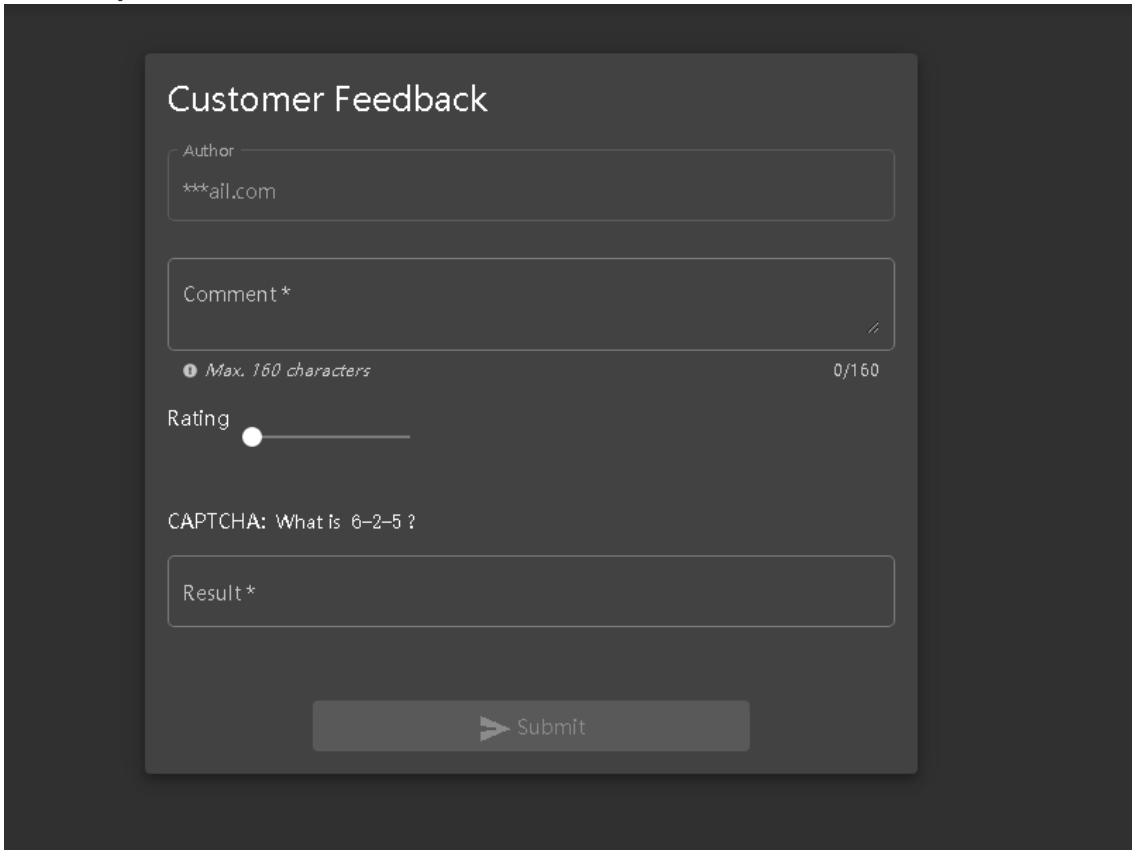
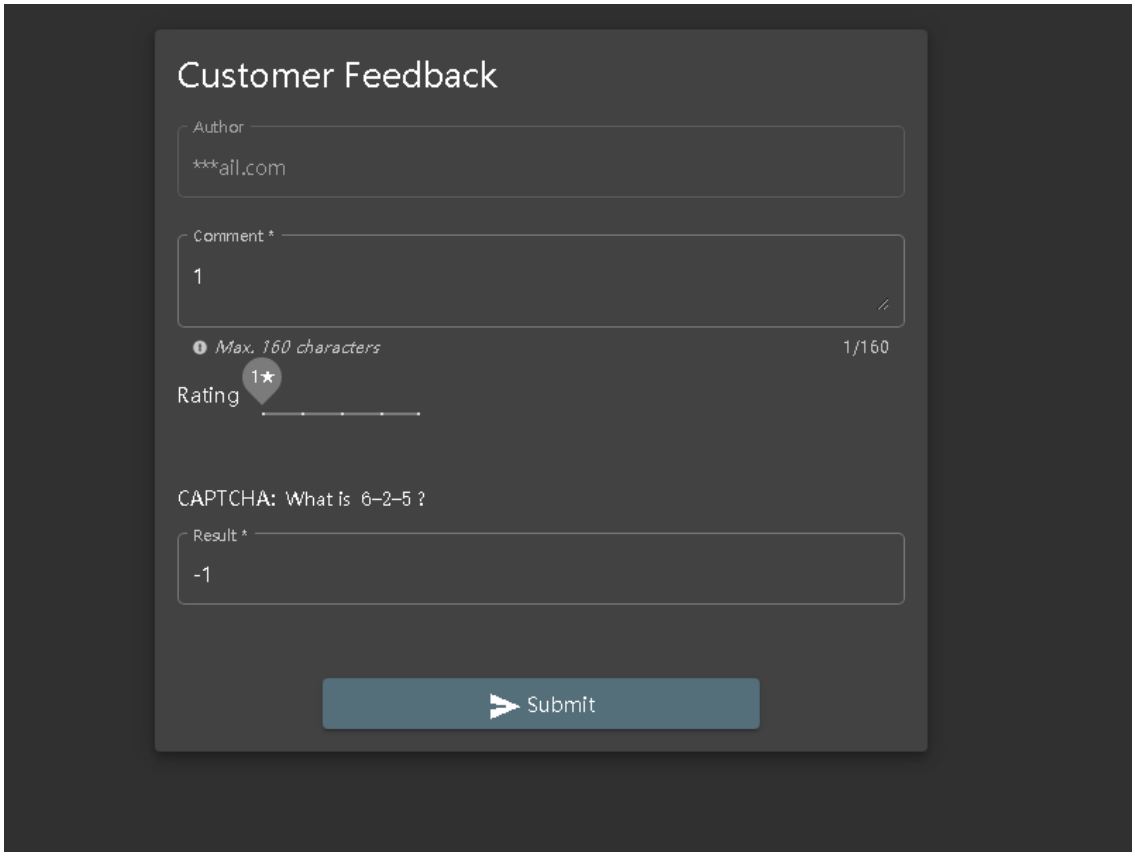
Proxy实战

Zero stars

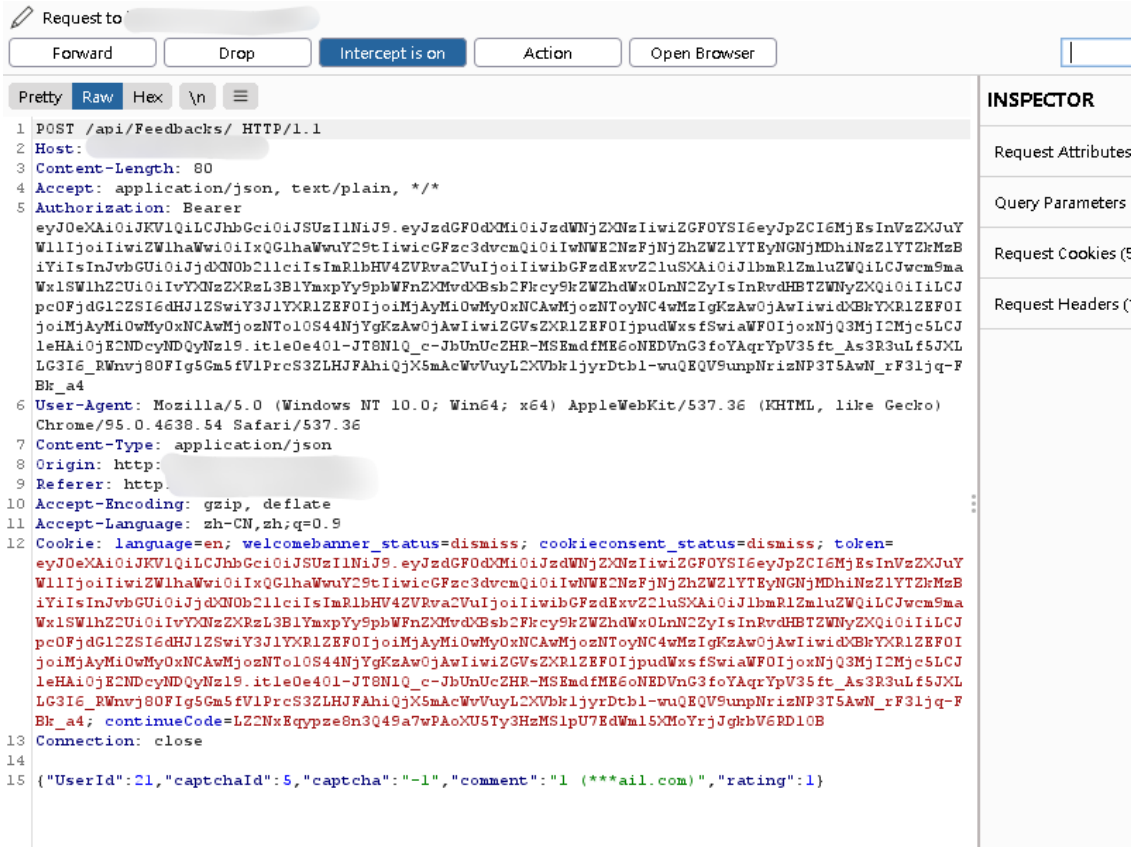
1. 输入链接**ip:3000/#/contact**进入顾客反馈界面



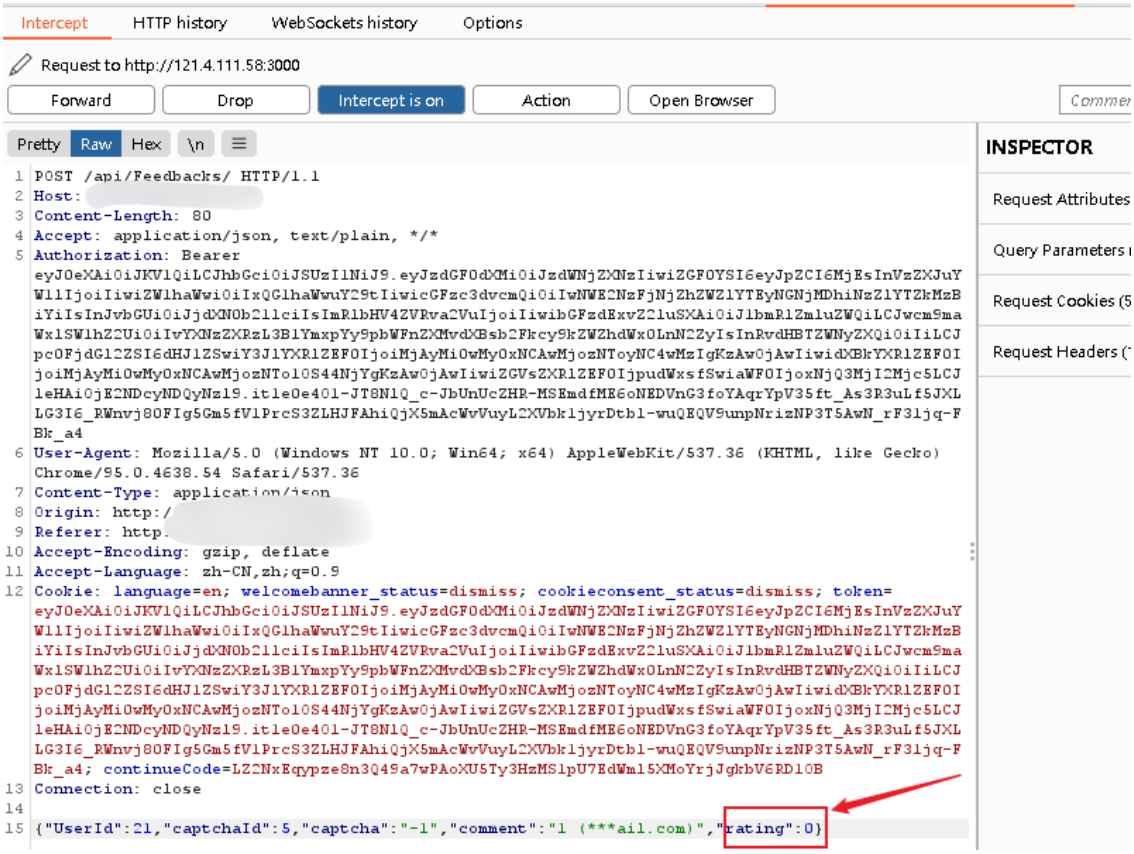
2. 题目要求评论零星，任意提交评论，只能提交1星



3. 配置代理，利用BurpSuite对评论提交数据包抓取



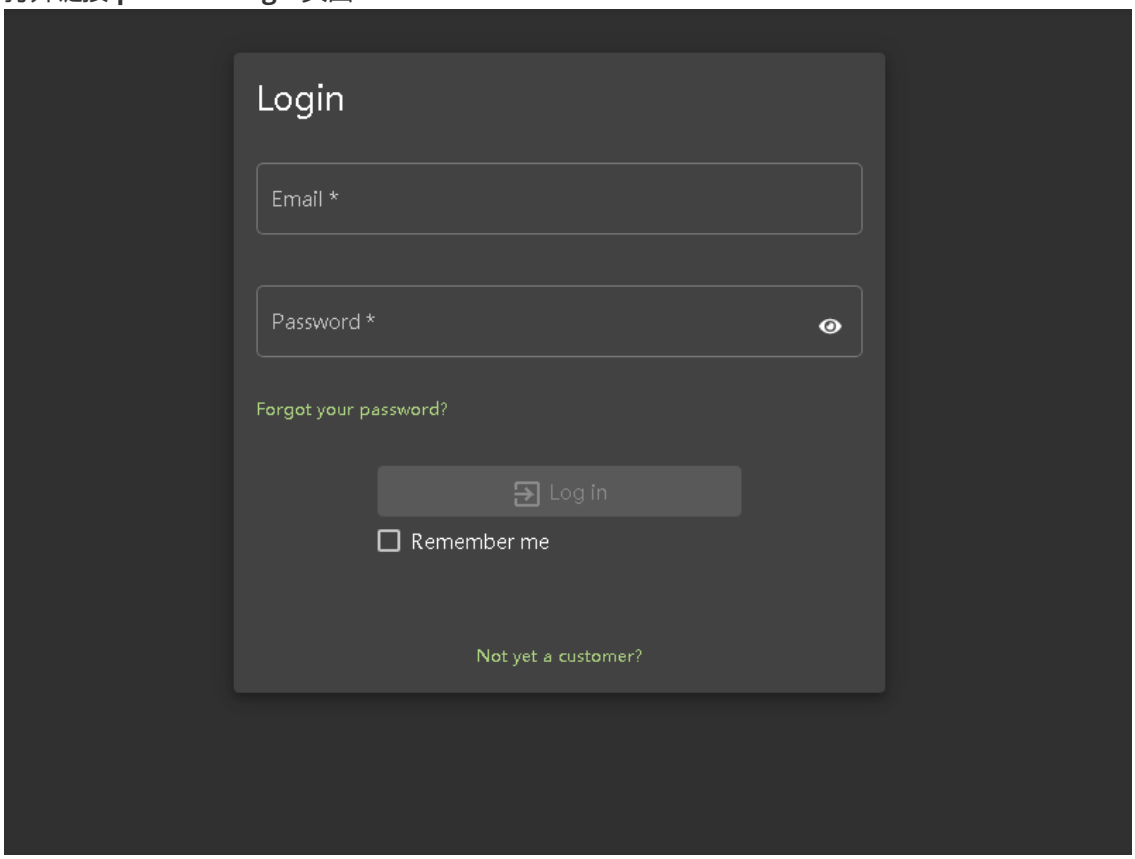
4. 抓取的数据包中，底部有数据名为rating，更改评分数值为0，点击Forward



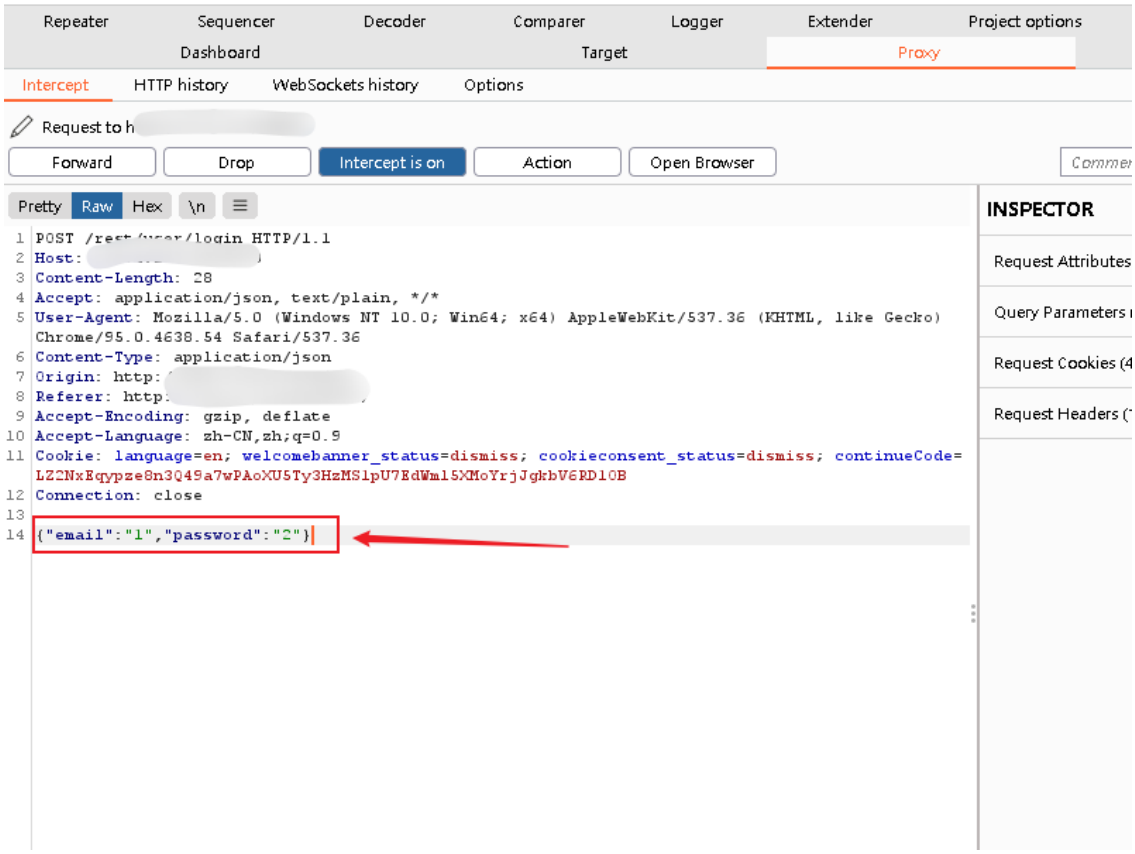
5. ScoreBoard挑战完成

login admin

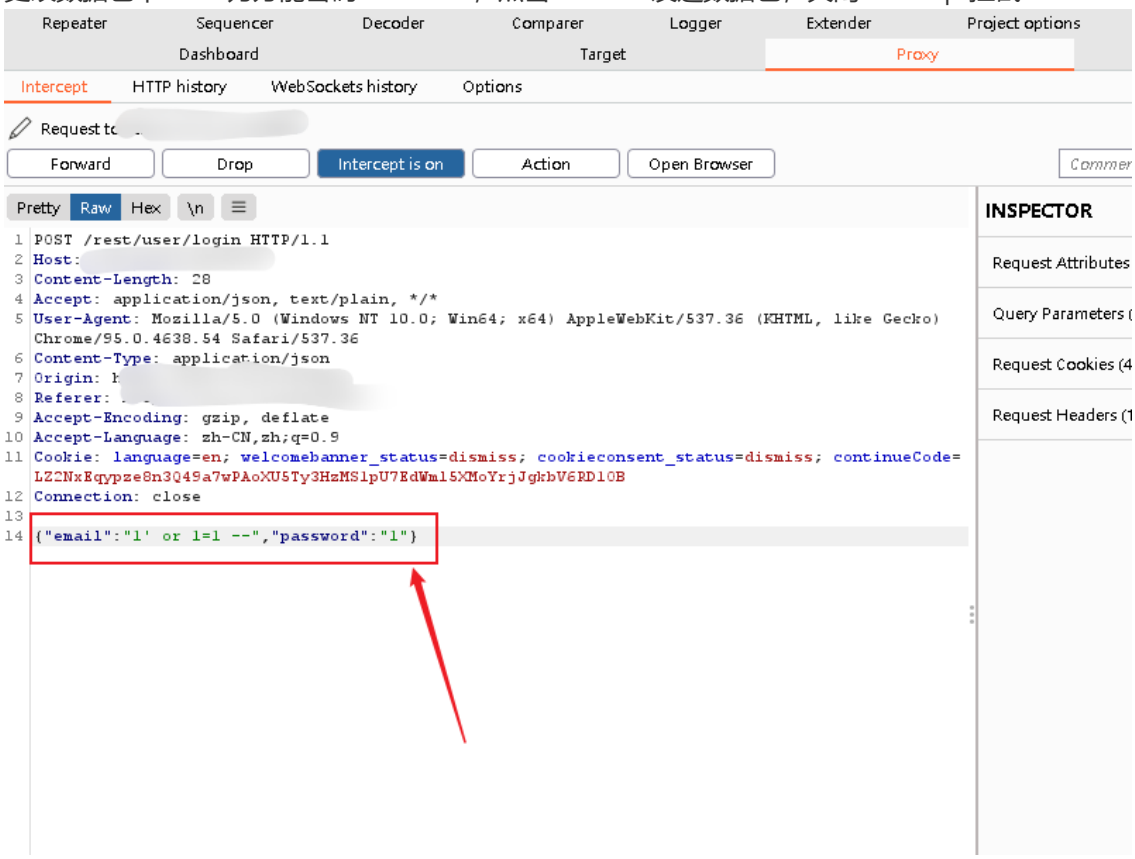
1. 打开链接**ip:3000/#/login**页面



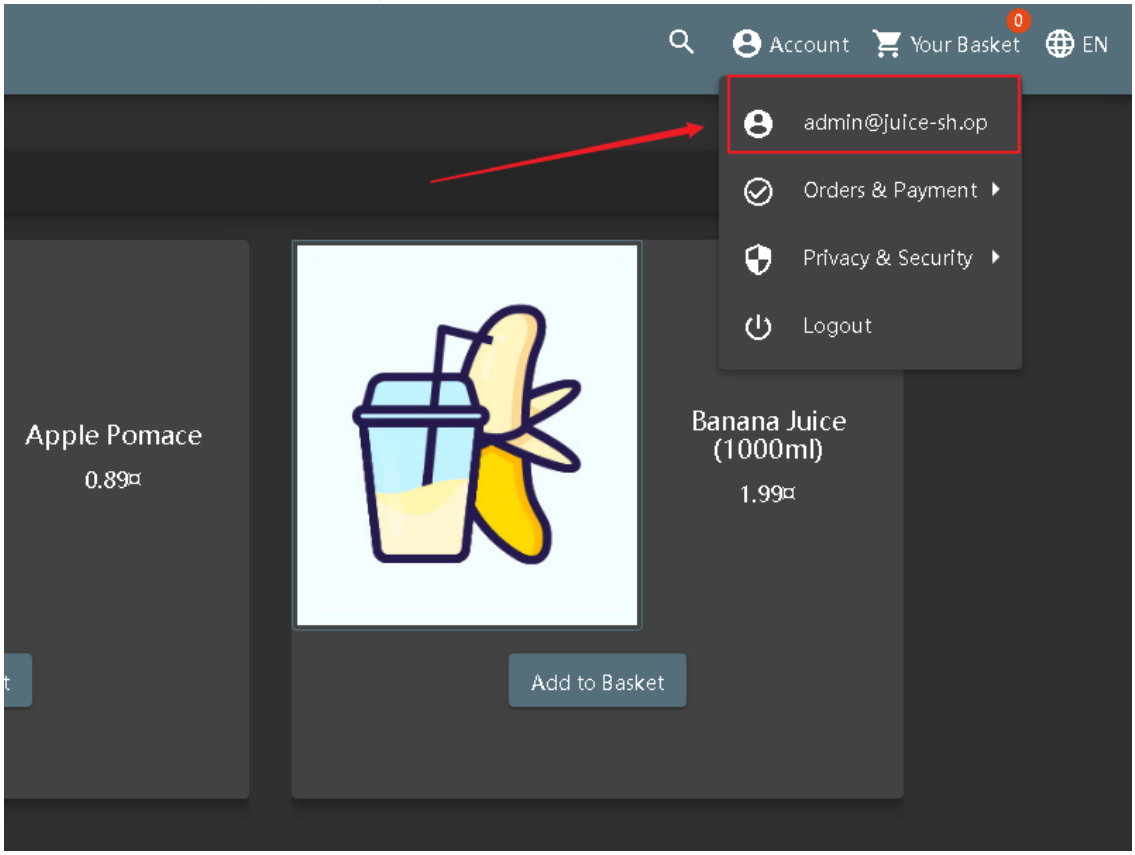
2. 填写任意用户名和密码，开启代理，使用BurpSuite抓取提交数据包



3. 更改数据包中email为万能密码' **or 1=1 --**，点击Forward发送数据包，关闭Intercept拦截



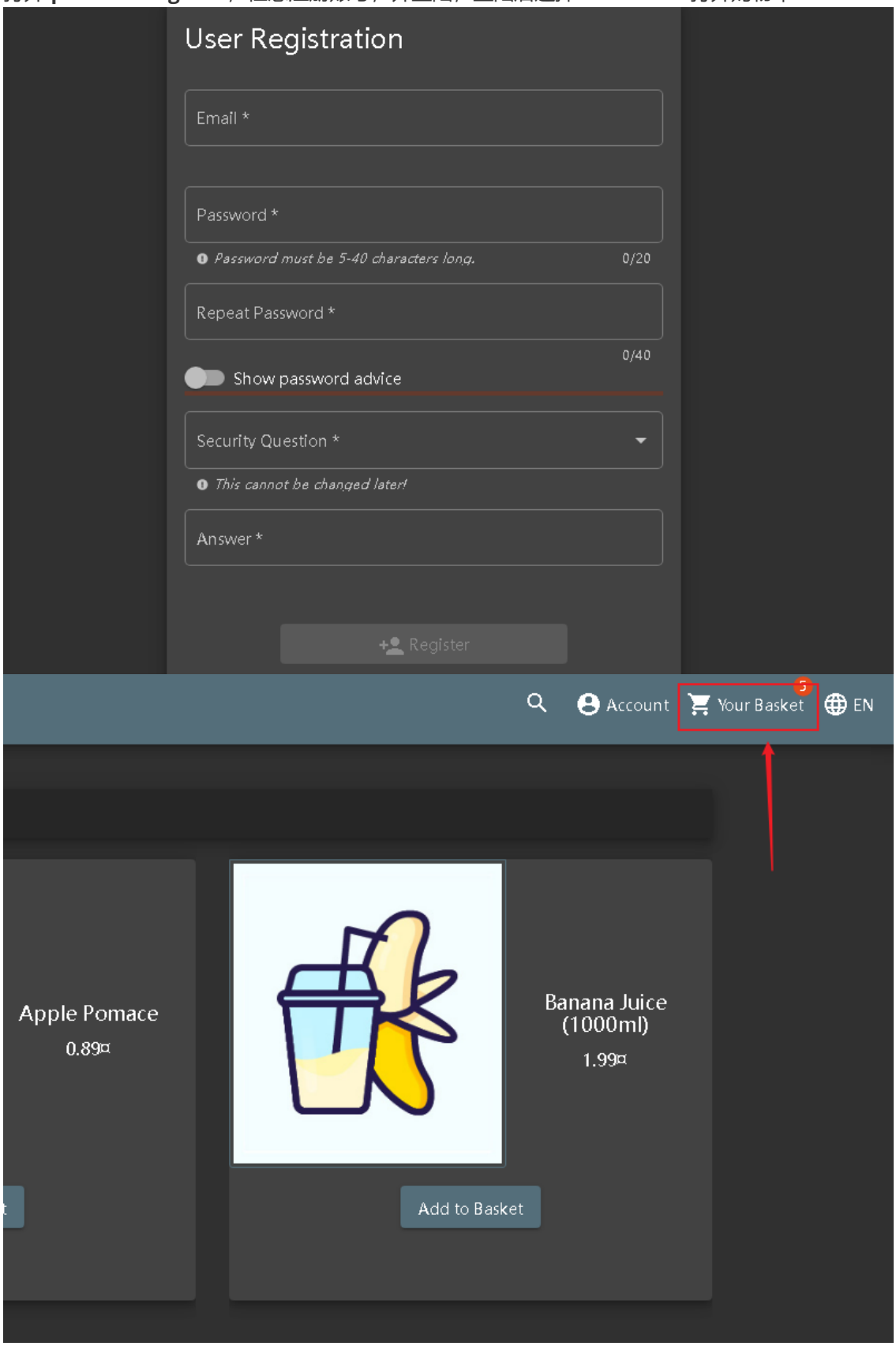
4. 登陆进角色为admin@juice-sh.op



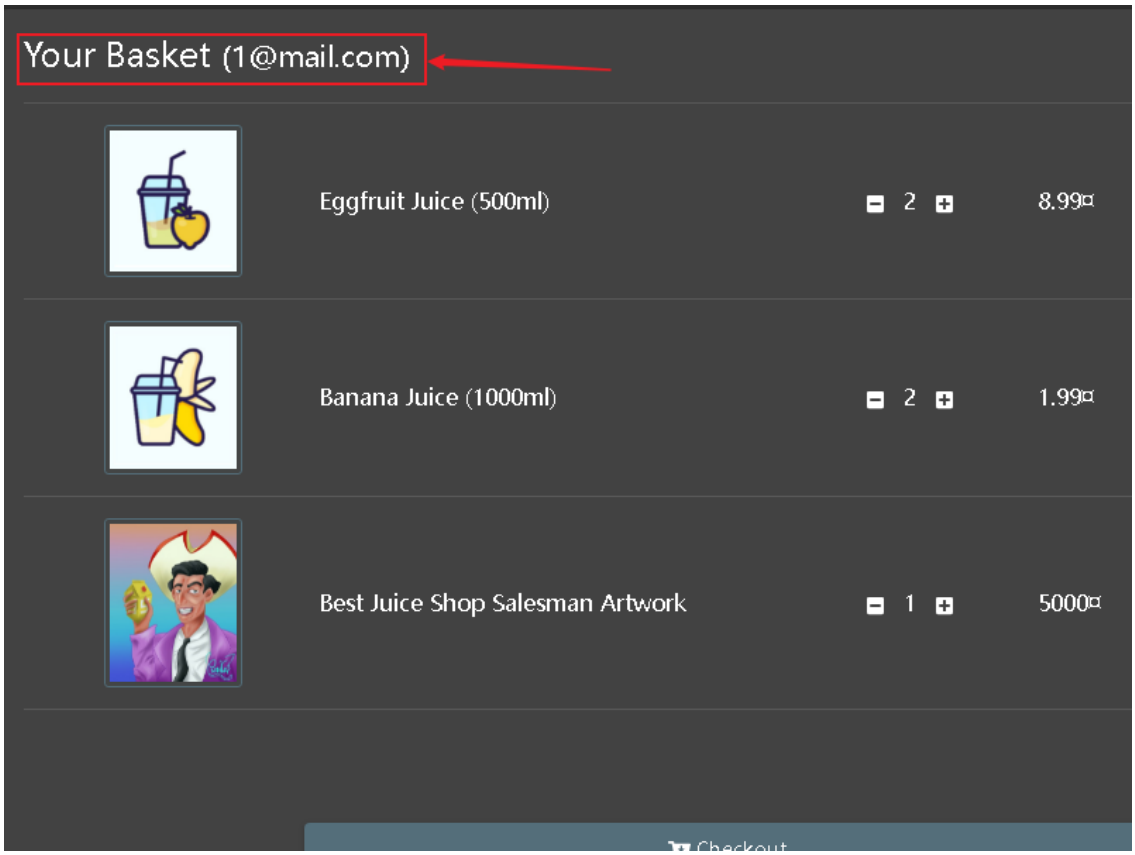
5. login admin挑战完成

view basket

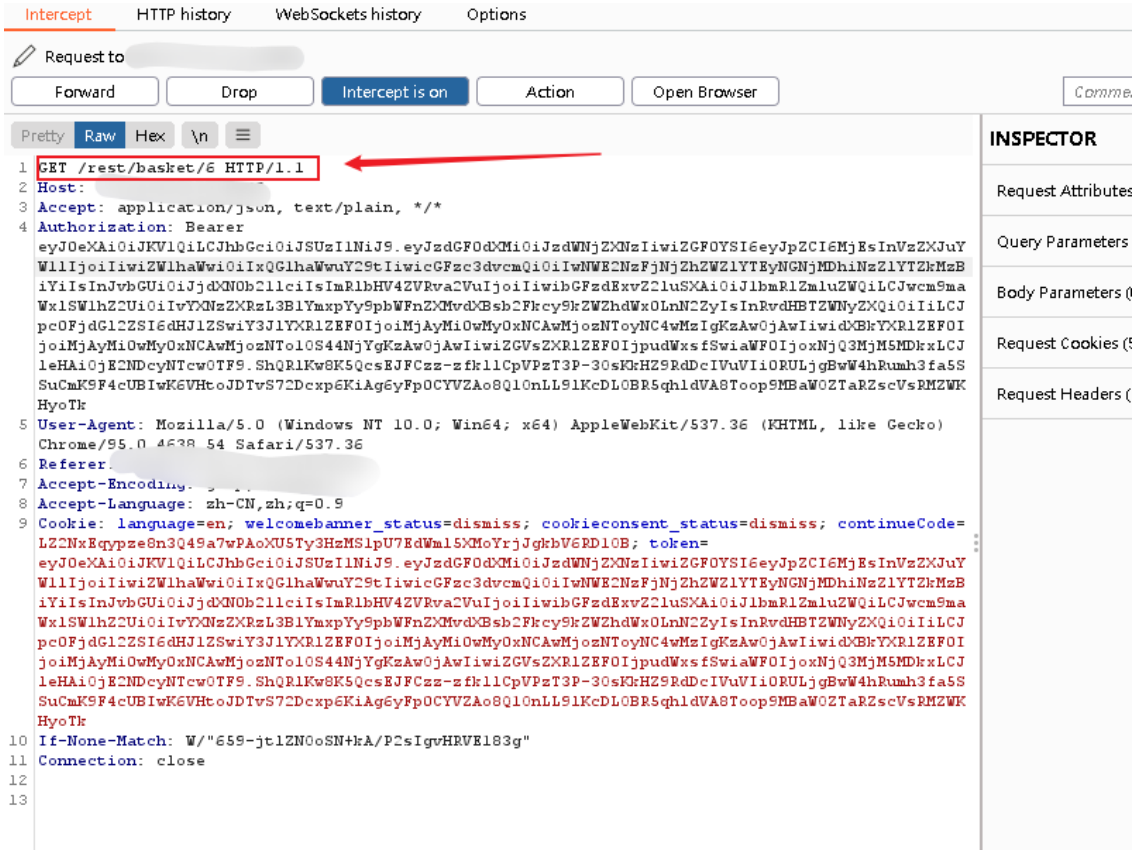
1. 打开**ip:3000/#/register**，任意注册账号，并登陆，登陆后选择Your Basket打开购物车



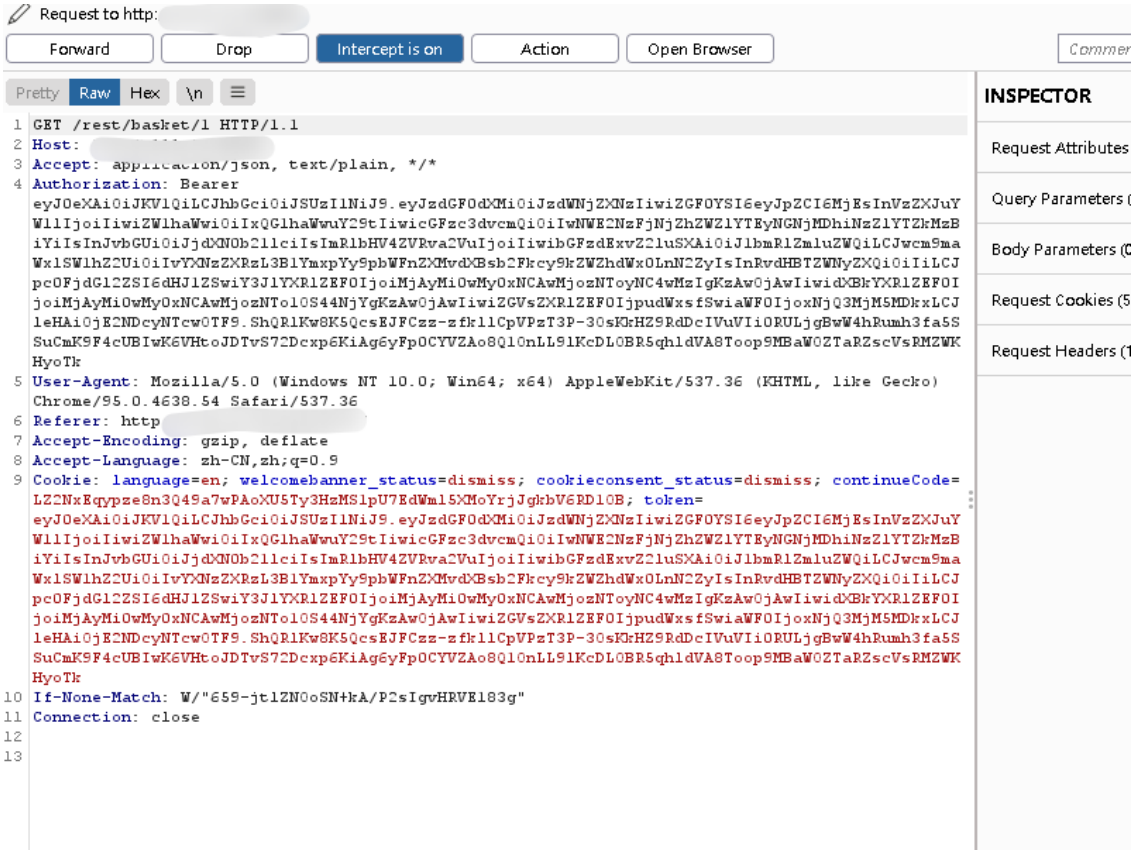
2. 购物车中可以看到当前用户的购物车信息



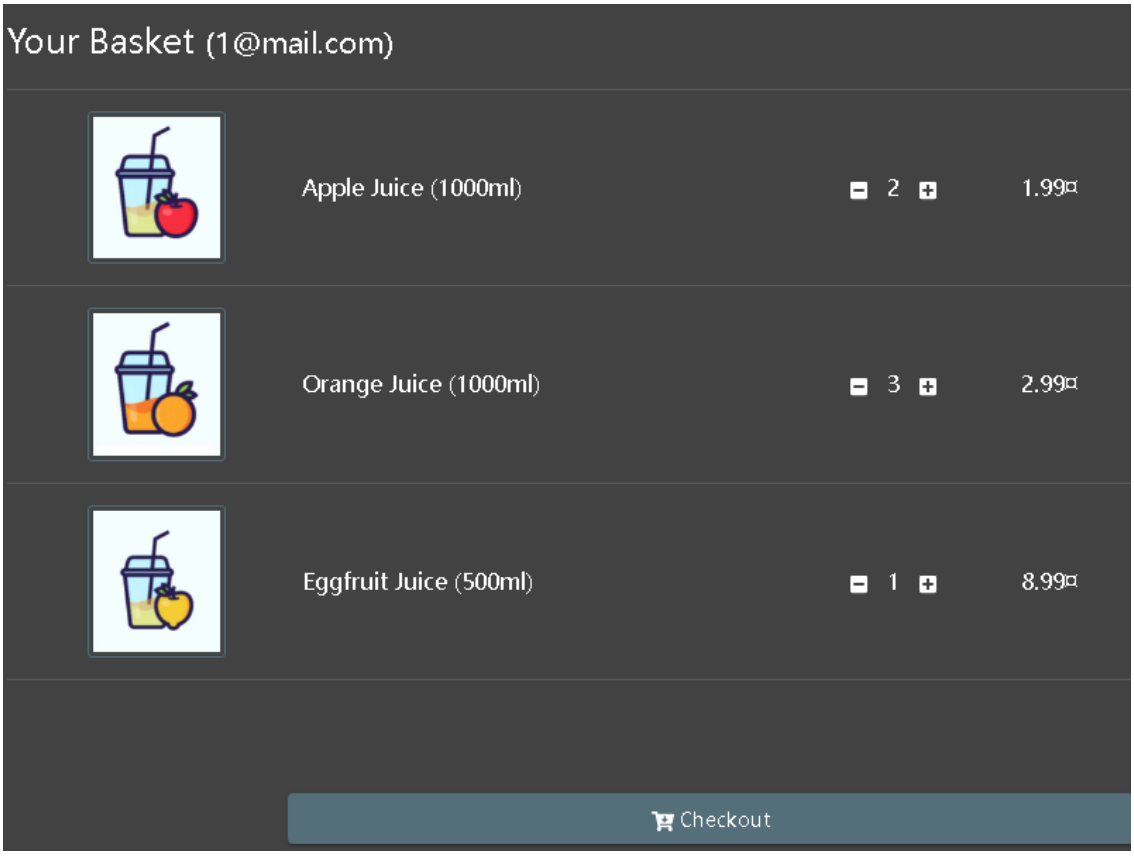
3. 开启代理，再次点击Your Basket，抓取访问购物车页面的数据包，头部URL路径显示/rest/basket/6



4. 修改数字为1，访问id为1的用户购物车



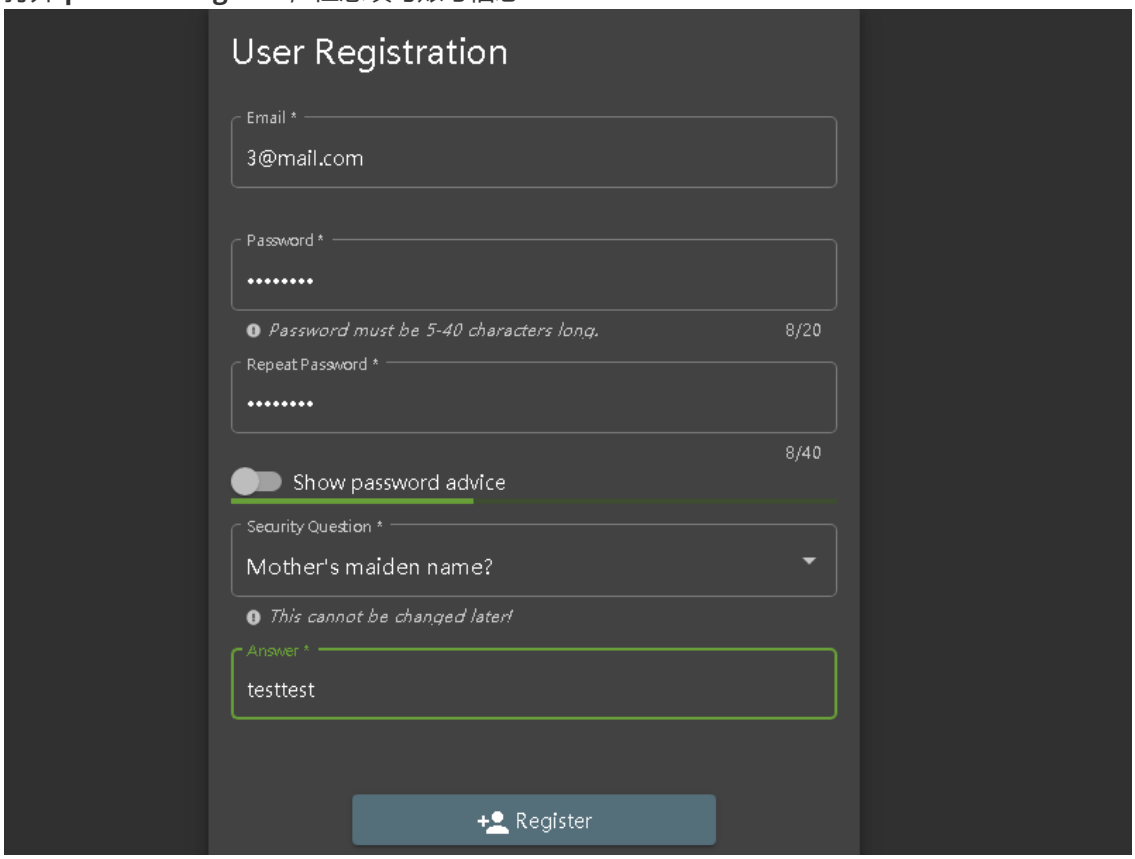
5. 点击Forward访问成功(上方显示用户名不改变)



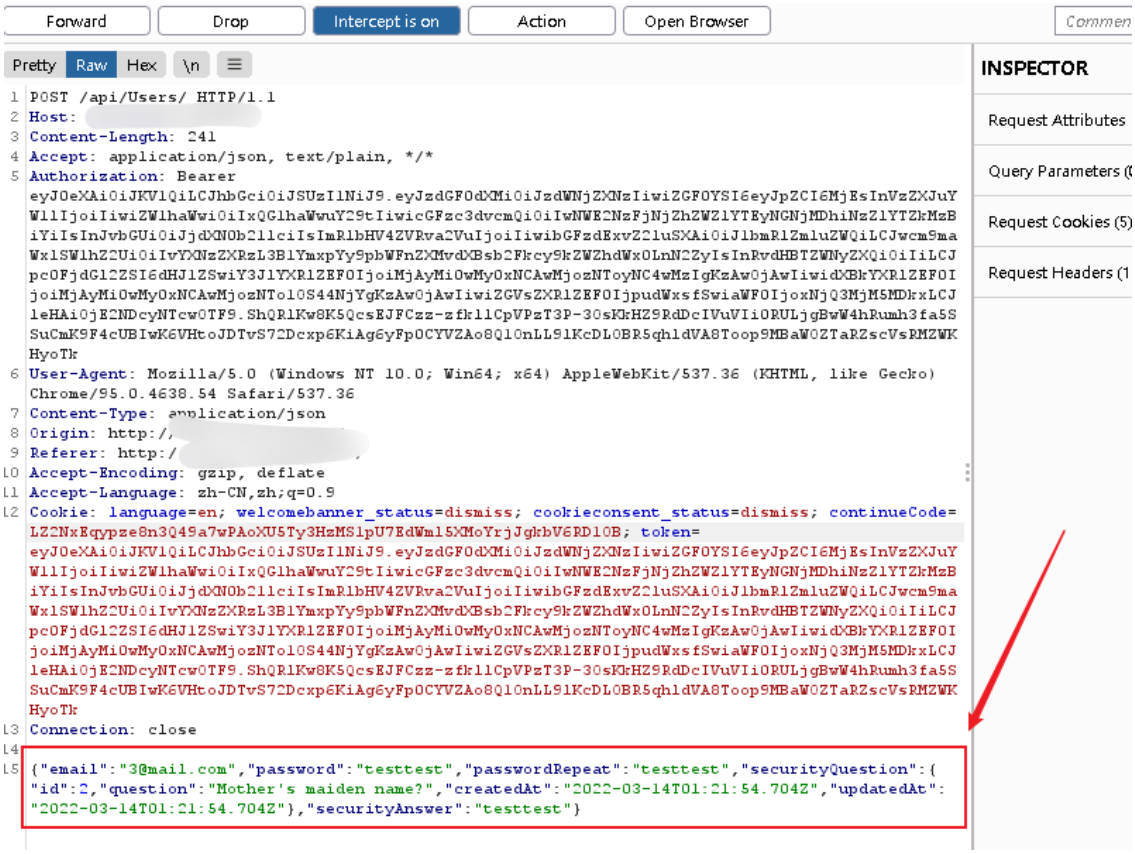
6. view basket挑战成功

admin registration

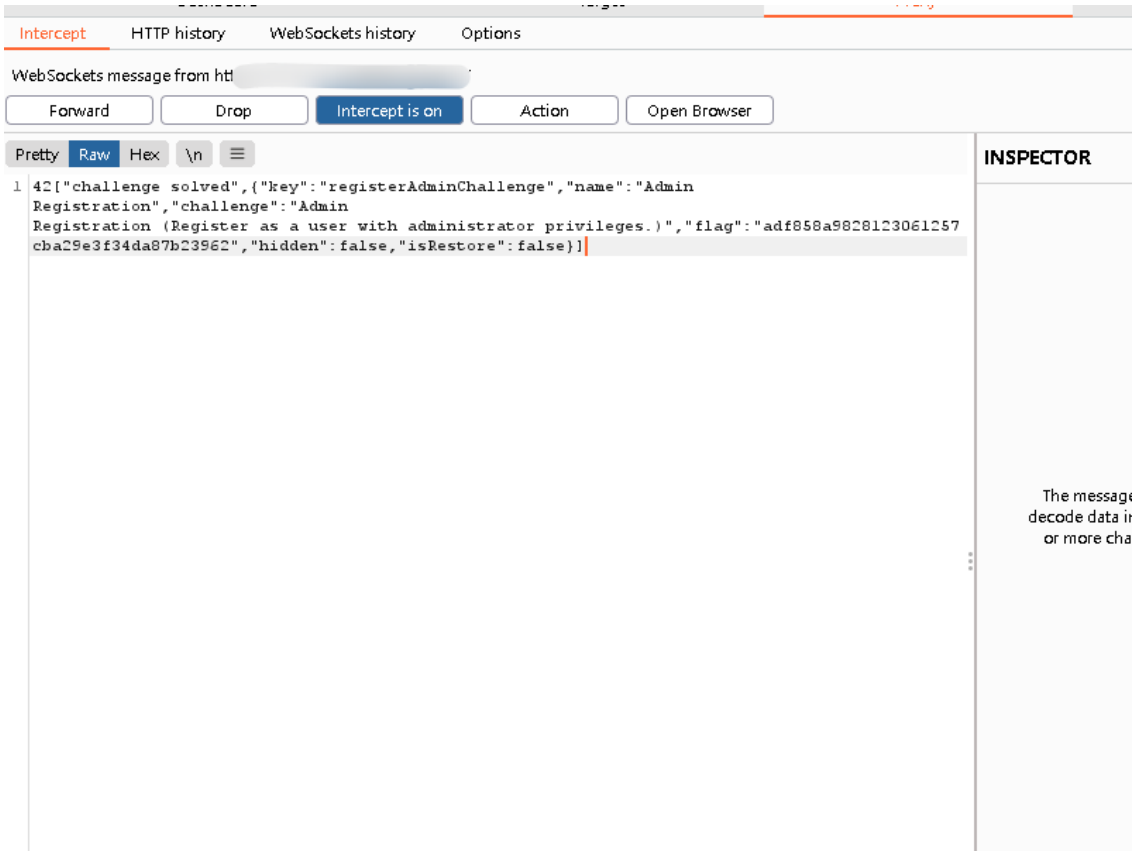
1. 打开**ip:3000/#/register**，任意填写账号信息



2. 开启代理，利用BurpSuite抓取提交注册请求的数据包，数据包下方显示注册信息



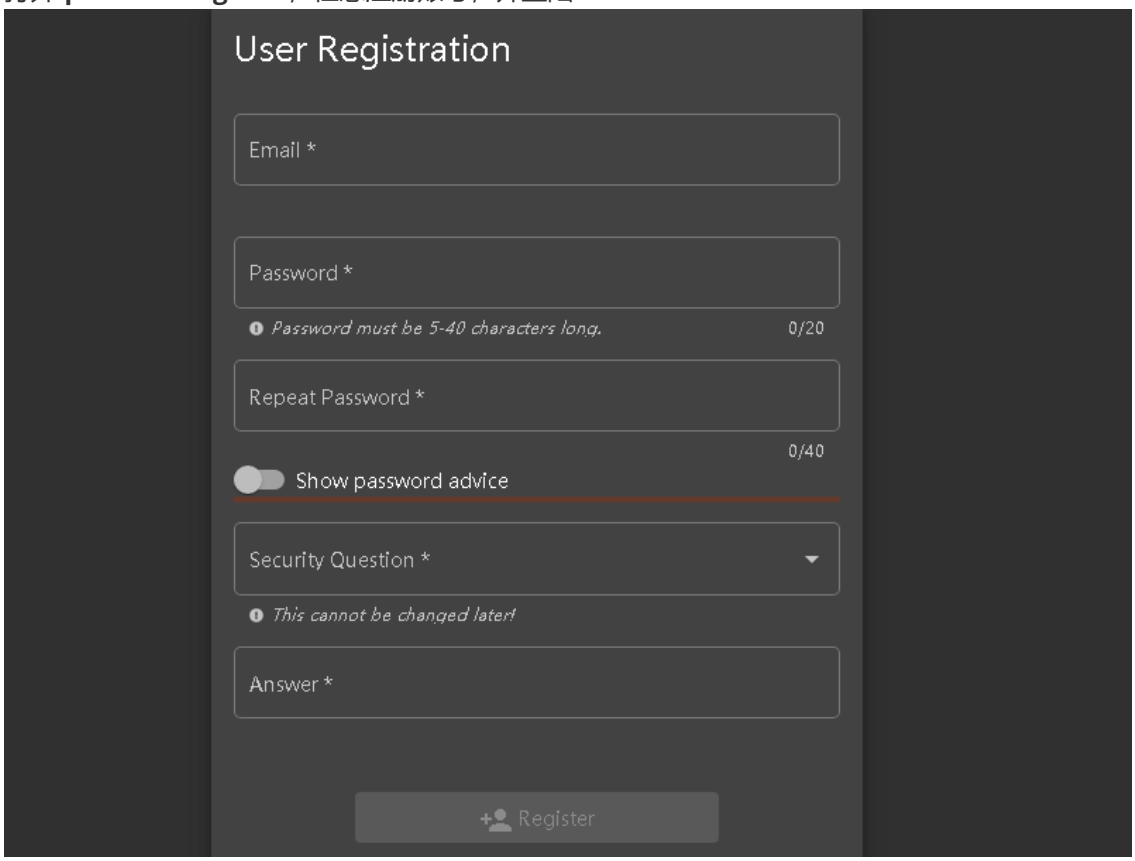
3. 添加**"role":"admin"**，点击Forward发送数据包，返回成功数据包



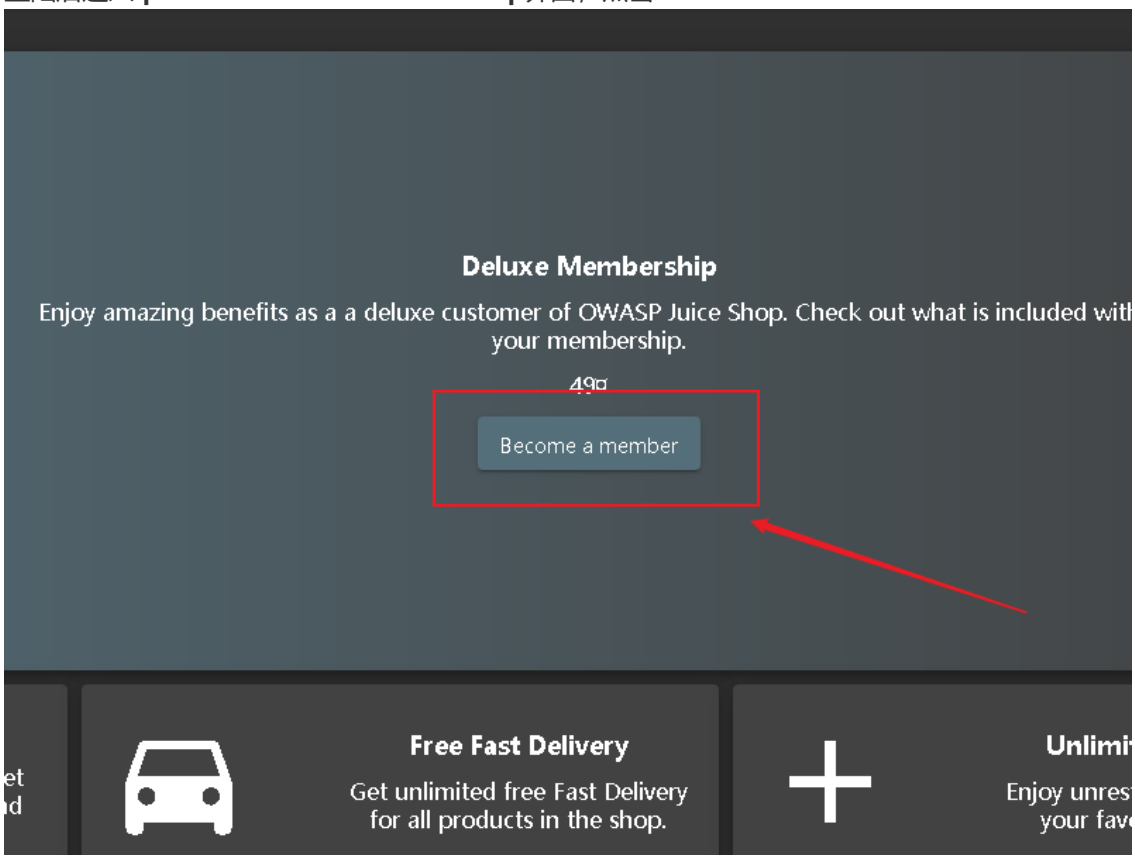
4. admin registration挑战成功

deluxe fraud

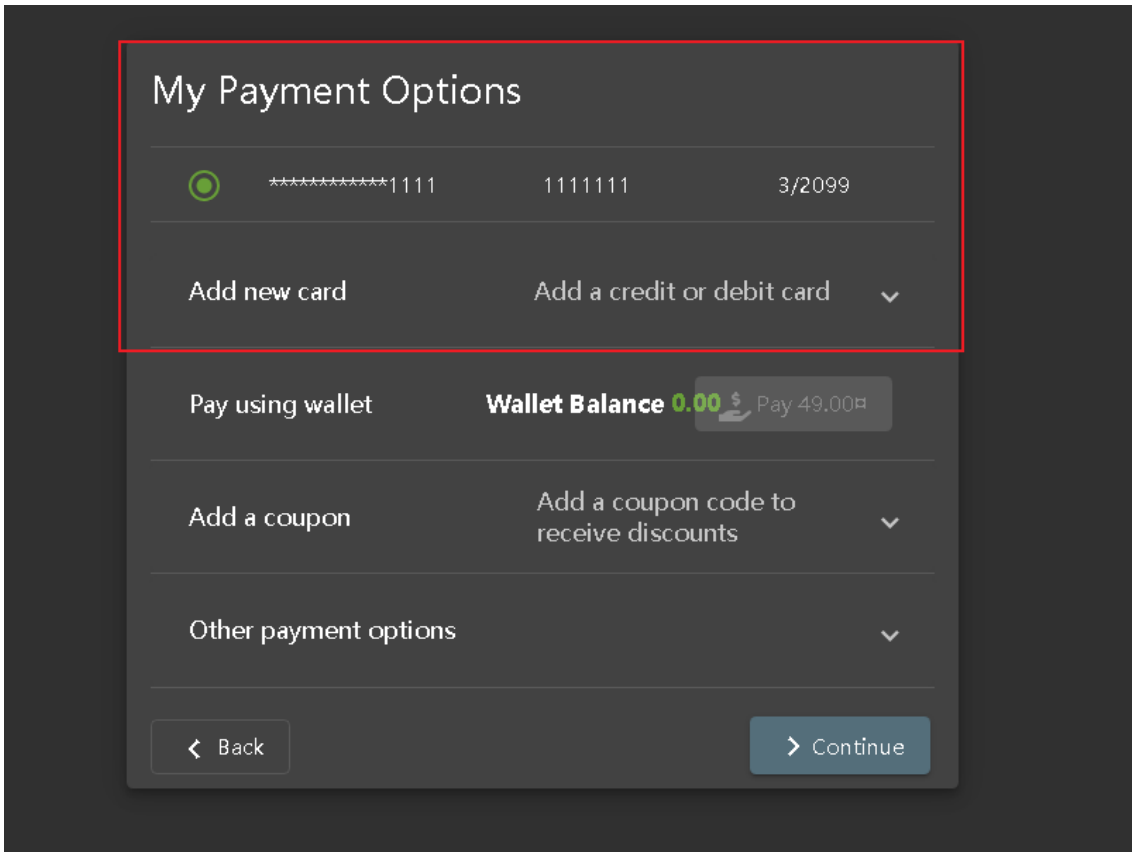
1. 打开**ip:3000/#/register**，任意注册账号，并登陆



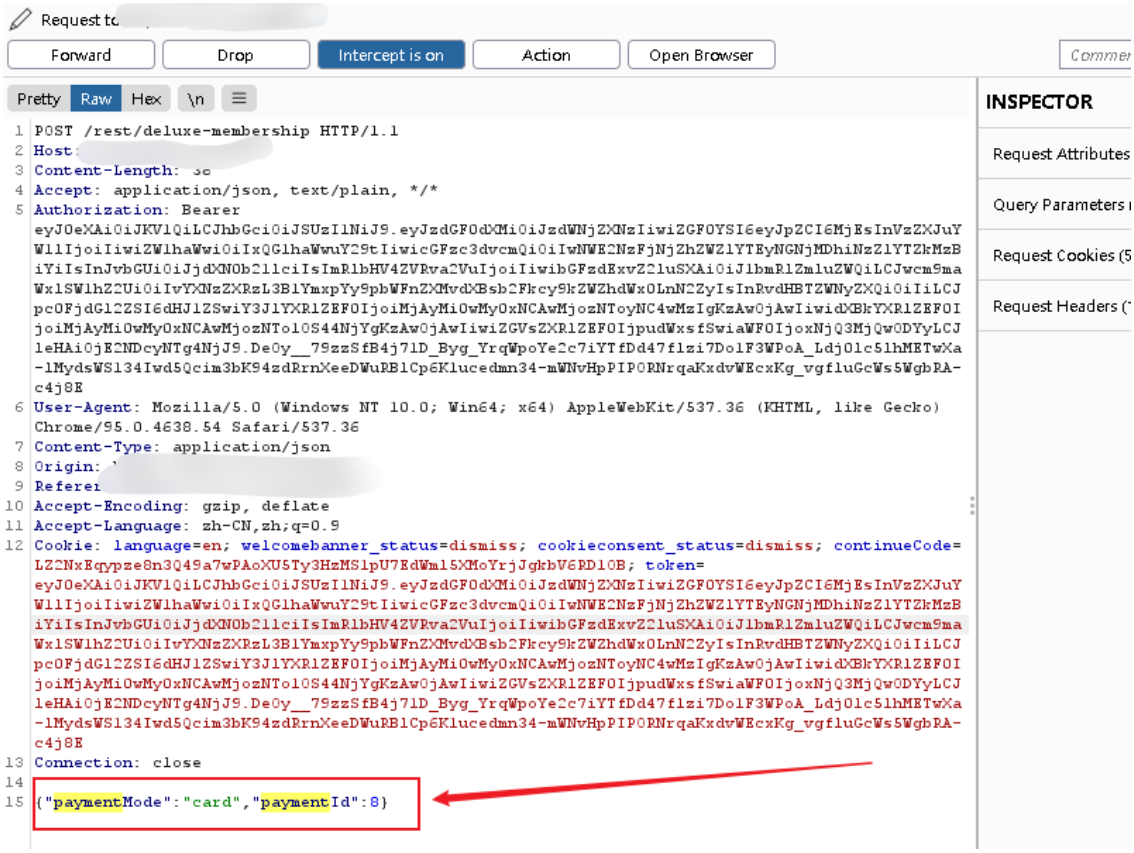
2. 登陆后进入**ip:3000/#/deluxe-membership**界面，点击Become a member



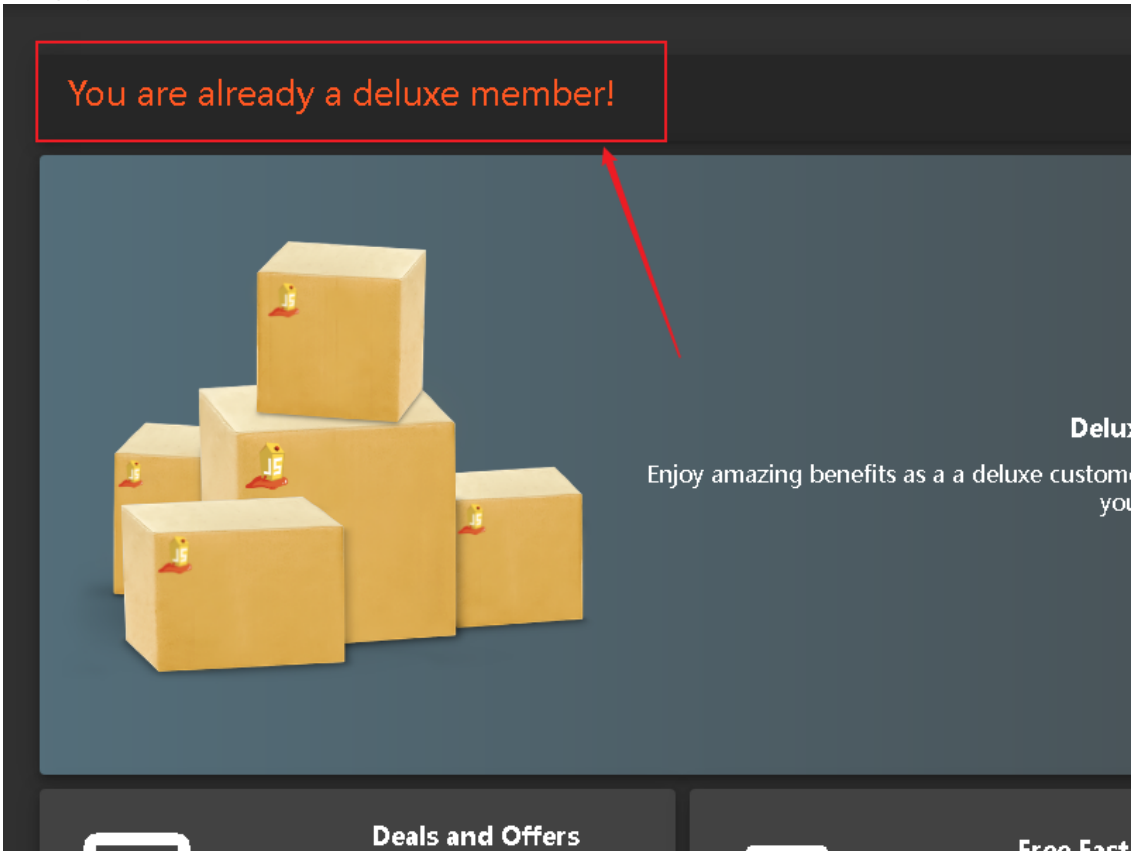
3. 在Add new card处添加任意卡信息



4. 开启代理，点击Continue抓取提交信息



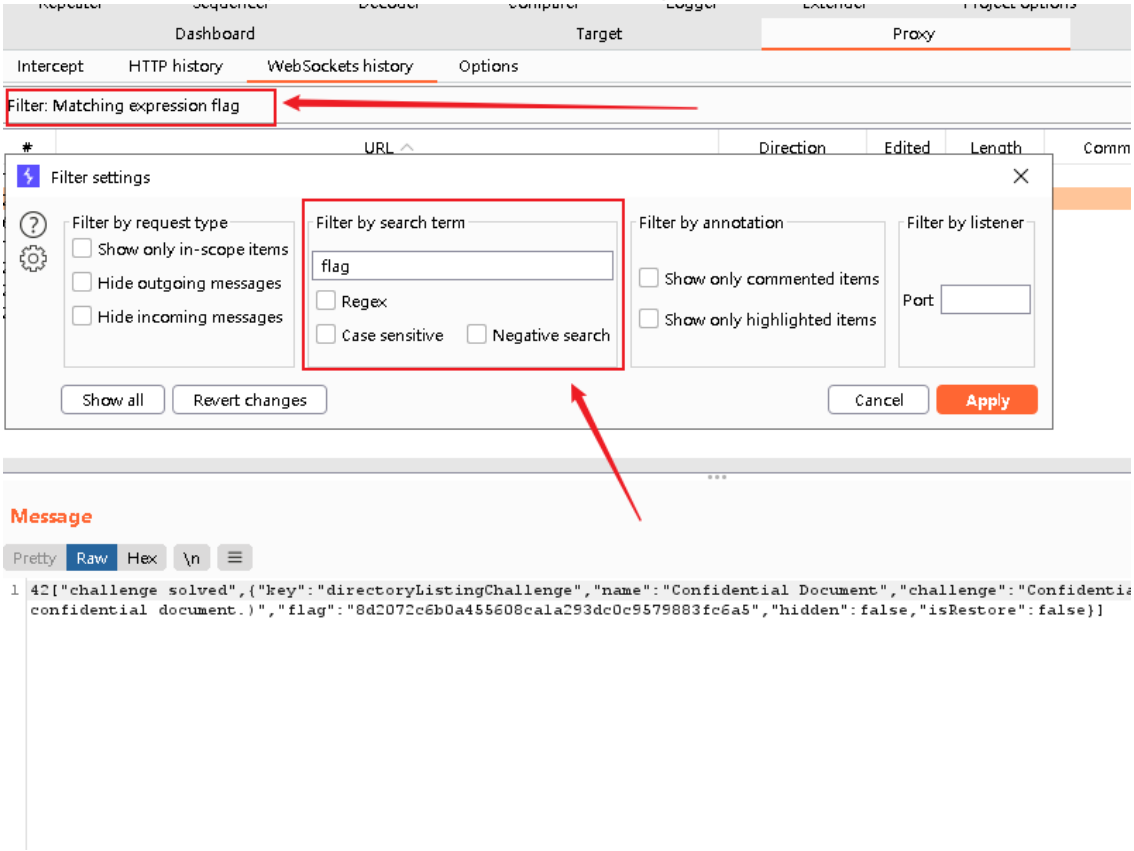
5. 更改paymentMode数据的值为none，点击Forward发送数据包



6. deluxe fraud挑战成功

找到flag

1. 打开WebSocket history，点击Filter，配置搜索内容为flag



2. 搜索出历史响应的flag值