安全小课堂第125期【业务逻辑漏洞挖掘】

京东安全应急响应中心 1月2日

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

JSRC **安全小课堂第125期**，邀请到**月神**作为讲师就**如何通过技术手段挖掘业务逻辑下的漏洞**为大家进行分享。同时感谢小伙伴们的精彩讨论。

业务逻辑漏洞常见发生位置?

京安小妹

月神:

要是按细节来说，每一处都可以是发生位置。

每种类型的APP都有自己的常见漏洞位置。

例如购买，出售，每一条协议的关键参数。

业务逻辑漏洞的分类?

京安小妹

月神：

本文中特定值指的是指当系统保存数据为int整型类型时：最大值/单价+1就是特定值了。当数量超出特定值后，又会从0开始计算

一、饮料贩卖机

n 替换订单ID，创建订单时在支付界面，在此创建订单替换订单ID（高价替换低价）

n 无限新用户优惠订单，重复创建优惠订单

n 替换优惠卷ID (未达到条件使用)

n 个别情况订单数量为1.99时，客户端只支付1元，实际上服务器认为支付了2元。

n 取货时并发（真实案例）

二、 直播

n 快速进出房间炸房

n 无限发送点赞协议

n 修改礼物数量，0，小数，负数，特定值（一般情况下为1073741824）

n 修改礼物ID，遍历尝试是否有隐藏ID。

n 并发送礼物，抽奖

n 无限创建首次优惠订单，有些首次优惠订单是一个特殊的pid，这种的直接替换pid进行支付。有些是相同的ID，这种的提前创建订单，记录多个订单号在依次修改订单支付。

n 刷屏：发言刷屏，分享，点赞等有提示的地方刷屏

n 房间内可以申请的地方进行申请取消操作，看看是否能炸房。

n 越权踢人，增加管理员，关闭房间等操作。

n 发送的表情是否可以修改长宽（真实案例）

三、购物app

n 购买数量：为0，小数，负数，正负值（A为-1，B为2，总值为1）

n 代金卷：并发领取，遍历领取，同一个代金卷重复使用，未满足条件使用代金卷

n 越权：登陆，操作别人订单，修改资料

四、外卖

n 商品数量，0，负数，小数，特定值，正负数（A为-1，B为2，总值为1）

n 送餐员评价修改，星级，打赏金额（小数，负数）

n 商品评价，星级，评论字数，上传图片是否可以自定义格式，

n 订单超出送餐地址

n 强行货到付款，取消订单，退款

n 强行负款，取消订单，退款
n 越权操作别人订单，登陆
n 优惠购买会员（重复使用优惠购买）

五、交易平台

n 钱包并发提现，负数提现
n 使用钱包支付时多个订单并发支付（是否支付金额能大于余额）
n 转账负数，并发转账
n 上架商品突破限制，例如数量，字数。
n 替换订单，创建订单号如果订单状态可修改，先进到支付界面，然后将订单修改成更大的金额，然后支付提前进入的支付界面
n 数量修改

六、社交

n 强行举报（读取本地消息上传那种）
n 强行加好友（一般尝试重发通过好友这条协议）
n 自由修改号码（靓号类）
n 群管理无限禁言
n 越权禁言，替人，拉黑
n 会员修改金额，数量。无限优惠购买
n 非会员使用会员功能

七、漫画

n 打赏金额为负数，小数，特定值（溢出）
n 越权删除评论，登陆
n 修改充值金额
n 付费漫画免费看
n 评论图片数量过多会导致客户端加载卡死

八、音乐

n 唱歌类软件修改上传分数等参数
n 付费下载尝试替换下载ID
n 修改付费下载金额
n F12查看下是否有歌曲地址

九、网约车

n 无限叫车，重复发送协议造成市场混乱
n 修改评价分数
n 修改限时优惠叫车关键参数
n 替换优惠卷

越权操作其他订单

讲师

业务逻辑漏洞的挖掘思路?

京安小妹

月神:

有时候你想到了一个奇葩逻辑，会通杀很多APP（我用了一个简单的支付逻辑在4家SRC每个洞都讹到了高危）所以逻辑漏洞虽然看似简单，如果奇葩也能通杀。我的挖掘思路就是拿到包后，先随便测，从登陆，资料评论这些简单的功能都过一遍，挖到低危不要紧，挖到了就是给自己建立了信心，没白挖。

然后简单功能过了一遍后，开始细扣每个功能例如支付这种容易出高危严重的地方可以先看一下，把自己积累的思路过一遍，比如先充几块钱，然后并发提现。或者充值5元后，用5块钱并发支付多个5元的订单，这个相比其他支付漏洞的出现率还是多一些的。最重要的是想别人想不到的，如果是小白，可以学习一些常见的思路，然后自己找些网站来测试，我给的建议就是别学太多，入门就行，剩下的自己在实践中悟，这样就不会被常识束缚住。不然挖逻辑漏洞时太容易就被已经掌握的常识所束缚了。

没去尝试过的东西永远别说不可能，上学的时候微X刚出，资料只能改30个字，那时候我刚教我朋友使用手机上的内存修改器，我们平时没事就找些网游刷一下，那天朋友突然和我说微X资料可以改内存把长度提升到100字。我第一反应是不可能，改了肯定没用，是不是你刚学不会改看错了。结果还真是能改。

从那以后我就告诉自己，别说不可能，没啥不可能的，出问题了第一反应不是否认，而是站在对方的角度去想，怎么复现这个漏洞。以前在第三方平台做游戏防外挂，由于游戏是代理的，很多时候看不到玩家的数据。玩家出现作弊后，开发通知到我这边，我这边只能猜测漏洞如何出现，大多数都是用目前已经掌握的知识就能猜的八九不离十了。但是只有一次我印象最深，那时候刚出了一款游戏，XX农药刷符文，大家都在玩，于是我也跟风玩了起来，然后在破解群出现了商人，代刷符文，听到刷符文，第一反应就是负数溢出了，但是如何尝试负溢出都不行（那个时候思路不是特别多，溢出只知道修改负数）机缘巧合下，那天我接触到了正数溢

出，在游戏里面通常最大数值就是2147483647，那么正溢出就是假如商品单价为2，那么我要做到的就是2*数量>2147483647，假如买1073741825个*2就是2147483650，在游戏中由于超出了最大值，总价格就会变成了3（超出后从0开始计算），于是去尝试了一下，果然是这样，经过计算后，成功刷到了符文箱。

所以一定要勇于尝试，丰富各种各样的奇葩思路

讲师

业务逻辑漏洞的案例分析

京安小妹

月神：

一、

先来讲一个某外卖平台订餐的软件吧，我和朋友说我把这个软件订餐的数量改了，改成了负数结果成功了，然后他表示他尝试过并没有成功。同样是负数为什么没有成功呢？我一开始的思路也是将其修改为负数，在点几个正数的保证达到送餐的数量。但是服务器有校验，单个金额和总体金额不能为负数，你们想一下，这样看起来就很完美了，于是我一直思考有没有什么逻辑是被我疏忽掉的呢。想了半小时终于想出来了。参数大概是这样的

{"total_price":"21.04","products":

[{"cart_id":"0","product_id":"277976516634","product_quantity":1,"produ

[{"cart_id":"0","product_id":"277976516634","product_quantity":1,"product_name":"芝麻糖饼","activity_num":1,"dish_activity":1,"cart_type":"cater"},{"cart_id":"0","product_id":"203689622554","product_quantity":2,"product_name":"鲜汁肉包(2个)"}]}

我们来看一下，其中有商品ID，单价，数量，活动优惠数量，总价，数量价格总价对不上都不让下单，看起来环环相扣，于是我尝试了将商品ID都改为同样了，数量这里一个为正一个为负，也就是这样的：

{"total_price":"XXX","products":
[{"cart_id":"0","product_id":"277976516634","product_quantity":-1,"product_name":"芝麻酱糖
饼","activity_num":1,"dish_activity":1,"cart_type":"cater"},
{"cart_id":"0","product_id":"277976516634","product_quantity":2,"product_name":"鲜汁肉包(2个)"}]}

修改后用计算器来计算一下总体价格，公式大概是这样的：总价=物品*-1+物品+优惠物品价格

算下来后下单成功了。绕过了服务器校验的单个数量不可以为负数的逻辑。（商家收到的图）

二、

在测试某款金融软件时，看了很多功能，逻辑都很严谨，在处处碰壁即将要放弃的时候，寻思试一下钱包吧，虽然感觉不太可能，但是梦想得有，万一实现了呢。于是提现时候试了一下负数~结果真的成功了。将下面参数中amount":"1"改为amount":"-1"

从图片中可以看出，负负得正，于是提现后钱包就多了相应得金额，如果被非法分子利用的话就拿去买东西或者直接提现了~

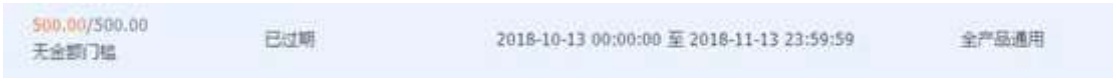
reqData=
{"amount":"1","cardId":"5612912350382","withdrawFlag":"0"}&sid=4dacbde55cfe1bd8fff6a9f2cc72c9ew&source=app

四、

某社交平台刷会员，这个纯是靠操作就能实现的一个逻辑漏洞了。在以前没有工具（还不懂）的时候经常靠操作来测试逻辑漏洞，也可以说是卡BUG，大家都知道有些软件推出了会员签约功能，签约付费就能以低价购买会员，这个漏洞是这样的，我第一次测试时，使用支付宝打开签约界面，然后使用微信在打签约界面，在依次支付，支付后系统提示，无法重复签约。我想难到系统有检测，舍不得孩子套不到狼。于是申请个新号再次测试，还是支付宝和微信都打开了签约界面，这次先签约其中一个比如签约微信，支付成功后，去微信取消签约，然后在去支付宝点击签约，奇迹发生了，到账了2个月的会员，也就是说服务器校验了不能同时签约，但是没有校验解约后再次签约的情况。提交漏洞后，等待漏洞修复又想出个测试方法，还是购买会员选择微信到签约界面，但是不签约，这时候换手机，登陆这个APP，再次打开微信签约界面，如此重复，打开N个微信签约界面后。签约又成功了。因为都是微信可能属于同类型的签约没有校验。

五、

再来说一个某云服务器刷代金卷。这个逻辑就比较简单了，测试的时候我发现了这个网站正在搞活动，送代金卷，根据我玩游戏的经验，程序总是喜欢在后台做一些隐藏的道具或者测试道具，只是屏蔽了前端。这时候我去领取代金卷时，用工具burp对ID进行遍历。13000-14000，遍历后发现居然领到了大金额无门槛的代金卷



领到了很多张这种无门槛的代金卷，我一看过期了，但是使用时候却能选择，并且成功使用购买的产品，于是我猜测应该是内部测试时程序给配置的吧，由于疏忽忘记加白名单所以谁都可以领取到了。

下面这个act_ids就是代金卷的组合。可以只保留一个然后进行遍历操作。

action=getVoucher&data={"activity_id":11177,"preview":false,"act_ids":[12637,12638,12639]}

六、

最后讲一个被忽略的漏洞吧，为啥被忽略呢，在下口才实在不行，辩不过审核小姐姐，某外卖软件强行货到付款，在测试某外卖软件时，测试了很多点，发现还挺安全的，反正一些小的逻辑漏洞都没有，于是在下单时看到了一个关键参数，这里面就不列举了，不然就知道是哪个了，该参数的值为0，其他参数都是地址，坐标，名字，订单号等信息，都能看懂是啥意思，唯独这个0不知道是干嘛的，于是改成1下单试一下，下单后我还没有支付就显示了订单成功，然后商家已接单，这个商家根本不支持货到付款（为了不造成影响找朋友的门店来测试的）不一会儿，外卖小哥就来到了店里，然后告知小哥这个订单是测试订单。我这边下单后可以直接点击确认收货，然后进行恶意差评。如果同行竞争的话利用这个漏洞简直太可怕了。用网上虚假手机号来下单，会给竞争对手造成很大的损失。但是审核小姐姐说这样做就违法了。我也不知道该说什么了，就这样吧哈哈直到今天这个漏洞也没修

复。。。

讲师

业务逻辑漏洞的防御手段

京安小妹

月神：

站在攻击者的角度看待问题，查找问题时先不去想如何防御，我是对破解的过程有特别的兴趣，所以拿到程序时我先大概看一下程序的主要功能都有什么，然后迅速在脑中构思出一个破解思路和过程，然后开始着手破解，不停的尝试，觉得差不多了就停止，等有了新思路在尝试，也可以找一些朋友来帮忙测试一下，看一下有没有漏掉的点，毕竟每个人的思路还是不同的，找到了所有点后整理个报告，在来想如何防御，漏洞修复后一定要尝试其他思路是否能继续绕过，我在某SRC提交刷会员的时候用了3种不同的思路来绕过了~

讲师

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂。如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，点击菜单栏进入“安全小课堂”即可浏览。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心