Redmark

2026-11-17

Redmark 弱點掃描報告

Vulnerability Scan Report

掃描目標

執行的掃描

Web 動態弱點掃描、主機/網路弱點掃描、外部曝險弱點掃描

開始掃描時間

2026-11-17 15:39:18(UTC+8)

結束掃描時間

2026-11-17 17:40:31(UTC+8)

103

本次發現弱點數

EXECUTIVE SUMMARY

整體風險概況

103

本次發現弱點數

嚴重	6
高危	39
中危	37
低危	21

掃描結果總結

本次掃描共發現103項弱點，含6項嚴重、39項高危、37項中危、21項低危，整體風險等級為嚴重，應優先修補Adminer相關弱點並限制其管理介面對外存取。

本次共檢出103項弱點，含6項嚴重、39項高危、37項中危、21項低危，整體風險等級為嚴重。嚴重與高危集中於Adminer管理介面多項已知弱點、PHP與AngularJS等疑似含已知弱點元件，以及可被公開存取的.env設定檔，可能造成資料庫帳密、金鑰等敏感資訊遭未授權取得；中危則涵蓋CSP設定不完整、CORS跨網域設定錯誤、缺少Anti-CSRF Token、SMTP明文登入與憑證已過期等，可能降低瀏覽器端防護並增加資料遭不當存取之風險。 整體修補應優先升級並限制Adminer管理介面對外存取，其次更新PHP、AngularJS等疑似含已知弱點元件版本，移除或限制.env等設定檔公開存取並更換可能暴露之帳密金鑰，補強CSP、CORS來源限制與Anti-CSRF Token等瀏覽器防護，調整SMTP加密設定並更新過期憑證，完成後應驗證修補結果並持續監控。

修復路線建議

01 **優先修補Adminer風險**
多項Adminer嚴重與高危弱點對外暴露，應立即升級版本並限制管理介面僅供信任網路存取

02 **更新已知弱點元件**
PHP版本與AngularJS等前端函式庫疑似含已知弱點，應升級至官方已修補版本並確認相依套件

03 **封鎖敏感設定檔外洩**
多個.env設定檔可被公開存取，應移出公開目錄並更換可能暴露之資料庫帳密與金鑰

04 **強化防護並驗證修補**
補強CSP、CORS來源限制與CSRF Token，調整SMTP加密及更新過期憑證，完成後驗證修補結果

VULNERABILITY LIST

弱點列表

弱點名稱	風險等級	首次發現時間
Adminer 低於 4.16.0 版多項弱點	嚴重	2026-11-17 17:40:31
Adminer 低於 4.16.0 版多項弱點	嚴重	2026-11-17 17:40:31
Adminer 低於 4.16.0 版多項弱點	嚴重	2026-11-17 17:40:31
Adminer 低於 4.16.0 版多項弱點	嚴重	2026-11-17 17:40:31
Adminer 低於 4.16.0 版多項弱點	嚴重	2026-11-17 17:40:31
Adminer 低於 4.16.0 版多項弱點	嚴重	2026-11-17 17:40:31
含已知弱點的 JavaScript 函式庫: angular-1.3.8.js	高危	2026-11-17 17:40:31
PHP 版本含已知弱點	高危	2026-11-17 17:40:31
PHP 遠端程式碼執行弱點（PHP2Shell，版本偵測）	高危	2026-11-17 17:40:31
Adminer <= 4.8.1 服務阻斷弱點	高危	2026-11-17 17:40:31
Adminer <= 4.8.1 服務阻斷弱點	高危	2026-11-17 17:40:31
Adminer <= 4.8.1 服務阻斷弱點	高危	2026-11-17 17:40:31
Adminer <= 4.8.1 服務阻斷弱點	高危	2026-11-17 17:40:31
Adminer <= 4.8.1 服務阻斷弱點	高危	2026-11-17 17:40:31
Adminer <= 4.8.1 服務阻斷弱點	高危	2026-11-17 17:40:31

VULNERABILITY LIST

弱點列表

弱點名稱	風險等級	首次發現時間
EasyPHP Webserver 12.1 以下版本多重弱點	高危	2026-11-17 17:40:31
EasyPHP Webserver 12.1 以下版本多重弱點	高危	2026-11-17 17:40:31
EasyPHP Webserver 12.1 以下版本多重弱點	高危	2026-11-17 17:40:31
EasyPHP Webserver 12.1 以下版本多重弱點	高危	2026-11-17 17:40:31
EasyPHP Webserver 12.1 以下版本多重弱點	高危	2026-11-17 17:40:31
EasyPHP Webserver 12.1 以下版本多重弱點	高危	2026-11-17 17:40:31
Laravel 敏感資訊洩露（.env 檔案外洩）	高危	2026-11-17 17:40:31
環境設定檔資訊洩漏	高危	2026-11-17 17:40:31
Adminer 4.6.2 - 5.4.1 未授權永久性服務阻斷弱點	高危	2026-11-17 17:40:31
Adminer 4.6.2 - 5.4.1 未授權永久性服務阻斷弱點	高危	2026-11-17 17:40:31
Adminer 4.6.2 - 5.4.1 未授權永久性服務阻斷弱點	高危	2026-11-17 17:40:31
Adminer 4.6.2 - 5.4.1 未授權永久性服務阻斷弱點	高危	2026-11-17 17:40:31
Adminer 4.6.2 - 5.4.1 未授權永久性服務阻斷弱點	高危	2026-11-17 17:40:31
Adminer 4.6.2 - 5.4.1 未授權永久性服務阻斷弱點	高危	2026-11-17 17:40:31
CodeIgniter .env 設定檔外洩	高危	2026-11-17 17:40:31

VULNERABILITY LIST

弱點列表

弱點名稱	風險等級	首次發現時間
CodeIgniter .env 設定檔外洩	● 高危	2026-11-17 17:40:31
CodeIgniter .env 設定檔外洩	● 高危	2026-11-17 17:40:31
CodeIgniter .env 設定檔外洩	● 高危	2026-11-17 17:40:31
CodeIgniter .env 設定檔外洩	● 高危	2026-11-17 17:40:31
CodeIgniter .env 設定檔外洩	● 高危	2026-11-17 17:40:31
Laravel 敏感資訊洩露（.env 檔案外洩）	● 高危	2026-11-17 17:40:31
Laravel 敏感資訊洩露（.env 檔案外洩）	● 高危	2026-11-17 17:40:31
Laravel 敏感資訊洩露（.env 檔案外洩）	● 高危	2026-11-17 17:40:31
Laravel 敏感資訊洩露（.env 檔案外洩）	● 高危	2026-11-17 17:40:31
Laravel 敏感資訊洩露（.env 檔案外洩）	● 高危	2026-11-17 17:40:31
環境設定檔資訊洩漏	● 高危	2026-11-17 17:40:31
環境設定檔資訊洩漏	● 高危	2026-11-17 17:40:31
環境設定檔資訊洩漏	● 高危	2026-11-17 17:40:31
環境設定檔資訊洩漏	● 高危	2026-11-17 17:40:31
環境設定檔資訊洩漏	● 高危	2026-11-17 17:40:31

VULNERABILITY LIST

弱點列表

弱點名稱	風險等級	首次發現時間
CSP style-src 允許 unsafe-inline	中危	2026-11-17 17:40:31
CSP 未定義無備援機制指令	中危	2026-11-17 17:40:31
CSP 萬用字元指令	中危	2026-11-17 17:40:31
缺少點擊劫持防護 HTTP 標頭	中危	2026-11-17 17:40:31
跨網域設定錯誤	中危	2026-11-17 17:40:31
未設定 Content-Security-Policy（CSP）標頭	中危	2026-11-17 17:40:31
缺少 Anti-CSRF Token	中危	2026-11-17 17:40:31
CSP script-src 允許 unsafe-inline	中危	2026-11-17 17:40:31
SMTP 明文登入未加密弱點	中危	2026-11-17 17:40:31
SMTP 郵件轉寄弱點（簡易測試）	中危	2026-11-17 17:40:31
SSL/TLS 憑證已過期	中危	2026-11-17 17:40:31
phpinfo() 輸出資訊洩露（HTTP）	中危	2026-11-17 17:40:31
phpinfo() 輸出資訊洩露（HTTP）	中危	2026-11-17 17:40:31
phpinfo() 輸出資訊洩露（HTTP）	中危	2026-11-17 17:40:31
phpinfo() 輸出資訊洩露（HTTP）	中危	2026-11-17 17:40:31

VULNERABILITY LIST

弱點列表

弱點名稱	風險等級	首次發現時間
phpinfo() 輸出資訊洩露（HTTP）	中危	2026-11-17 17:40:31
phpinfo() 輸出資訊洩露（HTTP）	中危	2026-11-17 17:40:31
敏感檔案洩漏（HTTP）	中危	2026-11-17 17:40:31
敏感檔案洩漏（HTTP）	中危	2026-11-17 17:40:31
敏感檔案洩漏（HTTP）	中危	2026-11-17 17:40:31
敏感檔案洩漏（HTTP）	中危	2026-11-17 17:40:31
敏感檔案洩漏（HTTP）	中危	2026-11-17 17:40:31
敏感檔案洩漏（HTTP）	中危	2026-11-17 17:40:31
版本控制系統（SCM）檔案／目錄可被存取（HTTP）	中危	2026-11-17 17:40:31
版本控制系統（SCM）檔案／目錄可被存取（HTTP）	中危	2026-11-17 17:40:31
版本控制系統（SCM）檔案／目錄可被存取（HTTP）	中危	2026-11-17 17:40:31
版本控制系統（SCM）檔案／目錄可被存取（HTTP）	中危	2026-11-17 17:40:31
版本控制系統（SCM）檔案／目錄可被存取（HTTP）	中危	2026-11-17 17:40:31
版本控制系統（SCM）檔案／目錄可被存取（HTTP）	中危	2026-11-17 17:40:31
透過 HTTP 明文傳輸敏感資訊	中危	2026-11-17 17:40:31

VULNERABILITY LIST

弱點列表

弱點名稱	風險等級	首次發現時間
Git 設定檔案外洩	中危	2026-11-17 17:40:31
Git 設定檔案外洩	中危	2026-11-17 17:40:31
Git 設定檔案外洩	中危	2026-11-17 17:40:31
Git 設定檔案外洩	中危	2026-11-17 17:40:31
Git 設定檔案外洩	中危	2026-11-17 17:40:31
Git 設定檔案外洩	中危	2026-11-17 17:40:31
開放重新導向（Open Redirect）弱點	中危	2026-11-17 17:40:31
Cookie 未設定 SameSite 屬性	低危	2026-11-17 17:40:31
Cookie 未設定 Secure 屬性	低危	2026-11-17 17:40:31
Server HTTP 回應標頭洩漏版本資訊	低危	2026-11-17 17:40:31
Unix 時間戳記資訊揭露	低危	2026-11-17 17:40:31
X-Powered-By HTTP 回應標頭資訊洩漏	低危	2026-11-17 17:40:31
未設定 Strict-Transport-Security 標頭	低危	2026-11-17 17:40:31
缺少 X-Content-Type-Options 標頭	低危	2026-11-17 17:40:31
頁面橫幅版本資訊洩漏	低危	2026-11-17 17:40:31

VULNERABILITY LIST

弱點列表

弱點名稱	風險等級	首次發現時間
HTTPS 內容可透過 HTTP 存取	低危	2026-11-17 17:40:31
私有 IP 資訊揭露	低危	2026-11-17 17:40:31
ICMP 時間戳記回應資訊洩露	低危	2026-11-17 17:40:31
SSH 支援弱 MAC 演算法	低危	2026-11-17 17:40:31
TCP 時間戳記資訊洩漏	低危	2026-11-17 17:40:31
PHPinfo 資訊洩漏頁面	低危	2026-11-17 17:40:31
PHPinfo 資訊洩漏頁面	低危	2026-11-17 17:40:31
PHPinfo 資訊洩漏頁面	低危	2026-11-17 17:40:31
PHPinfo 資訊洩漏頁面	低危	2026-11-17 17:40:31
PHPinfo 資訊洩漏頁面	低危	2026-11-17 17:40:31
PHPinfo 資訊洩漏頁面	低危	2026-11-17 17:40:31
SSL 憑證過期	低危	2026-11-17 17:40:31
自簽署 SSL 憑證	低危	2026-11-17 17:40:31

CRITICAL

Adminer 低於 4.16.0 版多項弱點

01

風險等級	CVSS	連接埠
● 嚴重	9.8	8080

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

Adminer 4.16.0 之前版本存在多項弱點，包含 SSRF、服務拒絕及檔案上傳問題（CVE-2023-45195/45196/45197）。

修復說明

01 將 Adminer 升級至 4.16.0 或更新版本以修補弱點。

02 限制並管控可存取 Adminer 管理介面的網路來源。

03 升級後請詳細確認是否有自訂修改或擴充套件與新版本產生衝突。

04 升級完成後持續監控系統紀錄，留意異常上傳或可疑請求活動。

修復驗證

- [ ] 確認 Adminer 版本已為 4.16.0 或以上。
- [ ] 測試 SSRF 與上傳相關問題已無法被利用。
- [ ] 重新掃描系統，確認該弱點已不再被偵測到。

修復路徑



先盤點所有受影響的 Adminer 系統範圍，將其升級至已修補的新版本，再重新掃描以確認弱點已完全排除且無殘留風險。

詳細資訊

Installed version: 4.8.1
Fixed version: 4.16.0
Installation path / port: /

CRITICAL

Adminer 低於 4.16.0 版多項弱點

02

風險等級	CVSS	連接埠
● 嚴重	9.8	443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

Adminer 4.16.0 之前版本存在多項弱點，包含 SSRF、服務拒絕及檔案上傳問題（CVE-2023-45195/45196/45197）。

修復說明

01 將 Adminer 升級至 4.16.0 或更新版本以修補弱點。

02 限制並管控可存取 Adminer 管理介面的網路來源。

03 升級後請詳細確認是否有自訂修改或擴充套件與新版本產生衝突。

04 升級完成後持續監控系統紀錄，留意異常上傳或可疑請求活動。

修復驗證

- [ ] 確認 Adminer 版本已為 4.16.0 或以上。
- [ ] 測試 SSRF 與上傳相關問題已無法被利用。
- [ ] 重新掃描系統，確認該弱點已不再被偵測到。

修復路徑



先盤點所有受影響的 Adminer 系統範圍，將其升級至已修補的新版本，再重新掃描以確認弱點已完全排除且無殘留風險。

詳細資訊

Installed version: 4.8.1
Fixed version: 4.16.0
Installation path / port: /

CRITICAL

Adminer 低於 4.16.0 版多項弱點

03

風險等級	CVSS	連接埠
● 嚴重	9.8	10443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

Adminer 4.16.0 之前版本存在多項弱點，包含 SSRF、服務拒絕及檔案上傳問題（CVE-2023-45195/45196/45197）。

修復說明

01 將 Adminer 升級至 4.16.0 或更新版本以修補弱點。

02 限制並管控可存取 Adminer 管理介面的網路來源。

03 升級後請詳細確認是否有自訂修改或擴充套件與新版本產生衝突。

04 升級完成後持續監控系統紀錄，留意異常上傳或可疑請求活動。

修復驗證

- [ ] 確認 Adminer 版本已為 4.16.0 或以上。
- [ ] 測試 SSRF 與上傳相關問題已無法被利用。
- [ ] 重新掃描系統，確認該弱點已不再被偵測到。

修復路徑



先盤點所有受影響的 Adminer 系統範圍，將其升級至已修補的新版本，再重新掃描以確認弱點已完全排除且無殘留風險。

詳細資訊

Installed version: 4.8.1
Fixed version: 4.16.0
Installation path / port: /

CRITICAL

Adminer 低於 4.16.0 版多項弱點

04

風險等級	CVSS	連接埠
● 嚴重	9.8	8443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

Adminer 4.16.0 之前版本存在多項弱點，包含 SSRF、服務拒絕及檔案上傳問題（CVE-2023-45195/45196/45197）。

修復說明

01 將 Adminer 升級至 4.16.0 或更新版本以修補弱點。

02 限制並管控可存取 Adminer 管理介面的網路來源。

03 升級後請詳細確認是否有自訂修改或擴充套件與新版本產生衝突。

04 升級完成後持續監控系統紀錄，留意異常上傳或可疑請求活動。

修復驗證

- [ ] 確認 Adminer 版本已為 4.16.0 或以上。
- [ ] 測試 SSRF 與上傳相關問題已無法被利用。
- [ ] 重新掃描系統，確認該弱點已不再被偵測到。

修復路徑



先盤點所有受影響的 Adminer 系統範圍，將其升級至已修補的新版本，再重新掃描以確認弱點已完全排除且無殘留風險。

詳細資訊

Installed version: 4.8.1
Fixed version: 4.16.0
Installation path / port: /

CRITICAL

Adminer 低於 4.16.0 版多項弱點

05

風險等級	CVSS	連接埠
● 嚴重	9.8	80

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

Adminer 4.16.0 之前版本存在多項弱點，包含 SSRF、服務拒絕及檔案上傳問題（CVE-2023-45195/45196/45197）。

修復說明

01 將 Adminer 升級至 4.16.0 或更新版本以修補弱點。

02 限制並管控可存取 Adminer 管理介面的網路來源。

03 升級後請詳細確認是否有自訂修改或擴充套件與新版本產生衝突。

04 升級完成後持續監控系統紀錄，留意異常上傳或可疑請求活動。

修復驗證

- [ ] 確認 Adminer 版本已為 4.16.0 或以上。
- [ ] 測試 SSRF 與上傳相關問題已無法被利用。
- [ ] 重新掃描系統，確認該弱點已不再被偵測到。

修復路徑



先盤點所有受影響的 Adminer 系統範圍，將其升級至已修補的新版本，再重新掃描以確認弱點已完全排除且無殘留風險。

詳細資訊

Installed version: 4.8.1
Fixed version: 4.16.0
Installation path / port: /

CRITICAL

Adminer 低於 4.16.0 版多項弱點

06

風險等級	CVSS	連接埠
● 嚴重	9.8	9443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

Adminer 4.16.0 之前版本存在多項弱點，包含 SSRF、服務拒絕及檔案上傳問題（CVE-2023-45195/45196/45197）。

修復說明

01 將 Adminer 升級至 4.16.0 或更新版本以修補弱點。

02 限制並管控可存取 Adminer 管理介面的網路來源。

03 升級後請詳細確認是否有自訂修改或擴充套件與新版本產生衝突。

04 升級完成後持續監控系統紀錄，留意異常上傳或可疑請求活動。

修復驗證

- [ ] 確認 Adminer 版本已為 4.16.0 或以上。
- [ ] 測試 SSRF 與上傳相關問題已無法被利用。
- [ ] 重新掃描系統，確認該弱點已不再被偵測到。

修復路徑



先盤點所有受影響的 Adminer 系統範圍，將其升級至已修補的新版本，再重新掃描以確認弱點已完全排除且無殘留風險。

詳細資訊

Installed version: 4.8.1
Fixed version: 4.16.0
Installation path / port: /

HIGH

含已知弱點的 JavaScript 函式庫: angular-1.3.8.js

07

風險等級	OWASP 分類	弱點實例數量
高危	A03:2025 軟體供應鏈失效	6

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

偵測到的 JavaScript 函式庫疑似含有已知弱點，可能帶來相關安全風險。

修復說明

01 確認受影響的 JavaScript 函式庫及目前部署版本。

02 將受影響的函式庫升級至可取得的最新版本，並依官方發行說明完成相依套件更新。

03 完成函式庫更新後，檢視應用程式主要功能與相關整合是否正常運作。

修復驗證

- [ ] 確認受影響函式庫已更新至預定的最新版本。
- [ ] 確認受影響函式庫已更新至預定最新版本，並記錄實際部署的版本資訊。
- [ ] 重新執行弱點掃描，確認不再檢出此項弱點。

修復路徑



先盤點受影響的 JavaScript 函式庫與目前版本，依官方指引升級至最新可用版本；完成部署後測試主要功能及相關整合，再重新掃描確認不再檢出此項弱點。

弱點實例列表 (6/6)

弱點實例	請求方法
[redacted]	GET
[redacted]	GET
[redacted]	GET
[redacted]	GET
[redacted]	GET
[redacted]	GET

HIGH

PHP 版本含已知弱點

08

風險等級	OWASP 分類	弱點實例數量
高危	A03:2025 軟體供應鏈失效	2

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

伺服器透過 HTTP 回應標頭揭露所使用的 PHP 版本，且該版本存在已知弱點，可能被用於辨識並嘗試相應攻擊手法。

修復說明

01 將伺服器所使用的 PHP 版本升級至目前仍受支援且已完成修補的版本。

02 確認所屬作業系統發行版是否已回溯套用相關安全修補程式。

03 於 php.ini 設定 expose_php = Off。

04 調整伺服器設定，隱藏或遮蔽 Server 標頭中的版本資訊。

05 重新啟動網站伺服器服務，以確保設定變更正式套用生效。

修復驗證

- [ ] 確認 HTTP 回應標頭不再顯示 PHP 版本資訊。
- [ ] 檢查已安裝 PHP 版本為受支援且已修補版本。
- [ ] 重新執行弱點掃描，確認此項弱點已不再被偵測到。

修復路徑



先確認所揭露的 PHP 版本與對應標頭來源，再升級 PHP 並關閉版本揭露設定，最後重新掃描以確認弱點已排除且無殘留風險。

弱點實例列表 (2/2)

弱點實例	請求方法
[redacted]	GET
[redacted]	GET

HIGH

PHP 遠端程式碼執行弱點（PHP2Shell，版本偵測）

09

風險等級	OWASP 分類	弱點實例數量
● 高危	A06:2025 不安全設計	1

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

回應標頭顯示 PHP/8.3.35，低於該分支已修補的穩定版本 8.3.36。此結果僅為版本指標，無法確認弱點是否真實存在或可被利用，標頭亦可能不準確或已回溯修補。

修復說明

01 請先確認伺服器上目前實際執行的 PHP 版本編號，以供後續比對。

02 查閱該 PHP 版本分支所對應的官方廠商安全公告內容。

03 將 PHP 升級至 8.3.36 或該分支更新的已修補版本。

04 完成修補升級作業後，請重新啟動所有相關的 PHP 工作程序。

05 暫時將 expose_php 設為 Off 隱藏版本標頭。

修復驗證

- [ ] 確認目前實際執行版本已更新至已修補版本。
- [ ] 檢查回應標頭內容已不再顯示 PHP 版本資訊。
- [ ] 重新執行掃描以確認此弱點已不再被偵測到。

修復路徑



先確認實際 PHP 版本與可用修補，再完成升級或回溯修補並重啟服務，最後重新掃描確認版本指標與標頭皆不再觸發此弱點。

弱點實例列表 (1/1)

弱點實例	請求方法
[redacted]	GET

HIGH

Adminer <= 4.8.1 服務阻斷弱點

10

風險等級	CVSS	連接埠
高危	7.8	10443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

Adminer 在處理特製序列化資料（如 s:1000000000）時會觸發 PHP 物件注入，造成記憶體過度消耗。未經驗證攻擊者可藉此使介面無回應甚至伺服器當機。

修復說明

01 立即將 Adminer 升級至 4.8.2 或更新版本以修補弱點。

02 限制 Adminer 管理介面僅供可信任內部網路存取使用。

03 持續監控伺服器記憶體使用狀況，並留意任何異常飆升情形發生。

04 當服務發生無回應情形時，請立即重新啟動相關服務程序。

修復驗證

- [ ] 確認 Adminer 版本已更新至 4.8.2 以上。
- [ ] 確認僅可信來源能存取 Adminer 介面。
- [ ] 執行重新掃描，確認此弱點已不再被偵測到。

修復路徑



先盤點受影響的 Adminer 環境範圍，升級至修補版本並限制存取來源，最後重新掃描以確認服務阻斷風險已完全排除。

詳細資訊

Installed version: 4.8.1
Fixed version: 4.8.2
Installation path / port: /

HIGH

Adminer <= 4.8.1 服務阻斷弱點

11

風險等級	CVSS	連接埠
高危	7.8	9443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

Adminer 在處理特製序列化資料（如 s:1000000000）時會觸發 PHP 物件注入，造成記憶體過度消耗。未經驗證攻擊者可藉此使介面無回應甚至伺服器當機。

修復說明

01 立即將 Adminer 升級至 4.8.2 或更新版本以修補弱點。

02 限制 Adminer 管理介面僅供可信任內部網路存取使用。

03 持續監控伺服器記憶體使用狀況，並留意任何異常飆升情形發生。

04 當服務發生無回應情形時，請立即重新啟動相關服務程序。

修復驗證

- [ ] 確認 Adminer 版本已更新至 4.8.2 以上。
- [ ] 確認僅可信來源能存取 Adminer 介面。
- [ ] 執行重新掃描，確認此弱點已不再被偵測到。

修復路徑



先盤點受影響的 Adminer 環境範圍，升級至修補版本並限制存取來源，最後重新掃描以確認服務阻斷風險已完全排除。

詳細資訊

Installed version: 4.8.1
Fixed version: 4.8.2
Installation path / port: /

HIGH

Adminer <= 4.8.1 服務阻斷弱點

12

風險等級	CVSS	連接埠
● 高危	7.8	8080

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

Adminer 在處理特製序列化資料（如 s:1000000000）時會觸發 PHP 物件注入，造成記憶體過度消耗。未經驗證攻擊者可藉此使介面無回應甚至伺服器當機。

修復說明

01 立即將 Adminer 升級至 4.8.2 或更新版本以修補弱點。

02 限制 Adminer 管理介面僅供可信任內部網路存取使用。

03 持續監控伺服器記憶體使用狀況，並留意任何異常飆升情形發生。

04 當服務發生無回應情形時，請立即重新啟動相關服務程序。

修復驗證

- [ ] 確認 Adminer 版本已更新至 4.8.2 以上。
- [ ] 確認僅可信來源能存取 Adminer 介面。
- [ ] 執行重新掃描，確認此弱點已不再被偵測到。

修復路徑



先盤點受影響的 Adminer 環境範圍，升級至修補版本並限制存取來源，最後重新掃描以確認服務阻斷風險已完全排除。

詳細資訊

Installed version: 4.8.1
Fixed version: 4.8.2
Installation path / port: /

HIGH

Adminer <= 4.8.1 服務阻斷弱點

13

風險等級	CVSS	連接埠
高危	7.8	8443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

Adminer 在處理特製序列化資料（如 s:1000000000）時會觸發 PHP 物件注入，造成記憶體過度消耗。未經驗證攻擊者可藉此使介面無回應甚至伺服器當機。

修復說明

01 立即將 Adminer 升級至 4.8.2 或更新版本以修補弱點。

02 限制 Adminer 管理介面僅供可信任內部網路存取使用。

03 持續監控伺服器記憶體使用狀況，並留意任何異常飆升情形發生。

04 當服務發生無回應情形時，請立即重新啟動相關服務程序。

修復驗證

- [ ] 確認 Adminer 版本已更新至 4.8.2 以上。
- [ ] 確認僅可信來源能存取 Adminer 介面。
- [ ] 執行重新掃描，確認此弱點已不再被偵測到。

修復路徑



先盤點受影響的 Adminer 環境範圍，升級至修補版本並限制存取來源，最後重新掃描以確認服務阻斷風險已完全排除。

詳細資訊

Installed version: 4.8.1
Fixed version: 4.8.2
Installation path / port: /

HIGH

Adminer <= 4.8.1 服務阻斷弱點

14

風險等級	CVSS	連接埠
● 高危	7.8	80

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

Adminer 在處理特製序列化資料（如 s:1000000000）時會觸發 PHP 物件注入，造成記憶體過度消耗。未經驗證攻擊者可藉此使介面無回應甚至伺服器當機。

修復說明

01 立即將 Adminer 升級至 4.8.2 或更新版本以修補弱點。

02 限制 Adminer 管理介面僅供可信任內部網路存取使用。

03 持續監控伺服器記憶體使用狀況，並留意任何異常飆升情形發生。

04 當服務發生無回應情形時，請立即重新啟動相關服務程序。

修復驗證

- ☐ 確認 Adminer 版本已更新至 4.8.2 以上。
- ☐ 確認僅可信來源能存取 Adminer 介面。
- ☐ 執行重新掃描，確認此弱點已不再被偵測到。

修復路徑



先盤點受影響的 Adminer 環境範圍，升級至修補版本並限制存取來源，最後重新掃描以確認服務阻斷風險已完全排除。

詳細資訊

Installed version: 4.8.1
Fixed version: 4.8.2
Installation path / port: /

HIGH

Adminer <= 4.8.1 服務阻斷弱點

15

風險等級	CVSS	連接埠
● 高危	7.8	443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

Adminer 在處理特製序列化資料（如 s:1000000000）時會觸發 PHP 物件注入，造成記憶體過度消耗。未經驗證攻擊者可藉此使介面無回應甚至伺服器當機。

修復說明

01 立即將 Adminer 升級至 4.8.2 或更新版本以修補弱點。

02 限制 Adminer 管理介面僅供可信任內部網路存取使用。

03 持續監控伺服器記憶體使用狀況，並留意任何異常飆升情形發生。

04 當服務發生無回應情形時，請立即重新啟動相關服務程序。

修復驗證

- [ ] 確認 Adminer 版本已更新至 4.8.2 以上。
- [ ] 確認僅可信來源能存取 Adminer 介面。
- [ ] 執行重新掃描，確認此弱點已不再被偵測到。

修復路徑



先盤點受影響的 Adminer 環境範圍，升級至修補版本並限制存取來源，最後重新掃描以確認服務阻斷風險已完全排除。

詳細資訊

Installed version: 4.8.1
Fixed version: 4.8.2
Installation path / port: /

HIGH

EasyPHP Webserver 12.1 以下版本多重弱點

16

風險等級	CVSS	連接埠
高危	7.5	8080

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

EasyPHP WebServer Manager 對特定請求略過身分驗證，可能導致繞過驗證、資訊外洩或遠端執行 PHP 程式碼，影響 12.1 以下版本。

修復說明

01 將 EasyPHP 升級至廠商已修補且持續支援的最新版本。

02 停用受影響的 WebServer Manager 功能。

03 若廠商至今尚無提供任何修補版本，應立即評估並移除此產品。

04 評估並改用其他持續獲得廠商積極維護的替代軟體產品。

05 限制管理介面之網路連線存取，僅允許受信任來源連入使用。

修復驗證

- [ ] 確認所有管理介面請求皆已強制要求身分驗證。
- [ ] 檢查 EasyPHP 版本已不受此弱點影響。
- [ ] 重新執行掃描，確認此弱點已無法再被偵測到。

修復路徑



先盤點並確認受影響之 EasyPHP 系統範圍，接著進行升級、停用或移除等修復措施，最後重新掃描以確認弱點已完全排除。

詳細資訊

Vulnerable URL:
Concluded from:

```
  <title>PHP 8.3.35 - phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" />
</head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/usr/local/etc/php </td></tr>
```

HIGH

EasyPHP Webserver 12.1 以下版本多重弱點

17

風險等級	CVSS	連接埠
高危	7.5	80

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

EasyPHP WebServer Manager 對特定請求略過身分驗證，可能導致繞過驗證、資訊外洩或遠端執行 PHP 程式碼，影響 12.1 以下版本。

修復說明

01 將 EasyPHP 升級至廠商已修補且持續支援的最新版本。

02 停用受影響的 WebServer Manager 功能。

03 若廠商至今尚無提供任何修補版本，應立即評估並移除此產品。

04 評估並改用其他持續獲得廠商積極維護的替代軟體產品。

05 限制管理介面之網路連線存取，僅允許受信任來源連入使用。

修復驗證

- [ ] 確認所有管理介面請求皆已強制要求身分驗證。
- [ ] 檢查 EasyPHP 版本已不受此弱點影響。
- [ ] 重新執行掃描，確認此弱點已無法再被偵測到。

修復路徑



先盤點並確認受影響之 EasyPHP 系統範圍，接著進行升級、停用或移除等修復措施，最後重新掃描以確認弱點已完全排除。

詳細資訊

Vulnerable URL:
Concluded from:

```
  <title>PHP 8.3.35 - phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" />
</head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/usr/local/etc/php </td></tr>
```

HIGH

EasyPHP Webserver 12.1 以下版本多重弱點

18

風險等級	CVSS	連接埠
高危	7.5	8443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

EasyPHP WebServer Manager 對特定請求略過身分驗證，可能導致繞過驗證、資訊外洩或遠端執行 PHP 程式碼，影響 12.1 以下版本。

修復說明

01 將 EasyPHP 升級至廠商已修補且持續支援的最新版本。

02 停用受影響的 WebServer Manager 功能。

03 若廠商至今尚無提供任何修補版本，應立即評估並移除此產品。

04 評估並改用其他持續獲得廠商積極維護的替代軟體產品。

05 限制管理介面之網路連線存取，僅允許受信任來源連入使用。

修復驗證

- [ ] 確認所有管理介面請求皆已強制要求身分驗證。
- [ ] 檢查 EasyPHP 版本已不受此弱點影響。
- [ ] 重新執行掃描，確認此弱點已無法再被偵測到。

修復路徑



先盤點並確認受影響之 EasyPHP 系統範圍，接著進行升級、停用或移除等修復措施，最後重新掃描以確認弱點已完全排除。

詳細資訊

Vulnerable URL:
Concluded from:

```
  <title>PHP 8.3.35 - phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" />
</head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/usr/local/etc/php </td></tr>
```

HIGH

EasyPHP Webserver 12.1 以下版本多重弱點

19

風險等級	CVSS	連接埠
高危	7.5	10443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

EasyPHP WebServer Manager 對特定請求略過身分驗證，可能導致繞過驗證、資訊外洩或遠端執行 PHP 程式碼，影響 12.1 以下版本。

修復說明

01 將 EasyPHP 升級至廠商已修補且持續支援的最新版本。

02 停用受影響的 WebServer Manager 功能。

03 若廠商至今尚無提供任何修補版本，應立即評估並移除此產品。

04 評估並改用其他持續獲得廠商積極維護的替代軟體產品。

05 限制管理介面之網路連線存取，僅允許受信任來源連入使用。

修復驗證

- [ ] 確認所有管理介面請求皆已強制要求身分驗證。
- [ ] 檢查 EasyPHP 版本已不受此弱點影響。
- [ ] 重新執行掃描，確認此弱點已無法再被偵測到。

修復路徑



先盤點並確認受影響之 EasyPHP 系統範圍，接著進行升級、停用或移除等修復措施，最後重新掃描以確認弱點已完全排除。

詳細資訊

Vulnerable URL:
Concluded from:

```
  <title>PHP 8.3.35 - phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" />
</head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/usr/local/etc/php </td></tr>
```

HIGH

EasyPHP Webserver 12.1 以下版本多重弱點

20

風險等級	CVSS	連接埠
高危	7.5	443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

EasyPHP WebServer Manager 對特定請求略過身分驗證，可能導致繞過驗證、資訊外洩或遠端執行 PHP 程式碼，影響 12.1 以下版本。

修復說明

01 將 EasyPHP 升級至廠商已修補且持續支援的最新版本。

02 停用受影響的 WebServer Manager 功能。

03 若廠商至今尚無提供任何修補版本，應立即評估並移除此產品。

04 評估並改用其他持續獲得廠商積極維護的替代軟體產品。

05 限制管理介面之網路連線存取，僅允許受信任來源連入使用。

修復驗證

- [ ] 確認所有管理介面請求皆已強制要求身分驗證。
- [ ] 檢查 EasyPHP 版本已不受此弱點影響。
- [ ] 重新執行掃描，確認此弱點已無法再被偵測到。

修復路徑



先盤點並確認受影響之 EasyPHP 系統範圍，接著進行升級、停用或移除等修復措施，最後重新掃描以確認弱點已完全排除。

詳細資訊

Vulnerable URL:
Concluded from:
<title>PHP 8.3.35 - phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" />
</head>
<tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/usr/local/etc/php </td></tr>

HIGH

EasyPHP Webserver 12.1 以下版本多重弱點

21

風險等級	CVSS	連接埠
高危	7.5	9443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

EasyPHP WebServer Manager 對特定請求略過身分驗證，可能導致繞過驗證、資訊外洩或遠端執行 PHP 程式碼，影響 12.1 以下版本。

修復說明

01 將 EasyPHP 升級至廠商已修補且持續支援的最新版本。

02 停用受影響的 WebServer Manager 功能。

03 若廠商至今尚無提供任何修補版本，應立即評估並移除此產品。

04 評估並改用其他持續獲得廠商積極維護的替代軟體產品。

05 限制管理介面之網路連線存取，僅允許受信任來源連入使用。

修復驗證

- [ ] 確認所有管理介面請求皆已強制要求身分驗證。
- [ ] 檢查 EasyPHP 版本已不受此弱點影響。
- [ ] 重新執行掃描，確認此弱點已無法再被偵測到。

修復路徑



先盤點並確認受影響之 EasyPHP 系統範圍，接著進行升級、停用或移除等修復措施，最後重新掃描以確認弱點已完全排除。

詳細資訊

Vulnerable URL:
Concluded from:

```
  <title>PHP 8.3.35 - phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" />
</head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/usr/local/etc/php </td></tr>
```

HIGH

Laravel 敏感資訊洩露（.env 檔案外洩）

22

風險等級	CVSS	CWE ID
高危	8.3	CWE-522

連接埠	首次發現時間	最近發現時間
80	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

系統可被公開存取 Laravel 的 .env 檔案，其中儲存資料庫帳密與金鑰等敏感資訊，可能遭未授權取得。

修復說明

01 將 Laravel 專案中的 .env 檔案移出網站伺服器的公開存取目錄之外。

02 於網站伺服器設定中新增規則，禁止外部直接存取 .env 檔案內容。

03 立即更換檔案中曾經外洩的所有資料庫帳密與金鑰資訊。

04 停用應用程式根目錄與相關子目錄的目錄列表顯示功能。

修復驗證

- [ ] 嘗試直接存取 .env 檔案路徑，確認請求已被伺服器拒絕。
- [ ] 檢查移動後的檔案新位置，確認無法由外部網路存取。
- [ ] 重新執行弱點掃描，確認此項弱點已不再出現於報告中。

修復路徑



先確認 .env 檔案於伺服器上的實際外洩位置與範圍，接著限制外部存取並更換所有已外洩之憑證資訊，最後重新掃描以確認該檔案已無法再被公開取得。

命中位置列表 (3/3)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

HIGH

環境設定檔資訊洩漏

23

風險等級	CVSS	CWE ID
● 高危	8.3	CWE-552

連接埠	首次發現時間	最近發現時間
80	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

系統中的 .env 設定檔可被公開存取，其內含資料庫帳密與權杖等敏感資訊，可能遭未授權人員取得並用於存取相關系統。

修復說明

01 將 .env 檔案移出網站伺服器的公開存取目錄，或直接將其刪除。

02 設定網站伺服器規則，禁止外部存取點號開頭的隱藏檔案。

03 立即更換並撤銷已外洩的資料庫帳密與權杖等所有憑證。

04 確認部署流程不會將 .env 檔案納入可公開存取的目錄中。

修復驗證

- [ ] 嘗試存取 .env 檔案網址，確認已無法讀取。
- [ ] 檢查網站伺服器設定，確認已限制點號開頭檔案的存取權限。
- [ ] 重新執行弱點掃描確認該弱點已不再被檢出。

修復路徑



先確認 .env 檔案於伺服器上的曝露位置與範圍，再移除公開存取權限並更換相關憑證，最後重新掃描確認檔案已無法被外部取得。

命中位置列表 (3/3)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

HIGH

Adminer 4.6.2 - 5.4.1 未授權永久性服務阻斷弱點

24

風險等級	CVSS	CWE ID
高危	7.5	CWE-20

連接埠	首次發現時間	最近發現時間
9443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

受影響版本的 Adminer 存在缺陷，未經驗證的攻擊者可觸發永久性服務阻斷狀況，導致服務無法正常使用。

修復說明

01 立即將 Adminer 升級至 5.4.2 或更新版本以修補此弱點。

02 設定存取控制，僅允許信任內部網路連線至 Adminer。

03 持續監控 Adminer 服務可用性，留意任何異常中斷情形。

04 若無法立即升級，暫時停用 Adminer 作為臨時措施。

修復驗證

- [ ] 確認已安裝之 Adminer 版本為 5.4.2 或以上。
- [ ] 驗證正常存取情況下 Adminer 服務維持可用。
- [ ] 重新執行弱點掃描，確認此弱點已不再被偵測到。

修復路徑



先盤點所有受影響之 Adminer 系統，將其升級至修補版本或限制網路存取，再重新掃描確認服務阻斷問題已完全排除。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
	2026-11-17 17:40:31	2026-11-17 17:40:31

HIGH

Adminer 4.6.2 - 5.4.1 未授權永久性服務阻斷弱點

25

風險等級	CVSS	CWE ID
高危	7.5	CWE-20

連接埠	首次發現時間	最近發現時間
8080	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

受影響版本的 Adminer 存在缺陷，未經驗證的攻擊者可觸發永久性服務阻斷狀況，導致服務無法正常使用。

修復說明

01 立即將 Adminer 升級至 5.4.2 或更新版本以修補此弱點。

02 設定存取控制，僅允許信任內部網路連線至 Adminer。

03 持續監控 Adminer 服務可用性，留意任何異常中斷情形。

04 若無法立即升級，暫時停用 Adminer 作為臨時措施。

修復驗證

- [ ] 確認已安裝之 Adminer 版本為 5.4.2 或以上。
- [ ] 驗證正常存取情況下 Adminer 服務維持可用。
- [ ] 重新執行弱點掃描，確認此弱點已不再被偵測到。

修復路徑



先盤點所有受影響之 Adminer 系統，將其升級至修補版本或限制網路存取，再重新掃描確認服務阻斷問題已完全排除。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
	2026-11-17 17:40:31	2026-11-17 17:40:31

HIGH

Adminer 4.6.2 - 5.4.1 未授權永久性服務阻斷弱點

26

風險等級	CVSS	CWE ID
高危	7.5	CWE-20

連接埠	首次發現時間	最近發現時間
10443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

受影響版本的 Adminer 存在缺陷，未經驗證的攻擊者可觸發永久性服務阻斷狀況，導致服務無法正常使用。

修復說明

01 立即將 Adminer 升級至 5.4.2 或更新版本以修補此弱點。

02 設定存取控制，僅允許信任內部網路連線至 Adminer。

03 持續監控 Adminer 服務可用性，留意任何異常中斷情形。

04 若無法立即升級，暫時停用 Adminer 作為臨時措施。

修復驗證

- [ ] 確認已安裝之 Adminer 版本為 5.4.2 或以上。
- [ ] 驗證正常存取情況下 Adminer 服務維持可用。
- [ ] 重新執行弱點掃描，確認此弱點已不再被偵測到。

修復路徑



先盤點所有受影響之 Adminer 系統，將其升級至修補版本或限制網路存取，再重新掃描確認服務阻斷問題已完全排除。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

HIGH

Adminer 4.6.2 - 5.4.1 未授權永久性服務阻斷弱點

27

風險等級	CVSS	CWE ID
高危	7.5	CWE-20

連接埠	首次發現時間	最近發現時間
443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

受影響版本的 Adminer 存在缺陷，未經驗證的攻擊者可觸發永久性服務阻斷狀況，導致服務無法正常使用。

修復說明

01 立即將 Adminer 升級至 5.4.2 或更新版本以修補此弱點。

02 設定存取控制，僅允許信任內部網路連線至 Adminer。

03 持續監控 Adminer 服務可用性，留意任何異常中斷情形。

04 若無法立即升級，暫時停用 Adminer 作為臨時措施。

修復驗證

- [ ] 確認已安裝之 Adminer 版本為 5.4.2 或以上。
- [ ] 驗證正常存取情況下 Adminer 服務維持可用。
- [ ] 重新執行弱點掃描，確認此弱點已不再被偵測到。

修復路徑



先盤點所有受影響之 Adminer 系統，將其升級至修補版本或限制網路存取，再重新掃描確認服務阻斷問題已完全排除。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
	2026-11-17 17:40:31	2026-11-17 17:40:31

HIGH

Adminer 4.6.2 - 5.4.1 未授權永久性服務阻斷弱點

28

風險等級	CVSS	CWE ID
高危	7.5	CWE-20

連接埠	首次發現時間	最近發現時間
80	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

受影響版本的 Adminer 存在缺陷，未經驗證的攻擊者可觸發永久性服務阻斷狀況，導致服務無法正常使用。

修復說明

01 立即將 Adminer 升級至 5.4.2 或更新版本以修補此弱點。

02 設定存取控制，僅允許信任內部網路連線至 Adminer。

03 持續監控 Adminer 服務可用性，留意任何異常中斷情形。

04 若無法立即升級，暫時停用 Adminer 作為臨時措施。

修復驗證

- [ ] 確認已安裝之 Adminer 版本為 5.4.2 或以上。
- [ ] 驗證正常存取情況下 Adminer 服務維持可用。
- [ ] 重新執行弱點掃描，確認此弱點已不再被偵測到。

修復路徑



先盤點所有受影響之 Adminer 系統，將其升級至修補版本或限制網路存取，再重新掃描確認服務阻斷問題已完全排除。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
	2026-11-17 17:40:31	2026-11-17 17:40:31

HIGH

Adminer 4.6.2 - 5.4.1 未授權永久性服務阻斷弱點

29

風險等級	CVSS	CWE ID
高危	7.5	CWE-20

連接埠	首次發現時間	最近發現時間
8443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

受影響版本的 Adminer 存在缺陷，未經驗證的攻擊者可觸發永久性服務阻斷狀況，導致服務無法正常使用。

修復說明

01 立即將 Adminer 升級至 5.4.2 或更新版本以修補此弱點。

02 設定存取控制，僅允許信任內部網路連線至 Adminer。

03 持續監控 Adminer 服務可用性，留意任何異常中斷情形。

04 若無法立即升級，暫時停用 Adminer 作為臨時措施。

修復驗證

- [ ] 確認已安裝之 Adminer 版本為 5.4.2 或以上。
- [ ] 驗證正常存取情況下 Adminer 服務維持可用。
- [ ] 重新執行弱點掃描，確認此弱點已不再被偵測到。

修復路徑



先盤點所有受影響之 Adminer 系統，將其升級至修補版本或限制網路存取，再重新掃描確認服務阻斷問題已完全排除。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
	2026-11-17 17:40:31	2026-11-17 17:40:31

HIGH

CodeIgniter .env 設定檔外洩

30

風險等級	CVSS	CWE ID
高危	—	CWE-552

連接埠	首次發現時間	最近發現時間
8443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

掃描發現可公開存取的 CodeIgniter .env 設定檔，該檔案通常存有資料庫帳密、API 金鑰等敏感設定，可能遭未授權人員取得。

修復說明

01 將 .env 設定檔案移出網站根目錄或任何可公開存取的目錄範圍。

02 於網站伺服器設定規則中，封鎖外部對 .env 檔案的任何存取請求。

03 立即更換檔案內已外洩的資料庫帳密、API 金鑰等敏感資訊。

04 嚴格限制檔案存取權限，僅允許授權系統帳戶讀取該檔案。

05 檢查並調整部署流程，確保 .env 檔案不會被放入公開目錄。

修復驗證

- [ ] 直接存取該 .env 網址，確認已遭拒絕存取。
- [ ] 檢視伺服器設定，確認已封鎖 .env 檔案存取。
- [ ] 重新掃描目標系統，確認該 .env 檔案已無法被外部發現。

修復路徑



先確認 .env 檔案外洩的實際位置，移除檔案或封鎖存取並更換已外洩的金鑰資訊，再重新掃描確認檔案已無法被公開存取。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

HIGH

CodeIgniter .env 設定檔外洩

31

風險等級	CVSS	CWE ID
高危	—	CWE-552

連接埠	首次發現時間	最近發現時間
8080	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

掃描發現可公開存取的 CodeIgniter .env 設定檔，該檔案通常存有資料庫帳密、API 金鑰等敏感設定，可能遭未授權人員取得。

修復說明

01 將 .env 設定檔案移出網站根目錄或任何可公開存取的目錄範圍。

02 於網站伺服器設定規則中，封鎖外部對 .env 檔案的任何存取請求。

03 立即更換檔案內已外洩的資料庫帳密、API 金鑰等敏感資訊。

04 嚴格限制檔案存取權限，僅允許授權系統帳戶讀取該檔案。

05 檢查並調整部署流程，確保 .env 檔案不會被放入公開目錄。

修復驗證

- [ ] 直接存取該 .env 網址，確認已遭拒絕存取。
- [ ] 檢視伺服器設定，確認已封鎖 .env 檔案存取。
- [ ] 重新掃描目標系統，確認該 .env 檔案已無法被外部發現。

修復路徑



先確認 .env 檔案外洩的實際位置，移除檔案或封鎖存取並更換已外洩的金鑰資訊，再重新掃描確認檔案已無法被公開存取。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

HIGH

CodeIgniter .env 設定檔外洩

32

風險等級	CVSS	CWE ID
高危	—	CWE-552

連接埠	首次發現時間	最近發現時間
9443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

掃描發現可公開存取的 CodeIgniter .env 設定檔，該檔案通常存有資料庫帳密、API 金鑰等敏感設定，可能遭未授權人員取得。

修復說明

01 將 .env 設定檔案移出網站根目錄或任何可公開存取的目錄範圍。

02 於網站伺服器設定規則中，封鎖外部對 .env 檔案的任何存取請求。

03 立即更換檔案內已外洩的資料庫帳密、API 金鑰等敏感資訊。

04 嚴格限制檔案存取權限，僅允許授權系統帳戶讀取該檔案。

05 檢查並調整部署流程，確保 .env 檔案不會被放入公開目錄。

修復驗證

- [ ] 直接存取該 .env 網址，確認已遭拒絕存取。
- [ ] 檢視伺服器設定，確認已封鎖 .env 檔案存取。
- [ ] 重新掃描目標系統，確認該 .env 檔案已無法被外部發現。

修復路徑



先確認 .env 檔案外洩的實際位置，移除檔案或封鎖存取並更換已外洩的金鑰資訊，再重新掃描確認檔案已無法被公開存取。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

HIGH

CodeIgniter .env 設定檔外洩

33

風險等級	CVSS	CWE ID
高危	—	CWE-552

連接埠	首次發現時間	最近發現時間
443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

掃描發現可公開存取的 CodeIgniter .env 設定檔，該檔案通常存有資料庫帳密、API 金鑰等敏感設定，可能遭未授權人員取得。

修復說明

01 將 .env 設定檔案移出網站根目錄或任何可公開存取的目錄範圍。

02 於網站伺服器設定規則中，封鎖外部對 .env 檔案的任何存取請求。

03 立即更換檔案內已外洩的資料庫帳密、API 金鑰等敏感資訊。

04 嚴格限制檔案存取權限，僅允許授權系統帳戶讀取該檔案。

05 檢查並調整部署流程，確保 .env 檔案不會被放入公開目錄。

修復驗證

- [ ] 直接存取該 .env 網址，確認已遭拒絕存取。
- [ ] 檢視伺服器設定，確認已封鎖 .env 檔案存取。
- [ ] 重新掃描目標系統，確認該 .env 檔案已無法被外部發現。

修復路徑



先確認 .env 檔案外洩的實際位置，移除檔案或封鎖存取並更換已外洩的金鑰資訊，再重新掃描確認檔案已無法被公開存取。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

HIGH

CodeIgniter .env 設定檔外洩

34

風險等級	CVSS	CWE ID
高危	—	CWE-552

連接埠	首次發現時間	最近發現時間
80	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

掃描發現可公開存取的 CodeIgniter .env 設定檔，該檔案通常存有資料庫帳密、API 金鑰等敏感設定，可能遭未授權人員取得。

修復說明

01 將 .env 設定檔案移出網站根目錄或任何可公開存取的目錄範圍。

02 於網站伺服器設定規則中，封鎖外部對 .env 檔案的任何存取請求。

03 立即更換檔案內已外洩的資料庫帳密、API 金鑰等敏感資訊。

04 嚴格限制檔案存取權限，僅允許授權系統帳戶讀取該檔案。

05 檢查並調整部署流程，確保 .env 檔案不會被放入公開目錄。

修復驗證

- [ ] 直接存取該 .env 網址，確認已遭拒絕存取。
- [ ] 檢視伺服器設定，確認已封鎖 .env 檔案存取。
- [ ] 重新掃描目標系統，確認該 .env 檔案已無法被外部發現。

修復路徑



先確認 .env 檔案外洩的實際位置，移除檔案或封鎖存取並更換已外洩的金鑰資訊，再重新掃描確認檔案已無法被公開存取。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

HIGH

CodeIgniter .env 設定檔外洩

35

風險等級	CVSS	CWE ID
高危	—	CWE-552

連接埠	首次發現時間	最近發現時間
10443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

掃描發現可公開存取的 CodeIgniter .env 設定檔，該檔案通常存有資料庫帳密、API 金鑰等敏感設定，可能遭未授權人員取得。

修復說明

01 將 .env 設定檔案移出網站根目錄或任何可公開存取的目錄範圍。

02 於網站伺服器設定規則中，封鎖外部對 .env 檔案的任何存取請求。

03 立即更換檔案內已外洩的資料庫帳密、API 金鑰等敏感資訊。

04 嚴格限制檔案存取權限，僅允許授權系統帳戶讀取該檔案。

05 檢查並調整部署流程，確保 .env 檔案不會被放入公開目錄。

修復驗證

- [ ] 直接存取該 .env 網址，確認已遭拒絕存取。
- [ ] 檢視伺服器設定，確認已封鎖 .env 檔案存取。
- [ ] 重新掃描目標系統，確認該 .env 檔案已無法被外部發現。

修復路徑



先確認 .env 檔案外洩的實際位置，移除檔案或封鎖存取並更換已外洩的金鑰資訊，再重新掃描確認檔案已無法被公開存取。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

HIGH

Laravel 敏感資訊洩露（.env 檔案外洩）

36

風險等級	CVSS	CWE ID
高危	8.3	CWE-522

連接埠	首次發現時間	最近發現時間
8443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

系統可被公開存取 Laravel 的 .env 檔案，其中儲存資料庫帳密與金鑰等敏感資訊，可能遭未授權取得。

修復說明

01 將 Laravel 專案中的 .env 檔案移出網站伺服器的公開存取目錄之外。

02 於網站伺服器設定中新增規則，禁止外部直接存取 .env 檔案內容。

03 立即更換檔案中曾經外洩的所有資料庫帳密與金鑰資訊。

04 停用應用程式根目錄與相關子目錄的目錄列表顯示功能。

修復驗證

- [ ] 嘗試直接存取 .env 檔案路徑，確認請求已被伺服器拒絕。
- [ ] 檢查移動後的檔案新位置，確認無法由外部網路存取。
- [ ] 重新執行弱點掃描，確認此項弱點已不再出現於報告中。

修復路徑



先確認 .env 檔案於伺服器上的實際外洩位置與範圍，接著限制外部存取並更換所有已外洩之憑證資訊，最後重新掃描以確認該檔案已無法再被公開取得。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

HIGH

Laravel 敏感資訊洩露（.env 檔案外洩）

37

風險等級	CVSS	CWE ID
高危	8.3	CWE-522

連接埠	首次發現時間	最近發現時間
8080	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

系統可被公開存取 Laravel 的 .env 檔案，其中儲存資料庫帳密與金鑰等敏感資訊，可能遭未授權取得。

修復說明

01 將 Laravel 專案中的 .env 檔案移出網站伺服器的公開存取目錄之外。

02 於網站伺服器設定中新增規則，禁止外部直接存取 .env 檔案內容。

03 立即更換檔案中曾經外洩的所有資料庫帳密與金鑰資訊。

04 停用應用程式根目錄與相關子目錄的目錄列表顯示功能。

修復驗證

- [ ] 嘗試直接存取 .env 檔案路徑，確認請求已被伺服器拒絕。
- [ ] 檢查移動後的檔案新位置，確認無法由外部網路存取。
- [ ] 重新執行弱點掃描，確認此項弱點已不再出現於報告中。

修復路徑



先確認 .env 檔案於伺服器上的實際外洩位置與範圍，接著限制外部存取並更換所有已外洩之憑證資訊，最後重新掃描以確認該檔案已無法再被公開取得。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

HIGH

Laravel 敏感資訊洩露（.env 檔案外洩）

38

風險等級	CVSS	CWE ID
● 高危	8.3	CWE-522
連接埠	**首次發現時間**	**最近發現時間**
443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

系統可被公開存取 Laravel 的 .env 檔案，其中儲存資料庫帳密與金鑰等敏感資訊，可能遭未授權取得。

修復說明

01 將 Laravel 專案中的 .env 檔案移出網站伺服器的公開存取目錄之外。

02 於網站伺服器設定中新增規則，禁止外部直接存取 .env 檔案內容。

03 立即更換檔案中曾經外洩的所有資料庫帳密與金鑰資訊。

04 停用應用程式根目錄與相關子目錄的目錄列表顯示功能。

修復驗證

- [ ] 嘗試直接存取 .env 檔案路徑，確認請求已被伺服器拒絕。
- [ ] 檢查移動後的檔案新位置，確認無法由外部網路存取。
- [ ] 重新執行弱點掃描，確認此項弱點已不再出現於報告中。

修復路徑



先確認 .env 檔案於伺服器上的實際外洩位置與範圍，接著限制外部存取並更換所有已外洩之憑證資訊，最後重新掃描以確認該檔案已無法再被公開取得。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

HIGH

Laravel 敏感資訊洩露（.env 檔案外洩）

39

風險等級	CVSS	CWE ID
高危	8.3	CWE-522

連接埠	首次發現時間	最近發現時間
10443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

系統可被公開存取 Laravel 的 .env 檔案，其中儲存資料庫帳密與金鑰等敏感資訊，可能遭未授權取得。

修復說明

01 將 Laravel 專案中的 .env 檔案移出網站伺服器的公開存取目錄之外。

02 於網站伺服器設定中新增規則，禁止外部直接存取 .env 檔案內容。

03 立即更換檔案中曾經外洩的所有資料庫帳密與金鑰資訊。

04 停用應用程式根目錄與相關子目錄的目錄列表顯示功能。

修復驗證

- [ ] 嘗試直接存取 .env 檔案路徑，確認請求已被伺服器拒絕。
- [ ] 檢查移動後的檔案新位置，確認無法由外部網路存取。
- [ ] 重新執行弱點掃描，確認此項弱點已不再出現於報告中。

修復路徑



先確認 .env 檔案於伺服器上的實際外洩位置與範圍，接著限制外部存取並更換所有已外洩之憑證資訊，最後重新掃描以確認該檔案已無法再被公開取得。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

HIGH

Laravel 敏感資訊洩露（.env 檔案外洩）

40

風險等級	CVSS	CWE ID
高危	8.3	CWE-522

連接埠	首次發現時間	最近發現時間
9443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

系統可被公開存取 Laravel 的 .env 檔案，其中儲存資料庫帳密與金鑰等敏感資訊，可能遭未授權取得。

修復說明

01 將 Laravel 專案中的 .env 檔案移出網站伺服器的公開存取目錄之外。

02 於網站伺服器設定中新增規則，禁止外部直接存取 .env 檔案內容。

03 立即更換檔案中曾經外洩的所有資料庫帳密與金鑰資訊。

04 停用應用程式根目錄與相關子目錄的目錄列表顯示功能。

修復驗證

- [ ] 嘗試直接存取 .env 檔案路徑，確認請求已被伺服器拒絕。
- [ ] 檢查移動後的檔案新位置，確認無法由外部網路存取。
- [ ] 重新執行弱點掃描，確認此項弱點已不再出現於報告中。

修復路徑



先確認 .env 檔案於伺服器上的實際外洩位置與範圍，接著限制外部存取並更換所有已外洩之憑證資訊，最後重新掃描以確認該檔案已無法再被公開取得。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

HIGH

環境設定檔資訊洩漏

41

風險等級	CVSS	CWE ID
高危	8.3	CWE-552

連接埠	首次發現時間	最近發現時間
9443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

系統中的 .env 設定檔可被公開存取，其內含資料庫帳密與權杖等敏感資訊，可能遭未授權人員取得並用於存取相關系統。

修復說明

01 將 .env 檔案移出網站伺服器的公開存取目錄，或直接將其刪除。

02 設定網站伺服器規則，禁止外部存取點號開頭的隱藏檔案。

03 立即更換並撤銷已外洩的資料庫帳密與權杖等所有憑證。

04 確認部署流程不會將 .env 檔案納入可公開存取的目錄中。

修復驗證

- [ ] 嘗試存取 .env 檔案網址，確認已無法讀取。
- [ ] 檢查網站伺服器設定，確認已限制點號開頭檔案的存取權限。
- [ ] 重新執行弱點掃描確認該弱點已不再被檢出。

修復路徑



先確認 .env 檔案於伺服器上的曝露位置與範圍，再移除公開存取權限並更換相關憑證，最後重新掃描確認檔案已無法被外部取得。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

HIGH

環境設定檔資訊洩漏

42

風險等級	CVSS	CWE ID
高危	8.3	CWE-552

連接埠	首次發現時間	最近發現時間
8443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

系統中的 .env 設定檔可被公開存取，其內含資料庫帳密與權杖等敏感資訊，可能遭未授權人員取得並用於存取相關系統。

修復說明

01 將 .env 檔案移出網站伺服器的公開存取目錄，或直接將其刪除。

02 設定網站伺服器規則，禁止外部存取點號開頭的隱藏檔案。

03 立即更換並撤銷已外洩的資料庫帳密與權杖等所有憑證。

04 確認部署流程不會將 .env 檔案納入可公開存取的目錄中。

修復驗證

- [ ] 嘗試存取 .env 檔案網址，確認已無法讀取。
- [ ] 檢查網站伺服器設定，確認已限制點號開頭檔案的存取權限。
- [ ] 重新執行弱點掃描確認該弱點已不再被檢出。

修復路徑



先確認 .env 檔案於伺服器上的曝露位置與範圍，再移除公開存取權限並更換相關憑證，最後重新掃描確認檔案已無法被外部取得。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

HIGH

環境設定檔資訊洩漏

43

風險等級	CVSS	CWE ID
● 高危	8.3	CWE-552

連接埠	首次發現時間	最近發現時間
10443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

系統中的 .env 設定檔可被公開存取，其內含資料庫帳密與權杖等敏感資訊，可能遭未授權人員取得並用於存取相關系統。

修復說明

01 將 .env 檔案移出網站伺服器的公開存取目錄，或直接將其刪除。

02 設定網站伺服器規則，禁止外部存取點號開頭的隱藏檔案。

03 立即更換並撤銷已外洩的資料庫帳密與權杖等所有憑證。

04 確認部署流程不會將 .env 檔案納入可公開存取的目錄中。

修復驗證

- [ ] 嘗試存取 .env 檔案網址，確認已無法讀取。
- [ ] 檢查網站伺服器設定，確認已限制點號開頭檔案的存取權限。
- [ ] 重新執行弱點掃描確認該弱點已不再被檢出。

修復路徑



先確認 .env 檔案於伺服器上的曝露位置與範圍，再移除公開存取權限並更換相關憑證，最後重新掃描確認檔案已無法被外部取得。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

HIGH

環境設定檔資訊洩漏

44

風險等級	CVSS	CWE ID
高危	8.3	CWE-552

連接埠	首次發現時間	最近發現時間
443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

系統中的 .env 設定檔可被公開存取，其內含資料庫帳密與權杖等敏感資訊，可能遭未授權人員取得並用於存取相關系統。

修復說明

01 將 .env 檔案移出網站伺服器的公開存取目錄，或直接將其刪除。

02 設定網站伺服器規則，禁止外部存取點號開頭的隱藏檔案。

03 立即更換並撤銷已外洩的資料庫帳密與權杖等所有憑證。

04 確認部署流程不會將 .env 檔案納入可公開存取的目錄中。

修復驗證

- [ ] 嘗試存取 .env 檔案網址，確認已無法讀取。
- [ ] 檢查網站伺服器設定，確認已限制點號開頭檔案的存取權限。
- [ ] 重新執行弱點掃描確認該弱點已不再被檢出。

修復路徑



先確認 .env 檔案於伺服器上的曝露位置與範圍，再移除公開存取權限並更換相關憑證，最後重新掃描確認檔案已無法被外部取得。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

HIGH

環境設定檔資訊洩漏

45

風險等級	CVSS	CWE ID
高危	8.3	CWE-552

連接埠	首次發現時間	最近發現時間
8080	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

系統中的 .env 設定檔可被公開存取，其內含資料庫帳密與權杖等敏感資訊，可能遭未授權人員取得並用於存取相關系統。

修復說明

01 將 .env 檔案移出網站伺服器的公開存取目錄，或直接將其刪除。

02 設定網站伺服器規則，禁止外部存取點號開頭的隱藏檔案。

03 立即更換並撤銷已外洩的資料庫帳密與權杖等所有憑證。

04 確認部署流程不會將 .env 檔案納入可公開存取的目錄中。

修復驗證

- [ ] 嘗試存取 .env 檔案網址，確認已無法讀取。
- [ ] 檢查網站伺服器設定，確認已限制點號開頭檔案的存取權限。
- [ ] 重新執行弱點掃描確認該弱點已不再被檢出。

修復路徑



先確認 .env 檔案於伺服器上的曝露位置與範圍，再移除公開存取權限並更換相關憑證，最後重新掃描確認檔案已無法被外部取得。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

MEDIUM

CSP style-src 允許 unsafe-inline

46

風險等級	OWASP 分類	弱點實例數量
中危	A02:2025 安全設定錯誤	5

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

CSP 的 style-src 指令包含 unsafe-inline，允許內嵌樣式，降低 CSP 對核准樣式來源的限制。

修復說明

01 確認受影響回應及其目前的 Content-Security-Policy 標頭設定。

02 自 Content-Security-Policy 的 style-src 指令移除 unsafe-inline。

03 依實際需求於 style-src 僅保留必要且核准的樣式來源。

修復驗證

- [ ] 檢查回應標頭，確認 style-src 未含 unsafe-inline 且僅列出核准來源。
- [ ] 重新執行弱點掃描，確認系統不再檢出此弱點。

修復路徑



先確認受影響回應與既有 CSP 設定，再調整 style-src 的核准樣式來源，最後透過標頭檢查與重掃確認不再檢出該設定問題。

弱點實例列表 (5/5)

弱點實例	請求方法
[redacted]	GET
[redacted]	GET
[redacted]	GET
[redacted]	GET
[redacted]	GET

MEDIUM

CSP 未定義無備援機制指令

47

風險等級	OWASP 分類	弱點實例數量
中危	A02:2025 安全設定錯誤	5

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

Content Security Policy 未定義沒有備援機制的指令；遺漏或排除該指令等同允許任何內容。

修復說明

01 盤點現行 CSP 中未定義且沒有備援機制的指令及其受影響頁面。

02 於 Content-Security-Policy 標頭明確定義各已識別指令。

03 將更新後的 CSP 標頭設定一致套用至所有受影響的網站回應。

修復驗證

- [ ] 檢查受影響回應的 CSP 標頭，確認已包含原缺漏指令。
- [ ] 重新執行弱點掃描，確認不再檢出此 CSP 弱點。

修復路徑



先確認 CSP 中缺少的無備援指令，再於 Content-Security-Policy 標頭明確定義並套用設定，最後透過回應檢查與重掃確認不再檢出弱點。

弱點實例列表 (5/5)

弱點實例	請求方法
[redacted]	GET
[redacted]	GET
[redacted]	GET
[redacted]	GET
[redacted]	GET

MEDIUM

CSP 萬用字元指令

48

風險等級	OWASP 分類	弱點實例數量
中危	A02:2025 安全設定錯誤	5

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

CSP 包含萬用字元指令，允許從廣泛來源載入內容，可能降低政策限制效果。

修復說明

01 檢視 CSP 各項指令，識別使用萬用字元的內容來源設定。

02 將萬用字元值替換為各受影響指令明確核准的來源清單。

03 設定 Content-Security-Policy 標頭，於適用回應套用修訂後的指令值。

修復驗證

- [ ] 檢查回應標頭，確認修訂後指令未包含萬用字元值。
- [ ] 重新執行弱點掃描，確認不再檢出此項弱點。

修復路徑



先確認 CSP 中萬用字元的適用範圍，再以明確核准來源修訂指令並套用標頭，最後透過回應檢查及重掃確認弱點不再檢出。

弱點實例列表 (5/5)

弱點實例	請求方法
[redacted]	GET
[redacted]	GET
[redacted]	GET
[redacted]	GET
[redacted]	GET

MEDIUM

缺少點擊劫持防護 HTTP 標頭

49

風險等級	OWASP 分類	弱點實例數量
中危	A02:2025 安全設定錯誤	5

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

回應未提供點擊劫持防護，應設定 Content-Security-Policy 的 frame-ancestors 指令或 X-Frame-Options HTTP 標頭。

修復說明

01 盤點網站或應用程式所回傳的全部網頁回應與處理範圍項目。

02 於所有網頁回應設定 Content-Security-Policy 的 frame-ancestors 指令。

03 依頁面嵌入需求設定適當的 frame-ancestors 存取來源。

04 無法使用 CSP 時，於所有網頁回應設定 X-Frame-Options 標頭。

修復驗證

- [ ] 檢查各網頁回應均含 frame-ancestors 或 X-Frame-Options 標頭。
- [ ] 確認 frame-ancestors 或 X-Frame-Options 設定符合頁面嵌入需求。
- [ ] 重新執行弱點掃描，確認不再檢出缺少點擊劫持防護標頭。

修復路徑



先確認所有需納入處理的網頁回應，再依嵌入需求設定 CSP frame-ancestors 或 X-Frame-Options，最後透過回應檢查與重新掃描確認防護標頭已生效。

弱點實例列表 (5/5)

弱點實例	請求方法
[redacted]	GET
[redacted]	GET
[redacted]	GET
[redacted]	GET
[redacted]	GET

MEDIUM

跨網域設定錯誤

50

風險等級	OWASP 分類	弱點實例數量
中危	A01:2025 存取控制失效	5

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

Web 伺服器的跨來源資源共用（CORS）設定錯誤，可能允許瀏覽器跨來源載入資料。

修復說明

01 確認目前未經驗證即可取得的敏感資料範圍，並盤點涉及的端點與回應內容。

02 將 Access-Control-Allow-Origin 限制為必要網域。

03 未需跨來源存取時，移除所有 CORS HTTP 標頭，避免瀏覽器接受非必要的跨域請求。

修復驗證

- [ ] 檢查回應中的敏感資料僅能依預期存取控制取得。
- [ ] 重新掃描受影響範圍，確認不再檢出此弱點。

修復路徑



先盤點未經驗證即可取得的敏感資料、端點與回應內容，接著將允許來源限縮至必要網域；若無跨來源需求則移除 CORS 標頭，最後重新掃描並確認存取控制符合預期。

弱點實例列表 (5/5)

弱點實例	請求方法
[redacted]	GET
[redacted]	GET
[redacted]	GET
[redacted]	GET
[redacted]	GET

未設定 Content-Security-Policy（CSP）標頭

51

風險等級	OWASP 分類	弱點實例數量
中危	A02:2025 安全設定錯誤	4

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

回應未設定 Content-Security-Policy 標頭，瀏覽器無法依網站宣告的內容來源限制載入，降低對 XSS 與資料注入的防護能力。

修復說明

01 確認受影響網站回應範圍，盤點所有應設定 CSP 標頭的頁面與端點。

02 在提供回應的適用元件設定 Content-Security-Policy 標頭。

03 依網站實際需求宣告瀏覽器可載入的核准內容來源與資源類型。

修復驗證

- [ ] 檢查受影響回應已包含 Content-Security-Policy 標頭及核准來源設定。
- [ ] 重新執行弱點掃描，確認不再檢出 CSP 標頭未設定問題。

修復路徑



先確認未設定 CSP 標頭的受影響回應，再於適用元件設定標頭與核准內容來源，最後透過回應檢查及重掃確認不再檢出問題。

弱點實例列表（4/4）

弱點實例	請求方法
[redacted]	GET
[redacted]	GET
[redacted]	GET
[redacted]	GET

MEDIUM

缺少 Anti-CSRF Token

52

風險等級	OWASP 分類	弱點實例數量
中危	A01:2025 存取控制失效	2

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

HTML 提交表單未發現 Anti-CSRF Token；若未驗證 Token，偽造請求可能以使用者權限執行操作。

修復說明

01 針對每個會變更狀態的表單產生不可預測且唯一的 Token

02 將不可預測的唯一 Token 納入每份表單，並於接收請求時驗證其有效性

03 禁止以 GET 方法處理任何會造成資料或系統狀態變更的請求

04 修正應用程式中的 XSS 問題，避免攻擊者繞過既有的 CSRF 防護機制

修復驗證

- [ ] 確認各變更狀態表單皆含唯一且不可預測的 Token
- [ ] 確認僅持有效 Token 的表單請求會被接受並變更狀態
- [ ] 重新執行弱點掃描，確認不再檢出缺少 Anti-CSRF Token

修復路徑



先確認受影響的表單與狀態變更請求，再導入 Token 驗證並限制 GET 用途，最後透過檢查與重掃確認缺少 Anti-CSRF Token 的情形已改善。

弱點實例列表 (2/2)

弱點實例	請求方法
[redacted]	GET
[redacted]	GET

MEDIUM

CSP script-src 允許 unsafe-inline

53

風險等級	OWASP 分類	弱點實例數量
中危	A02:2025 安全設定錯誤	1

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

CSP 的 script-src 指令允許 unsafe-inline 內嵌指令碼，會降低對 XSS 與資料注入攻擊的防護效果。

修復說明

01 檢視 CSP 標頭，確認 script-src 指令中含有 unsafe-inline 的設定。

02 從 script-src 移除 unsafe-inline，並明確定義允許的指令碼來源。

03 於適用回應一致設定 Content-Security-Policy 標頭及更新後的 script-src 指令。

修復驗證

- [ ] 檢查回應的 CSP 標頭，確認 script-src 已不含 unsafe-inline。
- [ ] 重新掃描目標頁面，確認此弱點已不再被檢出。

修復路徑



先確認受影響的 CSP 設定範圍，移除 script-src 中的 unsafe-inline 並定義允許來源，最後透過回應檢查與重新掃描確認弱點不再被檢出。

弱點實例列表 (1/1)

弱點實例	請求方法
[redacted]	GET

MEDIUM

SMTP 明文登入未加密弱點

54

風險等級	CVSS	連接埠
中危	4.8	587

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

遠端 SMTP 伺服器允許在未加密連線中以明文方式登入，攻擊者側錄網路流量即可取得帳號密碼。

修復說明

01 啟用 SMTPS 服務，確保 SMTP 連線全程加密傳輸。

02 設定伺服器強制於登入前執行 STARTTLS 加密指令。

03 於未加密連線中，完全停用明文帳號密碼驗證機制設定。

04 參考 SMTP 伺服器官方文件完成相關 TLS 加密設定。

修復驗證

- [ ] 嘗試不使用 TLS 加密登入，確認連線遭伺服器拒絕。
- [ ] 檢查服務是否強制啟用 STARTTLS 或 SMTPS。
- [ ] 重新掃描目標主機，確認明文登入弱點已修復排除。

修復路徑



先確認允許明文登入的 SMTP 服務範圍，再強制啟用 STARTTLS 或 SMTPS 加密，最後重新掃描驗證明文登入已被阻擋。

詳細資訊

The remote SMTP server accepts logins via the following cleartext authentication mechanisms over unencrypted connections:

PLAIN

MEDIUM

SMTP 郵件轉寄弱點（簡易測試）

55

風險等級	CVSS	連接埠
中危	4.3	587

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

遠端 SMTP 伺服器對郵件轉寄保護不足，可能遭垃圾郵件發送者利用，向外轉寄大量郵件。

修復說明

01 僅限制 SMTP 郵件轉寄功能，只允許經授權且信任的主機使用。

02 設定郵件伺服器，要求轉寄前必須先通過身分驗證機制。

03 停用 SMTP 伺服器組態中任何允許開放轉寄的相關設定。

04 將郵件轉寄範圍限制於內部網域或可信任的網路區段內。

05 定期檢查郵件伺服器日誌，找出異常的郵件轉寄嘗試紀錄。

修復路徑



先確認 SMTP 伺服器目前的轉寄設定範圍，接著限制並要求驗證轉寄權限，最後重新掃描以確認開放轉寄問題已完全排除。

修復驗證

- [ ] 由外部主機嘗試轉寄，確認該要求遭伺服器拒絕。
- [ ] 檢查 SMTP 伺服器設定，確認轉寄前已強制要求驗證。
- [ ] 重新掃描郵件伺服器，確認其已不再是開放轉寄伺服器。

詳細資訊

SMTP banner:

220 mailhog.example ESMTP MailHog<CR><LF>

The scanner was able to relay mail by sending the following sequences:

Request: HELO example.com<CR><LF>
Answer: 250 Hello example.com<CR><LF>
Request: MAIL FROM: <openvasvt@ospd-openvas.local><CR><LF>
Answer: 250 Sender openvasvt@ospd-openvas.local ok<CR><LF>
Request: RCPT TO: <openvasvt@example.com><CR><LF>
Answer: 250 Recipient openvasvt@example.com ok<CR><LF>
Request: data<CR><LF>
Answer: 354 End data with <CR><LF>.<CR><LF><CR><LF>
Request: Subject: OpenVASVT-Relay-Test<CR><LF>To: OpenVASVT-Relay-Test <openvasvt@example.com><CR><LF>From: OpenVASVT-Relay-Test <openvasvt@ospd-openvas.local><CR><LF><CR><LF>This is a OpenVASVT-Relay-Test to test the mail server <LF>if it is configured as an open mail relay.<CR><LF><CR><LF>If you have received this message please forward it to the administrator of this mail server and ask to protect it against mail relaying.<CR><LF>.<CR>

MEDIUM

<LF>
Answer: 250 Ok: queued as Dr-3×7iikRRfjEq1MguPzt86lnkrSF97xP985mcOp4Q=@mailhog.example<CR><LF>

SSL/TLS 憑證已過期

56

風險等級	CVSS	連接埠
中危	5.0	8443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

遠端伺服器的 SSL/TLS 憑證已逾有效期限，可能降低使用者信任，並增加連線遭攔截或偽冒的風險。

修復說明

01 盤點所有使用該已過期 SSL/TLS 憑證的服務與系統清單。

02 向可信任的憑證機構提出申請，並取得具正式效力的新憑證。

03 於伺服器完成新憑證安裝設定，並重新啟動相關服務以套用。

04 建立憑證到期監控機制，並設定提前更新提醒通知事項。

修復驗證

- [ ] 檢查該服務上目前所使用憑證的有效期限是否正常。
- [ ] 確認用戶端連線不再出現憑證過期警示訊息。
- [ ] 重新執行弱點掃描，以確認過期憑證問題已完全排除。

修復路徑



先確認所有使用過期憑證的服務範圍，接著取得並安裝新憑證並重啟服務套用，最後重新掃描以驗證憑證過期問題已完全解決。

詳細資訊

The certificate of the remote service expired on 2026-10-28 05:49:44.

Certificate details:
fingerprint (SHA-1) | F93F1A1FE109B4EAE70BB6AF595A4C0B818D414F
fingerprint (SHA-256) | E35744E1B40D966CE71EDE16A35F7DF1EE46493F0CB91C674D41C496F5EA1CFF
issued by | CN=Redmark synthetic lab CA
public key algorithm | RSA
public key size (bits) | 2048
serial | 1000
signature algorithm | sha256WithRSAEncryption
subject | CN=expired.example.invalid
subject alternative names (SAN) | None
valid from | 2026-08-30 05:49:44 UTC
valid until | 2026-10-28 05:49:44 UTC

MEDIUM

phpinfo() 輸出資訊洩露（HTTP）

57

風險等級	CVSS	連接埠
中危	5.3	8080

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

透過 HTTP 偵測到暴露 PHP phpinfo() 函式輸出內容的檔案，可能洩露執行帳號、伺服器 IP、伺服器與系統版本及網站根目錄路徑。

修復說明

01 刪除伺服器上所發現的全部 phpinfo() 輸出檔案，避免資訊外洩。

02 限制任何殘留診斷檔案的存取權限，僅允許必要人員讀取。

03 避免在正式環境部署含 phpinfo() 的測試腳本。

04 暫時可先於伺服器設定封鎖該檔案存取，待移除後解除。

修復驗證

- [ ] 重新存取該檔案網址，確認已不再輸出 phpinfo 內容。
- [ ] 檢查伺服器存取紀錄是否有異常存取該檔案。
- [ ] 重新執行弱點掃描，確認此弱點不再被檢出。

修復路徑



先找出所有暴露 phpinfo() 內容的檔案，接著移除或限制其存取權限，最後重新掃描確認資訊洩露問題已完全解決。

詳細資訊

The following files are calling the function phpinfo() which disclose potentially sensitive information:

Concluded from:

```
<title>PHP 8.3.35 - phpinfo()</title>
<tr><td class="e">Configuration File (php.ini) Path </td>
```

Concluded from:

```
<title>PHP 8.3.35 - phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" />
</head>
<tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/usr/local/etc/php </td></tr>
```

MEDIUM

phpinfo() 輸出資訊洩露（HTTP）

58

風險等級	CVSS	連接埠
中危	5.3	8443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

透過 HTTP 偵測到暴露 PHP phpinfo() 函式輸出內容的檔案，可能洩露執行帳號、伺服器 IP、伺服器與系統版本及網站根目錄路徑。

修復說明

01 刪除伺服器上所發現的全部 phpinfo() 輸出檔案，避免資訊外洩。

02 限制任何殘留診斷檔案的存取權限，僅允許必要人員讀取。

03 避免在正式環境部署含 phpinfo() 的測試腳本。

04 暫時可先於伺服器設定封鎖該檔案存取，待移除後解除。

修復驗證

- [ ] 重新存取該檔案網址，確認已不再輸出 phpinfo 內容。
- [ ] 檢查伺服器存取紀錄是否有異常存取該檔案。
- [ ] 重新執行弱點掃描，確認此弱點不再被檢出。

修復路徑



先找出所有暴露 phpinfo() 內容的檔案，接著移除或限制其存取權限，最後重新掃描確認資訊洩露問題已完全解決。

詳細資訊

The following files are calling the function phpinfo() which disclose potentially sensitive information:

Concluded from:

```
<title>PHP 8.3.35 - phpinfo()</title>
<tr><td class="e">Configuration File (php.ini) Path </td>
```

Concluded from:

```
<title>PHP 8.3.35 - phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" />
</head>
<tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/usr/local/etc/php </td></tr>
```

MEDIUM

phpinfo() 輸出資訊洩露（HTTP）

59

風險等級	CVSS	連接埠
中危	5.3	443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

透過 HTTP 偵測到暴露 PHP phpinfo() 函式輸出內容的檔案，可能洩露執行帳號、伺服器 IP、伺服器與系統版本及網站根目錄路徑。

修復說明

01 刪除伺服器上所發現的全部 phpinfo() 輸出檔案，避免資訊外洩。

02 限制任何殘留診斷檔案的存取權限，僅允許必要人員讀取。

03 避免在正式環境部署含 phpinfo() 的測試腳本。

04 暫時可先於伺服器設定封鎖該檔案存取，待移除後解除。

修復驗證

- [ ] 重新存取該檔案網址，確認已不再輸出 phpinfo 內容。
- [ ] 檢查伺服器存取紀錄是否有異常存取該檔案。
- [ ] 重新執行弱點掃描，確認此弱點不再被檢出。

修復路徑



先找出所有暴露 phpinfo() 內容的檔案，接著移除或限制其存取權限，最後重新掃描確認資訊洩露問題已完全解決。

詳細資訊

The following files are calling the function phpinfo() which disclose potentially sensitive information:

Concluded from:

```
<title>PHP 8.3.35 - phpinfo()</title>
<tr><td class="e">Configuration File (php.ini) Path </td>
```

Concluded from:

```
<title>PHP 8.3.35 - phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" />
</head>
<tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/usr/local/etc/php </td></tr>
```

MEDIUM

phpinfo() 輸出資訊洩露（HTTP）

60

風險等級	CVSS	連接埠
中危	5.3	10443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

透過 HTTP 偵測到暴露 PHP phpinfo() 函式輸出內容的檔案，可能洩露執行帳號、伺服器 IP、伺服器與系統版本及網站根目錄路徑。

修復說明

01 刪除伺服器上所發現的全部 phpinfo() 輸出檔案，避免資訊外洩。

02 限制任何殘留診斷檔案的存取權限，僅允許必要人員讀取。

03 避免在正式環境部署含 phpinfo() 的測試腳本。

04 暫時可先於伺服器設定封鎖該檔案存取，待移除後解除。

修復驗證

- [ ] 重新存取該檔案網址，確認已不再輸出 phpinfo 內容。
- [ ] 檢查伺服器存取紀錄是否有異常存取該檔案。
- [ ] 重新執行弱點掃描，確認此弱點不再被檢出。

修復路徑



先找出所有暴露 phpinfo() 內容的檔案，接著移除或限制其存取權限，最後重新掃描確認資訊洩露問題已完全解決。

詳細資訊

The following files are calling the function phpinfo() which disclose potentially sensitive information:

Concluded from:

```
<title>PHP 8.3.35 - phpinfo()</title>
<tr><td class="e">Configuration File (php.ini) Path </td>
```

Concluded from:

```
<title>PHP 8.3.35 - phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" />
</head>
<tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/usr/local/etc/php </td></tr>
```

MEDIUM

phpinfo() 輸出資訊洩露（HTTP）

61

風險等級	CVSS	連接埠
中危	5.3	9443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

透過 HTTP 偵測到暴露 PHP phpinfo() 函式輸出內容的檔案，可能洩露執行帳號、伺服器 IP、伺服器與系統版本及網站根目錄路徑。

修復說明

01 刪除伺服器上所發現的全部 phpinfo() 輸出檔案，避免資訊外洩。

02 限制任何殘留診斷檔案的存取權限，僅允許必要人員讀取。

03 避免在正式環境部署含 phpinfo() 的測試腳本。

04 暫時可先於伺服器設定封鎖該檔案存取，待移除後解除。

修復驗證

- [ ] 重新存取該檔案網址，確認已不再輸出 phpinfo 內容。
- [ ] 檢查伺服器存取紀錄是否有異常存取該檔案。
- [ ] 重新執行弱點掃描，確認此弱點不再被檢出。

修復路徑



先找出所有暴露 phpinfo() 內容的檔案，接著移除或限制其存取權限，最後重新掃描確認資訊洩露問題已完全解決。

詳細資訊

The following files are calling the function phpinfo() which disclose potentially sensitive information:

Concluded from:

```
<title>PHP 8.3.35 - phpinfo()</title>
<tr><td class="e">Configuration File (php.ini) Path </td>
```

Concluded from:

```
<title>PHP 8.3.35 - phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" />
</head>
<tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/usr/local/etc/php </td></tr>
```

MEDIUM

phpinfo() 輸出資訊洩露（HTTP）

62

風險等級	CVSS	連接埠
中危	5.3	80

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

透過 HTTP 偵測到暴露 PHP phpinfo() 函式輸出內容的檔案，可能洩露執行帳號、伺服器 IP、伺服器與系統版本及網站根目錄路徑。

修復說明

01 刪除伺服器上所發現的全部 phpinfo() 輸出檔案，避免資訊外洩。

02 限制任何殘留診斷檔案的存取權限，僅允許必要人員讀取。

03 避免在正式環境部署含 phpinfo() 的測試腳本。

04 暫時可先於伺服器設定封鎖該檔案存取，待移除後解除。

修復驗證

- [ ] 重新存取該檔案網址，確認已不再輸出 phpinfo 內容。
- [ ] 檢查伺服器存取紀錄是否有異常存取該檔案。
- [ ] 重新執行弱點掃描，確認此弱點不再被檢出。

修復路徑



先找出所有暴露 phpinfo() 內容的檔案，接著移除或限制其存取權限，最後重新掃描確認資訊洩露問題已完全解決。

詳細資訊

The following files are calling the function phpinfo() which disclose potentially sensitive information:

Concluded from:
<title>PHP 8.3.35 - phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" />
</head>
<tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/usr/local/etc/php </td></tr>

MEDIUM

敏感檔案洩漏（HTTP）

63

風險等級	CVSS	連接埠
中危	5.0	443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

網頁伺服器上存在可經由 HTTP 存取的敏感檔案，如設定、備份、記錄或私密金鑰檔案，攻擊者可藉此取得帳號密碼等機敏資訊。

修復說明

01 盤點網頁伺服器上所有可經由公開網路存取到的敏感檔案清單。

02 將已確認之敏感檔案自公開網頁目錄中完全移除，避免外洩。

03 透過伺服器設定限制剩餘敏感檔案的存取權限，僅限授權對象。

04 更換所有可能已外洩的帳號密碼與金鑰等重要憑證資料。

05 定期稽核網頁根目錄，避免再次出現敏感檔案外洩情形。

修復驗證

- [ ] 確認已識別之敏感檔案無法再經由 HTTP 存取。
- [ ] 檢查伺服器設定確實限制敏感路徑的存取權限。
- [ ] 重新掃描網頁伺服器確認不再檢出敏感檔案。

修復路徑



先盤點可公開存取的敏感檔案，接著移除或限制存取權限並視需要更換憑證，最後重新掃描確認檔案已不再外洩，確保修復成效。

詳細資訊

The following files containing sensitive information were identified:

Description: Laravel/Codeigniter/Generic ".env" file present that may contain sensitive information like database credentials.
Match: APP_NAME=RedmarkSecurityLab
APP_ENV=testing
APP_DEBUG=true
APP_KEY=lab-fixture-not-a-real-key
DB_HOST=example.invalid
DB_DATABASE=synthetic_lab
DB_USERNAME=not-a-real-user
DB_PASSWORD=not-a-real-password
Used regex:
^(APP_(NAME|ENV|KEY|DEBUG|URL|PASSWORD)|DB_(HOST|USERNAME|PASSWORD|DATABASE|URL)|(DATABASE|MAILER)_URL|PG_(USERNAME|PASSWORD|DATABASE))=.+
URL:

MEDIUM

敏感檔案洩漏（HTTP）

64

風險等級	CVSS	連接埠
中危	5.0	8443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

網頁伺服器上存在可經由 HTTP 存取的敏感檔案，如設定、備份、記錄或私密金鑰檔案，攻擊者可藉此取得帳號密碼等機敏資訊。

修復說明

01 盤點網頁伺服器上所有可經由公開網路存取到的敏感檔案清單。

02 將已確認之敏感檔案自公開網頁目錄中完全移除，避免外洩。

03 透過伺服器設定限制剩餘敏感檔案的存取權限，僅限授權對象。

04 更換所有可能已外洩的帳號密碼與金鑰等重要憑證資料。

05 定期稽核網頁根目錄，避免再次出現敏感檔案外洩情形。

修復驗證

- [ ] 確認已識別之敏感檔案無法再經由 HTTP 存取。
- [ ] 檢查伺服器設定確實限制敏感路徑的存取權限。
- [ ] 重新掃描網頁伺服器確認不再檢出敏感檔案。

修復路徑



先盤點可公開存取的敏感檔案，接著移除或限制存取權限並視需要更換憑證，最後重新掃描確認檔案已不再外洩，確保修復成效。

詳細資訊

The following files containing sensitive information were identified:

Description: Laravel/Codeigniter/Generic ".env" file present that may contain sensitive information like database credentials.
Match: APP_NAME=RedmarkSecurityLab
APP_ENV=testing
APP_DEBUG=true
APP_KEY=lab-fixture-not-a-real-key
DB_HOST=example.invalid
DB_DATABASE=synthetic_lab
DB_USERNAME=not-a-real-user
DB_PASSWORD=not-a-real-password
Used regex:
^(APP_(NAME|ENV|KEY|DEBUG|URL|PASSWORD)|DB_(HOST|USERNAME|PASSWORD|DATABASE|URL)|(DATABASE|MAILER)_URL|PG_(USERNAME|PASSWORD|DATABASE))=.+
URL:

MEDIUM

敏感檔案洩漏（HTTP）

65

風險等級	CVSS	連接埠
中危	5.0	10443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

網頁伺服器上存在可經由 HTTP 存取的敏感檔案，如設定、備份、記錄或私密金鑰檔案，攻擊者可藉此取得帳號密碼等機敏資訊。

修復說明

01 盤點網頁伺服器上所有可經由公開網路存取到的敏感檔案清單。

02 將已確認之敏感檔案自公開網頁目錄中完全移除，避免外洩。

03 透過伺服器設定限制剩餘敏感檔案的存取權限，僅限授權對象。

04 更換所有可能已外洩的帳號密碼與金鑰等重要憑證資料。

05 定期稽核網頁根目錄，避免再次出現敏感檔案外洩情形。

修復路徑



先盤點可公開存取的敏感檔案，接著移除或限制存取權限並視需要更換憑證，最後重新掃描確認檔案已不再外洩，確保修復成效。

修復驗證

- [ ] 確認已識別之敏感檔案無法再經由 HTTP 存取。
- [ ] 檢查伺服器設定確實限制敏感路徑的存取權限。
- [ ] 重新掃描網頁伺服器確認不再檢出敏感檔案。

詳細資訊

The following files containing sensitive information were identified:

Description: Laravel/Codeigniter/Generic ".env" file present that may contain sensitive information like database credentials.
Match: APP_NAME=RedmarkSecurityLab
APP_ENV=testing
APP_DEBUG=true
APP_KEY=lab-fixture-not-a-real-key
DB_HOST=example.invalid
DB_DATABASE=synthetic_lab
DB_USERNAME=not-a-real-user
DB_PASSWORD=not-a-real-password
Used regex:
^(APP_(NAME|ENV|KEY|DEBUG|URL|PASSWORD)|DB_(HOST|USERNAME|PASSWORD|DATABASE|URL)|(DATABASE|MAILER)_URL|PG_(USERNAME|PASSWORD|DATABASE))=.+
URL:

MEDIUM

敏感檔案洩漏（HTTP）

66

風險等級	CVSS	連接埠
中危	5.0	80

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

網頁伺服器上存在可經由 HTTP 存取的敏感檔案，如設定、備份、記錄或私密金鑰檔案，攻擊者可藉此取得帳號密碼等機敏資訊。

修復說明

01 盤點網頁伺服器上所有可經由公開網路存取到的敏感檔案清單。

02 將已確認之敏感檔案自公開網頁目錄中完全移除，避免外洩。

03 透過伺服器設定限制剩餘敏感檔案的存取權限，僅限授權對象。

04 更換所有可能已外洩的帳號密碼與金鑰等重要憑證資料。

05 定期稽核網頁根目錄，避免再次出現敏感檔案外洩情形。

修復路徑



先盤點可公開存取的敏感檔案，接著移除或限制存取權限並視需要更換憑證，最後重新掃描確認檔案已不再外洩，確保修復成效。

修復驗證

- [ ] 確認已識別之敏感檔案無法再經由 HTTP 存取。
- [ ] 檢查伺服器設定確實限制敏感路徑的存取權限。
- [ ] 重新掃描網頁伺服器確認不再檢出敏感檔案。

詳細資訊

The following files containing sensitive information were identified:

Description: Laravel/Codeigniter/Generic ".env" file present that may contain sensitive information like database credentials.
Match: APP_NAME=RedmarkSecurityLab
APP_ENV=testing
APP_DEBUG=true
APP_KEY=lab-fixture-not-a-real-key
DB_HOST=example.invalid
DB_DATABASE=synthetic_lab
DB_USERNAME=not-a-real-user
DB_PASSWORD=not-a-real-password
Used regex:
^(APP_(NAME|ENV|KEY|DEBUG|URL|PASSWORD)|DB_(HOST|USERNAME|PASSWORD|DATABASE|URL)|(DATABASE|MAILER)_URL|PG_(USERNAME|PASSWORD|DATABASE))=.+
URL:

MEDIUM

Description: Laravel/Codeigniter/Generic ".env" file present that may contain sensitive information like database credentials.
Match: APP_NAME=RedmarkMultiLocationFixture1
APP_ENV=testing
APP_KEY=FAKE_TEST_VALUE_NOT_A_REAL_KEY
DB_HOST=database.invalid
DB_DATABASE=synthetic_fixture
DB_PASSWORD=FAKE_TEST_VALUE_NOT_A_REAL_PASSWORD
Used regex:
^(APP_(NAME|ENV|KEY|DEBUG|URL|PASSWORD)|DB_(HOST|USERNAME|PASSWORD|DATABASE|URL)|(DATABASE|MAILER)_URL|PG_(USERNAME|PASSWORD|DATABASE))=.+
URL:

Description: Laravel/Codeigniter/Generic ".env" file present that may contain sensitive information like database credentials.
Match: APP_NAME=RedmarkMultiLocationFixture2
APP_ENV=testing
APP_KEY=FAKE_TEST_VALUE_NOT_A_REAL_KEY
DB_HOST=database.invalid
DB_DATABASE=synthetic_fixture
DB_PASSWORD=FAKE_TEST_VALUE_NOT_A_REAL_PASSWORD
Used regex:
^(APP_(NAME|ENV|KEY|DEBUG|URL|PASSWORD)|DB_(HOST|USERNAME|PASSWORD|DATABASE|URL)|(DATABASE|MAILER)_URL|PG_(USERNAME|PASSWORD|DATABASE))=.+
URL:

MEDIUM

敏感檔案洩漏（HTTP）

67

風險等級	CVSS	連接埠
中危	5.0	9443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

網頁伺服器上存在可經由 HTTP 存取的敏感檔案，如設定、備份、記錄或私密金鑰檔案，攻擊者可藉此取得帳號密碼等機敏資訊。

修復說明

01 盤點網頁伺服器上所有可經由公開網路存取到的敏感檔案清單。

02 將已確認之敏感檔案自公開網頁目錄中完全移除，避免外洩。

03 透過伺服器設定限制剩餘敏感檔案的存取權限，僅限授權對象。

04 更換所有可能已外洩的帳號密碼與金鑰等重要憑證資料。

05 定期稽核網頁根目錄，避免再次出現敏感檔案外洩情形。

修復驗證

- [ ] 確認已識別之敏感檔案無法再經由 HTTP 存取。
- [ ] 檢查伺服器設定確實限制敏感路徑的存取權限。
- [ ] 重新掃描網頁伺服器確認不再檢出敏感檔案。

修復路徑



先盤點可公開存取的敏感檔案，接著移除或限制存取權限並視需要更換憑證，最後重新掃描確認檔案已不再外洩，確保修復成效。

詳細資訊

The following files containing sensitive information were identified:

Description: Laravel/Codeigniter/Generic ".env" file present that may contain sensitive information like database credentials.
Match: APP_NAME=RedmarkSecurityLab
APP_ENV=testing
APP_DEBUG=true
APP_KEY=lab-fixture-not-a-real-key
DB_HOST=example.invalid
DB_DATABASE=synthetic_lab
DB_USERNAME=not-a-real-user
DB_PASSWORD=not-a-real-password
Used regex:
^(APP_(NAME|ENV|KEY|DEBUG|URL|PASSWORD)|DB_(HOST|USERNAME|PASSWORD|DATABASE|URL)|(DATABASE|MAILER)_URL|PG_(USERNAME|PASSWORD|DATABASE))=.+
URL:

MEDIUM

敏感檔案洩漏（HTTP）

68

風險等級	CVSS	連接埠
中危	5.0	8080

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

網頁伺服器上存在可經由 HTTP 存取的敏感檔案，如設定、備份、記錄或私密金鑰檔案，攻擊者可藉此取得帳號密碼等機敏資訊。

修復說明

01 盤點網頁伺服器上所有可經由公開網路存取到的敏感檔案清單。

02 將已確認之敏感檔案自公開網頁目錄中完全移除，避免外洩。

03 透過伺服器設定限制剩餘敏感檔案的存取權限，僅限授權對象。

04 更換所有可能已外洩的帳號密碼與金鑰等重要憑證資料。

05 定期稽核網頁根目錄，避免再次出現敏感檔案外洩情形。

修復驗證

- [ ] 確認已識別之敏感檔案無法再經由 HTTP 存取。
- [ ] 檢查伺服器設定確實限制敏感路徑的存取權限。
- [ ] 重新掃描網頁伺服器確認不再檢出敏感檔案。

修復路徑



先盤點可公開存取的敏感檔案，接著移除或限制存取權限並視需要更換憑證，最後重新掃描確認檔案已不再外洩，確保修復成效。

詳細資訊

The following files containing sensitive information were identified:

Description: Laravel/Codeigniter/Generic ".env" file present that may contain sensitive information like database credentials.
Match: APP_NAME=RedmarkSecurityLab
APP_ENV=testing
APP_DEBUG=true
APP_KEY=lab-fixture-not-a-real-key
DB_HOST=example.invalid
DB_DATABASE=synthetic_lab
DB_USERNAME=not-a-real-user
DB_PASSWORD=not-a-real-password
Used regex:
^(APP_(NAME|ENV|KEY|DEBUG|URL|PASSWORD)|DB_(HOST|USERNAME|PASSWORD|DATABASE|URL)|(DATABASE|MAILER)_URL|PG_(USERNAME|PASSWORD|DATABASE))=.+
URL:

MEDIUM

版本控制系統（SCM）檔案／目錄可被存取（HTTP）

69

風險等級	CVSS	連接埠
中危	5.0	443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

網站伺服器上可直接存取 Git、Mercurial、Bazaar、CVS 或 Subversion 等版本控制系統的檔案或目錄，攻擊者可藉此取得系統與應用程式架構的額外資訊。

修復說明

01 盤點並列出網站伺服器上所有可被外部存取的 SCM 檔案與目錄。

02 將 Git、Mercurial、Bazaar 等 SCM 目錄從公開網站根目錄中徹底移除。

03 於網站伺服器設定中，明確禁止外部存取所有 SCM 相關路徑。

04 調整部署流程，排除 SCM 中繼資料檔案，避免日後再次外洩。

修復驗證

- [ ] 嘗試存取已知 SCM 路徑，確認回應已遭拒絕。
- [ ] 檢查伺服器設定確實阻擋 SCM 相關副檔名與路徑。
- [ ] 重新執行弱點掃描，確認此項目不再被檢出。

修復路徑



先盤點網站伺服器上所有暴露的 SCM 路徑，接著於伺服器端設定中移除或封鎖其存取權限，最後重新掃描以確認資源已完全無法再被外部存取。

詳細資訊

The following SCM files/folders were identified:

Match: [core]
[remote "origin"]
Used regex: ^\[(core|receive|(remote|branch) .+)\]$
URL:

MEDIUM

版本控制系統（SCM）檔案／目錄可被存取（HTTP）

70

風險等級	CVSS	連接埠
中危	5.0	9443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

網站伺服器上可直接存取 Git、Mercurial、Bazaar、CVS 或 Subversion 等版本控制系統的檔案或目錄，攻擊者可藉此取得系統與應用程式架構的額外資訊。

修復說明

01 盤點並列出網站伺服器上所有可被外部存取的 SCM 檔案與目錄。

02 將 Git、Mercurial、Bazaar 等 SCM 目錄從公開網站根目錄中徹底移除。

03 於網站伺服器設定中，明確禁止外部存取所有 SCM 相關路徑。

04 調整部署流程，排除 SCM 中繼資料檔案，避免日後再次外洩。

修復驗證

- [ ] 嘗試存取已知 SCM 路徑，確認回應已遭拒絕。
- [ ] 檢查伺服器設定確實阻擋 SCM 相關副檔名與路徑。
- [ ] 重新執行弱點掃描，確認此項目不再被檢出。

修復路徑



先盤點網站伺服器上所有暴露的 SCM 路徑，接著於伺服器端設定中移除或封鎖其存取權限，最後重新掃描以確認資源已完全無法再被外部存取。

詳細資訊

The following SCM files/folders were identified:

Match: [core]
[remote "origin"]
Used regex: ^\[(core|receive|(remote|branch) .+)\]$
URL:

MEDIUM

版本控制系統（SCM）檔案／目錄可被存取（HTTP）

71

風險等級	CVSS	連接埠
中危	5.0	10443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

網站伺服器上可直接存取 Git、Mercurial、Bazaar、CVS 或 Subversion 等版本控制系統的檔案或目錄，攻擊者可藉此取得系統與應用程式架構的額外資訊。

修復說明

01 盤點並列出網站伺服器上所有可被外部存取的 SCM 檔案與目錄。

02 將 Git、Mercurial、Bazaar 等 SCM 目錄從公開網站根目錄中徹底移除。

03 於網站伺服器設定中，明確禁止外部存取所有 SCM 相關路徑。

04 調整部署流程，排除 SCM 中繼資料檔案，避免日後再次外洩。

修復驗證

- [ ] 嘗試存取已知 SCM 路徑，確認回應已遭拒絕。
- [ ] 檢查伺服器設定確實阻擋 SCM 相關副檔名與路徑。
- [ ] 重新執行弱點掃描，確認此項目不再被檢出。

修復路徑



先盤點網站伺服器上所有暴露的 SCM 路徑，接著於伺服器端設定中移除或封鎖其存取權限，最後重新掃描以確認資源已完全無法再被外部存取。

詳細資訊

The following SCM files/folders were identified:

Match: [core]
[remote "origin"]
Used regex: ^\[(core|receive|(remote|branch) .+)\]$
URL:

MEDIUM

版本控制系統（SCM）檔案／目錄可被存取（HTTP）

72

風險等級	CVSS	連接埠
中危	5.0	8080

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

網站伺服器上可直接存取 Git、Mercurial、Bazaar、CVS 或 Subversion 等版本控制系統的檔案或目錄，攻擊者可藉此取得系統與應用程式架構的額外資訊。

修復說明

01 盤點並列出網站伺服器上所有可被外部存取的 SCM 檔案與目錄。

02 將 Git、Mercurial、Bazaar 等 SCM 目錄從公開網站根目錄中徹底移除。

03 於網站伺服器設定中，明確禁止外部存取所有 SCM 相關路徑。

04 調整部署流程，排除 SCM 中繼資料檔案，避免日後再次外洩。

修復驗證

- [ ] 嘗試存取已知 SCM 路徑，確認回應已遭拒絕。
- [ ] 檢查伺服器設定確實阻擋 SCM 相關副檔名與路徑。
- [ ] 重新執行弱點掃描，確認此項目不再被檢出。

修復路徑



先盤點網站伺服器上所有暴露的 SCM 路徑，接著於伺服器端設定中移除或封鎖其存取權限，最後重新掃描以確認資源已完全無法再被外部存取。

詳細資訊

The following SCM files/folders were identified:

Match: [core]
[remote "origin"]
Used regex: ^\[(core|receive|(remote|branch) .+)\]$
URL:

MEDIUM

版本控制系統（SCM）檔案／目錄可被存取（HTTP）

73

風險等級	CVSS	連接埠
中危	5.0	80

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

網站伺服器上可直接存取 Git、Mercurial、Bazaar、CVS 或 Subversion 等版本控制系統的檔案或目錄，攻擊者可藉此取得系統與應用程式架構的額外資訊。

修復說明

01 盤點並列出網站伺服器上所有可被外部存取的 SCM 檔案與目錄。

02 將 Git、Mercurial、Bazaar 等 SCM 目錄從公開網站根目錄中徹底移除。

03 於網站伺服器設定中，明確禁止外部存取所有 SCM 相關路徑。

04 調整部署流程，排除 SCM 中繼資料檔案，避免日後再次外洩。

修復驗證

- [ ] 嘗試存取已知 SCM 路徑，確認回應已遭拒絕。
- [ ] 檢查伺服器設定確實阻擋 SCM 相關副檔名與路徑。
- [ ] 重新執行弱點掃描，確認此項目不再被檢出。

修復路徑



先盤點網站伺服器上所有暴露的 SCM 路徑，接著於伺服器端設定中移除或封鎖其存取權限，最後重新掃描以確認資源已完全無法再被外部存取。

詳細資訊

The following SCM files/folders were identified:

Match: [core]
[remote "origin"]
Used regex: ^\[(core|receive|(remote|branch) .+)\]$
URL:

MEDIUM

版本控制系統（SCM）檔案／目錄可被存取（HTTP）

74

風險等級	CVSS	連接埠
中危	5.0	8443

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

網站伺服器上可直接存取 Git、Mercurial、Bazaar、CVS 或 Subversion 等版本控制系統的檔案或目錄，攻擊者可藉此取得系統與應用程式架構的額外資訊。

修復說明

01 盤點並列出網站伺服器上所有可被外部存取的 SCM 檔案與目錄。

02 將 Git、Mercurial、Bazaar 等 SCM 目錄從公開網站根目錄中徹底移除。

03 於網站伺服器設定中，明確禁止外部存取所有 SCM 相關路徑。

04 調整部署流程，排除 SCM 中繼資料檔案，避免日後再次外洩。

修復驗證

- [ ] 嘗試存取已知 SCM 路徑，確認回應已遭拒絕。
- [ ] 檢查伺服器設定確實阻擋 SCM 相關副檔名與路徑。
- [ ] 重新執行弱點掃描，確認此項目不再被檢出。

修復路徑



先盤點網站伺服器上所有暴露的 SCM 路徑，接著於伺服器端設定中移除或封鎖其存取權限，最後重新掃描以確認資源已完全無法再被外部存取。

詳細資訊

The following SCM files/folders were identified:

Match: [core]
[remote "origin"]
Used regex: ^\[(core|receive|(remote|branch) .+)\]$
URL:

MEDIUM

透過 HTTP 明文傳輸敏感資訊

75

風險等級	CVSS	連接埠
中危	4.8	8080

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

主機或應用程式透過 HTTP 以明文傳輸帳號密碼等敏感資訊，攻擊者可藉中間人攻擊竊聽通訊並取得該資料。

修復說明

01 強制所有敏感資料必須透過加密的 SSL/TLS 連線進行傳輸作業。

02 將所有 HTTP 請求自動導向至加密的 HTTPS 連線。

03 確保登入與資料輸入表單僅接受 HTTPS 提交方式傳送。

04 啟用 HSTS 機制以防止連線協定遭到降級攻擊，強化整體傳輸安全性。

05 過渡期間可暫時停用明文 HTTP 服務，藉此降低資料外洩風險。

修復驗證

- [ ] 確認敏感頁面僅能透過 HTTPS 連線存取。
- [ ] 檢查 HTTP 請求是否正確導向 HTTPS。
- [ ] 重新掃描確認系統不再偵測到明文傳輸情形。

修復路徑



先確認傳輸敏感資料的頁面範圍，導入 SSL/TLS 強制加密與導向機制，再重新掃描以確認明文傳輸問題已完全排除且無殘留風險。

詳細資訊

The following input fields were identified (URL:input name):

Git 設定檔案外洩

76

風險等級	CVSS	CWE ID
中危	5.3	CWE-200

連接埠	首次發現時間	最近發現時間
443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

伺服器上可透過 /.git/config 路徑存取 Git 設定檔與相關紀錄檔，可能洩漏儲存庫資訊、遠端網址或憑證，增加後續攻擊風險。

修復說明

01 立即移除或嚴格限制對整個 .git 目錄的網頁公開存取權限。

02 於網頁伺服器設定規則，封鎖所有隱藏版本控制檔案存取。

03 部署正式環境前，務必完整排除 .git 資料夾內所有內容。

04 若無法立即修復，應暫時關閉對外公開存取，以降低被利用的風險。

05 仔細檢查已外洩內容，確認是否含有憑證或敏感網址等資訊。

修復驗證

- [ ] 存取 /.git/config 確認回應為 403 或 404。
- [ ] 檢查網頁伺服器設定，確認已封鎖隱藏檔案存取。
- [ ] 重新執行掃描，確認該弱點已不再被檢測出來。

修復路徑



先盤點所有可公開存取的 .git 路徑，接著於伺服器層級限制或移除存取權限，最後重新掃描確認檔案已無法被外部取得。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

Git 設定檔案外洩

77

風險等級	CVSS	CWE ID
中危	5.3	CWE-200

連接埠	首次發現時間	最近發現時間
8080	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

伺服器上可透過 /.git/config 路徑存取 Git 設定檔與相關紀錄檔，可能洩漏儲存庫資訊、遠端網址或憑證，增加後續攻擊風險。

修復說明

01 立即移除或嚴格限制對整個 .git 目錄的網頁公開存取權限。

02 於網頁伺服器設定規則，封鎖所有隱藏版本控制檔案存取。

03 部署正式環境前，務必完整排除 .git 資料夾內所有內容。

04 若無法立即修復，應暫時關閉對外公開存取，以降低被利用的風險。

05 仔細檢查已外洩內容，確認是否含有憑證或敏感網址等資訊。

修復驗證

- [ ] 存取 /.git/config 確認回應為 403 或 404。
- [ ] 檢查網頁伺服器設定，確認已封鎖隱藏檔案存取。
- [ ] 重新執行掃描，確認該弱點已不再被檢測出來。

修復路徑



先盤點所有可公開存取的 .git 路徑，接著於伺服器層級限制或移除存取權限，最後重新掃描確認檔案已無法被外部取得。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

Git 設定檔案外洩

78

風險等級	CVSS	CWE ID
中危	5.3	CWE-200

連接埠	首次發現時間	最近發現時間
8443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

伺服器上可透過 /.git/config 路徑存取 Git 設定檔與相關紀錄檔，可能洩漏儲存庫資訊、遠端網址或憑證，增加後續攻擊風險。

修復說明

01 立即移除或嚴格限制對整個 .git 目錄的網頁公開存取權限。

02 於網頁伺服器設定規則，封鎖所有隱藏版本控制檔案存取。

03 部署正式環境前，務必完整排除 .git 資料夾內所有內容。

04 若無法立即修復，應暫時關閉對外公開存取，以降低被利用的風險。

05 仔細檢查已外洩內容，確認是否含有憑證或敏感網址等資訊。

修復驗證

- [ ] 存取 /.git/config 確認回應為 403 或 404。
- [ ] 檢查網頁伺服器設定，確認已封鎖隱藏檔案存取。
- [ ] 重新執行掃描，確認該弱點已不再被檢測出來。

修復路徑



先盤點所有可公開存取的 .git 路徑，接著於伺服器層級限制或移除存取權限，最後重新掃描確認檔案已無法被外部取得。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

Git 設定檔案外洩

79

風險等級	CVSS	CWE ID
中危	5.3	CWE-200

連接埠	首次發現時間	最近發現時間
10443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

伺服器上可透過 /.git/config 路徑存取 Git 設定檔與相關紀錄檔，可能洩漏儲存庫資訊、遠端網址或憑證，增加後續攻擊風險。

修復說明

01 立即移除或嚴格限制對整個 .git 目錄的網頁公開存取權限。

02 於網頁伺服器設定規則，封鎖所有隱藏版本控制檔案存取。

03 部署正式環境前，務必完整排除 .git 資料夾內所有內容。

04 若無法立即修復，應暫時關閉對外公開存取，以降低被利用的風險。

05 仔細檢查已外洩內容，確認是否含有憑證或敏感網址等資訊。

修復驗證

- [ ] 存取 /.git/config 確認回應為 403 或 404。
- [ ] 檢查網頁伺服器設定，確認已封鎖隱藏檔案存取。
- [ ] 重新執行掃描，確認該弱點已不再被檢測出來。

修復路徑



先盤點所有可公開存取的 .git 路徑，接著於伺服器層級限制或移除存取權限，最後重新掃描確認檔案已無法被外部取得。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
	2026-11-17 17:40:31	2026-11-17 17:40:31

Git 設定檔案外洩

80

風險等級	CVSS	CWE ID
中危	5.3	CWE-200

連接埠	首次發現時間	最近發現時間
9443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

伺服器上可透過 /.git/config 路徑存取 Git 設定檔與相關紀錄檔，可能洩漏儲存庫資訊、遠端網址或憑證，增加後續攻擊風險。

修復說明

01 立即移除或嚴格限制對整個 .git 目錄的網頁公開存取權限。

02 於網頁伺服器設定規則，封鎖所有隱藏版本控制檔案存取。

03 部署正式環境前，務必完整排除 .git 資料夾內所有內容。

04 若無法立即修復，應暫時關閉對外公開存取，以降低被利用的風險。

05 仔細檢查已外洩內容，確認是否含有憑證或敏感網址等資訊。

修復驗證

- [ ] 存取 /.git/config 確認回應為 403 或 404。
- [ ] 檢查網頁伺服器設定，確認已封鎖隱藏檔案存取。
- [ ] 重新執行掃描，確認該弱點已不再被檢測出來。

修復路徑



先盤點所有可公開存取的 .git 路徑，接著於伺服器層級限制或移除存取權限，最後重新掃描確認檔案已無法被外部取得。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

Git 設定檔案外洩

81

風險等級	CVSS	CWE ID
中危	5.3	CWE-200

連接埠	首次發現時間	最近發現時間
80	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

伺服器上可透過 /.git/config 路徑存取 Git 設定檔與相關紀錄檔，可能洩漏儲存庫資訊、遠端網址或憑證，增加後續攻擊風險。

修復說明

01 立即移除或嚴格限制對整個 .git 目錄的網頁公開存取權限。

02 於網頁伺服器設定規則，封鎖所有隱藏版本控制檔案存取。

03 部署正式環境前，務必完整排除 .git 資料夾內所有內容。

04 若無法立即修復，應暫時關閉對外公開存取，以降低被利用的風險。

05 仔細檢查已外洩內容，確認是否含有憑證或敏感網址等資訊。

修復驗證

- [ ] 存取 /.git/config 確認回應為 403 或 404。
- [ ] 檢查網頁伺服器設定，確認已封鎖隱藏檔案存取。
- [ ] 重新執行掃描，確認該弱點已不再被檢測出來。

修復路徑



先盤點所有可公開存取的 .git 路徑，接著於伺服器層級限制或移除存取權限，最後重新掃描確認檔案已無法被外部取得。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

MEDIUM

開放重新導向（Open Redirect）弱點

82

風險等級	CVSS	CWE ID
中危	6.1	CWE-601

連接埠	首次發現時間	最近發現時間
8000	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

系統偵測到開放重新導向弱點，攻擊者可誘導使用者連至惡意網站，進而竊取資訊、竄改資料或執行未授權操作。

修復說明

01 針對所有重新導向目的地建立明確的允許清單，並於伺服器端嚴格比對驗證。

02 拒絕或忽略由使用者提供且指向外部未知網域的重新導向網址。

03 改用相對路徑或內部識別碼表示目的地，避免直接使用完整外部網址。

04 導向外部網站前，先顯示警示頁面提示使用者確認是否繼續前往。

05 若無法立即修正，暫時停用該重新導向功能以降低風險。

修復驗證

- [ ] 以外部網址測試重新導向參數，確認已被阻擋。
- [ ] 檢視伺服器邏輯，確認已實施允許清單驗證機制。
- [ ] 重新掃描系統，確認此弱點已不再被偵測到。

修復路徑



團隊先盤點所有重新導向參數，接著針對目的地實施允許清單驗證機制，最後重新掃描系統以確認開放重新導向弱點已完全排除。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

LOW

Cookie 未設定 SameSite 屬性

83

風險等級	OWASP 分類	弱點實例數量
低危	A01:2025 存取控制失效	5

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

Cookie 未設定 SameSite 屬性，可能隨跨網站請求傳送；該屬性可降低 CSRF、跨網站指令碼載入及時序攻擊風險。

修復說明

01 盤點應用程式所設定且未含 SameSite 屬性的所有 Cookie。

02 在不影響既有功能前提下，將適用 Cookie 設定為 SameSite=Strict。

03 將其餘 Cookie 設定為 SameSite=Lax，確保所有 Cookie 均含該屬性。

修復驗證

- [ ] 檢查所有 Set-Cookie 標頭，確認皆含 SameSite=Strict 或 SameSite=Lax。
- [ ] 重新執行弱點掃描，確認不再檢出 Cookie without SameSite Attribute。

修復路徑



先確認所有未含 SameSite 屬性的 Cookie 範圍，再依適用情況設定 Strict 或 Lax，最後透過回應檢查與重掃確認不再檢出。

弱點實例列表 (5/5)

弱點實例	請求方法
[redacted]	GET
[redacted]	POST
[redacted]	POST
[redacted]	POST
[redacted]	POST

LOW

Cookie 未設定 Secure 屬性

84

風險等級	OWASP 分類	弱點實例數量
低危	A02:2025 安全設定錯誤	5

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

Cookie 未設定 Secure 屬性，可透過未加密連線存取，可能使 Cookie 資訊暴露。

修復說明

01 盤點未設定 Secure 屬性的 Cookie 及其傳輸用途

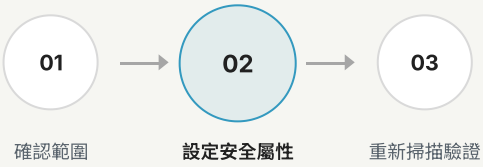
02 對含敏感資訊或工作階段權杖的 Cookie 設定 Secure 屬性

03 確保含敏感資訊的 Cookie 僅透過 HTTPS 加密通道安全傳輸

修復驗證

- [ ] 檢查回應中的 Set-Cookie 標頭，確認相關 Cookie 含有 Secure 屬性
- [ ] 確認相關 Cookie 不會透過未加密連線傳輸
- [ ] 重新執行弱點掃描並確認系統不再回報此項弱點

修復路徑



先確認未設定 Secure 屬性的 Cookie 與用途，再為含敏感資訊或工作階段權杖的 Cookie 啟用 Secure 屬性並限制加密傳輸，最後以設定檢查及弱點掃描確認修復結果。

弱點實例列表 (5/5)

弱點實例	請求方法
	GET
	GET
	POST
	POST
	POST

LOW

Server HTTP 回應標頭洩漏版本資訊

85

風險等級	OWASP 分類	弱點實例數量
低危	A02:2025 安全設定錯誤	5

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

Web 或應用程式伺服器透過 Server HTTP 回應標頭洩漏版本資訊，可能協助識別其相關弱點。

修復說明

01 檢視所有受影響服務所傳回 HTTP 回應中的 Server 標頭值。

02 設定伺服器與中介元件，避免在 HTTP 回應中輸出 Server 標頭。

03 無法移除標頭時，改為僅提供通用的 Server 資訊。

修復驗證

- [ ] 檢查受影響 HTTP 回應，確認不再包含版本資訊。
- [ ] 重新掃描受影響服務，確認不再檢出此弱點。

修復路徑



先確認所有受影響服務的 HTTP 回應範圍，再設定伺服器及中介元件抑制 Server 標頭版本資訊，最後重新掃描確認不再檢出此弱點。

弱點實例列表 (5/5)

弱點實例	請求方法
[redacted]	GET
[redacted]	GET
[redacted]	GET
[redacted]	GET
[redacted]	GET

LOW

Unix 時間戳記資訊揭露

86

風險等級	OWASP 分類	弱點實例數量
低危	A01:2025 存取控制失效	5

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

應用程式或 Web 伺服器揭露 Unix 時間戳記；若資料具敏感性或可彙整，可能暴露可利用模式。

修復說明

01 人工盤點各揭露端點的時間戳記內容，確認是否含有敏感業務或系統資訊。

02 評估跨頁面或跨時段彙整時間戳記後，是否可能推導可利用的行為模式。

03 於相關回應與頁面移除不必要時間戳記，並限制敏感資料僅供授權使用者存取。

修復驗證

- [ ] 確認揭露的時間戳記不具敏感性，亦不會形成可利用模式。
- [ ] 重新執行弱點掃描並檢查相關端點，確認系統不再回報此項弱點。

修復路徑



先盤點各端點揭露的時間戳記及其敏感性，評估彙整後能否推導可利用模式；再移除非必要資料或限制授權存取，最後重新掃描相關端點並確認不再檢出。

弱點實例列表 (5/5)

弱點實例	請求方法
[redacted]	GET
[redacted]	GET
[redacted]	GET
[redacted]	GET
[redacted]	GET

LOW

X-Powered-By HTTP 回應標頭資訊洩漏

87

風險等級	OWASP 分類	弱點實例數量
低危	A01:2025 存取控制失效	5

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

Web 或應用程式伺服器透過一個以上 X-Powered-By HTTP 回應標頭洩漏資訊，可能有助於識別相依元件及其潛在弱點。

修復說明

01 盤點網站、應用程式伺服器及反向代理的回應標頭設定來源

02 在各層設定中停用或移除 X-Powered-By 回應標頭輸出

03 部署後重新載入服務，避免預設值或中介層重新加入該標頭輸出設定

修復驗證

- [ ] 以瀏覽器開發工具或 curl 檢查各公開端點的回應標頭
- [ ] 確認正常與錯誤回應均未出現 X-Powered-By 標頭

修復路徑



先盤點各層標頭來源，再於伺服器、應用程式與代理停用輸出，重新載入後檢查公開端點的正常及錯誤回應是否皆未含 X-Powered-By 標頭。

弱點實例列表 (5/5)

弱點實例	請求方法
[redacted]	GET
[redacted]	GET
[redacted]	GET
[redacted]	POST
[redacted]	POST

LOW

未設定 Strict-Transport-Security 標頭

88

風險等級	OWASP 分類	弱點實例數量
低危	A02:2025 安全設定錯誤	5

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

未設定 Strict-Transport-Security 標頭，瀏覽器不會依 HSTS 政策僅透過 HTTPS 與網站連線。HSTS 由 RFC 6797 規範。

修復說明

01 確認提供受影響 HTTP 回應的所有相關服務元件範圍。

02 在相關服務元件設定強制套用 Strict-Transport-Security。

03 確認受影響回應均已套用 Strict-Transport-Security 標頭。

修復驗證

- [ ] 檢查受影響 HTTPS 回應是否包含 Strict-Transport-Security 標頭。
- [ ] 重新掃描受影響目標，確認不再檢出此弱點。

修復路徑



先確認提供受影響回應的元件範圍，再設定強制套用 HSTS，最後透過回應檢查與重新掃描確認標頭已生效且不再檢出弱點。

弱點實例列表 (5/5)

弱點實例	請求方法
[redacted]	GET
[redacted]	GET
[redacted]	GET
[redacted]	GET
[redacted]	GET

LOW

缺少 X-Content-Type-Options 標頭

89

風險等級	OWASP 分類	弱點實例數量
低危	A02:2025 安全設定錯誤	5

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

未將 X-Content-Type-Options 設為 nosniff，舊版 IE 與 Chrome 可能對回應本文進行 MIME 嗅探，並以不同於宣告的內容類型解譯及顯示。

修復說明

01 盤點所有網頁回應及其應宣告的 Content-Type 內容類型。

02 設定各網頁回應的 Content-Type 標頭，使其符合實際內容類型。

03 於所有網頁回應設定 X-Content-Type-Options: nosniff 標頭。

修復驗證

- [ ] 檢查各網頁回應的 Content-Type 標頭是否符合實際內容類型。
- [ ] 確認所有網頁回應均含 X-Content-Type-Options: nosniff 標頭。
- [ ] 重新執行弱點掃描，確認不再檢出此標頭缺失。

修復路徑



先盤點受影響網頁及其內容類型，再修正 Content-Type 並設定 nosniff 標頭，最後以回應檢查與弱點掃描確認缺失不再被檢出。

弱點實例列表 (5/5)

弱點實例	請求方法
[redacted]	GET
[redacted]	GET
[redacted]	GET
[redacted]	GET
[redacted]	GET

LOW

頁面橫幅版本資訊洩漏

90

風險等級	OWASP 分類	弱點實例數量
低危	A02:2025 安全設定錯誤	4

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

回應內容包含伺服器版本橫幅字串，可能使攻擊者進一步鎖定所使用產品及版本的特定問題。

修復說明

01 檢查回應本文與錯誤頁，盤點所有洩露產品或版本的橫幅字串。

02 在 Web 伺服器設定中關閉版本揭露，設定 Apache ServerTokens 與 ServerSignature。

03 設定 Tomcat server 指令並部署自訂錯誤頁，避免預設頁面洩露版本。

修復驗證

- [ ] 以正常與錯誤請求檢查回應本文，不應再出現產品或版本橫幅。
- [ ] 使用掃描工具重測公開頁面與錯誤頁，確認未回傳版本資訊。

修復路徑



依序盤點正常與錯誤頁面的版本橫幅，套用伺服器隱藏設定及自訂錯誤頁，最後重測公開回應，確認不再揭露產品、伺服器或版本資訊。

弱點實例列表 (4/4)

弱點實例	請求方法
[redacted]	GET
[redacted]	GET
[redacted]	GET
[redacted]	GET

LOW

HTTPS 內容可透過 HTTP 存取

91

風險等級	OWASP 分類	弱點實例數量
低危	A04:2025 加密機制失效	3

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

原先透過 HTTPS（SSL/TLS 加密）存取的內容，亦可透過未加密的 HTTP 存取，可能使傳輸內容暴露。

修復說明

01 確認可同時透過 HTTPS 與 HTTP 存取的受影響內容。

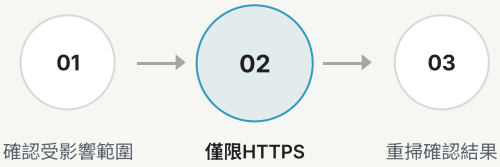
02 設定相關元件，確保受影響內容僅能透過 HTTPS 安全提供。

03 視受影響內容情況實作 HTTP Strict Transport Security。

修復驗證

- [ ] 檢查相關設定，確認受影響內容僅能透過 HTTPS 提供。
- [ ] 重新執行弱點掃描，確認不再檢出此項弱點。

修復路徑



先確認可透過 HTTP 存取的受影響內容與相關元件，將服務設定為僅以 HTTPS 提供，必要時導入 HSTS，最後檢查設定並重新掃描確認弱點已排除。

弱點實例列表（3/3）

弱點實例	請求方法
[redacted]	GET
[redacted]	GET
[redacted]	GET

LOW

私有 IP 資訊揭露

92

風險等級	OWASP 分類	弱點實例數量
低危	A01:2025 存取控制失效	1

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

HTTP 回應本文發現私有 IP 或 Amazon EC2 私有主機名稱，可能協助後續針對內部系統的攻擊。

修復說明

01 檢視受影響 HTTP 回應本文，確認所有私有 IP 資訊位置

02 移除 HTTP 回應本文中出現的私有 IP 位址與內部主機名稱資訊

03 將含位址的 HTML/JavaScript 註解改用伺服器端註解

修復驗證

- [ ] 檢查受影響 HTTP 回應本文，確認不再含私有 IP 或 EC2 私有主機名稱
- [ ] 重新執行弱點掃描，確認不再檢出 Private IP Disclosure

修復路徑



先確認受影響回應與註解中的私有 IP 與主機名稱資訊範圍，再予以移除或改為伺服器端註解，最後透過掃描確認不再檢出。

弱點實例列表 (1/1)

弱點實例	請求方法
[redacted]	GET

LOW

ICMP 時間戳記回應資訊洩露

93

風險等級	CVSS	連接埠
低危	2.1	general/icmp

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

遠端主機會回應 ICMP 時間戳記請求，洩露發送、接收與傳輸時間戳記。此資訊理論上可用於推測其他服務中較弱的時間型隨機數產生器。

修復說明

01 於遠端主機系統設定中，停用 ICMP 時間戳記回應功能，避免資訊洩露。

02 在邊界防火牆設定規則，封鎖雙向 ICMP 時間戳記請求與回應封包。

03 限制 ICMP 流量僅允許來自信任網路，阻擋外部不必要存取。

04 持續監控網路流量，留意不必要的 ICMP 時間戳記請求活動。

修復驗證

- [ ] 發送 ICMP 時間戳記請求確認不再收到回應。
- [ ] 檢查防火牆規則，確認已完整封鎖該類時間戳記封包。
- [ ] 重新掃描目標主機，確認此弱點已不再被偵測出現。

修復路徑



先確認會回應 ICMP 時間戳記請求的主機範圍，接著停用該功能或以防火牆完整封鎖流量，最後重新掃描以確認不再收到任何回應。

詳細資訊

The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0

LOW

SSH 支援弱 MAC 演算法

94

風險等級	CVSS	連接埠
低危	2.6	22

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

遠端 SSH 伺服器允許使用弱 MAC 演算法，可能降低連線資料完整性保護，增加資料遭竄改而未被偵測的風險。

修復說明

01 檢視並列出 SSH 伺服器目前所啟用的所有 MAC 演算法清單。

02 依清單停用已知強度不足、存在安全疑慮的弱 MAC 演算法設定。

03 僅保留並啟用目前業界建議之安全強度 MAC 演算法設定選項。

04 重新啟動 SSH 服務，以套用新設定並確保變更確實生效。

修復驗證

- [ ] 檢查 SSH 伺服器設定，確認弱 MAC 演算法已停用。
- [ ] 查詢伺服器支援之 MAC 演算法，確認僅剩安全選項。
- [ ] 重新執行弱點掃描，確認此弱點不再被檢出。

修復路徑



先確認伺服器目前啟用之弱 MAC 演算法清單，接著調整組態設定僅允許安全演算法，最後執行複掃以確認弱項已完全排除。

詳細資訊

The remote SSH server supports the following weak client-to-server MAC algorithm(s):

umac-64-etm@openssh.com
umac-64@openssh.com

The remote SSH server supports the following weak server-to-client MAC algorithm(s):

umac-64-etm@openssh.com
umac-64@openssh.com

LOW

TCP 時間戳記資訊洩漏

95

風險等級	CVSS	連接埠
低危	2.6	general

首次發現時間	上次發現時間
2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

遠端主機依 RFC1323/RFC7323 啟用 TCP 時間戳記選項，攻擊者可能藉此推算系統開機運作時間。

修復說明

01 Linux 主機於 sysctl 設定停用 TCP 時間戳記。

02 Windows 主機使用 netsh 指令停用時間戳記功能。

03 完成設定變更後，重新載入網路服務套用新的核心參數。

04 若系統無法完全停用時間戳記，應改為限制其對外回應行為。

修復驗證

- [ ] 擷取遠端主機的 TCP 封包，確認已無時間戳記選項存在。
- [ ] 檢查 sysctl 或 netsh 設定值已生效為停用。
- [ ] 重新執行弱點掃描，確認此項弱點已不再被回報出現。

修復路徑



先盤點受影響主機範圍，接著於作業系統層級停用或限制 TCP 時間戳記功能，最後重新執行掃描以確認該選項已不再對外暴露。

詳細資訊

It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 3242731869
Packet 2: 4239448010

LOW

PHPinfo 資訊洩漏頁面

96

風險等級	CVSS	CWE ID
低危	—	CWE-200

連接埠	首次發現時間	最近發現時間
443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

系統偵測到可公開存取的 PHPinfo 頁面，其輸出內容可能洩漏詳細且敏感的 PHP 環境資訊。

修復說明

01 從所有公開可存取的網站與系統中，移除 PHPinfo 診斷頁面。

02 若業務需求必須保留此頁面，應嚴格限制僅授權使用者可存取。

03 於正式上線環境中，停用 phpinfo 函式以降低風險。

04 檢查伺服器上是否仍存在其他診斷、除錯或測試用頁面。

修復驗證

- [ ] 確認 PHPinfo 頁面已無法於公開網路存取。
- [ ] 檢查存取控制設定，確保僅授權使用者可讀取頁面。
- [ ] 重新掃描目標系統，確認該弱點已不再被檢出。

修復路徑



先確認暴露的 PHPinfo 頁面範圍及影響程度，接著移除頁面或限制存取權限，最後重新掃描驗證該頁面已無法公開取得。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

LOW

PHPinfo 資訊洩漏頁面

97

風險等級	CVSS	CWE ID
低危	—	CWE-200

連接埠	首次發現時間	最近發現時間
8080	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

系統偵測到可公開存取的 PHPinfo 頁面，其輸出內容可能洩漏詳細且敏感的 PHP 環境資訊。

修復說明

01 從所有公開可存取的網站與系統中，移除 PHPinfo 診斷頁面。

02 若業務需求必須保留此頁面，應嚴格限制僅授權使用者可存取。

03 於正式上線環境中，停用 phpinfo 函式以降低風險。

04 檢查伺服器上是否仍存在其他診斷、除錯或測試用頁面。

修復驗證

- [ ] 確認 PHPinfo 頁面已無法於公開網路存取。
- [ ] 檢查存取控制設定，確保僅授權使用者可讀取頁面。
- [ ] 重新掃描目標系統，確認該弱點已不再被檢出。

修復路徑



先確認暴露的 PHPinfo 頁面範圍及影響程度，接著移除頁面或限制存取權限，最後重新掃描驗證該頁面已無法公開取得。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
	2026-11-17 17:40:31	2026-11-17 17:40:31

LOW

PHPinfo 資訊洩漏頁面

98

風險等級	CVSS	CWE ID
低危	—	CWE-200

連接埠	首次發現時間	最近發現時間
80	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

系統偵測到可公開存取的 PHPinfo 頁面，其輸出內容可能洩漏詳細且敏感的 PHP 環境資訊。

修復說明

01 從所有公開可存取的網站與系統中，移除 PHPinfo 診斷頁面。

02 若業務需求必須保留此頁面，應嚴格限制僅授權使用者可存取。

03 於正式上線環境中，停用 phpinfo 函式以降低風險。

04 檢查伺服器上是否仍存在其他診斷、除錯或測試用頁面。

修復驗證

- [ ] 確認 PHPinfo 頁面已無法於公開網路存取。
- [ ] 檢查存取控制設定，確保僅授權使用者可讀取頁面。
- [ ] 重新掃描目標系統，確認該弱點已不再被檢出。

修復路徑



先確認暴露的 PHPinfo 頁面範圍及影響程度，接著移除頁面或限制存取權限，最後重新掃描驗證該頁面已無法公開取得。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

LOW

PHPinfo 資訊洩漏頁面

99

風險等級	CVSS	CWE ID
低危	—	CWE-200

連接埠	首次發現時間	最近發現時間
8443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

系統偵測到可公開存取的 PHPinfo 頁面，其輸出內容可能洩漏詳細且敏感的 PHP 環境資訊。

修復說明

01 從所有公開可存取的網站與系統中，移除 PHPinfo 診斷頁面。

02 若業務需求必須保留此頁面，應嚴格限制僅授權使用者可存取。

03 於正式上線環境中，停用 phpinfo 函式以降低風險。

04 檢查伺服器上是否仍存在其他診斷、除錯或測試用頁面。

修復驗證

- [ ] 確認 PHPinfo 頁面已無法於公開網路存取。
- [ ] 檢查存取控制設定，確保僅授權使用者可讀取頁面。
- [ ] 重新掃描目標系統，確認該弱點已不再被檢出。

修復路徑



先確認暴露的 PHPinfo 頁面範圍及影響程度，接著移除頁面或限制存取權限，最後重新掃描驗證該頁面已無法公開取得。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
	2026-11-17 17:40:31	2026-11-17 17:40:31

LOW

PHPinfo 資訊洩漏頁面

100

風險等級	CVSS	CWE ID
低危	—	CWE-200

連接埠	首次發現時間	最近發現時間
10443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

系統偵測到可公開存取的 PHPinfo 頁面，其輸出內容可能洩漏詳細且敏感的 PHP 環境資訊。

修復說明

01 從所有公開可存取的網站與系統中，移除 PHPinfo 診斷頁面。

02 若業務需求必須保留此頁面，應嚴格限制僅授權使用者可存取。

03 於正式上線環境中，停用 phpinfo 函式以降低風險。

04 檢查伺服器上是否仍存在其他診斷、除錯或測試用頁面。

修復驗證

- [ ] 確認 PHPinfo 頁面已無法於公開網路存取。
- [ ] 檢查存取控制設定，確保僅授權使用者可讀取頁面。
- [ ] 重新掃描目標系統，確認該弱點已不再被檢出。

修復路徑



先確認暴露的 PHPinfo 頁面範圍及影響程度，接著移除頁面或限制存取權限，最後重新掃描驗證該頁面已無法公開取得。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
	2026-11-17 17:40:31	2026-11-17 17:40:31

LOW

PHPinfo 資訊洩漏頁面

101

風險等級	CVSS	CWE ID
低危	—	CWE-200

連接埠	首次發現時間	最近發現時間
9443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

系統偵測到可公開存取的 PHPinfo 頁面，其輸出內容可能洩漏詳細且敏感的 PHP 環境資訊。

修復說明

01 從所有公開可存取的網站與系統中，移除 PHPinfo 診斷頁面。

02 若業務需求必須保留此頁面，應嚴格限制僅授權使用者可存取。

03 於正式上線環境中，停用 phpinfo 函式以降低風險。

04 檢查伺服器上是否仍存在其他診斷、除錯或測試用頁面。

修復驗證

- [ ] 確認 PHPinfo 頁面已無法於公開網路存取。
- [ ] 檢查存取控制設定，確保僅授權使用者可讀取頁面。
- [ ] 重新掃描目標系統，確認該弱點已不再被檢出。

修復路徑



先確認暴露的 PHPinfo 頁面範圍及影響程度，接著移除頁面或限制存取權限，最後重新掃描驗證該頁面已無法公開取得。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
	2026-11-17 17:40:31	2026-11-17 17:40:31

LOW

SSL 憑證過期

102

風險等級	CVSS	CWE ID
低危	—	—

連接埠	首次發現時間	最近發現時間
8443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

SSL 憑證已過期，導致無法建立安全加密的 HTTPS 連線，用戶端存取時可能出現警告或連線被阻擋。

修復說明

01 盤點並列出所有目前使用該過期憑證的相關網域與子網域清單。

02 向憑證機構申請或自行產生新的有效 SSL/TLS 憑證。

03 將取得的新憑證正確安裝至所有受影響的伺服器及服務上。

04 設定憑證到期前自動更新機制，避免憑證未來再次過期失效。

05 重新啟動或重載網頁伺服器服務，使新憑證設定立即生效。

修復驗證

- [ ] 檢查伺服器上新憑證的有效起訖日期是否正確。
- [ ] 確認用戶端瀏覽 HTTPS 連線可正常建立且無警告訊息。
- [ ] 重新執行掃描，確認過期憑證已不再被系統偵測到。

修復路徑



先盤點所有受影響網域，申請並更換為有效的新憑證並完成安裝設定，最後重新驗證 HTTPS 連線並複測確認弱點已排除。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

LOW

自簽署 SSL 憑證

103

風險等級	CVSS	CWE ID
低危	—	—

連接埠	首次發現時間	最近發現時間
443	2026-11-17 17:40:31	2026-11-17 17:40:31

弱點說明

自簽署憑證並非由憑證授權機構核發，建立容易且無需成本，但缺乏信任價值，可能導致使用者難以驗證服務真實性。

修復說明

01 向正式的憑證授權機構申請或購買，並產生合法的 SSL 憑證。

02 將取得的受信任憑證安裝於受影響的伺服器或相關服務上。

03 設定該服務改用新核發的受信任憑證，以取代原有的自簽憑證。

04 在憑證核發期間，暫時限制對該服務的存取以降低風險。

修復驗證

- [ ] 確認該憑證確實由受信任的憑證授權機構核發。
- [ ] 確認瀏覽器與各用戶端不再顯示任何信任警告訊息。
- [ ] 重新掃描該服務，確認此弱點已不再被檢測出來。

修復路徑



先確認所有使用自簽署憑證的服務範圍，接著申請並部署受信任的憑證，最後重新掃描驗證服務信任關係已正確建立無誤，確保風險徹底排除。

命中位置列表 (1/1)

Matched at	首次發現時間	最近發現時間
[redacted]	2026-11-17 17:40:31	2026-11-17 17:40:31

EXTERNAL EXPOSURE SUMMARY

外部曝險摘要

12	53	6
發現子網域	公開 Web 資產	公開 IP

需優先確認

需關注對外服務	21	對外開放 Port	19	憑證異常	6

公開 Web 資產連線架構

經 CDN／WAF 代理 53 · 100%　　直接對外連線 0 · 0%

以 53 個可判定連線架構的活躍 Web 資產為統計基準

需關注對外服務

服務	建議確認事項
[redacted]	檢查資料庫連線來源限制
[redacted]	檢查資料庫連線來源限制
[redacted]	檢查資料庫連線來源限制
[redacted]	檢查資料庫連線來源限制
[redacted]	檢查資料庫連線來源限制
[redacted]	檢查資料庫連線來源限制
[redacted]	檢查資料庫連線來源限制
[redacted]	檢查資料庫連線來源限制

EXTERNAL EXPOSURE SUMMARY

外部曝險摘要

服務	建議確認事項
[redacted]	檢查資料庫連線來源限制
[redacted]	檢查資料庫連線來源限制
[redacted]	檢查資料庫連線來源限制
[redacted]	檢查資料庫連線來源限制
[redacted]	檢查資料庫連線來源限制
[redacted]	檢查資料庫連線來源限制
[redacted]	檢查資料庫連線來源限制
[redacted]	檢查資料庫連線來源限制
[redacted]	檢查資料庫連線來源限制
[redacted]	檢查資料庫連線來源限制
[redacted]	檢查資料庫連線來源限制
[redacted]	查核測試郵件查閱權限
[redacted]	查核測試郵件查閱權限
[redacted]	查核測試郵件查閱權限

對外暴露僅表示可由網際網路存取，不代表已確認存在可利用弱點。

EXTERNAL EXPOSURE DETAIL

外部曝險詳情

對外開放 Port 詳情

Port	協定	服務	IP
22	TCP	SSH	
80	TCP	HTTP	
443	TCP	HTTPS	
587	TCP	SMTP	
2052	TCP	HTTP	
2053	TCP	HTTPS	
2082	TCP	HTTP	
2083	TCP	HTTPS	
2086	TCP	HTTP	
2087	TCP	HTTPS	
2095	TCP	HTTP	
2096	TCP	HTTPS	
6379	TCP	REDIS	
8000	TCP	HTTP	
8080	TCP	HTTP	

EXTERNAL EXPOSURE DETAIL

外部曝險詳情 [redacted]

Port	協定	服務	IP
8443	TCP	HTTPS	[redacted]
8880	TCP	HTTP	[redacted]
9443	TCP	HTTPS	[redacted]
10443	TCP	HTTPS	[redacted]

憑證異常詳情

域名	異常問題
[redacted]	域名不符 (Port 443)、自簽憑證 (Port 443)、憑證信任未確認 (Port 443)、憑證過期 (Port 8443)、域名不符 (Port 8443)、憑證信任未確認 (Port 8443)、域名不符 (Port 9443)、憑證信任未確認 (Port 9443)、域名不符 (Port 10443)、憑證信任未確認 (Port 10443)
[redacted]	域名不符、憑證信任未確認
[redacted]	域名不符、憑證信任未確認
[redacted]	域名不符、憑證信任未確認
[redacted]	域名不符 (Port 443)、自簽憑證 (Port 443)、憑證信任未確認 (Port 443)、憑證過期 (Port 8443)、域名不符 (Port 8443)、憑證信任未確認 (Port 8443)、域名不符 (Port 9443)、憑證信任未確認 (Port 9443)、域名不符 (Port 10443)、憑證信任未確認 (Port 10443)

EXTERNAL EXPOSURE DETAIL

外部曝險詳情 [redacted]

域名	異常問題
[redacted]	域名不符 (Port 443)、自簽憑證 (Port 443)、憑證信任未確認 (Port 443)、憑證過期 (Port 8443)、域名不符 (Port 8443)、憑證信任未確認 (Port 8443)、域名不符 (Port 9443)、憑證信任未確認 (Port 9443)、域名不符 (Port 10443)、憑證信任未確認 (Port 10443)

域名資訊

本頁列示主要網域的註冊資訊、名稱伺服器、DNSSEC，以及 SSL／TLS 憑證資訊。

域名資訊

主要域名	
註冊日期	
到期日期	
註冊管理機構	
名稱伺服器	
DNSSEC	未啟用

SSL／TLS 憑證資訊

憑證簽發機構	Redmark synthetic lab 憑證已讀取，但未通過信任驗證；不代表連線安全。
憑證生效日	2026-10-29
憑證到期日	2027-10-29 （剩餘 345 天）
此次連線 TLS 版本	TLSv1.3

技術棧

以下技術資訊依公開回應、服務特徵及產品指紋識別結果彙整。

類別	元件	版本
JavaScript 框架	AngularJS	1.3.8
UI 框架	Bootstrap	3.3.2
JavaScript 函式庫	jQuery	1.11.0
JavaScript 函式庫	jQuery UI	1.10.4
Web 伺服器、反向代理	Nginx	1.30.6

完整資產附件

以下明細因資料量較大，不於 PDF 報告中逐筆列示；完整清冊請於 Redmark 平台下載 XLSX 附件。

域名清冊	13 個域名
公開 IP 清單	6 個
SSL／TLS 憑證清單	6 筆