# 有道精品课堂支付处生成二维码存在任意URL跳转

漏洞类型:逻辑漏洞

漏洞等级(自评): 低危

漏洞URL: <https://ke.youdao.com/user/order/>

漏洞概述:

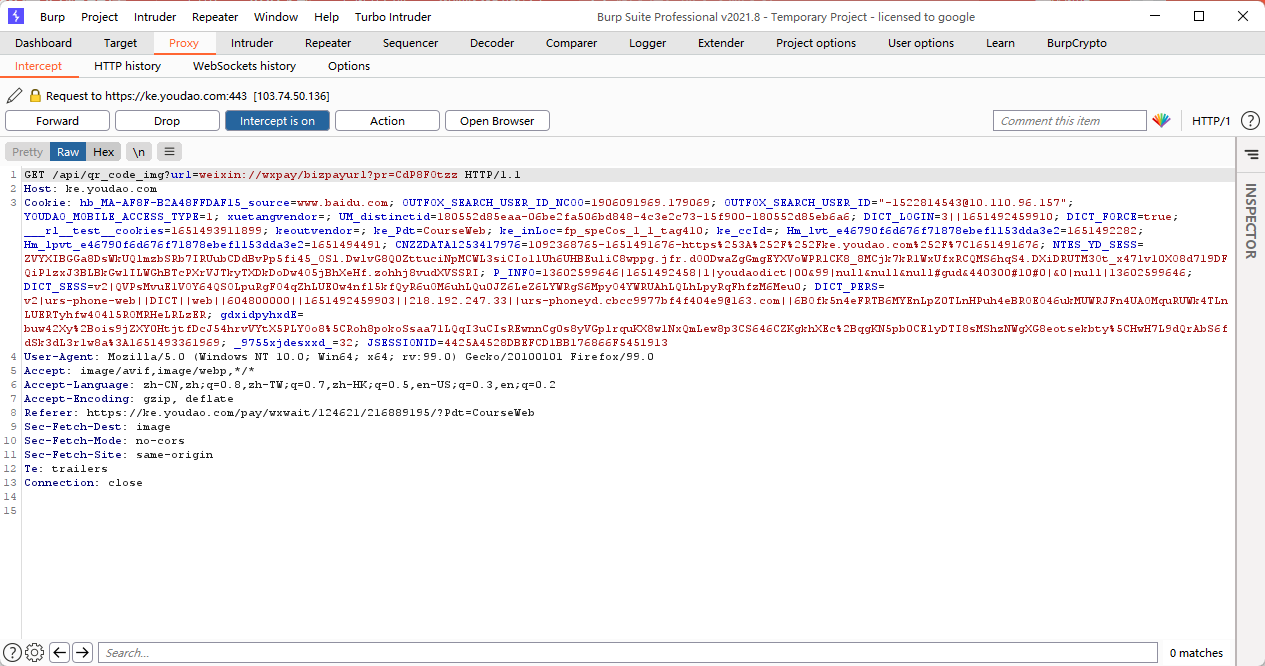
在有道精品课堂购买一门课程,但是不支付,退出界面,访问我的订单,点击继续支付会生成一个二维码,可以通过抓包更改二维码的内容.二维码可以改成任意URL,造成任意URL跳转.

漏洞复现:

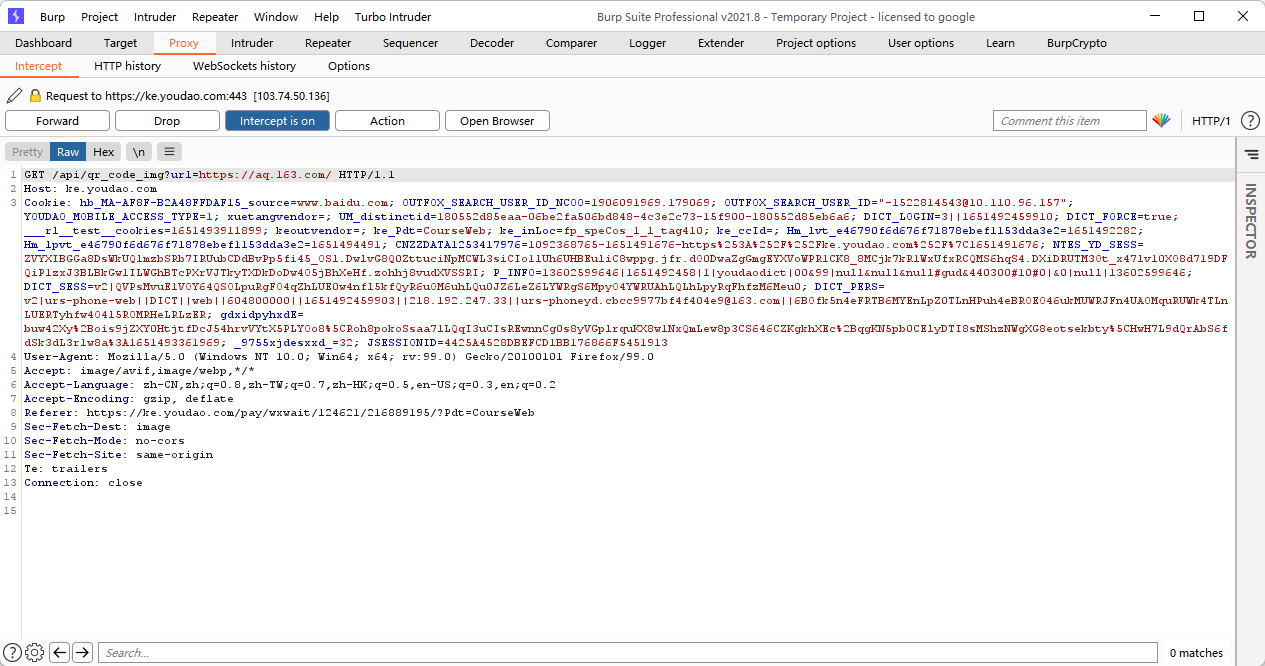
首先访问有道精品课堂的主页,随便选一门课订购,但是不支付退出支付界面,然后访问URL: <https://ke.youdao.com/user/order/>



点击继续支付,并开启burp suite进行数据包截获



在这个URL这里停下,发现一个URL参数,这里可以更改成任意URL,实现任意URL跳转的操作,这里我们已<https://aq.163.com/>为例子



修改放包后,截图生成的二维码,切换微信扫描



发现跳转到<https://aq.163.com/>即存在任意URL跳转