记一次逻辑漏洞实战-超低价购买商品

原创 whit 字节脉搏实验室 昨天

章源自【字节脉搏社区】-字节脉搏实验室
作者-whit
扫描下方二维码进入社区：

业务逻辑漏洞：

由于程序逻辑不严谨或逻辑太过复杂，导致一些逻辑分支不能正常处理或处理错误，统称为 业务逻辑漏洞。

关注重点：

业务流程
HTTP/HTTPS 请求分析
本片文章针对这几天发现的一个网站的漏洞，进行流程分析和漏洞复现，截止发稿之时，漏洞已提交客服反馈，且获得平台奖励，但尚未修复，请勿非法利用。

一、业务分析

首先需要注册登陆：

查看一下付费套餐：

二、业务分析

根据我经验，这个三天试用设置的有点不合理，一个月338，三天只要一块钱，那自然就能想到三十天只要10块钱了，然后先操作一波。

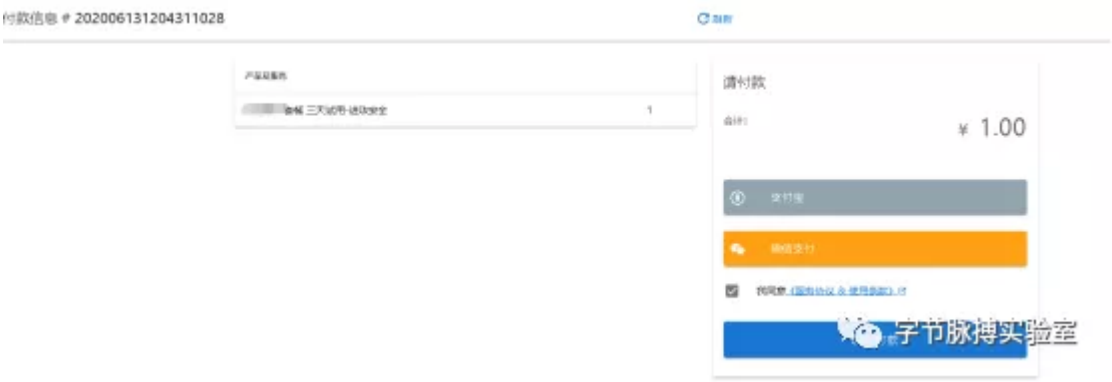
购买分为两步，一是生成订单，然后二是支付。

购买三天试用，下单支付一气呵成，然后再次下单支付，循环十次不就是一个月么，所以继续下单。

哦豁，有限制了，咋办？正常后台开发应该都有这个限制，但是想想是不是有其他办法绕过呢？

三、尝试绕过

捋一下，就知道，下单之后就会判断是否享受过三天试用，那么我先不支付会怎样？
我可以试着先生成多个订单。



尝试之后发现，可以一直生成三天试用得订单。

三、漏洞利用

这步当然是尝试付款，然后看套餐时间是否累加，打开订单详情，逐一进行付款操作，之后能看到套餐时间进行了叠加。

四、漏洞反馈及修复