Python Requests 学习 笔记

原创

烧包 于 2018-01-11 21:35:50 发布 157 收藏
分类专栏： WEB知识相关 文章标签： python 网络安全 脚本

本文链接：https://blog.csdn.net/qq_40476955/article/details/79038801

在做WEB题目的时候看到一道这样的题，要让我迅速提交，看到别人的writeup 发现要写python脚本，于是就来学一下python requests
题目连接

——来自网络安全实验室

该文档的内容来自 Pyhon Requests 快速入门

发送请求

```
r=requests.get("域名")
```

其他玩法
r=requests.put()
r=requests.delete()
等等，其他的HEAD,OPTIONS也是一样的。

用URL传递参数

```
>>> payload = {'key1': 'value1', 'key2': 'value2'}
>>> r = requests.get("http://xxx/get", params=payload)
```

通过print URL ,可以发现URL已经被正确编码。

响应内容

通过r.text 和r.encoding 可以改变文本编码
二进制的话，则用content来写
requests 内置json编译器，通过requests.json（） 能够处理json数据

原始响应内容

初始请求中，加上r = requests.get(“”,stream =True)
那么，就能用r.raw.read(字节数)来获取原始套接字、

定制请求头

这里直接拷贝代码了，其实就是构造一个请求头嘛

```
>>> import json
>>> url = 'https://api.github.com/some/endpoint'
>>> payload = {'some': 'data'}
>>> headers = {'content-type': 'application/json'}

>>> r = requests.post(url, data=json.dumps(payload), headers=headers)
```

定制POST请求

同样的方法，也可以用来定制post请求。

```
>>> payload = {'key1': 'value1', 'key2': 'value2'}
>>> r = requests.post("http://httpbin.org/post", data=payload)
>>> print r.text
{
  ...
  "form": {
    "key2": "value2",
    "key1": "value1"
  },
  ...
}
```

包含文件的POST请求

Requests使得上传多部分编码文件变得很简单:

```
>>> url = 'http://httpbin.org/post'
>>> files = {'file': open('report.xls', 'rb')}

>>> r = requests.post(url, files=files)
>>> r.text
{
  ...
  "files": {
    "file": "<censored...binary...data>"
  },
  ...
}
```

如果你想，你也可以发送作为文件来接收的字符串:

```
>>> url = 'http://httpbin.org/post'
>>> files = {'file': ('report.csv', 'some,data,to,send\nanother,row,to,send\n')}

>>> r = requests.post(url, files=files)
>>> r.text
{
  ...
  "files": {
    "file": "some,data,to,send\\nanother,row,to,send\\n"
  },
  ...
}
```

响应状态码

通过r.status_code 打印状态码
如果发送了失败请求，那么可以用 Response.raise_for_status()来抛出异常

响应头

看到这里，我感觉这个就是Burpsuite中的HTTP history + 改包嚒
只不过使用脚本的形式。

r.headers可以看响应头。

Cookies

可以通过r.cookies快速访问cookies，发送的是时候可以用cookies参数。

```
>>> url = 'http://example.com/some/cookie/setting/url'
>>> r = requests.get(url)

>>> r.cookies['example_cookie_name']
'example_cookie_value'

>>> url = 'http://httpbin.org/cookies'
>>> cookies = dict(cookies_are='working')

>>> r = requests.get(url, cookies=cookies)
>>> r.text
'{"cookies": {"cookies_are": "working"}}'
```

所以接下来我们来解题！

现在学了requests后，就可以写脚本来快速提交了。（我感觉我的手速能够在2S内，但是好像函数不是这么设置的。）

闲话不多少，直接上代码

```python
#coding=utf-8
import requests,re
def function1():
    s = requests.Session()
    url = 'http://lab1.xseclab.com/xss2_0d557e6d2a4ac08b749b61473a075be1/index.php'
    html = s.get(url).content #这个算数是动态的，别忘了
    reg = r'([0-9].+)=<'
    pattern = re.compile(reg)
    match = re.findall(pattern,html)
    payload = {'v': eval(match[0])} #通过截获包裹知道变量名是v
    print s.post(url, data=payload).content
```

GET FLAG

后来又遇到了一道这样的题目，来自实验吧 实验吧——编程题——百米赛跑
感兴趣的可以做一下