安全小课堂第九十四期【web漏洞之越权漏洞挖掘】

京东安全应急响应中心 5月7日

越权漏洞十分常见，属于OWASP TOP 10的漏洞类型之一，作为一个常见的逻辑漏洞，越权漏洞的危害和影响与对应业务的重要性成正相关，越权漏洞的挖掘常常要求白帽子足够的细心，对每一个可能产生问题的业务点都考虑到了权限问题。

JSRC **安全小课堂第九十四期**，邀请到**xyang**作为讲师就**web漏洞之权限绕过**为大家进行分享。感谢白帽子盆友的精彩提问与互动~

越权漏洞的原理?

京安小妹

xyang:

逻辑越权本质上来说是设计者或开发者在思考过程中做出的特殊假设存在明显或隐含的错误。简单来讲，开发者可能这样认为：“如果发生A，就一定会出现B，因此我执行C。”他们没考虑到这样的问题：“如果发生X会怎样？”也就是没有考虑到假设以外的情形。

讲师

越权漏洞如何防御?

京安小妹

xyang:

防御的话首先是

1、以最小权限原则设置访问控制策略。
2、敏感/关键接口的读写增加session鉴权。
3、对交易参数进行签名校验，防止用户篡改。
4、开发者尽可能多的考虑用户的反常行为和输入。

讲师

越权漏洞的分类?

京安小妹

xyang：

基于访问控制可以将越权分为水平越权和垂直越权，

其中水平越权是指攻击者执行了与自己所属角色同级别的其他用户能够执行的操作，比如注册某招聘网站成为应聘者后可以查看到平台其他应聘者的简历。

垂直越权是指攻击者执行了自己所属角色并不具备权限的操作，比如普通用户可以浏览到特权用户才能看到的页面。

如何发现逻辑漏洞？

京安小妹

xyang：
参考原理挖掘此类漏洞实际上就是要去设法了解设计者与开发者做出的可能假设，然后考虑如何攻破这些假设。
说一下我碰到的比较多的三类情况
1、发现隐藏的URL：很多开发者通过在菜单栏隐藏URL实现对普通用户和特权用户的访问控制，他们认为普通用户不知道或者猜不到这些URL，但忽略了普通用户可以通过Google Hacking、前端源码（路由）分析、路径扫描或利用其他漏洞来发现这些特权用户才能访问到的URL。
2、关注请求参数（包括Header）中的各种id：这个也好理解，从前端获取回来的id直接带入业务逻辑，未校验该id的归属是否为当前登录账户。这种问题的场景实在太多了，而且大多数情况下是可以对id进行遍历的，所以这类问题很可能导致大面积敏感信息泄露。平时测试过程中对这些含id的参数敏感一些即可。
3、看似顺序执行的流程：很多功能的实现都需要分阶段请求，比如找回密码、购买商品等，以找回密码为例，第一阶段对当前需要找回密码的账户进行认证，认证通过后到第二阶段，此阶段发起修改密码请求，通过拦截修改请求数据包中的账号为受害者账号，若开发者认为到达验证通过后的第二阶段的用户一定已经拥有了相关的权限，并在后续阶段执行操作时不再对用户提交的请求进行验证，那么此时会成功修改掉受害者账号密码。当然找回密码处的问题除了这类越权外，还有很多可以挖掘的点，比如验证码泄露、验证码认证绕过、邮箱弱token等。

讲师

挖掘越权漏洞的自动化思路?

京安小妹

xyang:
平常我们检测越权问题思路是准备两个账号，在不同的浏览器里登录后，互相测试是否能对另一方数据进行越权操作，这个过程可能涉及到需要对很多请求参数进行修改，而这些都是得根据具体的业务场景来判断的，所以越权类问题的自动化检测一直没想到比较完美的方案，这里抛砖引玉，有两个简单的场景下的自动化扫描思路（也可能是坑：））， 做好了能cover部分越权检测工作。
1、越权遍历id型，爬取收集带参数id的url，设置阈值N，对id参数遍历N次，N次返回结果都不一样则告警输出并人工介入分析，误报的情况加白名单处理。
2、垂直越权类问题，结合自身业务特点建立不同角色访问控制模型，准备不同级别的账户登录认证Cookie，扫描器交叉请求，根据返回不满足模型的就告警输出并人工介入分析。：

讲师

总结一些越权漏洞的常见场景?

京安小妹

xyang:
个人碰到比较多的场景，
1、菜单url越权访问，不同角色账号访问系统菜单url不一样，互相访问并未做限制。
2、订单/用户等信息遍历，未校验id是否归属于当前认证用户，修改id，能看到id对应的相关信息。
3、找回/修改密码，修改密码阶段未校验用户真实性。
4、交易流程，下单阶段未校验订单数量、价格。

讲师

挖掘越权漏洞的一些奇淫技巧?

京安小妹

xyang:
说两个实际案例，
1、看似访问页面被403了，但是给请求的头里加一个X-Forwarded-For，设置值为127.0.0.1就可以绕过验证逻辑访问到页面了。
2、看似需要验证码登录的后台，抓包后观察参数，把POST参数verifycode2换成verifycode绕过验证码登录策略。我这算不上什么奇淫技巧，主要还是要做到大胆假设，小心求证。

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