

【web】【爆破】gobuster

```
# 安裝
sudo apt-get update
sudo apt-get install gobuster

# git hub
# https://github.com/OJ/gobuster
```

```
# 1. **基本目錄爆破：**
# 在目標網站進行基本的目錄爆破，使用默認的字典文件：
gobuster dir -u http://example.com -t 10

# 2. **指定字典文件：**
# 使用自定義的字典文件進行目錄爆破：
gobuster dir -u http://example.com -w /path/to/custom-wordlist.txt -t 10

gobuster dir -u http://offsecwp/ -w /usr/share/wordlists/dirb/common.txt
gobuster dir -u http://offsecwp/ -w /usr/share/wordlists/dirb/big.txt
gobuster dir -u http://offsecwp/ -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt
gobuster dir -u http://offsecwp/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
gobuster dir -u http://offsecwp/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt

# 3. **多線程設置：**
# 設置併發線程數為 20：
gobuster dir -u http://example.com -w /path/to/wordlist.txt -t 20

# 4. **狀態碼過濾：**
# 過濾掉 HTTP 狀態碼為 404 的響應：
gobuster dir -u http://example.com -w /path/to/wordlist.txt -t 10 -s 404

# 5. **遞歸掃描：**
# 對找到的每個目錄進行遞歸掃描：
gobuster dir -u http://example.com -w /path/to/wordlist.txt -t 10 -r

# 6. **擴展名爆破：**
# 嘗試查找具有特定文件擴展名的文件：
# gobuster
# --exclude-length 40182: 排除指定長度的響應。在此示例中，排除了長度為 40182 的響應。這有助於過濾掉一些不感興趣的目錄。
# -f: 在結果中顯示完整的 URL 路徑。使用此標誌，gobuster 將顯示完整的 URL 路徑，而不僅僅是相對路徑。
gobuster dir -u http://offsecwp/ -w /usr/share/wordlists/dirb/common.txt --exclude-length 40182 -f
gobuster dir -u http://offsecwp/ -w /usr/share/wordlists/dirb/common.txt --exclude-length 40182 -f -x php,jsp
gobuster dir -u http://example.com -w /path/to/wordlist.txt -t 10 -x php,txt

# 7. **添加自定義 HTTP 頭：**
# 在請求中添加自定義的 HTTP 頭信息：
gobuster dir -u http://example.com -w /path/to/wordlist.txt -t 10 -H "Custom-Header: Value"

# 8. **URL 編碼啟用：**
# 啟用 URL 編碼以處理特殊字符：
gobuster dir -u http://example.com -w /path/to/wordlist.txt -t 10 -e
```

Gobuster 字典檔，一定要用對
/usr/share/wordlists/dirb/common.txt ← 起手式
/usr/share/wordlists/dirb/big.txt ← 進階
/usr/share/wordlists/dirbuster ← 最後階段(紅色字體)，用完就不建議在嘗試，換方向

```
/usr/share/wordlists/dirbuster/
└─$ wc -l /usr/share/wordlists/dirb/common.txt
4614 /usr/share/wordlists/dirb/common.txt
└─$ wc -l /usr/share/wordlists/dirb/big.txt
20469 /usr/share/wordlists/dirb/big.txt
└─$ ls -al /usr/share/wordlists/dirbuster/
total 7584
```

```
-rw-r--r-- 1 root root 71638 Feb 27 2009 apache-user-enum-1.0.txt
-rw-r--r-- 1 root root 90418 Feb 27 2009 apache-user-enum-2.0.txt
-rw-r--r-- 1 root root 546618 Feb 27 2009 directories.jbrofuzz
-rw-r--r-- 1 root root 1802668 Feb 27 2009 directory-list-1.0.txt
-rw-r--r-- 1 root root 1980043 Feb 27 2009 directory-list-2.3-medium.txt
-rw-r--r-- 1 root root 725439 Feb 27 2009 directory-list-2.3-small.txt
-rw-r--r-- 1 root root 1849676 Feb 27 2009 directory-list-lowercase-2.3-medium.txt
-rw-r--r-- 1 root root 676768 Feb 27 2009 directory-list-lowercase-2.3-small.txt
```

☺修訂版本 #4

★由 treeman 建立於 17 🍀Q🍀G🍀🍀 2023 12:50:08

✍由 treeman 更新於 7 🍀@🍀🍀 2024 19:31:17