php代码审计基础篇

第13课 业务逻辑（二）

漏洞介绍

越权漏洞

越权访问，这类漏洞是指应用在检查授权时存在纰漏，使得攻击者在获得低权限用户帐后后，可以利用一些方式绕过权限检查，访问或者操作到原本无权访问的高权限功能。在实际的代码安全审查中，这类漏洞往往很难通过工具进行自动化检测，因此在实际应用中危害很大。其与未授权访问有一定差别。目前存在着两种越权操作类型：横向越权操作(水平越权)和纵向越权(垂直越权)_操作

水平越权：就是相同级别(权限)的用户或者同一角色不同的用户之间，可以越权访问、修改或者删除的非法操作。如果出现次漏洞，那么将可能会造成大批量数据泄露，严重的甚至会造成用户信息被恶意篡改。

垂直越权：垂直越权是不同级别之间或不同角色之间的越权；垂直越权又别分为向上越权与向下越权。比如，某些网站，像发布文章、删除文章等操作属于管理员该做的事情。假设一个匿名用户也可以做相同的事情，这就叫做向上越权；向下越权是一个高级用户可以访问低级用户信息。

支付漏洞

商城源码

支付漏洞属于逻辑漏洞的一种，是和支付的业务有关，支付业务中出现的逻辑漏洞全部属于支付漏洞

修改支付价格、修改支付状态、修改订单数量、修改优惠价优惠价格和使用限制、越权支付、无限试用L

订单数量的操作一般都是负数，买一个贵的，几个便宜的商品，然后贵的商品的价格为-1,于是乎这个贵的商品的价格就是个负数，比如-8999,然后我再买几个商品，加起来也是8999,那么计算总金额的时候就是-8999+8999 ==0,于是乎0元购买了

主要是通过抓包，比如你买一个电脑，标价6999,然后你发现数据包里面有6999的传参，然后我

改成了6.999,然后跳转到支付页面，我付了6.999将这个电脑买下，也可以把金额改为负数比如你购买一个1000的商品，然后又购买一个10块的商品，两个订单号不同，然后你抓包，将1000块支付发送的数据包的订单号改为10块，然后付了10块钱，发现商品买到手了

挖掘思路

水平越权测试方法主要就是看看能否通过A用户操作影响到B用户垂直越权的测试思路就是低权限用户越权使用高权限用户的功能比如普通用户可使用管理员功能。

支付

直接定位支付功能点，找文件看防护看参数

实例代码分析

cmseasy支付漏洞

LJCMS越权漏洞

谢谢观赏