WordPress用戶枚舉漏洞的檢測

報告日期：2021/10/20

組員：李威辰、吳冠廷、張允瀚

目錄

名詞介紹

內容管理系統（Content Management System，縮寫為 CMS）是指在一個合作模式下，用於管理工作流程的一套制度。該系統可應用於手工操作中，也可以應用到電腦或網路裡。作為一種中央儲存器（Central Repository），內容管理系統可將相關內容集中儲存並具有群組管理、版本控制等功能。版本控制是內容管理系統的一個主要優勢。

應用程式介面（Application Programming Interface，縮寫為API）用於打造應用程式軟體的一組副程式定義、協定與工具。一般而言，API 是指各種軟體組件之間一套明確定義的溝通方法。

端點（Endpoint）是通過網路存取的服務、工具或應用程式的連接點。當想要連接到應用程式、服務、工具來交換資料時，可以連接到其端點。

端點的基本URL為https://example.com/v1，後面加上端點對應的路徑（Path）（例：若路徑為 /me 其對應URL即 https://example.com/v1/me ）

WordPress介紹

WordPress介紹

WordPress是一個以PHP和MySQL為平台的部落格軟體平台，也是目前最大的網站內容管理系統，WordPress具有外掛插件架構，使用者可以安裝並切換各種主題

目前有超過1.7億個以上的網站，其支援分散式系統、多用戶系統、及許多功能的可達性，使包含電子商務，新聞，電子雜誌等等都使用WordPress架設。

但也因為各種插件的版本漏洞，如果不定時更新與維護，便會協助駭客攻擊網頁獲取資料或使網頁變成不可使用的狀態。

WordPress系統架構

WordPress的系統架構分為前端與後端，這個漏洞使用的層面都在於後端，因此只介紹後端的部分。

後端控制平台：文章管理、媒體管理、頁面管理、留言管理、外觀管理、外掛管理、使用者管理、工具管理，設定。

使用者管理：

一般網站的管理者可能寥寥幾位，但如果是Blog形式或者購物、會員等網站，就會有一般使用者註冊並登入，這時可以透過使用者管理介面進行批次管理，包含帳號、密碼及權限等設定。

可能遭受的威脅

大多數人在使用WordPress時並未更新到最新版本，造成其中包含漏洞代碼。

攻擊者會使用Python或其他程式語言腳本來偵測WordPress的插件版本、核心本和常見的WordPress漏洞，一旦發現漏洞就會設定目標並使用腳本攻擊。

駭客選擇攻擊的漏洞，最多是偵測插件版本約占57%，其次是使用Brute Force（蠻力攻擊）16%與偵測核心版本8%。

常見的攻擊方式

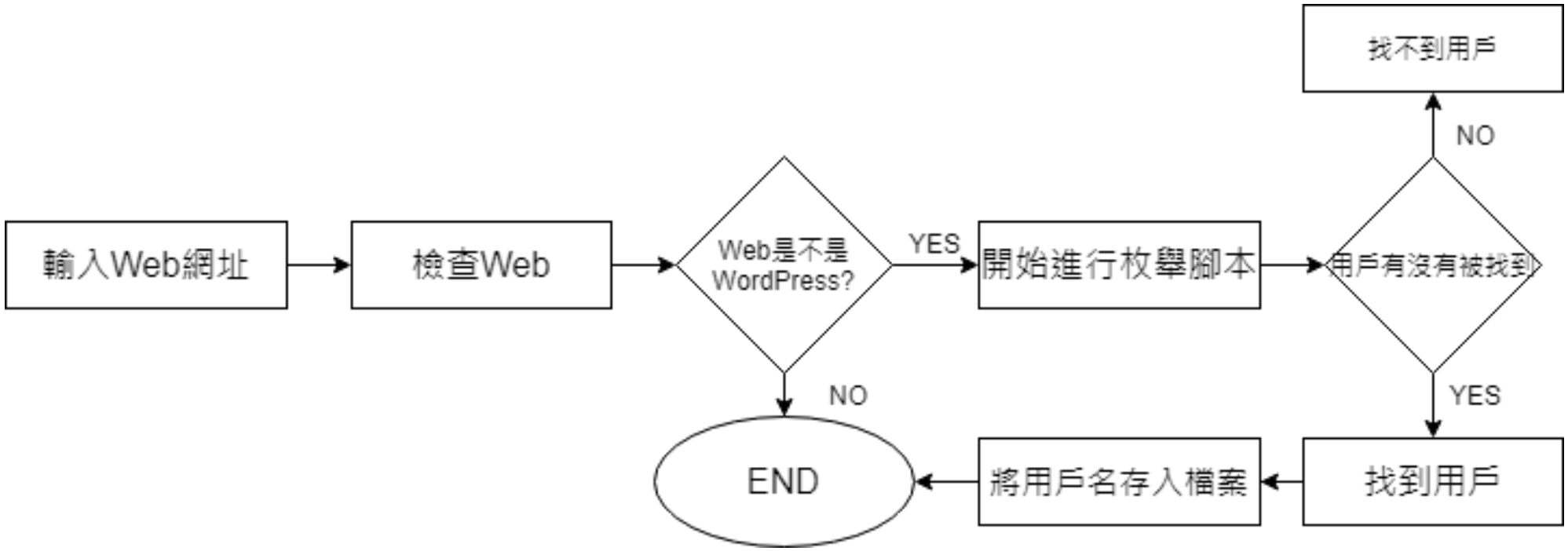
- SQL injection（SQL注入）：是使用任何Web表單或輸入字段實現或完全銷毀數據庫。
- XSS attack （跨網站攻擊）：攻擊者輸入了惡意的JavaScript，該代碼在客戶端加載後開始收集數據。
- Malicious Software（惡意軟體）：惡意軟體被注入WordPress通過感染主體。
- Brute Force（蠻力攻擊）：通過嘗試無數種組合來猜測正確的用戶名稱或是密碼，這種攻擊很難成功，但仍然是WordPress常見的攻擊方式，因為WordPress不會阻止用戶嘗試多次的失敗。
- DDoS（阻斷服務攻擊）：透過向Web伺服器發出大量的請求使其運行緩慢並最終崩潰。

枚舉攻擊介紹

三種枚舉攻擊

1. 透過遍歷作者檔案進行枚舉攻擊
   - 此攻擊方式為本篇論文重點，將在下頁介紹
2. 透過JSON API進行枚舉攻擊
   - 使用JSON端點（Endpoint）可以獲得網頁上的用戶列表
3. 透過登入表格進行枚舉攻擊
   - 在登入表格中有效帳戶跟無效帳戶的回應不同，可使用工具自動輸入用戶名稱並得到HTTP POST

枚舉攻擊的流程圖


輸入Web網址
檢查Web
Web是不是WordPress?
YES
開始進行枚舉腳本
用戶有沒有被找到
NO
找不到用戶
YES
找到用戶
將用戶名存入檔案
END
NO

枚舉攻擊原理

此方式是適用於所有WordPress版本的技術。

用戶具有唯一的用戶ID，該ID由資料庫中的程式使用並用於引用用戶帳號。通過嘗試每個用戶ID來取得作者檔案，可以快速分辨有效帳號與該帳號匹配的用戶名稱。這包括管理員名稱（通常ID為1）

枚舉攻擊原理

向https://wordpressexample.com/?author=1發出簡單的HTTP請求，若是作者存在，會看到以下訊息。

Connection: keep-alive

Content-Type: text/html; charset=UTF-8

Date: Thu, 17 Oct 2019 23:12:26 GMT

Location: https://wordpressexample.com/author/fred/

Server: nginx/1.10.3 (Ubuntu)

可以看到Location標頭將用戶ID 1 取代成fred，這表示管理員帳號被重新命名成fred，我們便可獲得用戶名稱。

防禦漏洞方式

- 監控登入次數：

可使用Limit Login Attempts這個外掛，這個外掛會監控使用者登入的狀況，超過一定次數的密碼嘗試就會被鎖定、紀錄IP甚至是封鎖IP。

- 隱藏後台及登入網址：

將WordPress後台的預設網址/wp-admin及/wp-login.php隱藏起來，也可使用HC Custom WP-Admin URL此外掛，自動隱藏。

← Limit Login Attempts

HC Custom WP-Admin URL→

防禦漏洞方式

- 不顯示WordPress版本：

根目錄的readme.html請直接刪除，以及限制wp-content之下的version.php的存取。

- 加強帳號密碼的安全性

刪除WordPress預設的Admin帳號，加入特殊符號增加密碼複雜度。

務必修改跟目錄系統檔案wp-config.php裡面的金鑰設定。

結論

由於WordPress是開放原始碼的平台，每個網站的架構、資料夾名稱、登入網址連結都一模一樣。因此使用了相同版本WordPress的網站，都會存在類似的漏洞，沒有做好防護措施的話，WordPress便容易被入侵。

Reference

Isrg Rajan,"Detection of WordPress User Enumeration,"11 Nov 2018

Chatwork,"Endpoints （資料傳輸接點）",29 OCT 2015

Wayne Fu,"WordPress 防駭 + 建立安全防護心得紀錄,"31 May 2017

HACKER TARGET,"WordPress User Enumeration" 10 OCT 2019

我瘋程式工作室,"WP前後端功能基本講解,"20 Set 2020

ALPHA Camp,"API是什麼？認識 Web API、HTTP 和 JSON 資料交換格式"24 APR 2020

https://zh.wikipedia.org/wiki/WordPress