安全小课堂第七十七期【聊聊越权的那些事】

京东安全应急响应中心 2017-11-13

越权漏洞正在泄露你的隐私。作为一种很常见的逻辑安全漏洞，越权漏洞的危害和影响与对应业务的重要性成正相关。如果存在平行越权的话，就可以查看所有用户的敏感信息，而这些敏感信息在黑产眼中简直就是珍宝。

JSRC **安全小课堂第七十七期**，邀请到两位老师分享越权漏洞那些事,同时感谢白帽子们的精彩讨论。

越权漏洞的原理是什么?

京安小妹

hackbar:

越权漏洞的原理：系统资源被访问时，未验证当前用户的身份，使得攻击者越权访问其它同级别用户的系统资源。

主要分为两种类型，根据用户角色区分，简答来说：

水平越权：同样权限的用户角色

垂直越权：不同权限的用户角色

花生:

一句话概括就是未正确判断用户权限

讲师

越权漏洞的危害有哪些呢?

京安小妹

hackbar:

1）获取系统管理权限

主要针对垂直越权，一般权限的账号垂直越权后，访问高权限账号的功能模块，进而获取系统管理权限。（当然，垂直越权本身也是可以获取用户敏感信息的）

2）获取用户敏感信息

主要针对水平越权，越权访问其他用户的资源，比如订单、个人信息等，或者获取其他用户的操作权限，侵害用户的权益。

讲师： hackbar、花生

两位师傅能否分享一些挖掘越权漏洞猥琐的思路或者方法呢?

京安小妹

hackbar:

首先，普通越权，用户订单遍历、收货地址遍历等，比较简单，时间有限，这边就不讲了

我这边主要讲两种我自己平时用的比较多的思路
主要针对有条件的越权利用的
第一种：空值处理
主要针对多参数值匹配查询，如
userID=1111&userIDcard=340121231231212&。。。。。。等多条件匹配，获取用户数据时，可以考虑程序是否对空值有校验，如果未对空值处理，我们可以通过尝试将userIDcard等参数赋值为空或者尝试将这些参数去除，看看是否可以通过userID越权遍历相关信息。还有如前端限定只能查询某一时间段（如三个月）的信息时，我们也可以通过类似操作，在数据包中更改时间段或者对时间参数赋值为空等处理，进行绕过相关限定。
大家自己举一反三！
大家有疑问吗 没疑问我继续了哈
第二种：签名绕过
这里主要针对那些有签名，防止数据包篡改的。如果数据包有签名校验，我们可以尝试通过以下方法进行绕过：
【首先明确数据包中的key值，你需要去替换或者遍历的参数；明确签名参数！】
a.签名空值处理：这个跟越权的空值处理一样，我们可以尝试看看签名参数或参数值是否对空值有做处理，如果没有，看看能否通过空值绕过。
b.签名机制是否完善：这里主要是分析签名的处理机制，看看签名是否只对当前数据包参数值做验证，即只要我们修改当前数据包key值时，请求失效。当数据包中的key值通过其他方式进行绕过处理（不在当前数据包进行修改），数据包请求合法。这时我们可以分析一下key值的来源，比如是否是从上一个数据包返回值中调取的，我们是否可以通过修改上一个数据包返回值中的key值，让API主动去调用key值，从而进行绕过等。
花生：
hackbar师傅的思路确实不错，测试越权给大家个建议：最好准备两个以上测试账号，以免因为大意，误改对其他用户造成影响。还有就是越权首先要搞清楚待测功能点的查询条件
1.明显的测试点
http://test.com/edituser/1
我们可以从url里直接看出的，可以通过这个直接测试http://test.com/edituser/2，看反馈内容是否是其他用户信息
2.不明显的测试点
如果url里没有明显的id、name等可测试字段，那我们要分析http头里有没有特殊字段，比如token、并分析cookie字段还有body体；是否有明文或者容易获取的字段比如jd的pin码；如果有，我们就要找出查询条件去测试。剩下的就是分析，配合hackbar这样的分析技巧就差不多了。每个公司的情况不太一样，不过有很多是通过数字id作为查询条件，我这里提供一个测试思路，在被动扫描里写一个插件，正则依次替换数字，判断响应内容。这样只能粗略判断，深入的还需要根据功能定制策略。

讲师

两位师傅能否推荐一些检测越权漏洞的工具以及小脚本？

京安小妹

hackbar：

Authz、Autorize

：

讲师

站在企业的角度，如何如何有效防御越权漏洞的产生？

京安小妹

hackbar：

我这简单从两个方面讲一下吧

1）对相关的API进行权限校验，防止用户越权操作

2）对用户敏感信息进行脱敏，退一万步说，就算是发生了越权，如果数据已脱敏，攻击者也获取不到有价值的信息。

花生：

1.db中存储用户唯一标识

2.用户登录之后，将用户唯一标识映射存入session中

3.用户所有操作，通过session来唯一确定权限

：

讲师

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，回复“安全小课堂”或者点击阅读原文进行查看。

最后，广告时间，京东安全招人，安全开发、运营、风控、安全研究等多个职位虚位以待，招聘内容具体信息请扫描二维码了解。

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