TLP:WHITE

網站安全管理指南

臺灣學術網路危機處理中心團隊(TACERT)製

2022 年 8 月修訂 V2 版

一、網站安全緣起

在網路蓬勃發展的世界，不論是線上購物、玩遊戲、銀行轉帳、瀏覽新聞…等等很多事情都是透過網站提供服務來完成的，而網站的架設是各機關、學校與企業必備的業務。當一個網站架設完成，後續的維護管理是一個很重要的議題，而如何讓一個網站能在正常運作之下免於駭客入侵與使用者個資外洩的問題是很重要的。有鑑於此，本文將針對如何加強網站安全進行探討。

二、網站風險

提到網站安全風險，就必須說到 OWASP 的前十大網站安全風險排名，在 2021 年 OWASP 公布最新版的風險排名如下。

1.權限控制失效(Broken Access Control)

相對於上一個版本(2017 版)，此類排名上升了四個名次，而名列榜首。權限控制失效是指未將相關系統設定適當的權限控管，而容易讓駭客利用此類漏洞來對系統內相關資訊進行更動，甚至可將惡意軟體安裝到系統中。

2.加密機制失效(Cryptographic Failures)

此類問題主要在說明系統加密機制的失敗，而造成敏感性資料外洩或系統被破壞，例如:以明碼（http）的方式而非以加密(https)的方式傳輸機敏資料而被駭客所擷取。又或者密碼等機敏資料未進行有效的保護，例如:未以受信任的加密方式來對系統內的密碼資訊進行加密。

3.注入式攻擊(Injection)

此類攻擊為最古老且最廣泛的攻擊。最廣為人知的攻擊方式即為跨網站攻擊(Cross-Site Scripting)及 SQL Injection 等攻擊方式。在此類攻擊中，駭客

利用程式或系統的漏洞，將惡意指令注入至系統來執行未經授權的命令，以取得敏感資料破壞系統。一般而言，此類攻擊可透過程式碼檢視(Code Review)來修補程式漏洞，或利用 Web 應用程式防火牆 (Web Application Firewall,WAF)來偵測及阻擋惡意的攻擊流量，以預防此類攻擊。

4.不安全設計(Insecure Design)

此為新進榜的漏洞，主要說明在應用程式的開發過程中，設計階段因未嚴謹的考量安全問題而造成的相關風險。例如：系統設計當登入錯誤達 5 次即直接鎖定該用戶，如此即可讓駭客利用來針對合法的用戶故意輸入錯誤的密碼，而導致該用戶被系統所鎖定。

5.安全設定缺陷(Security Misconfiguration)

此類漏洞主要發生在系統未設定適當的安全組態，例如在系統上線前未更改預設的組態或未將系統從偵錯（Debug）模式改為上線(Release)模式，導致可能洩漏過多的系統資訊而造成潛在的資安危害。

6.危險或過舊的元件(Vulnerable and Outdated Components)

此類漏洞主要發生在未適時的更新系統內具有危險或過舊的元件，通常會建議管理者可定期的進行漏洞掃描，並定時更新相關元件。

7.認證及驗證機制失效(Identification and Authentication Failures)

此類漏洞主要發生在系統採用無效的身份認證機制，導致駭客可繞過相關機制而登入至系統。例如：除了帳號/密碼的方式來驗證外，另外可再加上圖形驗證的機制來避免系統遭受暴力攻擊。除此之外，可適當的採取時限鎖定的方式（如 5 分鐘內登入錯誤達 10 次即鎖定 10 分鐘），即可有效提升認證及驗證機制的安全性。

8.軟體及資料完整性失效(Software and Data Integrity Failures)

這是全新的漏洞種類，主要在說明系統中程式與資料因缺乏資料完整性驗

證機制而遭到篡改或損壞。例如：系統內程式已被置換為惡意軟體，若系統無有效的完整性驗證將無法得知此類狀況，進而擴大危害的災情。建議可在系統導入如單向雜湊（HASH）等機制來確保系統程式與資料的完整性安全。

9.資安記錄及監控失效(Security Logging and Monitoring Failures)

此類漏洞主要發生在系統未採用有效的記錄及監控機制將導致在資安事件發生後，無法有效的回溯相關證據或發現當下駭客入侵的跡象。建議系統需監控並確認需記錄的重要事件（例如登入失敗事件），以便可日常檢核及事後回溯。

10.伺服端請求偽造(Server-Side Request Forgery (SSRF))

隨著雲端服務的盛行，有越來越多的服務是透過中介伺服器上的 API 來取得使用者的要求，而後再傳遞至後端的服務伺服器進行處理。此類漏洞即是未能有效的驗證使用者的要求，而可能導致駭客利用一個捏造的惡意請求，即可傳遞至後端的服務伺服器，進而導致後端的服務伺服器遭受攻擊。

在學術網路中，除了上述的網站風險外，比較常出現的網站安全缺失如下:

(1)系統管理者使用同一組帳號與密碼管理多台網站主機。

(2)網站主機內開啟常被駭客攻擊的 port，如 445 port 或 3389 port。

(3)系統管理者未定期更換密碼。

(4)網站提供上傳檔案功能，但未限制上傳檔案格式與進行檔案存取權限的控管。

(5)系統管理者未時常檢視網站狀態，尤其是因計畫而建立的網站。

(6)網站主機內有連結網路芳鄰的共用資料夾存在，提高主機感染病毒的風險。

(7)網站主機未安裝防毒軟體。

(8)網站主機未開啟主機內的防火牆功能。

(9)系統管理者未修補系統或應用程式的漏洞。

(10)系統管理者未發現網站主機被植入挖礦程式。

(11)網站主機開啟遠端桌面連線功能，但未限制連線來源 IP。

(12) 網站缺乏有效的輸入驗證機制，攻擊者將惡意程式碼作為輸入內容植入網頁或 URL，使用者端瀏覽時執行惡意程式碼。

三、校園網站常見之網頁攻擊

1.網頁置換

該攻擊手法也可稱為網頁竄改，此為系統遭駭客入侵後，取得系統管理員權限，以進行更換網頁的手法。早期該手法以惡意作劇性質為目的，演變至現今，則以設置跳板主機、惡作劇、中繼站性質居多。在此類攻擊中，駭客通常會將原本的網頁置換成自己的內容，大膽地去表達政治或社會訴求。他們也可從被置換的網頁中進行惡意的重新導向或放置漏洞攻擊程式碼，以便在瀏覽者電腦上安裝惡意軟體。

2.惡意網頁

它是指網頁被寫入惡意程式碼或惡意連結，而這些網頁內容包含隱藏或彈出視窗，連結到包含有病毒、木馬程式、Badware 或大量不當廣告的網頁都算惡意網頁。例如:網站隱碼，在網頁上看不到任何連結，但是網頁語法內有隱藏連結與廣告內容。解碼前為一大段亂碼，解碼後內容會顯現，主要是因為設定「display:none」，故網頁上未顯示出來內容。

3.釣魚網頁

駭客會架設假冒的網站或登入網頁來蒐集機敏資訊，也開發出網址嫁接攻擊。網址嫁接攻擊會附上一個惡意網址，讓受害者將網址複製貼上到瀏覽

器內並連上該網站。網址嫁接攻擊技巧會篡改本機的網域名稱系統快取，以便在使用者試圖連上某組織的官方網站時，將使用者導向假冒的網站。例如:網站遭駭客入侵後，建置偽冒 Outlook Webmail 變更密碼之釣魚網站，並攻擊政府機關人員以竊取郵件帳密。

四、網站安全檢測

關於網站安全的檢測，有下列幾點檢視方向提供系統管理者參考。

(1) 查看事件檢視器的紀錄是否有異常 IP 登入主機(登入類型 3 為網路、登入類型 10 為遠端桌面連線)。

(2) 檢視網站日誌是否有異常 IP 的存取紀錄。

(3) 查看主機內應用程式對外連線的狀態。

(4) 檢視主機內應用程式運作情形。

(5) 查看主機內網站檔案被存取情形。

(6) 檢視主機內登錄檔與開機後所啟動的程式內容。

(7) 查看主機應用程式安裝狀態與系統更新紀錄。

(8) 檢視主機之防火牆的輸入規則設定。

(9) 使用防毒軟體掃描網站主機。

(10) 使用掃 port 軟體掃描網站 port 開啟的狀態。

(11) 檢視網站程式內容是否有被修改情形。

(12) 查看 Windows 系統檔資料夾是否有新增或修改檔案之情形。

(13) 檢視資源回收桶是否有放置異常檔案。

(14) 檢視系統管理者所屬的資料夾內是否有異常新增或修改的檔案存在。

五、網站安全防護措施

談到網站的安全防護，除了網站本身系統之安全外，還需考量底層系統之安

全性，有下列幾個方面提供系統管理者參考。

1.備份與還原

人們經常將備份視為安全因素，而如何安全備份是很重要的，可將備份保存在遠離網站伺服器的安全位置。 安全備份為網站系統和數據的最新副本提供可信的儲存庫，可以部署這些儲存庫來將已知的、乾淨的系統恢復到運行狀態。另外，主機的備份計畫和恢復策略非常重要，例如:備份的頻率是每週，每月還是每天？是否可以從備份檔案中恢復網站，還是檔案僅供資料備份用？是否能查找並恢復丟失或損壞的檔案，或者是否只能從最近的備份中完全替換？

下面為執行 Web 伺服器備份的幾個重點：

(1) 創建 Web 伺服器備份策略。

(2) 每天或每週以差異或遞增方式備份 Web 伺服器。

(3) 每周至每月完全備份 Web 伺服器。

(4) 定期歸檔備份。

(5) 維護網站的權威副本。

2.網路監控

能監控內部網路是否存在入侵和異常活動是資安防護上重要一環，勤奮的監控可以在惡意軟體到達網站伺服器之前阻止伺服器到伺服器之間的傳播。

3.防火牆設定和 DDoS 預防

在主機的防火牆設定方面，檢視主機是否有開啟易受駭客攻擊的 Port(如 445 port 與 3389 port)與這些 port 是否有開啟之必要性，是系統管理者需要特別注意的防活火牆輸入規則設定。

DDoS 攻擊發生在向網站發送大量流量時，使訪問者無法使用網站，防護方式可從具有良好防火牆的網路邊緣開始，但是防火牆阻止 DDoS 攻擊的程度有限。目前在學術網路中可透過申請 ASOC 介入清洗的方式阻止 DDoS 大量

流量的攻擊。

4.防毒軟體的保護

安裝防毒軟體於網站伺服器上是必須的，它將即時偵測網站是否被植入惡意軟體或惡意檔案。因此，定期更新病毒碼是網站主機維護的例行工作之一。

5.應用程序的管理

主機上運行的應用程序很多，但是未必每一個程序都是必須的或有用的，刪除伺服器上任何未使用的、未維護的應用程序，以便避免駭客利用未修補的程序漏洞進行攻擊，在伺服器上僅運行真正需要的功能和服務。

6.保護底層操作系統的安全

一個網站除了網站系統的保護很重要外，其底層操作系統也是整個網站能否運作的關鍵點。駭客除了透過網站登入入侵外，另一個入侵方式是透過登入底層操作系統的方式登入網站伺服器，進而控制整台網站主機。因此，在底層操作系統的安全考量上，需定期更換系統管理者密碼、加強密碼強度與定期更新系統與備份系統資料。

7.軟體更新與漏洞修補

在網站主機上不論作業系統或者應用程序都會需要定期進行軟體更新，讓系統保持在最新狀態。雖然網站有備份能讓網站再次恢復，但它無法解決導致網站崩潰的根本問題，例如:如果駭客使用漏洞來滲透網站，則該漏洞仍然存在於網站備份副本中，那麼需要立即修補漏洞來預防駭客再次利用漏洞來攻擊主機。

8.密碼管理與訪問權限控管

系統管理者擁有管理網站、訪客作者和潛在網站訪問者的密碼，因此，為擁有後端訪問權限的每個人建立並實施密碼強度策略是很重要的，而系統管理者和訪客作者需要更強的密碼，因為他們的帳戶權限可能會對網站產生更大

的影響。另外，對於系統管理者需定期更改密碼，當設備或人員變更時，伺服器的密碼應該有對應的更改策略，也需加強系統管理者帳戶的密碼強度，勿使用相同帳號與相同密碼管理多台主機，也避免多個服務所用之帳號共用同一組密碼。

每個帳戶持有者都應該擁有完成工作所需的最少權限，而網站使用者應具有分級別的權限，例如:控管他們上傳資料的權限。每個使用者都應擁有自己的登錄信息，因此他們對該帳戶所做的所有更改負責。

在控管網站目錄的使用者存取權限方面，永遠不要允許不受限制的文件上傳，限制由使用者上傳檔案至網站伺服器的檔案類型，並排除腳本或其他可執行代碼。若使用者上傳可執行文件，又加上糟糕的文件訪問設定，將使入侵者即時控制網站。

9.檢查網站程式碼

程式碼審查是在網站系統開發完成並且可以發布之後，對應用程序進行深入檢查。 最好通過混合使用自動化工具和人工檢查來完成。審核是在使用應用程序的完整環境中進行的 - 從網站登錄、身份驗證到數據處理、加密和儲存，需警惕是否有讓第三方插入網站文件的 SQL 漏洞存在。SQL 注入是一種攻擊者使用有效的 SQL 命令響應輸入請求的方法。 這些命令可以訪問數據或刪除它。因此，檢查網站系統程式碼是網站安全防護上重要一環。

10.使用 HTTPS 加強安全性

當敏感數據傳輸到伺服器或從伺服器傳輸時，需要 SSL 技術。 SSL 憑證不會保護網站伺服器免受惡意攻擊，而是加密並保護網站伺服器與網站的使用者之間的通信。通過使用 SSL，可以保護使用者的信息並保持他們對網站的信任。

11.執行紀錄的保存

在網站安全的管理上，紀錄的保存很重要，一般分為系統日誌與網站日誌兩

種紀錄。當有資安事件發生時，這些紀錄將是追蹤駭客來源與惡意行為的重要資料。在日誌的保存方面，提供下列幾點參考建議。

(1) 為由虛擬機所建置的 Web 網站建立不同的日誌文件名稱。

(2) 將日誌儲存在單獨的主機上。

(3) 確保主機內有足夠的日誌容量。

(4) 根據單位需求歸檔日誌。

(5) 定期查看日誌與備份日誌。

(6) 使用自動日誌文件分析工具。

12.遠端管理和網站內容更新

駭客常會利用遠端桌面連線方式登入網站伺服器，因此需特別注意網站主機透過遠端連線來進行管理與更新網站內容的安全性，下面有幾點建議提供系統管理者參考。

(1) 使用強大的身份驗證機制（例如，公鑰/私鑰對，雙因素身份驗證）。

(2) 限制以 RDP 方式遠端連線網站伺服器之來源 IP。

(3) 使用安全協定（例如，SSH，HTTPS）。

(4) 在遠端管理和內容更新上實施最小特權的概念（例如:嘗試最小化遠端管理/更新帳戶的訪問權限）。

(5) 從遠端管理實用程序或應用程序更改任何預設的帳戶或密碼。

(6) 除非使用 VPN 等機制，否則不允許從 Internet 進行遠端管理。

(7) 不要從 Web 伺服器所在內部網路上安裝任何文件共享，反之亦然。

13.測試網站安全性

在網站運作後，針對測試網站安全性方面，有下列幾點提供參考。

(1) 定期對 Web 伺服器、動態生成的內容和支持的網路進行漏洞掃描。

(2) 在測試之前更新漏洞掃描程序。

(3) 糾正漏洞掃描程序發現的任何缺陷。

(4) 在 Web 伺服器和支持網路基礎架構上進行滲透測試。

(5) 通過滲透測試確定的正確缺陷。

六、參考資料

1. Guidelines on Securing Public Web Servers

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-44ver2.pdf

2. 14 Web Hosting Security Best Practices (2019) — Top Hosts & Servers

https://www.hostingadvice.com/how-to/web-hosting-security-best-practices/

3.新版 OWASP 十大網站安全風險排名出爐，微服務風潮帶來三大新安全風險

https://www.ithome.com.tw/news/118411

4. OWASP Top 10 Web Application Security Risks - 2021

https://owasp.org/www-project-top-ten/

5. OWASP Top 10 2021 介紹

https://owasp.org/Top10/zh_TW/