

# 记一次对QQ小程序下单平台的安全测试

---

原创 Ma4ter HACK学习呀

2021-01-09原文

## 0x01 前言

原因就是我想吃辣条了 然后就去学生自己搞的小程序平台下单闲起来了 就进行了一点简单的测试

## 0x02 订单查看越权

先 把 手 机 连 到 电 脑 的 一 个 局 域 网 内 的 wifi  
开启burpSuite抓包，然后在查看订单处

查看订单处 Burpsuite抓包拦截数据，进行修改，可以越权查看他人订单



## 我的订单



全部

待支付

待发货

待收货

待评价

退款售后



不二零食铺4栋 订单编号: P1607868324150 待发货



亲嘴烧

¥ 1.50

×2



口水鸡

¥ 2.50

×2

共4件商品 合计 ¥ 8.00 (含运费 ¥ 0.00)



不二零食铺4栋 订单编号: P1607178129352 待发货



卫龙大面筋

¥ 3.00

×1



臭干子

¥ 2.50

×1



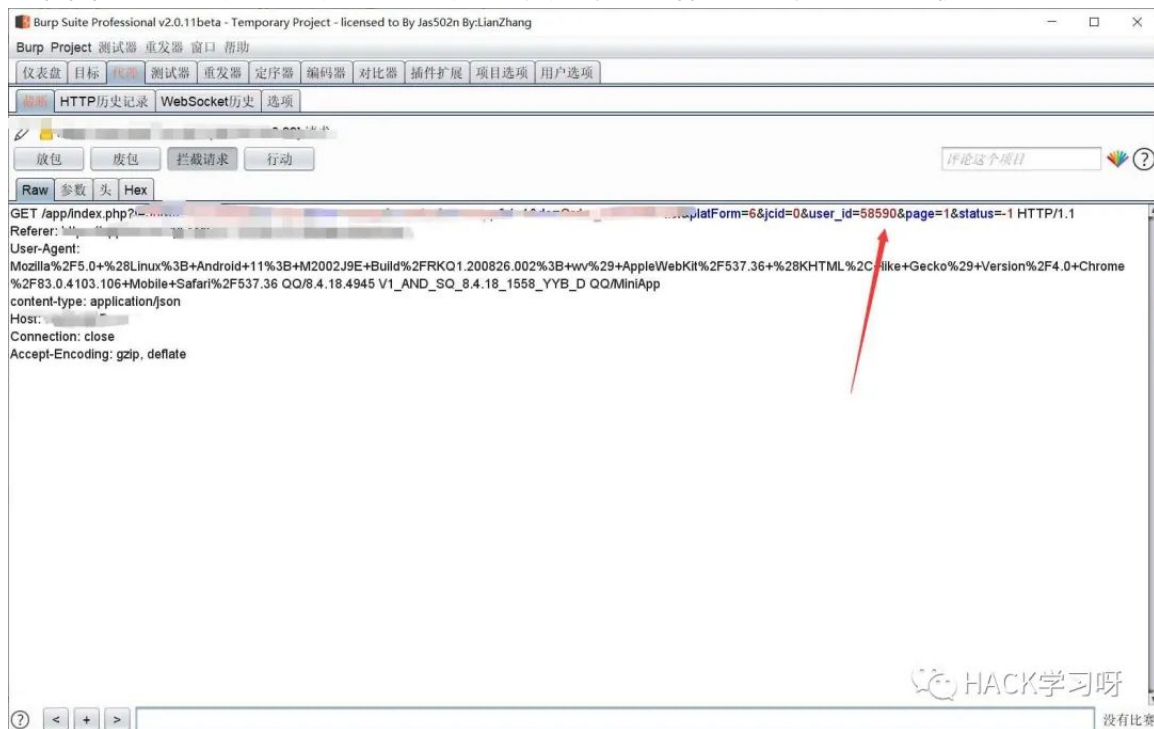
亲嘴烧

¥ 1.50

×2

共4件商品 合计 ¥ 8.50 (含运费 ¥ 0.00)

把图中userid 加一 就看到了别人买的奥里给2333，平行越权漏洞Get



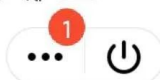


晚上10:39

HD HD 10%



## 我的订单



全部

待支付

待发货

待收货

待评价

退款售后



不二零食铺3栋 订单编号: P1606828826429 待发货



香飘飘

¥ 5.00

×1

共1件商品 合计 ¥ 5.00 (含运费 ¥ 0.00)



不二零食铺3栋 订单编号: P1606743285543 待发货



奥利奥

¥ 7.00

×1

共1件商品 合计 ¥ 7.00 (含运费 ¥ 0.00)

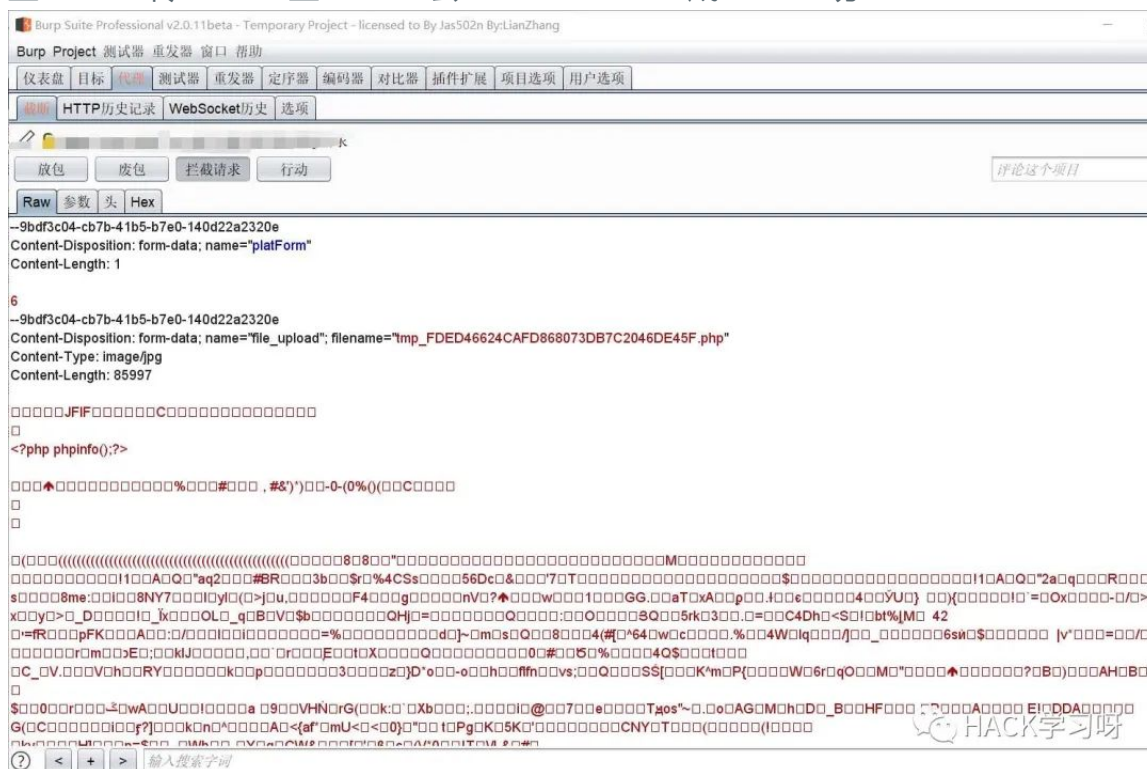
垂直越权:指使用权限低的用户可以访问到权限较高的用户

水平越权测试方法：主要通过看看能否通过A用户操作影响到B用户

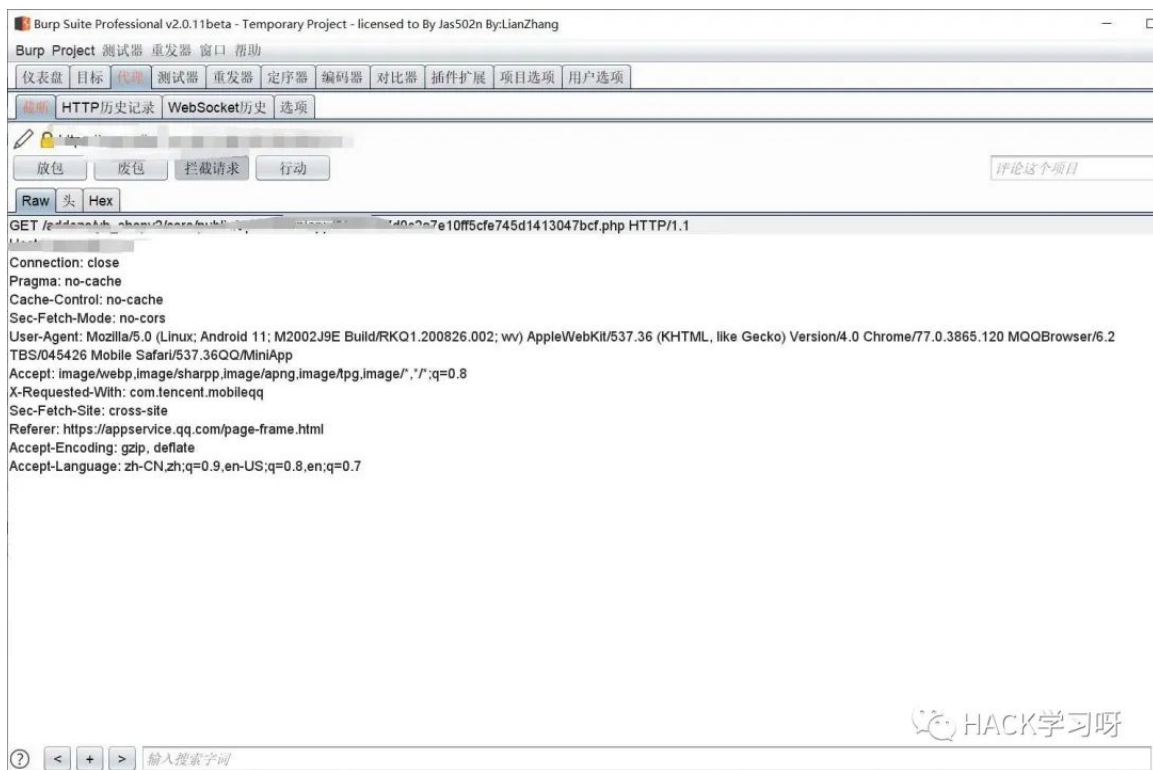
垂直越权测试思路：看看低权限用户是否能越权使用高权限用户的功能，比如普通用户可以使用管理员的功能。

### 0x03 文件上传 getshell

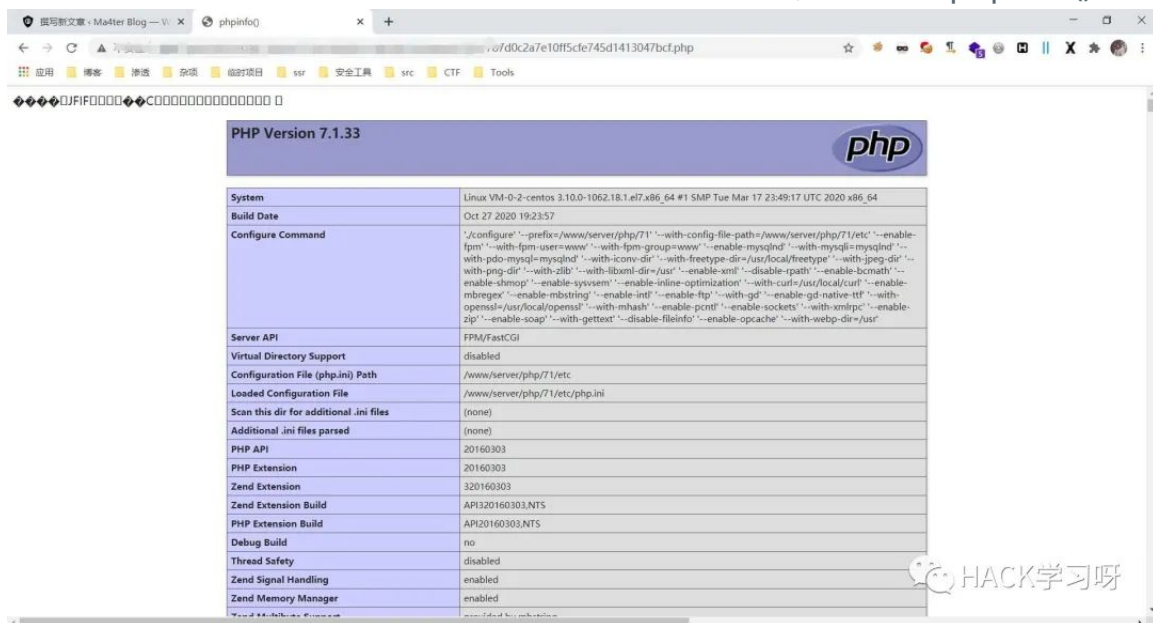
第二个，咱们来到头像上传处 上传头像 抓包 然后直接把后缀改为php  
上传上去 成功 Getshell



放包后 没有返回上传的地址 但是他会去自动访问这个上传上去的 文件  
过 了 一 会 就 抓 到 了 请 求 包



访 问 该 地 址 , phpinfo()




传统功夫 点到为止



2021年性价比最高-网络安全系列课程

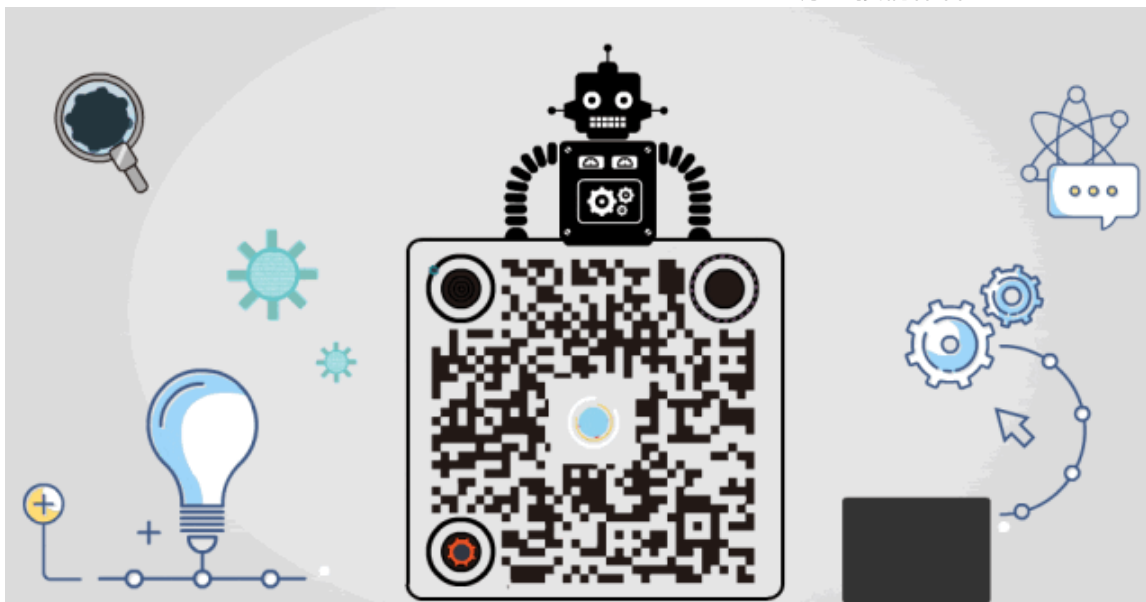
# 报名线上学习

从零开始学习白帽黑客

 HACK学习呀

点赞，转发，在看

原创投稿作者：Ma4ter



精选留言



用户设置不下载评论