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

（未指定委託單位）

TARGET WEBSITE ・ 掃描目標網站

http://120.126.223.31/

PROJECT ・ 所屬專案

—

SCAN DATE ・ 掃描日期

2026-08-25

SCAN TIME ・ 掃描時間

10:30 – 10:32

歷時 1m 13s

REPORT DATE ・ 報告產生日期

2026 年 08 月 25 日

掃描模式：ZAP Baseline（快速被動掃描）

OVERALL RISK LEVEL ・ 整體風險等級

LOW

共 19 筆　C0 H0 M0 L19 I0

67 個頁面／URL

一、執行摘要

整體風險等級：LOW

本次掃描結果顯示整體風險偏低，僅發現 19 個低等級（Low）漏洞或設定問題。建議於例行維護週期中一併修復。

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 **http://120.126.223.31/** 進行自動化安全檢測。 掃描作業於 2026年08月25日 10:30 開始， 歷時 1m 13s 完成，涵蓋 OWASP Top 10 等主流弱點類型。 本次共掃描 **67** 個頁面／URL。

0	0	0	19	0
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）

- LOW **Cookie No HttpOnly Flag** → http://120.126.223.31/
- LOW **Cookie No HttpOnly Flag** → http://120.126.223.31/login/student
- LOW **Cookie No HttpOnly Flag** → http://120.126.223.31/captcha/flat?EA7rSyun
- LOW **Cookie No HttpOnly Flag** → http://120.126.223.31/captcha/flat?lyIGfl4v
- LOW **Cookie No HttpOnly Flag** → http://120.126.223.31/login/mentor
- LOW **Server Leaks Version Information via "Server" HTTP Response Header Field** → http://120.126.223.31/
- LOW **Server Leaks Version Information via "Server" HTTP Response Header Field** → http://120.126.223.31/robots.txt
- LOW **Server Leaks Version Information via "Server" HTTP Response Header Field** → http://120.126.223.31/css/custom.css
- LOW **Server Leaks Version Information via "Server" HTTP Response Header Field** → http://120.126.223.31/css/jquery.tagsinput-revisited.css
- LOW **Server Leaks Version Information via "Server" HTTP Response Header Field** → http://120.126.223.31/sitemap.xml

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	—	✓未發現
A03:2021	注入式攻擊	—	✓未發現
A04:2021	不安全設計	—	✓未發現
A05:2021	**安全設定錯誤**	**19**	**⚠ 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	LOW	**Cookie No HttpOnly Flag**	為所有敏感 Cookie（特別是 Session Cookie）設定 HttpOnly 屬性。
2	LOW	**Cookie No HttpOnly Flag**	為所有敏感 Cookie（特別是 Session Cookie）設定 HttpOnly 屬性。
3	LOW	**Cookie No HttpOnly Flag**	為所有敏感 Cookie（特別是 Session Cookie）設定 HttpOnly 屬性。
4	LOW	**Cookie No HttpOnly Flag**	為所有敏感 Cookie（特別是 Session Cookie）設定 HttpOnly 屬性。
5	LOW	**Cookie No HttpOnly Flag**	為所有敏感 Cookie（特別是 Session Cookie）設定 HttpOnly 屬性。
6	LOW	**Cross-Origin-Embedder-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。
7	LOW	**Cross-Origin-Embedder-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。
8	LOW	**Cross-Origin-Embedder-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。
9	LOW	**Cross-Origin-Embedder-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。
10	LOW	**Cross-Origin-Embedder-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 19 筆）

LOW

#001

Cookie No HttpOnly Flag

zap-10010 A05:2021

影響網址位置

http://120.126.223.31/

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：11 處

zap plugin-10010

LOW

#002

Cookie No HttpOnly Flag

zap-10010 A05:2021

影響網址位置

http://120.126.223.31/login/student

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：11 處

zap plugin-10010

LOW

#003

Cookie No HttpOnly Flag

zap-10010 A05:2021

影響網址位置

http://120.126.223.31/captcha/flat?EA7rSyun

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：11 處

zap plugin-10010

LOW

#004

Cookie No HttpOnly Flag

zap-10010 A05:2021

影響網址位置

http://120.126.223.31/captcha/flat?lyIGfI4v

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：11 處

zap plugin-10010

LOW
#005

Cookie No HttpOnly Flag

zap-10010 A05:2021

影響網址位置
http://120.126.223.31/login/mentor

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：11 處

zap plugin-10010

LOW
#006

Server Leaks Version Information via "Server" HTTP Response Header Field

zap-10036 A05:2021

影響網址位置
http://120.126.223.31/

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/10036/

技術資訊

ID：zap-10036
類型：HTTP
發現次數：11 處

zap plugin-10036

LOW
#007

Server Leaks Version Information via "Server" HTTP Response Header Field

zap-10036 A05:2021

影響網址位置
http://120.126.223.31/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/10036/

技術資訊

ID：zap-10036
類型：HTTP
發現次數：11 處

zap plugin-10036

LOW
#008

Server Leaks Version Information via "Server" HTTP Response Header Field

zap-10036 A05:2021

影響網址位置
http://120.126.223.31/css/custom.css

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/10036/

技術資訊

ID：zap-10036
類型：HTTP
發現次數：11 處

zap plugin-10036

LOW
#009

Server Leaks Version Information via "Server" HTTP Response Header Field

zap-10036 A05:2021

影響網址位置
http://120.126.223.31/css/jquery.tagsinput-revisited.css

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/10036/

技術資訊

ID：zap-10036
類型：HTTP
發現次數：11 處

zap plugin-10036

LOW

#010

Server Leaks Version Information via "Server" HTTP Response Header Field

zap-10036 A05:2021

影響網址位置

http://120.126.223.31/sitemap.xml

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/10036/

技術資訊

ID：zap-10036
類型：HTTP
發現次數：11 處

zap plugin-10036

LOW

#011

Big Redirect Detected (Potential Sensitive Information Leak)

zap-10044 A05:2021

影響網址位置

http://120.126.223.31/login/student

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/10044/

技術資訊

ID：zap-10044
類型：HTTP
發現次數：4 處

zap plugin-10044

LOW

#012

Big Redirect Detected (Potential Sensitive Information Leak)

zap-10044 A05:2021

影響網址位置

http://120.126.223.31/login/manager

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/10044/

技術資訊

ID：zap-10044
類型：HTTP
發現次數：4 處

zap plugin-10044

LOW

#013

Big Redirect Detected (Potential Sensitive Information Leak)

zap-10044 A05:2021

影響網址位置

http://120.126.223.31/login/dedicated_tutor

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/10044/

技術資訊

ID：zap-10044
類型：HTTP
發現次數：4 處

zap plugin-10044

LOW

#014

Big Redirect Detected (Potential Sensitive Information Leak)

zap-10044 A05:2021

影響網址位置

http://120.126.223.31/login/mentor

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/10044/

技術資訊

ID：zap-10044
類型：HTTP
發現次數：4 處

zap plugin-10044

LOW
#015

Cross-Origin-Embedder-Policy Header Missing or Invalid

zap-90004 A05:2021

影響網址位置

http://120.126.223.31/

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：10 處

zap plugin-90004

LOW
#016

Cross-Origin-Embedder-Policy Header Missing or Invalid

zap-90004 A05:2021

影響網址位置

http://120.126.223.31/

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：10 處

zap plugin-90004

LOW
#017

Cross-Origin-Embedder-Policy Header Missing or Invalid

zap-90004 A05:2021

影響網址位置

http://120.126.223.31/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：10 處

zap plugin-90004

LOW
#018

Cross-Origin-Embedder-Policy Header Missing or Invalid

zap-90004 A05:2021

影響網址位置

http://120.126.223.31/css/custom.css

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：10 處

zap plugin-90004

LOW
#019

Cross-Origin-Embedder-Policy Header Missing or Invalid

zap-90004 A05:2021

影響網址位置

http://120.126.223.31/css/jquery.tagsinput-revisited.css

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：10 處

zap plugin-90004