典型业务逻辑漏洞挖掘




陆柏廷 | BT

漏洞盒子 高级安全研究员

漏洞盒子简介

TOPHANT
斗象科技

FreeBuf
互联网安全新媒体

漏洞盒子
互联网安全服务平台

网藤风险感知
基于SaaS模式的自动化企业安全风险感知服务平台

漏洞盒子
WWW.VULBOX.COM

自有安全团队与外部安全专家结合，共同为厂商提供安全一体化解决方案


安全专家


相关机构


厂商

- 厂商：金融、保险、电商、互联网、通信等
- 相关机构：CNCERT、CNNVD、 SERCIS、SHCERT、公安部第三研究所、中国民航测评中心、天津网安等

演讲提纲

前　　言

场　　景

方　　法

企业安全测试进化史

基于功能 / 性能的”安全测试”

基于漏洞类型的安全测试

基于业务场景的安全测试

何为业务场景

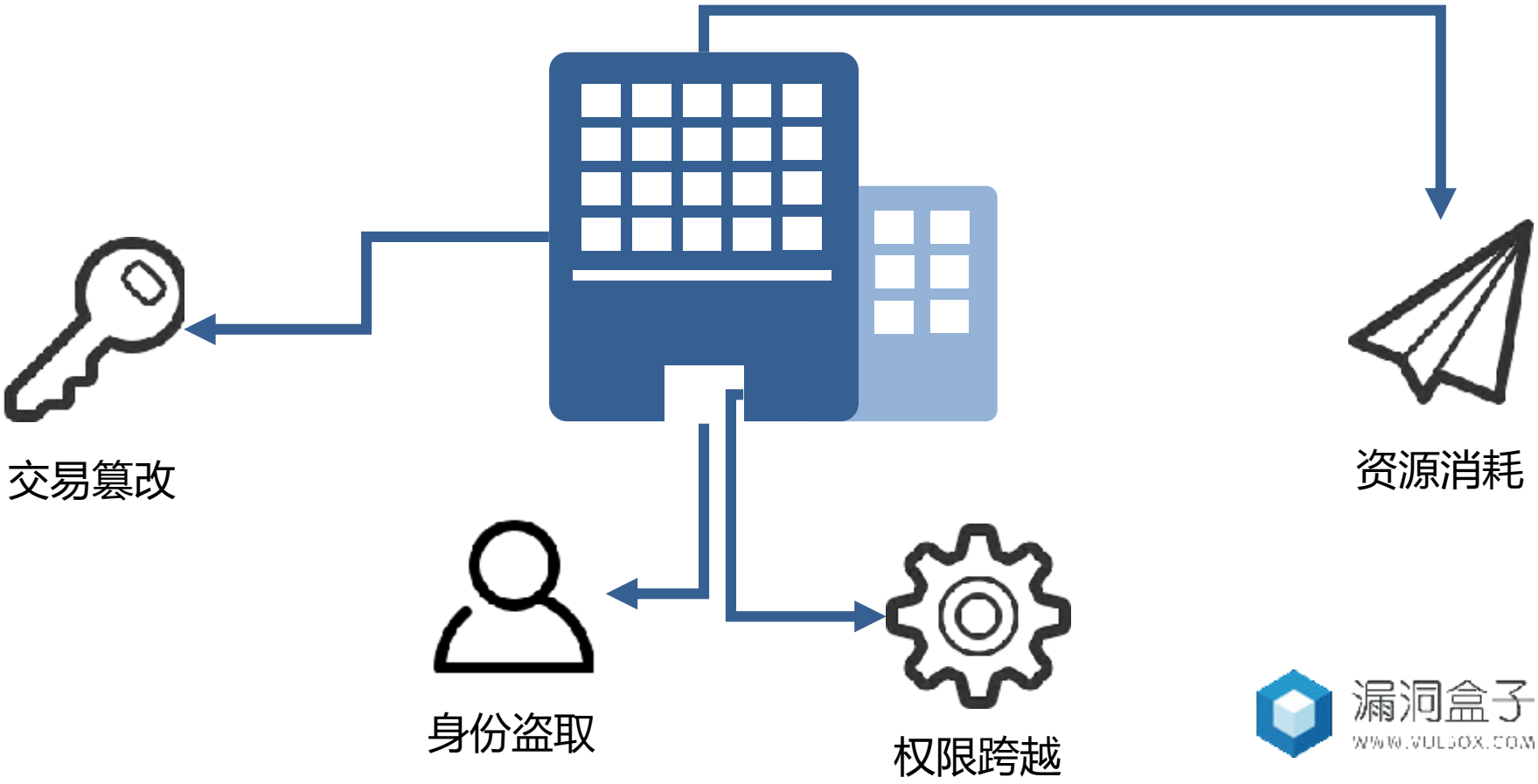
一个业务系统包含的交互场景

业务逻辑漏洞是怎样的存在

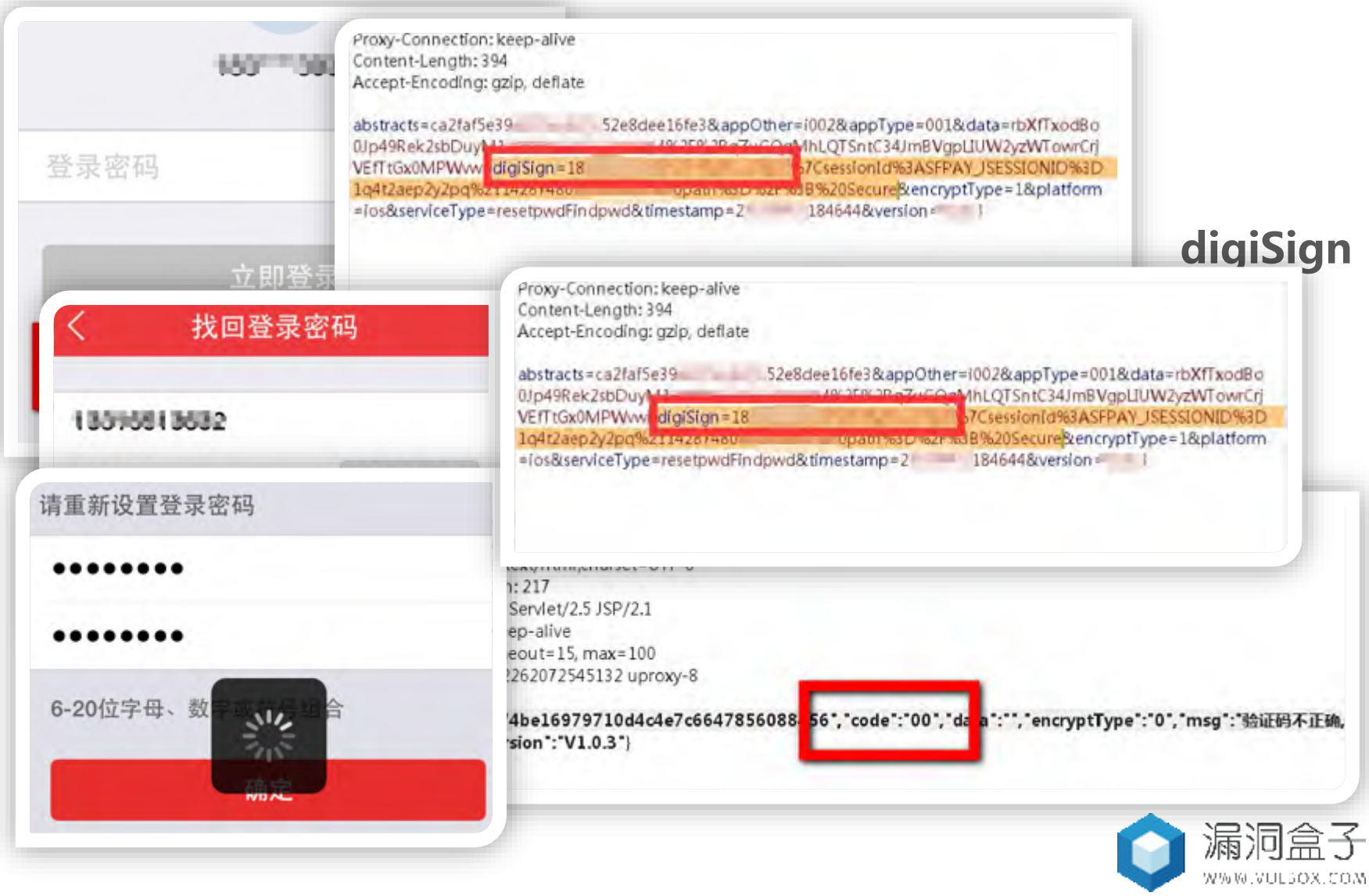
- Bypass一切防护设备
- 至今还没有一款有效的全自动化工具
- 再资深的程序员都可能造坑
- 即使安全人员开发的程序也可能有坑

开发人员ＶＳ安全人员

一个对外业务可能面临哪些业务风险？



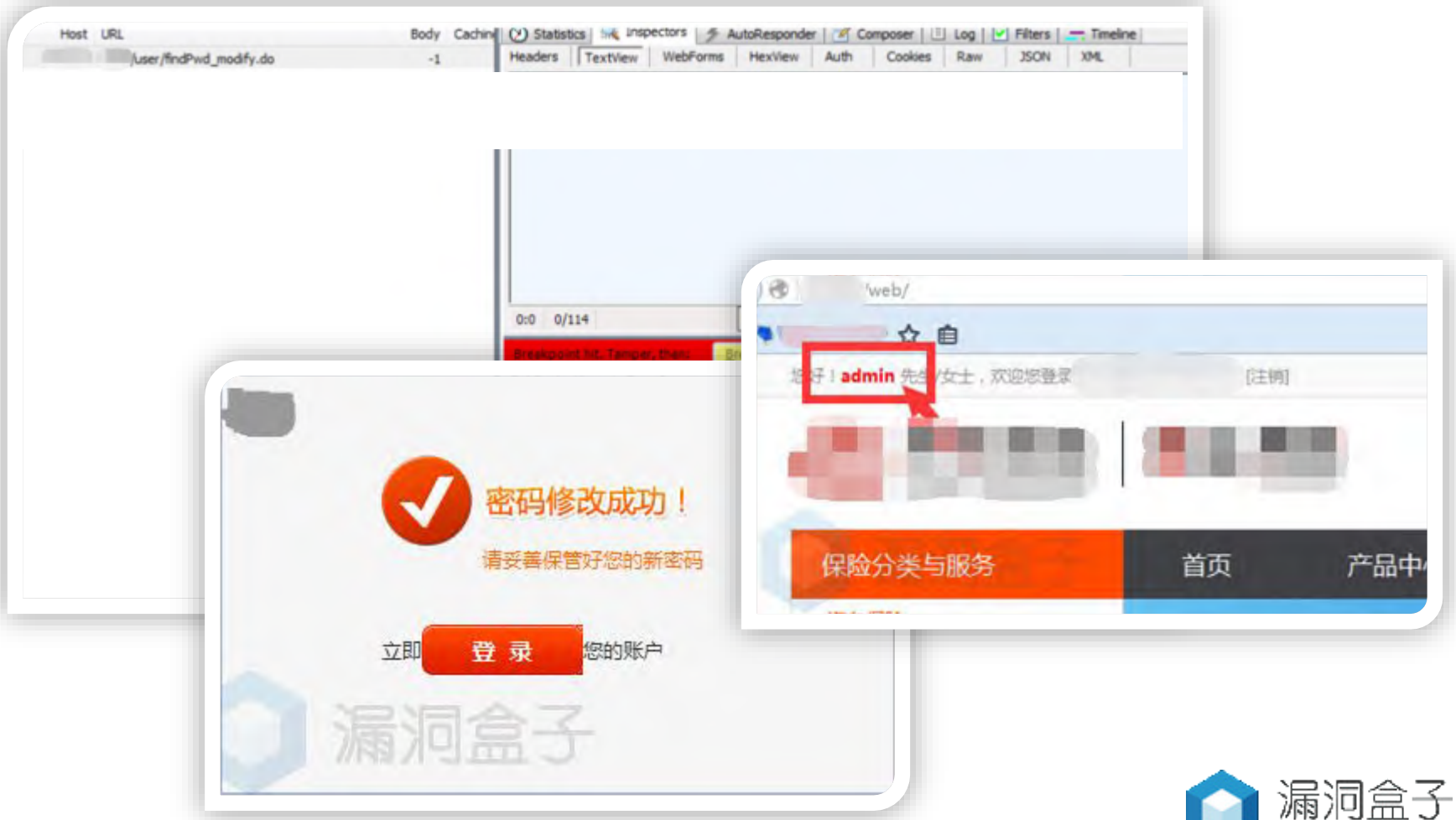
身份盗取 | 迷失的穿云箭



漏洞盒子
WWW.VULSOX.COM

身份盗取 | 简单认证

身份盗取 | 最后一公里



漏洞盒子
WWW.VULSOX.COM

权限跨越 | 垂直水平

Cookie: SESSION=USER-334dsf9ref8esg8erg390g
Cookie: SESSION=USER-3dfg34768jh4h234g5h5jk
Cookie: SESSION=USER-304jkh6g9090ertk45g0s9

Cookie: SESSION=USER-**2**dfg34768jh4h234g5h5jk
Cookie: SESSION=USER-**1**dfg34768jh4h234g5h5jk

权限跨越 | 垂直水平

用户检查：

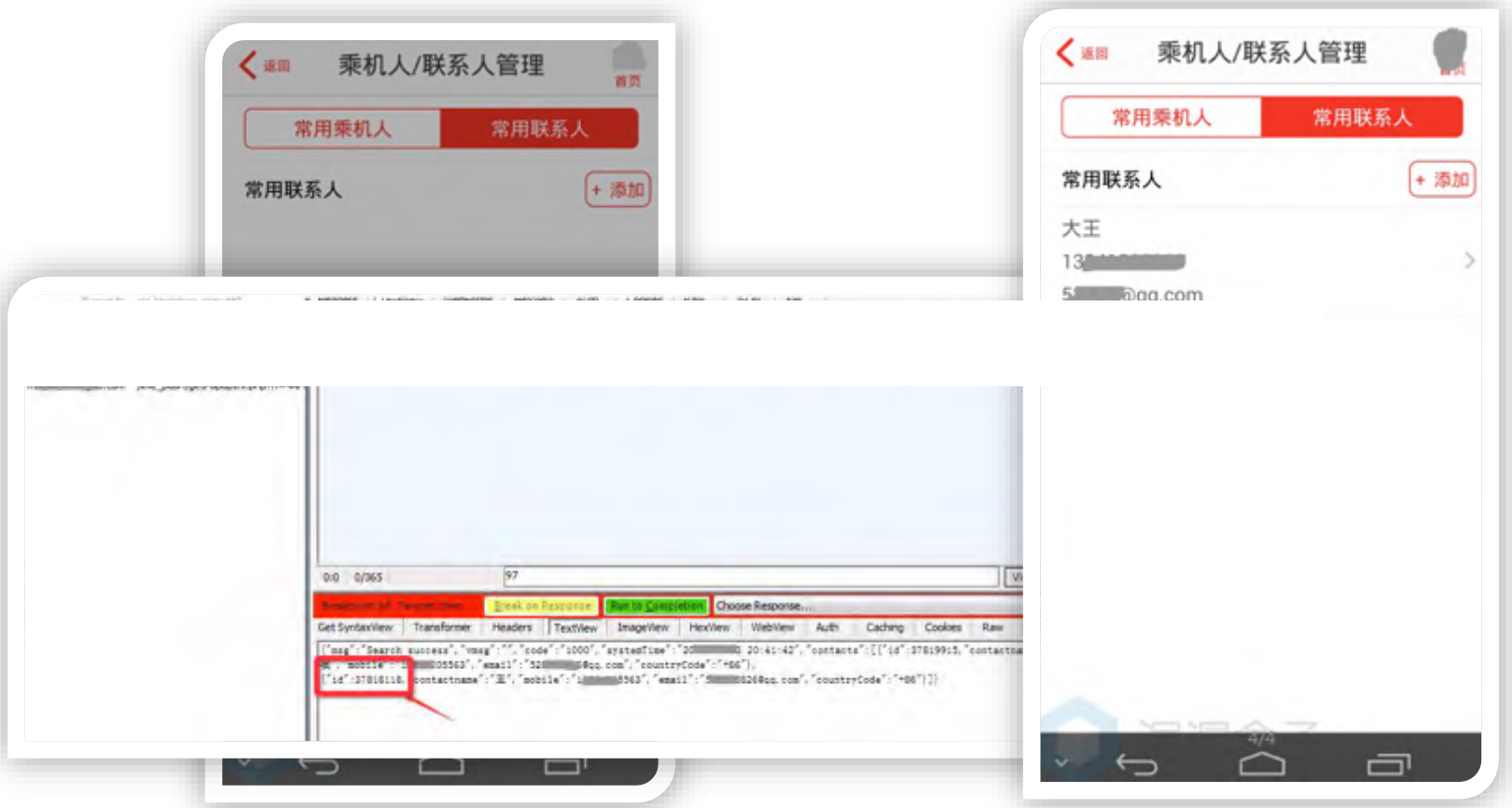
session=34dsf9ref8esg8erg390g

权限检测：

level=3

level=1：admin
level=2：vip user
level=3：normal user

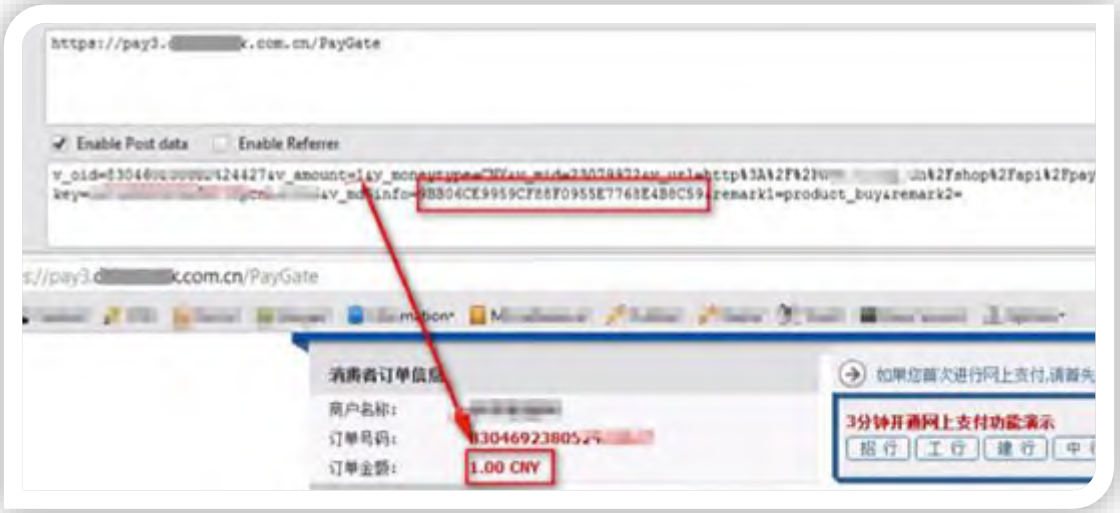
权限跨越 | 签名突破



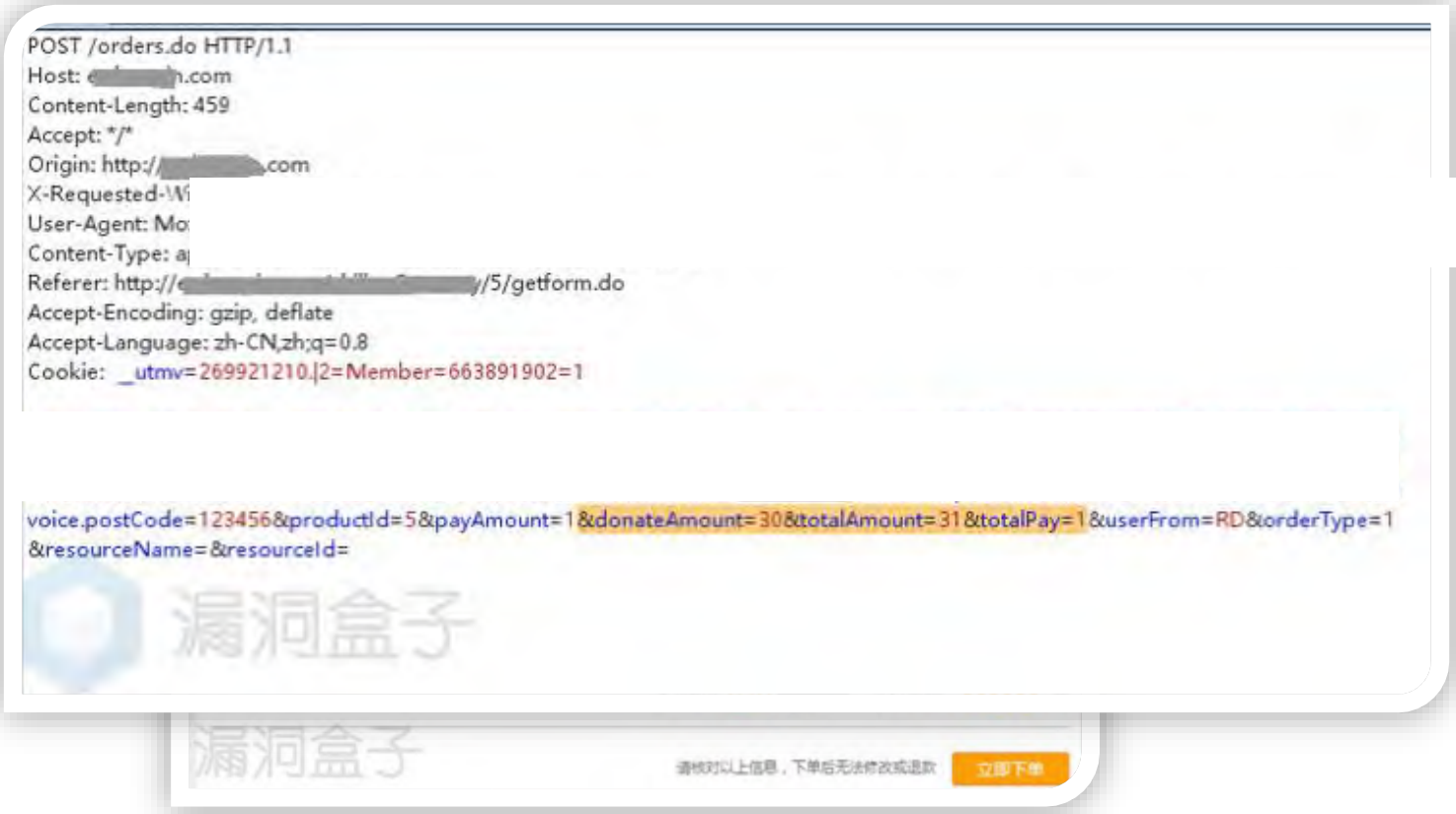
权限跨越 | 签名突破

交易篡改 | 签名破解

将订单中的v_amount,v_moneytype,v_oid,v_mid,v_url参数的value值拼成一个无间隔的字符串,使用key作为salt即生成任意伪造数据签名



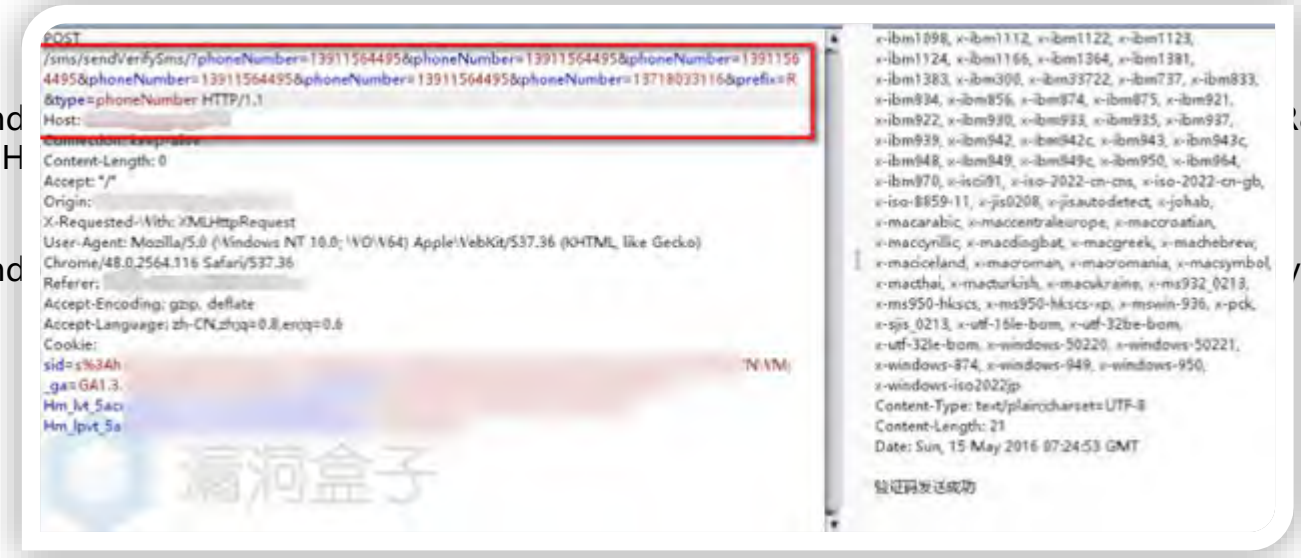
交易篡改 | 局部验证


POST /orders.do HTTP/1.1
Host: [redacted].com
Content-Length: 459
Accept: */*
Origin: http://[redacted].com
X-Requested-[redacted]
User-Agent: Mo[redacted]
Content-Type: a[redacted]
Referer: http://[redacted]//5/getform.do
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie: _utmv=269921210.|2=Member=663891902=1
voice.postCode=123456&productId=5&payAmount=1&donateAmount=30&totalAmount=31&totalPay=1&userFrom=RD&orderType=1
&resourceName=&resourceId=
漏洞盒子
漏洞盒子
请核对以上信息，下单后无法修改或退款
立即下单

资源消耗 | 变量覆盖

GET /sms/sendVerifySms/?phoneNumber=18666666666&prefix=R&type=phoneNumber HTTP/1.1

GET
/sms/send
Number H

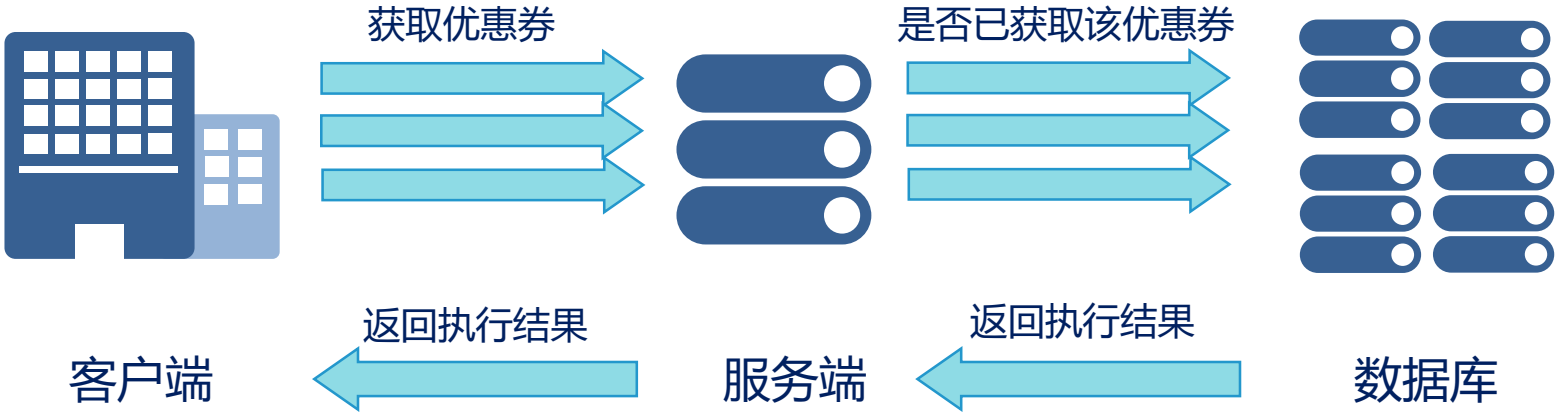


GET
/sms/send
HTTP/1.1

资源消耗 | 并发请求

【购买须知】每工作日限量1000份抢兑，活动期间每位客户仅有1次抢兑资格，仅限兑换1份

资源消耗 | 并发请求



资源消耗 | 薅羊毛

- 花8000万做推广，3000万被羊毛党薅走
- 需要什么给什么，只要收益大于付出

防治

- 提高门槛：用户流失
- 后期检测：成本高、误差大

如何高效测试

- ✓ 业务场景建模
- ✓ 业务流程梳理
- ✓ 风险点识别

业务场景建模 - 1

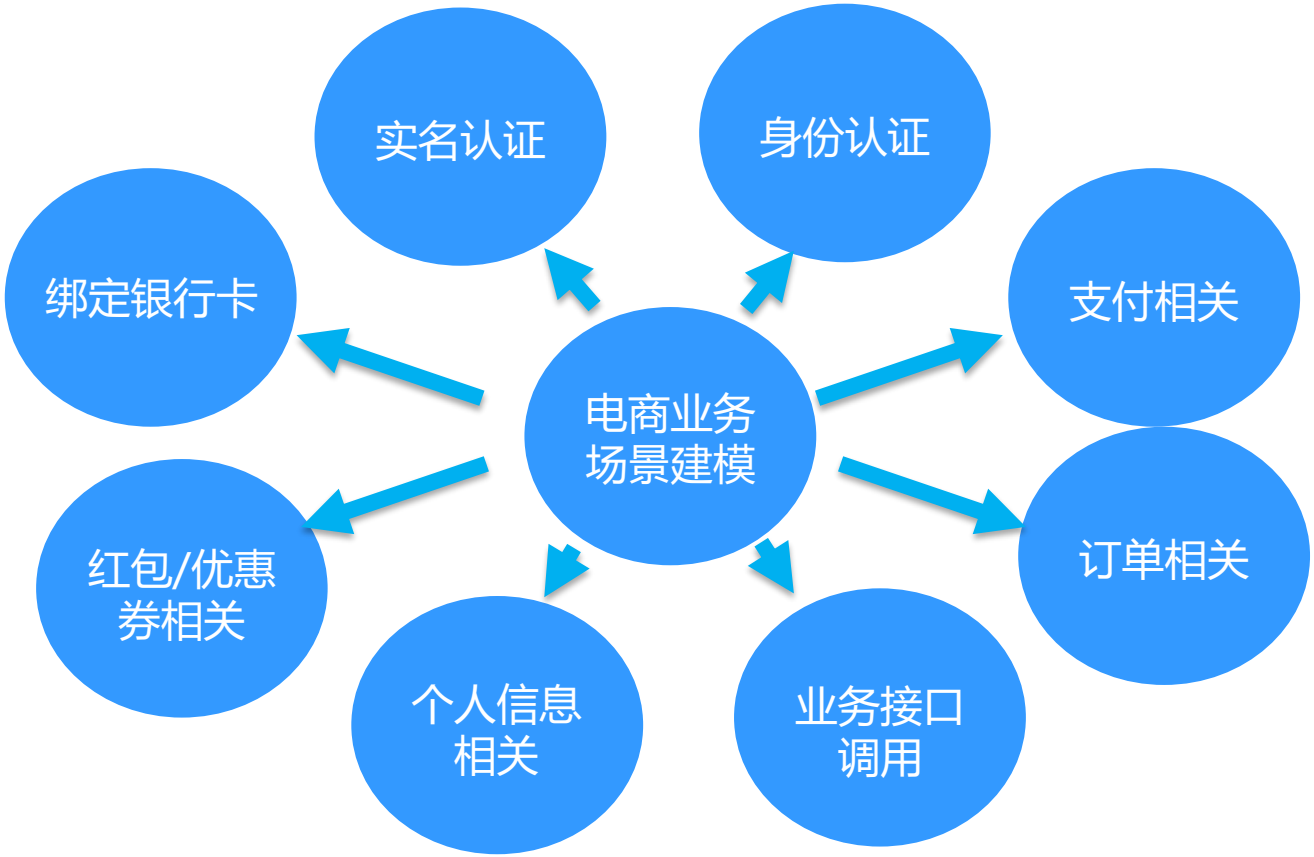
不同行业业务场景有所异同

如：银行、金融、保险、证券、电商、020、游戏、社交、招聘、航空

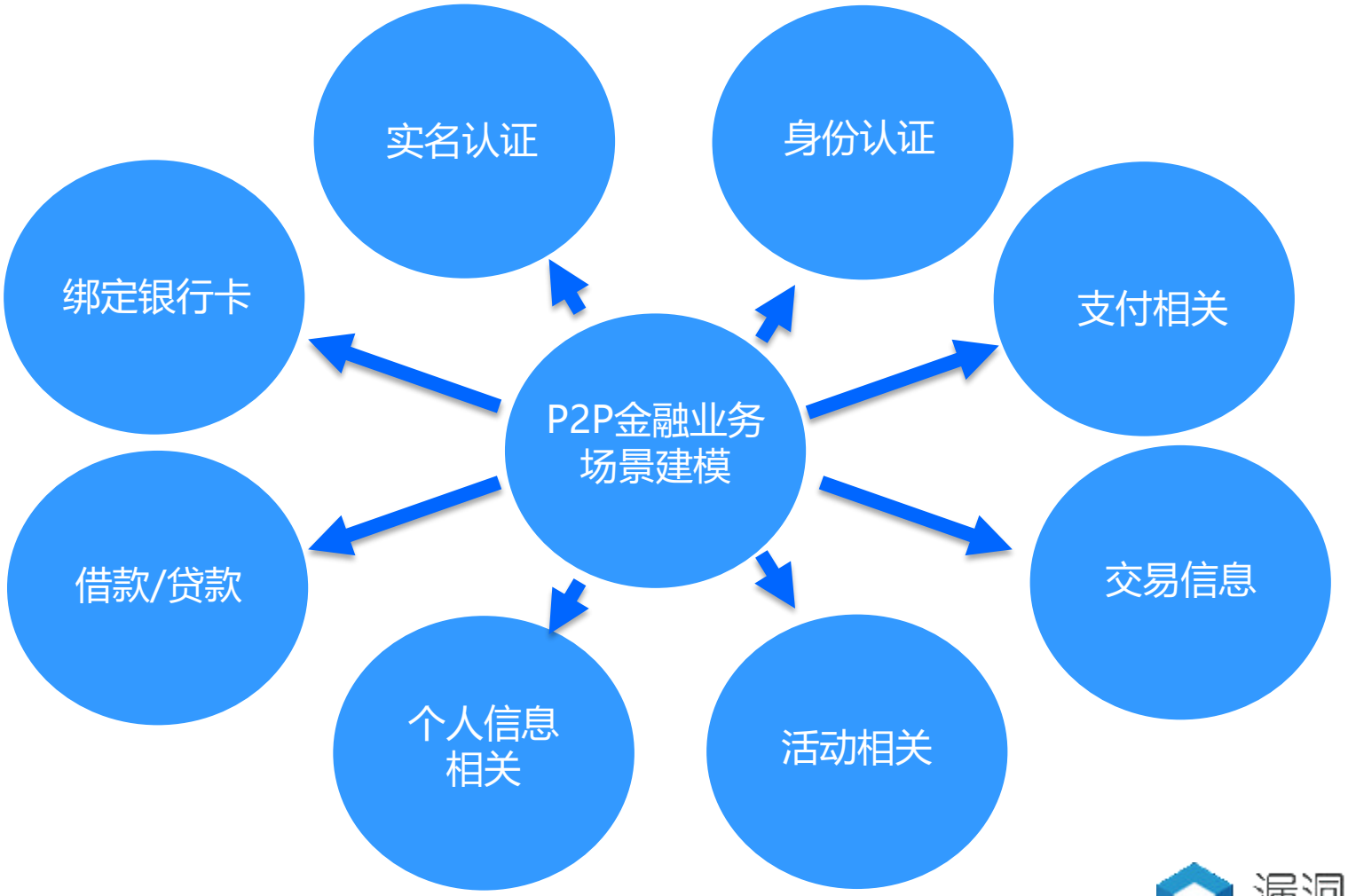
白盒：开发文档

黑盒：主动识别

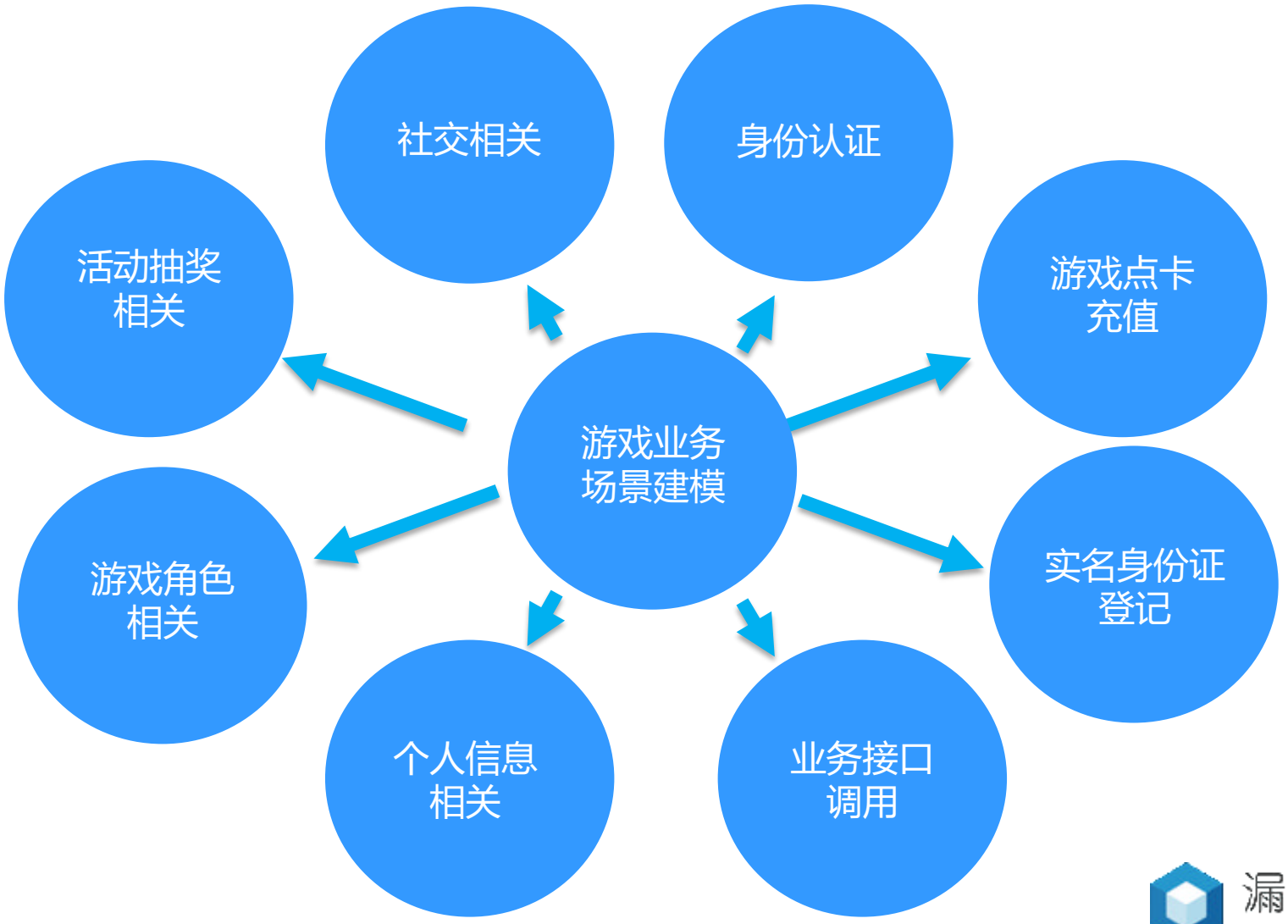
业务场景建模-1 | 电商



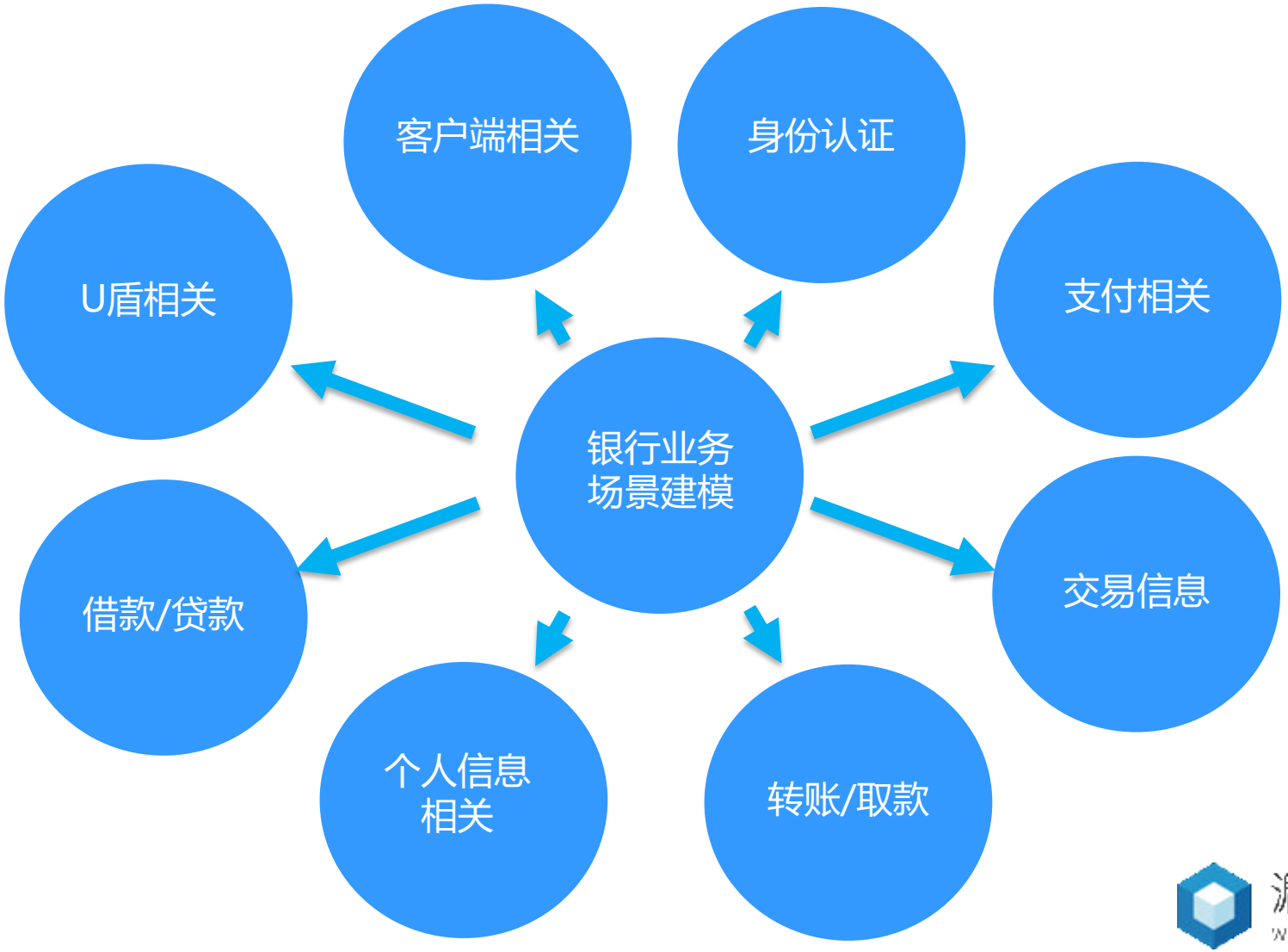
业务场景建模-1 | P2P金融



业务场景建模-1 | 游戏



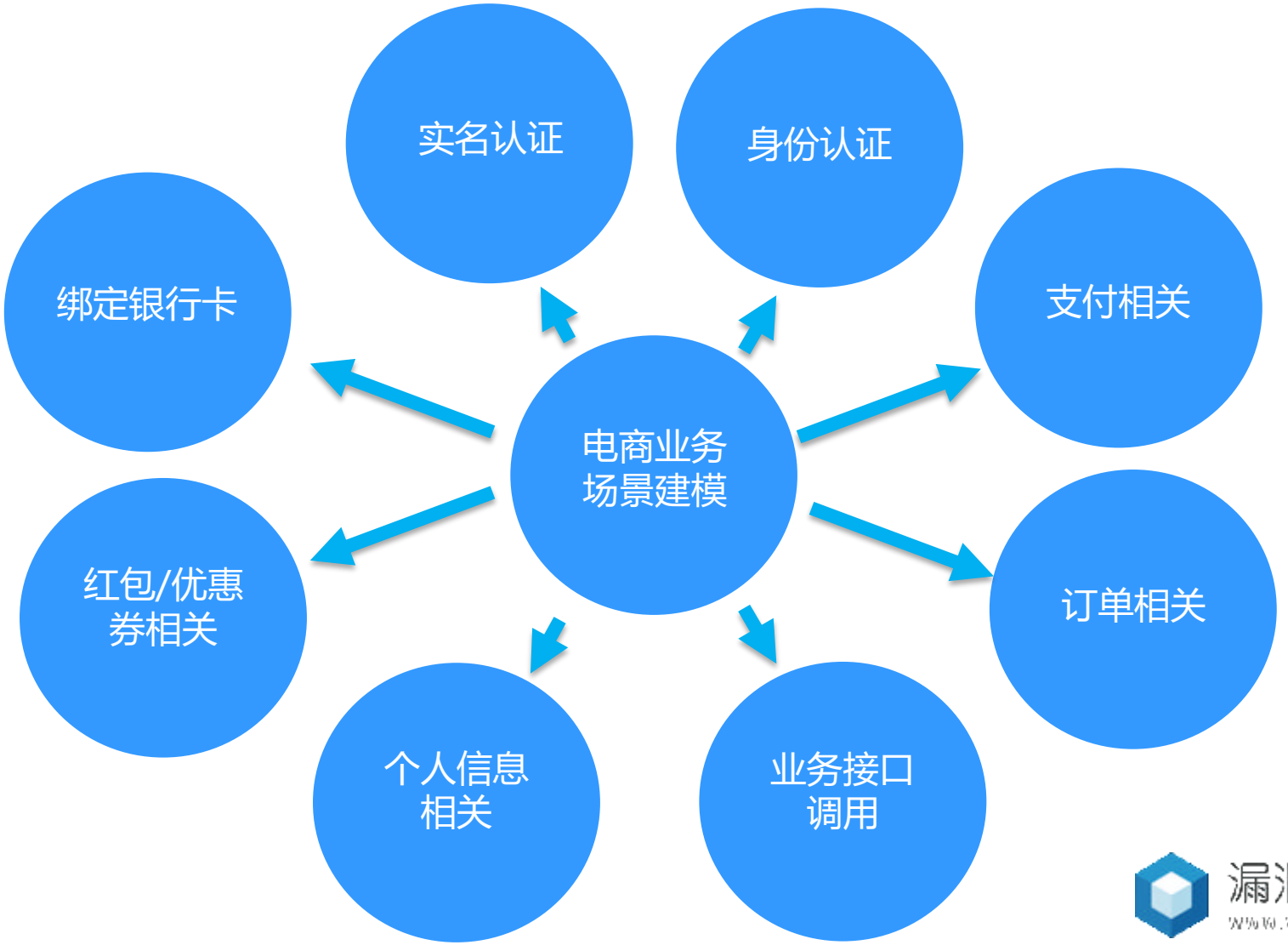
业务场景建模-1 | 银行



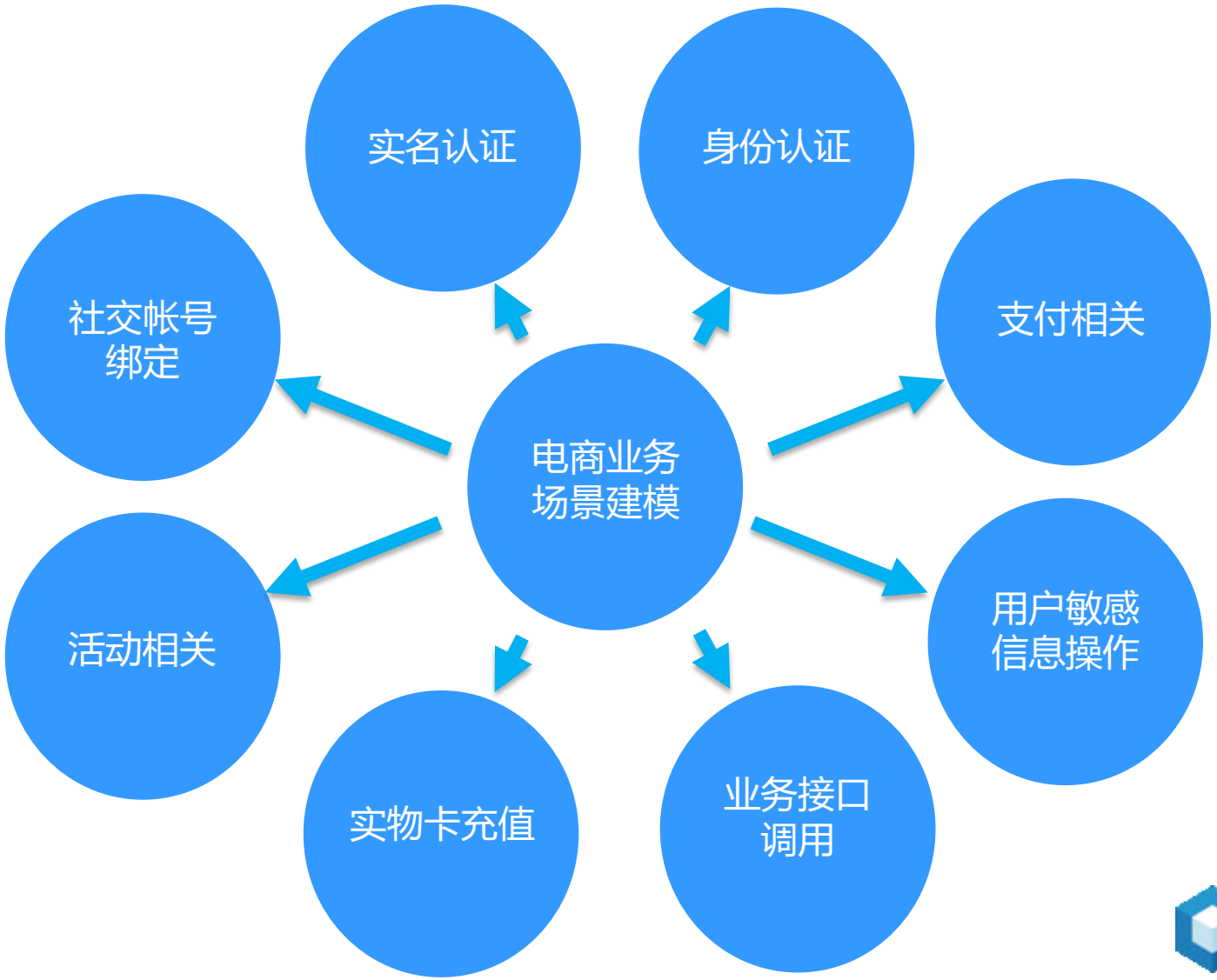
业务场景建模-2

- ✓ 相同行业，即使是相同业务系统，业务场景也不是一成不变的
- ✓ 高风险业务场景识别
- ✓ 需求沟通

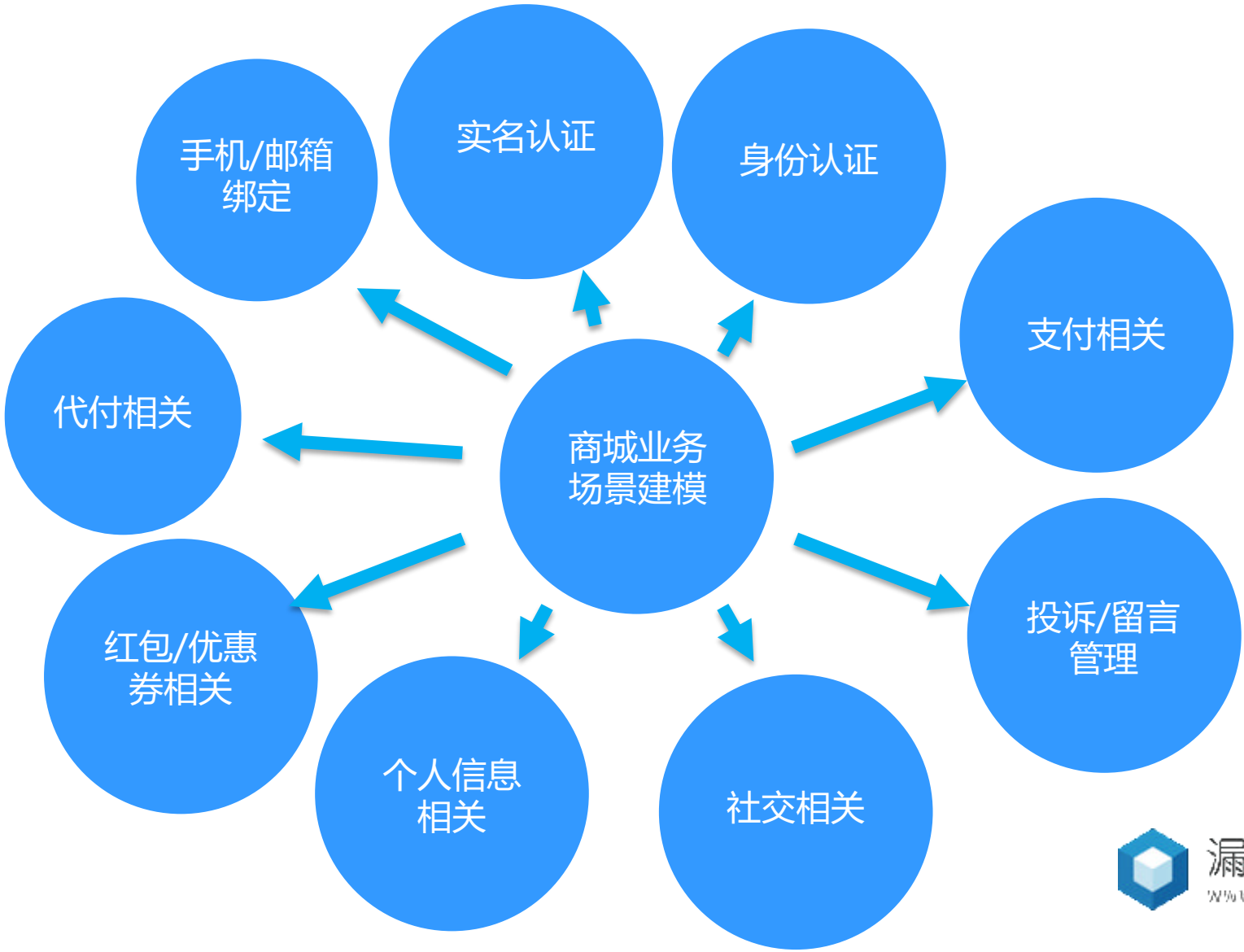
业务场景建模-2 | Plan-A



业务场景建模-2 | Plan-B



业务场景建模-2 | Plan-C



业务流程梳理

- ✓ 识别业务逻辑
- ✓ 应用层数据包梳理
- ✓ 字段功能辨析

密码重置

订单查询

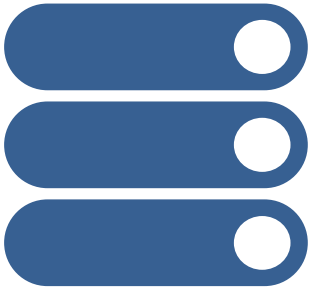
客户端

预查询订单ID

返回用户订单ID

查询用户订单ID详情

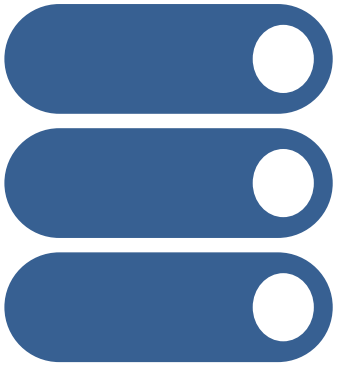
返回订单详情



服务端

支付交易

客户端

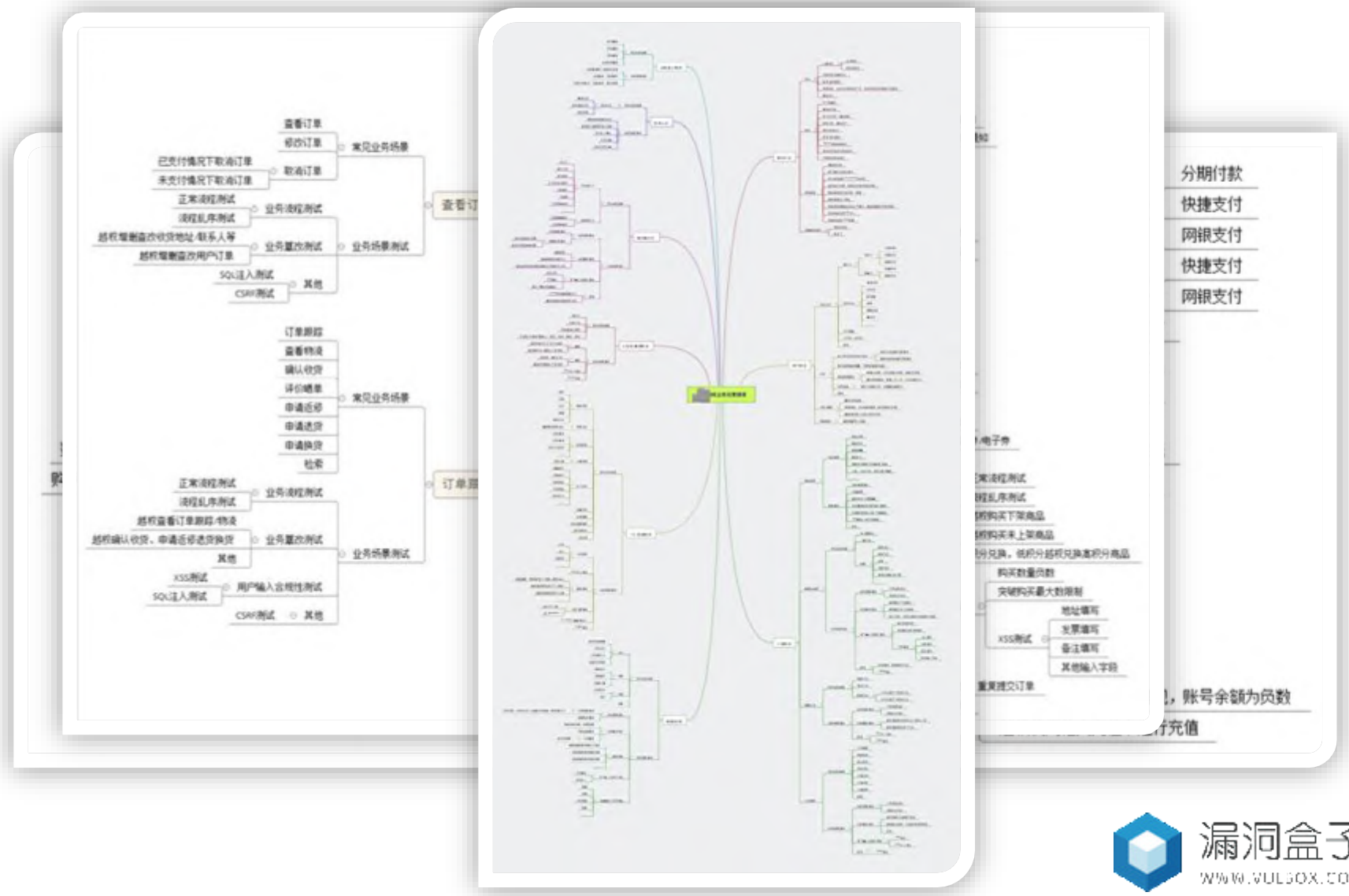


服务端

风险点识别

- ✓ 已知风险对照
- ✓ STRIDE分析方法

风险点识别



密码重置

客户端

Step 1 输入用户名 → **遍历用户名**

验证用户名存在后返回第二步 ← **篡改响应包**

Step 2 发送短信验证码请求 → **篡改手机号**

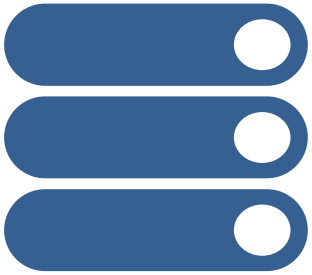
发送验证码后返回第三步 ← **获取验证码**

Step 3 输入短信验证码 → **爆破验证码**

验证短信验证码后返回第四步 ← **篡改响应包**

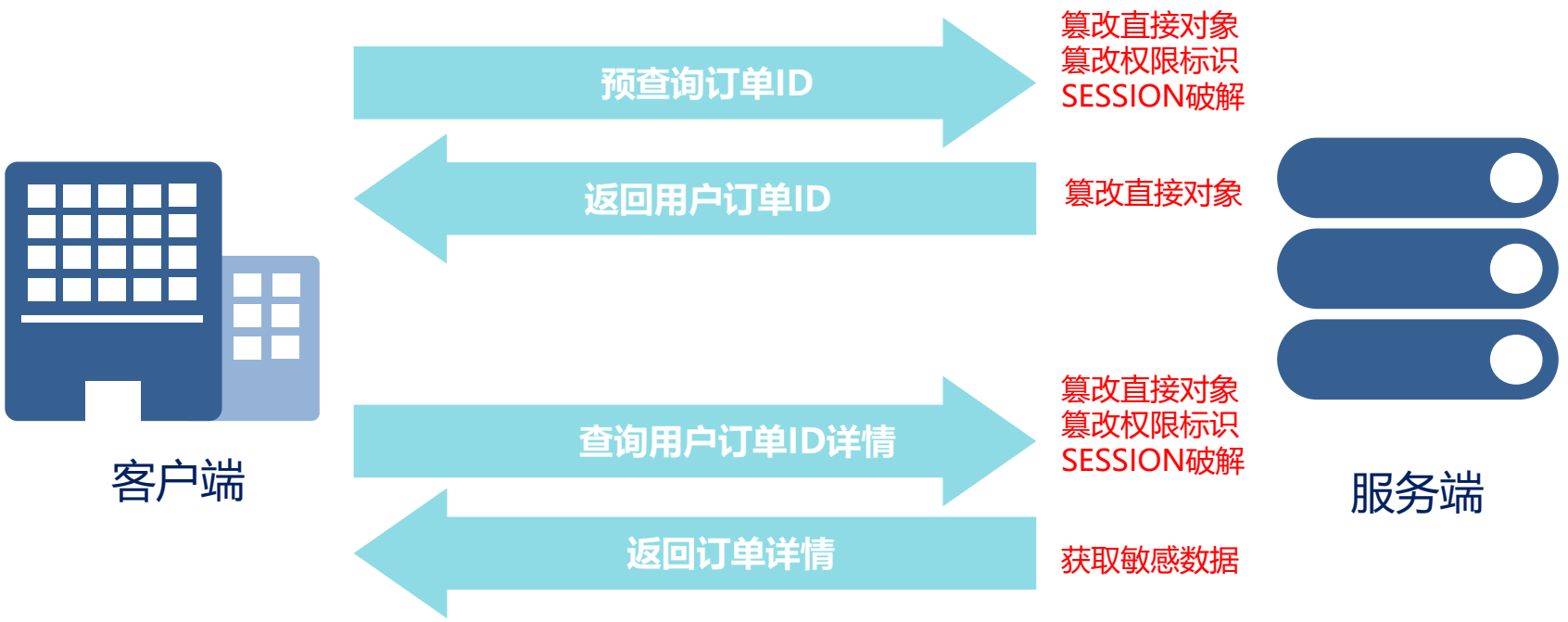
Step 4 输入新密码 → **爆破验证码**

密码修改成功 ← **篡改响应包**



服务端

订单查询



支付交易

客户端

提交订单相关信息

篡改金额
篡改数额
签名破解

返回生成的订单

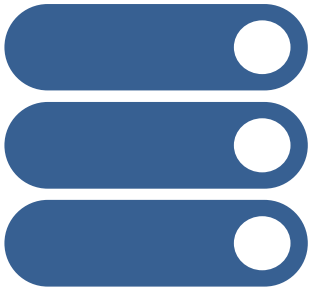
篡改金额
获取敏感数据

支付订单

篡改金额
签名破解

返回支付结果

获取敏感数据



服务端

The STRIDE Threat Model

- ✓ Spoofing identity
- ✓ Tampering with data
- ✓ Repudiation
- ✓ Information disclosure
- ✓ Denial of service
- ✓ Elevation of privilege

业务流程元素	假冒（S）	篡改（T）	否认（R）	信息泄漏（I）	拒绝服务（D）	提升权限（E）
信息流					✖	✖
数据储存	✖	✖		✖	✖	
操作	✖		✖	✖	✖	✖
交互方	✖		✖			✖

THANKS

www.vulbox.com | 漏洞盒子

crs.vulbox.com | 网藤风险感知

www.freebuf.com | FreeBuf