基于业务场景的安全测试

曾裕智

漏洞盒子

WWW.VULBOX.COM

介　绍

About me

- ID：曾老师
- 目前就职于漏洞盒子
- 专业的业余摄影师
- 不会修飞机的摄影师不是好渗透工程师

- 以前懂SQL注入技巧，畅通无阻
- 现在即使有SQL注入，也未必能轻易获取到数据
- 业务层漏洞反而容易被忽视
- 业务逻辑层的安全漏洞，安全防护设备很难有效识别

企业级安全测试进化史

1.0	以业务需求为导向，功能、性能为主，缺乏必要的安全评估与测试
2.0	基于漏洞类型的安全测试，以自动化扫描为主，人工测试为辅
3.0	基于业务场景的安全测试，以业务场景、业务流程为重心，人工测试主导，人机结合

1.0 阶段

- 企业是以业务需求为导向，功能、性能、稳定性为主导
- 事前缺乏必要的安全评估与测试
- 事中缺乏安全监控
- 事后难溯源

2.0 阶段

- 企业已经意识到安全问题并投入安全建设
- 防护监控设备：WAF，IPS等
- 以自动化扫描为代表，基于漏洞类型的安全测试；不与业务挂钩，检测出的漏洞不是企业所关心的业务范畴
- 人工测试为辅
- 网络层，系统层，组件套件层漏洞难以利用
- 攻击者目标开始转向业务逻辑层

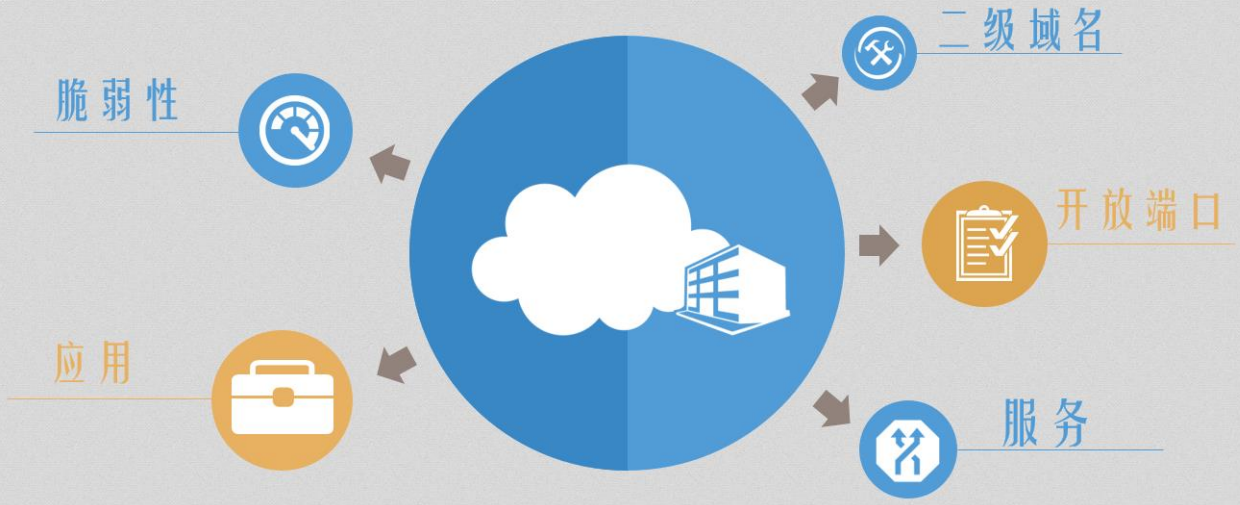
3.0 阶段

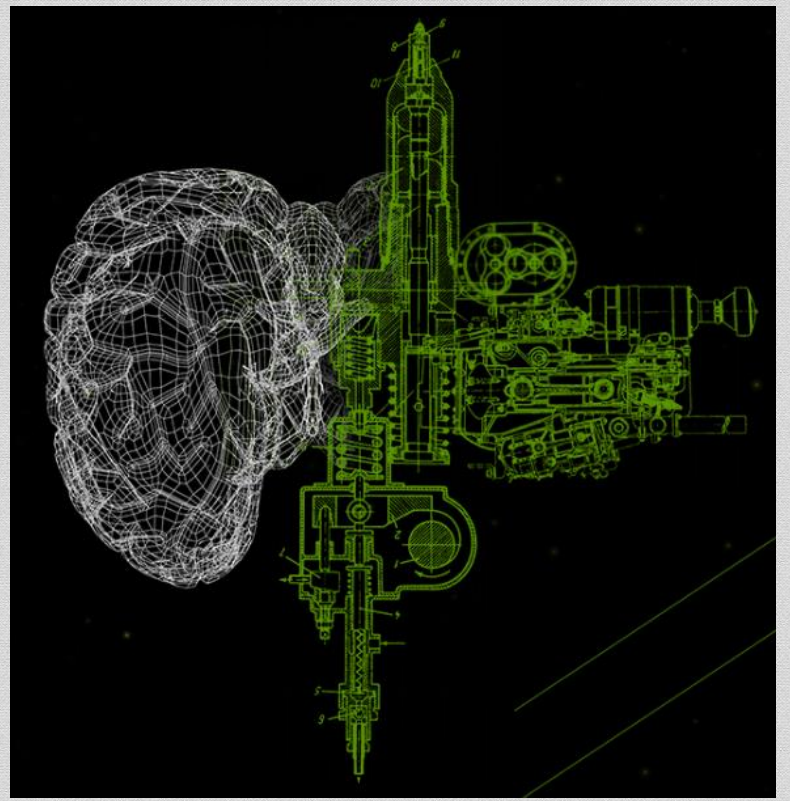
思考：

- 怎么才能最大限度发现业务逻辑层的安全问题？
- 企业能否主动选择关心的业务场景重点测试？
- 漏洞挖出不少，但业务全面覆盖到了吗？

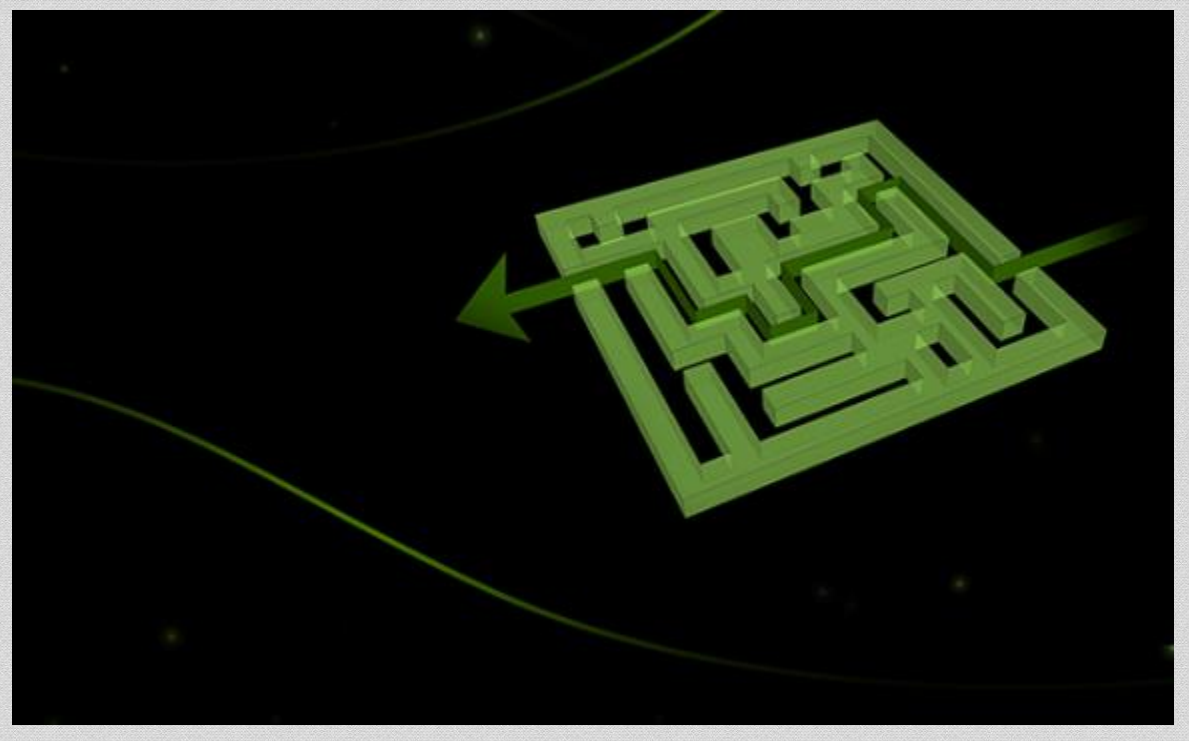
3.0 阶段

- 企业级的安全测试重心应基于业务场景，业务流程进行
- 以人工测试为主导
- 人机结合



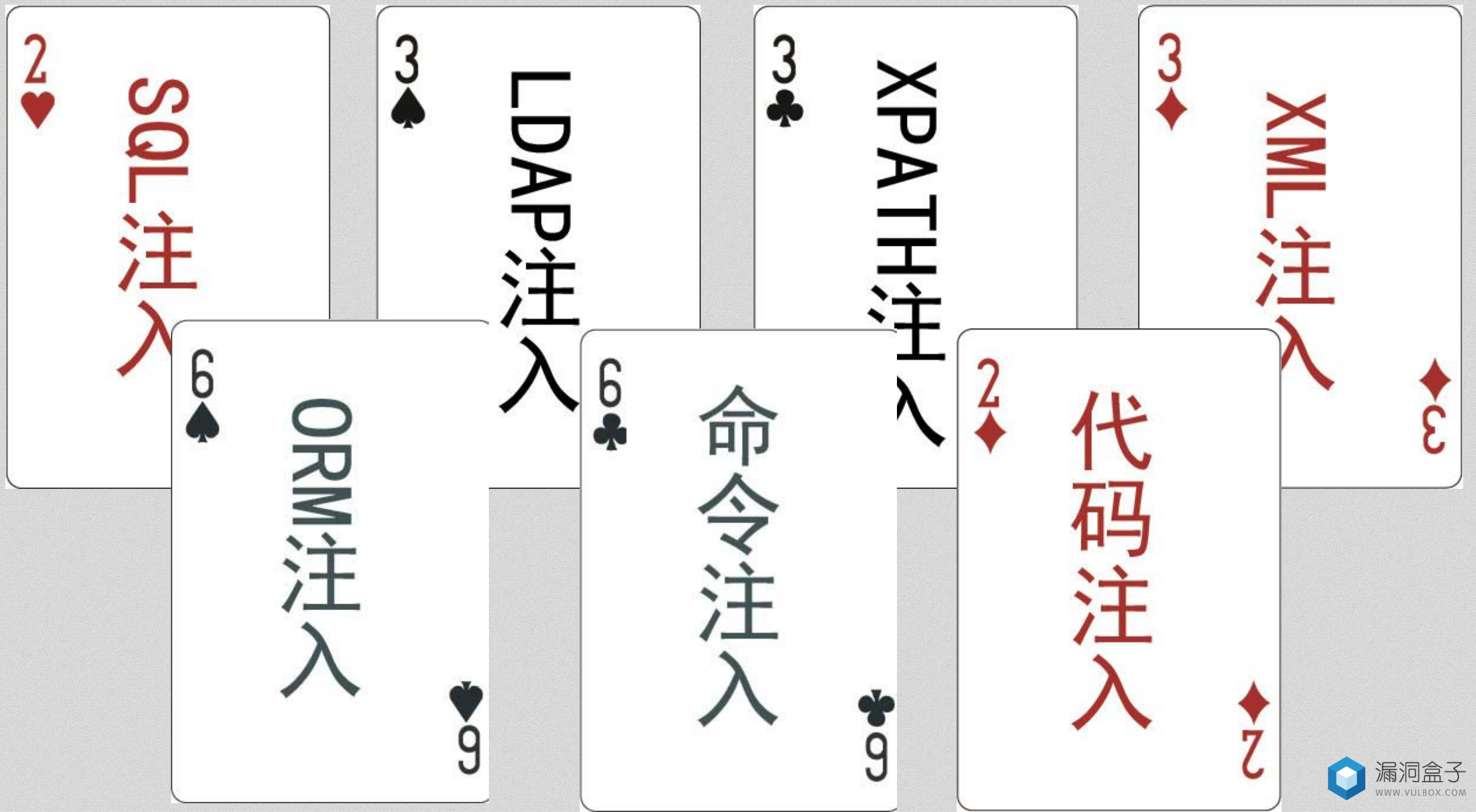


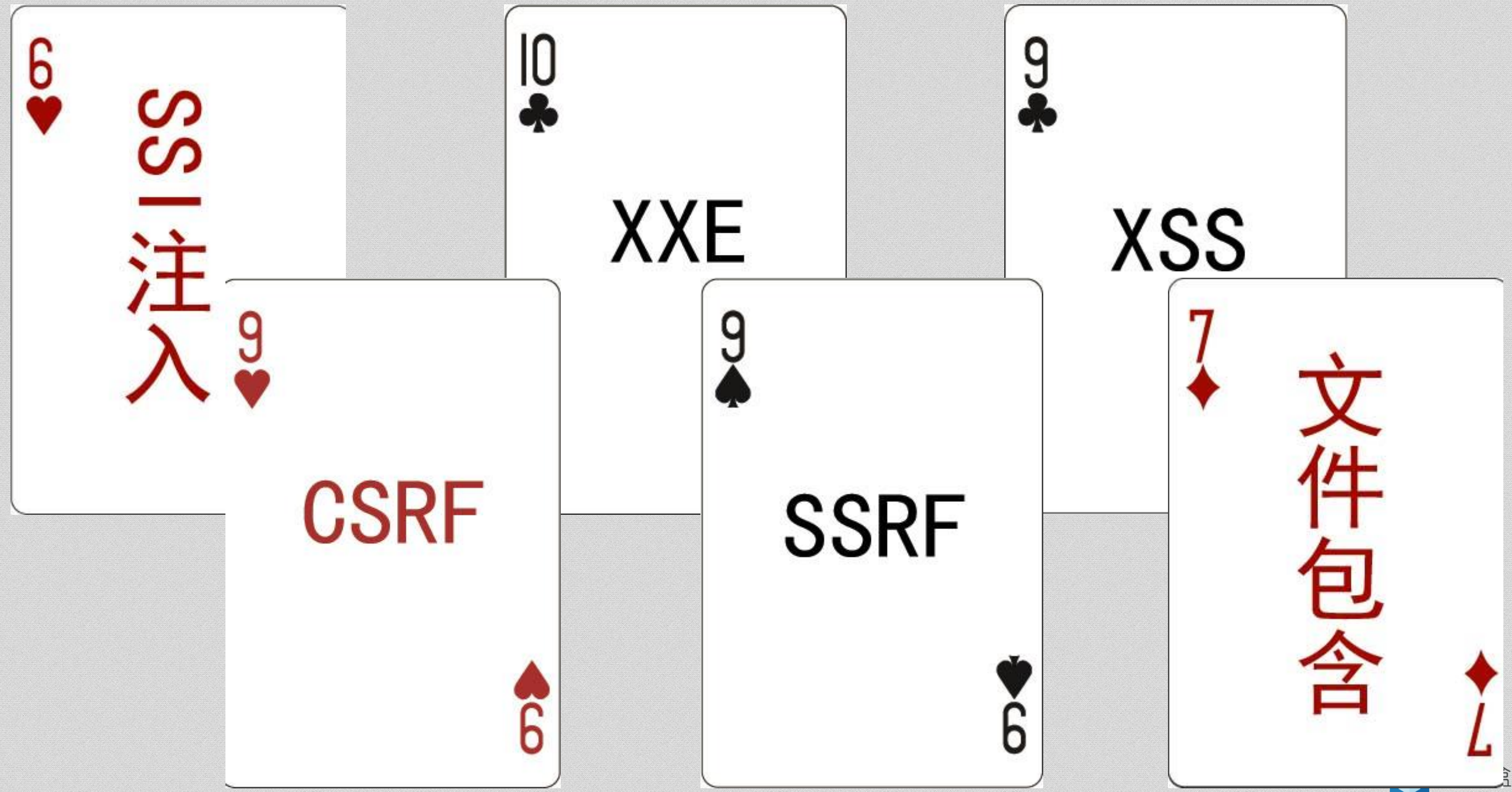
企业的业务好比是一个迷宫，寻找出口的可能路径，这是机器最擅长做的事情，再由人工各个击破。



漏洞类型vs业务场景

基于漏洞类型的安全测试

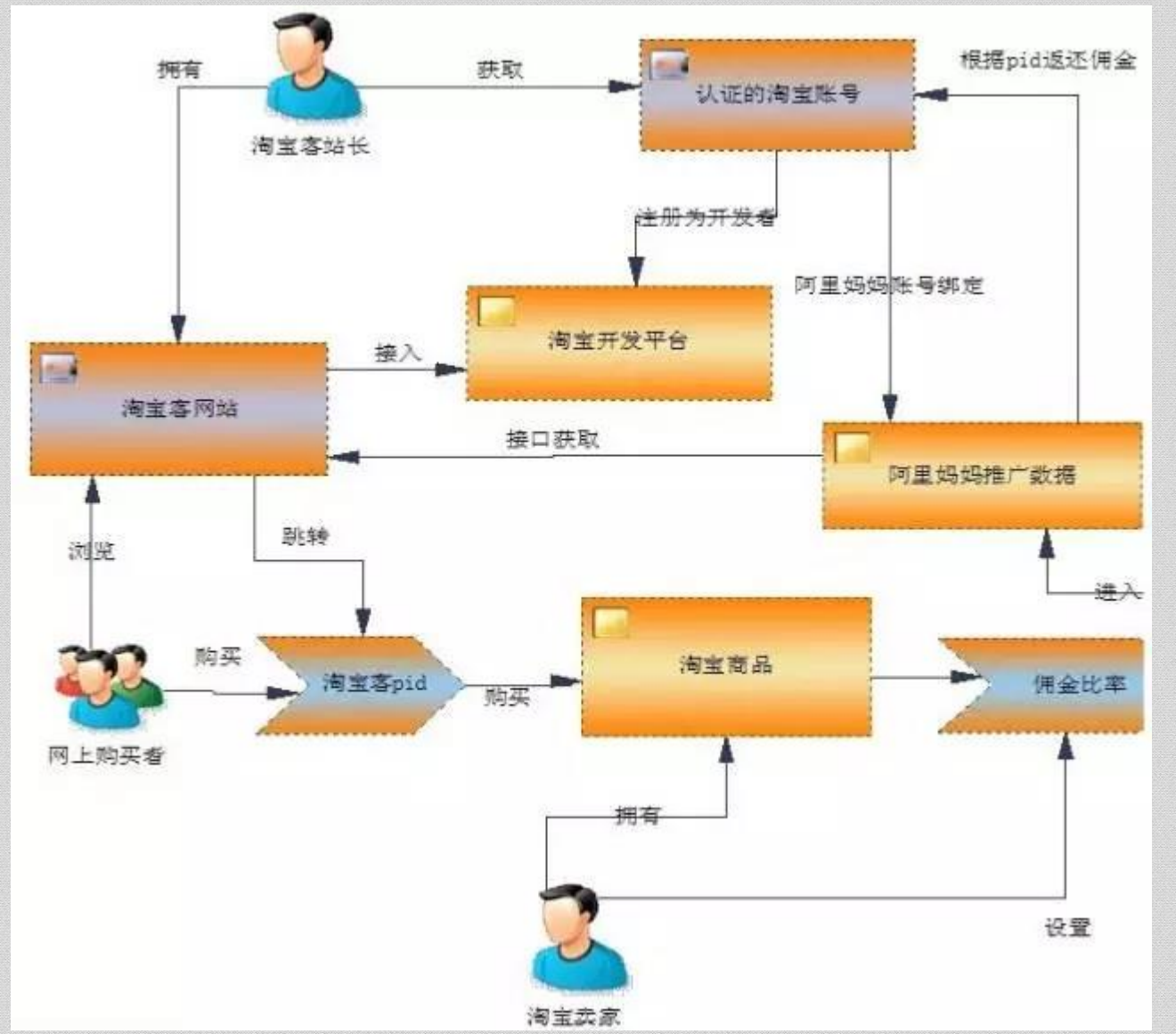




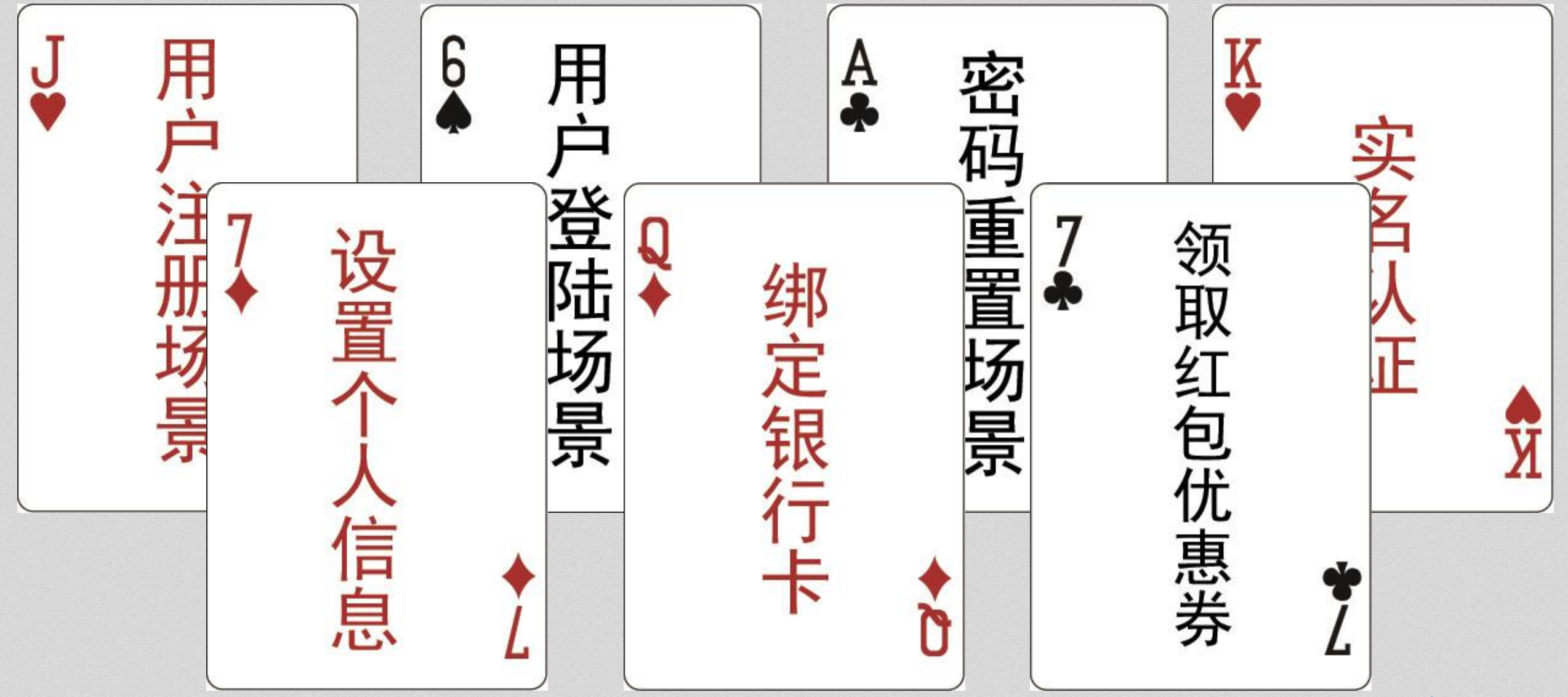
基于业务场景的安全测试

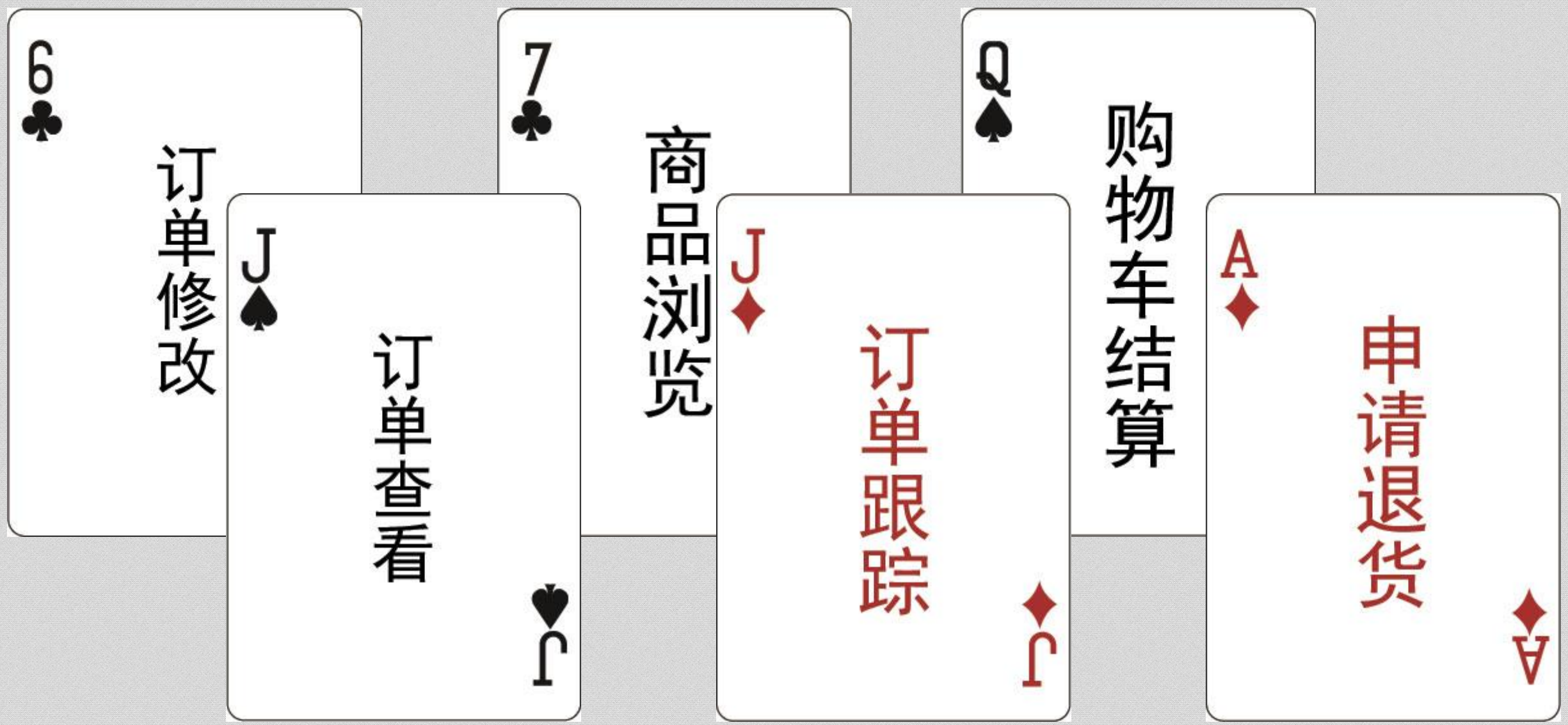
核心工作：

业务流程梳理，业务风险建模



返利类网站业务流程





业务场景测试流程

1. 业务流程梳理及业务风险梳理
2. 根据业务流程划分若干业务场景
3. 确定重点业务场景及业务风险点
4. 基于业务场景，流程，业务风险点执行安全测试

例：电商安全测试场景

身 份 认 证 场 景

包括注册场景、登陆场景、密码重置场景、界面解锁场景

支 付 场 景

购物及订单场景

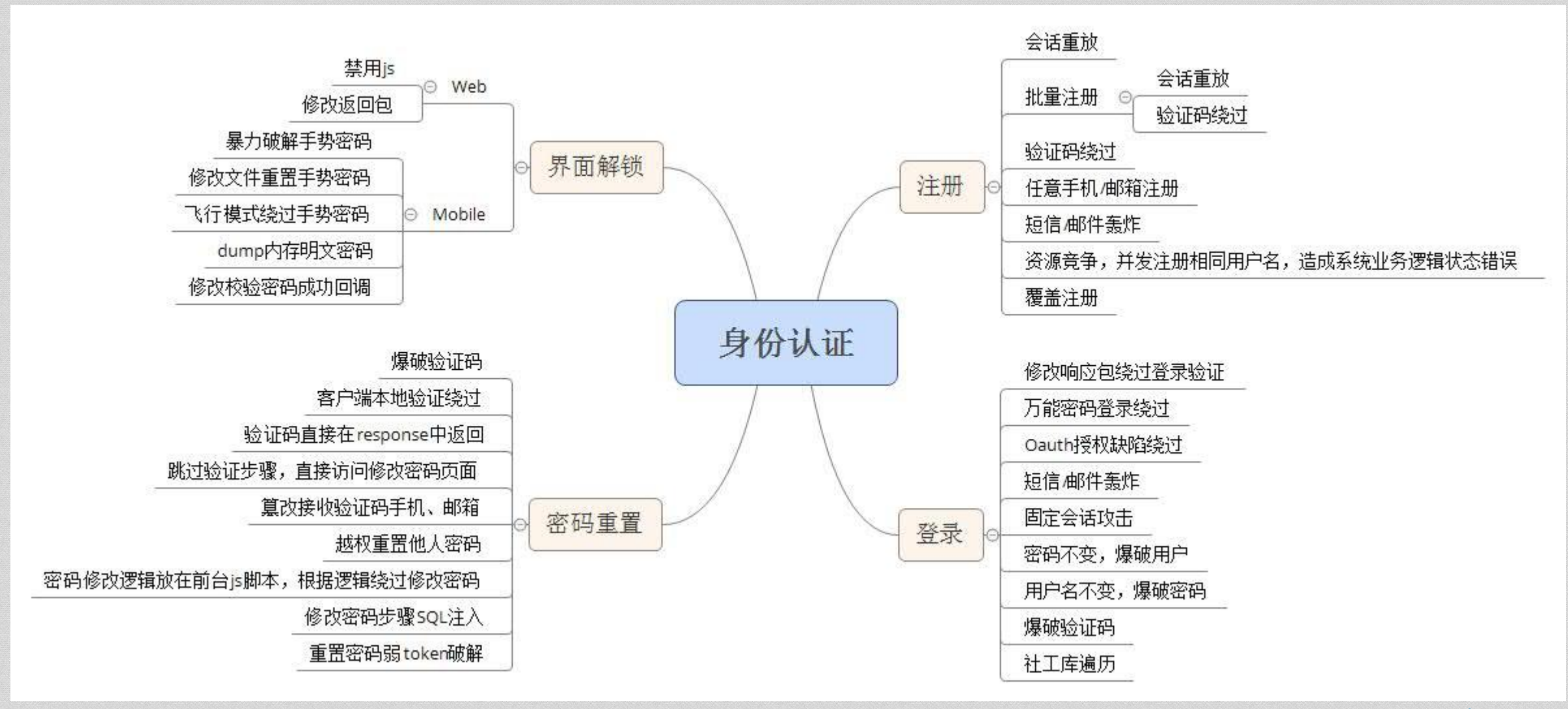
实名认证场景

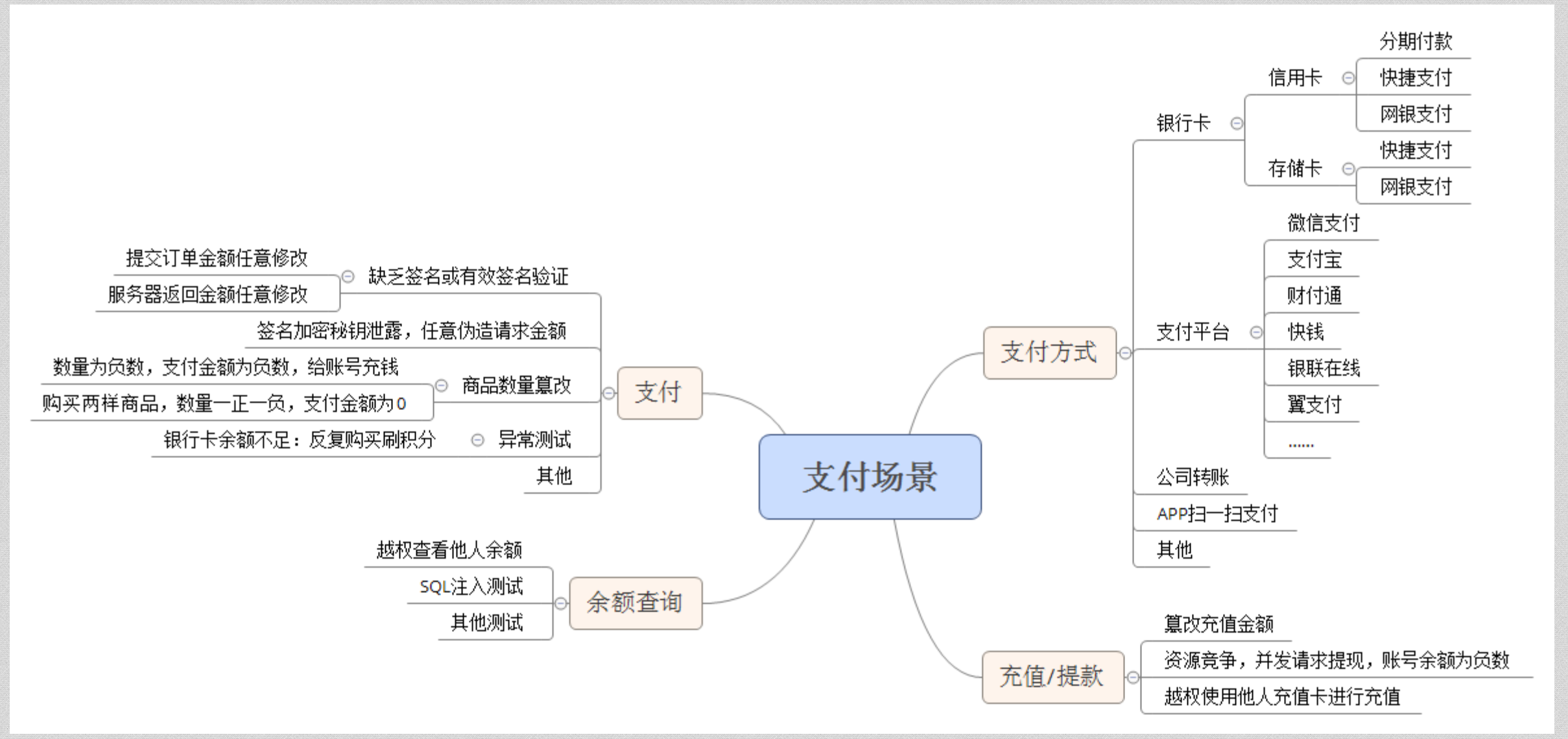
.....

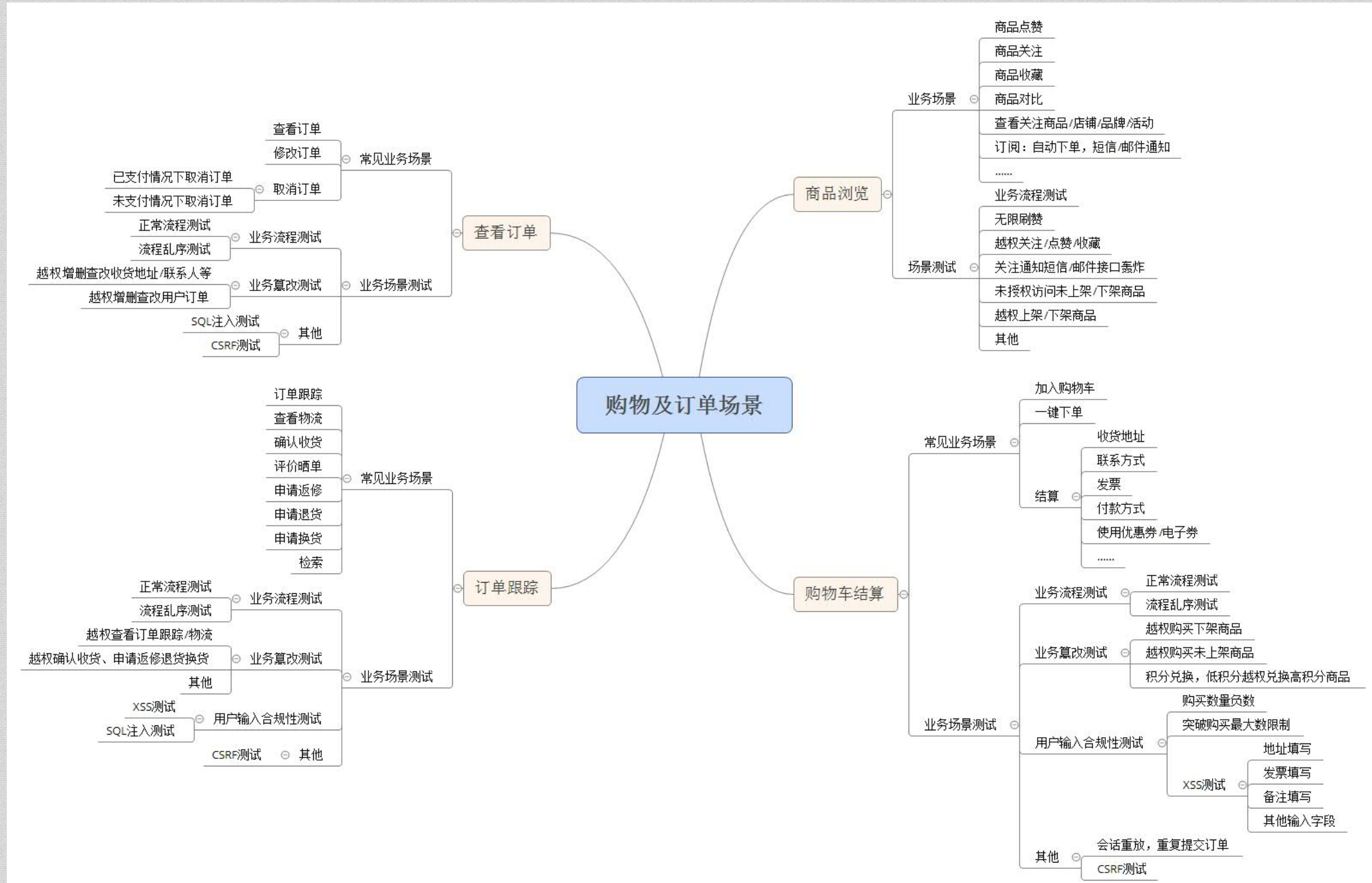
其 他 场 景

业务场景划分

业务场景风险点梳理







业务场景测试要点

- 从银行、金融、保险、证券到电商、O2O、游戏、社交、航空等行业，业务操作越权无处不在。业务场景测试重点关注对象。
- 原因都是服务端以客户端传入的参数为依据，没有对session或会话权限做严格判断造成的。
- 测试方向：平行权限、垂直权限
- 部分应用过分依赖数字签名，服务端忽略了对会话权限做判断

漏洞盒子案例：绕过数字签名越权查询

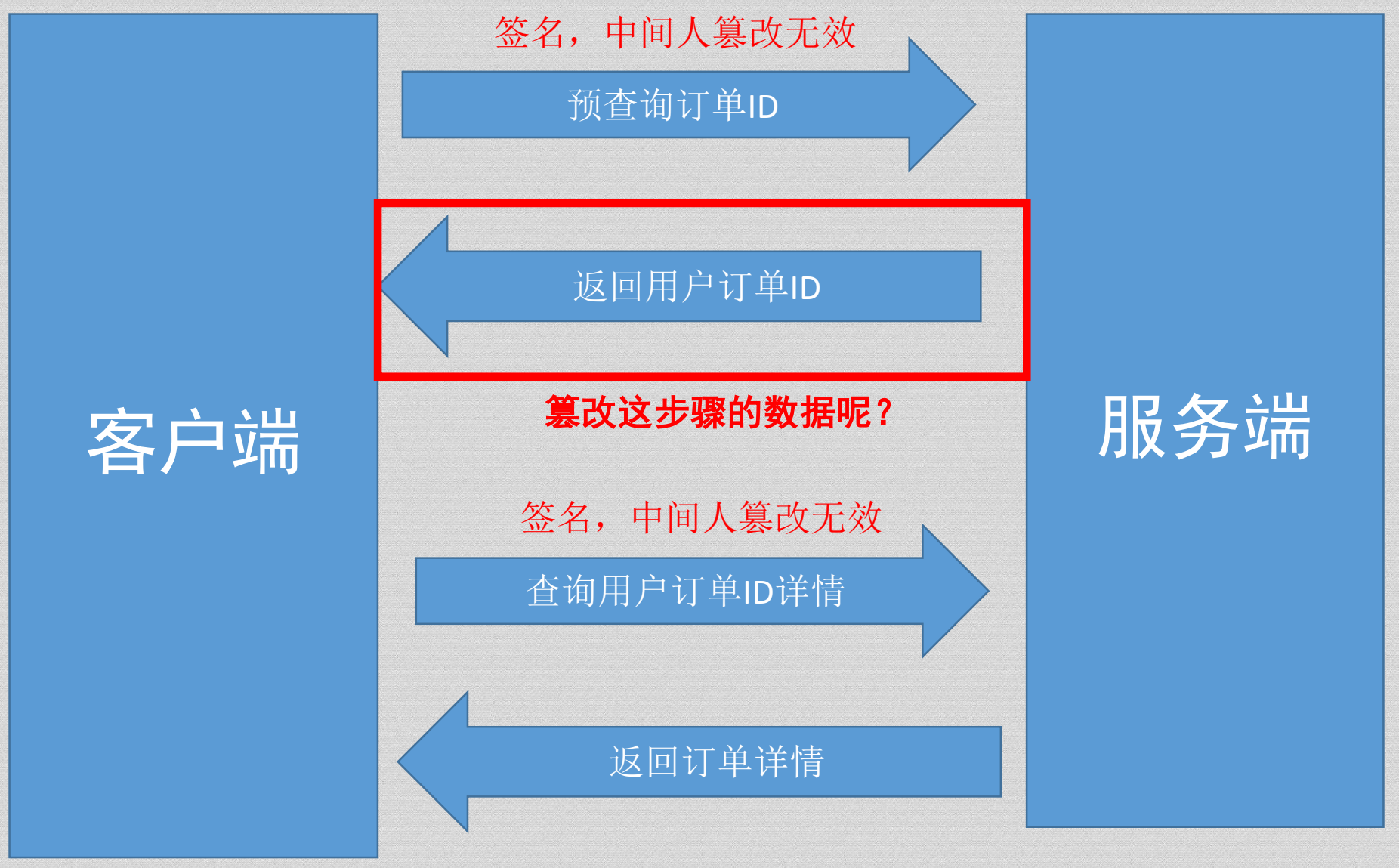
■某APP任意订单查看/无需密码登陆任意用户账号

客户端使用了HMAC哈希运算消息认证，正常情况下修改客户端请求包任何参数，服务端都报错。

通过业务流程分析，发现APP所有查询都分两个步骤：

1.预查询（查询用户有哪些订单ID，地址ID，用户名对应ID）

2.详情查询（根据返回的订单ID，地址ID，用户ID查询详情）



Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Mon, 23 Nov 2015 14:37:38 GMT
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Length: 227

{"code":"1000","systemTime":"2015-11-23 22:37:38","orderNum":"WP1511232240092501","apiOrderNum":"W
22:57:38","currency":"[illegible]","totalAmount":"6095","bookingTime":"2015-11-23 22:37:38"}
```

根据业务流程特点，篡改返回包，绕过签名限制越权查看任意订单

Thank You

漏洞盒子

WWW.VULBOX.COM