# 短信轰炸(两处，注册、重置密码)

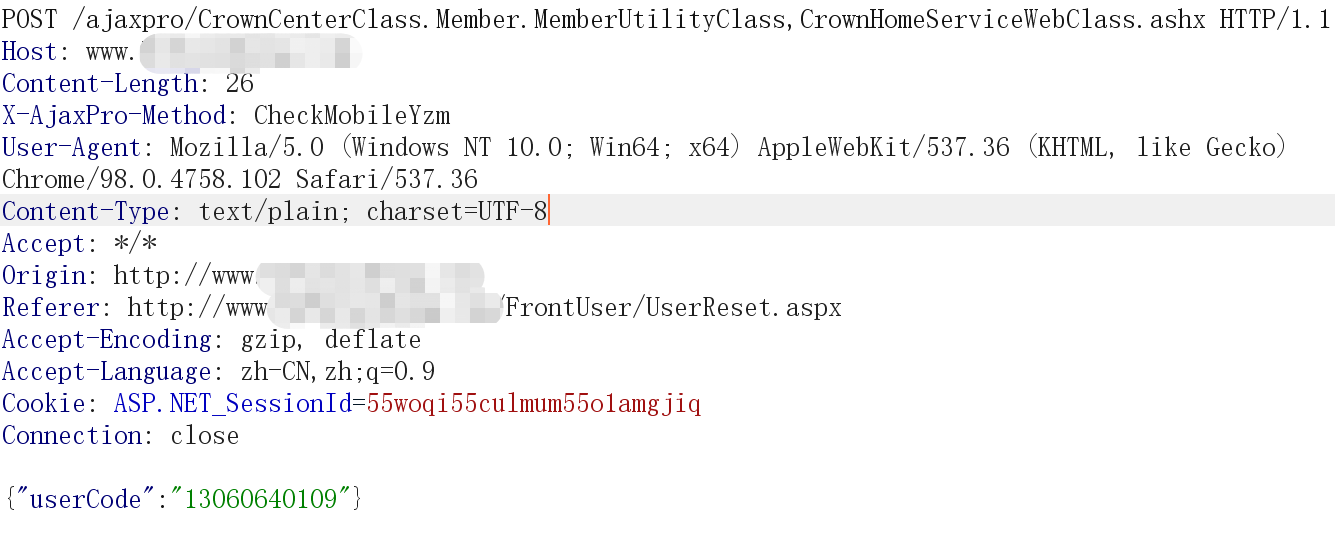
①漏洞url:http://www.example.com/FrontUser/UserRegister.aspx 注册账号处

输入手机号码，不断重放数据包，经测试无次数限制



②漏洞url:http://www.example.com/FrontUser/UserReset.aspx 密码重置处

输入手机号码，然后进行抓包，然后进行重放数据包



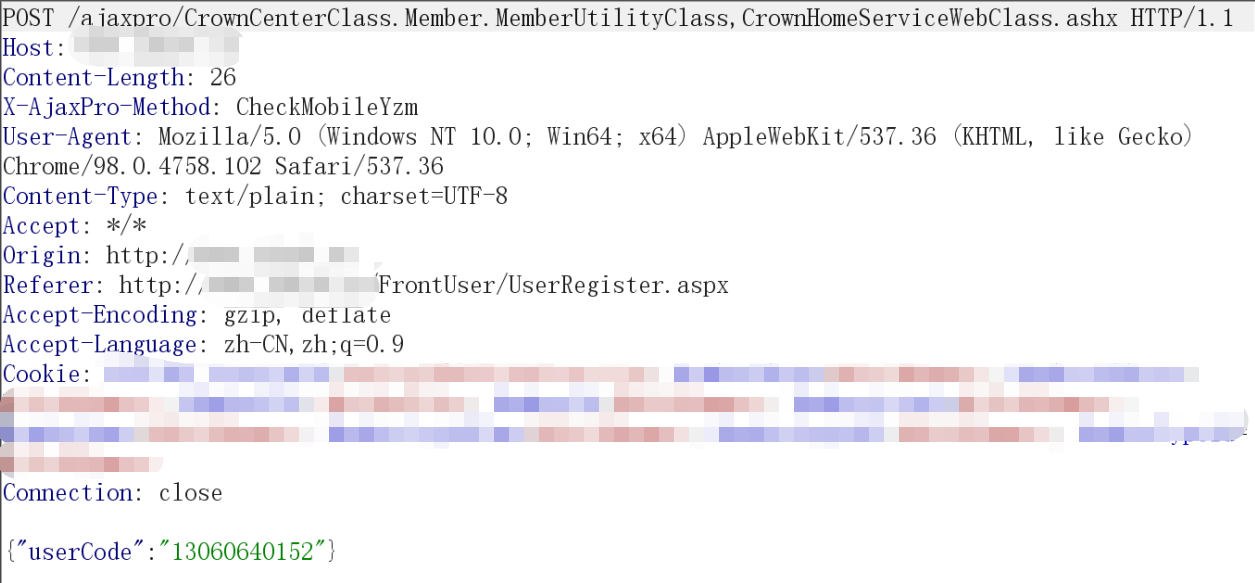


输入手机号码，不断重放数据包，经测试无次数限制

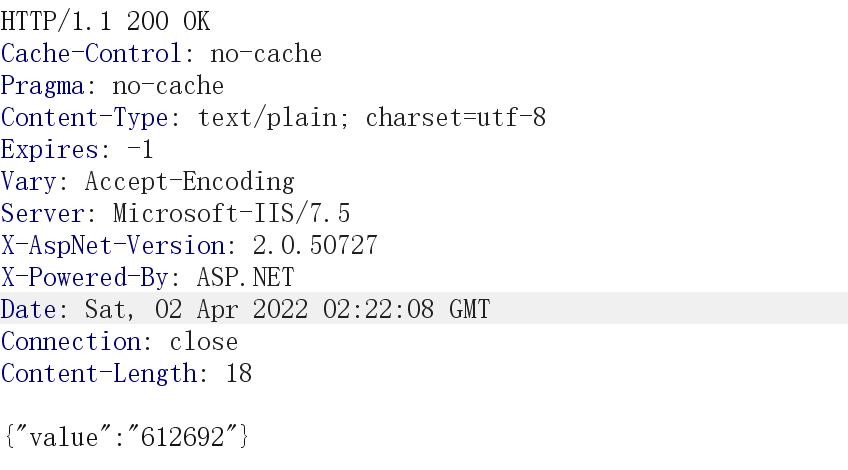
# 任意用户注册

原因：因为验证码直接回显到数据包中

请求包：



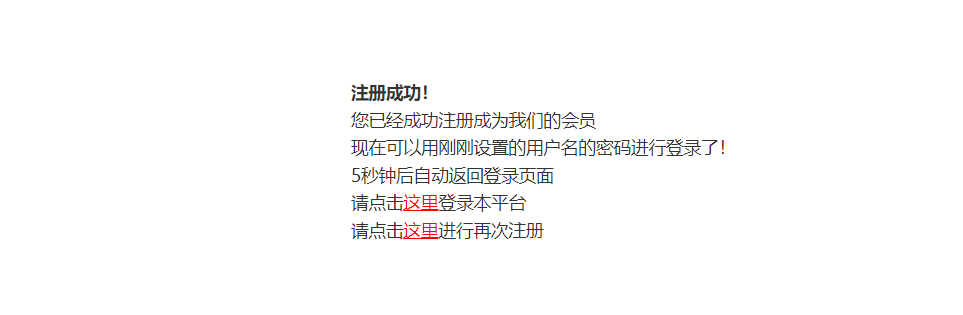
响应包：



知道该值为验证码是因为用自己的手机号收取的验证码即为响应的value值,该账号为任意输入的账号



注册成功

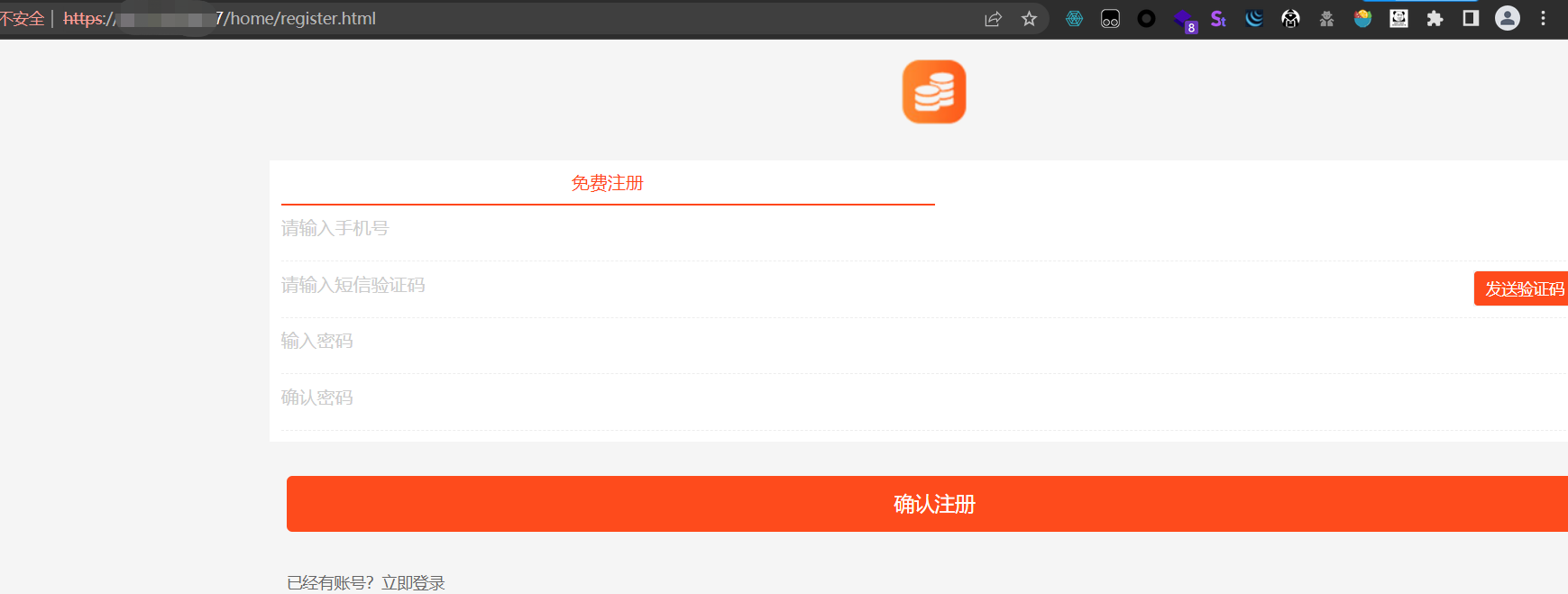


# 区别于验证码回显的任意用户注册

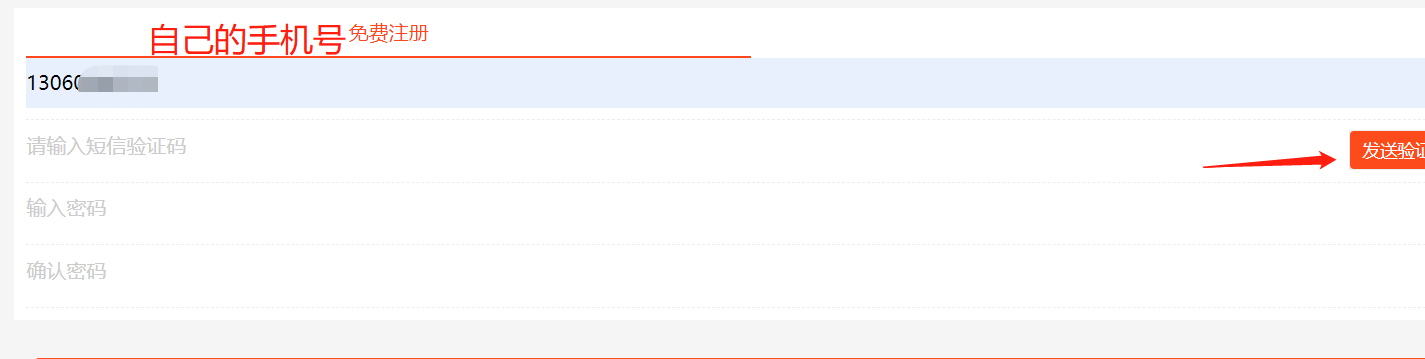
原因：只验证下发的验证码是否正确，而没有将手机号与验证码做临时绑定关系，导致在提交的刹那，注册别的账号

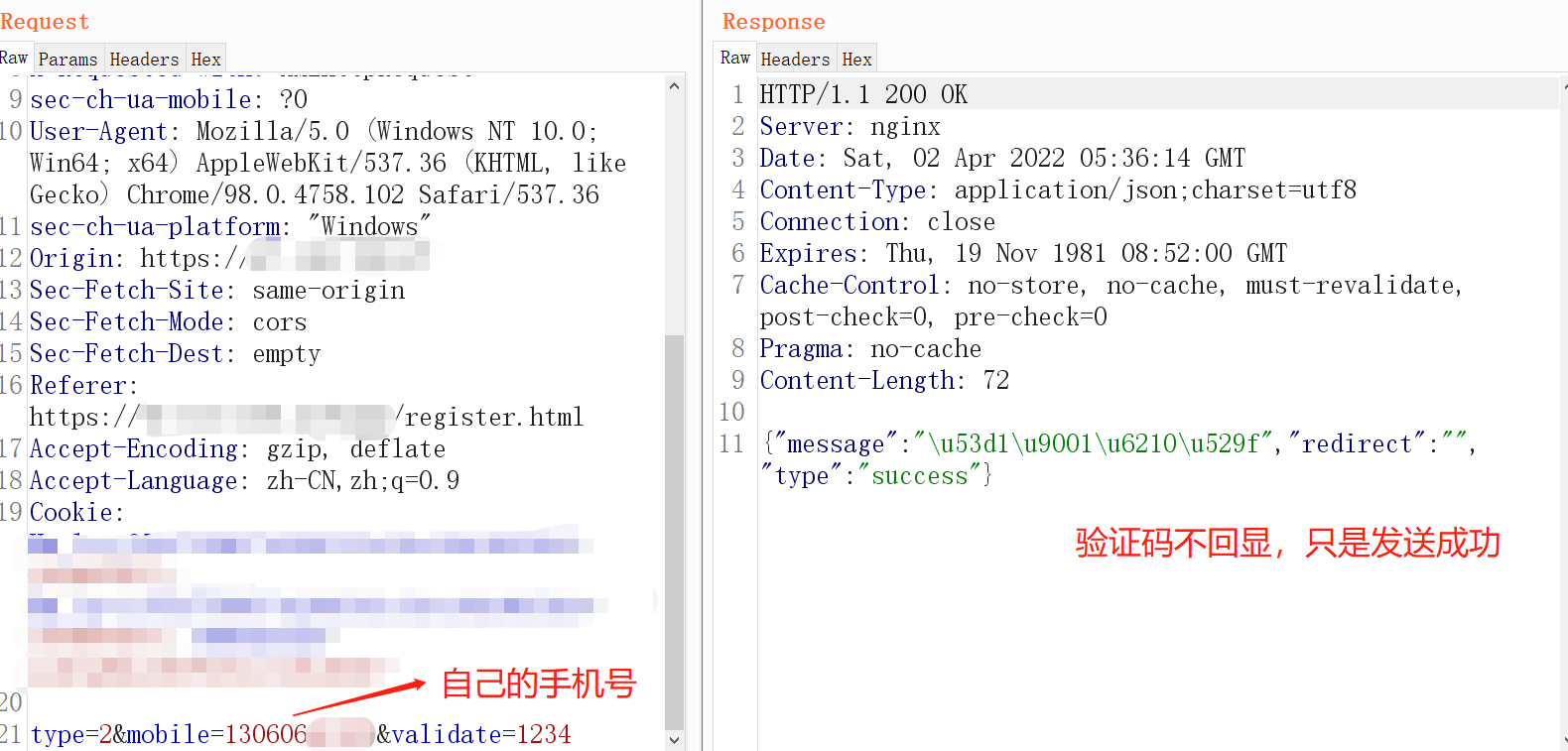
大多数注册不会在响应包中显示验证码，那么就没有了嘛，当然不是，还是得测试

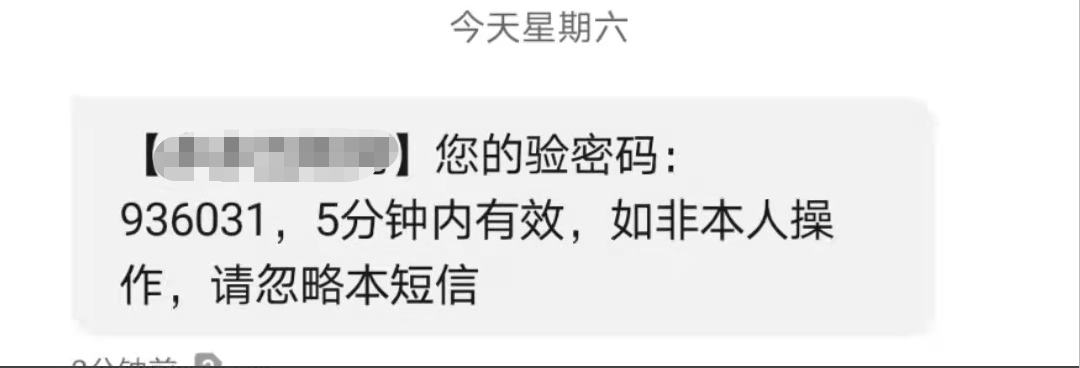
这是另外一个网站



发送验证码



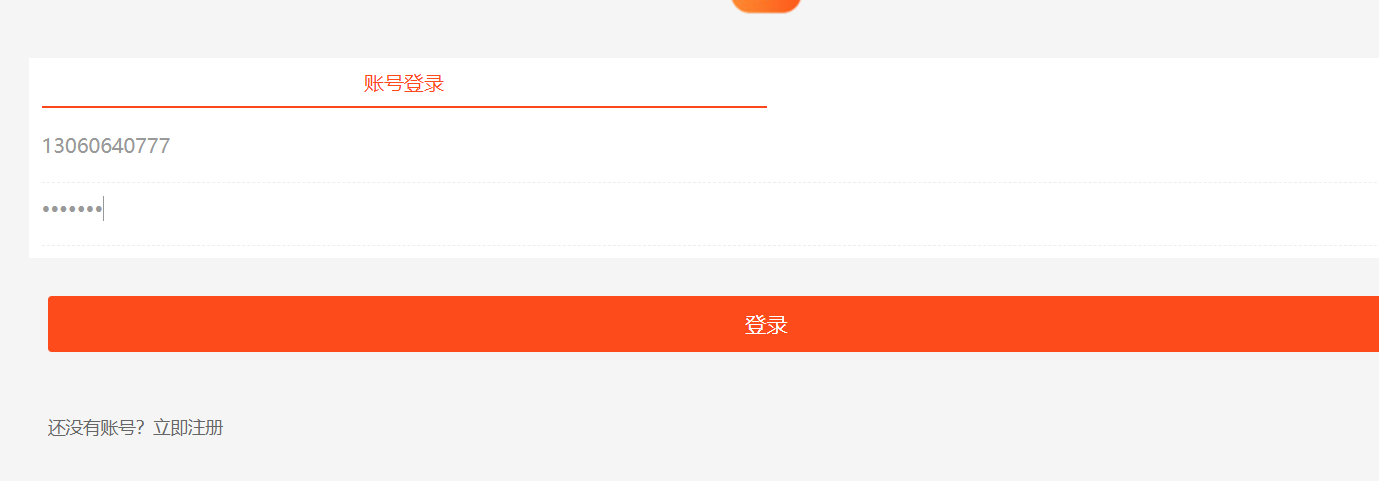














# 任意用户密码重置

回到上一个网站的密码重置功能

原因：和上面一样，验证码回显

使用号码18888888888



然后重定向到登录，答案是登录不了，因为虽然可能有这个漏洞，但是原本这个手机号本来就没注册过，因此尝试重置上面的账号13060640152



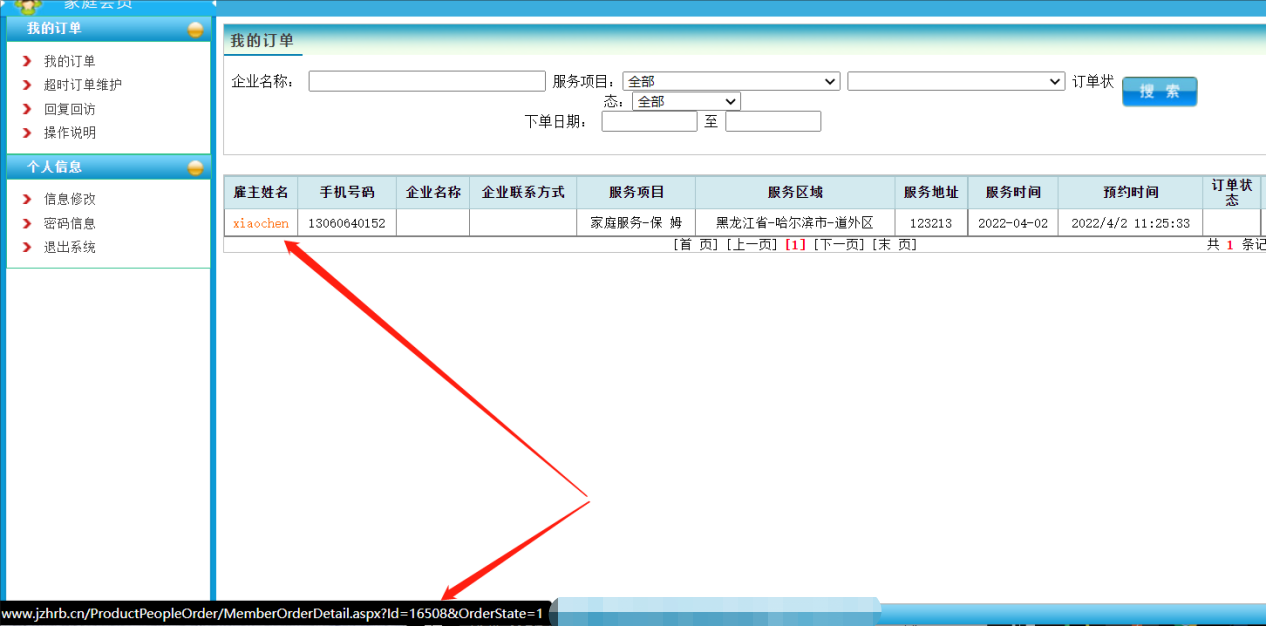
原来为Wasd6050 现在修改为wasdwasd6050

再次登陆

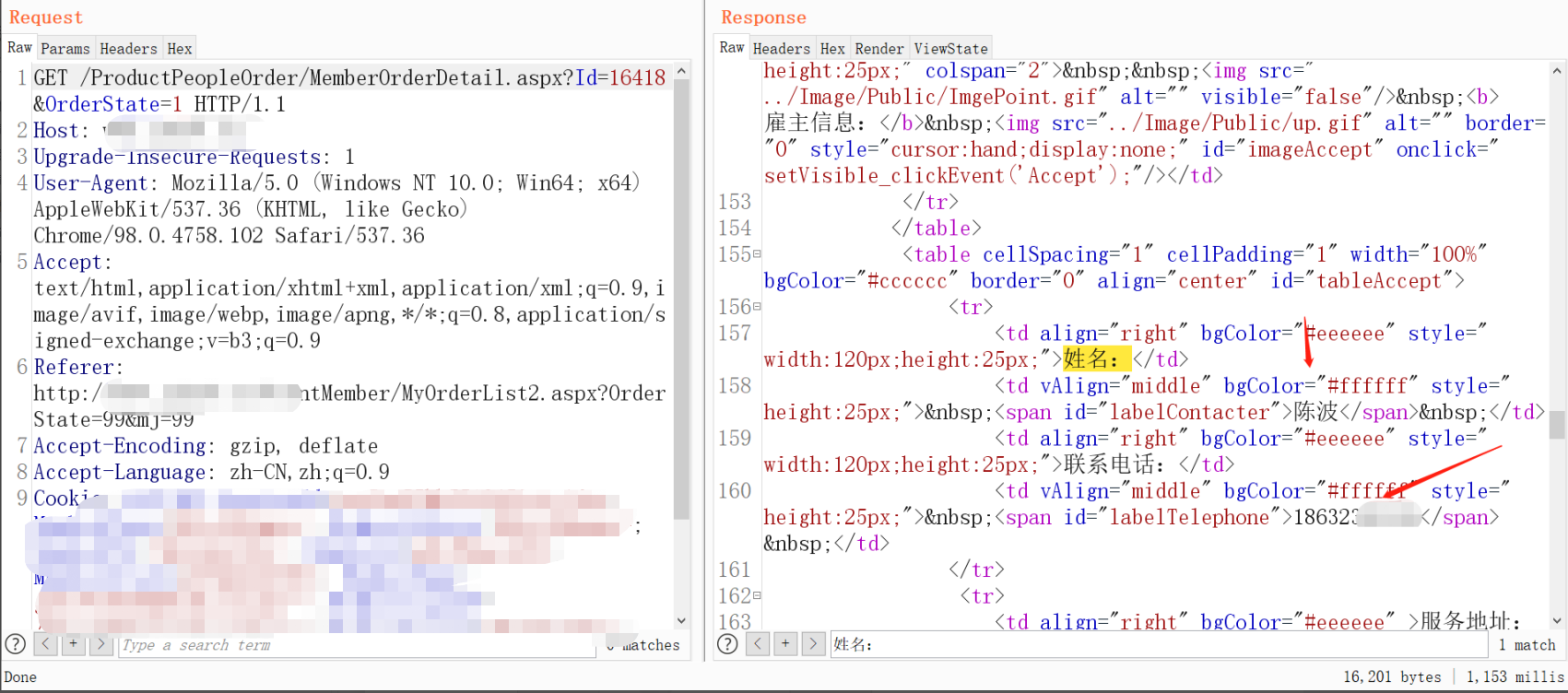


# 越权查看订单信息

观察a标签的url地址，点击抓包



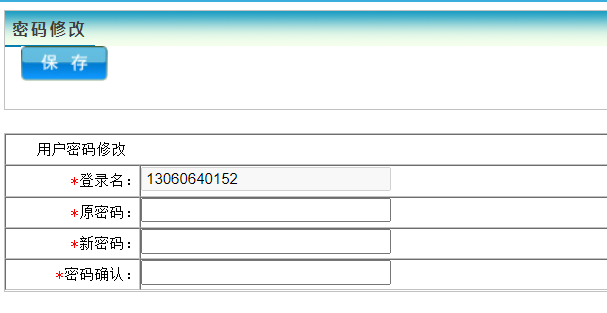
通过修改id值，可以水平越权查看他人的订单详细信息





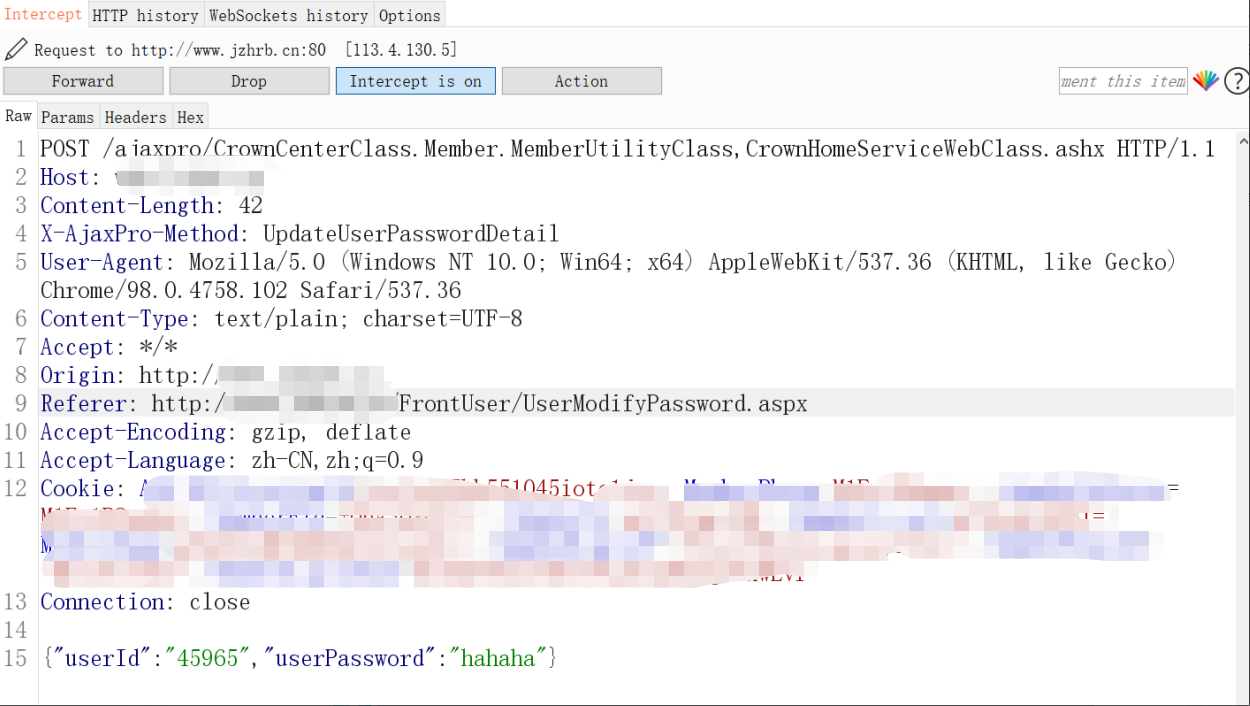
# 后台任意密码修改

原因：修改密码的包分两次发的，第一步是确定原密码是否正确，第二个包是真正修改的包，那么存在逻辑漏洞，第一步输入当前账号的旧密码，通过后第二个包对其他账号进行密码修改



第一个包，直接发出去





第二个包的userid参数需要进行修改，知道了另一个账号的userid为45964（不知道情况下遍历）

修改成功后重新登陆 13060640108的userid为45964，而该账号成功使用被越权修改的密码hahaha成功登录系统



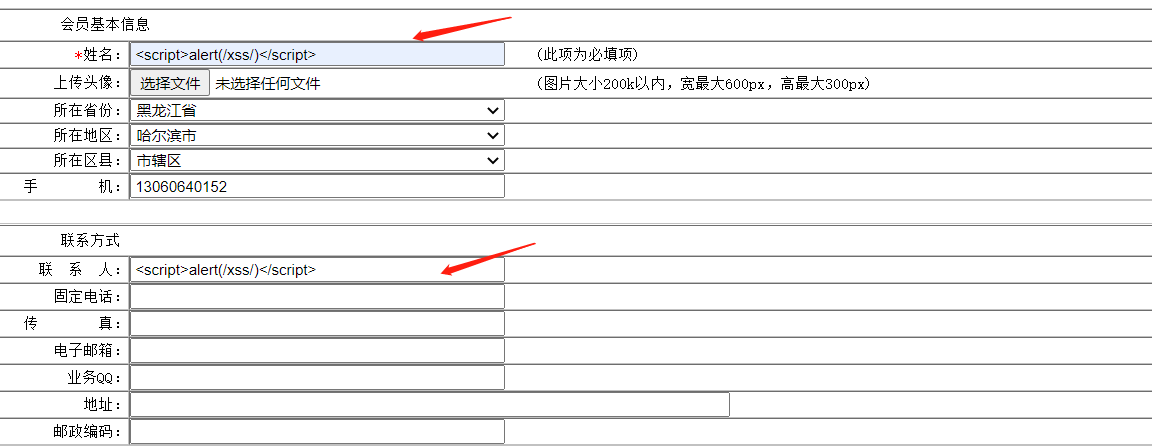
# 会话固定

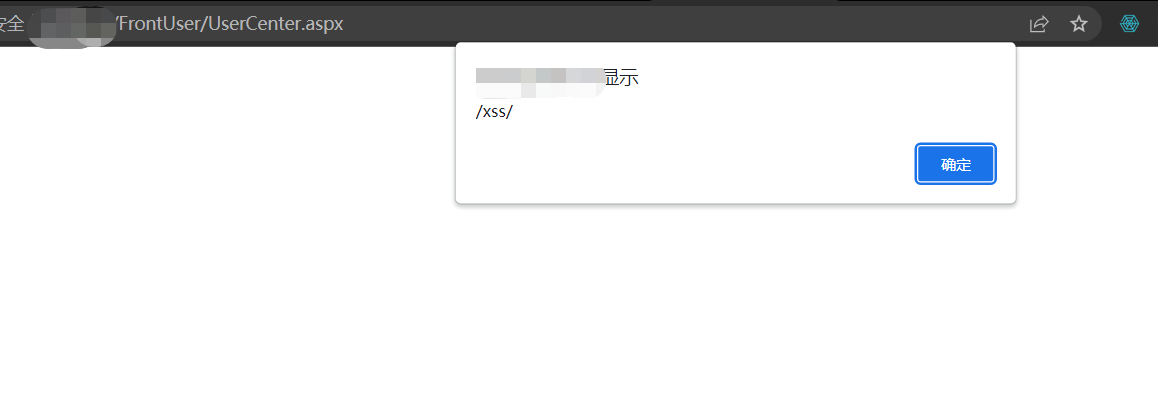
该系统还存在一个问题，修改密码后不会自动跳转到登陆，需要手动退出....

# 其他漏洞：

## Xss(基本资料两处xss)

由于会话固定的原因，重新登陆





后台功能比较少，功能多的情况下，更多测试的点