安全小课堂第131期【越权漏洞的挖掘】

京东安全应急响应中心 3月5日

越权漏洞是Web应用程序中一种常见的安全漏洞，攻击者可以利用这些缺陷访问未经授权的功能或数据，例如：访问其他用户的帐户、查看敏感文件、修改其他用户的数据、更改访问权限等。

JSRC **安全小课堂第131期**，邀请到**g0ku**师傅就**越权漏洞的挖掘**为大家进行分享。同时感谢白帽子们的精彩讨论。

什么是越权？

京安小妹

g0ku:

越权是最常见的web应用漏洞之一，即OWASP中的失效的访问控制，对于用户所能够执行的操作缺乏有效的限制，使用户可以操作未授权的数据。

越权的危害

京安小妹

g0ku：

攻击者可以利用这些缺陷来访问未经授权的功能或数据，例如访问其他用户的账户，查看敏感文件，修改其他用户的数据，更改访问权限等。

讲师

如何挖掘越权漏洞？

京安小妹

g0ku：

举例几个常用的挖掘手法：

1. 操作时分析请求中的数据包，看看每个参数的作用，修改参数查看变化。
2. 拥有更多权限的账号，把能访问的URL都提取出来，给低权限用户访问或者直接访问，查看能否访问。
3. 猜测隐藏的API，如:guest/getorder，修改成admin/getorder。
4. 通过搜索引擎，或者提取JS中的URL，查找隐藏功能。如burpsuite中有一个BHP JS scraper的插件。
5. 猜测隐藏的参数，添加进去查看变化，如修改信息的时候加个ID。
6. 抓取所有的数据包，搜索用户名等关键词，比如我的用户名是test，在burpsuite中的HTTP history搜索test，看看有没有哪个数据包包含这个参数,将其修改为其他的用户名，查看变化。

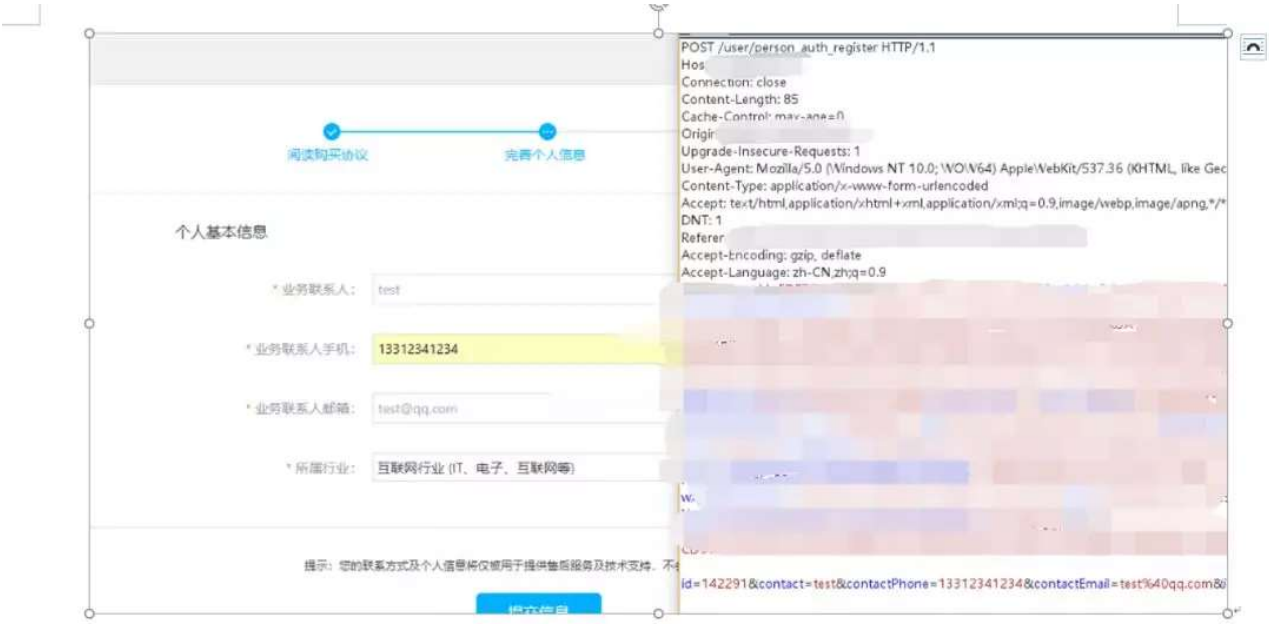
讲师

越权的实战案例1

京安小妹

g0ku:

通过猜测或寻找隐藏的参数来修改其他用户信息；新用户注册时会需要认证信息，提交信息的时候查看数据包内容，可以看到有个参数是id，应该是用户id,这里修改无效，寻找相似的地方。



来到个人信息处

修改的时候抓包，发现没有可以越权的参数，查看新用户注册时的API。与调用时

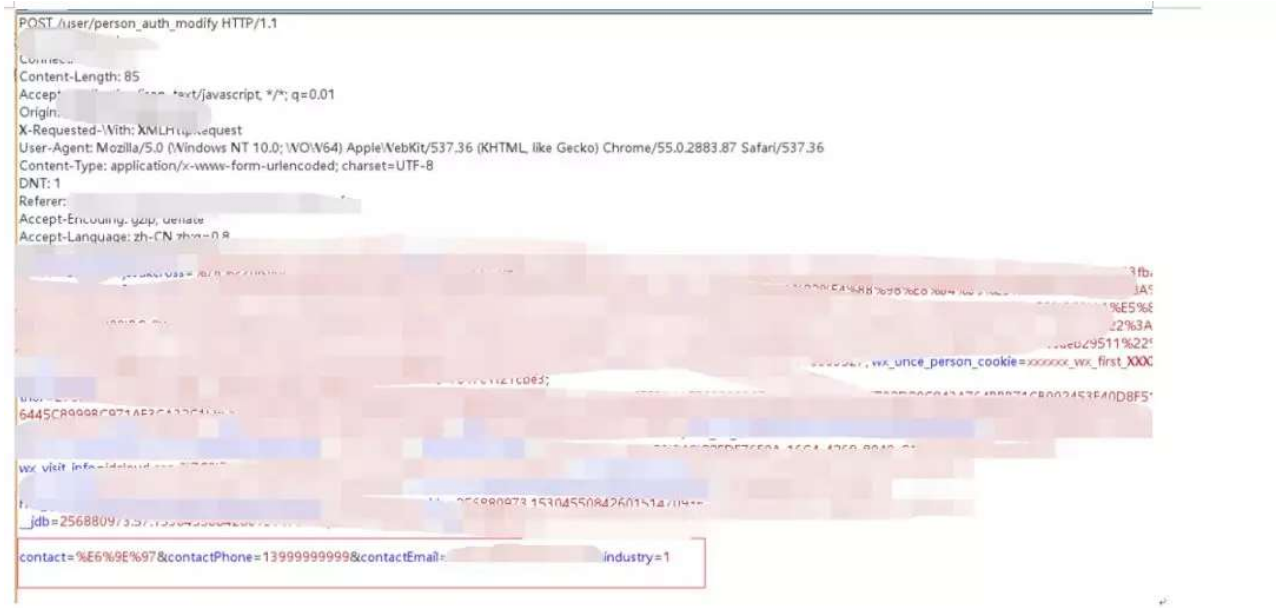
的API有共同点，猜测有隐藏参数。

注册时:

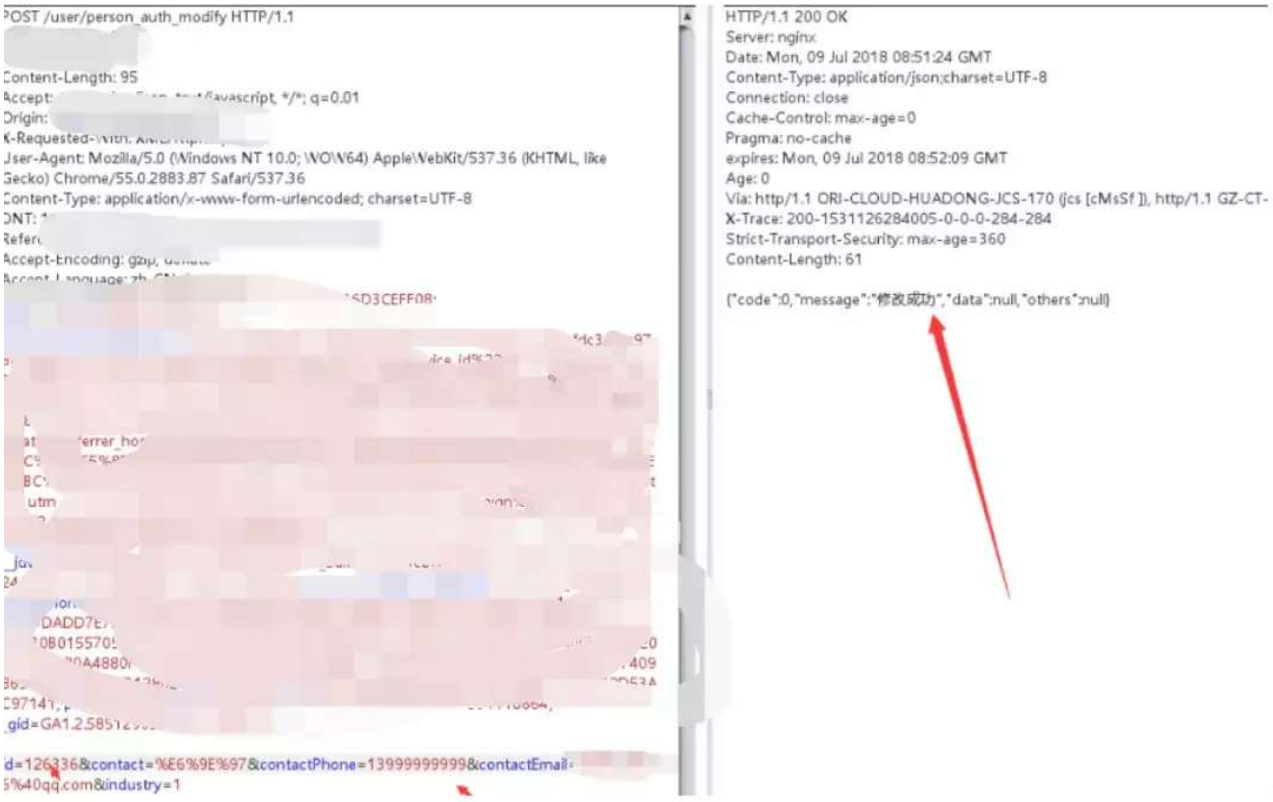
https://*.*.*/user/person_auth_register

修改时:

https://*.*.*/user/person_auth_modify



直接添加ID参数，成功修改其他用户信息。



讲师

越权的实战案例2

京安小妹

g0ku:

查询订单的时候，一般会验证用户cookie，如果把cookie置空，程序可能会获取不到cookie而返回全部订单信息。

登陆账号查询订单信息，PS：啥都没买所以没数据

再次查询的时候抓包将cookie置空

```
POST /getorder HTTP/1.1
Host
Content-Length: 129
Accept: application/json, text/plain, */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36
Content-Type: application/x-www-form-urlencoded
DNT: 1
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:

startTime=2018-03-01&endTime=2018-04-06
```

发送数据包后返回所有订单信息

讲师

互动问答环节：

1. 除了修改用户ID越权还有什么方式吗?

讲师:cookie中的参数,尝试对cookie进行解码,有时候也会有收获。

2.删除了用户cookie，服务器是怎么认证的?

讲师:服务器啥都验证不到了,就返回所有信息给你了,这是因为程序对cookie权限没控制好。

3.怎么越过手势密码这类功能?

讲师:比如可以尝试清空app数据，可以参考一下这个 https://www.cnblogs.com/pshell/p/8191341.html。

4.订单遍历还有什么其他方法吗?

讲师:订单遍历我遇到的都是跟修改参数有关的，主要还是看程序员怎么开发的，具体情况具体分析。

5.burpsuite的BHP JS scraper的插件地址

讲师:https://github.com/Lopseg/Jsdir。

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：anquan@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