

1、dirscan.py 目录爆破工具

```
C:\Users\DELL\Desktop\dirscan>python dirscan.py -h
usage: dirscan.py [-h] [-u URL] [-t THREAD] [-p [PROXY]] [-d [DINGS]]

This is the help!

optional arguments:
  -h, --help            show this help message and exit
  -u URL, --url URL      要检测的url
  -t THREAD, --thread THREAD 指定线程 默认30
  -p [PROXY], --proxy [PROXY] 指定是否使用代理 无参数自动5000端口代理 指定格式:127.0.0.1:5000
  -d [DINGS], --dings [DINGS] 指定动态代理（读取代理txt文件）详情请看runproxy()函数
```

- 1 正常使用:
- 2 `python dirscan.py -u http://192.168.0.155`
- 3 设置线程:
- 4 `python dirscan.py -u http://192.168.0.155 -t 5`
- 5 使用静态代理
- 6 `python dirscan.py -u http://192.168.0.155 -t 5 -p 127.0.0.1:5000`
- 7 使用动态代理:
- 8 `python dirscan.py -u http://192.168.0.155 -t 5 -d`
- 9
- 10 工具介绍:
- 11 一款继承性目录爆破工具，可使用静态代理，动态代理，还可对根目录无法访问的页面进行爆破

2、MyProxy.py免费代理爬取工具

- 1 所在位置: Proxy代理爬取 文件夹下（位置请不要随意更换）
- 2 使用方法:
- 3 `python MyProxy.py`
- 4
- 5 工具介绍:
- 6 自动生成代理在 Proxy代理爬取/Proxy 文件夹下
- 7 自动筛选可用代理 如指定网站筛选请修改文件夹 常量检测地址

```
# 删除文件夹
shutil.rmtree("Proxy")
# 创建代理文件夹
os.mkdir("Proxy")
CURL = 'https://www.baidu.com' # "" 检测地址 常量""

""" 稻壳代理爬取检测 """
url1 = "https://www.docip.net/data/free.json"
GetProxy.getproxys(url1, localproxy) # 获取稻壳代理 写入文件 接受一个爬取页
filename = "Proxy/daokedaili.txt" # 稻壳代理文件名
threading.Thread(target=GetProxy.requirs, args=(localproxy, filename, CURL))
```

3、pageCrawling.py页面URL爬虫

- 1 使用方法:
- 2 python pageCrawling.py -u https://www.baidu.com/
- 3
- 4 工具介绍:
- 5 自动爬取页面的 url链接 / JavaScript链接 / CSS链接 / 图片链接 / Js文件中的链接

```
C:\Users\DELL\Desktop\dirscan>python pageCrawling.py -u https://www.baidu.com/

Hello, welcome to use the url DirScan tool of Chinese hacker Xue
Please enter the - h parameter for help

++++++URL 链接++++++
++++++JavaScript 链接++++++
https://www.baidu.com/www.baidu.com/s?rtt=1&bsst=1&cl=2&tn=news&word=",t.setAttribute("sync",!0))}});}();</script
><script type="text/javascript" src="https://pss.bdstatic.com/r/www/cache/static/protocol/https/bundles/es6-poly
fill_388d059.js
https://www.baidu.com/hectorstatic.baidu.com/cd37ed75a9387c5b.js
++++++CSS 链接++++++
++++++图片 链接++++++
https://www.baidu.com/www.baidu.com/img/PCtm_d9c8750bed0b3c7d089fa7d55720d6cf.png
https://www.baidu.com/www.baidu.com/img/PCfb_5bf082d29588c07f842ccde3f97243ea.png
https://www.baidu.com/www.baidu.com/img/flexible/logo/pc/result.png
https://www.baidu.com/www.baidu.com/img/flexible/logo/pc/result@2.png
https://www.baidu.com/www.baidu.com/img/flexible/logo/pc/peak-result.png
=====JS 文件中的链接=====
http://nsclick.baidu.com
https://www.baidu.com/nocache/fesplg/s.gif?log_type=sp
https://www.baidu.com/s?wd=
https://www.baidu.com/nocache/fesplg/s.gif?log_type=hm&type=ssl&
```

4、Dos.py DOS工具

- 1 慎用:
- 2 基于多进程多线程发送大量请求, 致使目标宕机
- 3 使用方法:
- 4 `python Dos.py -u http://192.168.0.152`
- 5 工具介绍:
- 6 伤敌一千自损八百, 纯破坏性工具

笔者公众号 HexaGon 欢迎技术交流