流量分析

1、请求一个 location 没啥卵用

Req：

```
GET http://seat.lib.whu.edu.cn/ HTTP/1.1
Host: seat.lib.whu.edu.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: JSESSIONID=35D29F58753C6BCF42CE20D596A83AF7
Upgrade-Insecure-Requests: 1
```

Param:JESSIONID

Res:

```
HTTP/1.1 302 Found
Date: Mon, 10 Dec 2018 01:37:30 GMT
Server: Apache-Coyote/1.1
X-Frame-Options: SAMEORIGIN
Location: http://seat.lib.whu.edu.cn/login?targetUri=%2F
Content-Length: 0
Keep-Alive: timeout=5, max=1000
Connection: Keep-Alive
```

2、请求获得主页(重定向来的)

Req: JESSIONID 同上一个

```
GET http://seat.lib.whu.edu.cn/login?targetUri=%2F HTTP/1.1
Host: seat.lib.whu.edu.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: JSESSIONID=35D29F58753C6BCF42CE20D596A83AF7
Upgrade-Insecure-Requests: 1
```

Res: 返回首页信息。(里面藏有 token)

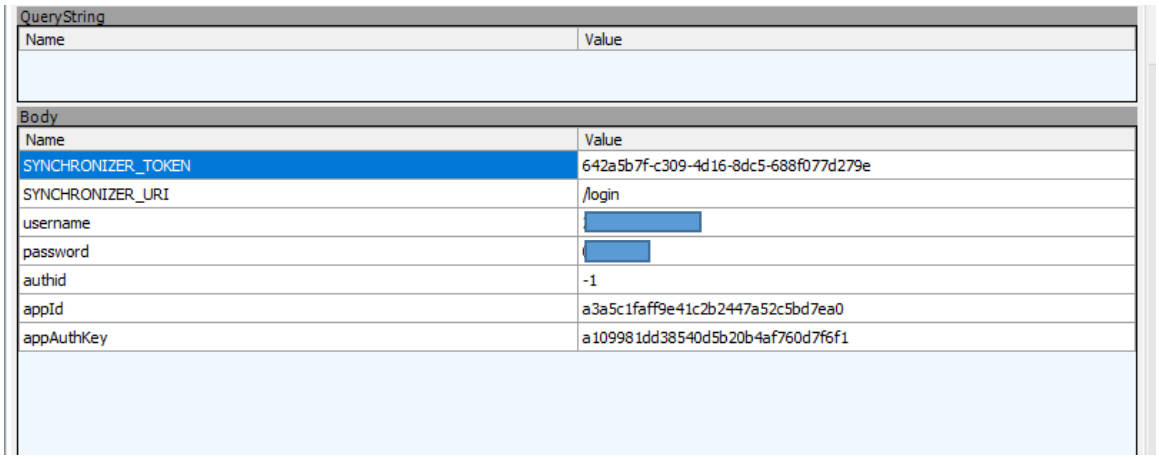
XML

```
HTTP/1.1 200 OK
Date: Mon, 10 Dec 2018 01:37:30 GMT
Server: Apache-Coyote/1.1
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;charset=UTF-8
Content-Language: zh-CN
Keep-Alive: timeout=5, max=999
Connection: Keep-Alive
Content-Length: 9010

<!DOCTYPE html>

<html>
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
    <title>首页</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link rel="shortcut icon" href="/static/D4IVMkzmNj72OjJFh2C2TffEqedXopZEw95HhtmKMIm.ico" type="image/x-ic
```

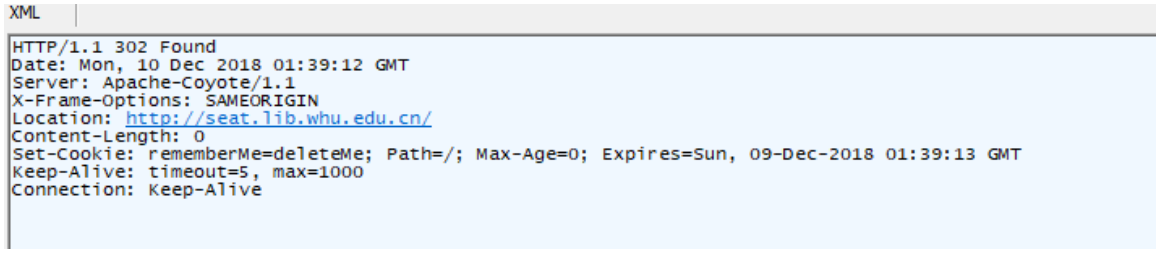
3、登录认证

Req：

Param:TOKEN 和 URI 来自登陆页面， authid 固定，appid 和 appAuthKey 固定写在前面的某个 js 里，直接用



Res:



4、请求登陆后页面(重定向来的?)

Req:

```
GET http://seat.lib.whu.edu.cn/ HTTP/1.1
Host: seat.lib.whu.edu.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://seat.lib.whu.edu.cn/login?targetUri=%2F
Connection: keep-alive
Cookie: JSESSIONID=35D29F58753C6BCF42CE20D596A83AF7
Upgrade-Insecure-Requests: 1
```

Res:

```
HTTP/1.1 200 OK
Date: Mon, 10 Dec 2018 01:39:13 GMT
Server: Apache-Coyote/1.1
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;charset=UTF-8
Content-Language: zh-CN
Keep-Alive: timeout=5, max=999
Connection: Keep-Alive
Content-Length: 37743



<html>
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
    <title>自选座位 :: 图书馆空间预约系统</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta name="keywords" content="利昂系统，利昂软件，图书馆空间预约系统，占座系统，私有云网盘开发商"/>
    <meta name="description" content=""/>
    <link rel="shortcut icon" href="/static/D4IVMkzmNj72OjJFh2C2TffEqedXopZEw95HhtmKMIm.ico" type="image/x-ic
```

得到登陆后页面源码和一个 css

5、获得座位相关信息

Req:

```
POST http://seat.lib.whu.edu.cn/freeBook/ajaxGetRooms HTTP/1.1
Host: seat.lib.whu.edu.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://seat.lib.whu.edu.cn/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 4
Connection: keep-alive
Cookie: JSESSIONID=35D29F58753C6BCF42CE20D596A83AF7

id=1
```

Res:各个区域的对应 value

```
HTTP/1.1 200 OK
Date: Mon, 10 Dec 2018 01:39:50 GMT
Server: Apache-Coyote/1.1
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;charset=UTF-8
Content-Length: 888
Keep-Alive: timeout=5, max=1000
Connection: Keep-Alive


    <a href="javascript:void(0)" value="4">3C创客空间</a>

    <a href="javascript:void(0)" value="5">创新学习讨论区</a>

    <a href="javascript:void(0)" value="6">西自然科学区</a>

    <a href="javascript:void(0)" value="7">东自然科学区</a>

    <a href="javascript:void(0)" value="8">西社会科学区</a>

    <a href="javascript:void(0)" value="9">西图书阅览区</a>

    <a href="javascript:void(0)" value="10">东社会科学区</a>

    <a href="javascript:void(0)" value="11">东图书阅览区</a>

    <a href="javascript:void(0)" value="12">自主学习区</a>

    <a href="javascript:void(0)" value="13">3C创客电子阅读</a>

    <a href="javascript:void(0)" value="14">3C创客双屏电脑</a>

    <a href="javascript:void(0)" value="15">创新学习苹果区</a>

    <a href="javascript:void(0)" value="16">创新学习云桌面</a>
```

6、指定区域座位搜索功能：

Req：

```
POST http://seat.lib.whu.edu.cn/freeBook/ajaxSearch HTTP/1.1
Host: seat.lib.whu.edu.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://seat.lib.whu.edu.cn/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 89
Connection: keep-alive
Cookie: JSESSIONID=35D29F58753C6BCF42CE20D596A83AF7

onDate=2018-12-10&building=1&room=6&hour=1&startMin=720&endMin=780&power=null&window=null
```

参数：

Body

Name	Value
onDate	2018-12-10
building	1
room	6
hour	1
startMin	720
endMin	780
power	null
window	null

这里以信图实验的话：

building=1 是信图

room 6 是前面所说 西自然科学，

hour 表示时长

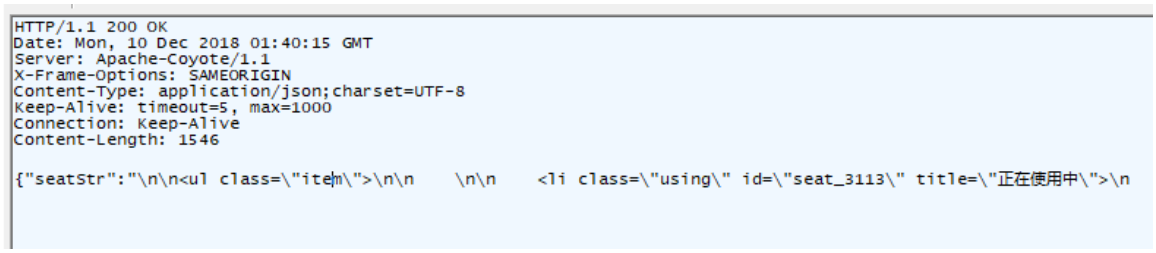
startMin 开始时间　12-> 12*60=720

endMin 结束时间　13-> 13&60=780

power 带插座

window 靠窗

Res：



整理如下：

{“seatStr”:

“

<ul class=\”item\”>

```
<li class=\"using\" id=\"seat_3113\" title=\"正在使用中\">
<dl>
    <dt>005<\u002fdt>
    <dd>西自然科学区<\u002fdd>
    <\u002fdl>
    <\u002fli>
```

”,

“seatNum”:7,

“onDate”:”2018-12-10”,

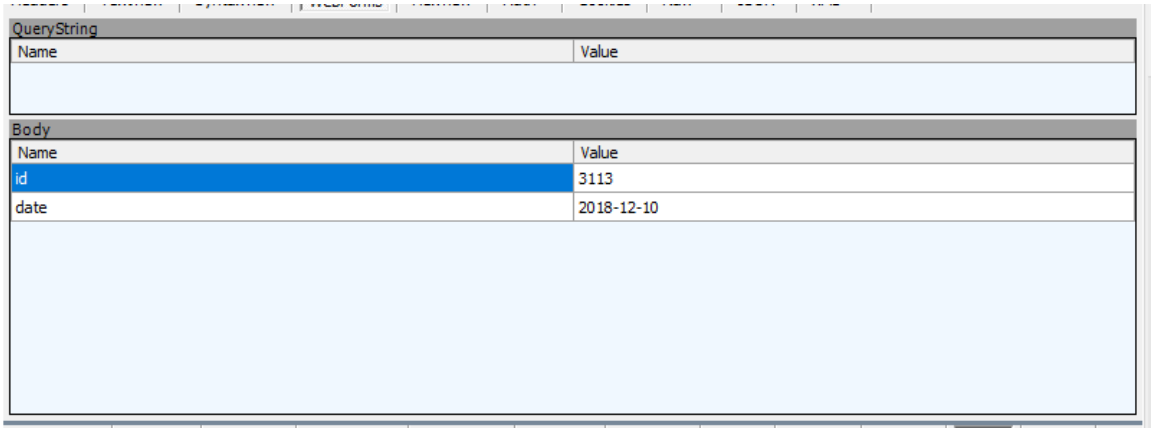
“offset”:-1

}

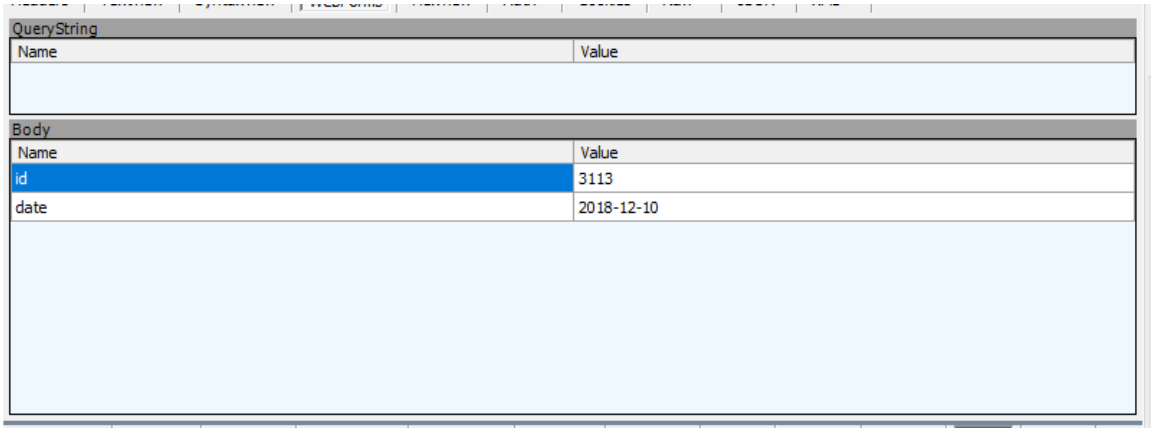
7、选定座位后确定时间：由于抢座都是事先确定好了位置直接发包，所以应该没卵用

流程：先点击座位会得到开始时间，然后选完开始时间会得到结束时间

第一次 Req：发送选择的座位号



Res:



座位当前可以预约的开始时间：

```
HTTP/1.1 200 OK
Date: Mon, 10 Dec 2018 01:47:37 GMT
Server: Apache-Coyote/1.1
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;charset=UTF-8
Content-Length: 491
Keep-Alive: timeout=5, max=1000
Connection: Keep-Alive

<input type="hidden" name="seat" value="3113" id="seat" />
<input type="hidden" name="room" value="西自然科学区" id="room" />
<input type="hidden" name="building" value="信息馆" id="building" />


    <li><a href="#" time="690">11:30</a></li>
    <li><a href="#" time="720">12:00</a></li>
    <li><a href="#" time="750">12:30</a></li>
    <li><a href="#" time="780">13:00</a></li>
    <li><a href="#" time="810">13:30</a></li>
    <li><a href="#" time="1320">22:00</a></li>
```

第二次发包对应点完起始时间获得右边窗口结束时间：

Req:

QueryString

Name	Value

Body

Name	Value
start	720
seat	3113
date	2018-12-10

Res:

```
HTTP/1.1 200 OK
Date: Mon, 10 Dec 2018 01:47:38 GMT
Server: Apache-Coyote/1.1
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;charset=UTF-8
Content-Length: 191
Keep-Alive: timeout=5, max=999
Connection: Keep-Alive

    <li><a href="#" time="750">12:30</a></li>

    <li><a href="#" time="780">13:00</a></li>

    <li><a href="#" time="810">13:30</a></li>

    <li><a href="#" time="840">14:00</a></li>
```

8、发送预约包，这是主要的步骤之一

Req：

```
POST http://seat.lib.whu.edu.cn/selfRes HTTP/1.1
Host: seat.lib.whu.edu.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://seat.lib.whu.edu.cn/
Content-Type: application/x-www-form-urlencoded
Content-Length: 213
Connection: keep-alive
Cookie: JSESSIONID=35D29F58753C6BCF42CE20D596A83AF7
Upgrade-Insecure-Requests: 1

SYNCHRONIZER_TOKEN=00d64940-9fe3-4e0e-b508-9b09b239aeb7&SYNCHRONIZER_URI=%2F&date=2018-12-10&seat=3113&start=72
```

Param:

Body

Name	Value
SYNCHRONIZER_TOKEN	00d64940-9fe3-4e0e-b508-9b09b239aeb7
SYNCHRONIZER_URI	/
date	2018-12-10
seat	3113
start	720
end	780
authid	-1
appId	a3a5c1faff9e41c2b2447a52c5bd7ea0
appAuthKey	a109981dd38540d5b20b4af760d7f6f1

Date\seat\start\end\authid\appId\appAuthKey 都如前所述

这个 SYNCHRONIZER_TOKEN 和 URI 藏在登陆后的界面里，到时候模拟发包验证下

Res: 预约成功会出现,正则匹配下'系统已经为您 xxxx'

```
<dt>系统已经为您预定好了<span style="color:red">座位</span></dt>
<dd><em>凭证号  :  </em>0200-175-1</dd>
<dd><em>日    期 :  </em>2018 年 12 月 10 日</dd>
<dd><em>时    间 :  </em>12 : 00 - 13 : 00</dd>
<dd><em>位    置 :  </em>信息馆2层西区西自然科学区，座位号005</dd>
<dd><em>状    态 :  </em>预约</dd>

<!--dd>如您已经关联空间预约微信号，可发送<strong>CX</strong>至空间预约微信账号获取预约凭证</dd-->
<dd><span>请在 12月10日11点45分 至 12点35分 之间前往场馆签到</span></dd>
```

就上面分析来看的话，如果只发送登录包和最后的预约包就行，可以 python 模拟登陆试一下。

实际使用 python 的 requests 发包登陆时，由于重定向原因，返回包顺序与上述不太一样，一些包并没有收到，不过大致思路一样，时间仓促，随便写写…