智新資通
資安檢測服務

CONFIDENTIAL

OWASP ZAP
VSTABLE

WEB APPLICATION SECURITY ASSESSMENT

弱點掃描報告

Vulnerability Assessment Report

PREPARED FOR ・ 委託單位

苗栗縣特教科

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

2026-07-21

SCAN TIME ・ 掃描時間

11:29 – 11:33

歷時 4m 38s

REPORT DATE ・ 報告產生日期

2026 年 07 月 21 日

掃描模式：ZAP Baseline（快速被動掃描）

OVERALL RISK LEVEL ・ 整體風險等級

HIGH

共 83 筆　C 0　H 1　M 28　L 49　I 5

7,336 個頁面／URL

一、執行摘要

整體風險等級：HIGH

本次掃描發現 1 個高等級（High）漏洞，系統存在重大安全風險。若未及時修復，攻擊者可能造成資料洩漏或服務異常。建議於 7 天內完成修補。

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21日 11:29 開始， 歷時 4m 38s 完成，涵蓋 OWASP Top 10 等主流弱點類型。 本次共掃描 **7,336** 個頁面／URL。

0	1	28	49	5
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）、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）

- HIGH **Secure Pages Include Mixed Content** → https://spc.mlc.edu.tw/
- 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/cache/wpfc-minified/kdh6x471/6aemt.js
- MEDIUM **Vulnerable JS Library** → https://spc.mlc.edu.tw/wp-content/themes/happykids/front/js/jquery.validate.min.js?ver=1.0
- MEDIUM **Vulnerable JS Library** → https://spc.mlc.edu.tw/wp-content/plugins/elementor/assets/lib/swiper/swiper.min.js?ver=5.3.6
- MEDIUM **Vulnerable JS Library** → https://spc.mlc.edu.tw/wp-content/plugins/wpdatatables/assets/js/bootstrap/bootstrap.min.js?ver=2.2.3
- MEDIUM **Missing Anti-clickjacking Header** → https://spc.mlc.edu.tw/
- MEDIUM **Missing Anti-clickjacking Header** → https://spc.mlc.edu.tw/sitemap/
- MEDIUM **Missing Anti-clickjacking Header** → https://spc.mlc.edu.tw/elementor-2420/
- MEDIUM **Missing Anti-clickjacking Header** → https://spc.mlc.edu.tw/37-2/

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**	**11**	**⚠ 發現**
A04:2021	不安全設計	—	✓未發現
A05:2021	**安全設定錯誤**	**55**	**⚠ 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	HIGH	Secure Pages Include Mixed Content	對所有使用者輸入進行嚴格的輸入驗證和輸出編碼，實作 Content Security Policy。
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	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。
7	MEDIUM	Missing Anti-clickjacking Header	設定 X-Frame-Options: DENY 或 SAMEORIGIN，或使用 CSP frame-ancestors 指令。
8	MEDIUM	Missing Anti-clickjacking Header	設定 X-Frame-Options: DENY 或 SAMEORIGIN，或使用 CSP frame-ancestors 指令。
9	MEDIUM	Missing Anti-clickjacking Header	設定 X-Frame-Options: DENY 或 SAMEORIGIN，或使用 CSP frame-ancestors 指令。
10	MEDIUM	Missing Anti-clickjacking Header	設定 X-Frame-Options: DENY 或 SAMEORIGIN，或使用 CSP frame-ancestors 指令。
11	MEDIUM	Missing Anti-clickjacking Header	設定 X-Frame-Options: DENY 或 SAMEORIGIN，或使用 CSP frame-ancestors 指令。
12	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。
13	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。
14	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。
15	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。
16	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。
17	MEDIUM	Application Error Disclosure	移除 X-Powered-By、Server 等暴露技術資訊的回應標頭。
18	MEDIUM	Application Error Disclosure	移除 X-Powered-By、Server 等暴露技術資訊的回應標頭。
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 No HttpOnly Flag	為所有敏感 Cookie（特別是 Session Cookie）設定 HttpOnly 屬性。
22	LOW	Cookie No HttpOnly Flag	為所有敏感 Cookie（特別是 Session Cookie）設定 HttpOnly 屬性。
23	LOW	Cookie No HttpOnly Flag	為所有敏感 Cookie（特別是 Session Cookie）設定 HttpOnly 屬性。
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	Cookie Without Secure Flag	為所有 Cookie 設定 Secure 屬性，確保只透過 HTTPS 傳送。
27	LOW	Cookie Without Secure Flag	為所有 Cookie 設定 Secure 屬性，確保只透過 HTTPS 傳送。
28	LOW	Cookie Without Secure Flag	為所有 Cookie 設定 Secure 屬性，確保只透過 HTTPS 傳送。
29	LOW	X-Content-Type-Options Header Missing	在所有回應中設定 X-Content-Type-Options: nosniff 標頭。
30	LOW	X-Content-Type-Options Header Missing	在所有回應中設定 X-Content-Type-Options: nosniff 標頭。
31	LOW	X-Content-Type-Options Header Missing	在所有回應中設定 X-Content-Type-Options: nosniff 標頭。
32	LOW	X-Content-Type-Options Header Missing	在所有回應中設定 X-Content-Type-Options: nosniff 標頭。
33	LOW	X-Content-Type-Options Header Missing	在所有回應中設定 X-Content-Type-Options: nosniff 標頭。
34	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。
35	LOW	Cross-Origin-Resource-Policy Header Missing or	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。

		Invalid	
36	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。
37	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。
38	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 83 筆）

HIGH
#001

Secure Pages Include Mixed Content

zap-10040 A03:2021

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、損毀或系統入侵。

漏洞說明

偵測到跨站腳本（XSS）漏洞，攻擊者可注入惡意腳本執行於使用者瀏覽器。

建議解法

對所有使用者輸入進行嚴格的輸入驗證和輸出編碼，實作 Content Security Policy。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10040/

技術資訊

ID：zap-10040
類型：HTTP
發現次數：1 處

zap plugin-10040

MEDIUM
#002

Vulnerable JS Library

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。

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：10 處

zap plugin-10003

MEDIUM
#003

Vulnerable JS Library

zap-10003

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

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。

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：10 處

zap plugin-10003

MEDIUM
#004

Vulnerable JS Library

zap-10003

影響網址位置
https://spc.mlc.edu.tw/wp-content/themes/happykids/front/js/jquery.validate.min.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。

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：10 處

zap plugin-10003

MEDIUM
#005

Vulnerable JS Library

zap-10003

影響網址位置
https://spc.mlc.edu.tw/wp-content/plugins/elementor/assets/lib/swiper/swiper.min.js?ver=5.3.6

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。

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：10 處

zap plugin-10003

MEDIUM #006

Vulnerable JS Library

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。

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：10 處

zap plugin-10003

MEDIUM #007

Missing Anti-clickjacking Header

zap-10020 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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

漏洞說明

缺少 X-Frame-Options 或 CSP frame-ancestors 標頭，網站可能被嵌入 iframe，導致 Clickjacking。

建議解法

設定 X-Frame-Options: DENY 或 SAMEORIGIN，或使用 CSP frame-ancestors 指令。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10020/

技術資訊

ID：zap-10020
類型：HTTP
發現次數：11 處

zap plugin-10020

MEDIUM #008

Missing Anti-clickjacking Header

zap-10020 A05:2021

影響網址位置

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

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。

漏洞說明

缺少 X-Frame-Options 或 CSP frame-ancestors 標頭，網站可能被嵌入 iframe，導致 Clickjacking。

建議解法

設定 X-Frame-Options: DENY 或 SAMEORIGIN，或使用 CSP frame-ancestors 指令。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10020/

技術資訊

ID：zap-10020
類型：HTTP
發現次數：11 處

zap plugin-10020

MEDIUM #009

Missing Anti-clickjacking Header

zap-10020 A05:2021

影響網址位置

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

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。

漏洞說明

缺少 X-Frame-Options 或 CSP frame-ancestors 標頭，網站可能被嵌入 iframe，導致 Clickjacking。

建議解法

設定 X-Frame-Options: DENY 或 SAMEORIGIN，或使用 CSP frame-ancestors 指令。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10020/

技術資訊

ID：zap-10020
類型：HTTP
發現次數：11 處

zap plugin-10020

MEDIUM #010

Missing Anti-clickjacking Header

zap-10020 A05:2021

影響網址位置

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

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。

漏洞說明

缺少 X-Frame-Options 或 CSP frame-ancestors 標頭，網站可能被嵌入 iframe，導致 Clickjacking。

建議解法

設定 X-Frame-Options: DENY 或 SAMEORIGIN，或使用 CSP frame-ancestors 指令。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10020/

技術資訊

ID：zap-10020
類型：HTTP
發現次數：11 處

zap plugin-10020

MEDIUM

#011

Missing Anti-clickjacking Header

zap-10020 A05:2021

影響網址位置

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

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。

漏洞說明

缺少 X-Frame-Options 或 CSP frame-ancestors 標頭，網站可能被嵌入 iframe，導致 Clickjacking。

建議解法

設定 X-Frame-Options: DENY 或 SAMEORIGIN，或使用 CSP frame-ancestors 指令。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10020/

技術資訊

ID：zap-10020
類型：HTTP
發現次數：11 處

zap plugin-10020

MEDIUM

#012

Content Security Policy (CSP) Header Not Set

zap-10038 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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

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

zap plugin-10038

MEDIUM

#013

Content Security Policy (CSP) Header Not Set

zap-10038 A05:2021

影響網址位置

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

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。

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

zap plugin-10038

MEDIUM

#014

Content Security Policy (CSP) Header Not Set

zap-10038 A05:2021

影響網址位置

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

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。

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

zap plugin-10038

MEDIUM

#015

Content Security Policy (CSP) Header Not Set

zap-10038 A05:2021

影響網址位置

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

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。

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

zap plugin-10038

MEDIUM

#016

Content Security Policy (CSP) Header Not Set

zap-10038 A05:2021

影響網址位置

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

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。

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

zap plugin-10038

MEDIUM

#017

HTTPS to HTTP Insecure Transition in Form Post

zap-10042 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、開放式雲端存儲、錯誤的 HTTP 標頭、詳細錯誤訊息等。

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/10042/

技術資訊

ID：zap-10042
類型：HTTP
發現次數：1 處

zap plugin-10042

MEDIUM

#018

Absence of Anti-CSRF Tokens

zap-10202

影響網址位置

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

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。

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：12 處

zap plugin-10202

MEDIUM

#019

Absence of Anti-CSRF Tokens

zap-10202

影響網址位置

https://spc.mlc.edu.tw/2026/01/%e5%ad%b8%e7%94%9f%e5%86%8d%e7%94%b3%e8%a8%b4/

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。

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：12 處

zap plugin-10202

MEDIUM

#020

Absence of Anti-CSRF Tokens

zap-10202

影響網址位置

https://spc.mlc.edu.tw/2026/01/%e9%ab%98%e7%b4%9a%e4%b8%ad%e7%ad%89%e4%bb%a5%e4%b8%8b%e5%ad%b8%e6%a0%a1%e5%ad%b8%e7%94%9f%e7%94%b3%e8%a8%b4%e5%8f%8a%e5%86%8d%e7%94%b3%e8%a8%b4%e8%a9%95%e8%ad%b0%e5%a7%94%e5%93%a1%e6%9c%83%e7%b5%84/

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。

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：12 處

zap plugin-10202

MEDIUM #021

Absence of Anti-CSRF Tokens

zap-10202

影響網址位置

https://spc.mlc.edu.tw/2026/01/%e3%80%8c%e9%ab%98%e7%b4%9a%e4%b8%ad%e7%ad%89%e4%bb%a5%e4%b8%8b%e5%ad%b8%e6%a0%a1%e5%ad%b8%e7%94%9f%e7%94%b3%e8%a8%b4%e5%8f%8a%e5%86%8d%e7%94%b3%e8%a8%b4%e8%a9%95%e8%ad%b0%e5%a7%94%e5%93%a1%e6%9c%83/

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。

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：12 處

zap plugin-10202

MEDIUM #022

Absence of Anti-CSRF Tokens

zap-10202

影響網址位置

https://spc.mlc.edu.tw/2026/01/%e9%ab%98%e7%b4%9a%e4%b8%ad%e7%ad%89%e5%ad%b8%e6%a0%a1%e5%ad%b8%e7%94%9f%e7%94%b3%e8%a8%b4%e6%a1%88%e4%bb%b6%e9%81%8b%e4%bd%9c%e6%b5%81%e7%a8%8b%e5%9c%96/

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。

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：12 處

zap plugin-10202

MEDIUM #023

Sub Resource Integrity Attribute Missing

zap-90003 A03:2021

影響網址位置

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

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。

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

zap plugin-90003

MEDIUM #024

Sub Resource Integrity Attribute Missing

zap-90003 A03:2021

影響網址位置

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

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。

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

zap plugin-90003

MEDIUM #025

Sub Resource Integrity Attribute Missing

zap-90003 A03:2021

影響網址位置

https://spc.mlc.edu.tw/2026/01/%e5%ad%b8%e7%94%9f%e5%86%8d%e7%94%b3%e8%a8%b4/

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。

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

zap plugin-90003

MEDIUM

#026

Sub Resource Integrity Attribute Missing

zap-90003 A03:2021

影響網址位置

https://spc.mlc.edu.tw/2026/01/%e9%ab%98%e7%b4%9a%e4%b8%ad%e7%ad%89%e4%bb%a5%e4%b8%8b%e5%ad%b8%e6%a0%a1%e5%ad%b8%e7%94%9f%e7%94%b3%e8%a8%b4%e5%8f%8a%e5%86%8d%e7%94%b3%e8%a8%b4%e8%a9%95%e8%ad%b0%e5%a7%94%e5%93%a1%e6%9c%83%e7%b5%84/

⚠ 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

zap plugin-90003

MEDIUM

#027

Sub Resource Integrity Attribute Missing

zap-90003 A03:2021

影響網址位置

https://spc.mlc.edu.tw/2026/01/%e3%80%8c%e9%ab%98%e7%b4%9a%e4%b8%ad%e7%ad%89%e4%bb%a5%e4%b8%8b%e5%ad%b8%e6%a0%a1%e5%ad%b8%e7%94%9f%e7%94%b3%e8%a8%b4%e5%8f%8a%e5%86%8d%e7%94%b3%e8%a8%b4%e8%a9%95%e8%ad%b0%e5%a7%94%e5%93%a1%e6%9c%83/

⚠ 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

zap plugin-90003

MEDIUM

#028

Application Error Disclosure

zap-90022 A05:2021

影響網址位置

https://spc.mlc.edu.tw/wp-content/uploads/2018/06/download-e1530019199427.png

⚠ 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

伺服器暴露了應用程式的技術指紋資訊，攻擊者可針對已知漏洞進行攻擊。

建議解法

移除 X-Powered-By、Server 等暴露技術資訊的回應標頭。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/90022/

技術資訊

ID：zap-90022
類型：HTTP
發現次數：2 處

zap plugin-90022

MEDIUM

#029

Application Error Disclosure

zap-90022 A05:2021

影響網址位置

https://spc.mlc.edu.tw/wp-content/uploads/2019/05/admin_division.gif

⚠ 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

伺服器暴露了應用程式的技術指紋資訊，攻擊者可針對已知漏洞進行攻擊。

建議解法

移除 X-Powered-By、Server 等暴露技術資訊的回應標頭。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/90022/

技術資訊

ID：zap-90022
類型：HTTP
發現次數：2 處

zap plugin-90022

LOW

#030

Cookie No HttpOnly Flag

zap-10010 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。

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：15 處

zap plugin-10010

LOW

#031

Cookie No HttpOnly Flag

zap-10010 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。

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：15 處

zap plugin-10010

LOW

#032

Cookie No HttpOnly Flag

zap-10010 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。

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：15 處

zap plugin-10010

LOW

#033

Cookie No HttpOnly Flag

zap-10010 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。

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：15 處

zap plugin-10010

LOW

#034

Cookie No HttpOnly Flag

zap-10010 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。

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：15 處

zap plugin-10010

LOW

#035

Cookie Without Secure Flag

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。

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

zap plugin-10011

LOW

#036

Cookie Without Secure Flag

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。

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

zap plugin-10011

LOW

#037

Cookie Without Secure Flag

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。

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

zap plugin-10011

LOW

#038

Cookie Without Secure Flag

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。

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

zap plugin-10011

LOW

#039

Cookie Without Secure Flag

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。

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

zap plugin-10011

LOW

#040

Cross-Domain JavaScript Source File Inclusion

zap-10017 A05:2021

影響網址位置

https://spc.mlc.edu.tw/2026/01/%e5%ad%b8%e7%94%9f%e5%86%8d%e7%94%b3%e8%a8%b4/

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。

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：12 處

zap plugin-10017

LOW

#041

Cross-Domain JavaScript Source File Inclusion

zap-10017 A05:2021

影響網址位置

https://spc.mlc.edu.tw/2026/01/%e9%ab%98%e7%b4%9a%e4%b8%ad%e7%ad%89%e4%bb%a5%e4%b8%8b%e5%ad%b8%e6%a0%a1%e5%ad%b8%e7%94%9f%e7%94%b3%e8%a8%b4%e5%8f%8a%e5%86%8d%e7%94%b3%e8%a8%b4%e8%a9%95%e8%ad%b0%e5%a7%94%e5%93%a1%e6%9c%83%e7%b5%84/

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。

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：12 處

zap plugin-10017

LOW

#042

Cross-Domain JavaScript Source File Inclusion

zap-10017 A05:2021

影響網址位置

https://spc.mlc.edu.tw/2026/01/%e3%80%8c%e9%ab%98%e7%b4%9a%e4%b8%ad%e7%ad%89%e4%bb%a5%e4%b8%8b%e5%ad%b8%e6%a0%a1%e5%ad%b8%e7%94%9f%e7%94%b3%e8%a8%b4%e5%8f%8a%e5%86%8d%e7%94%b3%e8%a8%b4%e8%a9%95%e8%ad%b0%e5%a7%94%e5%93%a1%e6%9c%83/

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。

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：12 處

zap plugin-10017

LOW

#043

Cross-Domain JavaScript Source File Inclusion

zap-10017 A05:2021

影響網址位置

https://spc.mlc.edu.tw/2026/01/%e9%ab%98%e7%b4%9a%e4%b8%ad%e7%ad%89%e5%ad%b8%e6%a0%a1%e5%ad%b8%e7%94%9f%e7%94%b3%e8%a8%b4%e6%a1%88%e4%bb%b6%e9%81%8b%e4%bd%9c%e6%b5%81%e7%a8%8b%e5%9c%96/

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。

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：12 處

zap plugin-10017

LOW
#044

Cross-Domain JavaScript Source File Inclusion

zap-10017 A05:2021

影響網址位置

https://spc.mlc.edu.tw/2026/01/%e7%89%b9%e6%ae%8a%e6%95%99%e8%82%b2%e5%ad%b8%e7%94%9f%e5%8f%8a%e5%b9%bc%e5%85%92%e7%94%b3%e8%a8%b4%e6%9c%8d%e5%8b%99%e8%be%a6%e6%b3%95/

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。

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：12 處

zap plugin-10017

LOW
#045

X-Content-Type-Options Header Missing

zap-10021 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。

漏洞說明

回應缺少 X-Content-Type-Options: nosniff，允許瀏覽器進行 MIME 嗅探，可能導致安全問題。

建議解法

在所有回應中設定 X-Content-Type-Options: nosniff 標頭。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10021/

技術資訊

ID：zap-10021
類型：HTTP
發現次數：11 處

zap plugin-10021

LOW
#046

X-Content-Type-Options Header Missing

zap-10021 A05:2021

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。

漏洞說明

回應缺少 X-Content-Type-Options: nosniff，允許瀏覽器進行 MIME 嗅探，可能導致安全問題。

建議解法

在所有回應中設定 X-Content-Type-Options: nosniff 標頭。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10021/

技術資訊

ID：zap-10021
類型：HTTP
發現次數：11 處

zap plugin-10021

LOW
#047

X-Content-Type-Options Header Missing

zap-10021 A05:2021

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。

漏洞說明

回應缺少 X-Content-Type-Options: nosniff，允許瀏覽器進行 MIME 嗅探，可能導致安全問題。

建議解法

在所有回應中設定 X-Content-Type-Options: nosniff 標頭。

參考資料

https://owasp.org/Top10/
https://www.zaproxy.org/docs/alerts/10021/

技術資訊

ID：zap-10021
類型：HTTP
發現次數：11 處

zap plugin-10021

LOW

#048

X-Content-Type-Options Header Missing

zap-10021 A05:2021

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。

漏洞說明

回應缺少 X-Content-Type-Options: nosniff，允許瀏覽器進行 MIME 嗅探，可能導致安全問題。

建議解法

在所有回應中設定 X-Content-Type-Options: nosniff 標頭。

參考資料

https://owasp.org/Top10/

https://www.zaproxy.org/docs/alerts/10021/

技術資訊

ID：zap-10021

類型：HTTP

發現次數：11 處

zap plugin-10021

LOW

#049

X-Content-Type-Options Header Missing

zap-10021 A05:2021

影響網址位置

https://spc.mlc.edu.tw/%e6%b3%95%e4%bb%a4/

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。

漏洞說明

回應缺少 X-Content-Type-Options: nosniff，允許瀏覽器進行 MIME 嗅探，可能導致安全問題。

建議解法

在所有回應中設定 X-Content-Type-Options: nosniff 標頭。

參考資料

https://owasp.org/Top10/

https://www.zaproxy.org/docs/alerts/10021/

技術資訊

ID：zap-10021

類型：HTTP

發現次數：11 處

zap plugin-10021

LOW

#050

Information Disclosure - Debug Error Messages

zap-10023 A05:2021

影響網址位置

https://spc.mlc.edu.tw/wp-content/uploads/2018/06/download-e1530019199427.png

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。

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/10023/

技術資訊

ID：zap-10023

類型：HTTP

發現次數：2 處

zap plugin-10023

LOW

#051

Information Disclosure - Debug Error Messages

zap-10023 A05:2021

影響網址位置

https://spc.mlc.edu.tw/wp-content/uploads/2019/05/admin_division.gif

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。

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/10023/

技術資訊

ID：zap-10023

類型：HTTP

發現次數：2 處

zap plugin-10023

LOW

#052

Strict-Transport-Security Header Not Set

zap-10035 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。

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：11 處

zap plugin-10035

LOW

#053

Strict-Transport-Security Header Not Set

zap-10035 A05:2021

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。

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：11 處

zap plugin-10035

LOW

#054

Strict-Transport-Security Header Not Set

zap-10035 A05:2021

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。

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：11 處

zap plugin-10035

LOW

#055

Strict-Transport-Security Header Not Set

zap-10035 A05:2021

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。

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：11 處

zap plugin-10035

LOW

#056

Strict-Transport-Security Header Not Set

zap-10035 A05:2021

影響網址位置

https://spc.mlc.edu.tw/%e6%b3%95%e4%bb%a4/

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。

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：11 處

zap plugin-10035

LOW

#057

Cookie without SameSite Attribute

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。

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

zap plugin-10054

LOW

#058

Cookie without SameSite Attribute

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。

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

zap plugin-10054

LOW

#059

Cookie without SameSite Attribute

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。

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

zap plugin-10054

LOW

#060

Cookie without SameSite Attribute

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。

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

zap plugin-10054

LOW

#061

Cookie without SameSite Attribute

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。

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

zap plugin-10054

LOW

#062

Permissions Policy Header Not Set

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。

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

zap plugin-10063

LOW

#063

Permissions Policy Header Not Set

zap-10063 A05:2021

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。

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

zap plugin-10063

LOW

#064

Permissions Policy Header Not Set

zap-10063 A05:2021

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。

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

zap plugin-10063

LOW

#065

Permissions Policy Header Not Set

zap-10063 A05:2021

影響網址位置

https://spc.mlc.edu.tw/%e6%b3%95%e4%bb%a4/

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。

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

zap plugin-10063

LOW

#066

Permissions Policy Header Not Set

zap-10063 A05:2021

影響網址位置

https://spc.mlc.edu.tw/2024/09/%e9%91%91%e5%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。

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

zap plugin-10063

LOW

#067

Dangerous JS Functions

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。

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

zap plugin-10110

LOW

#068

Dangerous JS Functions

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。

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

zap plugin-10110

LOW

#069

Dangerous JS Functions

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。

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

zap plugin-10110

LOW

#070

Dangerous JS Functions

zap-10110 A03:2021

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。

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

zap plugin-10110

LOW

#071

Dangerous JS Functions

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。

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

zap plugin-10110

LOW

#072

Private IP Disclosure

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。

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

zap plugin-2

LOW

#073

Private IP Disclosure

zap-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。

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

zap plugin-2

LOW

#074

Cross-Origin-Resource-Policy Header Missing or Invalid

zap-90004 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。

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

zap plugin-90004

LOW

#075

Cross-Origin-Resource-Policy Header Missing or Invalid

zap-90004 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。

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

zap plugin-90004

LOW

#076

Cross-Origin-Resource-Policy Header Missing or Invalid

zap-90004 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。

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

zap plugin-90004

LOW

#077

Cross-Origin-Resource-Policy Header Missing or Invalid

zap-90004 A05:2021

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。

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

zap plugin-90004

LOW

#078

Cross-Origin-Resource-Policy Header Missing or Invalid

zap-90004 A05:2021

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。

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

zap plugin-90004

INFO

#079

Timestamp Disclosure - Unix

zap-10096 A05:2021

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。

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：13 處

zap plugin-10096

INFO

#080

Timestamp Disclosure - Unix

zap-10096 A05:2021

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。

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：13 處

zap plugin-10096

INFO

#081

Timestamp Disclosure - Unix

zap-10096 A05:2021

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。

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：13 處

zap plugin-10096

INFO

#082

Timestamp Disclosure - Unix

zap-10096 A05:2021

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。

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：13 處

zap plugin-10096

INFO

#083

Timestamp Disclosure - Unix

zap-10096 A05:2021

影響網址位置

https://spc.mlc.edu.tw/2025/10/114%e5%ad%b8%e5%b9%b4%e5%ba%a6%e8%8b%97%e6%a0%97%e7%b8%a3%e5%b9%bc%e5%85%92%e5%9c%92%e8%ba%ab%e5%bf%83%e9%9a%9c%e7%a4%99%e5%b9%bc%e5%85%92%e6%a0%a1%e7%af%a9%e4%ba%ba%e5%93%a1%e5%9f%b9%e8%a8%93-2/

⚠ 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：13 處

zap plugin-10096