登录

SecWiki技术分享——漏洞挖掘之逻辑漏洞

secwiki / 2017-04-12 03:59:40 / 浏览数 4465 安全技术 技术讨论 顶(0) 踩(0)

原文首发SecWiki微信公众号 未授权请勿转发

2017年4月10日，晚上9点，伴随着一阵琴声，secwiki的第二次技术分享大会正式开始。这次的主讲人是Blood_zer0，是一个去年开始活跃在部分src的白帽子，并且希望与

那些年错过的大雨，那些年错过的逻辑

有些时候，我们费尽心思找洞，各种套路都上用了，奈何甲方的安全做的太足，苦苦找了一天，最后却以失败收场。过了一天后，偶然看到别的白帽子在漏洞平台提交了一篇

什么是逻辑漏洞

Blood_zer0总结为：利用业务的设计缺陷，获取敏感信息或破坏业务完整。一般出现在任意密码修改（没有旧密码验证）、越权访问、密码找回、交易支付金额。其中越权访

安全测试阶段

发展经历了三个阶段。首先，最早的时候的漏洞测试是不分什么类型的测试的，也没有src这种组织，一般是"基于功能/性能"的安全测试，如压测，软件bug。之后才进入到

关注的原因

关注的原因有两点，一点是"Bypass一切防护设备"，另外一点是"没有很好的解决方案，比如再牛逼程序员都可能挖坑，互联网公司业务迭代太快等。回顾以往，Blood_zer0

如何挖掘逻辑漏洞

Blood_zer0指出，要测试一个网站的逻辑漏洞，首先应该知道它的各个业务的流程。如现在的一些p2p理财网站，首先是注册，然后是实名，之后领红包什么的，这是一个必

关于数据包，Blood_zer0指出，对于抓取的海量的数据包，我们更应该关注的是一些get，post请求的数据包，包括这些数据包里面的一些参数，如get里面的http头里面的

用到的一些工具

接下来Blood_zer0为我们介绍了几个在挖掘逻辑漏洞方面会用到的一些工具。

Burpsuite，这款工具是收费的，网络上也有破解版，并且网络上也有很多的使用教程，同学们将这个软件用好，对于渗透的帮助是很大的。

Fiddler，这款工具和Burpsuite相差不多，各方面也是非常的优秀，Blood_zer0指出，它和Burpsuite可能就是在爆破上差了点。

Charies，这款工具是收费的，网上也没有很好的破解版本，然后这个工具主要是针对Linux和Mac的一个抓包工具，功能上可能没有Burpsuit强大，但是大道至简，对于一些

Mitmproxy，这是一个python语言编写的抓包工具，并且是开源的。Blood_zer0建议我们可以抱着学习的态度去用这个工具，学习下它的设计理念，包括它的代码开发。

案例

案例（一）

Blood_zer0为我们分享了一个购物的优惠券使用的案例。

环境：购物时拥有优惠券，但是优惠券不可用！简单的来说，就是拥有的这个优惠券是A店铺的，只能用在A店铺，不能用在B店铺。

条件1：当我不是一个白帽子，是一个普通用户。

姿势：在这个A店铺购买商品，给自己买或者送人。

条件2：我是个白帽子。

姿势：我会去测试一下这个优惠券能否修改相应参数，从而达到在B店铺购买的目的。在B店铺购买商品的时候，因为没有优惠券，所以提交订单时的优惠券的id参数里面是空

案例（二）

Blood_zer0为我们分享的第二个案例是等级提升，发放优惠券奖励。

环境：等级提升，发放优惠卷，但是每次只发一张！

条件1：当我不是一个白帽子。

姿势：不断刷级让系统发放。

条件2：当我是个白帽子。

姿势：利用并发请求让一次升级收获N张优惠卷。类似于薅羊毛。在发送升级请求之后，系统并没有对程序加“锁”，系统没有判定这个请求是否完成，之后发送领取优惠券的

案例（三）

Blood_zer0为我们分享的第三个案例是关于self-xss和越权一起打“组合拳”的案例。

目的：一个self-xss，我想扩大危害！

环境：在个人资料修改的地方有一个self-xss。

初始想法：利用csrf篡改他人信息。Blood_zer0认为self-xss这个漏洞有点鸡肋，打cookie的话，打的是自己的cookie，所以，可以利用csrf做个钓鱼界面，来修改他人的信

姿势：利用越权修改他人信息获取他人cookie。当时Blood_zer0看到了数据包中有个Pid参数，他马上认真的分析了这个参数的作用，之后发现，这个参数是他自己的用户名

总结

最后，Blood_zer0为我们展示了他的一些对于逻辑漏洞的总结——一张画了很多次，删了很多次，修改了很多次的思维导图。Blood_zer0希望大家能够多多在一起交流，慢

上一篇：phpcms v9.6.0 wap... 下一篇：文件包含漏洞(绕过姿势)

1. 1 条回复

lixx 2017-04-14 09:20:52

username

0 回复Ta
