的 CSP 標頭，限制可載入腳本、樣式和其他資源的來源。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10038/

技術資訊

ID：zap-10038

類型：HTTP

發現次數：12 處

zapplugin-10038

MEDIUM

Content Security Policy (CSP) Header Not Set

#009zap-10038A05:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/wp-json/wp/v2/users/179

⚠️ 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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

Content Security Policy (CSP) 標頭遺失或設定不當，可能允許惡意腳本在網頁中執行。

建議解法

實作嚴格的 CSP 標頭，限制可載入腳本、樣式和其他資源的來源。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10038/

技術資訊

ID：zap-10038

類型：HTTP

發現次數：12 處

zapplugin-10038

MEDIUM

Content Security Policy (CSP) Header Not Set

#010zap-10038A05:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/wp-json/wp/v2/users/1177

⚠️ 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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

Content Security Policy (CSP) 標頭遺失或設定不當，可能允許惡意腳本在網頁中執行。

建議解法

實作嚴格的 CSP 標頭，限制可載入腳本、樣式和其他資源的來源。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10038/

技術資訊

ID：zap-10038

類型：HTTP

發現次數：12 處

zapplugin-10038

MEDIUM

CSP: script-src unsafe-inline

#011zap-10055A05:2021

🔗 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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

缺少 Content Security Policy 標頭，網站易受跨站腳本等注入類攻擊。

建議解法

部署強健的 Content Security Policy，定義允許的資源來源。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10055/

技術資訊

ID：zap-10055
類型：HTTP
發現次數：9 處

zapplugin-10055

MEDIUM

CSP: script-src unsafe-inline

#012zap-10055A05:2021

🔗 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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

缺少 Content Security Policy 標頭，網站易受跨站腳本等注入類攻擊。

建議解法

部署強健的 Content Security Policy，定義允許的資源來源。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10055/

技術資訊

ID：zap-10055
類型：HTTP
發現次數：9 處

zapplugin-10055

MEDIUM

CSP: script-src unsafe-inline

#013zap-10055A05:2021

🔗 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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

缺少 Content Security Policy 標頭，網站易受跨站腳本等注入類攻擊。

建議解法

部署強健的 Content Security Policy，定義允許的資源來源。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10055/

技術資訊

ID：zap-10055
類型：HTTP
發現次數：9 處

zapplugin-10055

MEDIUM

CSP: script-src unsafe-inline

#014zap-10055A05:2021

🔗 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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

缺少 Content Security Policy 標頭，網站易受跨站腳本等注入類攻擊。

建議解法

部署強健的 Content Security Policy，定義允許的資源來源。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10055/

技術資訊

ID：zap-10055
類型：HTTP
發現次數：9 處

zapplugin-10055

MEDIUM

CSP: script-src unsafe-inline

#015zap-10055A05:2021

🔗 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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

缺少 Content Security Policy 標頭，網站易受跨站腳本等注入類攻擊。

建議解法

部署強健的 Content Security Policy，定義允許的資源來源。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10055/

技術資訊

ID：zap-10055
類型：HTTP
發現次數：9 處

zapplugin-10055

MEDIUM

Absence of Anti-CSRF Tokens

#016zap-10202

🔗 影響網址位置

https://spc.mlc.edu.tw/2026/07/%e8%8b%97%e6%a0%97%e7%b8%a3114%e5%ad%b8%e5%b9%b4%e5%ba%a6%e7%89%b9%e6%ae%8a%e6%95%99%e8%82%b2%e6%95%99%e6%9d%90%e8%a8%ad%e8%a8%88%e6%af%94%e8%b3%bd%e5%be%97%e7%8d%8e%e5%90%8d%e5%96%ae/

⚠️ 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。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://www.zaproxy.org/docs/alerts/10202/

技術資訊

ID：zap-10202

類型：HTTP

發現次數：13 處

zapplugin-10202

MEDIUM

Absence of Anti-CSRF Tokens

#017zap-10202

🔗 影響網址位置

https://spc.mlc.edu.tw/2025/12/%e8%8b%97%e6%a0%97%e7%b8%a3114%e5%b9%b4%e5%ba%a6%e9%81%a9%e6%87%89%e9%ab%94%e8%82%b2%e8%9e%8d%e5%90%88%e7%b1%83%e7%90%83%e8%b3%bd%e5%be%97%e7%8d%8e%e5%90%8d%e5%96%ae/

⚠️ 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。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://www.zaproxy.org/docs/alerts/10202/

技術資訊

ID：zap-10202

類型：HTTP

發現次數：13 處

zapplugin-10202

MEDIUM

Absence of Anti-CSRF Tokens

#018zap-10202

🔗 影響網址位置

https://spc.mlc.edu.tw/2024/12/%e8%8b%97%e6%a0%97%e7%b8%a3113%e5%b9%b4%e5%ba%a6%e6%bb%be%e7%90%83%e6%af%94%e8%b3%bd%e5%be%97%e7%8d%8e%e5%90%8d%e5%96%ae/

⚠️ 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。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://www.zaproxy.org/docs/alerts/10202/

技術資訊

ID：zap-10202

類型：HTTP

發現次數：13 處

zapplugin-10202

MEDIUM

Absence of Anti-CSRF Tokens

#019zap-10202

🔗 影響網址位置

https://spc.mlc.edu.tw/2026/06/115%e5%b9%b4%e5%ba%a6%e6%a0%a1%e5%a4%96%e5%b0%88%e5%ae%b6%e6%9a%a8%e8%89%af%e5%b8%ab%e5%85%b8%e7%af%84%e6%94%af%e6%8f%b4%e8%b3%87%e5%84%aa%e6%95%99%e8%82%b2%e6%96%b9%e6%a1%88-%e5%9c%8b%e9%9a%9b/

⚠️ 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。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://www.zaproxy.org/docs/alerts/10202/

技術資訊

ID：zap-10202

類型：HTTP

發現次數：13 處

zapplugin-10202

MEDIUM

Absence of Anti-CSRF Tokens

#020zap-10202

🔗 影響網址位置

https://spc.mlc.edu.tw/2026/06/115%e5%b9%b4%e5%ba%a6%e6%a0%a1%e5%a4%96%e5%b0%88%e5%ae%b6%e6%9a%a8%e8%89%af%e5%b8%ab%e5%85%b8%e7%af%84%e6%94%af%e6%8f%b4%e8%b3%87%e5%84%aa%e6%95%99%e8%82%b2%e6%96%b9%e6%a1%88-%ef%bc%8d-%e5%b8%ab/

⚠️ 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。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://www.zaproxy.org/docs/alerts/10202/

技術資訊

ID：zap-10202

類型：HTTP

發現次數：13 處

zapplugin-10202

MEDIUM

Sub Resource Integrity Attribute Missing

#021zap-90003A03:2021

🌐 影響網址位置

https://spc.mlc.edu.tw/wp-content/themes/happykids/front/js/jquery.prettyPhoto.js?ver=1.0

⚠️ 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

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、損毀或系統入侵。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/90003/

技術資訊

ID：zap-90003
類型：HTTP
發現次數：12 處

zapplugin-90003

MEDIUM

Sub Resource Integrity Attribute Missing

#022zap-90003A03:2021

🌐 影響網址位置

https://spc.mlc.edu.tw/2026/07/%e8%8b%97%e6%a0%97%e7%b8%a3114%e5%ad%b8%e5%b9%b4%e5%ba%a6%e7%89%b9%e6%ae%8a%e6%95%99%e8%82%b2%e6%95%99%e6%9d%90%e8%a8%ad%e8%a8%88%e6%af%94%e8%b3%bd%e5%be%97%e7%8d%8e%e5%90%8d%e5%96%ae/

⚠️ 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

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、損毀或系統入侵。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/90003/

技術資訊

ID：zap-90003
類型：HTTP
發現次數：12 處

zapplugin-90003

MEDIUM

Sub Resource Integrity Attribute Missing

#023zap-90003A03:2021

🌐 影響網址位置

https://spc.mlc.edu.tw/2025/12/%e8%8b%97%e6%a0%97%e7%b8%a3114%e5%b9%b4%e5%ba%a6%e9%81%a9%e6%87%89%e9%ab%94%e8%82%b2%e8%9e%8d%e5%90%88%e7%b1%83%e7%90%83%e8%b3%bd%e5%be%97%e7%8d%8e%e5%90%8d%e5%96%ae/

⚠️ 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

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、損毀或系統入侵。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/90003/

技術資訊

ID：zap-90003
類型：HTTP
發現次數：12 處

zapplugin-90003

MEDIUM

Sub Resource Integrity Attribute Missing

#024zap-90003A03:2021

🌐 影響網址位置

https://spc.mlc.edu.tw/2024/12/%e8%8b%97%e6%a0%97%e7%b8%a3113%e5%b9%b4%e5%ba%a6%e6%bb%be%e7%90%83%e6%af%94%e8%b3%bd%e5%be%97%e7%8d%8e%e5%90%8d%e5%96%ae/

⚠️ 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

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、損毀或系統入侵。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/90003/

技術資訊

ID：zap-90003
類型：HTTP
發現次數：12 處

zapplugin-90003

MEDIUM

Sub Resource Integrity Attribute Missing

#025zap-90003A03:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/2026/06/115e5%b9%b4e5%ba%6e6%a0%a1e5%a4%96e5%b0%88e5%ae%b6e6%9a%a8e8%89%af%e5%b8%ab%e5%85%b8e7%af%84e6%94%af%e6%8f%b4%e8%b3%87e5%84aa%e6%95%99e8%82%b2e6%96%b9%e6%a1%88-%e5%9c%8b%e9%9a%9b/

⚠️ 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

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、損毀或系統入侵。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/90003/

技術資訊

ID：zap-90003
類型：HTTP
發現次數：12 處

zapplugin-90003

LOW

Cookie No HttpOnly Flag

#026zap-10010A05:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/?rest_route=/openid/login

⚠️ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

Cookie 未設定 HttpOnly 旗標，JavaScript 可讀取 Cookie 值，增加 XSS 竊取 Session 的風險。

建議解法

為所有敏感 Cookie（特別是 Session Cookie）設定 HttpOnly 屬性。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10010/

技術資訊

ID：zap-10010
類型：HTTP
發現次數：12 處

zapplugin-10010

LOW

Cookie No HttpOnly Flag

#027zap-10010A05:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/wp-login.php?action=lostpassword&redirect_to=%2F37-2%2F

⚠️ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

Cookie 未設定 HttpOnly 旗標，JavaScript 可讀取 Cookie 值，增加 XSS 竊取 Session 的風險。

建議解法

為所有敏感 Cookie（特別是 Session Cookie）設定 HttpOnly 屬性。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10010/

技術資訊

ID：zap-10010
類型：HTTP
發現次數：12 處

zapplugin-10010

LOW

Cookie No HttpOnly Flag

#028zap-10010A05:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/wp-login.php

⚠️ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

Cookie 未設定 HttpOnly 旗標，JavaScript 可讀取 Cookie 值，增加 XSS 竊取 Session 的風險。

建議解法

為所有敏感 Cookie（特別是 Session Cookie）設定 HttpOnly 屬性。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10010/

技術資訊

ID：zap-10010
類型：HTTP
發現次數：12 處

zapplugin-10010

LOW

Cookie No HttpOnly Flag

#029

zap-10010

A05:2021

🔍 影響網址位置

https://spc.mlc.edu.tw/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fspc.mlc.edu.tw%2Fwp-admin%2F

⚠️ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

Cookie 未設定 HttpOnly 旗標，JavaScript 可讀取 Cookie 值，增加 XSS 竊取 Session 的風險。

建議解法

為所有敏感 Cookie（特別是 Session Cookie）設定 HttpOnly 屬性。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10010/

技術資訊

ID：zap-10010
類型：HTTP
發現次數：12 處

zapplugin-10010

LOW

Cookie No HttpOnly Flag

#030

zap-10010

A05:2021

🔍 影響網址位置

https://spc.mlc.edu.tw/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fspc.mlc.edu.tw%2Fwp-admin%2F

⚠️ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

Cookie 未設定 HttpOnly 旗標，JavaScript 可讀取 Cookie 值，增加 XSS 竊取 Session 的風險。

建議解法

為所有敏感 Cookie（特別是 Session Cookie）設定 HttpOnly 屬性。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10010/

技術資訊

ID：zap-10010
類型：HTTP
發現次數：12 處

zapplugin-10010

LOW

Cookie Without Secure Flag

#031

zap-10011

A05:2021

🔍 影響網址位置

https://spc.mlc.edu.tw/?rest_route=/openid/login

⚠️ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

Cookie 未設定 Secure 旗標，可能透過非加密的 HTTP 連線傳送敏感 Cookie。

建議解法

為所有 Cookie 設定 Secure 屬性，確保只透過 HTTPS 傳送。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10011/

技術資訊

ID：zap-10011
類型：HTTP
發現次數：12 處

zapplugin-10011

LOW

Cookie Without Secure Flag

#032

zap-10011

A05:2021

🔍 影響網址位置

https://spc.mlc.edu.tw/wp-login.php?action=lostpassword&redirect_to=%2F37-2%2F

⚠️ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

Cookie 未設定 Secure 旗標，可能透過非加密的 HTTP 連線傳送敏感 Cookie。

建議解法

為所有 Cookie 設定 Secure 屬性，確保只透過 HTTPS 傳送。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10011/

技術資訊

ID：zap-10011
類型：HTTP
發現次數：12 處

zapplugin-10011

LOW

Cookie Without Secure Flag

#033

zap-10011

A05:2021

🔍 影響網址位置

https://spc.mlc.edu.tw/wp-login.php

⚠️ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

Cookie 未設定 Secure 旗標，可能透過非加密的 HTTP 連線傳送敏感 Cookie。

建議解法

為所有 Cookie 設定 Secure 屬性，確保只透過 HTTPS 傳送。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10011/

技術資訊

ID：zap-10011
類型：HTTP
發現次數：12 處

zapplugin-10011

LOW

Cookie Without Secure Flag

#034

zap-10011

A05:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fspc.mlc.edu.tw%2Fwp-admin%2F

⚠️ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

Cookie 未設定 Secure 旗標，可能透過非加密的 HTTP 連線傳送敏感 Cookie。

建議解法

為所有 Cookie 設定 Secure 屬性，確保只透過 HTTPS 傳送。

參考資料

<https://owasp.org/Top10/>
<https://www.zaproxy.org/docs/alerts/10011/>

技術資訊

ID：zap-10011
類型：HTTP
發現次數：12 處

zapplugin-10011

LOW

Cookie Without Secure Flag

#035

zap-10011

A05:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fspc.mlc.edu.tw%2Fwp-admin%2F

⚠️ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

Cookie 未設定 Secure 旗標，可能透過非加密的 HTTP 連線傳送敏感 Cookie。

建議解法

為所有 Cookie 設定 Secure 屬性，確保只透過 HTTPS 傳送。

參考資料

<https://owasp.org/Top10/>
<https://www.zaproxy.org/docs/alerts/10011/>

技術資訊

ID：zap-10011
類型：HTTP
發現次數：12 處

zapplugin-10011

LOW

Cross-Domain JavaScript Source File Inclusion

#036

zap-10017

A05:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/2026/07/%e8%8b%97%e6%a0%97%e7%b8%a3114%e5%ad%b8%e5%b9%b4%e5%ba%a6%e7%89%b9%e6%ae%8a%e6%95%99%e8%82%b2%e6%95%99%e6%9d%90%e8%a8%ad%e8%a8%88%e6%af%94%e8%b3%bd%e5%be%97%e7%8d%8e%e5%90%8d%e5%96%ae/

⚠️ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

[\(請參考右側參考資料\)](#)

建議解法

[\(請參考 OWASP 防禦指南\)](#)

參考資料

<https://owasp.org/Top10/>
<https://www.zaproxy.org/docs/alerts/10017/>

技術資訊

ID：zap-10017
類型：HTTP
發現次數：13 處

zapplugin-10017

LOW

Cross-Domain JavaScript Source File Inclusion

#037

zap-10017

A05:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/2025/12/%e8%8b%97%e6%a0%97%e7%b8%a3114%e5%b9%b4%e5%ba%a6%e9%81%a9%e6%87%89%e9%ab%94%e8%82%b2%e8%9e%8d%e5%90%88%e7%b1%83%e7%90%83%e8%b3%bd%e5%be%97%e7%8d%8e%e5%90%8d%e5%96%ae/

⚠️ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

[\(請參考右側參考資料\)](#)

建議解法

[\(請參考 OWASP 防禦指南\)](#)

參考資料

<https://owasp.org/Top10/>
<https://www.zaproxy.org/docs/alerts/10017/>

技術資訊

ID：zap-10017
類型：HTTP
發現次數：13 處

zapplugin-10017

LOW

Cross-Domain JavaScript Source File Inclusion

#038zap-10017A05:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/2024/12/%e8%8b%97%e6%a0%97%e7%b8%a3113%e5%b9%b4%e5%ba%a6%e6%bb%be%7%90%83%e6%af%94%e8%b3%bd%e5%be%97%e7%8d%8e%e5%90%8d%e5%96%ae/

⚠ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10017/

技術資訊

ID：zap-10017
類型：HTTP
發現次數：13 處

zapplugin-10017

LOW

Cross-Domain JavaScript Source File Inclusion

#039zap-10017A05:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/2026/06/115%e5%b9%b4%e5%ba%a6%e6%a0%a1%e5%a4%96%e5%b0%88%e5%ae%b6%e6%9a%a8%e8%89%af%e5%b8%ab%e5%85%b8%e7%af%84%e6%94%af%e6%8f%b4%e8%b3%87%e5%84%aa%e6%95%99%e8%82%b2%e6%96%b9%e6%a1%88-%e5%9c%8b%e9%9a%9b/

⚠ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10017/

技術資訊

ID：zap-10017
類型：HTTP
發現次數：13 處

zapplugin-10017

LOW

Cross-Domain JavaScript Source File Inclusion

#040zap-10017A05:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/2026/06/115%e5%b9%b4%e5%ba%a6%e6%a0%a1%e5%a4%96%e5%b0%88%e5%ae%b6%e6%9a%a8%e8%89%af%e5%b8%ab%e5%85%b8%e7%af%84%e6%94%af%e6%8f%b4%e8%b3%87%e5%84%aa%e6%95%99%e8%82%b2%e6%96%b9%e6%a1%88-%ef%bc%8d-%e5%b8%ab/

⚠ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10017/

技術資訊

ID：zap-10017
類型：HTTP
發現次數：13 處

zapplugin-10017

LOW

Strict-Transport-Security Header Not Set

#041zap-10035A05:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/wp-json/wp/v2/users/189

⚠ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10035/

技術資訊

ID：zap-10035
類型：HTTP
發現次數：12 處

zapplugin-10035

LOWStrict-Transport-Security Header Not Set		
#042	zap-10035	A05:2021
🔗 影響網址位置 https://spc.mlc.edu.tw/wp-json/wp/v2/users/1054		
⚠️ 對應風險分類 LOW 危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。 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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。	i 漏洞說明 (請參考右側參考資料) 建議解法 (請參考 OWASP 防禦指南)	參考資料 https://owasp.org/Top10/ https://www.zaproxy.org/docs/alerts/10035/ 技術資訊 ID：zap-10035 類型：HTTP 發現次數：12 處 zapplugin-10035

LOWStrict-Transport-Security Header Not Set		
#043	zap-10035	A05:2021
🔗 影響網址位置 https://spc.mlc.edu.tw/wp-json/wp/v2/users/433		
⚠️ 對應風險分類 LOW 危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。 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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。	i 漏洞說明 (請參考右側參考資料) 建議解法 (請參考 OWASP 防禦指南)	參考資料 https://owasp.org/Top10/ https://www.zaproxy.org/docs/alerts/10035/ 技術資訊 ID：zap-10035 類型：HTTP 發現次數：12 處 zapplugin-10035

LOWStrict-Transport-Security Header Not Set		
#044	zap-10035	A05:2021
🔗 影響網址位置 https://spc.mlc.edu.tw/wp-json/wp/v2/users/179		
⚠️ 對應風險分類 LOW 危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。 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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。	i 漏洞說明 (請參考右側參考資料) 建議解法 (請參考 OWASP 防禦指南)	參考資料 https://owasp.org/Top10/ https://www.zaproxy.org/docs/alerts/10035/ 技術資訊 ID：zap-10035 類型：HTTP 發現次數：12 處 zapplugin-10035

LOWStrict-Transport-Security Header Not Set		
#045	zap-10035	A05:2021
🔗 影響網址位置 https://spc.mlc.edu.tw/wp-json/wp/v2/users/1177		
⚠️ 對應風險分類 LOW 危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。 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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。	i 漏洞說明 (請參考右側參考資料) 建議解法 (請參考 OWASP 防禦指南)	參考資料 https://owasp.org/Top10/ https://www.zaproxy.org/docs/alerts/10035/ 技術資訊 ID：zap-10035 類型：HTTP 發現次數：12 處 zapplugin-10035

LOWCookie without SameSite Attribute		
#046	zap-10054	A02:2021
🔗 影響網址位置 https://spc.mlc.edu.tw/?rest_route=/openid/login		
⚠️ 對應風險分類 LOW 危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。 OWASP Top 10 2021 A02:2021 加密機制失效 與加密相關的失敗，通常導致敏感資料暴露。包括明文傳輸、弱加密演算法、不安全的金鑰管理。	i 漏洞說明 (請參考右側參考資料) 建議解法 (請參考 OWASP 防禦指南)	參考資料 https://owasp.org/Top10/ https://www.zaproxy.org/docs/alerts/10054/ 技術資訊 ID：zap-10054 類型：HTTP 發現次數：12 處 zapplugin-10054

Cookie without SameSite Attribute		
#047	zap-10054	A02:2021
🔍 影響網址位置 https://spc.mlc.edu.tw/wp-login.php?action=lostpassword&redirect_to=%2F37-2%2F		
⚠️ 對應風險分類 LOW 危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。 OWASP Top 10 2021 A02:2021 加密機制失效 與加密相關的失敗，通常導致敏感資料暴露。包括明文傳輸、弱加密演算法、不安全的金鑰管理。	i 漏洞說明 (請參考右側參考資料) 建議解法 (請參考 OWASP 防禦指南)	參考資料 https://owasp.org/Top10/ https://www.zaproxy.org/docs/alerts/10054/ 技術資訊 ID：zap-10054 類型：HTTP 發現次數：12 處 zapplugin-10054

Cookie without SameSite Attribute		
#048	zap-10054	A02:2021
🔍 影響網址位置 https://spc.mlc.edu.tw/wp-login.php		
⚠️ 對應風險分類 LOW 危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。 OWASP Top 10 2021 A02:2021 加密機制失效 與加密相關的失敗，通常導致敏感資料暴露。包括明文傳輸、弱加密演算法、不安全的金鑰管理。	i 漏洞說明 (請參考右側參考資料) 建議解法 (請參考 OWASP 防禦指南)	參考資料 https://owasp.org/Top10/ https://www.zaproxy.org/docs/alerts/10054/ 技術資訊 ID：zap-10054 類型：HTTP 發現次數：12 處 zapplugin-10054

Cookie without SameSite Attribute		
#049	zap-10054	A02:2021
🔍 影響網址位置 https://spc.mlc.edu.tw/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fspc.mlc.edu.tw%2Fwp-admin%2F		
⚠️ 對應風險分類 LOW 危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。 OWASP Top 10 2021 A02:2021 加密機制失效 與加密相關的失敗，通常導致敏感資料暴露。包括明文傳輸、弱加密演算法、不安全的金鑰管理。	i 漏洞說明 (請參考右側參考資料) 建議解法 (請參考 OWASP 防禦指南)	參考資料 https://owasp.org/Top10/ https://www.zaproxy.org/docs/alerts/10054/ 技術資訊 ID：zap-10054 類型：HTTP 發現次數：12 處 zapplugin-10054

Cookie without SameSite Attribute		
#050	zap-10054	A02:2021
🔍 影響網址位置 https://spc.mlc.edu.tw/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fspc.mlc.edu.tw%2Fwp-admin%2F		
⚠️ 對應風險分類 LOW 危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。 OWASP Top 10 2021 A02:2021 加密機制失效 與加密相關的失敗，通常導致敏感資料暴露。包括明文傳輸、弱加密演算法、不安全的金鑰管理。	i 漏洞說明 (請參考右側參考資料) 建議解法 (請參考 OWASP 防禦指南)	參考資料 https://owasp.org/Top10/ https://www.zaproxy.org/docs/alerts/10054/ 技術資訊 ID：zap-10054 類型：HTTP 發現次數：12 處 zapplugin-10054

Permissions Policy Header Not Set		
#051	zap-10063	A05:2021
🔍 影響網址位置 https://spc.mlc.edu.tw/		
⚠️ 對應風險分類 LOW 危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。 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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。	i 漏洞說明 (請參考右側參考資料) 建議解法 (請參考 OWASP 防禦指南)	參考資料 https://owasp.org/Top10/ https://www.zaproxy.org/docs/alerts/10063/ 技術資訊 ID：zap-10063 類型：HTTP 發現次數：11 處 zapplugin-10063

LOW

Permissions Policy Header Not Set

#052zap-10063A05:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/elementor-2420/

⚠️ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10063/

技術資訊

ID : zap-10063
類型: HTTP
發現次數: 11 處

zapplugin-10063

LOW

Permissions Policy Header Not Set

#053zap-10063A05:2021

🔗 影響網址位置

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

⚠️ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10063/

技術資訊

ID : zap-10063
類型: HTTP
發現次數: 11 處

zapplugin-10063

LOW

Permissions Policy Header Not Set

#054zap-10063A05:2021

🔗 影響網址位置

https://spc.mlc.edu.tw

⚠️ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10063/

技術資訊

ID : zap-10063
類型: HTTP
發現次數: 11 處

zapplugin-10063

LOW

Permissions Policy Header Not Set

#055zap-10063A05:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/2024/09/%e9%91%91e5%ae%9aqa/

⚠️ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10063/

技術資訊

ID : zap-10063
類型: HTTP
發現次數: 11 處

zapplugin-10063

LOW

Dangerous JS Functions

#056zap-10110A03:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/wp-includes/js/tw-sack.min.js?ver=1.6.1

⚠️ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、損毀或系統入侵。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10110/

技術資訊

ID : zap-10110
類型: HTTP
發現次數: 9 處

zapplugin-10110

LOW

Dangerous JS Functions

#057

zap-10110

A03:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/wp-content/plugins/gravityforms/js/jquery.json.min.js?ver=2.4.9

⚠ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、損毀或系統入侵。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10110/

技術資訊

ID：zap-10110
類型：HTTP
發現次數：9 處

zapplugin-10110

LOW

Dangerous JS Functions

#058

zap-10110

A03:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/wp-content/plugins/gravityforms/js/gravityforms.min.js?ver=2.4.9

⚠ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、損毀或系統入侵。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10110/

技術資訊

ID：zap-10110
類型：HTTP
發現次數：9 處

zapplugin-10110

LOW

Dangerous JS Functions

#059

zap-10110

A03:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/wp-content/cache/wpfc-minified/l0tpmwia/6aemt.js

⚠ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、損毀或系統入侵。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10110/

技術資訊

ID：zap-10110
類型：HTTP
發現次數：9 處

zapplugin-10110

LOW

Dangerous JS Functions

#060

zap-10110

A03:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/wp-content/cache/wpfc-minified/kdh6x471/6aemt.js

⚠ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、損毀或系統入侵。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10110/

技術資訊

ID：zap-10110
類型：HTTP
發現次數：9 處

zapplugin-10110

LOW

Private IP Disclosure

#061

zap-2

🔗 影響網址位置

https://spc.mlc.edu.tw/wp-json/wp/v2/pages/37

⚠ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://www.zaproxy.org/docs/alerts/2/

技術資訊

ID：zap-2
類型：HTTP
發現次數：2 處

zapplugin-2

LOW

Private IP Disclosure

#062zap-2

🔗 影響網址位置

https://spc.mlc.edu.tw/wp-json/wp/v2/pages/1870

⚠️ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://www.zaproxy.org/docs/alerts/2/

技術資訊

ID：zap-2
類型：HTTP
發現次數：2 處

zapplugin-2

LOW

Cross-Origin-Resource-Policy Header Missing or Invalid

#063zap-90004A05:2021

🔗 影響網址位置

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

⚠️ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

Cross-Origin-Embedder-Policy (COEP) 標頭遺失或無效，降低旁信道攻擊（如 Spectre）的防護能力。

建議解法

設定 Cross-Origin-Embedder-Policy: require-corp 標頭，強制跨來源資源必須明確允許共享。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/90004/

技術資訊

ID：zap-90004
類型：HTTP
發現次數：13 處

zapplugin-90004

LOW

Cross-Origin-Resource-Policy Header Missing or Invalid

#064zap-90004A05:2021

🔗 影響網址位置

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

⚠️ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

Cross-Origin-Embedder-Policy (COEP) 標頭遺失或無效，降低旁信道攻擊（如 Spectre）的防護能力。

建議解法

設定 Cross-Origin-Embedder-Policy: require-corp 標頭，強制跨來源資源必須明確允許共享。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/90004/

技術資訊

ID：zap-90004
類型：HTTP
發現次數：13 處

zapplugin-90004

LOW

Cross-Origin-Resource-Policy Header Missing or Invalid

#065zap-90004A05:2021

🔗 影響網址位置

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

⚠️ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

Cross-Origin-Embedder-Policy (COEP) 標頭遺失或無效，降低旁信道攻擊（如 Spectre）的防護能力。

建議解法

設定 Cross-Origin-Embedder-Policy: require-corp 標頭，強制跨來源資源必須明確允許共享。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/90004/

技術資訊

ID：zap-90004
類型：HTTP
發現次數：13 處

zapplugin-90004

LOW

Cross-Origin-Resource-Policy Header Missing or Invalid

#066zap-90004A05:2021

🔗 影響網址位置

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

⚠️ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

Cross-Origin-Embedder-Policy (COEP) 標頭遺失或無效，降低旁信道攻擊（如 Spectre）的防護能力。

建議解法

設定 Cross-Origin-Embedder-Policy: require-corp 標頭，強制跨來源資源必須明確允許共享。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/90004/

技術資訊

ID：zap-90004
類型：HTTP
發現次數：13 處

zapplugin-90004

LOW

Cross-Origin-Resource-Policy Header Missing or Invalid

#067zap-90004A05:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/elementor-2420/

⚠️ 對應風險分類

LOW

危害程度較低，通常為設定不當或資訊暴露。建議例行維護時修復。

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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

Cross-Origin-Embedder-Policy (COEP) 標頭遺失或無效，降低旁信道攻擊（如 Spectre）的防護能力。

建議解法

設定 Cross-Origin-Embedder-Policy: require-corp 標頭，強制跨來源資源必須明確允許共享。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/90004/

技術資訊

ID：zap-90004
類型：HTTP
發現次數：13 處

zapplugin-90004

INFO

Timestamp Disclosure - Unix

#068zap-10096A05:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/elementor-2420/

⚠️ 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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10096/

技術資訊

ID：zap-10096
類型：HTTP
發現次數：12 處

zapplugin-10096

INFO

Timestamp Disclosure - Unix

#069zap-10096A05:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/37-2/

⚠️ 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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10096/

技術資訊

ID：zap-10096
類型：HTTP
發現次數：12 處

zapplugin-10096

INFO

Timestamp Disclosure - Unix

#070zap-10096A05:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/37-2/

⚠️ 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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10096/

技術資訊

ID：zap-10096
類型：HTTP
發現次數：12 處

zapplugin-10096

INFO

Timestamp Disclosure - Unix

#071zap-10096A05:2021

🔗 影響網址位置

https://spc.mlc.edu.tw/2021/07/%e6%94%bf%e5%ba%9c%e7%b6%b2%e7%ab%99%e8%b3%87%e6%96%99%e9%96%8b%e6%94%be%e5%ae%a3%e5%91%8a/

⚠️ 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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

i 漏洞說明

(請參考右側參考資料)

建議解法

(請參考 OWASP 防禦指南)

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10096/

技術資訊

ID：zap-10096
類型：HTTP
發現次數：12 處

zapplugin-10096

INFO Timestamp Disclosure - Unix #072zap-10096A05:2021		
🌐 影響網址位置 https://spc.mlc.edu.tw/2024/10/elementor-10298/		
⚠️ 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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。		
i 漏洞說明 (請參考右側參考資料) 建議解法 (請參考 OWASP 防禦指南)		參考資料 https://owasp.org/Top10/ https://www.zaproxy.org/docs/alerts/10096/ 技術資訊 ID：zap-10096 類型：HTTP 發現次數：12 處 zapplugin-10096