

# CÔNG CỤ DIRSEARCH

## Giới thiệu chung:

**Dirsearch** là một công cụ mã nguồn mở được viết bằng Python hoạt động theo kiểu brute-forcing cấu trúc thư mục, file của web. Nó có thể chạy trên Windows, Linux, macOS. **Dirsearch** sử dụng các dòng lệnh đơn giản mà hiệu quả, nó hỗ trợ rất nhiều options. Chính vì thế **dirsearch** trở thành công cụ phổ biến mà hầu hết các hacker hay pentester đều sử dụng.

**Dirsearch** hỗ trợ các kỹ thuật như sau:

- Đa luồng
- Recursive brute-forcing
- Hỗ trợ HTTP proxy
- Phát hiện các trang web không hợp lệ
- User agent randomization và Batch processing
- Hỗ trợ Request delaying
- Tìm kiếm theo list extensions
- Set cookie

## Các câu lệnh cơ bản:

- Xem các options

```
# python3 dirsearch.py -h
```

- Scan web

```
# python3 dirsearch.py -u https://target
```

### – Scan using extensions

```
# python3 dirsearch.py -e php,html,js -u https://target
```

### – Scan using wordlist

```
# python3 dirsearch.py -e php,html,js -u https://target -w  
/path/to/wordlist
```

### – Scan exclude status code

```
# python3 dirsearch.py -u http://target -e php,html,txt -x  
403,400
```

### – Scan sub-directories

```
# python3 dirsearch.py -e php,html,js -u https://target --  
subdirs /,admin/,folder/
```

### – Proxies

```
# python3 dirsearch.py -e php,html,js -u https://target --  
proxy 127.0.0.1:8080
```

```
# python3 dirsearch.py -e php,html,js -u https://target --  
proxy socks5://10.10.0.1:8080
```

```
# python3 dirsearch.py -e php,html,js -u https://target --  
proxylist proxyservers.txt
```

### – Reports

```
# python3 dirsearch.py -e php -l URLs.txt --format plain -o  
report.txt
```

```
# python3 dirsearch.py -e php -u https://target --format html  
-o target.js
```