【列舉】wpscan

WPScan 是一款用於檢測 WordPress 網站安全性的開源工具。以下是一些常見的指令用法的繁體中文說明。請注意，WPScan 的命令行參數和選項可能會因版本而略有變化，建議在使用時查閱最新的官方文件。

```
# -enumerate p 掃描 WordPress 核心、插件和主題的漏洞：
# --plugins-detection aggressive 以詳細模式運行掃描
# -o websrv1/wpscan #output file

wpscan --enumerate p --plugins-detection aggressive -o wpscan.log \
--url http://192.168.50.244
```

```
# 1. **基本掃描：**
# - 掃描一個 WordPress 網站：
wpscan --url http://example.com

# 2. **插件和主題掃描：**
#- 掃描所有插件：
wpscan --url http://example.com --enumerate p
#- 掃描所有主題：
wpscan --url http://example.com --enumerate t


# 3. **使用者枚舉：**
# - 嘗試枚舉使用者：
wpscan --url http://example.com --enumerate u

# 4. **密碼破解：**
# - 使用使用者名稱進行密碼破解：
wpscan --url http://example.com --passwords wordlist.txt --username admin

# 5. **漏洞掃描：**
# - 掃描 WordPress 核心、插件和主題的漏洞：
wpscan --url http://example.com --enumerate vp

# 6. **更多選項：**
#- 以詳細模式運行掃描：
wpscan --url http://example.com --enumerate vp --log wpscan.log
# - 顯示所有掃描選項：
wpscan --help
```

修訂版本 #4
★由 treeman 建立於 17 ﷽Q﷽G﷽﷽ 2023 11:32:02
✎由 treeman 更新於 7 ﷽@﷽﷽ 2024 19:30:26