## 业务逻辑漏洞

——————代金卷使用逻辑漏洞

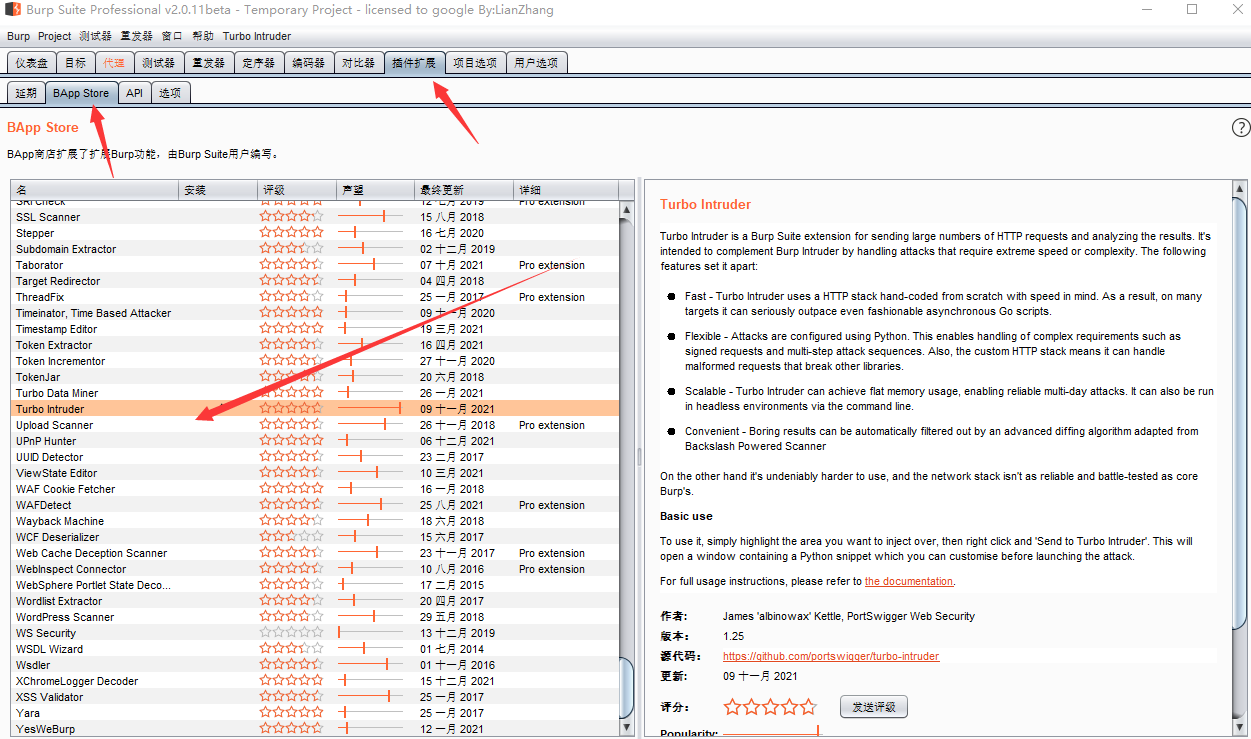
1. 漏洞描述：

代金卷逻辑介绍:代金劵可进行拆分使用。第一次购买服务价格为10元，使用上该代金卷那么该订单支付时就会为0元，那么50元的代金卷-10元就剩下40元，该逻辑存在一个漏洞点 出在拆分支付时。  
 我们先使用该50元的代金卷进行3次10.80元的订单支付，此时代金卷剩下17.6元

我们在创建第四次10.80订单时我们可以使用Turbo intruder进行一次并发，并发完成卷会看见两个0元订单

#### 2.漏洞测试工具：

Turbo intruder 工具是burp自带的插件，可以用于对密码的爆破，验证码的爆破和并发漏洞测试。

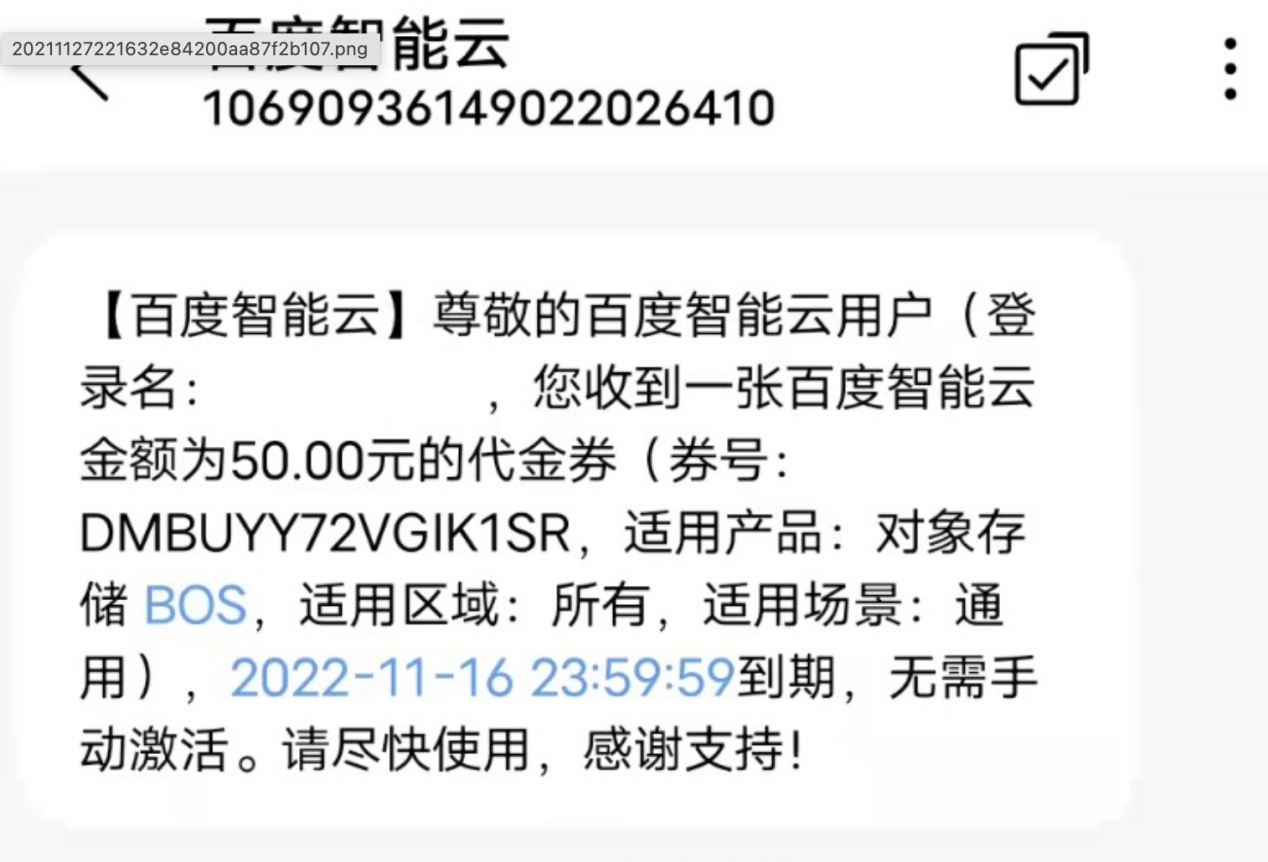


测试方法:使用Turbo intruder模块对其抓包进行测试：

#### 3.案例 ：

百度智能云代金劵逻辑漏洞：

百度智能云送了两张对象存储bos服务的50元代金卷

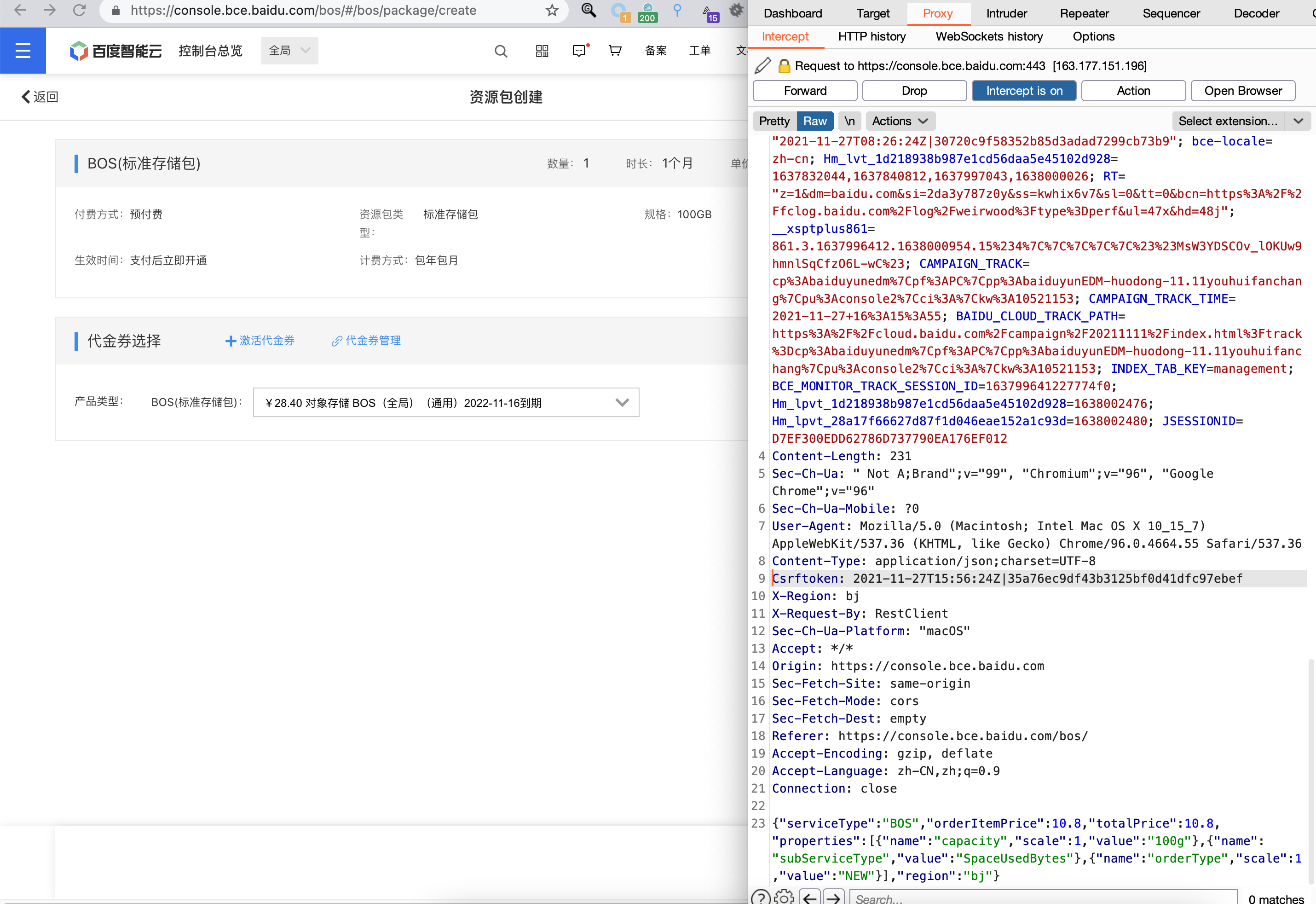
2. 购买500g bos资源需要 53.5元

注释:该图中是使用了代金劵的

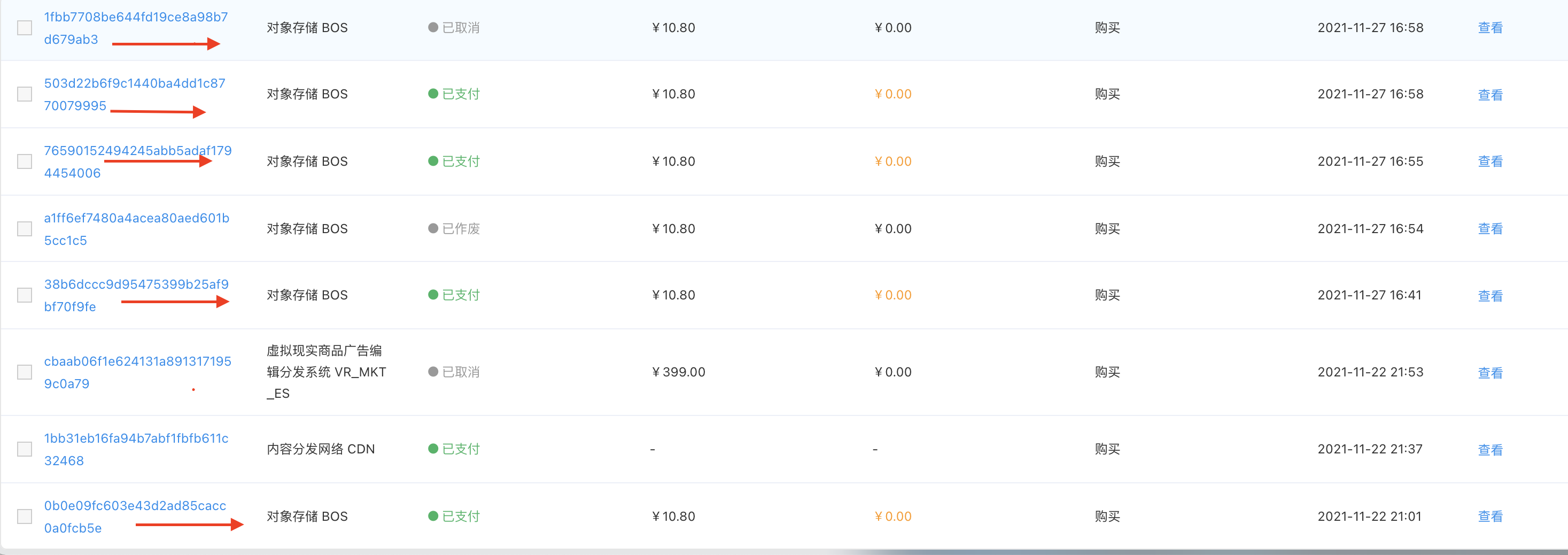


1. 进行拆分购买

只需要进行拆分在 第四和第五订单时一起创建 即可实现 花 50购买 53.8的资源。最后一个订单是可以支付不小心被我点掉了没截到图



如下图红色标志 成功使用50元代金劵 购买了53.80元的服务



该漏洞百度是给了 200块

