电子支付漏洞专题报告

北京市海淀区西北旺东路 10 号院西区 11 号楼东侧 天融信科技集团

100193

电话：+8610-82776666

传真：+8610-82776677

服务热线：+86-4007770777

https://www.topsec.com.cn

版权声明

商标声明

信息反馈

+8610-82776666

目录

文章摘要：电子支付漏洞是指在支付过程中，攻击者可以通过利用漏洞获取用户支付信息，甚至非法转移资金。本文对电子支付的现状，电子支付漏洞的定义、原因、影响以及防范措施进行了深入探讨。

关键词：电子支付；漏洞；解决方案

1. 电子支付的现状

1.1 电子支付的定义

根据中国人民银行在 2005 年 10 月公布的《电子支付指引（第一号）》，电子支付被定义为“单位、个人直接或授权他人通过电子终端发出支付指令，实现货币支付与资金转移的行为。电子支付的类型按照电子支付指令发起方式分为网上支付、电话支付、移动支付、销售点终端交易、自动柜员机交易和其他电子支付”[1](中国人民银行,电子支付指引（第一号）)。在现代电子商务系统中，电子支付是主要的支付手段。电子支付以接受线上转账和其他电子化付款方式为主要特点，已经成为我国最常见的支付手段之一，其影响力仍在不断扩大。

电子支付依赖现代密码学实现的身份认证技术和安全通信协议。以目前应用最为广泛的线上电子支付技术为例，用户完成支付之前，需要借助 PKI（全称：Public Key Infrastructure，公钥基础设施）来和金融机构的服务接口建立一个经过 CA（全称：Certificate Authority,权威证书签发机构）认证身份的安全连接。大多数情况下，该连接会直接使用 TLS（全称：Transport Layer Security，传输层安全协议），以确保数据在公共互联网上传输时的隐蔽性和完整性。

本文提及的电子支付包括线上转账和实体商户使用的 POS 机等收款手段，但不会涉及加密货币等新兴支付方式。

1.2 电子支付在我国的应用

我国电子支付分为传统金融机构提供的支付手段（如网络银行）和第三方支付两大主流类型。传统金融机构和第三方支付手段均覆盖线上和线下两种支付场景，电子支付的应用场景大致相同。“第三方支付”指非金融机构作为商户与消费者的支付中介，通过网联对接而促成交易双

方进行交易的网络支付模式。近年来，在我国电子商务持续繁荣、移动支付快速发展的推动下，我国第三方支付交易规模持续扩大。移动支付是第三方支付增长的主要驱动力，据统计截至 2022 年，我国移动支付用户规模约为 9.04 亿，77.5%的手机用户每天都会使用移动支付[2]。

图 1-1 中国第三方支付综合交易规模发展趋势

图 1-2 中国非银行互联网支付与移动支付市场规模对比

1.3 电子支付的主要形式

从中国人民银行文件可以看出，我国对电子支付的形式划分为如下几类：

- 网上支付
- 电话支付
- 移动支付
- 销售点终端交易
- 自动柜员机交易
- 其他电子支付

其中网上支付也就是线上支付，是现代电子商务系统的核心支付方式。在线上支付流程中，付款者使用银行或第三方支付机构提供的数字金融工具，以互联网和 web 技术为基础，完成对收款者的资金转移。

电话支付、移动支付、销售点终端交易、自动柜员机交易等均属于线下支付的范畴。在线下支付场景中，付款者通过电话银行、智能手机、银行卡、生物特征等可以有效认证身份的终端完成对自己金融账户的资金划转，从而完成支付。

1.4 电子支付相关漏洞的统计

根据《国家信息安全漏洞共享平台》(CNVD) 每年公布的电子支付相关漏洞进行统计，2019 年之前电子支付相关漏洞数量保持了较快增长趋势，2019 年后，相关漏洞数量逐渐减少，天融信阿尔法实验室调研发现，漏洞减少的原因主要有以下几点：

1. 第三方支付业务聚拢在头部厂商，该类厂商具备完善的运营机制和风控机制。
2. 相关企业对电子支付漏洞越来越重视，逐年加大漏洞治理投入力度。
3. 攻击者未将掌握的相关漏洞公开。

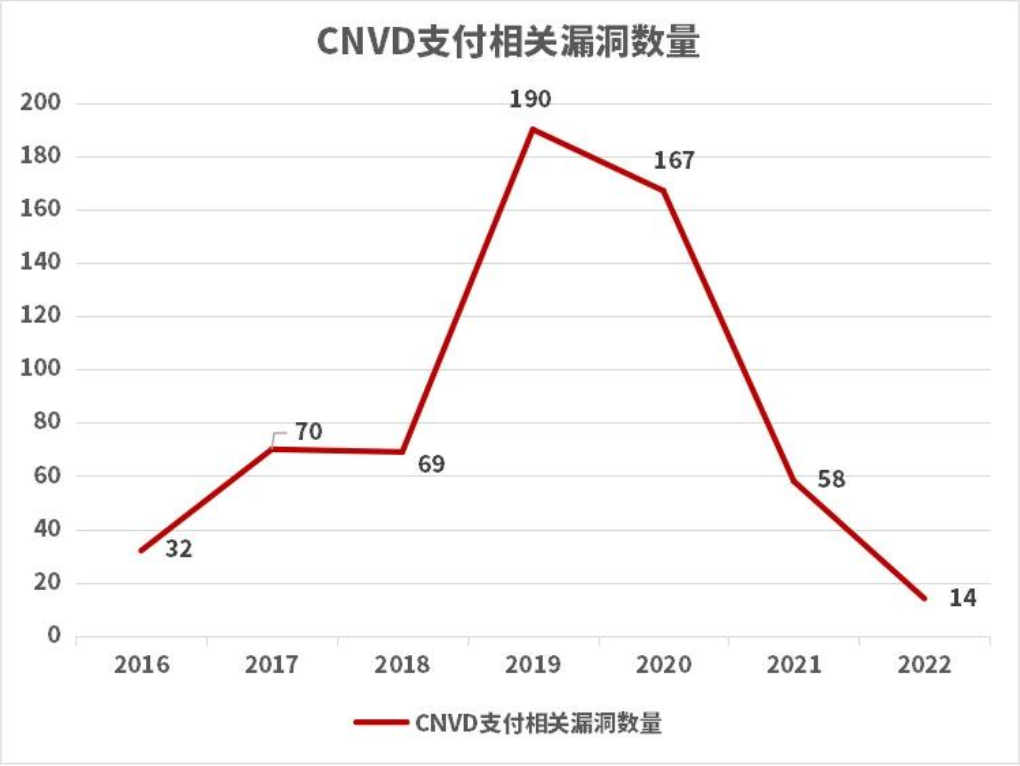

图 1-3 支付漏洞趋势

1.5 电子支付的安全风险

1.5.1 线下支付安全风险

线下交易要求付款者必须持有有效支付工具，如银行卡和智能手机 APP。

银行卡可产生的安全问题包括：

1. 卡遗失导致被冒用。
2. 商户终端的安全问题，如针对信用卡系统的中间人攻击[3]。
3. SDA（静态数据认证）的安全问题可以导致重放攻击等[3]。

针对目前流行的智能手机 APP 使用二维码支付的场景，安全问题如下：

(1) 越权扣款，本质上是攻击者使用扫码枪盗刷付款者的一次性付款码，也就是用户凭据的易失性。

(2) 二维码欺骗，由于二维码不具备可读性，付款者扫描商家付款码时也可能扫描到攻击者留下的恶意二维码，从而被引导进入钓鱼页面进行扣款或产生其他危害。

1.5.2 线上支付安全风险

线上支付场景中，传统信用卡支付仍可使用。但由于缺少实体卡的认证保护，付款者必须输入信用卡安全信息来证明自己持卡人的身份。针对身份认证问题，Mastercard，Visa 等卡组织推出了 3D Secure 协议[4]，而第三方支付平台则会使用自己的身份认证协议。

针对以上场景，可能的攻击面如下：

1. 协议本身的安全缺陷，如 3D Secure 协议的 iframe 应用导致的不可辨识性[3]。
2. 钓鱼攻击，攻击者可能伪造商家或付款页面并欺骗付款者进行付款。
3. 电子商务网站存在的安全漏洞导致的身份冒用或者恶意消费等。

4. 第三方支付平台的安全漏洞导致的其他问题。

2. 电子支付原理与实现

2.1 简述

电子支付通用支付流程一般涉及四个主体：消费者、商家、金融机构以及移动运营商。电子支付的具体原理根据不同的支付方式有所不同，电子支付一般可以分为线下支付与线上支付。线下支付主要使用的通信技术有 RFID（Radio Frequency Identification）、NFC（Near Field Communication，简称 NFC）、蓝牙。线上支付一般通过短信、邮件、移动网络等完成。

2.2 线下支付

2.2.1 线下支付概念

线下支付一般指用户在购买完商品后，通过手机或者智能卡等设备，在现场完成支付过程。常见的线下支付方式有 NFC 支付、RFID 支付、蓝牙支付、扫码支付等。

2.2.2 线下支付一般流程

线下支付的一般流程为：

用户进入商店选择购买的商品，商家在其收费终端设备上输入用户的消费金额向用户发起收款，用户携带的支付设备与商家的收款设备进行通信、数据传输完成支付过程，商家的终端设备将数据上传到第三方的交易系统，交易系统根据商家的结算周期以及数据定期向银行发起付款请求。如下图 2-1 所示：

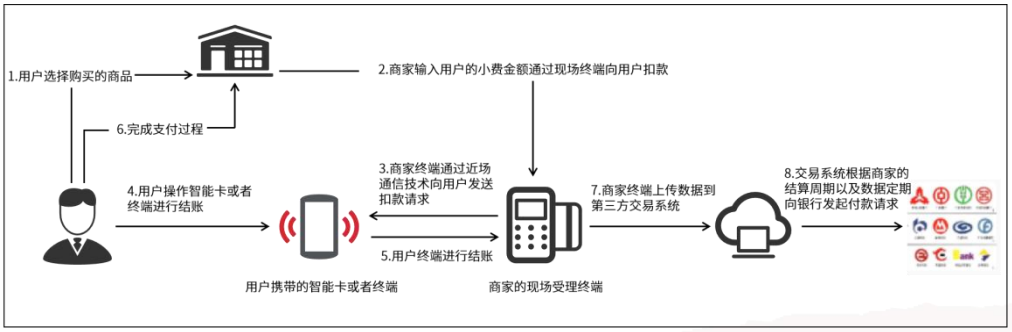

图 2-1 线下支付原理图

2.2.3 线下支付技术分类

1) NFC 支付

NFC 支付是使用 NFC 通信技术在读卡器和支付设备之间交换数据。NFC 设备必须在较近的距离（通常相距小于 2 英寸）才能完成支付。

NFC 技术在单一芯片上结合感应式读卡器、感应式卡片和点对点功能，当支付设备和 NFC 芯片相互靠近并激活时，NFC 芯片交换加密数据并完成支付。NFC 芯片使用特定的 RFID 射频（13.56MHz），仅在芯片非常靠近时才起作用。

图 2-2 线下支付展示

2) RFID 支付

RFID 支付使用 RFID 技术进行支付，RFID 技术（也被称为射频识别）通过磁场或者电磁场，利用无线电射频方式进行双向通信，以达到识别目的并交换数据。在电子支付中，基于 RFID 技术的支付方式主要有 NFC、eNFC、SIMpass、RF-SIM 这四种方式。

RFID 支付过程主要是支付设备靠近识别设备，然后双方进行数据交换，完成支付过程。

3) 蓝牙支付

蓝牙支付主要使用蓝牙技术进行支付。在蓝牙支付系统中，通常情况下支持蓝牙支付的手机和商家的蓝牙传感器是系统中的核心设备。使用蓝牙的支付设备通过相同的无线电波传输信息，蓝牙支付中的蓝牙标准被称为低功耗蓝牙（BLE），比正常情况下的蓝牙功耗要小。该标准（BLE）已经被 Apple、Android、Windows 和黑莓手机所支持。与 NFC 支付方式相比，蓝牙支付技术的主要优点有传输距离远，速率快等。

4) 扫码支付

扫码支付通常指二维码支付，这是一种无线支付方案。商家可以将自己的支付账号，商品价格等交易信息汇于一个二维码中。用户通过二维码识别设备识别商家的二维码进行付款。除此之外，用户也可以将自己的付款信息汇于二维码中，让商家识别自己的二维码进行付款。因为扫码支付在线下的应用场景较多，因此将其归类于线下支付中。

2.3 线上支付

2.3.1 线上支付概述

如今我们日常生活中比较常见的支付方式就是线上支付，比如支付宝支付，微信支付，短

信支付，语音提示支付等。线上支付也被称为远程支付，它通过连接到通信网络，然后接入支付后台系统完成支付过程。移动网络以及移动终端的发展推动了线上支付的全面推广，在一些较为偏远的地区，银行等机构部署支付设备费用较为高昂，线上支付的出现就很好的解决了这一问题。

2.3.2 线上支付一般流程

线上支付的一般流程：

用户到在线商城挑选商品并添加到购物车，然后用户选择下单，网站系统分别在前后端对用户提交的信息进行校验，校验无误之后在服务器端创建订单，否则向用户返回审核失败的提示，在创建完订单之后，用户进行支付，完成购物过程。如下图 2-3 所示：

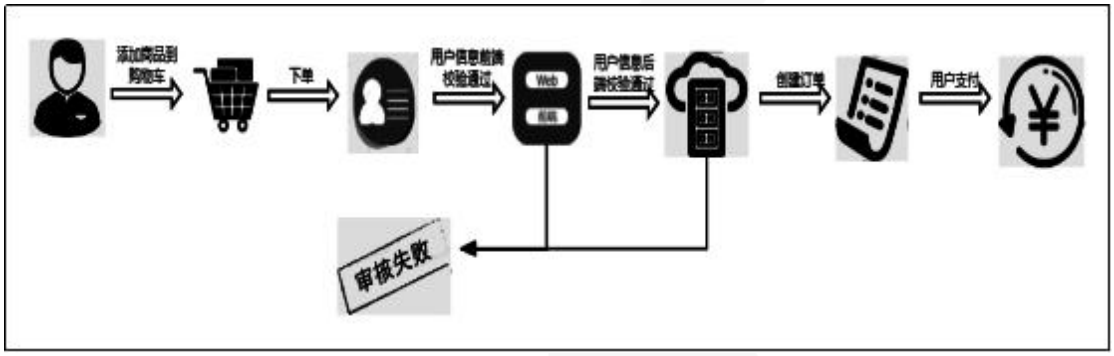

图 2-3 线上支付流程图

2.3.3 第三方支付的流程

现如今，用户用到最多的线上支付方式就是第三方支付，如微信支付，支付宝支付等，因此这里将第三方支付单独列出来进行讲解。

第三方支付的一般流程是：

用户向商家请求进行在线支付，商家根据支付公司的接口规范返回数据，这里的返回数据一般是带有第三方支付公司的接口参数的 URL，用户根据商家提供的接口规范请求第三方支付系统，第三方支付系统按照银行提供的接入规范接入网银系统，网银系统转账给第三方支付公司，

第三方支付系统返回给商家用户支付成功的返回信息，商家返回更新的订单信息给用户，整个支付流程结束。如下图 2-4 所示：

3. 支付环节攻击方式与漏洞类型

对已知支付环节的攻击方式进行分类，可以分为：物理攻击、网络攻击和社会工程学攻击，这三种攻击方式的简单介绍在表 1 中列出。

物理攻击是指通过物理接触方式对感知设备本身进行攻击（例如 IC 卡、射频卡等），包括但不限于卡号篡改、卡号覆盖、卡号复制、扇区密码破解、扇区数据未加密等。由于该类设备具有应用场景广泛、保有量较大、更新迭代复杂的特点，所以一旦受到攻击将可能产生较大的经济损失。

对于日常生活中常见的交易支付卡片主要有两种，低频 ID 卡和高频 IC 卡，它们按照各自特性分别应用在我们日常生活中的方方面面。例如我们日常使用的水卡、电卡、饭卡、银行卡、燃气卡等等。对 ID 卡主要攻击方式为卡复制，对 IC 卡的攻击方式主要有卡数据嗅探、卡数据重放、卡复制、卡数据破解与篡改。攻击者在支付环节较多采用卡复制、卡数据破解与篡改两种方式进行攻击，对支付环节构成危害。

网络攻击方式是指对支付环节的客户端、服务端、支付相关数据（支付金额、产品数量等）通过一系列手段包括但不限于对身份进行伪造、绕过逻辑判断、篡改数据等对支付环节进行攻击，获取相应的收益。

社会工程学攻击是指利用人性的弱点，通过欺骗被害人的手段包括构造钓鱼邮件、通过社交软件欺骗、电信诈骗、网址仿冒、木马病毒等方式进行钓鱼攻击或者通过伪造替换收付款码、伪造纸质优惠券等方式对交易规则进行破坏，造成支付攻击。

分类	特点
物理攻击	获取 ID 卡用户凭据，对其进行篡改、复制等
	破解射频卡数据区密码、修改扇区金额数据等
网络攻击	通过身份伪造、篡改数据、绕过逻辑判断等方式对支付环节实施网络攻击
社会工程学攻击	通过水坑攻击、鱼叉攻击等方式进行钓鱼攻击
	通过替换收付款码、伪造纸质优惠券等破坏交易规则的方式进行攻击

表 1 攻击者模型及其特点

3.1 卡复制

3.1.1 卡复制简介

部分可交易卡片，经常使用存储器里面的身份凭证（ID 值），查询数据库认证用户身份，与刷卡机交互进行交易。如果攻击者直接将它的数据写入一张空白卡中，就可复制出一张身份信息相同的卡片，攻击者可以利用复制的卡片进行盗刷。

3.1.2 卡复制原理分析

射频识别卡内有电磁感应线圈，连接着 ID 或 IC 芯片。当这个组合体靠近读卡器时，会在读卡器电磁场中产生感应电流，从而驱动芯片读取卡内信息，再通过自身的感应线圈将信息以电磁波的形式发送出来，被读卡器接收到，之后由读卡器系统进行数据交互。

如果射频识别卡中数据未进行加密处理，便可通过读写卡设备读取卡中数据并写入空白卡中，实现卡的复制。

3.1.3 卡复制案例

案例如下[5]

由于该门禁卡未对数据进行加密，导致可以通过手机 NFC 对门禁卡进行复制同时通过 NFC 解锁门禁。

下载 NFC 门禁卡模拟器

图 3-1 NFC 门禁卡模拟器

然后进行 root 手机，部分机型还需要解锁 system，搞定后运行软件，软件第一次运行需要点击右上角问号的关于界面进行注册。

图 3-2 注册 NFC 门禁卡模拟器

一切正常后，就可以去刷一张卡片了，刷卡后在卡片维护里可以修改名称，并可以发送卡片快捷方式到桌面，方便以后一键模拟。

图 3-3 模拟复制门禁卡

点击开始模拟，选择好卡片后点击确定，程序会自动模拟该卡片。模拟成功后，关闭程序，到这里，攻击者可以使用手机去刷卡。

图 3-4 复制成功进行刷卡

3.2 卡数据破解与篡改

3.2.1 卡数据破解与篡改简介

射频 IC 卡种类繁多，标准也比较多，以目前广泛使用的 M1 卡为例。读卡器使用分为两种情况，一种是需要先判断 UID 是否正确，再对卡密码进行验证；另一种是读卡器不判断 UID，只对扇区进行验证。这两种方式均存在一个问题，即对卡密码验证成功则允许篡改卡内数据。

3.2.2 卡数据破解与篡改原理分析

1) 默认密码攻击

很多射频 IC 卡没有更改默认密码，攻击者可以直接使用默认密码来尝试接入 IC 卡，常见的默认密码有：

ffffffffffff 、 000000000000 、 a0a1a2a3a4a5 、 b0b1b2b3b4b5 、 aabbccddeeff 、

4d3a99c351dd、a982c7e459a、d3f7d3f7d3f7、14c5c886e97、87ee5f9350f、a0478cc39091、33cb6c723f6、fd0a4f256e9、fzzzzzzzzzz、a0zzzzzzzzzz

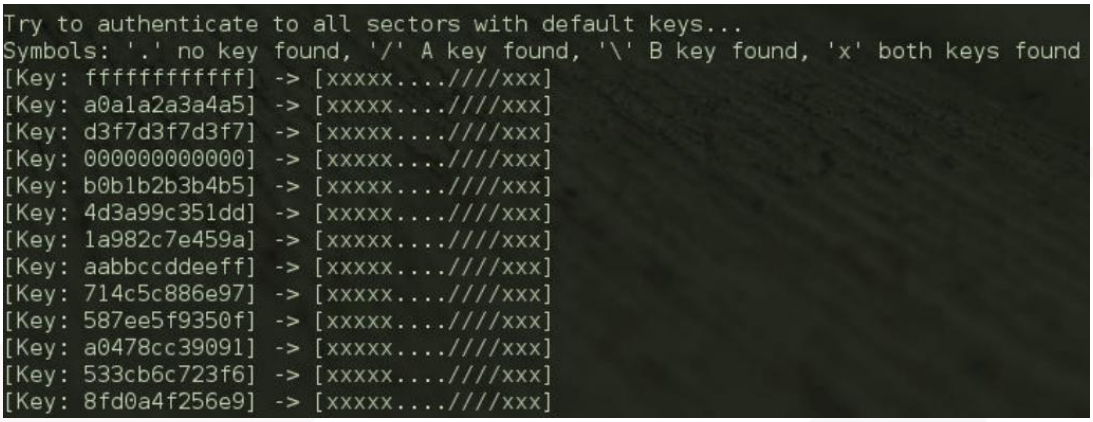

图 3-5 默认密码破解

2) Nested Authentication 攻击

Nested Authentication 攻击是在已知任意一个扇区密钥的情况下，攻击得到其他加密扇区密钥的一种攻击手法。从原理上来说，这种攻击并不是直接破解出密钥，而是通过获取已知加密随机数的情况下，极大地缩短破解密钥的时间，增加密钥破解的可能性。主要破解工具为 mfoc 和 mfcuk（主要用于全加密卡）。

3.2.3 卡数据破解与篡改案例

案例如下[6]

破解 IC 卡,最重要的就是把 IC 卡的数据破解出来，破解的方法,比较普遍的是用 ACR122U，ACR122U NFC 读写器是一款基于 13.56 MHz 非接触（RFID)技术开发出来的连机非接触式智能卡读写器。

解析完一张卡。PM3（PM3 可以在水卡、公交卡、门禁卡等一系列 RFIDNFC 卡片和与其相对应的机器读取、数据交换的时候进行嗅探攻击，并利用嗅探到的数据通过 XOR 校验工具把扇区的密钥计算出来，当然 PM3 也能用于破解门禁实施物理入侵。）反馈数据：

sec	key A	res	key B	res
000	583c7bed6262	1	9aba2c965997	1
001	583c7bed6262	1	9aba2c965f95	1
002	000000000000	0	9eb62cea5993	1
003	087737859406	1	9eb624ea5b8d	1
004	087737859406	1	9aaa24ee598f	1
005	087737859406	1	9aaa24ee578d	1
006	583c7bed6262	1	96ae24eaa9b3	1
007	087737859406	1	96ae3ceaabb5	1
008	583c7bed6262	1	aaaa3cf6a9b7	1
009	087737859406	1	aaaa3cf6afb5	1
010	bf0eab4eedcd	1	aed63cfaa9b3	1
011	be0faa4feccc	1	aed624faabbd	1
012	b908ad48ebcb	1	000000000000	0
013	b809ac49eaca	1	aada24feb7bd	1
014	000000000000	0	b6de24fab9b3	1
015	ba0bae4be8c8	1	000000000000	0

图 3-6 PM3 反馈的数据

得出各个扇区的密码以后 Dump（数据导出、转存成文件或静态形式。）导出来。进行分析，结果如下

214444 为卡号，用红框标出来的是名字和所对的 16 进制，下面的红框就是储存金额。

对多个不通的金额进分析，得到如下结果：

C8 64 是金额

64 c8 换成十进制就是 25800 即金额 258.00

65 EA 是校验码

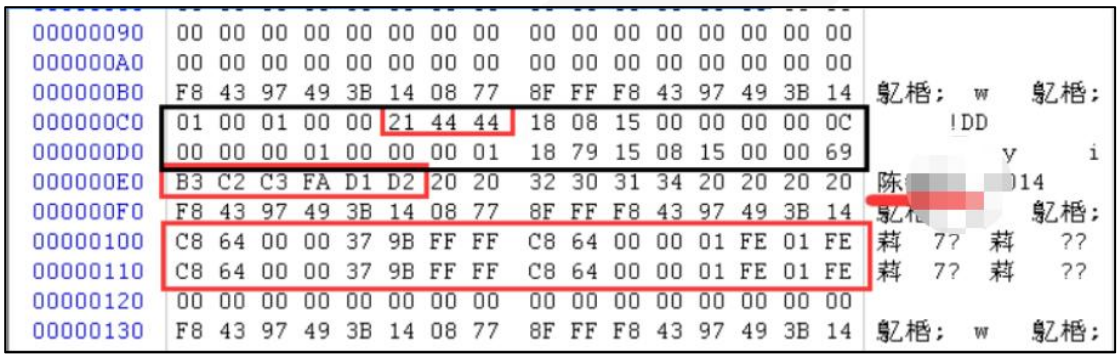

图 3-7 导出数据进行篡改金额

3.3 网络欺骗攻击

3.3.1 网络欺骗攻击简介

在日常生活中，我们经常会遭遇网络欺骗攻击。攻击者通常通过社会工程学进行攻击，利用人的本能反应、好奇心、信任、贪婪、侥幸等心理欺骗用户进行支付。

3.3.2 网络欺骗攻击原理分析

常见的攻击方式主要有以下几种：

1) 仿冒网站钓鱼

攻击者大量发送欺诈性邮件或短信，多以中奖、采购、对帐等内容引诱收件人在在仿冒网站中填入金融账号和密码，或是以各种紧迫的理由要求收件人登录攻击者构造的恶意网页提交用户名、密码、身份证号、信用卡号等信息，继而盗窃受害者资金。

2) 电信诈骗

电信诈骗是指通过电话、网络和短信方式，编造虚假信息设置骗局，对受害人实施远程、非接触式诈骗，诱使受害人打款或转账的犯罪行为。攻击者通过冒充他人，仿冒、伪造各种合法外衣等手段获取受害者信任，如冒充公检法、商家公司厂家、国家机关工作人员、银行工作人员等各类机构工作人员。利用冒充招工、刷单、贷款等事由对受害者进行诈骗，迫使受害人转账。

3.3.2 网络欺骗攻击案例

1) 仿冒网站钓鱼案例

攻击者会提前准备恶意网站，网站通常以获取信用卡账号、失效日期、CNV 码为主，使用诱惑引导性质的话术，将恶意网站发送给用户，安全意识薄弱的群体一般会中招。

图 3-8 网络钓鱼邮件

图 3-9 伪造劳动补贴通知

图 3-10 ETC 失效短信伪造

图 3-11 伪造 ETC 网站

图 3-12 伪造 ETC 网站

2) 电信诈骗案例

攻击者通常准备诱惑性质的工作信息，以及专业的话术，引诱群众上当受骗，丢失钱财。因大部分群众防诈骗意识较强，所以诈骗分子主要诈骗手段有两种，一是铺设大量广告，在各种微信群或者网页散布消息，主动联系参与的一般就是容易被骗的。二是通过网上泄露的个人信息，精准电话诈骗，以违法出入境、违法转账、快递丢件等术语，欺骗受害人转账。

图 3-13 伪造招聘信息

3.4 线下欺骗攻击

3.4.1 线下欺骗攻击简介

线下欺骗攻击主要是以物理手段使正常群众或经营者钱财受损，近年来频发线下欺骗攻击，具有代表性的两种攻击方式：商户收付款码伪造、纸质优惠券伪造。

3.4.2 线下欺骗攻击原理分析

1) 商户收付款码伪造

移动支付具有诸多优势，比如保证了支付的相对安全性、避免收到假钞、方便快捷、节省付款时间、提升商家运营效率等，但是提供方便的同时也为犯罪分子打开了方便之门。近年来，

就出现了替换电子支付二维码的新型盗窃方式，通过二维码生成器伪造收款码或者直接使用盗窃者自身的二维码，对商家的二维码进行替换，如若商家对账不及时可能会造成一定的损失。

2) 纸质优惠券伪造

纸质优惠券是由发券人印制，可在特约商户消费时享受指定产品优惠、满减等优惠活动的纸质券。通常情况下伪造的难度相对较低，但是可以带来较大收益，只要该优惠券未过期，收银员也没有觉察出异常的话，攻击者可以通过该方式减免一些支付金额，给商家造成财产损失。

3.5 支付身份伪造

3.5.1 支付身份伪造简介

交易身份伪造主要是指通过系统设计缺陷，对支付账户、收货（款）的用户身份进行伪造以达到欺骗交易的目的，主要有账户伪造和生物识别伪造。

3.5.2 支付身份伪造原理分析

1) 账户伪造

账户伪造主要是通过网络钓鱼、渗透攻击、欺骗等方式获取受害者账户权限进行支付。较为常见的便是银行卡盗刷、恶意代替支付等。

2) 生物识别伪造

生物识别技术主要是指通过人类生物特征进行身份认证的一种技术，这里的生物特征通常具有独一的（与他人不同）、可以测量或可自动识别和验证、遗传性或终身不变等特点，包括了指纹识别、静脉识别、虹膜识别、视网膜识别、面部识别、DNA 识别等。其中指纹识别、面部识别广泛应用在我们的日常支付交易中，如果实现技术不完善就可能导致一定的财产损失。

3.5.3 支付身份伪造案例

1) 账户伪造案例

账户伪造一般发生在网络欺骗之后，当攻击者获取受害人账户信息后，会对银行卡、信用卡、其他资产账户进行盗刷。

2) 支付身份伪造案例

对于支付身份伪造，这里以某品牌快递柜出现过的刷脸取件漏洞为例，由于人脸识别的技术缺陷无法辨别是否为真人，导致可以通过人像图片进行刷脸取件（现已修复），实现身份伪造。

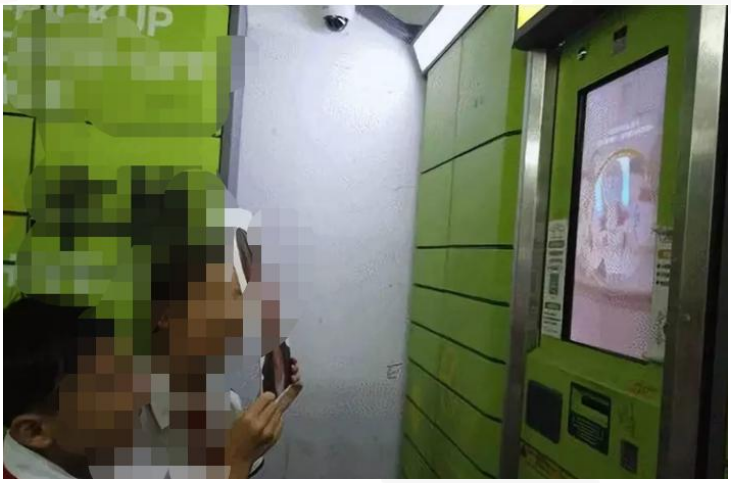

图 3-14 生物识别伪造

3.6 支付逻辑绕过

3.6.1 支付逻辑绕过简介

支付逻辑绕过主要是由于程序设计不合理，导致逻辑设计缺陷，攻击者可以利用缺陷对支付环节造成影响，主要包括数据不同步、优惠券反复使用、支付环节绕过等。

```
//coupon优惠券数量
if(coupon>0){
  totalAmount = (Amount*num)-20;
  sql = "insert into order(`id`,`num`,`totalAmount`)values('2021xxx01','2',totalAmount)";
  //执行sql语句，写入到数据库，生成订单
  //生成之后没有对优惠券数量减1，造成优惠券可重复使用
}
```

图 3-15 代码示例

3.6.2 支付逻辑绕过原理分析

在生成订单时，应当判断优惠券数量，生成一个订单之后要把对应使用的优惠券消除，不能在下次生成订单时使用。下图源码中，只判断了优惠券是否大于 0，如果大于 0，直接就进行插入数据库的操作，并且在插入数据库之后没有把对应的数量减 1，造成优惠券一直可以使用。

```
//coupon优惠券数量
if(coupon>0){
  totalAmount = (Amount*num)-20;
  sql = "insert into order(`id`,`num`,`totalAmount`)values('2021xxx01','2',totalAmount)";
  //执行sql语句，写入到数据库，生成订单
  //生成之后没有对优惠券数量减1，造成优惠券可重复使用
}
```

图 3-6-1 代码示例

3.6.3 支付逻辑绕过案例

部分交易平台对优惠券的使用校验不合理，未校验优惠券有效性，攻击者可以重复使用优惠券。如图 3-16 和图 3-17 在使用优惠券的情况下重复提交订单时，可对所有订单均使用优惠券进行减免。

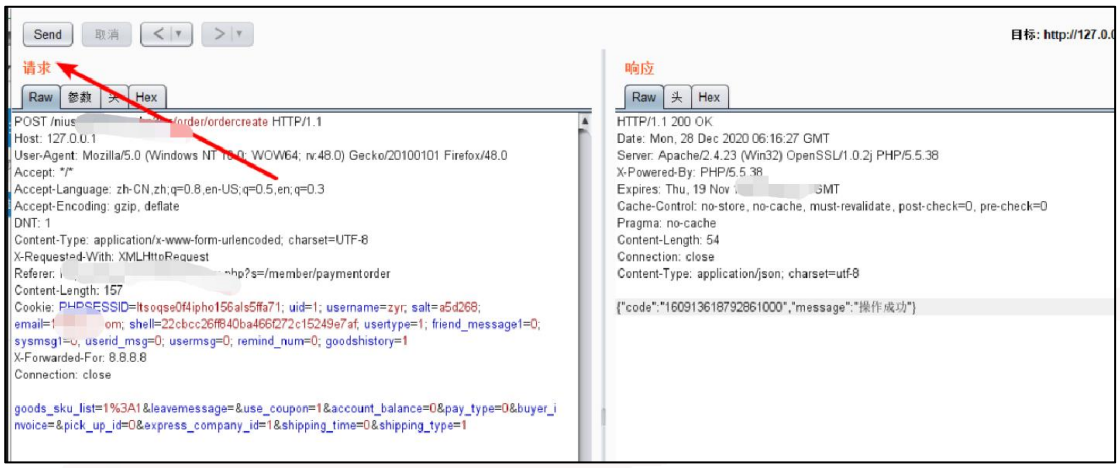

图 3-16 重复发送数据包

图 3-17 下单结果展示

3.7 数据不同步

3.7.1 支付数据不同步漏洞简介

数据不同步主要是由于并发时数据丢失修改、不可重复读、读“脏”数据或其他逻辑设计问题等造成多平台间数据不同步从而导致支付漏洞。

3.7.2 支付数据不同步漏洞原理分析

在退单时，没有对订单的状态做判断，并且每做一次优惠券的数量都会加 1，导致在不同平台进行退单时，都会更新一下订单的状态，然后退一个优惠券。

正常的操作应该在每次退单之前查询一下数据库，查处订单的状态，然后再去做下一步操作。

```
if(applets==True){
  //微信小程序退单 state 代表订单状态 -1 代表退单
  //执行sql语句，更新订单状态
  sql = "update order set state='-1' where id='2021xxxx01'";
  //优惠券数量加 1
  coupon += 1;
}

if(app==True){
  //APP退单 state 代表订单状态 -1 代表退单
  //执行sql语句，更新订单状态
  sql = "update order set state='-1' where id='2021xxxx01'";
  //优惠券数量加 1
  coupon += 1;
}
```

图 3-18 代码展示

3.7.3 支付数据不同步案例

近期较为经典的案例便是某快餐平台的支付漏洞，由于某快餐平台 APP 客户端和微信客户端之间数据不同步，攻击者通过骗取兑换券或取餐码，给某快餐平台公司造成一定的损失。具体漏洞逻辑如图 3-19：

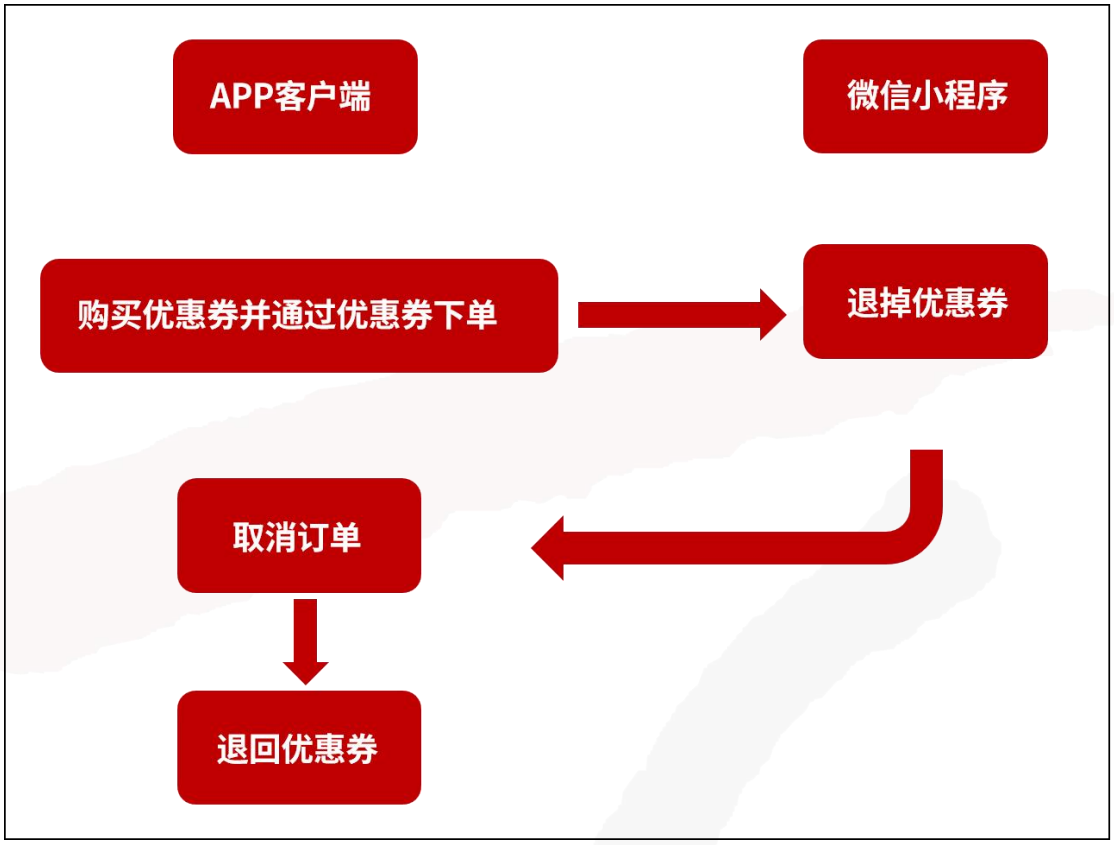

图 3-19 支付数据不同步

3.8 支付数据篡改

3.8.1 支付数据篡改简介

支付数据篡改主要是未对业务数据的完整性和一致性进行保护，未校验用户客户端与服务端、业务系统接口之间数据传输的一致性。导致攻击者可以通过对订单数据包中的金额、数量、支付账户、商品 ID、余额、返回数据包等进行修改。

3.8.2 支付数据篡改原理分析

常见的攻击方式为篡改支付金额、篡改数量、篡改支付账户、篡改支付商品、篡改余额、篡改返回包、整数溢出等。具体数据流图见 3-20。

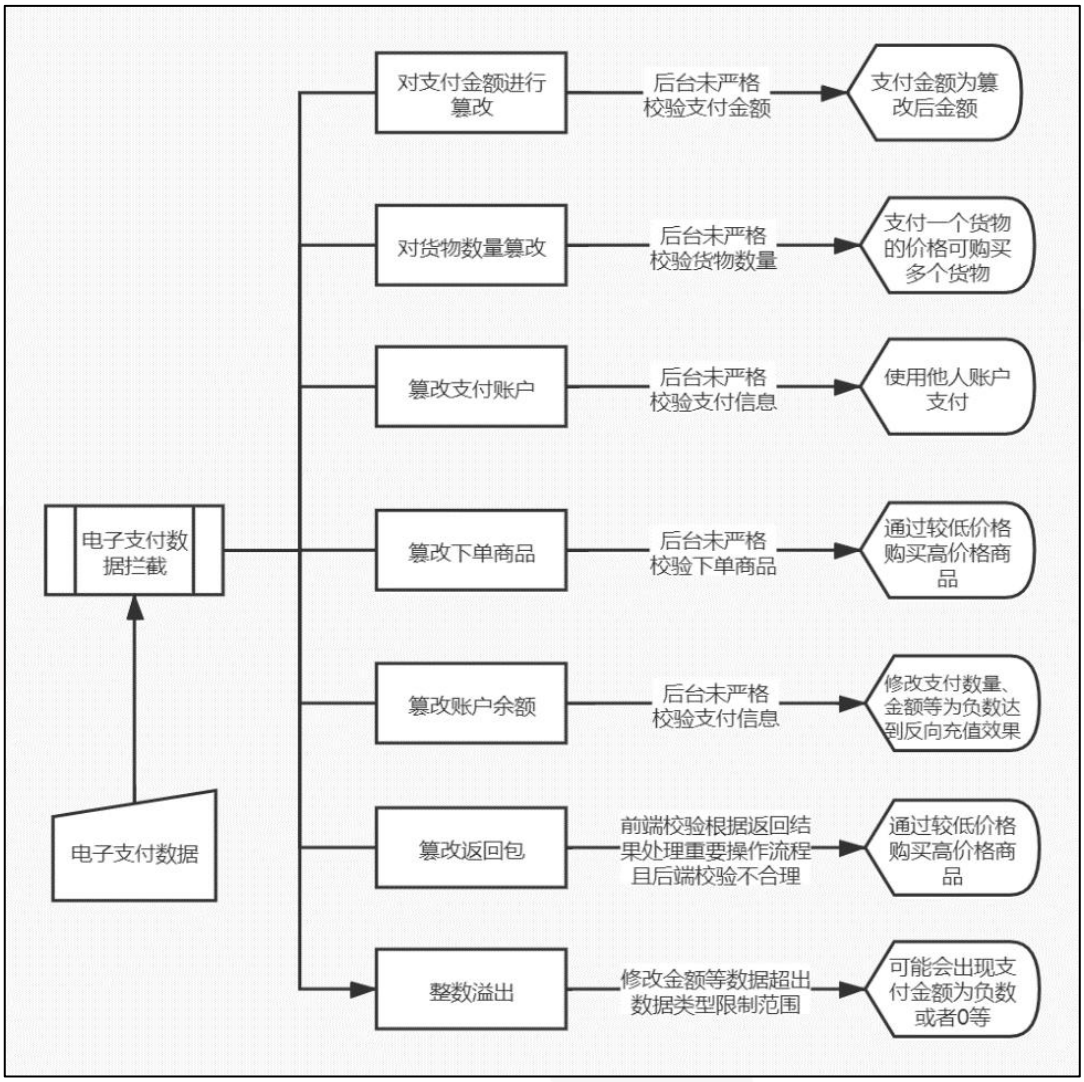

图 3-20 支付数据篡改的数据流图

其中篡改支付金额、货物数量、支付账户、下单商品、篡改账户余额的原理是通过抓包软件对下单过程中的数据进行分析，拦截相关数据包并对数据包中的数值修改，修改后发送给服务端，由于服务端对数据校验不充分，导致攻击者通过更低的价格获得更多更有价值的商品；篡改返回包数据造成支付漏洞主要是因为前端根据返回结果处理重要操作流程且后端校验不合理，前端常用的校验字段有 true、1、ok、success、200 等；整数溢出是由于有的交易在开发当中，商品的金额会用 int 型来定义，其中 int 的最大值为 2147483647，当数值 int 值超过最大值后，结果会出现改变，如变成负数等，图 3-21 为整数溢出原理的一个简单案例。

```
root@lys:/tmp# cat test.c
#include <stdio.h>
#include <stdlib.h>

void main(){
        int a = 2147483647;
        printf("%d\n",a+1);

}
root@lys:/tmp# ./test
-2147483648
```

图 3-21 整数溢出原理

3.8.3 支付数据篡改案例

1) 篡改支付金额案例

该案例是在支付过程中，由于后端未对支付金额进行校验导致可以通过篡改数据包中的支付金额达到以低价格支付高价格商品的目的。详见图 3-22、图 3-23、图 3-24。

选择相应商品下单：

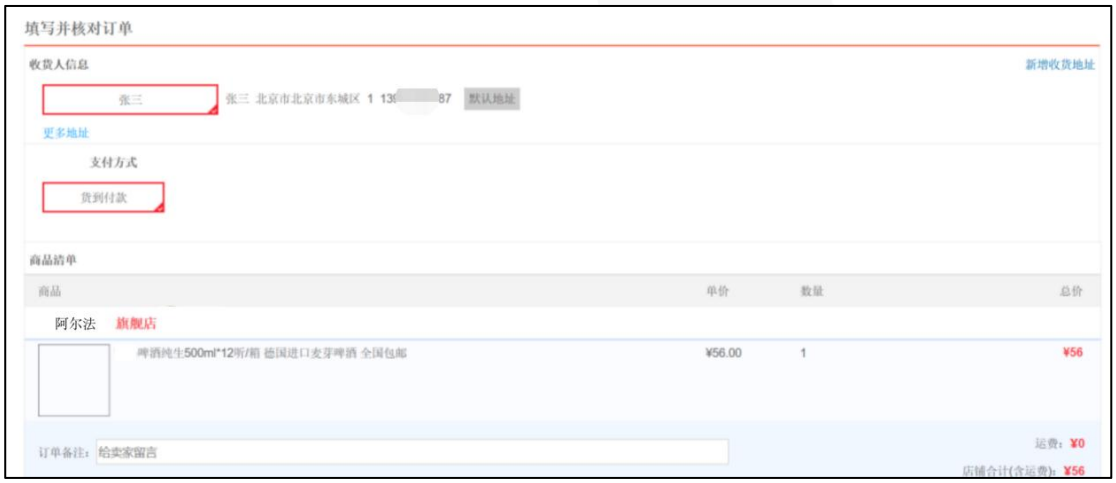

图 3-22 下单

修改商品金额：

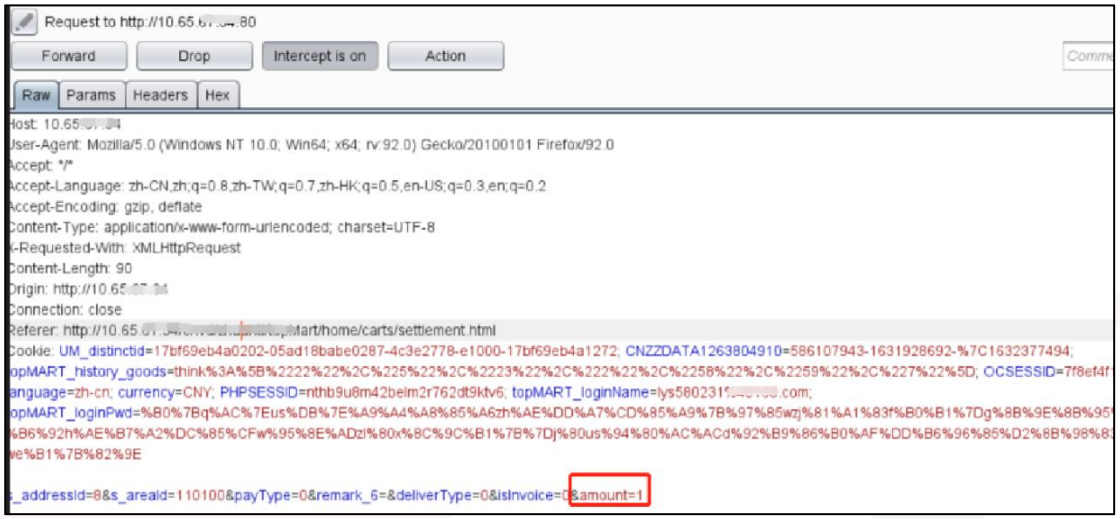

图 3-23 修改金额

查看订单：

图 3-24 订单成功提交

2) 篡改数量案例

该案例是在支付过程中，由于后端未对商品数量进行校验导致可以通过篡改数据包中的商品数量以购买一份商品的价格，购买多个商品。详见图 3-25、图 3-26、图 3-27。

选取商品下单：

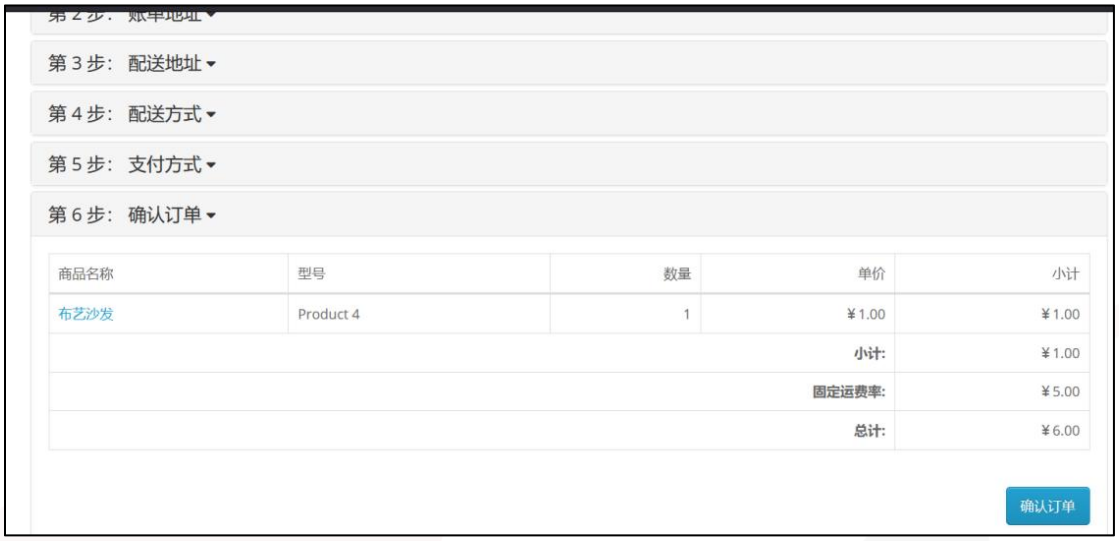

图 3-25 提交订单

篡改下单数据包：

图 3-26 修改产品数量

查看订单：

图 3-27 查看历史订单结果

3）篡改支付商品案例

该案例是在支付过程中，由于后端校验不严格导致可以修改商品 token，以低价格支付高价格商品。详见图 3-28、图 3-29、图 3-30。

选取低价商品下单：

图 3-28 下单低价格产品

获取高价商品的 token 值并对低价商品 token 篡改：

图 3-29 篡改产品 token

查看订单结果：

图 3-30 获取订单结果

4) 篡改余额案例

该案例由于未对支付时金额进行校验，可以通过在下单时将支付金额修改为负数使得账户在最中结算时导致余额增加。

查看账户余额为 0 元：

图 3-31 原始账户余额

下单通过预存款支付：

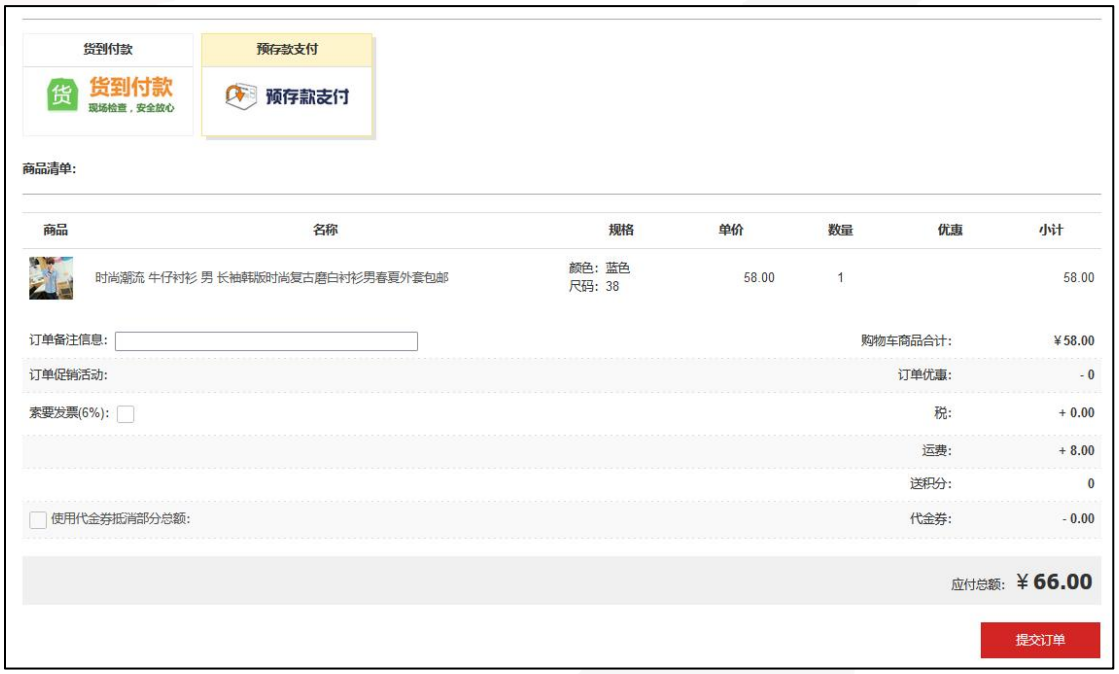

图 3-32 下单采用预存款支付

修改支付数据包中的金额为负数：

图 3-33 修改支付金额为负数

查看余额增加：

图 3-34 账户余额增加

5）篡改返回包案例

该案例由于校验下单是否成功只通过返回码进行校验，可以尝试使用预存款下单支付商品，由于账户余额为 0，导致无法支付，同时通过修改返回包响应码为 200 进行绕过，达到下单成功的效果。

图 3-35 下单拒绝支付

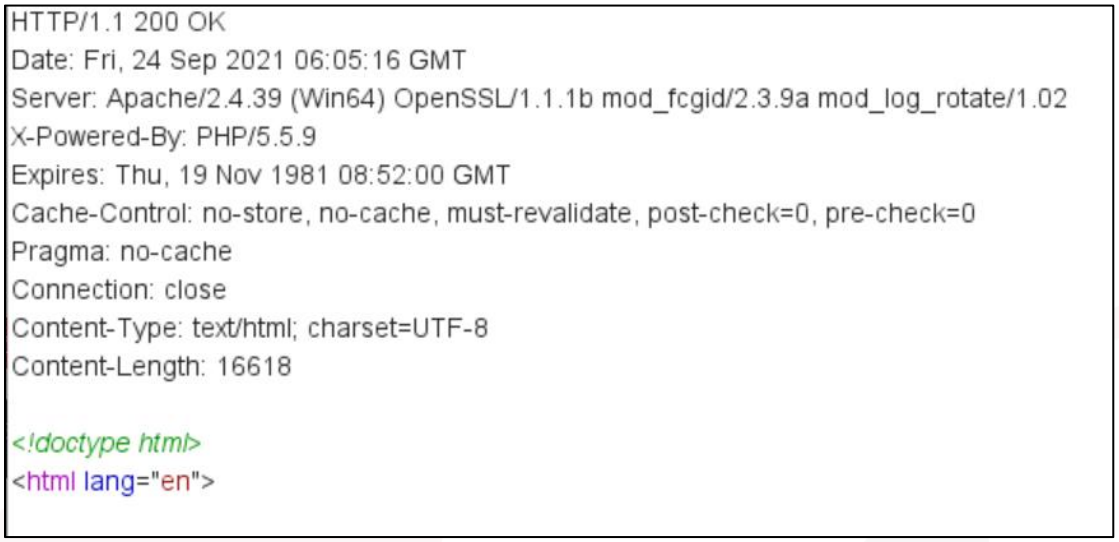

图 3-36 篡改返回包

图 3-37 下单成功

3.9 条件竞争漏洞（并发）

3.9.1 条件竞争漏洞简介

条件竞争支付漏洞主要是因多线程并发没有实时、有效的处理各种状态导致。攻击者对下单数据进行并发请求时，可以该利用漏洞，使用一笔订单的金额完成多笔订单，导致商家受到损失。

3.9.2 条件竞争漏洞原理分析

新用户进行购买时，会存在优惠价格，在代码中，没有在生成订单时，就把用户状态更新，导致可以使用多个手机，生成多个新用户的订单，在支付时同时支付，就会造成并发漏洞。正常应该控制用户支付的线程，在生成订单时就将用户状态更新，在支付之后重新查询数据库，查询

用户是否只使用了一次优惠。

```
if(session['user']!=null){
  //用户已经登录
  sql = "select * from user where id="+session['id'];
  //查询数据库，处理数据阶段
  .....
  //判断用户是否为新用户
  if(reslut['state'] == 0){
    //生成新用户优惠订单
    sql1 = 'insert into order(`id`,'amount',`state`) values('2021xxxxx01','100','0')';
    //数据库处理操作
    .....
    //用户支付，如果支付成功
    if(pay_state==True){
      sql2 = 'update user set state=1 where id='+session['id'];
    }
  }
}
```

图 3-38 代码分析

3.9.3 条件竞争漏洞案例

新用户首次购买优惠，可同时生成多个新用户的订单，再进行支付，生成多少个订单就会优惠多少次。

首次购买是 1 元 1 年，平台限制单用户只能参与一次活动。

图 3-39 首次购买

使用两部手机同时支付，可以绕过限制，2 元生成 2 年的会员。

图 3-40 首次购买会员，生成 2 年的会员

3.10 拒绝服务

3.10.1 拒绝服务漏洞简介

支付场景的拒绝服务攻击主要有两种，一种是由于系统本身的防护不足，攻击者可以进行拒绝服务攻击，导致支付系统无法访问。另一种是通过某种方式使得支付账户锁定无法支付，比如利用某些银行卡密码输入三次错误便会锁定的机制，攻击性可以利用该机制使用户无法支付，影响用户体验。

3.10.2 拒绝服务漏洞原理分析

用户在支付时，会有失败次数限制，如果同一用户在连续三次失败之后，会禁止此用户进行支付，造成拒绝服务攻击。

```php
//支付状态
$pay_state = False;
//支付尝试次数
$pay_num = 0;
//失败次数小于3
if($pay_num<3){
  //密码与用户输入的密码不同
  if(password!=$_POST['password']){
    $pay_num +=1;
  }else{
    $pay_state = True;
  }
}else{
  //失败次数过多，禁止支付
  return False;
}
```

图 3-41 代码分析

3.10.3 拒绝服务漏洞案例

登陆处，多次使用同一个手机号进行登陆，每次都输入错误的验证码，系统会将此手机号进行锁定。导致正常用户登陆时，也登陆不上此系统。

图 3-42 验证码

多次验证，导致被锁定

图 3-43 拒绝服务数据包

4. 安全风险防范措施

4.1 卡复制以及卡数据破解与篡改防御

用户在刷卡前后，保证卡片不离开自己的视线，当发现自己的卡片被收款人员异常操作时，立即停止刷卡。刷完卡后，保证卡片会立即归还给自己，防止卡落入攻击者手中。除此之外，还需要注意卡自身的安全，比如：生成唯一的卡号，可以自研算法生成卡号；将数据写入卡中前提前进行加密，然后再写入卡中；IC 卡设置成读的时候不须要密码，里面写的时候验证密码；使用更为安全的 CPU 卡。

4.2 网络欺骗防御

网络欺骗类的防御需要用户提高自身的安全意识，相应的防范措施主要有：平时不要相信来历不明的邮件短信等，尤其是需要用户提供个人信息，如银行卡号，密码等的邮件短信；在网上浏览一些金融平台的网站前，要仔细核对网站域名是否正确；将自己的手机号与银行卡进行绑定，如果收到自己银行卡异常消费的提示时，立即进行核对；密码不要重复，不同的银行卡设置不同的密码。

4.3 线下欺骗防御

商家需要定期检查自己提供给顾客的收款信息，如二维码等，防止被恶意替换。

对于用户提供的优惠券等信息，首先确认信息无误再允许用户使用，防止用户使用假冒的优惠券骗取优惠金额。

4.4 支付身份伪造防御

平时不要随意透露自己的支付信息，并时刻留意自己银行账户的余额，发现异常及时冻结账户并报警。支付时使用多因素验证，并不要将自己的指纹等信息透露给其他人。

4.5 支付逻辑绕过防御

对于这类漏洞，需要网站开发人员在开发过程中仔细考虑支付过程中的每一个步骤，前后支付过程的关联等。比如针对优惠券重用的漏洞，应该设置判断语句，当支付时优惠券的数量大于规定的数量时，应该禁止用户交易；对于支付绕过类漏洞，应该在每一个步骤前设置检查操作，只有用户完成上一步的支付环节之后才能进行下一步的环节。所有环节进行完之后，再次查询数据库，对数据库中的商品数量和金额优惠券等信息进行校验，若不匹配将数据回滚。

4.6 支付数据不同步防御

不同的平台，使用同一个业务接口，防止因为接口的不同造成数据不同步。

优化程序算法以及数据库查询语句，提高处理速度。除了使用同一个接口这种防御方式之外，还可以增加登录状态检测，只能让用户在同时在一个客户端登陆，当用户尝试在另一个客户端登录时，禁止该用户登录，不过这种方式可能不利于用户体验。

4.7 支付数据篡改防御

对传输到网站服务器端的数据进行加密以及签名校验，以防止用户抓取数据进行篡改。数据传输到后端之后，与后端数据库中的数据进行比对，比如商品价格，商品数量是否与数据库中的数据一致，不能通过用户从前端传入的数据值进行支付操作，而是要根据先前数据库中已经存入的值进行支付。

4.8 条件竞争防御

条件竞争类漏洞的防御措施主要有：设置回滚机制，以及对数据库操作加锁；对于拥有对平台的程序，在不影响业余以及用户使用的前提下，最好设置同一个用户每次只能登陆一个平台。

4.9 拒绝服务防御

拒绝服务类攻击，主要从两方面入手，对于系统本身层面的拒绝服务攻击，可以增加 CDN 或者其它防护软件进行防护;对于程序逻辑层面的拒绝服务攻击,如用户输错三次密码无法支付，可以对当前输入密码的用户进行身份校验,防止恶意用户利用他人银行卡故意输错密码造成他人无法支付。

5. 参考文章

[1] 中国人民银行.电子支付指引（第一号）[DB/OL].(2005-10-26)[2023-03-06].http://www.gov.cn/gongbao/content/2006/content_375800.htm.

[2] 袁小康、韦夏怡.经济参考报[EB/OL].(2023-02-22)[2023-03-06].https://www.cs.com.cn/lc/202302/t20230222_6324849.html.

[3] Siamak Solat.Security of Electronic Payment Systems: A Comprehensive Survey[DB/OL].(2017-01-17)[2023-03-06].https://arxiv.org/abs/1701.04556.

[4] stripe.Card authentication and 3D Secure[EB/OL].[2023-03-06].https://stripe.com/docs/payments/3d-secure

[5] 邱烈.如何用 NFC 门禁卡模拟器让手机模拟门禁卡[EB/OL].(2016-05-25)[2023-03-06].https://jingyan.baidu.com/article/fa4125ace018f328ac709228.html.

[6] Merlin.关于 IC 卡的破解与写入[EB/OL].(2017-07-21)[2023-03-06].https://www.52pojie.cn/thread-625863-1-1.html.