KMB接口API测试总结

1. 接口测试方法
2. 抓包分析
3. 分析接口的访问方式是(get、post、delete及header等)中的cookies信息或者UA等重要信息，分析响应头中诸如referer等信息（主要用来定位判断接口的通信是否安全）。
4. 分析接口的参数设计。检查是否存在不需要的参数、是否存在不安全因素的参数。接口的参数直接与数据库字段钩挂，参数设计应尽量参照数据库字段来定义，不需要再通过不确定的前端传入，这样会减弱程序的健壮性，增加冗余。原则是能在服务器端获取的尽量不要传，参数个数尽量精简。（主要用来分析接口的参数构成是否合理）
5. 看所传参数对敏感数据是否采用加密传输。比如说用户名或userid、password等数据如果不使用https进行通信，最好使用加密的方式进行传输，这也是业界通用的标准，并且存入数据库也需是加密的。
6. 看接口的返回是否会返回一些不必要的敏感信息，返回格式是否合理等
7. 数据验证
8. 请求体中参数的常规修改。常规修改就是通用的边界值方法，如极大值、极小值、极长值、null、空。未对这些值做校验的后果可大可小。（非常重要，必做）
9. 请求参数的修改，对于整个接口的安全性。比如：修改密码、修改银行账号。接口的传参步骤至关重要。
10. 业务逻辑验证
11. 与业务强相关的参数修改，各项参数都对应了数据库中的某个业务字段。需要测试人员深入到功能内部，了解各功能间各个因素的触发规则，再针对不同数据的传入去梳理业务逻辑验证点。举例：开卖吧商家活动。比如修改活动id为一个还未开始的任务id，会不会就可以删除这个活动。又或者修改订单id为已取消的订单id，是不是可以发货。（没有固定的方法，需要测试人员在实际中去积累）。
12. 请求消息体中的字段修改。有些人习惯在cookie中传输大量的信息，也是值得关注的测试点。