



# 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



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



- ◆ 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

前 言

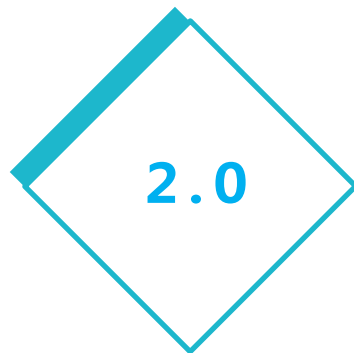
场 景

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



漏洞盒子

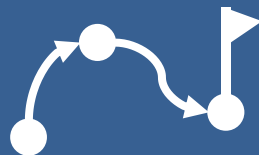
WWW.VULBOX.COM

# 何为业务场景

一个业务系统包含的交互场景



身份认证场景



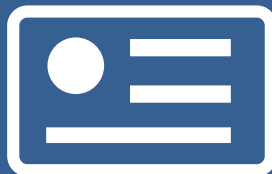
活动场景



支付场景



购物及订单场景



实名认证场景



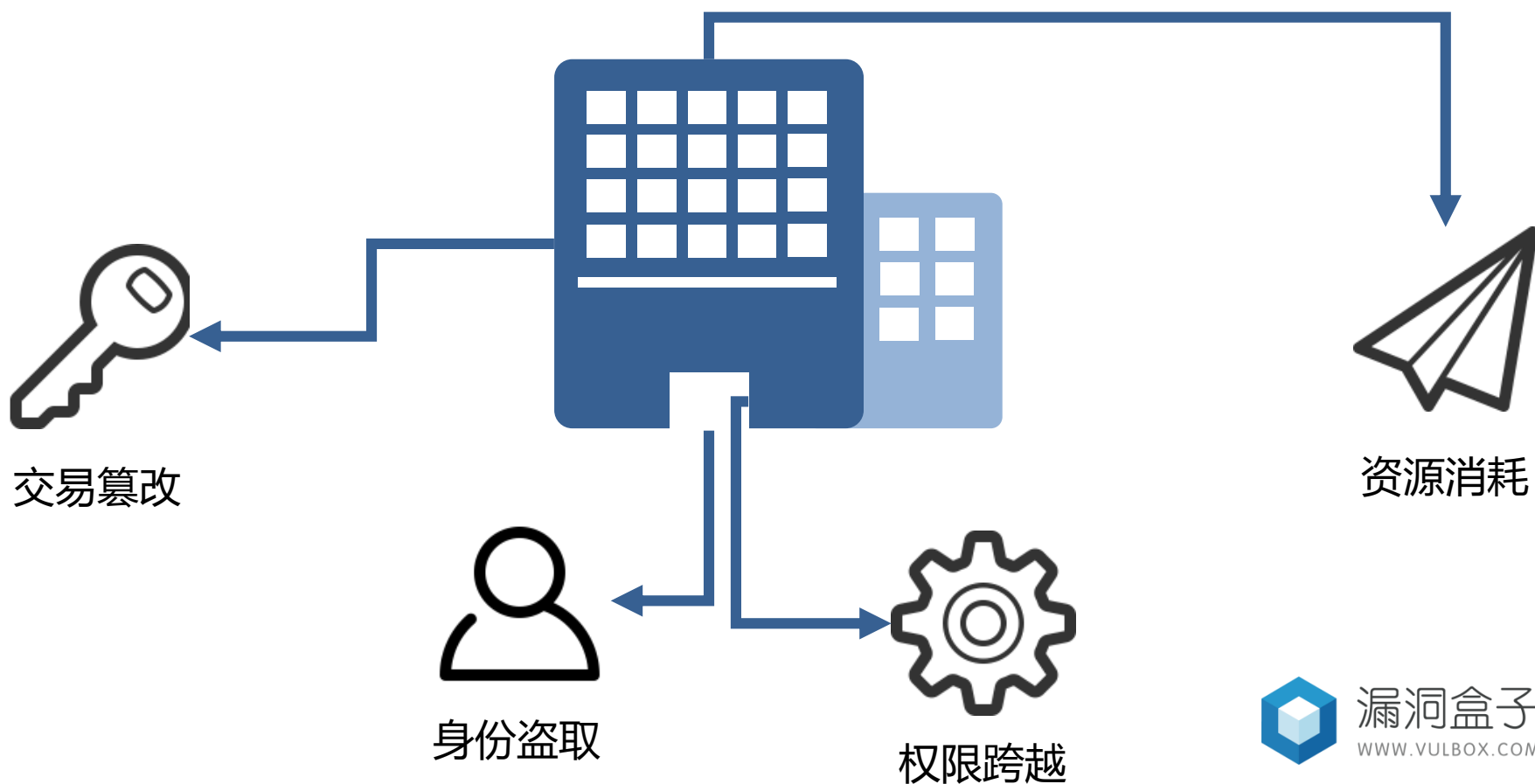
其他场景

# 业务逻辑漏洞是怎样的存在

- ◆ Bypass一切防护设备
- ◆ 至今还没有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 V S 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

登录密码

立即登录

< 找回登录密码

13378813332

请重新设置登录密码

●●●●●●●●

●●●●●●●●

6-20位字母、数字或符号组合

确定

```
Proxy-Connection: keep-alive
Content-Length: 394
Accept-Encoding: gzip, deflate
```

```
abstracts=ca2faf5e3952e8dee16fe3&appOther=i002&appType=001&data=rbXftxodBo
0Jp49Rek2sbDuyM1148%2F%3B%20Secure&encryptType=1&platform
VEftTgX0MPWwwidigiSign=1867CsessionId%3ASFPAY_JSESSIONID%3D
1q4t2aep2y2pq%z114z87480opain%3D%zF%3B%20Secure&encryptType=1&platform
=ios&serviceType=resetpwdFindpwd&timestamp=2184644&version=}
```

diqiSign

```
Proxy-Connection: keep-alive
Content-Length: 394
Accept-Encoding: gzip, deflate
```

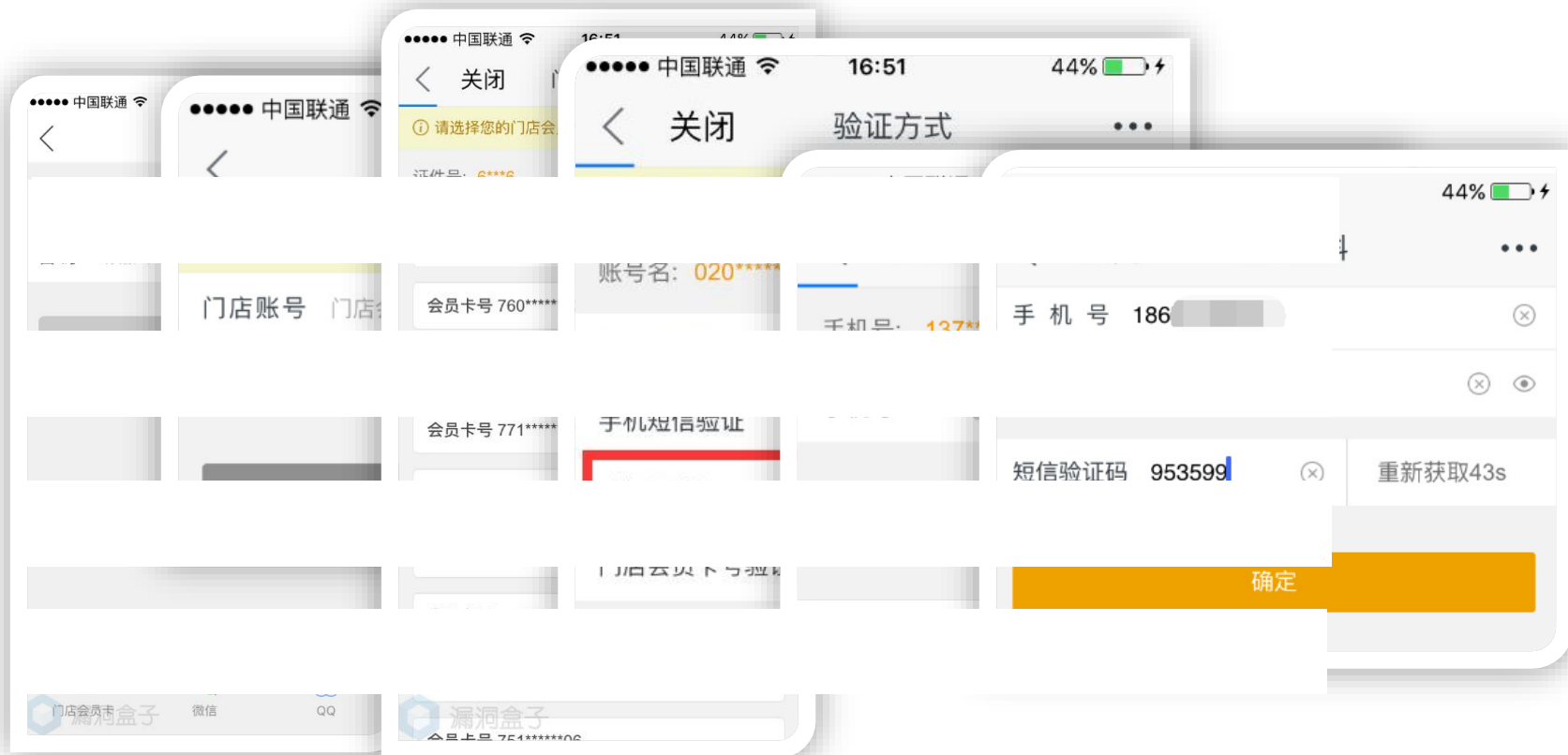
```
abstracts=ca2faf5e3952e8dee16fe3&appOther=i002&appType=001&data=rbXftxodBo
0Jp49Rek2sbDuyM1148%2F%3B%20Secure&encryptType=1&platform
VEftTgX0MPWwwidigiSign=1867CsessionId%3ASFPAY_JSESSIONID%3D
1q4t2aep2y2pq%z114z87480opain%3D%zF%3B%20Secure&encryptType=1&platform
=ios&serviceType=resetpwdFindpwd&timestamp=2184644&version=}
```

```
Content-Length: 217
Servlet/2.5 JSP/2.1
keep-alive
Content-Length: 15, max=100
262072545132 uproxy-8
```

```
4be16979710d4c4e7c664785608856", "code": "00", "data": "", "encryptType": "0", "msg": "验证码不正确",
"session": "V1.0.3")
```



# 身份盗取 | 简单认证



# 身份盗取 | 最后一公里

The image displays a sequence of web browser screenshots illustrating a security breach. The top screenshot shows a browser window with the URL `/user/findPwd_modify.do` and a status bar indicating a breakpoint hit. Below this, a success message is shown: "密码修改成功!" (Password change successful!) with a checkmark icon and the instruction "请妥善保管好您的新密码" (Please妥善保管好您的新密码). A "登录" (Login) button is visible. The bottom screenshot shows a user profile page for "admin" with a red box highlighting the name and a mouse cursor pointing to it. The page includes a navigation bar with "保险分类与服务" (Insurance categories and services), "漏洞盒子" (VulnBox), "首页" (Home), and "产品中心" (Product center).

# 权限跨越 | 垂直水平

Cookie: SESSION=USER-334dsf9ref8esg8erg390g

Cookie: SESSION=USER-3dfg34768jh4h234g5h5jk

Cookie: SESSION=USER-304jkh6g9090ertk45g0s9

Cookie: SESSION=USER-2dfg34768jh4h234g5h5jk

Cookie: SESSION=USER-1dfg34768jh4h234g5h5jk

# 权限跨越 | 垂直水平



用户检查：

session=34dsf9ref8esg8erg390g

权限检测：

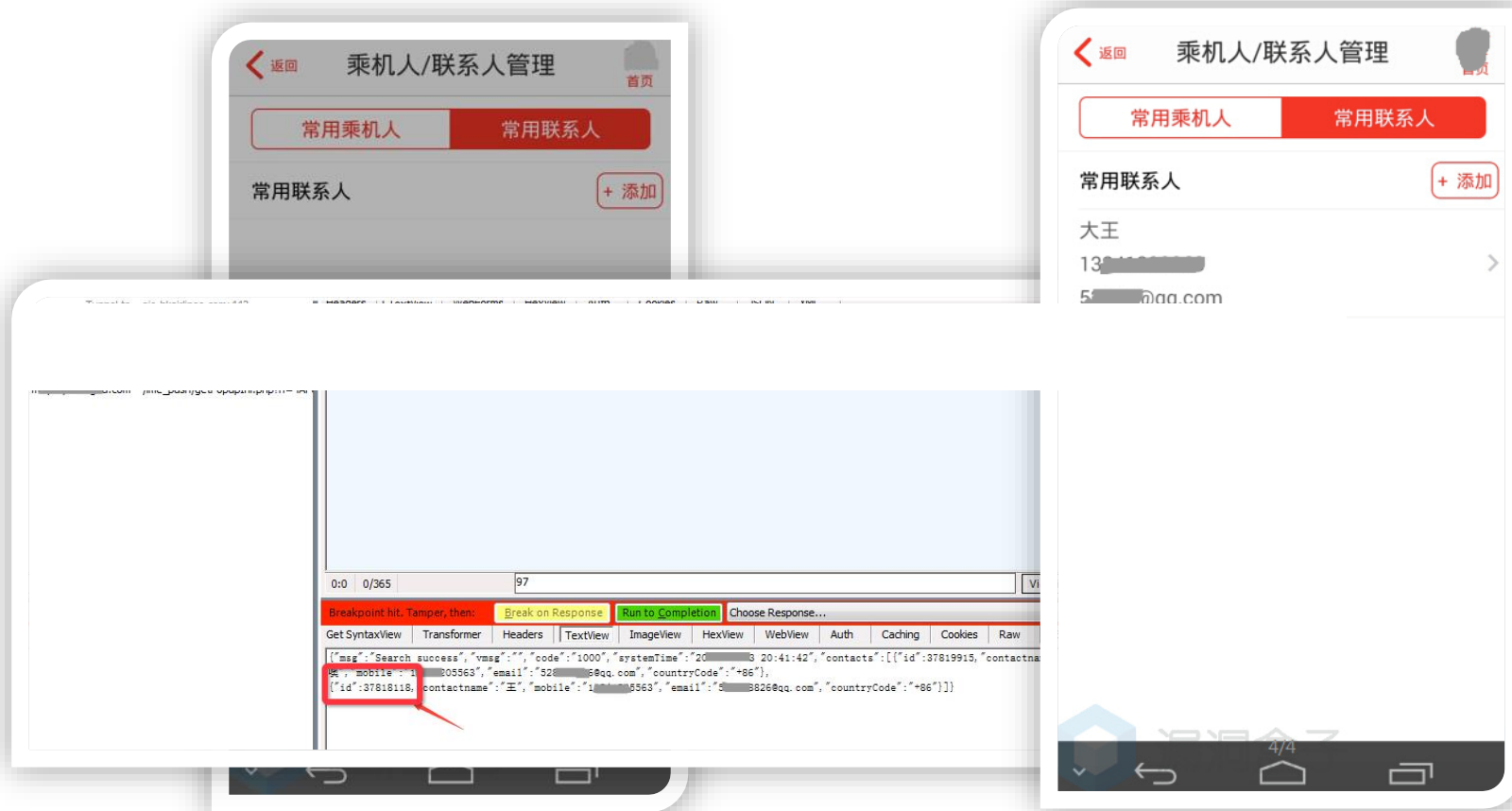
level=3

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

```
CNZZDATA1252940216=13084554... 5880408-%7C1415890632; IESESSION=alive;
```

Content-Length: 769

```
A988_secocode8173bd43=myt5IDr8PqdqMmeSXf... mdojrdhBrQU_kNmF;
```

```
A988_msgnewnum427=0; A988_cart_goods_num=1
```

```
Connection: keep-alive
```

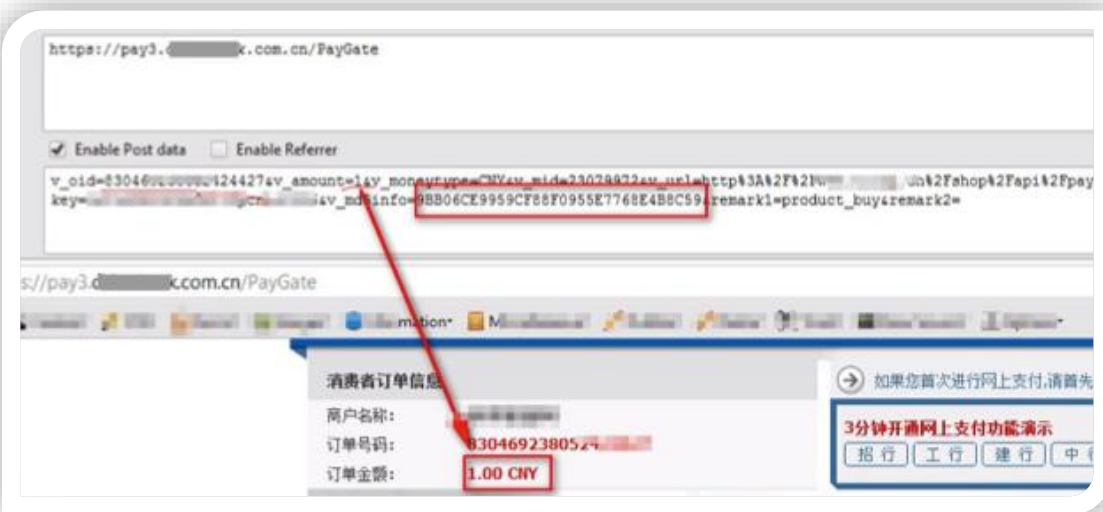
```
Content-Type: application/x-www-form-urlencoded
```

```
Content-Length: 71
```

```
pay_sn=900469... 799427&payment_code=chinabank&order_type=product_buy
```

```
type='hidden' name='v_moneytype' value='CNY' /> <input type='hidden'  
value='23079972' /> <input type='hidden' name='v_url'  
value='http://www.gllzp.cn/shop/api/payment/chinabank/return_url.php'  
name='key' value='la... 006' /> <input type='hidden' na  
value='4A6530A781122A091BEE650F51E924F9' /> <input type='hidden'  
value='product_buy' /> <input type='hidden' name='remark2' value='' /  
type="text/javascript"> document.E_FORM.submit(); </script> </body
```

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-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.101 Mobile Safari/537.36
Content-Type: application/json
Referer: http://[REDACTED].com/5/getform.do
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie: _utmv=269921210.12=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



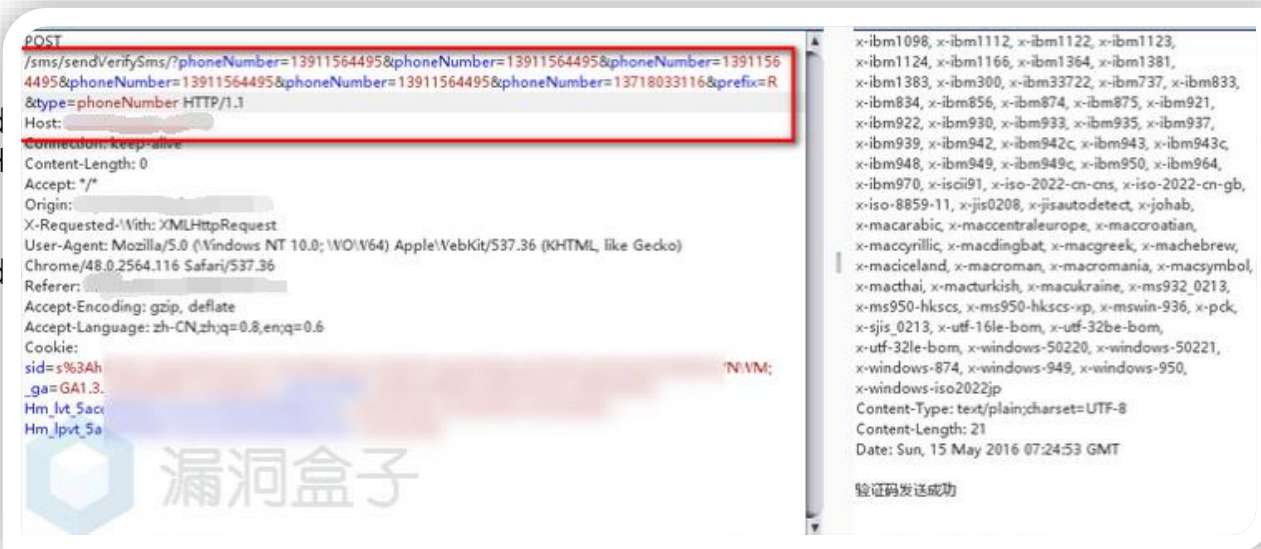
# 资源消耗 | 变量覆盖



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

GET /sms/send  
Number H

GET /sms/send  
HTTP/1.1



&type=phone

pe=phoneNumber

# 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

可使用

已使用

已作废

**肯德基**

肯德基冰淇淋花筒1只

1张

可使用

**肯德基**

肯德基冰淇淋花筒1只

1张

可使用

**肯德基**

肯德基冰淇淋花筒1只

1张

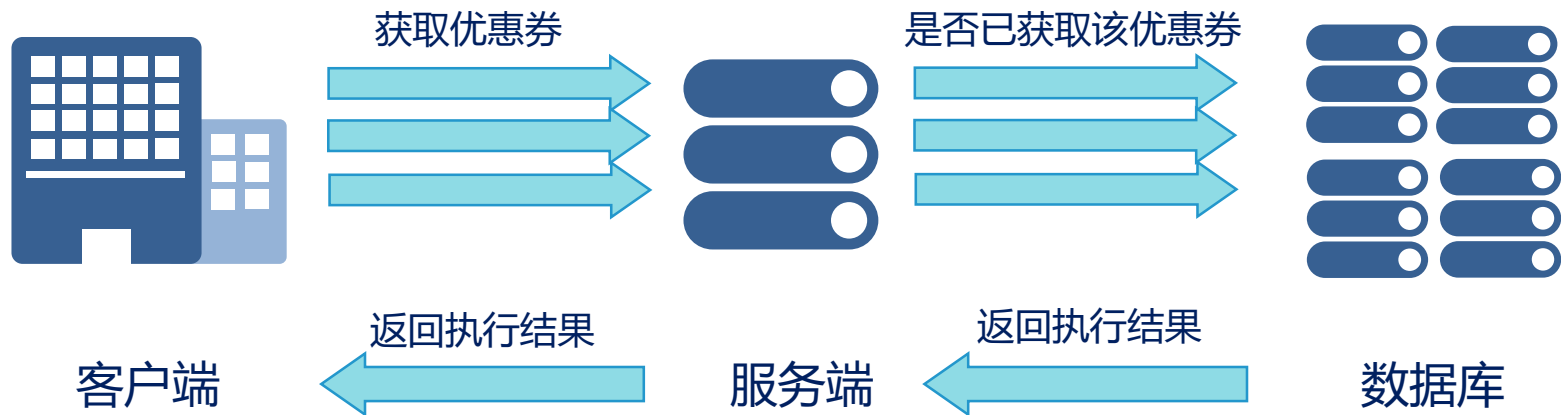
可使用



漏洞盒子

WWW.VULBOX.COM

# 资源消耗 | 并发请求



- ◆ 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



2014年5月6日 - 不知道从啥时候开始,白领流行薅羊毛~~由于红影很久以前就混迹于各大理财网站,于是,也跟着羊友开始薅羊毛了~~这几年,也陆陆续续薅过一些羊毛,比如话费啊,实物...

[www.talica.com/diary/...](http://www.talica.com/diary/) - 百度快照 - 65%好评

### [网上分分钟薅羊毛 网下分分钱都要赚\\_凤凰网资讯](#)

2014年6月13日 - 根据“滴滴打车”公布的数据,在一个月里,“滴滴打车”平均每天有微信支付订单70万单,补贴总额4亿元。同时,如何更高效地薅羊毛,利用打车软件赚钱的攻...

[news.ifeng.com/a/20140...](http://news.ifeng.com/a/20140...) - 百度快照 - 166条评价

### [“薅羊毛”致富全攻略 教你避开90%的理财陷阱-搜狐](#)

2016年4月20日 - 薅羊毛也能月入五万?是的,最近有媒体记者潜伏在羊毛党群里,发现P2P圈里存在着大量的羊毛党,对于职业羊毛党来说,月入三五万的也是很正常的。P2P的...

[mt.sohu.com/20160420/n...](http://mt.sohu.com/20160420/n...) - 百度快照 - 674条评价

### [90后的省钱妙招:教你怎样薅羊毛\\_凤凰网财经](#)

2015年2月13日 - 相较于需要更多知识与经济基础的投资理财来说,一种更为“低门槛”的“薅羊毛”式的变相理财方式也日渐为“80后”、“90后”们所推崇。因为“薅...

[finance.ifeng.com/a/20...](http://finance.ifeng.com/a/20...) - 百度快照 - 124条评价

### [薅羊毛有技巧 千万别羊毛没薅到还丢了剪刀-希财网](#)

2015年5月16日 - 事实上,薅羊毛这个词并非天生和p2p联系在一起。根据网络解释,薅羊毛的群体多以80后人群为主,对银行等金融机构以及各类商家开展的一些优惠活动引发兴趣...

[www.csai.cn/p2pzixun/7...](http://www.csai.cn/p2pzixun/7...) - 百度快照 - 688条评价

### [听说有大神一年羊毛收入过千万~~ 薅羊毛 - 信用卡论坛-... 我爱卡](#)

13条回复 - 发帖时间: 2015年2月20日

2015年2月20日 - 卡论坛»论坛,信用卡与生活,薅羊毛,听说有大神一年羊毛收入过...每张卡最少兑换一两千万的积分,最多的一张卡兑换了8000多万积分,总共兑换的...

[bbs.51credit.com/for.....](http://bbs.51credit.com/for.....) - 百度快照 - 63条评价

### [一夜之间羊毛族薅走上千万元\\_财经\\_环球网](#)

2015年11月11日 - 据了解,9日晚间,不少兴奋的“羊毛族”在微信、微博等晒出多笔交易记录,有人甚至炫耀,“已薅80万,准备跑路”。市场人士预测,快操盘一夜之间损失的...

[finance.huanqiu.com/ro...](http://finance.huanqiu.com/ro...) - 百度快照 - 142条评价

## 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

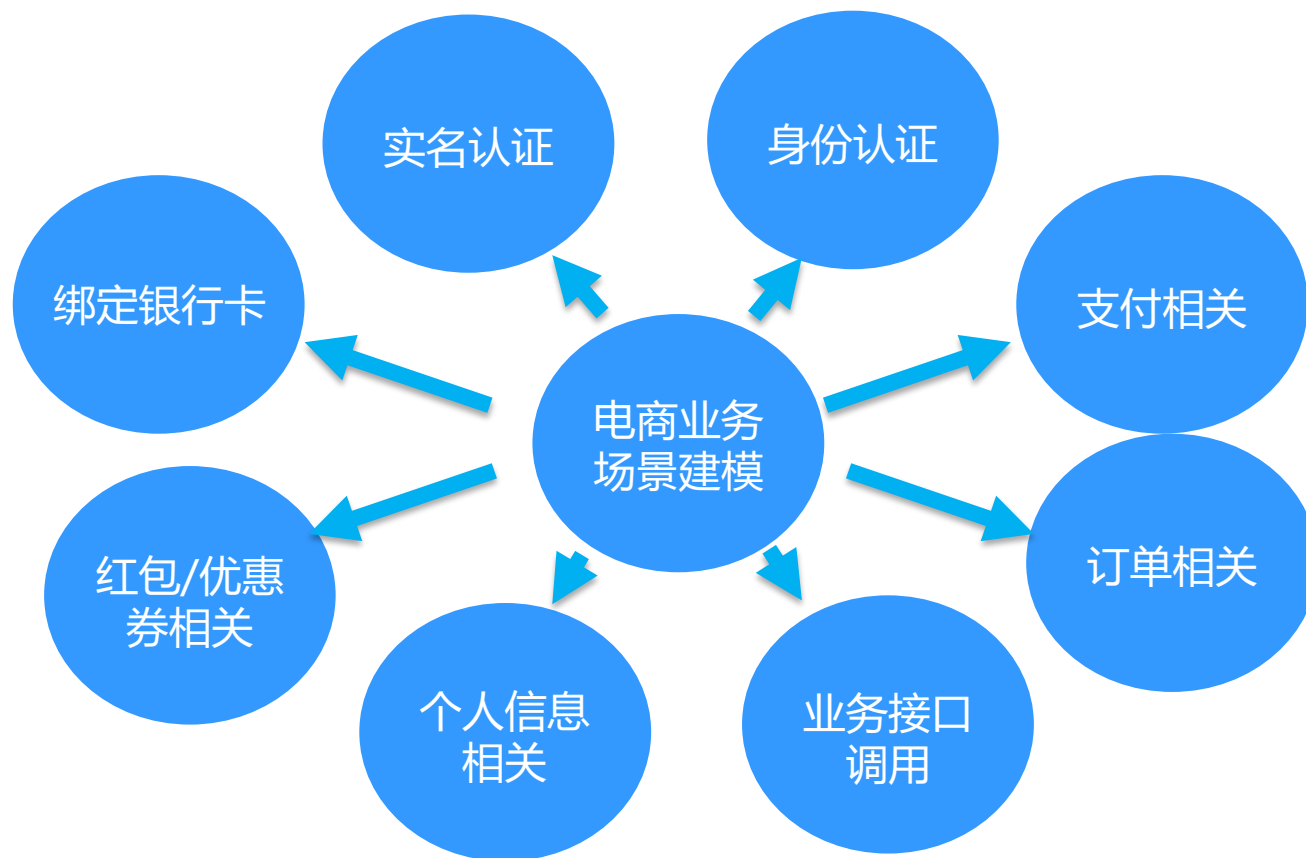
## 不同行业业务场景有所异同

如：银行、金融、保险、证券、电商、O2O、游戏、社交、招聘、航空

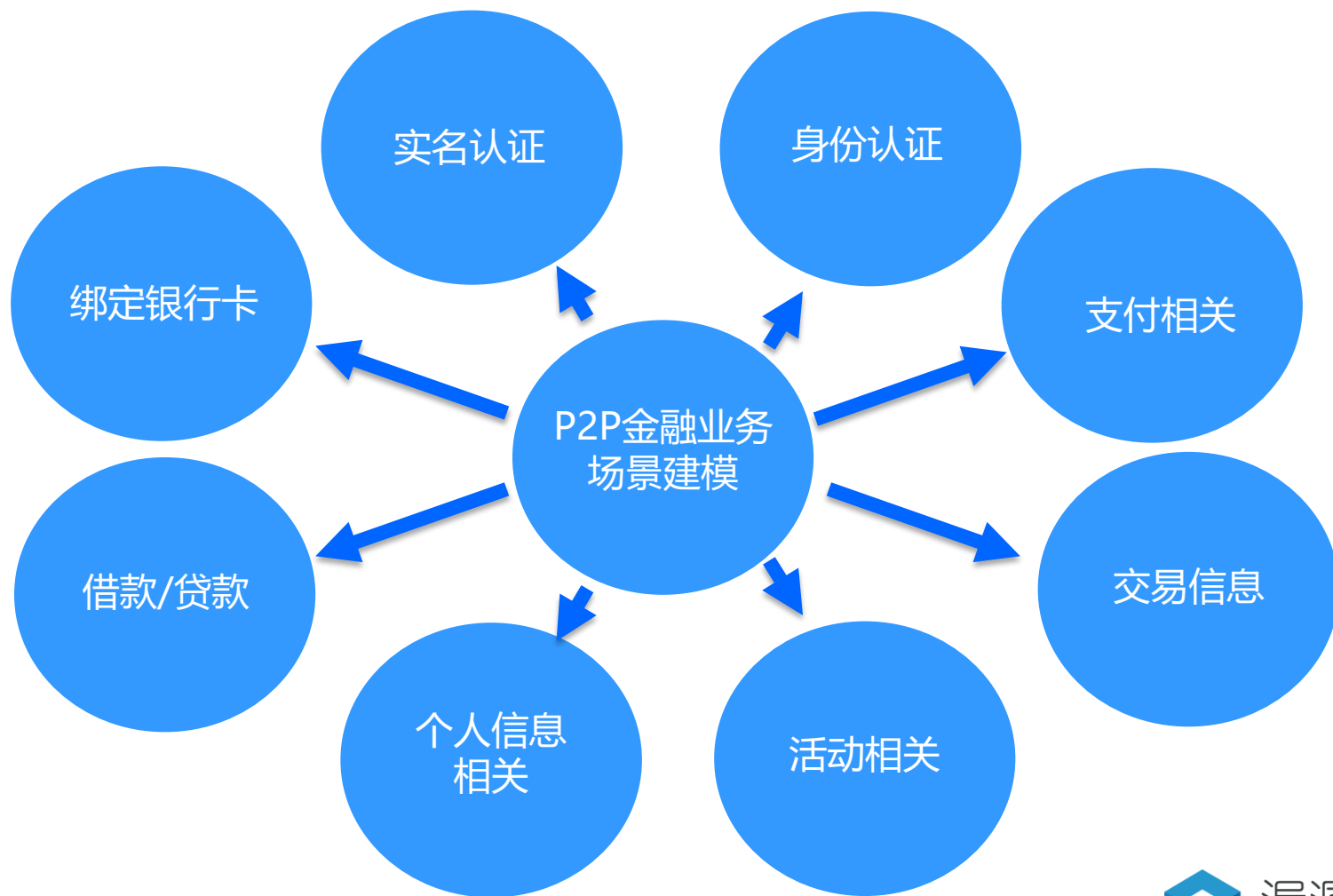
白盒：开发文档

黑盒：主动识别

# 业务场景建模-1 | 电商

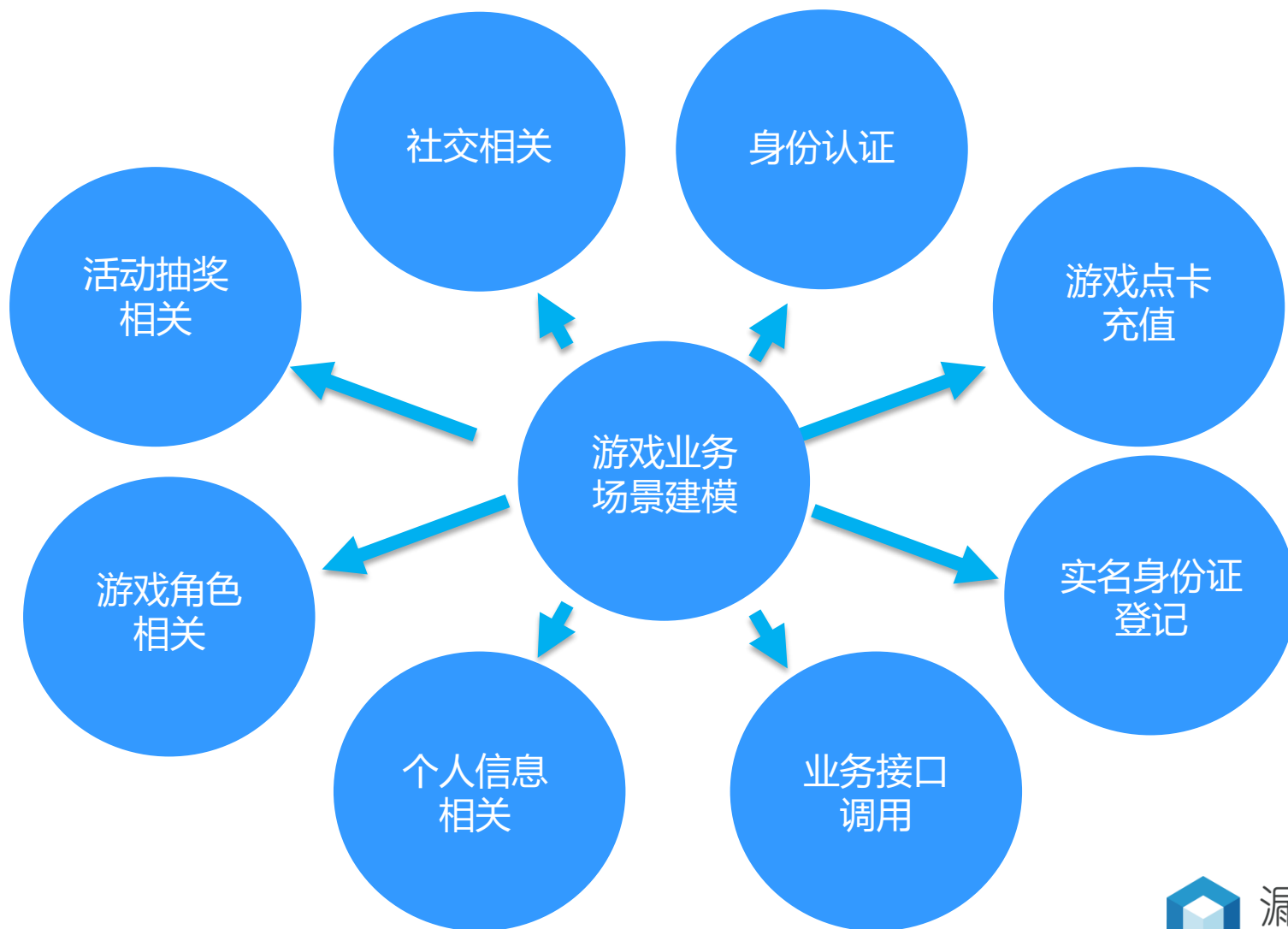


# 业务场景建模-1 | P2P金融

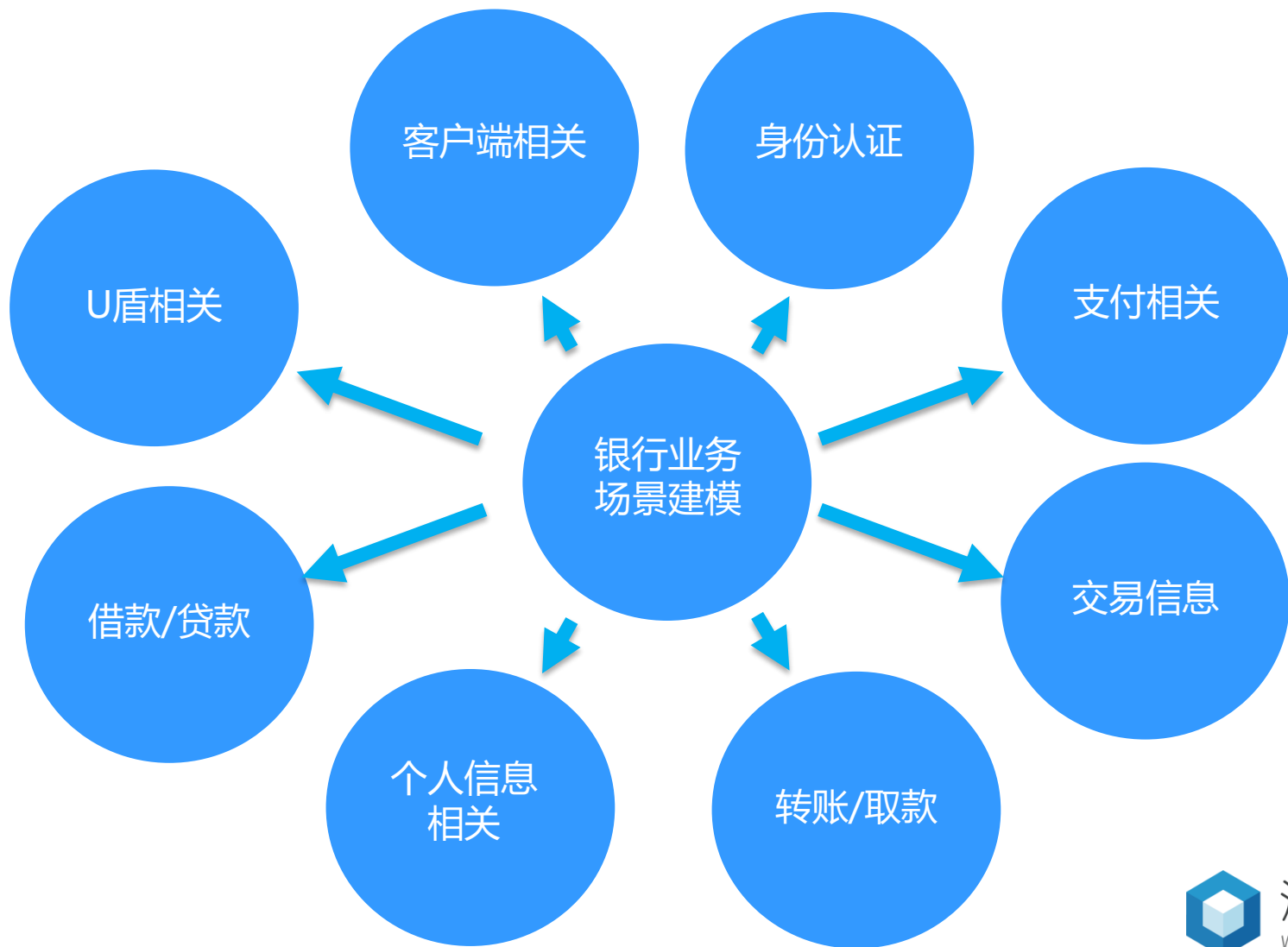




# 业务场景建模-1 | 游戏



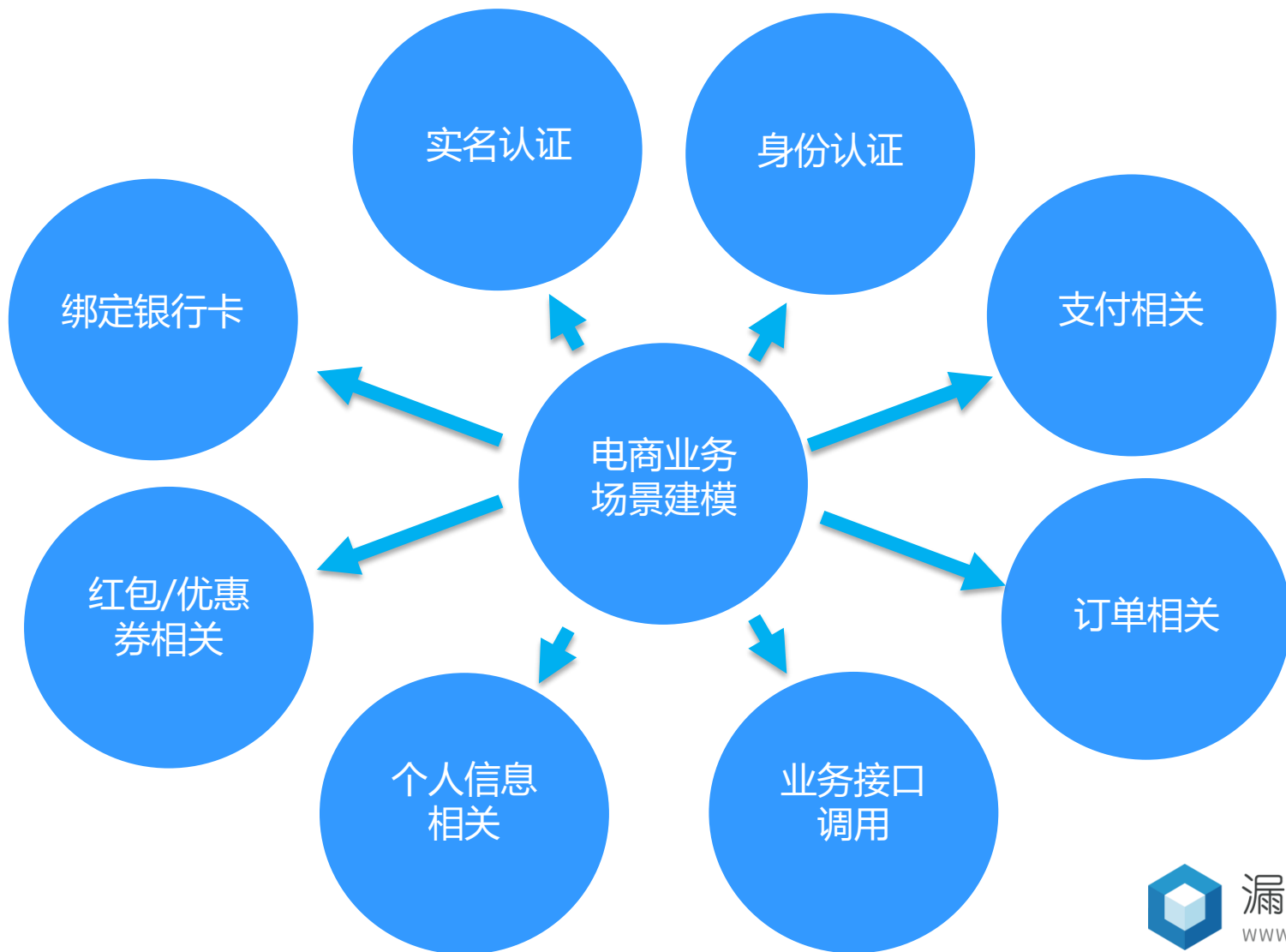
# 业务场景建模-1 | 银行



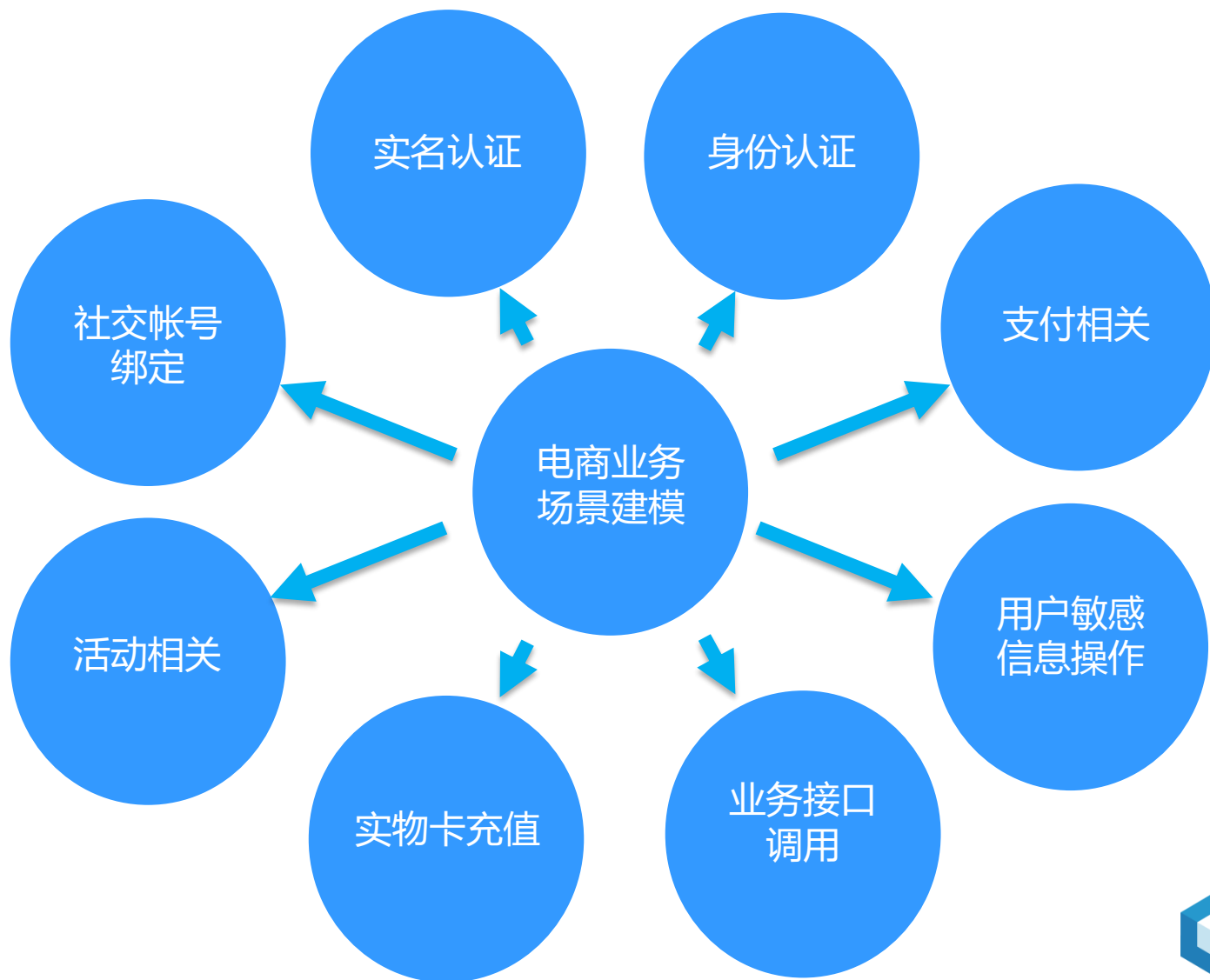
## 业务场景建模-2

- ✓ 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

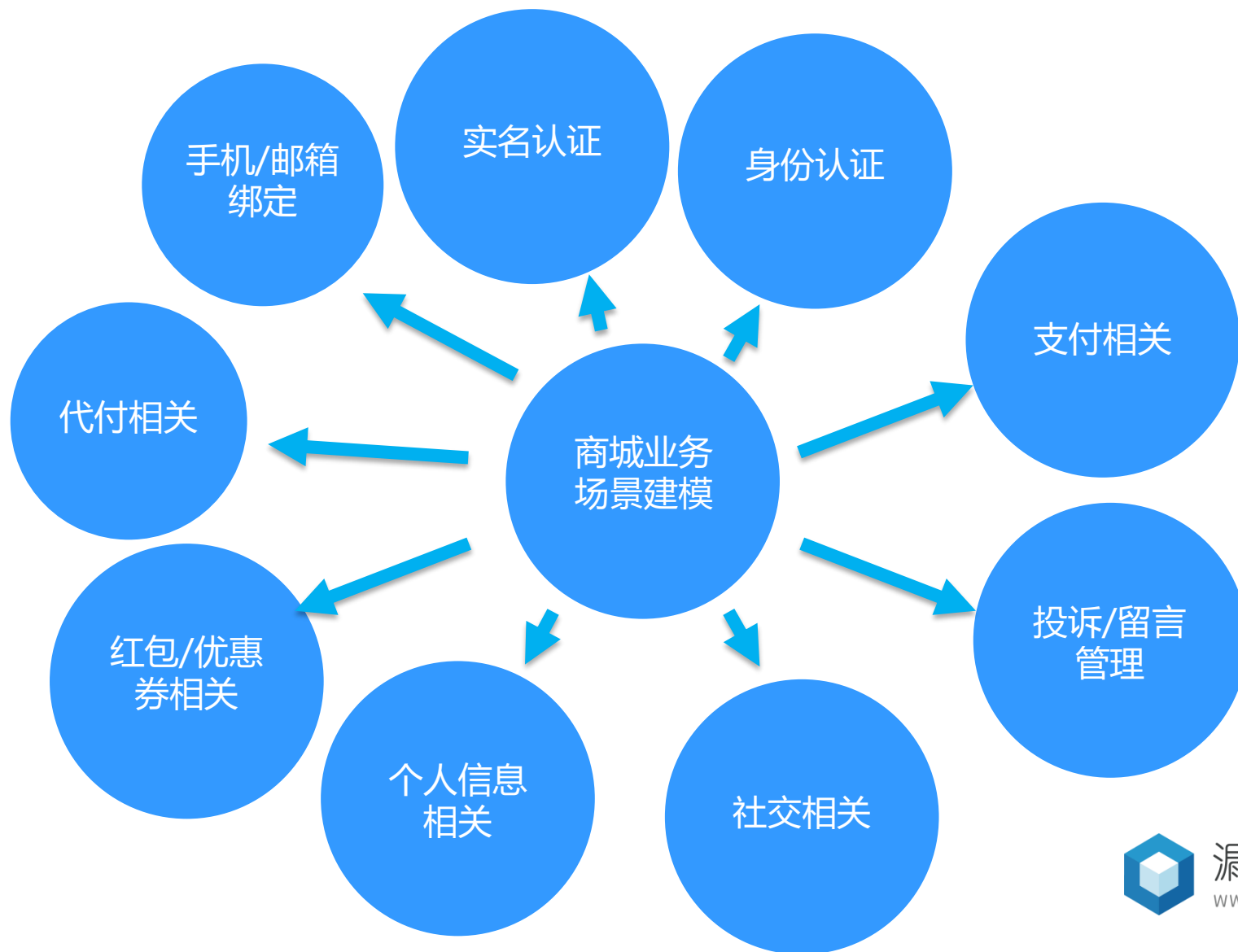
# 业务场景建模-2 | Plan-A



# 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



客户端

Step 1

输入用户名

验证用户名存在后返回第二步

Step 2

发送短信验证码请求

发送验证码后返回第三步

Step 3

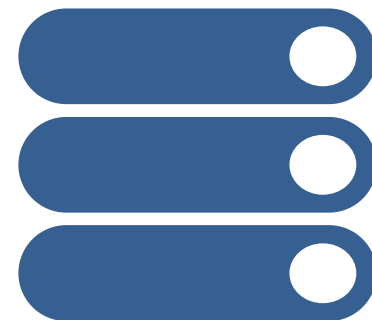
输入短信验证码

验证短信验证码后返回第四步

Step 4

输入新密码

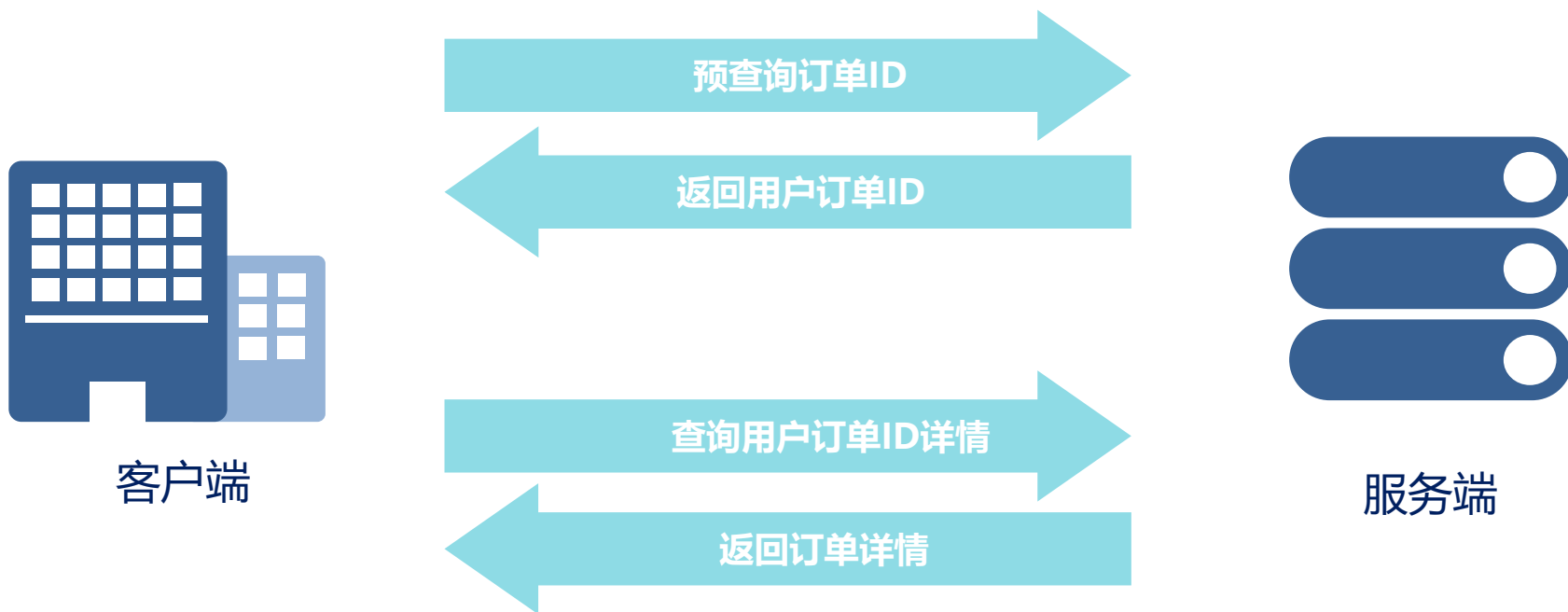
密码修改成功



服务端



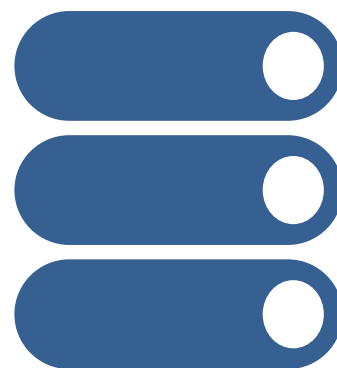
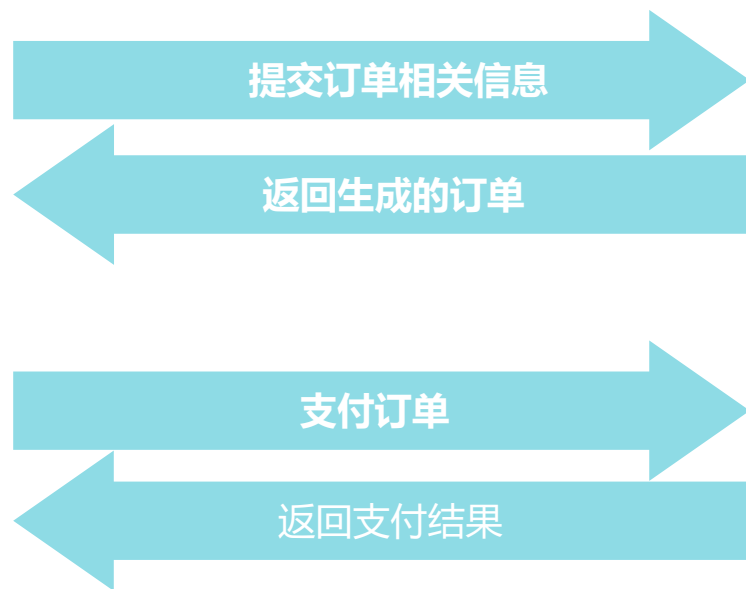
# 订单查询



# 支付交易



客户端

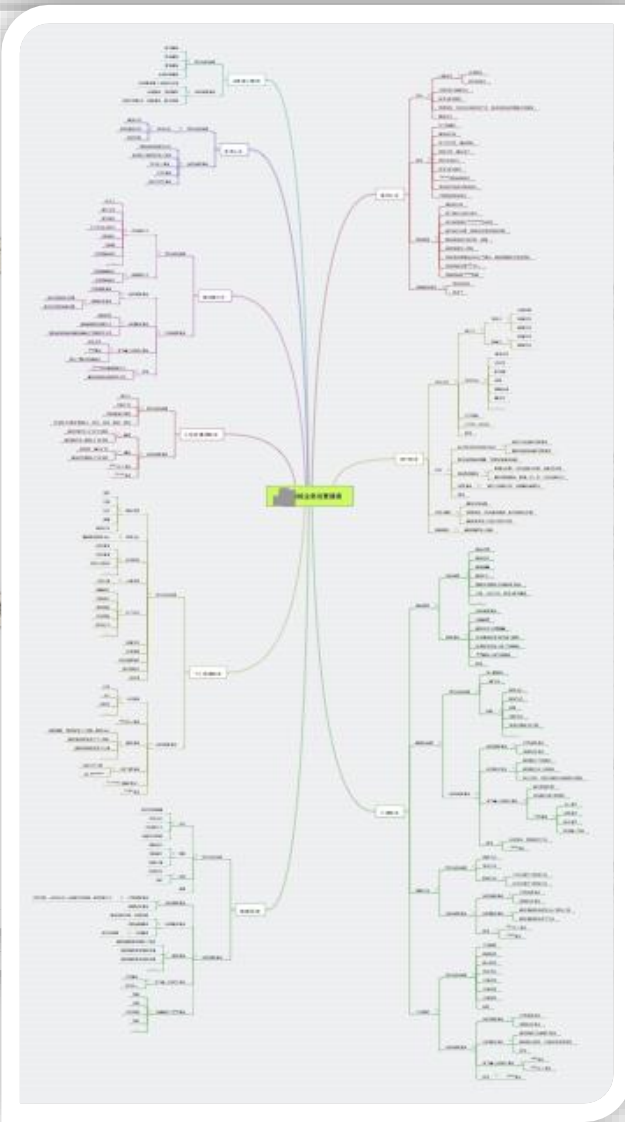


服务端

# 风险点识别

- ✓ 已知风险对照
- ✓ STRIDE分析方法

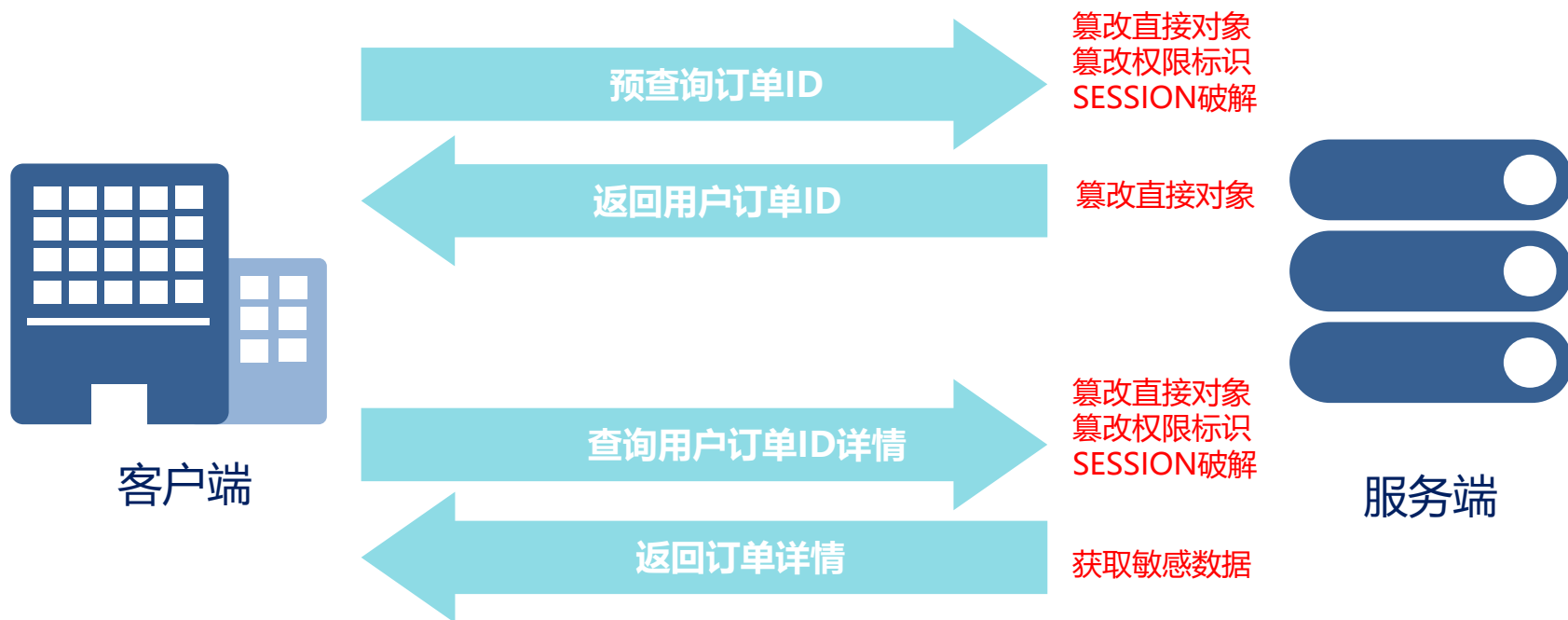
# 风险点识别



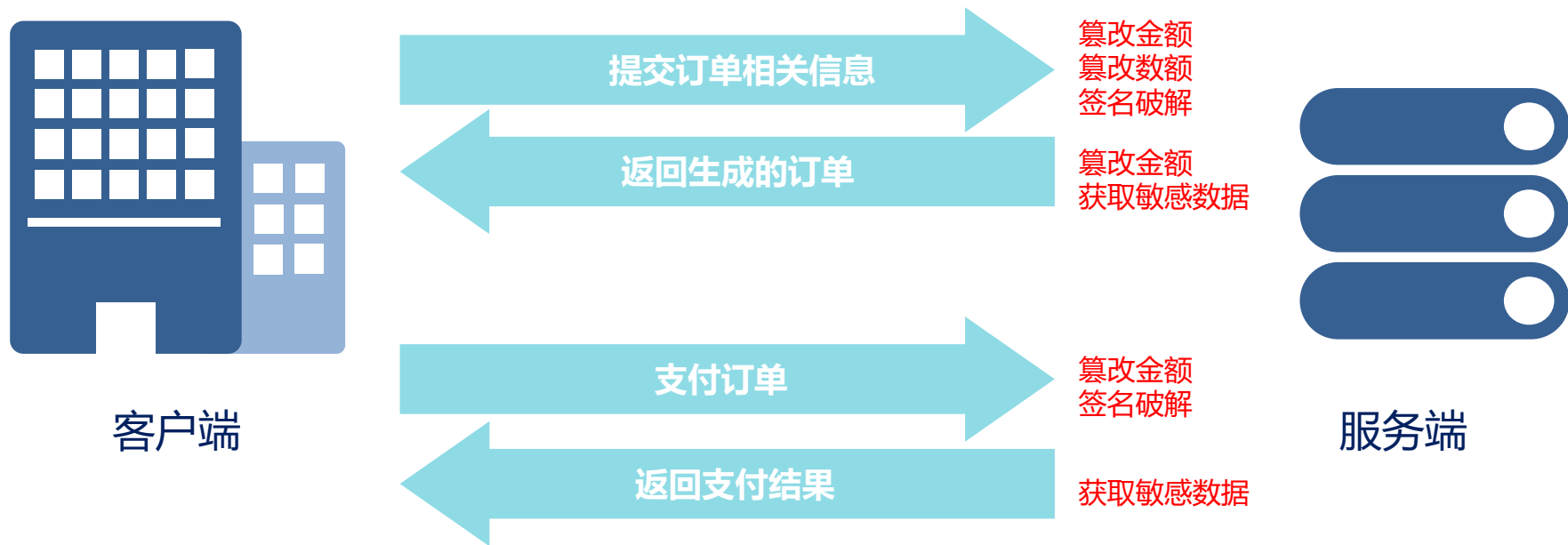
# 密码重置



# 订单查询



# 支付交易



# 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](http://www.vulbox.com) | 漏洞盒子

[crs.vulbox.com](http://crs.vulbox.com) | 网藤风险感知

[www.freebuf.com](http://www.freebuf.com) | FreeBuf