WordPress - CMS**系統**

**架網站用的、網站後台**

1. **客戶端**
2. **管理端**
3. **數據流**

**加載核心文件**

**執行設定檔**

**加載模板**

Hooks

Actions **回傳值無意義**

Filters **回傳值有意義**

---------------------------------------------------------

**漏洞分析**

---------------------------------------------------------

RCE**代碼**

CVE-2019-8943

**版本**：WordPress <= 5.00

**條件**：author**權限**

**要素**：**變量覆蓋**、**目錄穿越**、**模板包含**

---------------------------------------------------------

**靶機環境**

---------------------------------------------------------

WordPress4.9.4

Windows7 + XAMPP

WordPress5.6.40 + imagick 6.9.7

---------------------------------------------------------

**實際演示**

---------------------------------------------------------

**結論**

---------------------------------------------------------

**沒有絕對安全的系統**

**即便是低風險的漏洞也不可忽視**

**目錄及檔案權限設定必須要設定**

**寫入資料庫及檔案的程式碼必須要做好過濾**

**系統及軟體請隨時更新到最新版本**

---------------------------------------------------------