TLP:WHITE

熱門架站工具 Wordpress 之漏洞威脅分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2025 年 04 月

一、引言

1. WordPress 是可架設網站的開源自由軟體，它適合架設部落格、小型企業網站與電商平台。對於有架站需求又經費不足的使用者或組織而言，它是一個很好的選擇。
2. WordPress 軟體有兩種版本，一為 WordPress.com，另一為 WordPress.org。
   (1) WordPress.com 為線上部落格平台，專門提供在平台上免費使用，或付費建立 WordPress 網站。申請者無法獲得完整的網站控制權。在免費版本中無法上傳佈景主題與外掛程式，也不允許修改程式碼。
   (2) WordPress.org 提供一個開源的自由軟體，可以下載 WordPress 的原始碼到自己的主機上。使用者可以自行修改原始碼、更換佈景主題與外掛程式等等。
3. 目前全球使用 WordPress 架站的網站很多，而從 2025/01~2025/04 至今陸續發生多起 WordPress 網站漏洞利用的攻擊事件，可見 WordPress 軟體之安全性與漏洞修補是一個重要議題。

二、 近期 WordPress 網站漏洞利用的攻擊事件

1. 2025/01 SlashNext 發現意圖使用合法網站來竊取購物者信用卡資料的 WordPress 外掛程式 PhishWP。
2. 2025/01 WordPress 知名快取套件 W3 Total Cache 被發現因為缺少權限檢查，使具有訂閱者等級權限的使用者可進行未經授權的操作，受影響網站可能超過百萬個。(CVE-2024-12365)
3. 2025/01 Patchstack 發現 WordPress 佈景主題 RealHome 與外掛程式 Easy Real Estate 存在重大漏洞。

(1) 佈景主題 RealHome:未經身分驗證的權限提升漏洞。(CVE-2024-32444)

(2) 外掛程式 Easy Real Estate:因為外掛程式未驗證電子郵件信箱發出的 POST 請求，攻擊者只要知道管理者的電子郵件信箱，就能在無須掌握對應密碼的情況下，登入任何使用者的帳號。(CVE-2024-32445)

4. 2025/02 Patchstack 發現 WordPress 管理流程改善外掛程式 Admin and Site Enhancements（ASE）存在高風險權限提升漏洞。(CVE-2024-4333、CVE-2025-24648)
5. 2025/02 Wordfence 揭露 WordPress 表單外掛程式 Everest Forms 存在任意檔案上傳漏洞(CVE-2025-1128)，讓未經身分驗證的攻擊者可將任意檔案上傳網站後，從遠端執行任意程式碼並且讀取或刪除網站上檔案。
6. 2025/03 主機代管公司 GoDaddy 發現駭客使用 DollyWay 惡意軟體，來控制受害網站後將使用者重新導向特定廣告網站牟利。
7. 2025/03 Patchstack 揭露 WordPress 免費資安與防火牆外掛程式 WP Ghost 存在本機檔案包含（LFI）漏洞(CVE-2025-26909)，影響高達 20 萬個網站。
8. 2025/03 Wordfence 指出 WordPress 網站會員系統外掛程式 User Registration & Membership 存在未經身分驗證權限提升漏洞 (CVE-2025-2563)，導致未經授權的攻擊者可藉由建立新的使用者帳號，得到管理員的角色。

三、 2024 年 WordPress 漏洞威脅分析

1. 根據 Wordfence 在 2024/4 發佈的「2024 年 WordPress 安全性報告」，可得知下列重點資訊。

(1) 2024 年揭露的 WordPress 漏洞數量較 2023 年增加了 68%。

(2) 2024 年揭露的 WordPress 漏洞中有 81% 的 CVSS 嚴重程度評分為「中等」。

(3) 2024 年揭露的所有漏洞中約有 35% 在 2025 年仍未修補。

(4) 跨站腳本漏洞是 2024 年揭露的第一大漏洞類型。

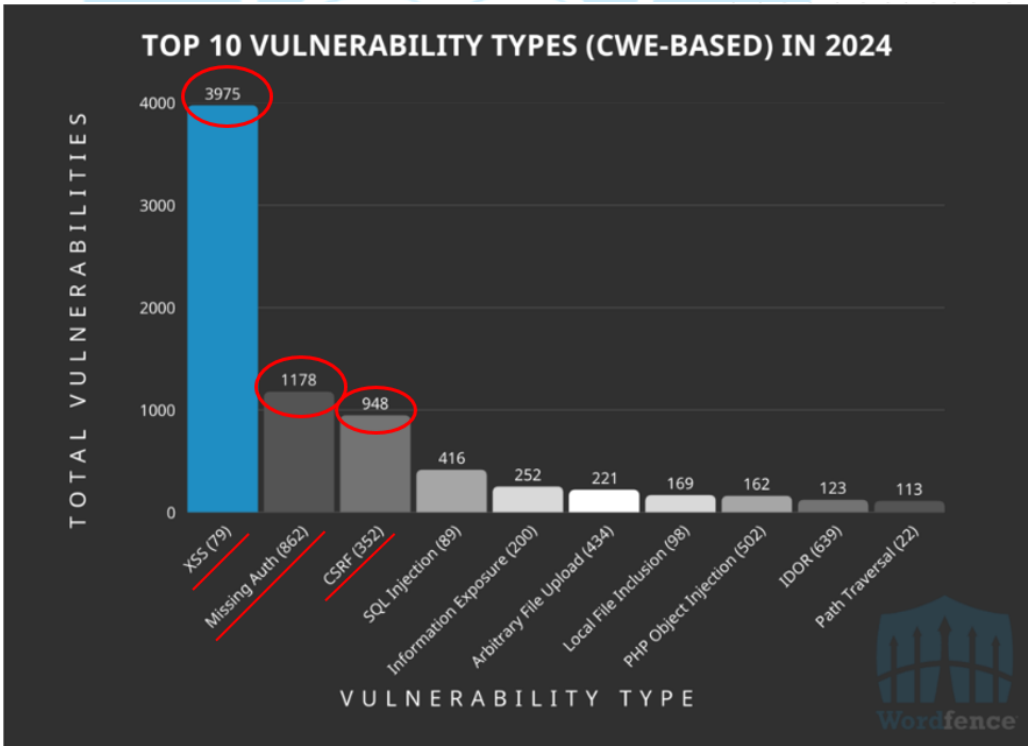
(5) 2024 年揭露的所有漏洞中有 7.4% 被認為是高威脅。這比 2023 年揭露的高威脅問題數量增加了 149%。

(6) 外掛程式漏洞仍然是 WordPress 面臨的最大軟體威脅，佔已揭露所有漏洞的 96%。

(7) 截至 2024 年底，對 WordPress 進行的密碼攻擊整體呈現下降趨勢，而針對軟體漏洞的攻擊則呈現上升趨勢。

2. 2024 年揭露的最常見漏洞類型

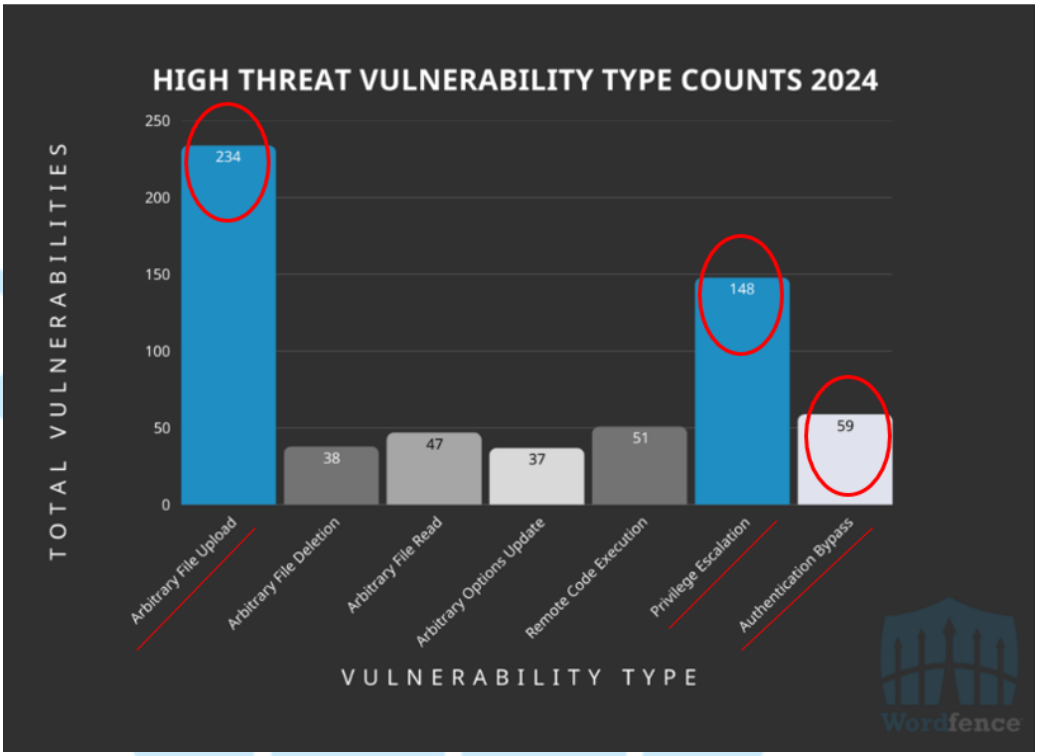
所揭露的最常見漏洞類型是跨站腳本 (CWE-79)，佔所揭露漏洞的 46%。排名第二的是缺少授權（CWE-862），佔所有漏洞的 13%。跨站請求偽造（CWE-352）則位居第三，，佔所有漏洞的 11%。



資料來源:Wordfence 之「2024 年 WordPress 安全性報告」

3. 2024 年揭露的高風險漏洞

2024 年最常見的高威脅漏洞類型是“任意檔案上傳”，佔總數的 38%。第二常見的是權限提升，佔總數的 24%，其次是繞過身份驗證，佔總數的 10%。由於攻擊者只需利用單一漏洞即可輕鬆獲得存取，而且通常只需很少的要求，因此這些漏洞被認為是威脅性最高的漏洞之一。



資料來源:Wordfence 之「2024 年 WordPress 安全性報告」

(1) 任意文件上傳

此漏洞使攻擊者能夠將惡意檔案（通常是 PHP 腳本）上傳到 Web 伺服器。若可以存取並執行該檔案，就有可能控制該網站。

(2) 任意檔案刪除

此漏洞允許攻擊者刪除伺服器上的關鍵檔案。例如: wp-config.php，包含資料庫連接詳細資訊和安全金鑰。

(3) 任意選項更新

此漏洞允許攻擊者修改關鍵網站選項。例如，可以更改預設用戶角

色或註冊設定，以允許任何人註冊為管理員。這為攻擊者提供了登入和控制網站的直接途徑。

(4) 任意文件讀取

此漏洞使攻擊者能夠讀取伺服器上的敏感檔案。這可能包括資料庫憑證、 安全性金鑰的設定檔案，甚至是可能洩露有關伺服器設定和潛在漏洞的資訊的系統檔案。

(5) 遠端程式碼執行

這是最嚴重的漏洞之一，因為它允許攻擊者在 Web 伺服器上執行任意程式碼。這實際上使攻擊者能夠完全控制網站甚至伺服器本身。

(6) 權限提升

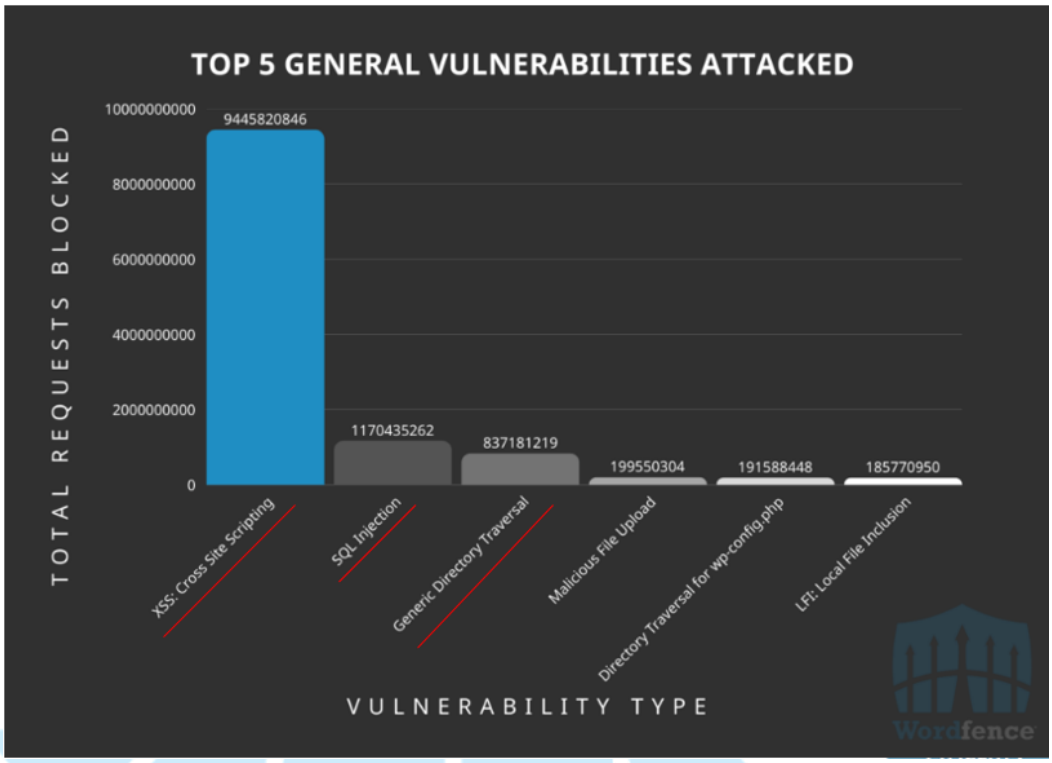
此漏洞允許攻擊者提升其在系統上的權限。例如，存取權限有限的使用者（例如:訂閱者）可以利用漏洞來取得管理權限。

(7) 繞過身份驗證

此漏洞允許攻擊者繞過標準登入程序並在無需提供有效憑證的情況下存取網站。這通常會導致權限提升，因為攻擊者可能能夠承擔管理員或其他高權限使用者的角色。

4. 2024 年遭受攻擊的前 5 種通用漏洞類型

2024 年跨網站腳本 (XSS) 成為惡意行為者最常攻擊的漏洞，SQL 注入為第二大最常被攻擊的漏洞類型，通用目錄遍歷位居第三。針對這些漏洞的大量攻擊凸顯了 Web 應用程式防火牆 (WAF) 的迫切必要性。建置 WAF 可以識別和阻止惡意的請求，從而有效地防止這些常見漏洞被利用(即使在沒有修補程式的情況下)。



資料來源:Wordfence 之「2024 年 WordPress 安全性報告」

四、 漏洞利用:Must-Use Plugins 外掛程式資料夾

1. 2025/04 Sucuri 揭露駭客利用 Must-Use Plugins(mu-plugins)外掛程式資料夾，在網站植入後門程式，以便遠端執行惡意程式碼。
2. mu-plugins 是 WordPress 中的一個特殊資料夾，位於「wp-content/mu-plugins/」。
3. 在此資料夾內的外掛程式會自動對所有網頁啟動，攻擊者利用此資料夾來保持持久性並逃避偵測，因為放置在此處的檔案會自動執行，並且不容易從 WordPress 管理面板中停用(因為 mu-plugins 沒有列在 WordPress 外掛程式介面中)。攻擊者會安裝多個後門以確保持久性。
   (1) 遠端執行任意 PHP 程式碼：透過解碼和評估從外部來源取得的有效負載。
   (2) 通訊加密：透過使用 AES 加密，攻擊者隱藏了惡意 URL 和命令，使得偵測更加困難。

(3) 保持控制：使用多個後門意味著即使發現一個後門，也可以使用其他後門重新獲得存取權限。

4. 有三種型態的攻擊行動如下:

(1) 藉由假的軟體更新網站的名義，將使用者重新導向外部網站。例如: wp-content/mu-plugins/redirect.php 將網站訪客重新導向到外部惡意網站。

(2) 在網站植入 Web Shell，使攻擊者可執行任意程式碼。例如:./wp-content/mu-plugins/index.php 允許攻擊者執行任意程式碼，來完全控制網站。

(3) 利用指令碼在網站裡注入垃圾內容，來提升搜尋引擎最佳化 SEO 排名或是進行詐欺行為。例如:位於 wp-content/mu-plugins/ custom-js-loader.php 的垃圾郵件注入腳本。該腳本被用來向受感染的網站注入不需要的垃圾內容。

5. WordPress 網站如何被入侵

(1) 利用易受攻擊的外掛程式或佈景主題—如果網站執行過時的軟體，攻擊者可能會利用已知漏洞上傳惡意檔案。

(2) 洩漏管理員憑證－如果攻擊者獲得管理員帳戶的存取權限，就可以手動將惡意軟體放入 mu-plugins 中。

(3) 濫用安全性較差的託管環境—弱的檔案權限或過時的伺服器設定可能允許攻擊者修改 WordPress 核心檔案。

6. WordPress 網站受攻擊後的特徵

(1) 將網路流量重定導向到惡意網站。

(2) 透過後門程式保持持續存取網站。

(3) 注入垃圾內容來操縱 SEO 排名。

7. 處理方式

(1) 掃描 WordPress 安裝資料夾中是否有惡意檔案，尤其是 mu-plugins

資料夾中的檔案。

(2) 檢查未經授權的管理員帳戶，並刪除任何可疑的帳戶。

(3) 審核所安裝的外掛程式，並刪除任何看起來不熟悉的外掛程式。

(4) 使用可信任的網站安全掃描程式，來識別其他受感染的檔案。

(5) 透過將下列語法新增至 .htaccess 檔案來防止在 uploads 資料夾中執行 PHP：

```
<FilesMatch "\.php$"> Deny from all </FilesMatch>
```

(6) 將 WordPress 核心、外掛程式和佈景主題更新到最新版本，以防止再次感染。

(7) 安裝資安防護的外掛程式來監控檔案完整性和異常活動。

(8) 變更所有管理員密碼，並啟用雙重認證 (2FA) 以增強安全性。

五、 總結與建議

1. 由於 Wordfence 漏洞賞金計畫的鼓勵，使得 WordPress 被揭露的漏洞數量持續增加，也促進資安研究人員與軟體開發商之間合作，快速修補這些漏洞。
2. 發現的大多數漏洞被歸類為「中等」嚴重性，需要特定層級的存取權限才能利用，對一般的 WordPress 網站產生最小的威脅，而高威脅漏洞雖然增加，但仍只佔總數的一小部分。
3. 駭客攻擊 WordPress 網站的事件頻傳，其中較常見的攻擊手法是利用外掛程式的弱點，進一步控制整個網站。因此，刪除未使用和廢棄的 WordPress 外掛程式和佈景主題是很重要的防範措施。
4. 在校園內常出現在因執行計畫架設的 WordPress 網站或因經費少而架設 WordPress 的學校網站，這些網站的管理者若沒定期維護網站與修補漏洞，將會使網站淪為駭客發動攻擊時的跳板主機(中繼站)。

5. 在處理 WordPress 網站的攻擊事件方面，可從網站管理與防護方向思考，提供下面 2 個面向來偵測與防範。

(1) 管理面

定期檢視所使用的外掛程式是否存在漏洞，並定期更新軟體。

刪除未使用和廢棄的 WordPress 外掛程式和佈景主題。

(2) 技術面

建置 Web 應用程式防火牆 (WAF)來識別和阻止惡意的請求。

進行網路流量監控，例如:異常流量的檢測。

在網站伺服器上安裝端點保護軟體，例如:採用 EDR 能偵測到記憶體內的執行、程序注入和異常腳本等行為。

參考資料

1. **2024 Annual WordPress Security Report by Wordfence** (https://www.wordfence.com/blog/2025/04/2024-annual-wordpress-security-report-by-wordfence/)
2. **WordPress 外掛程式資料夾成網路攻擊溫床！網站被植入惡意程式及垃圾內容**(https://www.ithome.com.tw/news/168179)
3. **提供會員系統的 WordPress 外掛存在重大漏洞，6 萬網站受到波及** (https://www.ithome.com.tw/news/168100)
4. **WordPress 外掛 WP Ghost 有重大漏洞，高達 20 萬個網站暴露在這個風險之下**(https://www.ithome.com.tw/news/168047)
5. **2 萬個 WordPress 網站淪陷，遭到惡意軟體攻擊 DollyWay 入侵** (https://www.ithome.com.tw/news/168034)
6. **WordPress 表單外掛 Everest Forms 存在重大漏洞，10 萬網站曝險** (https://www.ithome.com.tw/news/167602)
7. **WordPress 管理流程強化外掛存在高風險漏洞，逾 10 萬網站恐曝險** (https://www.ithome.com.tw/news/167310)
8. **供房地產網站使用的 WordPress 佈景主題、外掛存在重大漏洞，攻擊者有機會得到 3 萬個網站的管理權限** (https://www.ithome.com.tw/news/167149)

9. **W3 Total Cache 修補高風險漏洞，百萬 WordPress 網站曝攻擊風險**
(https://www.ithome.com.tw/news/167033)
10. **駭客打造惡意 WordPress 外掛 PhishWP，意圖藉由合法網站竊取購物者信用卡資料**(https://www.ithome.com.tw/news/166870)
11. **Hidden Malware Strikes Again: Mu-Plugins Under Attack**
(https://blog.sucuri.net/2025/03/hidden-malware-strikes-again-mu-plugins-under-attack.html)
12. **Hidden Backdoors Uncovered in WordPress Malware Investigation**
(https://blog.sucuri.net/2025/02/hidden-backdoors-uncovered-in-wordpress-malware-investigation.html)