

# 資安實務自主學習專題 — 使用 DirBuster 工具

## 一、背景

在現今的數位世代，網站已成為生活中不可或缺的一部分，人們透過網站取得資訊、進行社交或執行各種任務，網站中目錄功能有助於使用者瀏覽網站和快速訪問不同頁面。然而架設網站時，有些路徑因會隱私、機密文件或其他敏感因素而故意被網站管理員隱藏，這些被隱藏的路徑在使用者正常瀏覽時不會輕易的被訪問，只有特定權限的人才可以訪問。

## 二、動機

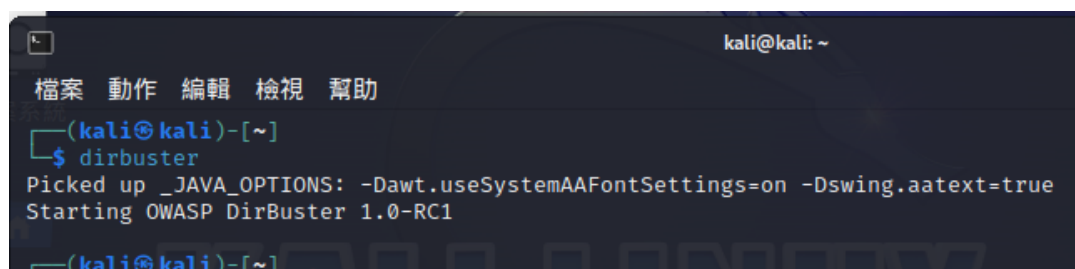
我選擇使用 DirBuster 工具進行網站目錄分析，我想透過分析目錄深入研究網站的隱藏目錄的目的與曝光對於網站造成的影響，也透過分析網站瞭解到其結構與安全性，從中學習如何預防網站漏洞、瞭解弱點，提高資安意識，促進更安全的網路環境，以應對長期的資安挑戰。

## 三、工具及服務介紹

DirBuster 是一款強大的開源工具，由 OWASP ( Open Web Application Security Project ) 開發和維護。DirBuster 的主要功能是進行目錄和隱藏文件的暴力破解，此工具使用 Java 編寫且支援多線程，使工具可同時發送多個請求，提高掃描速率，在運行前需安裝 Java 環境。不過這次測試這次會使用 Kali Linux 中執行 DirBuster，Kali Linux 內建就有此工具，所以不需再次安裝。此外 DirBuster 會將掃描結果生成詳細報告，供使用者進行分析和整合，進一步評估網站的安全問題。

## 四、使用流程與產出

1. 在 Linux 指令輸入指令‘\$ dirbuster’以啟動 DirBuster 工具，啟動後會看到 DirBuster 主畫面(圖一、圖二)。



```
kali@kali: ~  
檔案 動作 編輯 檢視 幫助  
└─(kali@kali)-[~]  
└─$ dirbuster  
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true  
Starting OWASP DirBuster 1.0-RC1  
└─(kali@kali)-[~]
```

圖 一

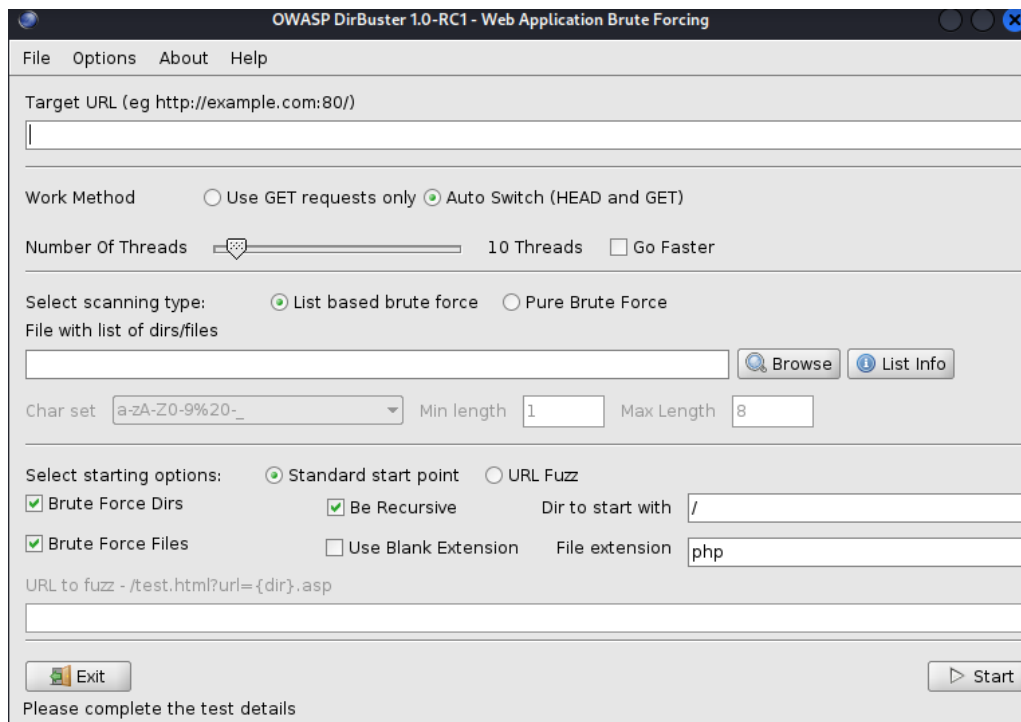


圖 二

2. 在主畫面上輸入想掃描的目標網站，我這次掃描的 <https://dvwa.co.uk/>
3. 接下來選擇線程數，選擇線程數可以在運行時根據系統性能和資源再進行調整。 初始的線程數我先設定為 80。
4. 選擇列表文件(圖三)。在掃描過程中，DirBuster 使用一個列表文件來猜測可能存在的目錄和文件名。選擇的列表文件對於掃描的效果和時間都有影響，這次我選擇一個包含 141,694 個單詞的列表文件。
5. 最後按下 START 開始掃描，DirBuster 將根據設定的參數，對目標網站進行目錄和文件的掃描。此工具使用列表文件中的每個單詞組合成 URL，並發送請求進行測試。
6. 等待掃描完成，掃描的時間取決於目標網站的大小和性能。這次掃描大約花費 20 小時，過程中我逐漸增加線程數量，最後調整到 180。這樣的調整可以提高掃描速度，同時逐漸調整也避免造成系統產生過大負荷，而影響系統正常運行。
7. 檢視掃描結果(圖四)。當掃描完成後，DirBuster 會產生一個 TXT 檔案，包含發現的目錄和文件、相關的 HTTP 狀態碼、請求時間等信息。

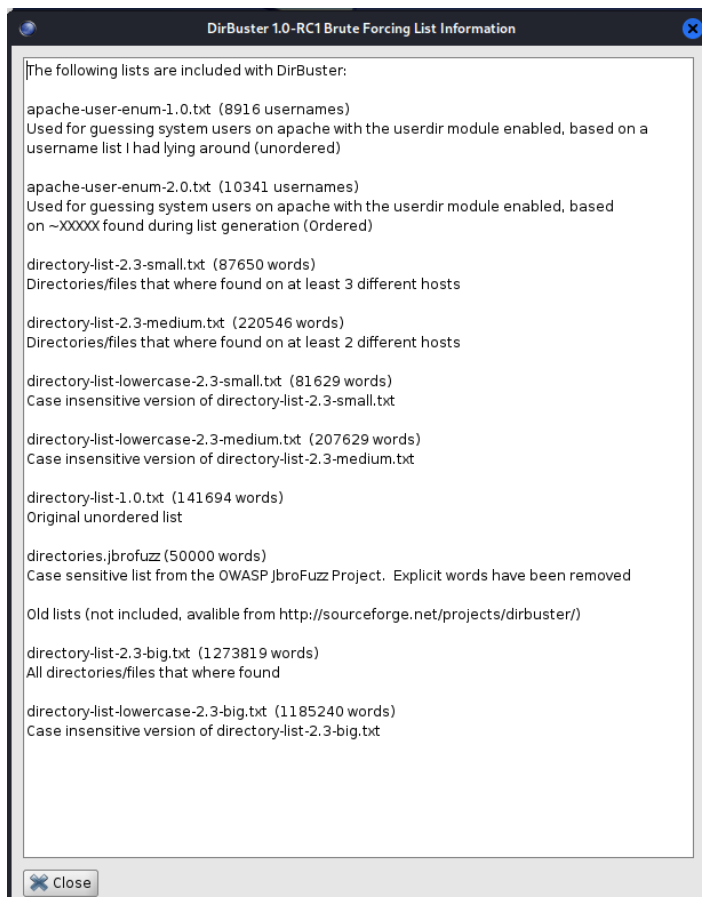


圖 三

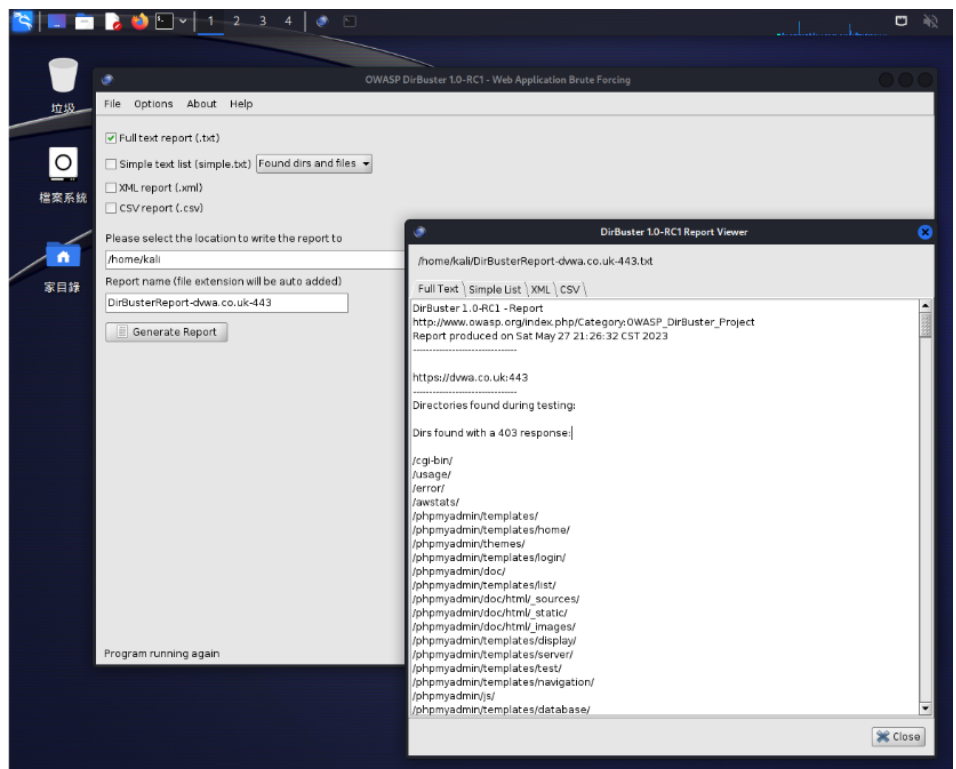


圖 四

## 五、問題說明

首先，分析報告中發現了特定狀態碼，觀察到當 Dirbuster 掃描到某些目錄時會返回 403 的狀態碼。這表示 server 雖然有成功理解請求，但是 client 端沒有存取資源的權限，這些目錄被設為僅限特定使用者可以訪問，其他未經授權的使用者將被拒絕存取(圖四)。所以猜測這個目錄或文件可能包含敏感資訊，為了確保網站安全而被嚴格控制訪問權限。



圖 五

再進一步觀察發現，不僅回傳 403 狀態碼的目錄被限制，且子目錄也同樣的被返回 403 狀態碼。同樣設定是為了確保整個目錄結構的安全性，避免未經授權使用者繞過主目錄的限制，直接訪問到敏感資訊。



圖 六

在分析報告中也有許多包含.php、.txt 和.html 檔案的路徑，這些路徑可能帶來資安威脅和敏感性問題。PHP 是 HTML 和 CSS 等前端技術結合使用通過處理 server 端請求，由於 PHP 包含執行程式碼，如果這些檔案未經適當保護和驗證，可能會導致安全漏洞。如:程式碼注入、跨站腳本 (XSS) 攻擊等。

這次實作 DirBuster 掃描此網址，總共成功掃描到 432 個路徑。但當掃描結果呈現大量路徑時，一個一個分析一定會耗費大量且不必要的時間，在這情況下可以使用一些方法和工具來更有效率的篩選和分析結果。根據資安知識，可以優先關注包含敏感資訊和易受攻擊的目錄和檔案類型，包含資料庫連接設定檔、登入頁面、管理員介面，將注意力擊中在最有可能存在資安風險的路徑上，從而減少分析範圍。其次，使用關鍵字篩選路徑，專注於可能含有敏感資訊或常見漏洞，例如：admin, passwd 等等，這些關鍵字可以優先篩選。另外，使用自動化工具分析掃描結果也是有效的選擇。工具可

以幫助我們自動篩選、分析和識別可能的資安風險，使能更快速確定那些路徑可能涉及敏感資訊。

### 參考資料：

<https://ithelp.ithome.com.tw/articles/10215002>

<https://dvwa.co.uk/> (目標網站)

<https://www.tsg.com.tw/blog-detail4-234-0-403.htm> (圖六來源)

<https://ithelp.ithome.com.tw/questions/10213109#answer-390215>