支付逻辑漏洞

1：低价充值、越权花别人的钱

2：服务年限延长、更少的钱获取服务，并发生成多个优惠订单

3：交易密码绕过

案列1、负数购买

大于100金币的时候，可兑换

（1）

场景：假设火腿肠的价格时 10 块，买2跟，正常的支付是：200-2*10=200-20=180

利用：200-（-2）*10=200--20=200+20=220（可以尝试修改金额）（可以尝试修改数量）

把【1】改成了【-90000000】

知识：没有多余的金币，金币不足，尝试来到购买界面 修改返回包。

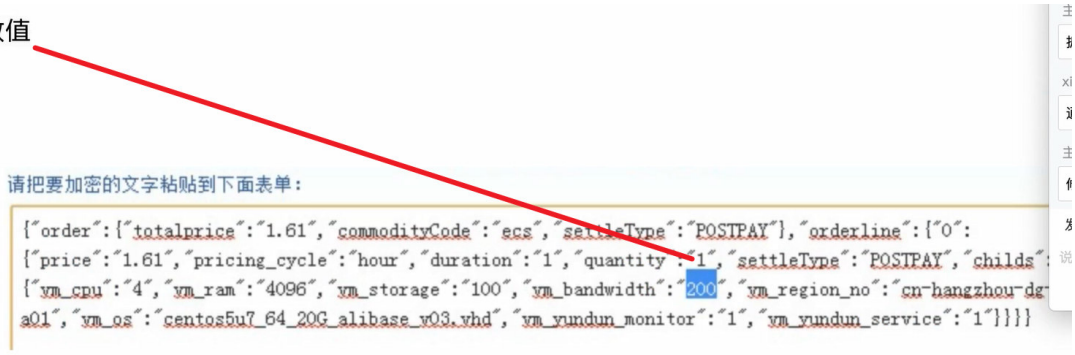
案列2、修改内容

同样的钱或者更少的钱，购买更多的服务

云主机购买逻辑设计不严密，经过base64编码的数据可以被篡改，实现原有买低配的价格可以直接买高配

还原原始数据定位参数

修改参数值



知识：有时候在生成订单时，有时候在支付的数据库包修改。

案列3、修改支付金额

GET请求中 可能也存在修改内容和金额

查看支付跳转链接如下:
http://xxx.com/goPay.html?amount=3489&pId=&oId=&stage=1&pInfo=3489

把两处金额改为0.1元：
http://xxx.com/goPay.html?amount=0.1&pId=&oId=&stage=1&pInfo=0.1

案列4、无线重放

场景：新用户优惠

案例4、无限重放(并发)

```
POST /errnav/getAData HTTP/1.1
Host: xxx.com
Connection: keep-alive
Content-Length: 26
Cache-Control: max-age=0
Accept: */*
Origin:
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer:
Accept-Encoding: gzip,deflate,sdch
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.6,en;q=0.4

t=rateb&UserID=1111
```

知识：退款并发

案列5、修改运费

运费原本是20元，商品是21，通过修改运费金额

运费已经变成1块钱

案列6、修改下单金额

案列7、正负叠加

尝试购买两件商品，商品为数据一正一负提交订单

A商品：30*1

B商品：-10*（2）

案列8、优惠卷

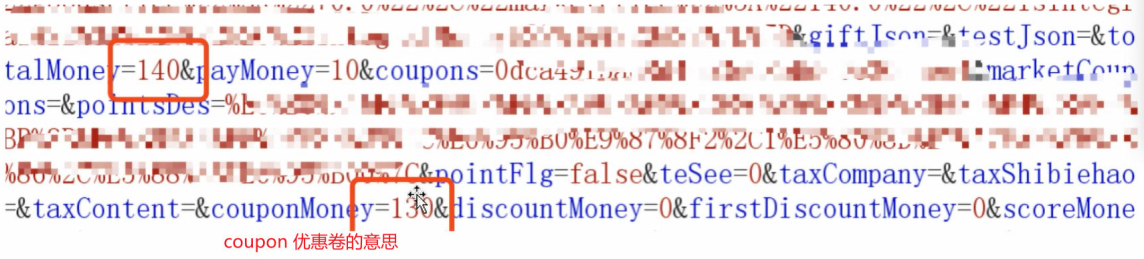
漏洞：首先并发

漏洞：修改优惠卷金额

案例8、优惠券漏洞

随便找了一个可以优惠的课程

数据包



签约漏洞

场景：新用户买VIP会员 首月优惠6元，只能买一个月！

条件：支持多种支付方式，微信和支付宝

利用：选择支付宝支付生成订单，但不支付，在使用另外一部手机登录此商店账号，选择微信支付生成订单。同时付款！

变形：支付时抓包reperater 重放数据包。

并发：可以尝试并发 产生多个订单，一一点支付查看。

溢出漏洞

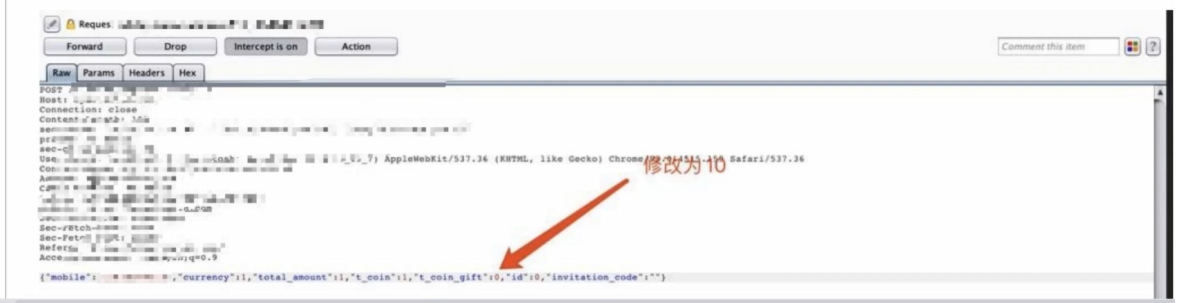
溢出：充值xx个亿

漏洞成因：int32最大值为4 294 967 296，充值98 998 996 172 801，支付溢出

充值金额 98998996172801

修改数据包

抓包，修改 t_coin_gift 为 10，这个参数的意思为赠送的意思



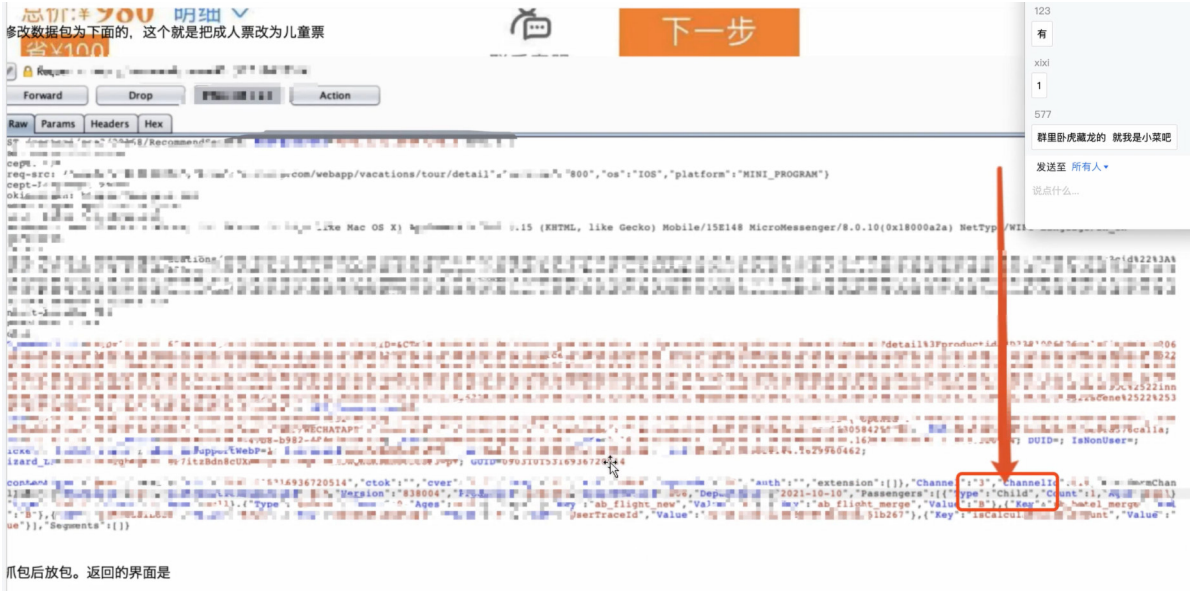
修改类型

场景：成人票980

修改数据包，将成人票改为儿童票

1.跟团游模块，预定一个成人一个儿童票

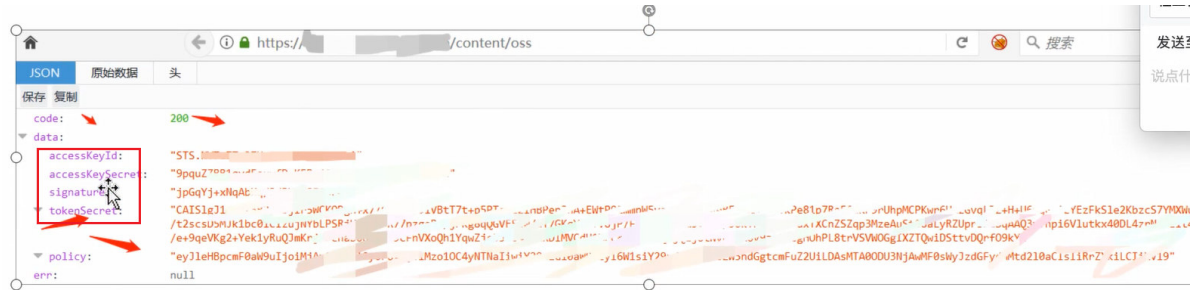
可以看到一个成人票的价格是980



爪包后放包。返回的界面是

高危漏洞挖掘

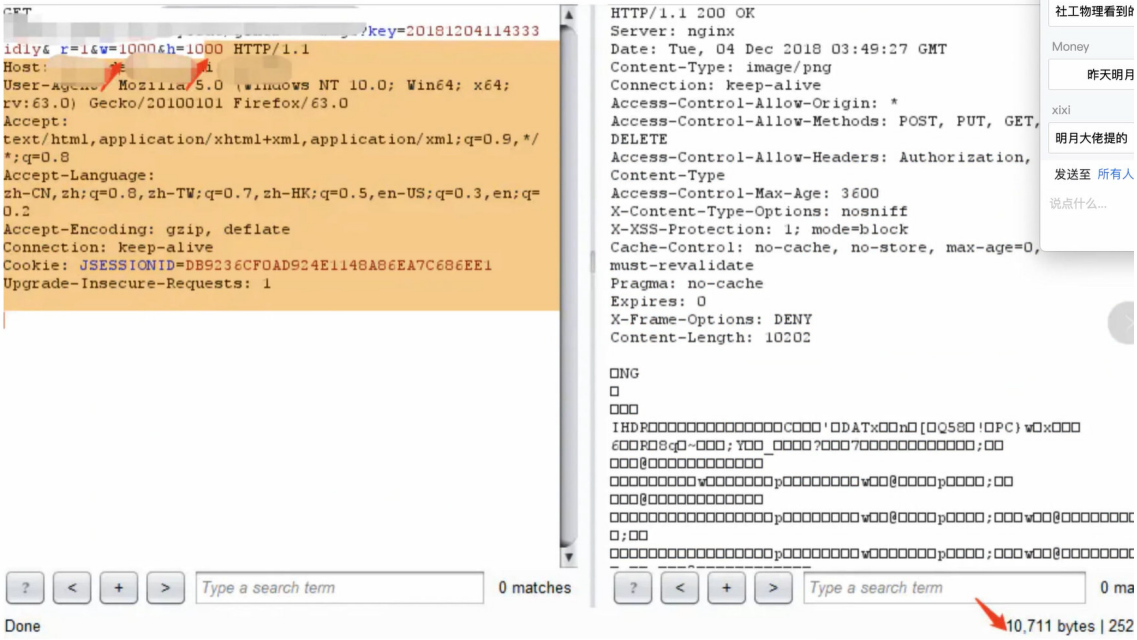
信息泄露 AK登录 content oss 泄露



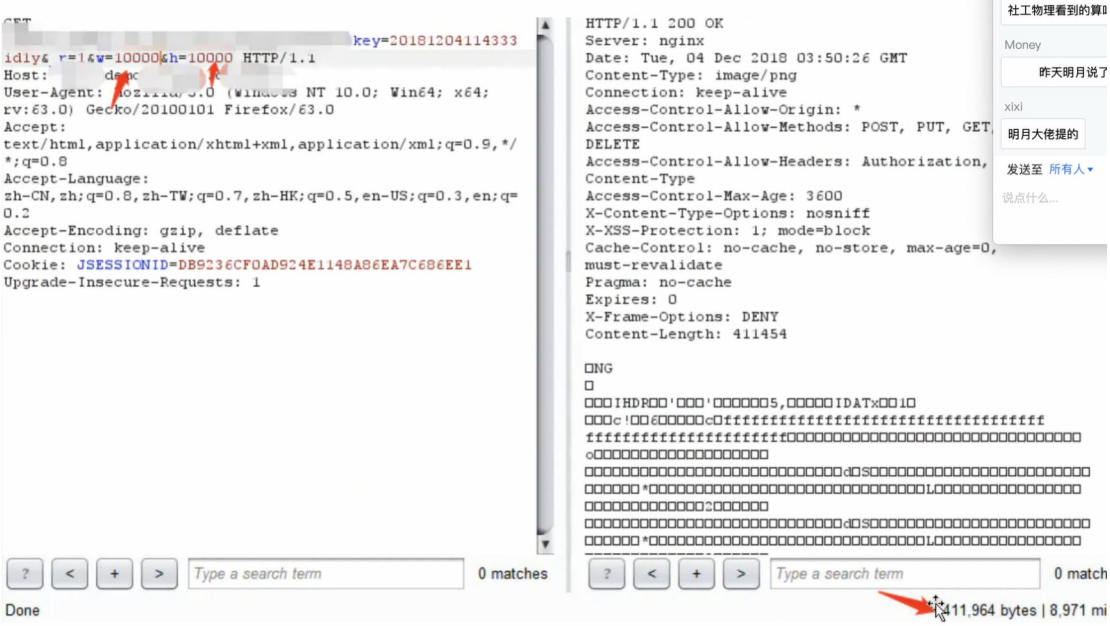
验证码大小 可以控导致拒绝服务

案例4、验证码大小可控导致拒绝服务

得到URL后在得到了上面的链接地址之后呢 我们进行如下修改：H=1000，W=1000分别设置为1000，看到服务器响应



接着将H=10000，W=10000，看到服务器响应字节为411964.



相差非常大说明存在漏洞

3.怎么造成DDOS攻击？
通过上面的测试我们知道了漏洞存在，如果我们发送一个10000的数据包到服务器，服务器需要 10s 理，那么我们如果发送 10 个 10000的数据包呢？
10x10 = 100s

也就是服务器需要花费100s时间去处理，当我们发送 100 个这样的数据包（当然你千万不要用100个数据包扔过去，一般来说经过测试结果 20-50个就能导致网站瘫痪。）