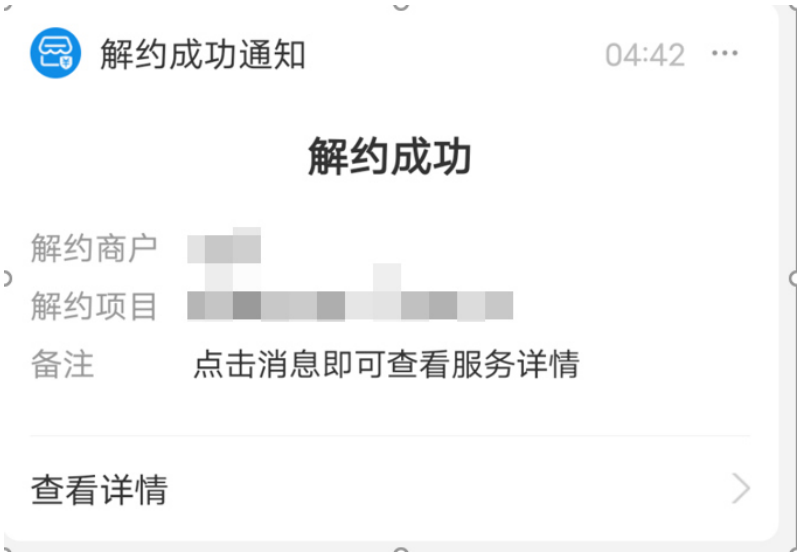
漏洞 url：
https://xxxxxxxx/

仅限一次购买（表面上）
抓包看，发现生成订单路径

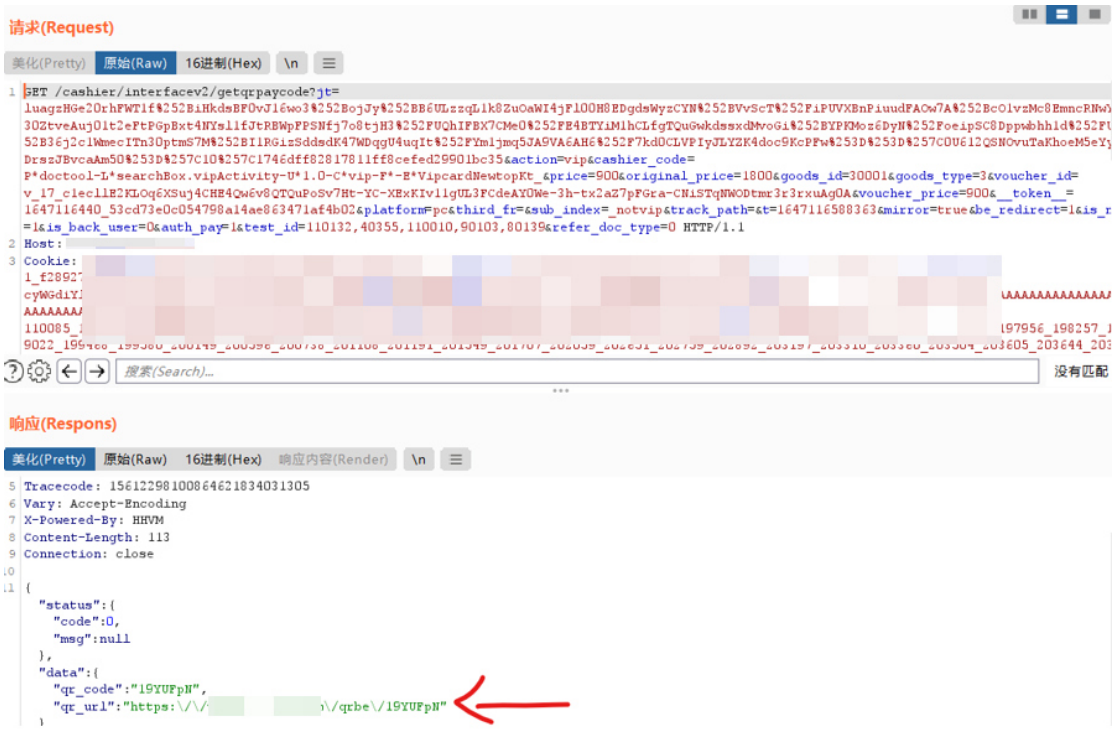
这是订单路径：https://xxxxxxx/qrbe/19YU9qM

付款后会自动签约自动续费，先取消自动续费



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://xxxxx/qrbe/19YUFpN）



用手机打开该支付路径

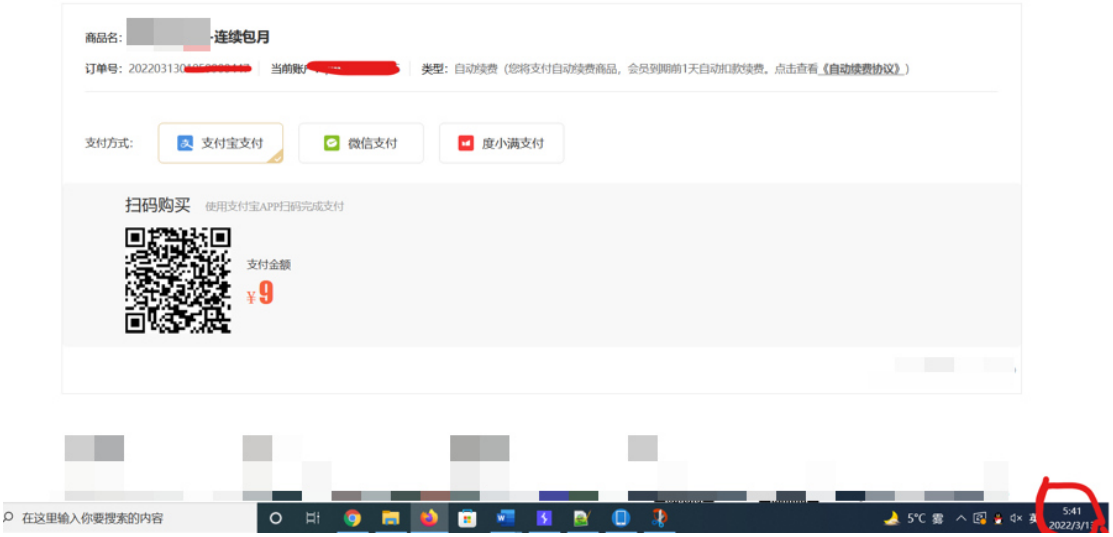
依然能支付成功

并且 vip 天数用之前的 4 月 12 日变为 5 月 12 日

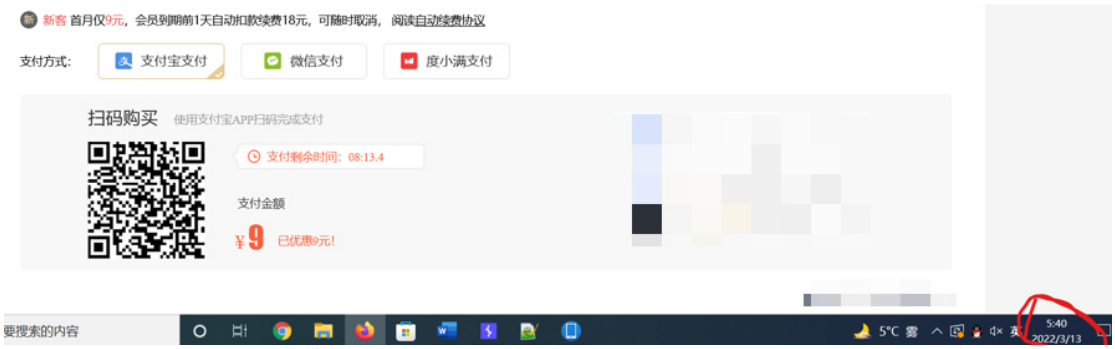
因为该优惠是集合包，相对应的其他月卡也依然会有，如下面的首汽约车月卡

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去进行支付刷 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**

最后也发现是由该链接生成的支付地址

https://xxxxxxx/cashier/interfacev2/getqrpaycode?jt=luagzHGe20rhFWT1f%252BiHkdsBF0vJ16wo3%252BojJy%252BB6ULzzqL1k8ZuOaWI4jFI00H8EDgdsWyzCYN%252BVvScT%252FiPUVXBnPiuudFAOw7A%252BcO1vzMc8EmncRNwY18iVUpuh30ZtveAuj01t2eFtPGpBxt4NYsI1fJtRBWpFPSNfj7o8tjH3%252FUQhIFBX7CMe0%252FE4BTYiM1hCLfgTQuGwkdssxdMvoGi%252BYPKMoz6DyN%252FoeipSC8Dppwbhh1d%252FU6GJhJe%252B36j2c1WmeclTn30ptmS7M%252BI1RGizSddsdK47WDqgU4uqIt%252FYm1jmq5JA9VA6AH6%252F7kd0CLVPIyJLYZK4doc9KcPFw%253D%253D%257C0U612QSNOvuTaKhoeM5eYyWY2ztz1RDrszJBvcaAm50%253D%257C10%257C1746dff82817811ff8cefed29901bc35&action=vip&cashier_code=P*doctool-L*searchBox.vipActivity-U*1.0-C*vip-F*-E*VipcardNewtopKt_&price=900&original_price=1800&goods_id=30001&goods_type=3&voucher_id=v_17_c1eclIE2KLOq6XSuj4CHE4Qw6v8QTQuPoSv7Ht-YC-XExKlv11gUL3FCdeAY0We-3h-tx2aZ7pFGra-CNiSTqNWODtmr3r3rxuAg0A&voucher_price=900&__token__=1647116440_53cd73e0c054798a14ae863471af4b02&platform=pc&third_fr=&sub_index=_notvip&track_path=&t=1647116588363&mirror=true&be_redirect=1&is_new_user=1&is_back_user=0&auth_pay=1&test_id=110132,40355,110010,90103,80139&refer_doc_type=0

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。