

抓包看，发现生成订单路径

```

1 GET /cs
   luaqzH
   gdaWyz
   ug0it2+
   -----
       apocde?jt=
       J16wo3#2528ojJy#2528B6ULZsqLlk8ZuOaWI4jF100)
       P1uudFAOw/A#2528oIvzMcoBmncFMwF181VUpuh3U2)
       Htg7oEtgH3#2528FUqhIFBX/CMeD#2528FR4BTYlM1bCT-
       .Ma
       'I:
       [3]
       :=f
       10
       %x: {
           ex
           l,
           },
           "data":{
               "qr_code":"19YU9qm",
               "qr_url":"https://\wenen
                   oe\19YU9qm"
           }
       )

```

 支付助手

04:39

付款成功

¥ 9.00

付款方式

交易对象

商品说明

本次奖励

取

付款后会自动签约自动续费，先取消自动续费

 解约成功通知

04:42 ...

解约成功

解约商户

解约项目

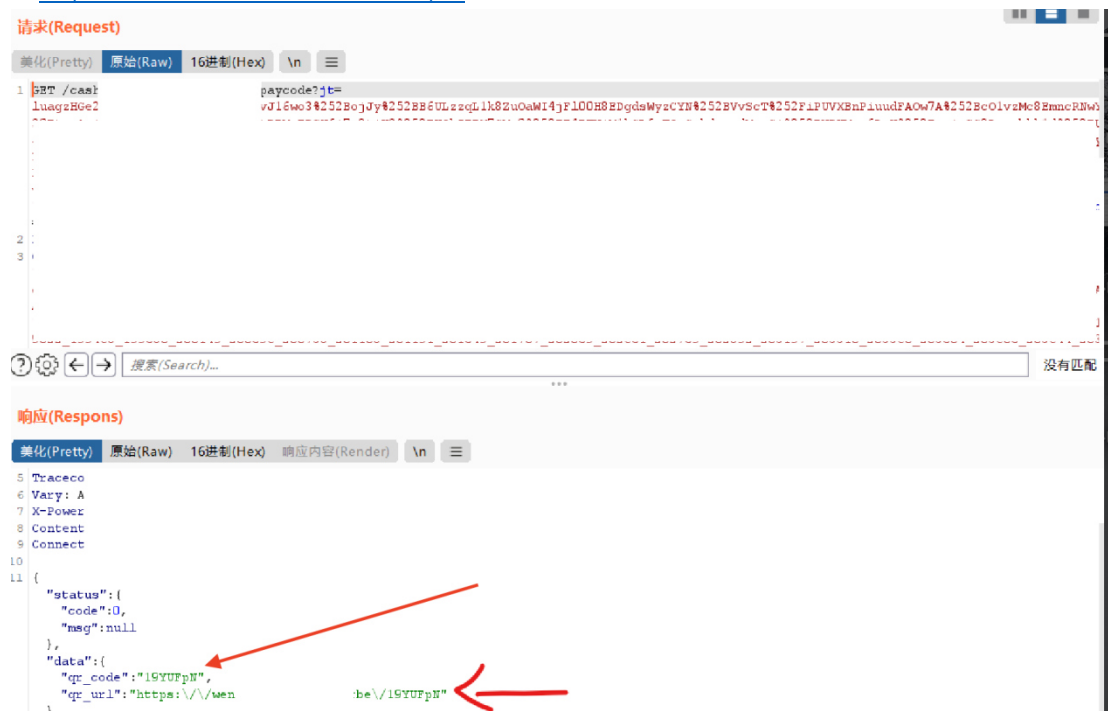
备注 点击消息即可查看服务详情

查看详情 >

查看 vip 到期时间, 现在是 2022-04-12



将上述数据包发送到 burp 的 repeater 模块, 重放数据包得到另外一个支付地址
(<https://xxx.xxx.com/xxrbe/19YUFpN>)



用手机打开该支付路径

¥9.00

开通服务账号

开通服务内容

自动扣款方式

立即支付并开通

依然能支付成功

✓

支付成功，开通扣款成功

开通服务账号

开通服务内容

本次支付金额

自动扣款方式

服务开通时间

并且 vip 天数用之前的 4 月 12 日变为 5 月 12 日



因为该优惠是集合包，相对应的其他月卡也依然会有，如下面的首汽约车月卡

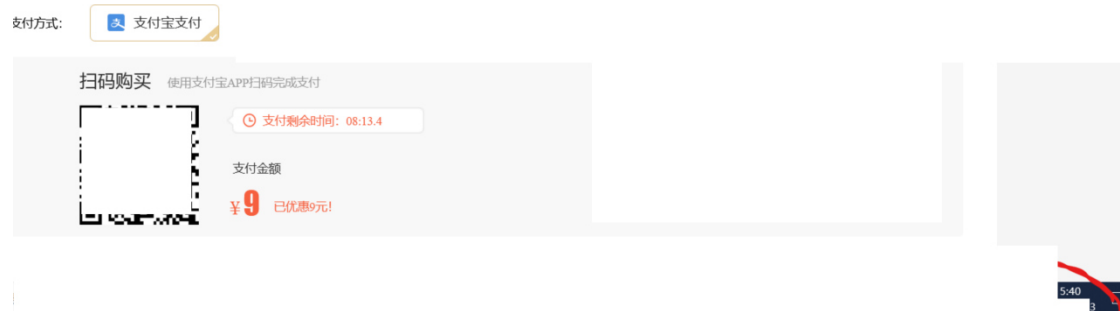


经过实验得出数据包可以一直使用, 只需要每次将自动续费关闭, 就可以一直享受这个福利, 并且经过观察生成的支付路径, 可以看出来只是最后的 6 位不一样, 所以猜想还可以通过爆破路径而不需要重放数据包来获取路径。

因为我开始点进去该活动的时候应该是多生成了一个订单, 再去我的订单里查看时发现有两个订单 (没截图, 后面点我的订单进不去了)。最后发现, 只要不付款, 可以一直创建订单, 并且订单编号也不一样。下面这个为我第一个创建的订单, 我付款是付了第二个订单。



并且我一直没刷新支付页面, 发现只需在该页面刷新二维码依然可以购买



而将该链接复制去另外一个页面后发现 9 元的活动消失了。但是依然可以通过生成支付地址的方式进行支付刷 vip，最后我也就付款了两个，来证明漏洞存在，并且证明了 **vip 时间可以叠加**

最后得出只要不退出活动页面或者不支付就可以无限创建订单，并且 vip 时间可以一直叠加。