业务逻辑漏洞

1.漏洞描述：

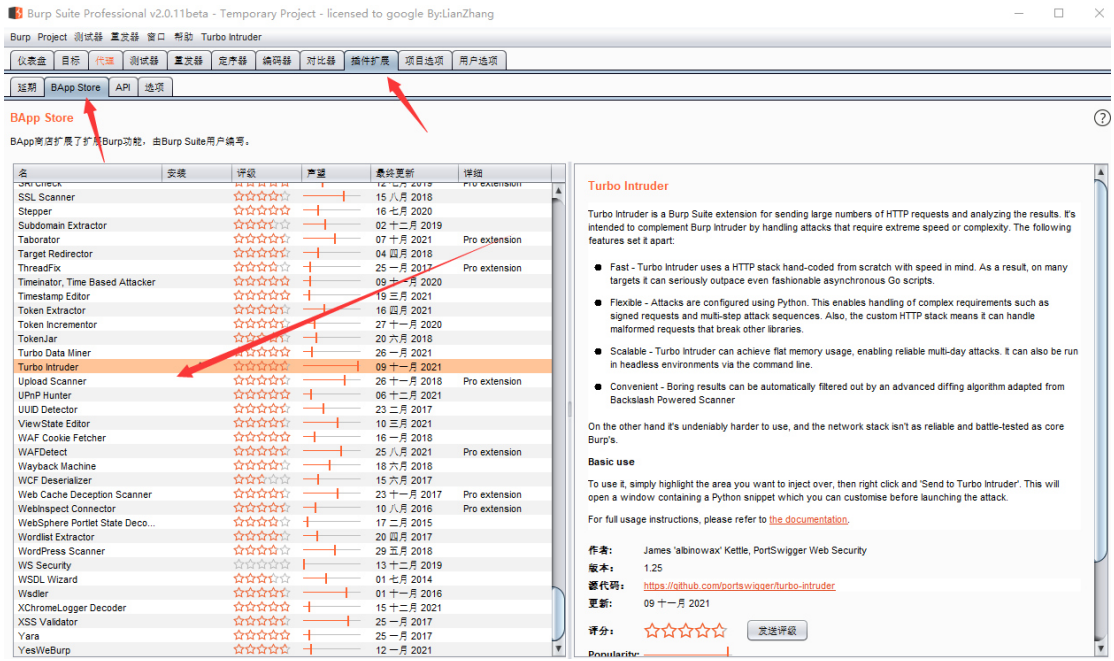
代金卷逻辑介绍:代金券可进行拆分使用。第一次购买服务价格为 10 元，使用上该代金卷那么该订单支付时就会为 0 元，那么 50 元的代金卷-10 元就剩下 40 元，该逻辑存在一个漏洞点 出在拆分支付时。

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 ：

某云代金券逻辑漏洞：

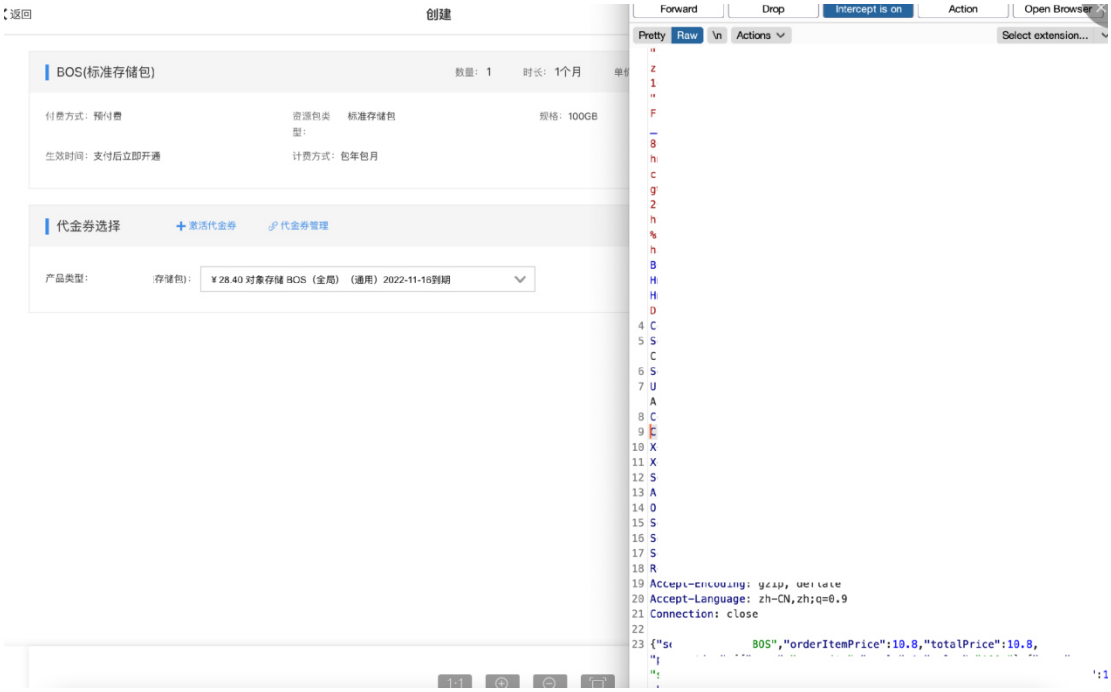
某云送了两张对象存储服务的 50 元代金卷

2. 购买 500g bos 资源需要 53.5 元

注释:该图中是使用了代金券的

3.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 元代金券 购买了 53.80 元的服务