## 限制购买逻辑漏洞

1. 漏洞描述：

很多厂商都会搞一些活动，在享受优惠的时候，会标上用户只能购买一次或者只能充值一次vip的条件，但是这种地方也是会有漏洞产生的，就是程序员在开发的时候会忽悠掉用户 可以在不支付前多次创建订单还突破这个限制。

#### 2.漏洞测试工具：

**1.浏览器多开窗口**或**一个浏览器是pc端一个浏览器设置为手机端来进行测试**

**2.burp抓第一次订单的包，试试是否可以无限支付，导致时间累加**

**测试环境：**

**标有仅限购买1台或者首单优惠这样的地方**

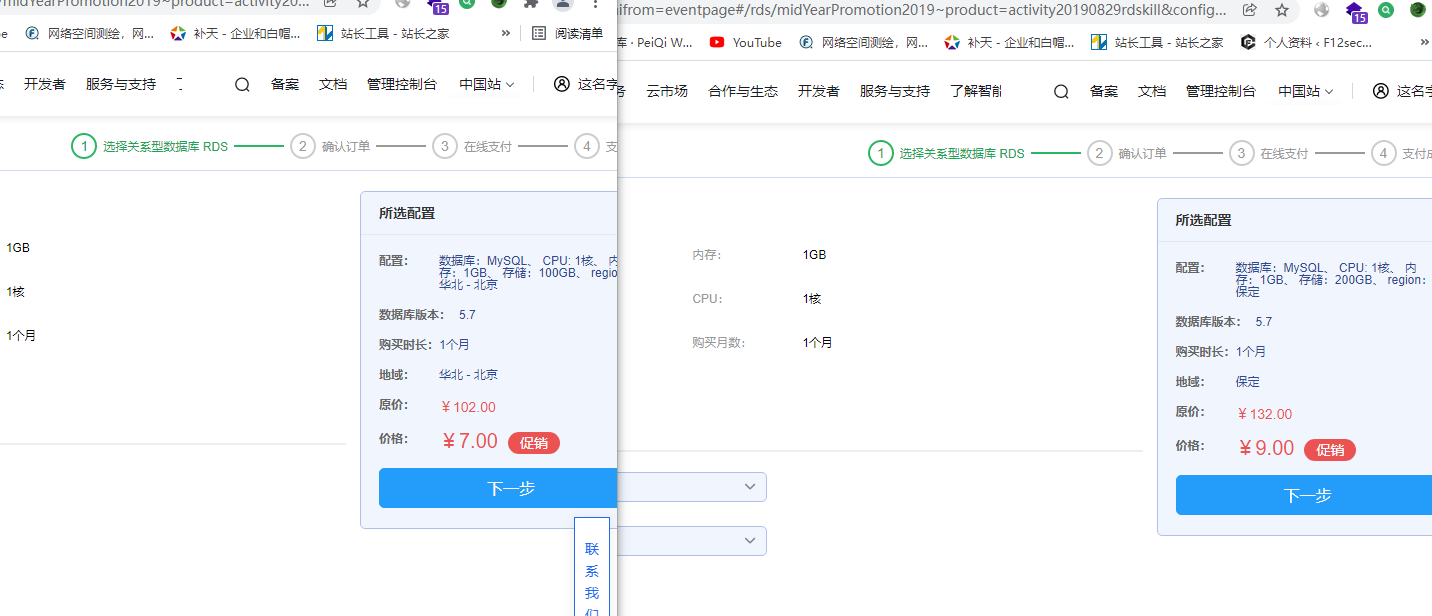
#### 3.案例 ：

百度智能云活动中对学生的优惠，就是学生可以特价购买一台服务器

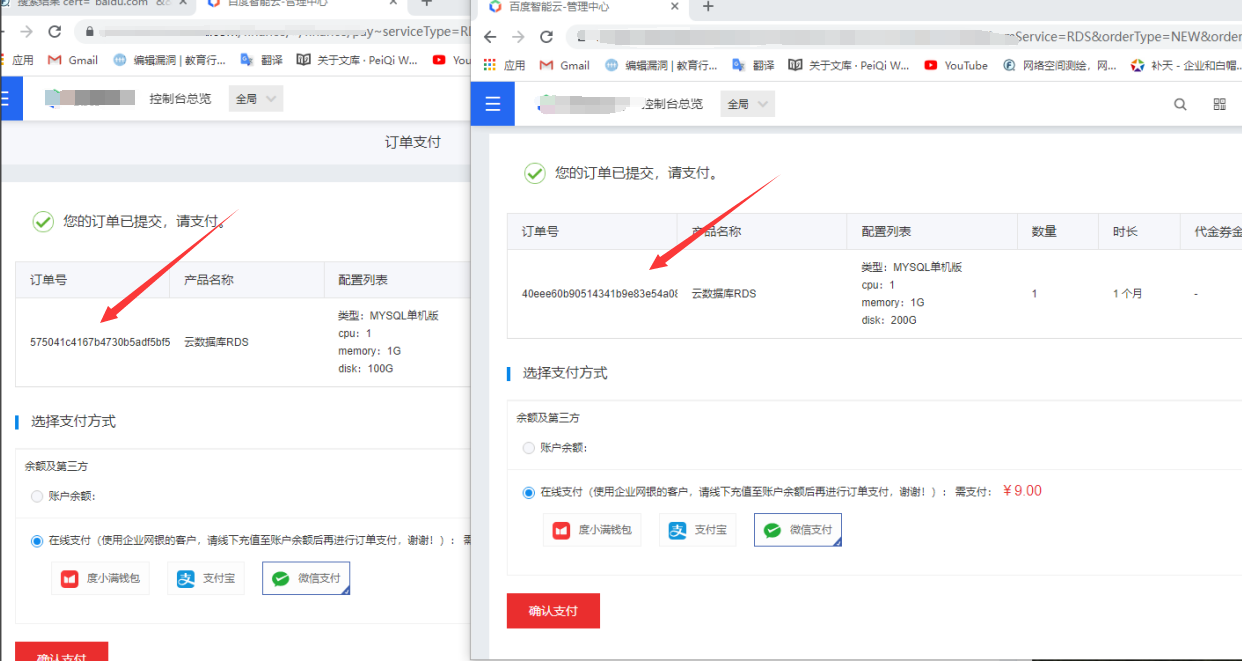
登录后访问活动页：



此页面选择不同的配置同时创建订单（只要不要付款，可以无限创建账单而且成功购买，复现时只购买了两个）下图是新账号复现，所以订单有所不同

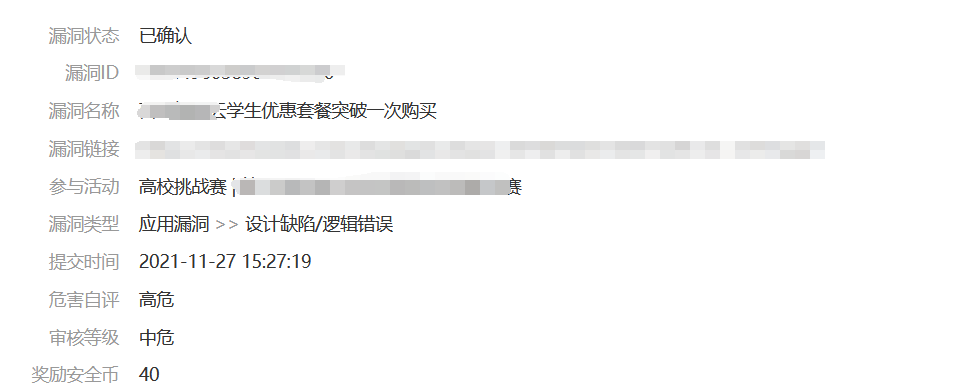


**创建后可以明显发现订单号不同：**



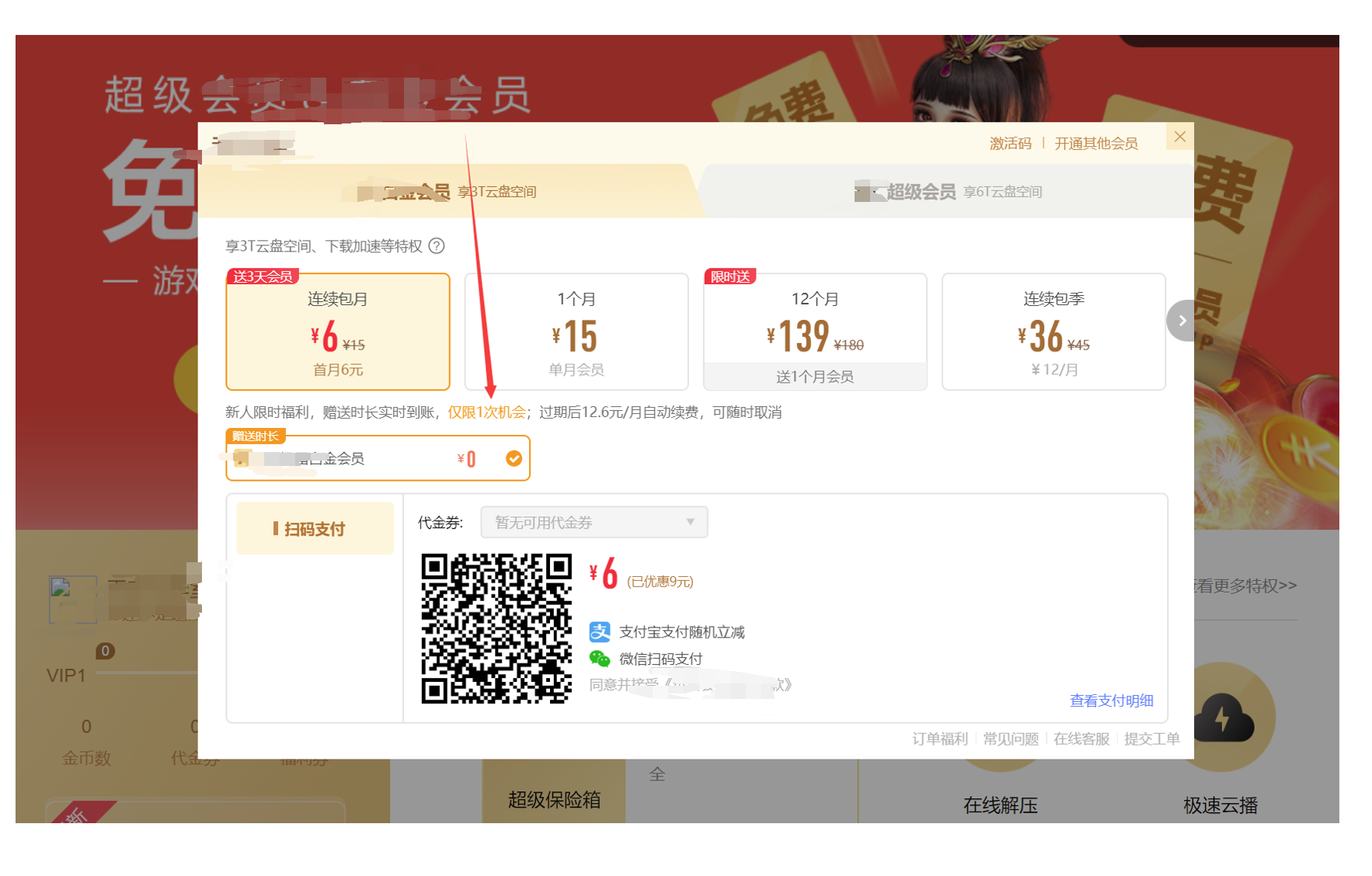


此漏洞是因为服务器时间不可叠加，故业务src给的中危 40币，如果时间可以叠加，则稳稳的高危

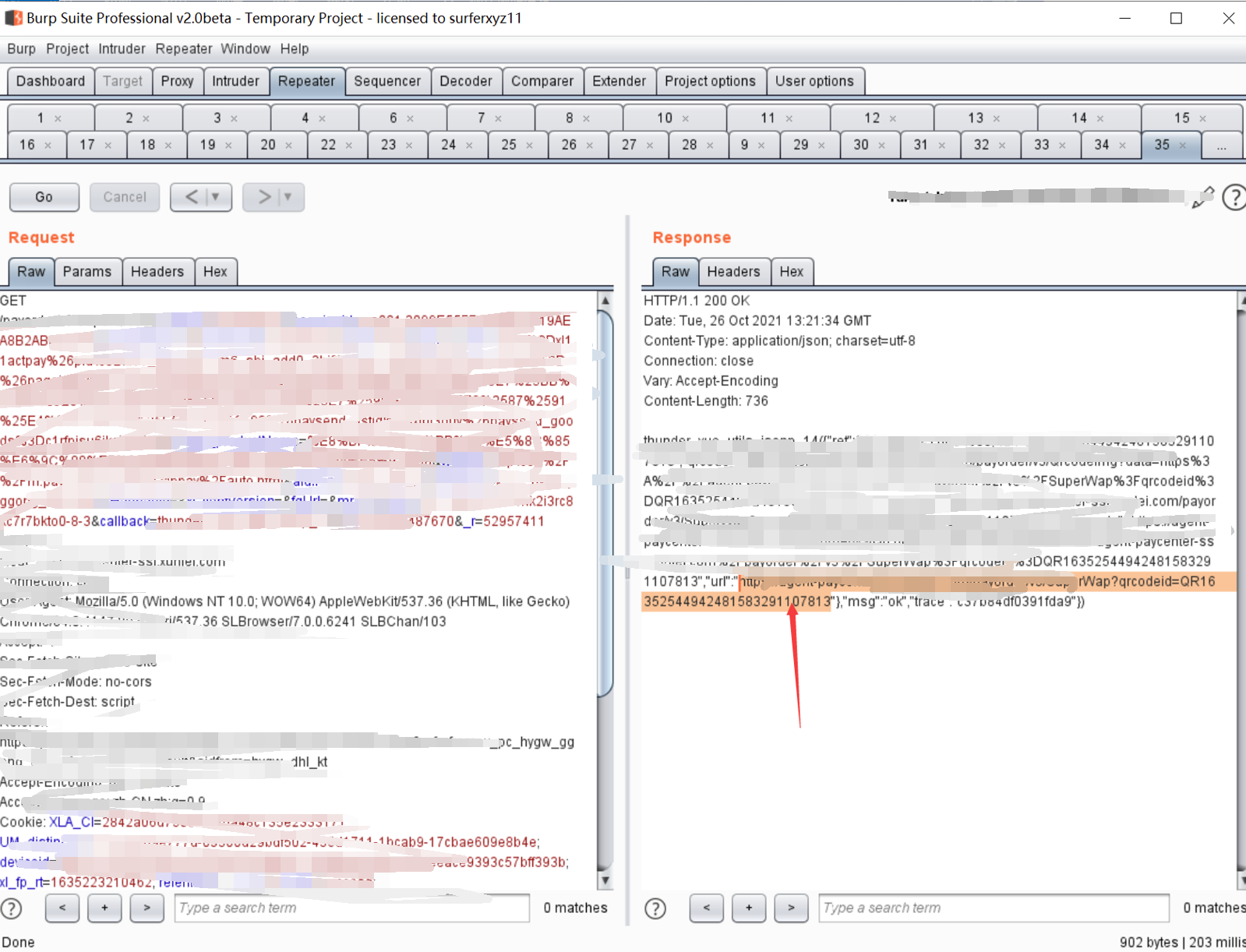


第二个案例：（此案例在我们的免费web星球上有公布）

此漏洞通常出现差价活动上面

仅限一次机会购买（表面）

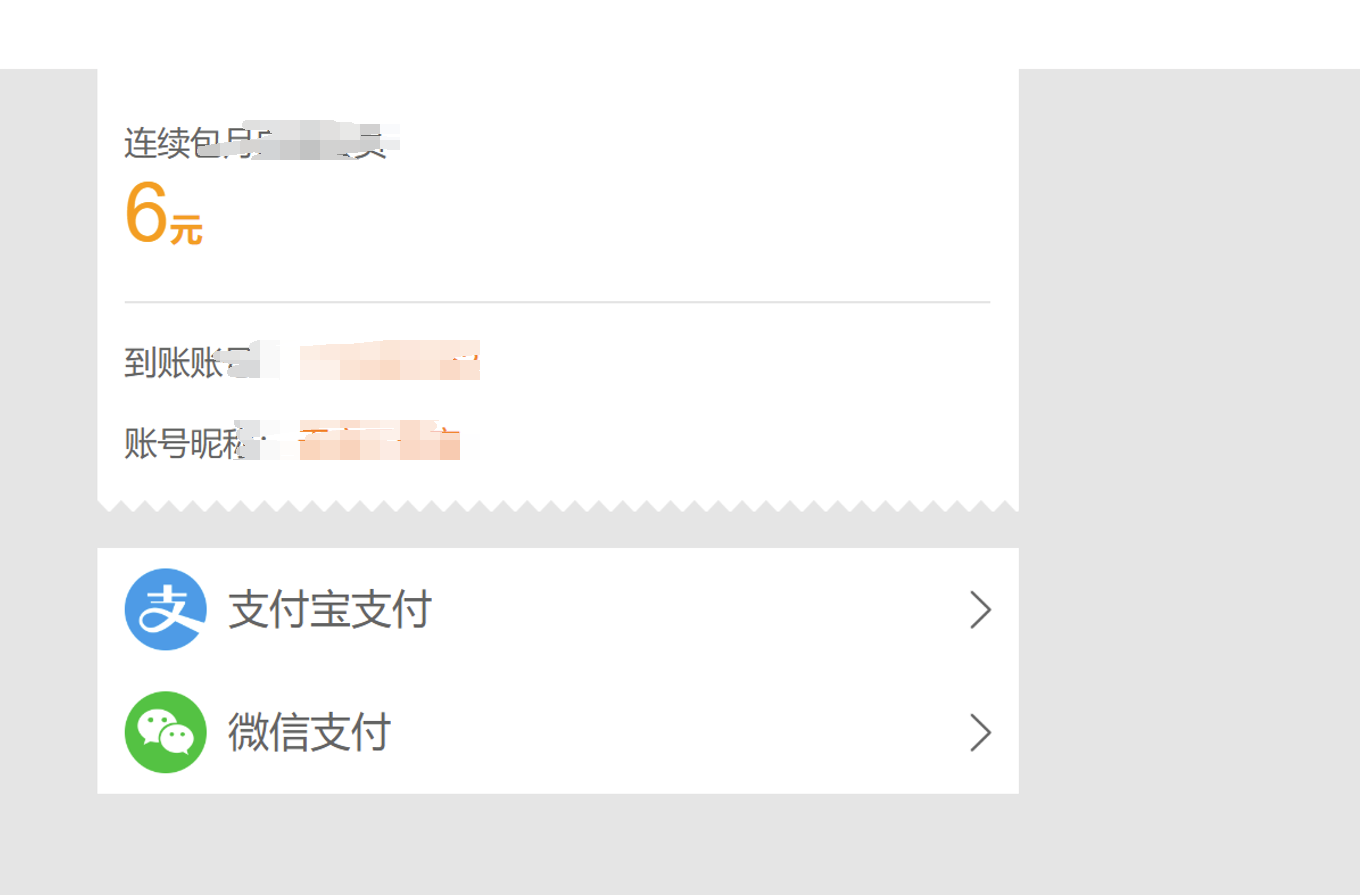
我们抓包看看



这是订单路径

[https://xxxxxxxx.com/xxxxxxxx/xx/SuperWap?qrcodeid=QR16352544942481583291107813](https://agent-paycenter-ssl.xunlei.com/payorder/v3/SuperWap?qrcodeid=QR16352544942481583291107813)

我们先保存下来，发现支付完后订单不会消失



由于支付后会和微信签约自动续费





这里的话我们直接关闭续费，才能批量刷之前的订单支付



这样算的话

每次购买还多送三天，

6元=购买34天

买一年=406天

只需要72元

72=406天

