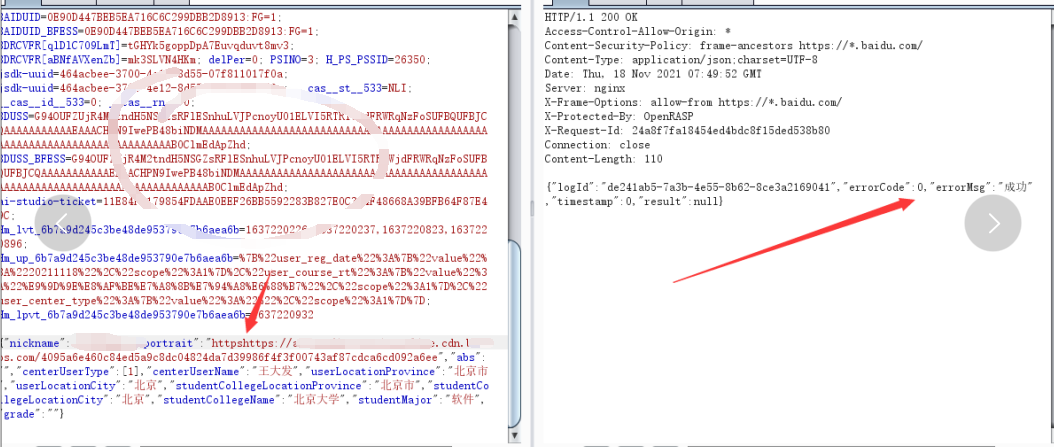
某src的一个站点的个人信息中心，发现保存图片的参数可控，于是发现有了下列：

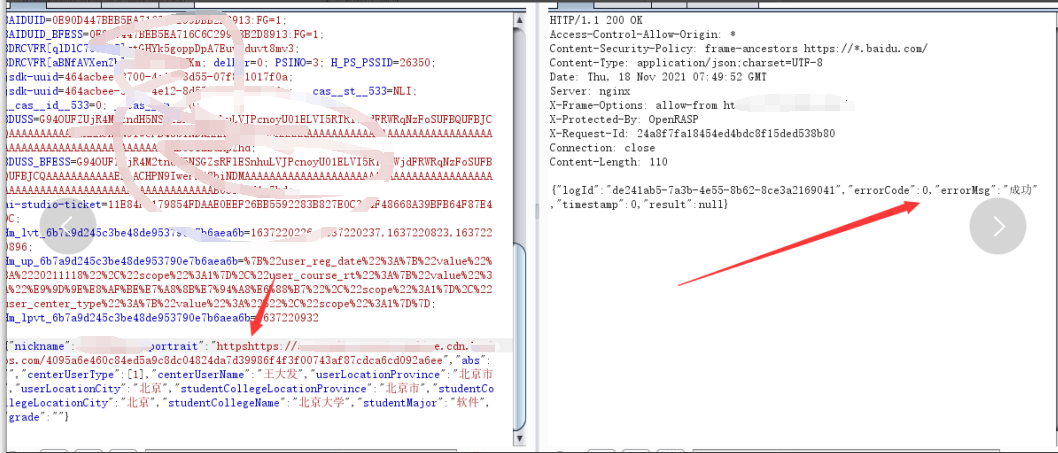
登录之后来到个人中心



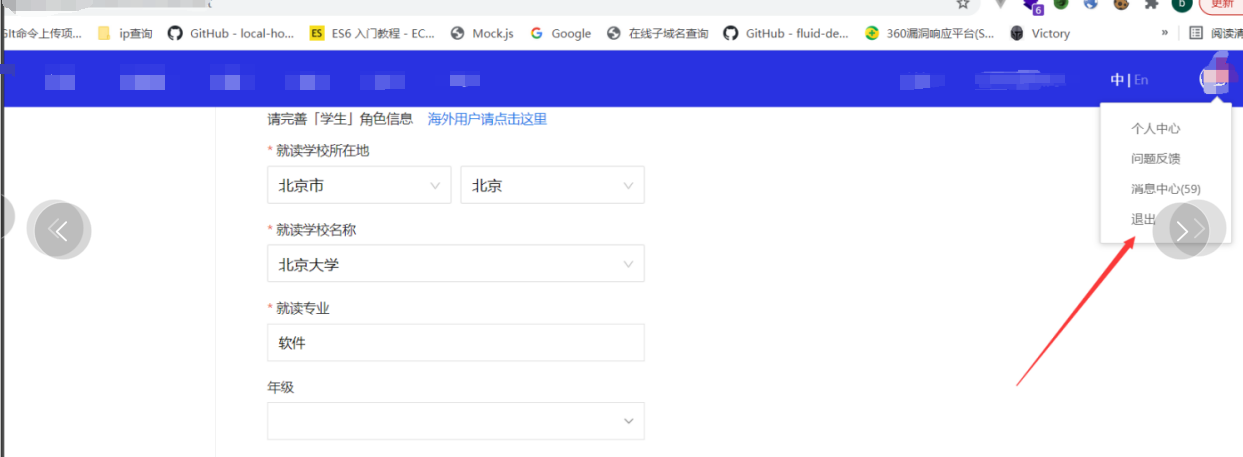
再点击更换头像的时候抓包：



可以发现portrait 参数 就是存头像的地址，把这个包发送到repeat尝试修改：



于是我们就去获取退出时的链接来替换此时的头像链接：

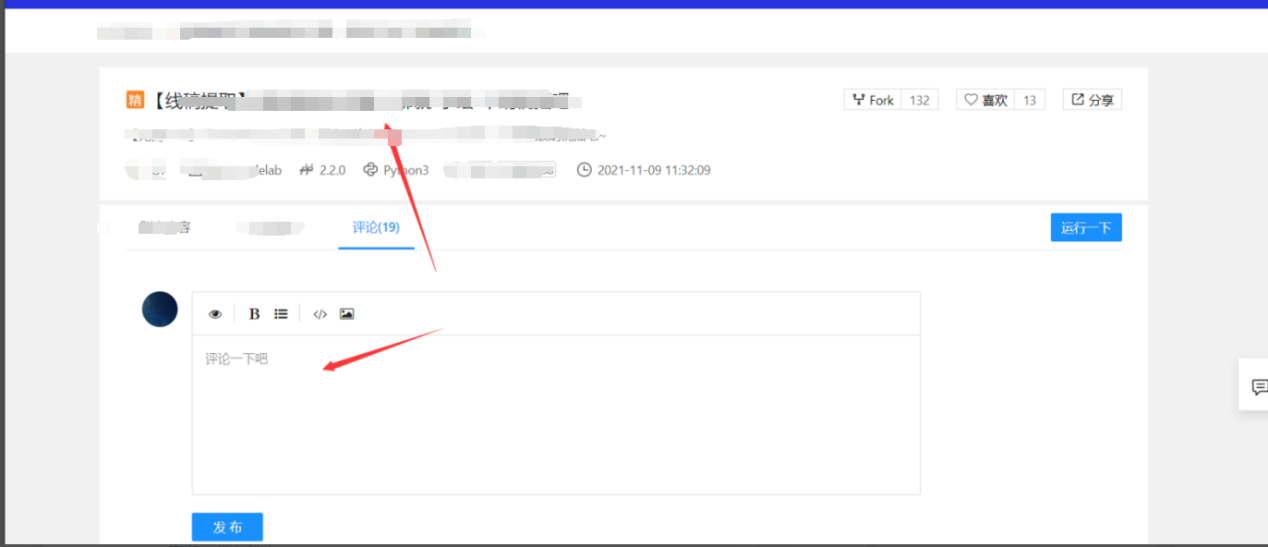


[https://xxxxx.du.com/xxx/logout?r=https://passport.xxxdu.com/?logout&u=http%3A%2F%2Fxxxx.xxxxdu.com%2Faistudio%2Fuserinfoedit](https://aistudio.baidu.com/studio/logout?r=https://passport.baidu.com/?logout&u=http%3A%2F%2Faistudio.baidu.com%2Faistudio%2Fuserinfoedit)

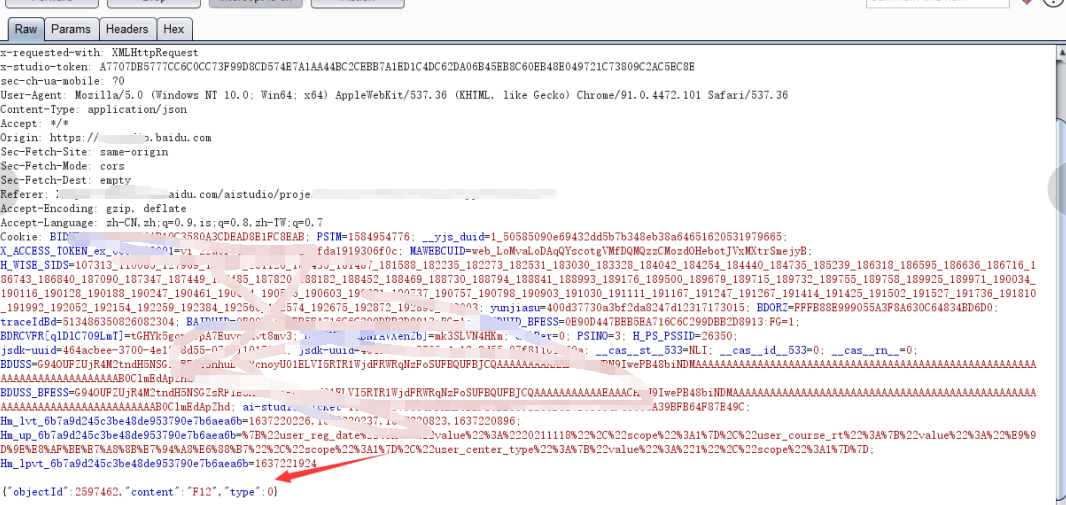
这是退出的请求，也是我们下面必须的操作，具体利用过程是下面的操作，上面的操作是解释这一个点：

**这个漏洞的思想就是利用csrf漏洞让别人在访问该站点的某个地方的时候突然掉线，而有交互的地方就是在论坛、评论、留言板等地方。**

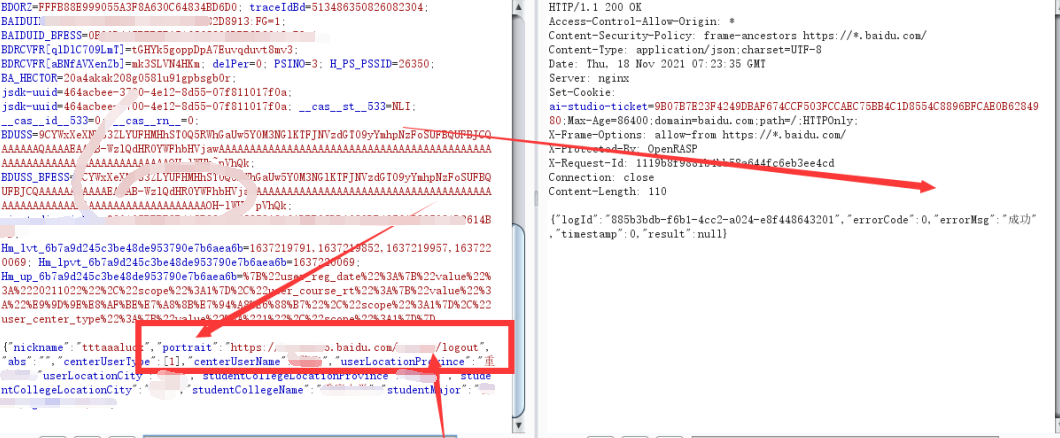
回到上述案例中，我们在该站点中发现了有评论留言的地方：



于是开始评论，然后发表的时候抓包：



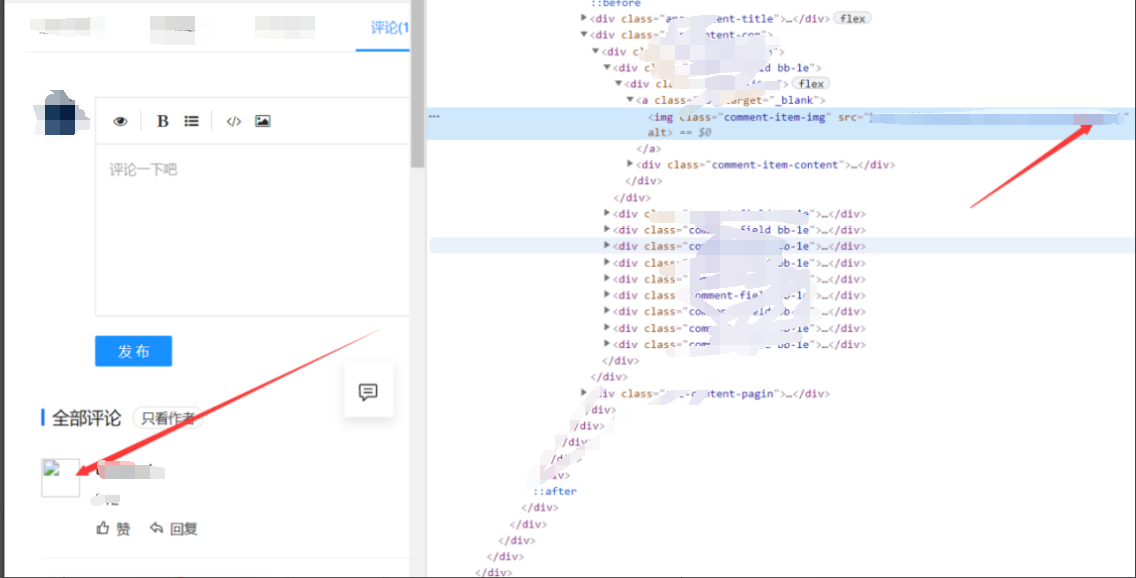
然后放包后会抓取到获取我们的个人信息的资料的包，此时我们就可以进行操作了：

****

然后放包即可评论成功，但是头像处的链接被我换成了退出连接，当别的用户来访问时，自动就退出登录：



进行元素审查，我们可以发现此时头像位置是退出登录的链接



此时当别的用户访问到我们的留言时，系统也是自动就退出来。