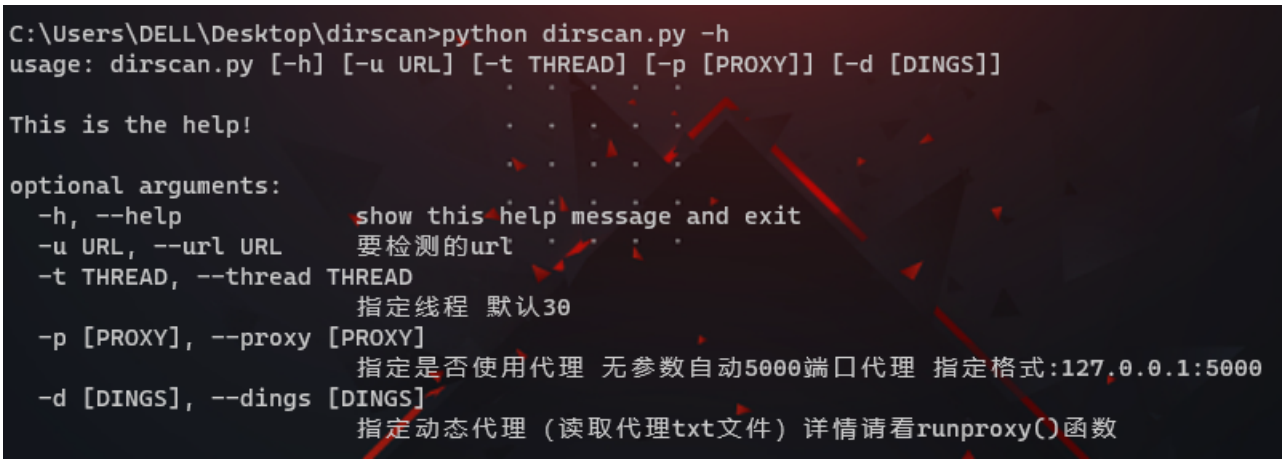
# 1、dirscan.py 目录爆破工具




```
正常使用:
    python dirscan.py -u http://192.168.0.155
设置线程:
    python dirscan.py -u http://192.168.0.155 -t 5
使用静态代理
    python dirscan.py -u http://192.168.0.155 -t 5 -p 127.0.0.1:5000
使用动态代理:
    python dirscan.py -u http://192.168.0.155 -t 5 -d

工具介绍:
    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

```
所在位置：Proxy代理爬取 文件夹下（位置请不要随意更换）
使用方法:
    python MyProxy.py

工具介绍:
    自动生成代理在 Proxy代理爬取/Proxy 文件夹下
    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
```

```python
# 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.requrls,args=(localproxy,filename,CURL)
```

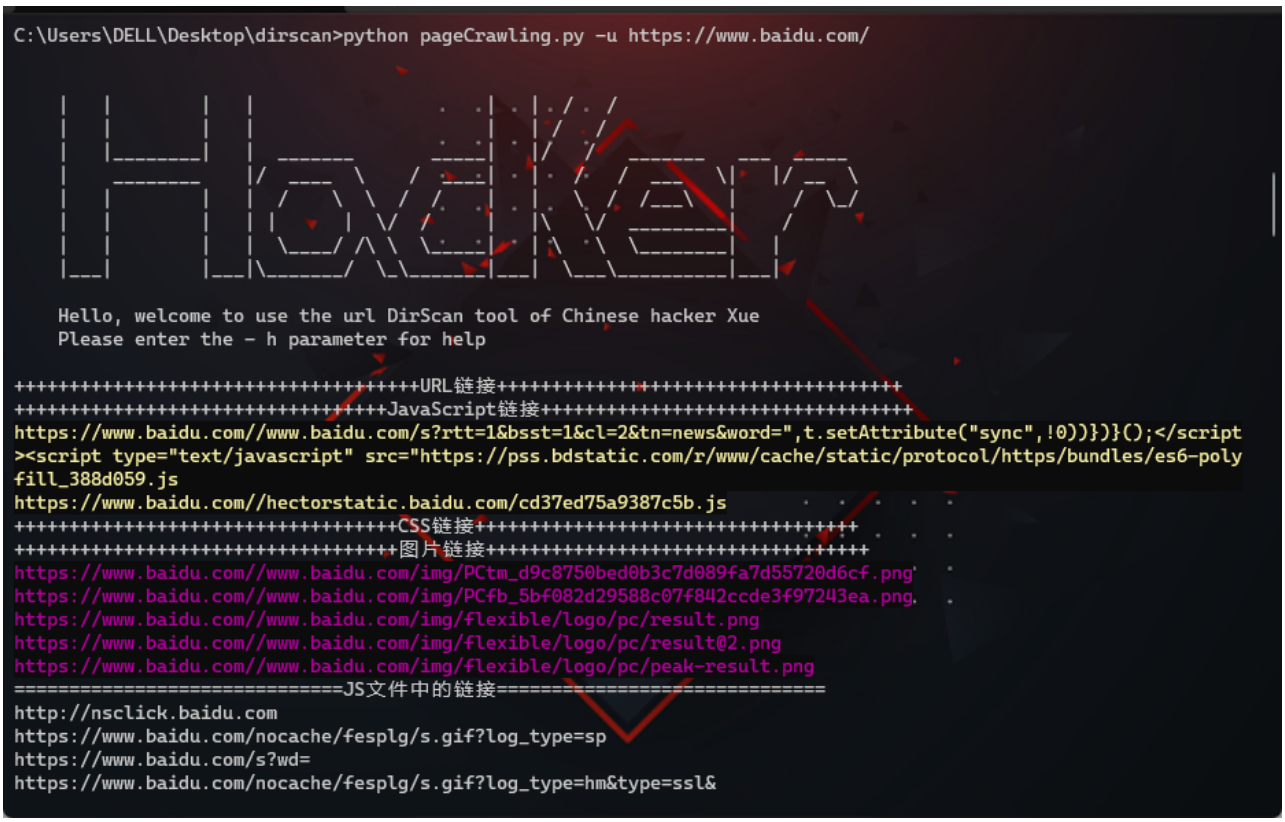
# 3、pageCrawling.py页面URL爬虫

使用方法：

```
python pageCrawling.py -u https://www.baidu.com/
```

工具介绍：

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




# 4、Dos.py DOS工具

```
慎用：
    基于多进程多线程发送大量请求，致使目标宕机
使用方法：
    python Dos.py -u http://192.168.0.152
工具介绍：
    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