逻辑漏洞

问题：
公司新上线了一个系统，需要你对它进行测试，
如何从业务逻辑的层面对它进行测试？

学院介绍

学院宗旨：专注网安人才实战技能培养

学院官网：https://edu.hetianlab.com/

合天网安实验室：https://www.hetianlab.com/

主打课程：

《web安全》：OWASP TOP 10漏洞原理及测试

《渗透测试》：渗透测试流程及工具的使用

《安全开发》：用python写一个综合的扫描器

《CTF-PWN》：CTF中的PWN相关

《CTF-WEB》：CTF中WEB相关

目录
CONTENTS

/01 越权

1.1 越权简述

顾名思义，越权漏洞就是由于设计上的缺陷对应用程序的权限做的不好。通俗点来说，就是用户A可以通过某种方式查看到用户B的个人信息，或者可以查看管理员C的一些相关信息。

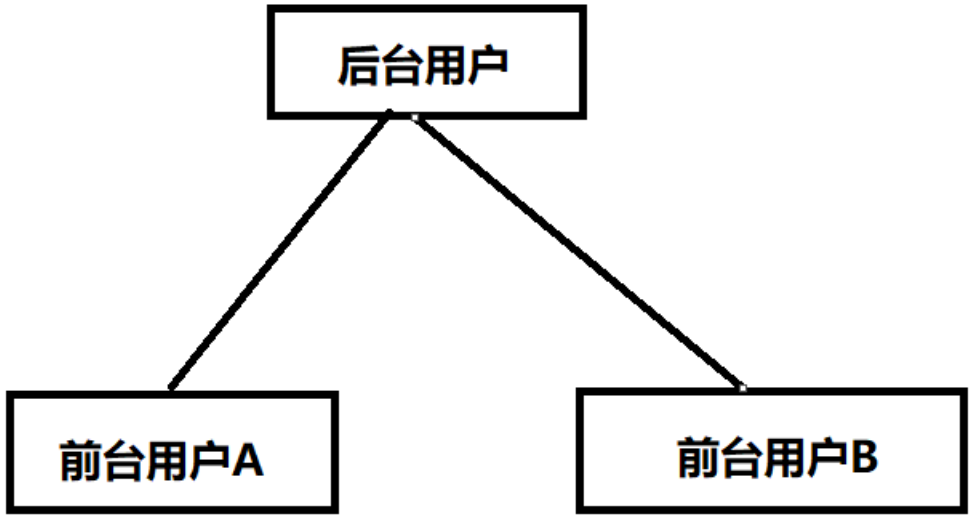
1.2 漏洞成因

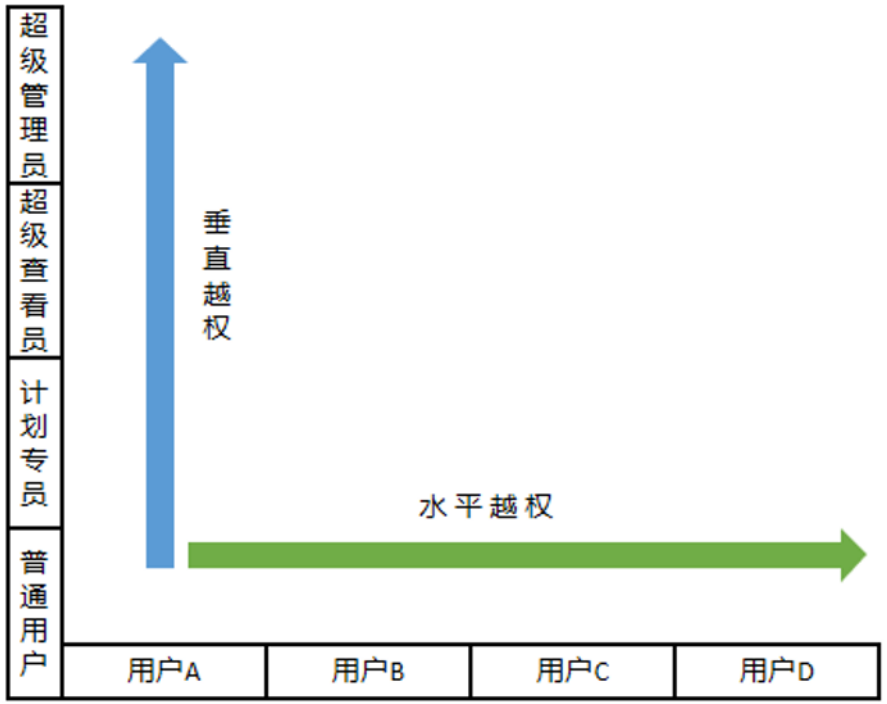
越权漏洞的成因主要是因为开发人员在对数据进行增、删、改、查询时对客户端请求的数据过分相信而遗漏了权限的判定

1.3 分类

水平越权：权限不变，身份改变

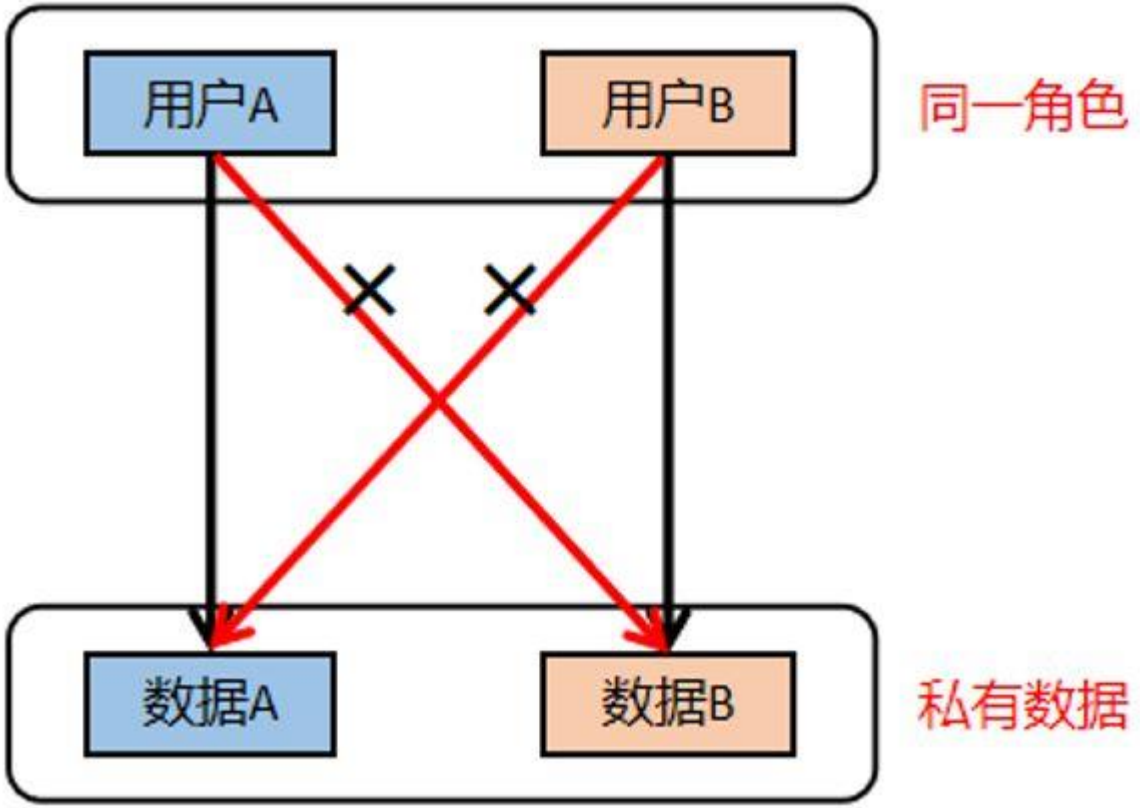
垂直越权：身份不变，权限改变





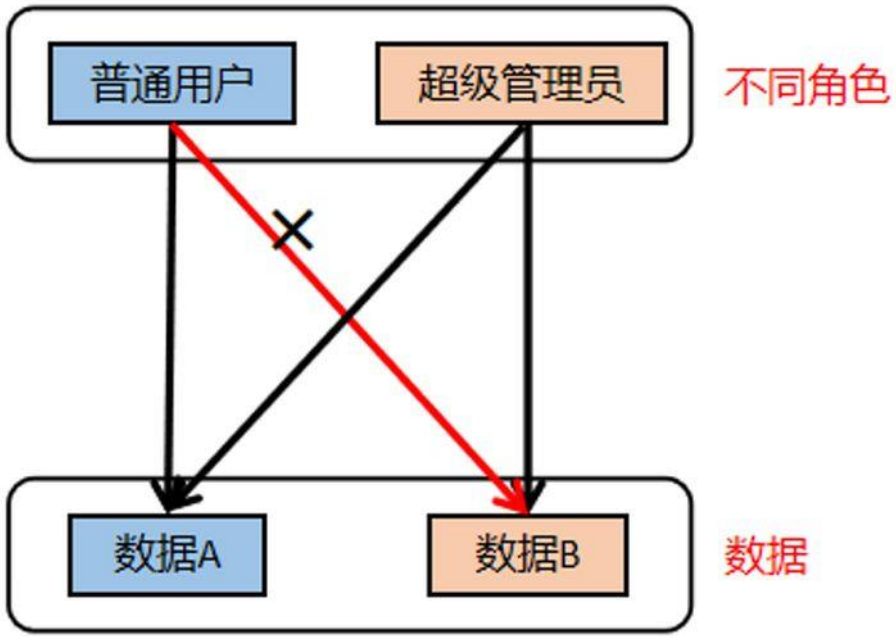
1.3.1 水平越权

水平越权漏洞是可以操作同一个层次的账号权限之间进行操作，以及访问到一些账号敏感信息，比如可以修改任意账号的资料，包括 查看会员的手机号，姓名，充值记录，撤单记录，提现记录，注单记录等等。



1.3.2 垂直越权

垂直越权漏洞可以使用低权限的账号来执行高权限账号的操作，比如可以操作管理员的账号功能。隐藏式后台也属于垂直越权的一种。



1.4 越权漏洞挖掘示例

以合天网安实验室创建实验来举例：

1. 首先观察自己添加实验的包，未添加实验参数是 ec，添加完实验是 ce

2. 观察评论，可以发现每个人都有一个 ceid 来判断，仔细观察可以发现这个 ceid 对应的就是自己的实验认证参数

思路：

1. 能不能越权创建实验
2. 能不能越权销毁实验
3. 能不能越权进入别人的实验环境
4. 能不能越权评价
5. 能不能越权查看指导书
6. 能不能越权问答

.....

1.5 修复方案

1、基础安全架构，完善用户权限体系。要知道哪些数据对于哪些用户，哪些数据不应该由哪些用户操作；

2、鉴权，服务端对请求的数据和当前用户身份做校验；

3、不要直接使用对象的实名或关键字。

4、对于可控参数进行严格的检查与过滤！

/02 支付逻辑漏洞

2.1 背景

随着互联网的发展，生活变得越来越方便，往日需要我们跋山涉水购买的物品，如今只要在网上下个订单就可以送到家中。网上购物给我们带来极大的便利的同时也带来了安全风险，而支付漏洞就是影响我们网上购物的安全风险之一。

2.2 产生原因

开发人员往往会为了方便，直接在支付的关键步骤数据包中直接传递需要支付的金额。而这种金额后端没有做校验，传递过程中也没有做签名，导致可以随意篡改金额提交。

2.3 如何测试逻辑漏洞

1、在购买产品过程中修改产品数量、价格；

2、在支付时修改总价格或者优惠价格；

3、订单生成后，编辑订单把A商品的价格改成B商品的价格，实现低价支付。测试时，修改数量、单价，优惠价格参数为负数、小数，无限大，看是否能生成订单，能生成进入支付即说明存在逻辑漏洞了。

2.4 支付逻辑漏洞常见类型

- 修改购买数量
- 修改支付价格
- 修改支付对应的商品
- 修改支付的状态
- 修改附属优惠、领取优惠
- 测试数据包未删除

2.4.1 修改购买数量

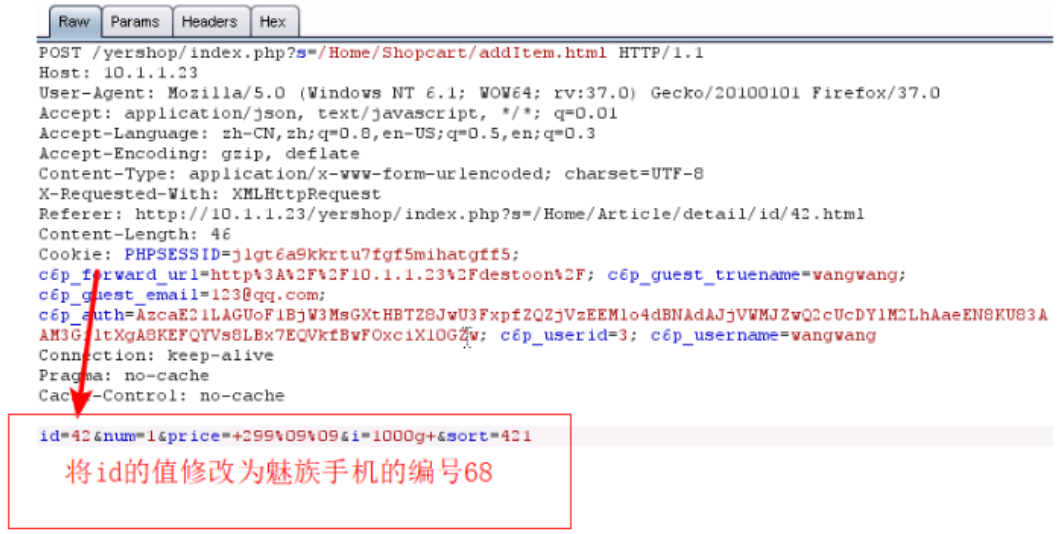
在进行支付订单的时候，可以修改物品的数量来进行操作，可以通过支付一件的价格购买多件，或者修改成负数进行增加资金

2.4.2 修改支付价格

在支付当中，购买商品一般分为三步骤：订购、确认信息、付款，在这三个步骤中都有可能存在漏洞，金额可以尝试修改小额或者修改负

2.4.3 修改支付对应的商品

通过修改商品对应的 id 号，可以用低价购买高价格商品



修改此商品的id参数值为魅族手机的id号68，当继续发包时，传递的id参数，在数据库查询为魅族手机的商品名，而传递的price价格参数为苹果的价格。导致加入到购物车后显示的业务信息不一致。

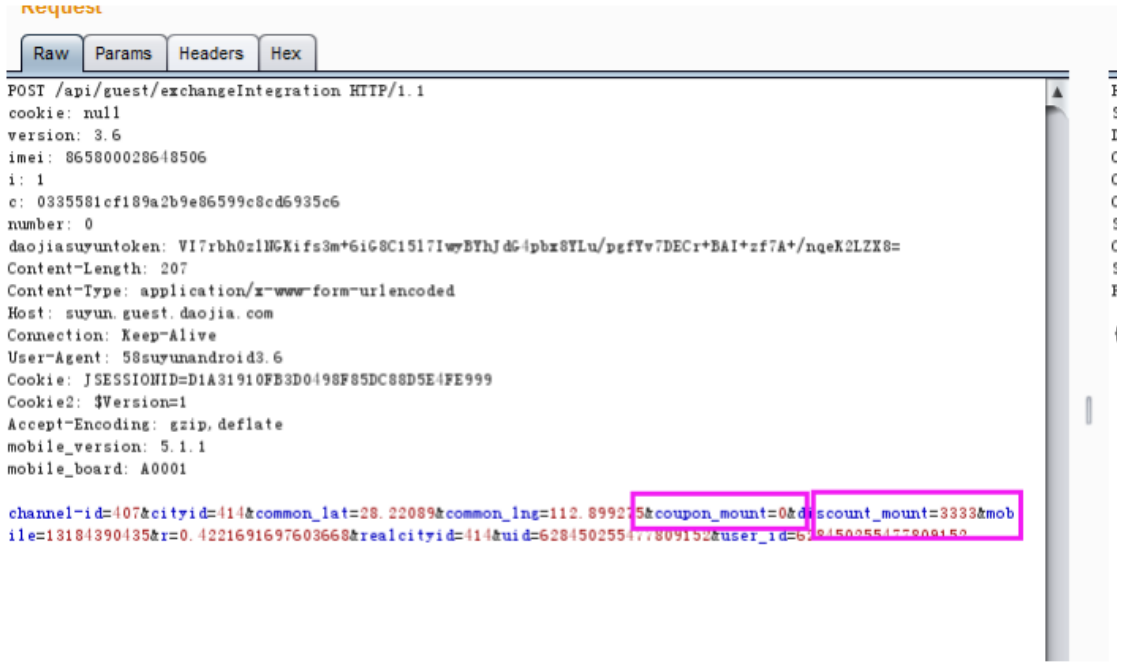
到网站购物车查看，发现只需要苹果的价格299元就可以购买到价格2268元的魅族手机，并且最后可以成功下单。

2.4.4 修改支付的状态

没有对支付状态的值跟实际订单支付状态进行校验，导致点击支付时抓包修改决定支付或未支付的参数为支付状态的值从而达到支付成功。

2.4.5 修改附属优惠/状态

比如一些商品有优惠价，优惠多少多少，那么在支付时抓包，修改这个优惠价就可造成支付问题的产生



2.5 修复方案

1、在后端检查订单的每一个值，包括支付状态；

2、校验价格、数量参数，比如产品数量只能为整数，并限制最大购买数量 ；

3、与第三方支付平台检查，实际支付的金额是否与订单金额一致；

4、另外，如果给用户退款，要使用原路、原订单退回。比如：退押金，按用户原支付订单原路退回；

5、MD5 加密、解密、数字签名及验证，这个可以有效的避免数据修改，重放攻击中的各种问题；

6、金额超过指定值，进行人工审核等。

感谢您的聆听

学习工具、资料及课程回放

扫码免费领取