



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



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



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

前 言

场 景

方 法

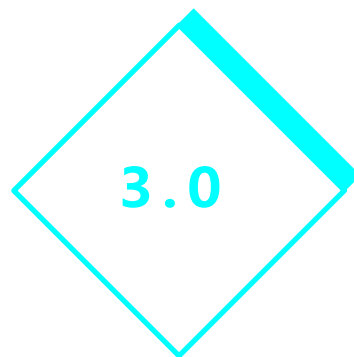
企业安全测试进化史



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



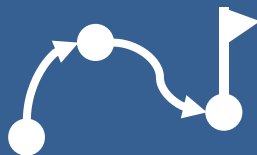
漏洞盒子
WWW.VULBOX.COM

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



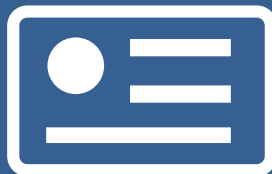
活动场景



支付场景



购物及订单场景



实名认证场景



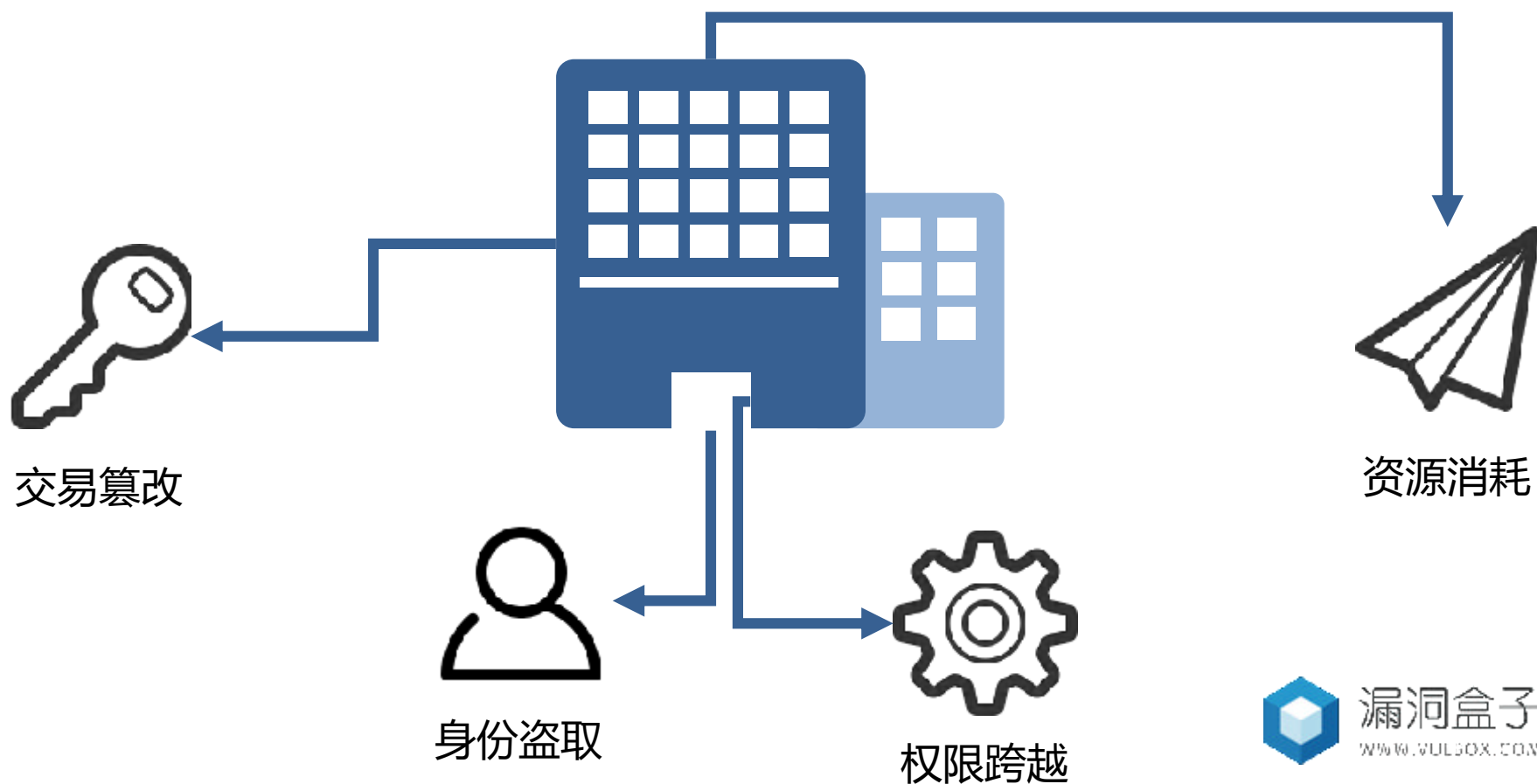
其他场景

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

135****3632

登录密码

立即登录

< 找回登录密码

135****3632

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=ca2faf5e39.....52e8dee16fe3&appOther=i002&appType=001&data=rbXfTxdBo
0Jp49Rek2sbDuyM1.....MhLQTSntC34JmBVgpLIUW2yzWTowrCrj
VEfTtGx0MPWww.....digiSign=18.....67CsessionId%3ASFPAY_JSESSIONID%3D
1q4t2aep2y2pq%2114261480.....opain%3D%2F%3B%20Secure&encryptType=1&platform
=ios&serviceType=resetpwdFindpwd×tamp=2.....184644&version=.....}

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

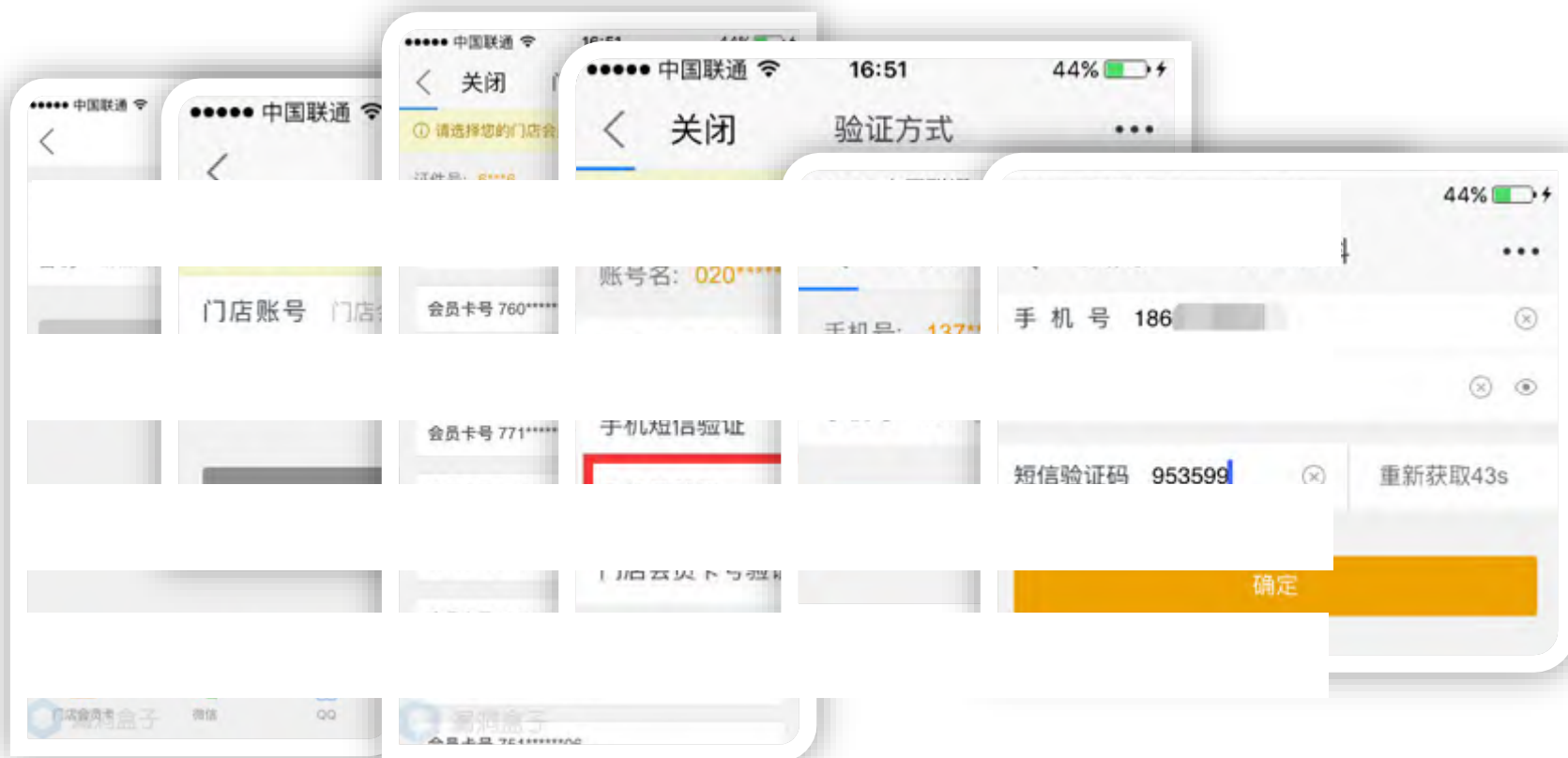
abstracts=ca2faf5e39.....52e8dee16fe3&appOther=i002&appType=001&data=rbXfTxdBo
0Jp49Rek2sbDuyM1.....MhLQTSntC34JmBVgpLIUW2yzWTowrCrj
VEfTtGx0MPWww.....digiSign=18.....67CsessionId%3ASFPAY_JSESSIONID%3D
1q4t2aep2y2pq%2114261480.....opain%3D%2F%3B%20Secure&encryptType=1&platform
=ios&serviceType=resetpwdFindpwd×tamp=2.....184644&version=.....}

Servlet/2.5 JSP/2.1
ep-alive
eout=15, max=100
1262072545132 uproxy-8

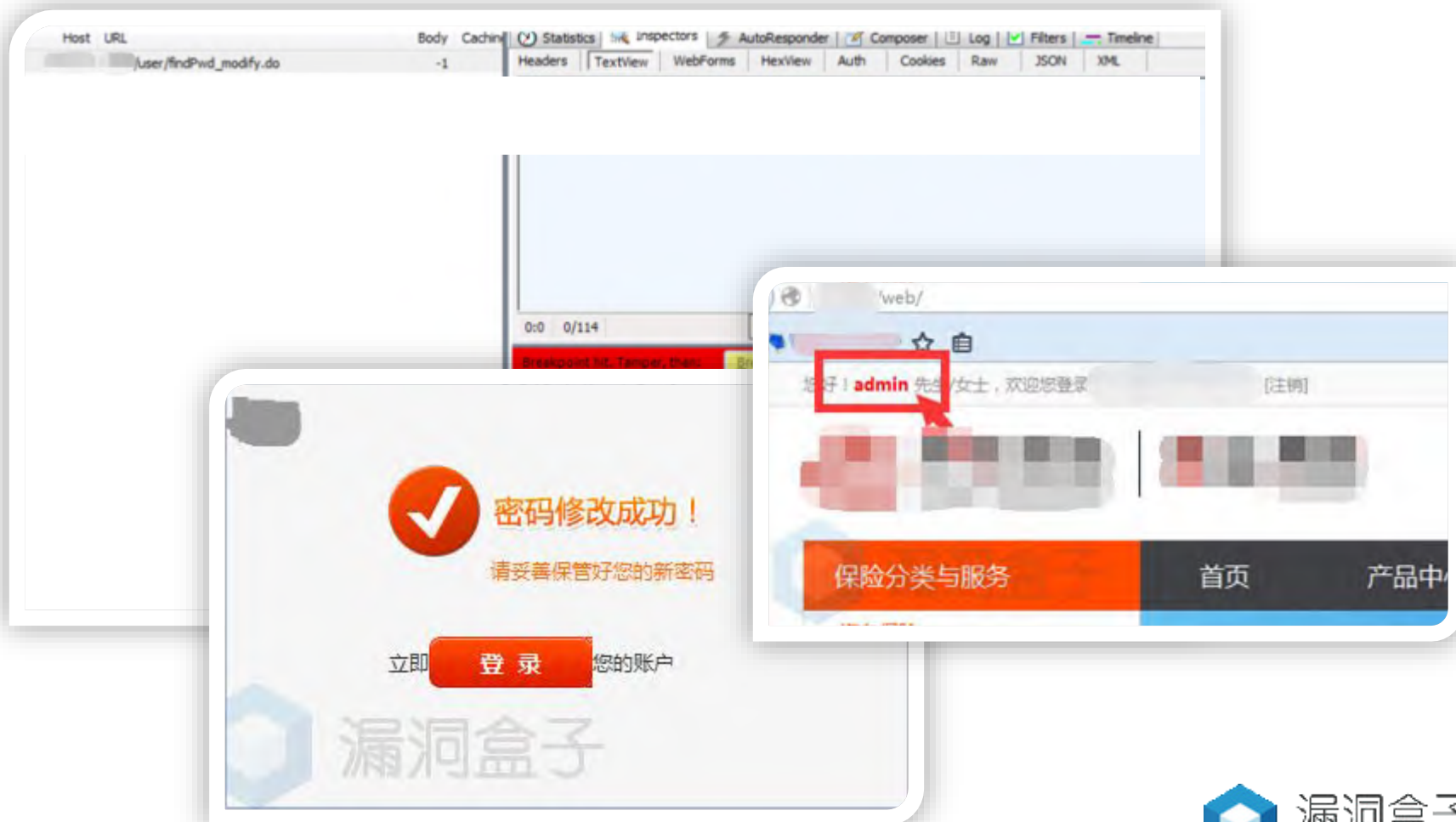
4be16979710d4c4e7c6647856088.....56","code":"","data":"","encryptType":"","msg":"验证码不正确,
sion":"V1.0.3")

digiSign

身份盗取 | 简单认证



身份盗取 | 最后一公里



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：

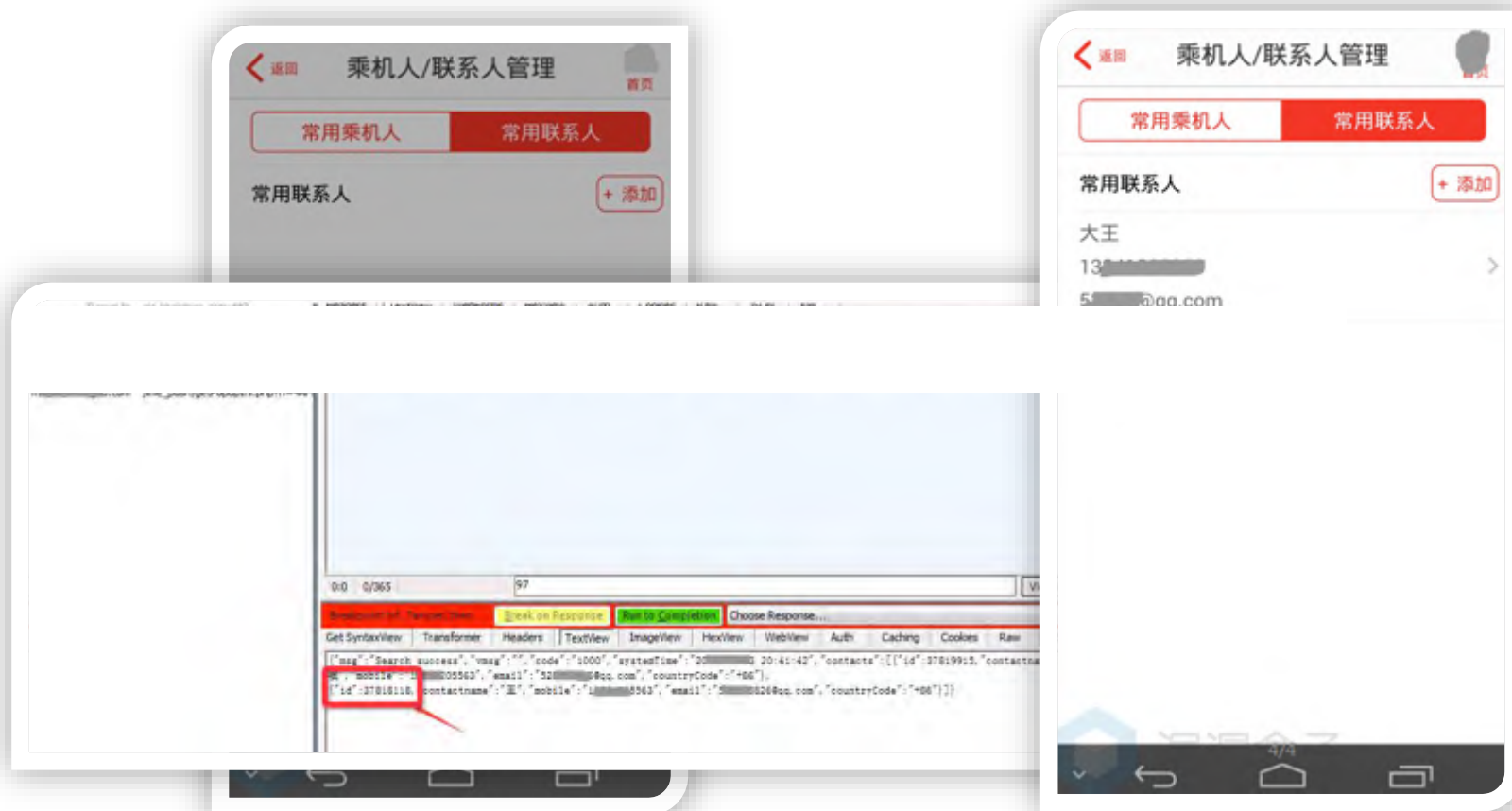
level=3

level=1 : admin

level=2 : vip user

level=3 : normal user

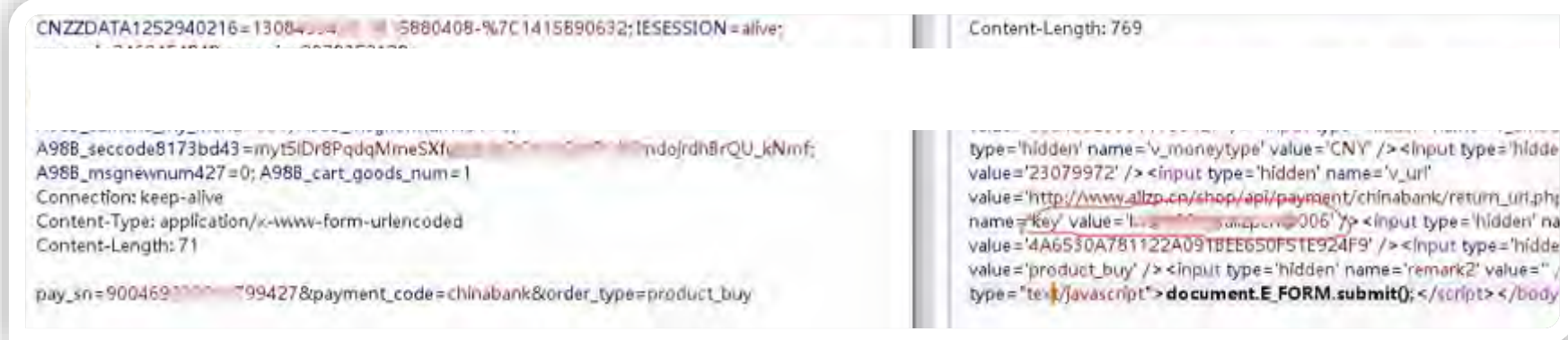
权限跨越 | 签名突破



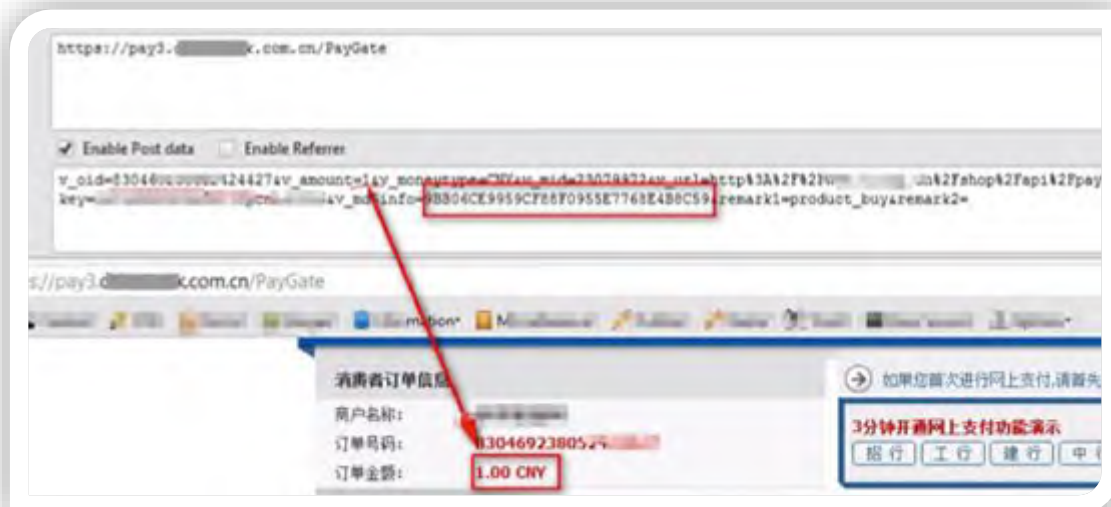
权限跨越 | 签名突破



交易篡改 | 签名破解



将订单中的v_amount,v_moneyp_type,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: e[REDACTED]h.com
Content-Length: 459
Accept: */*
Origin: http://[REDACTED].com
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36
Content-Type: application/json
Referer: http://e[REDACTED]h.com/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

● 手机号

Downloaded from <http://ajph.org/> on November 10, 2014

请输入验证码

重发给评稿

書

```
GET
/sms/send
HTTP/1.1
```

```
type=phoneNumber
```

POST

```
/sms/sendVerifySms/?phoneNumber=13911564495&phoneNumber=13911564495&phoneNumber=13911564495&phoneNumber=13911564495&phoneNumber=13911564495&phoneNumber=13911564495&phoneNumber=13718033116&prefix=R  
&type=phoneNumber HTTP/1.1
```

Hosts:

Correction: Inappropriate

Content-Length: 0

Accept[®]

Origins:

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; AppleWebKit/537.36 (KHTML, like Gecko))

Chrome/48.0.2564.116 Safari/537.36

Referer:

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN; q=0.9

Cookie:

side

045641.3

Him 1st 5ac

Min. Invt. \$0

Peri-implantitis

```
x-ibm109R, x-ibm111Z, x-ibm112Z, x-ibm112Z,
x-ibm1124, x-ibm1166, x-ibm1364, x-ibm1381,
x-ibm1383, x-ibm1390, x-ibm3372Z, x-ibm737, x-ibm833,
x-ibm934, x-ibm856, x-ibm874, x-ibm875, x-ibm921,
x-ibm922, x-ibm930, x-ibm933, x-ibm935, x-ibm937,
x-ibm939, x-ibm942, x-ibm942c, x-ibm943, x-ibm943c,
x-ibm948, x-ibm949, x-ibm949c, x-ibm950, x-ibm964,
x-ibm970, x-iso191, x-iso-2022-cn-cn, x-iso-2022-cn-gb,
x-iso-8859-11, x-jis0208, x-jisauto-detect, x-johab,
x-macarabic, x-maccentral-europe, x-macromanian,
x-macrylic, x-macdiagonal, x-macgreek, x-machebrew,
x-macelcand, x-maoroman, x-maoromania, x-macymalay,
x-machal, x-macturkish, x-macukraine, x-ms932-0213,
x-ms950-hkscs, x-ms950-hkscs-vp, x-mseinc-936, x-pck,
x-sjis-0213, x-utf-16le-bom, x-utf-32be-bom,
x-utf-32le-bom, x-windows-50220, x-windows-50221,
x-windows-874, x-windows-949, x-windows-950,
x-windows-iso2022jp
Content-Type: text/plain; charset=UTF-8
Content-Length: 21
Date: Sun, 15 May 2016 07:24:53 GMT
```

验证模型的有效性



漏洞盒子

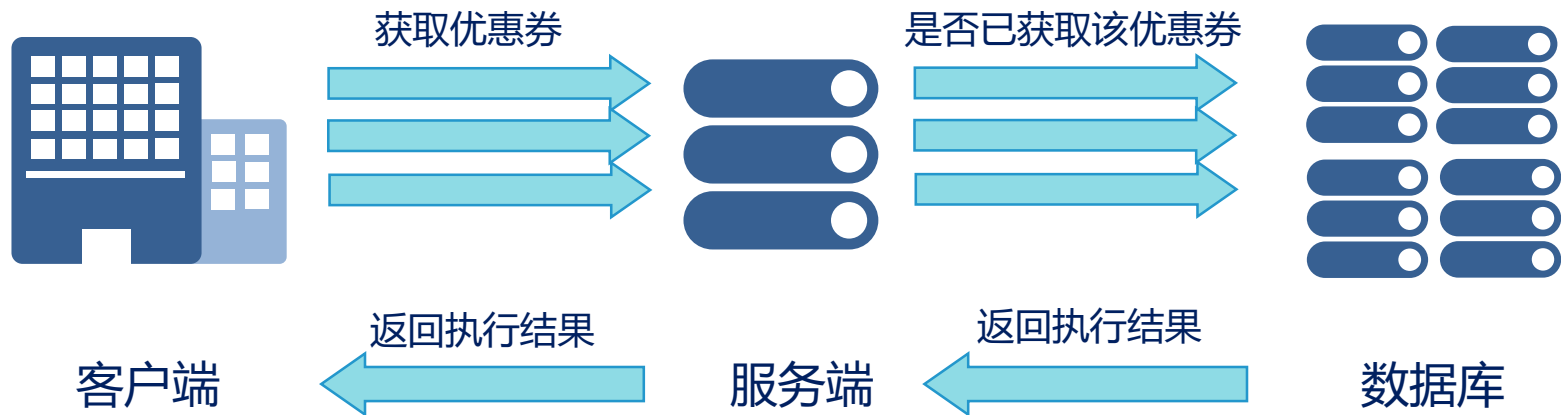
WWW.BILBO.COM

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
	肯德基冰淇淋花筒1只 1张 可使用	
	肯德基冰淇淋花筒1只 1张 可使用	
	肯德基冰淇淋花筒1只 1张 可使用	

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

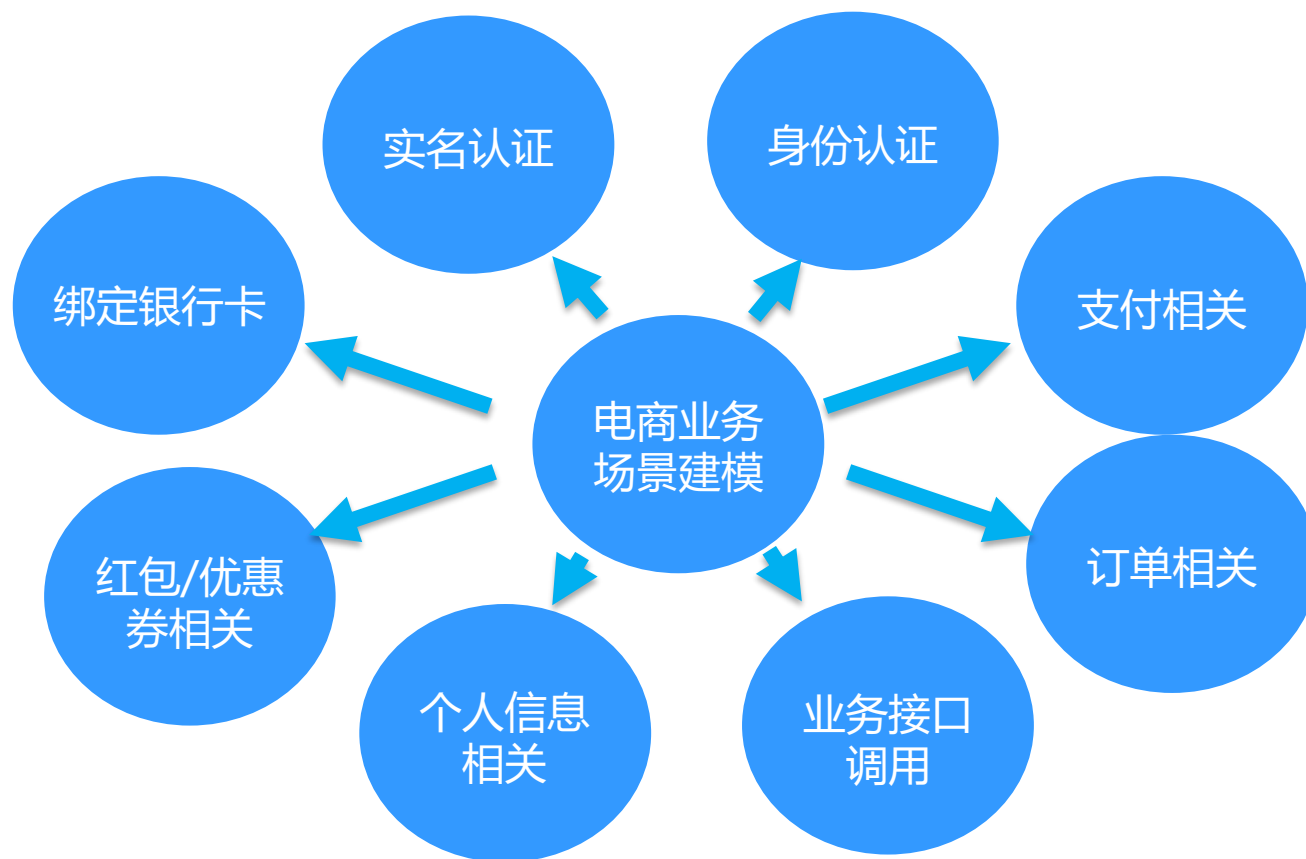
不同行业业务场景有所异同

如：银行、金融、保险、证券、电商、O2O、游戏、社交、招聘、航空

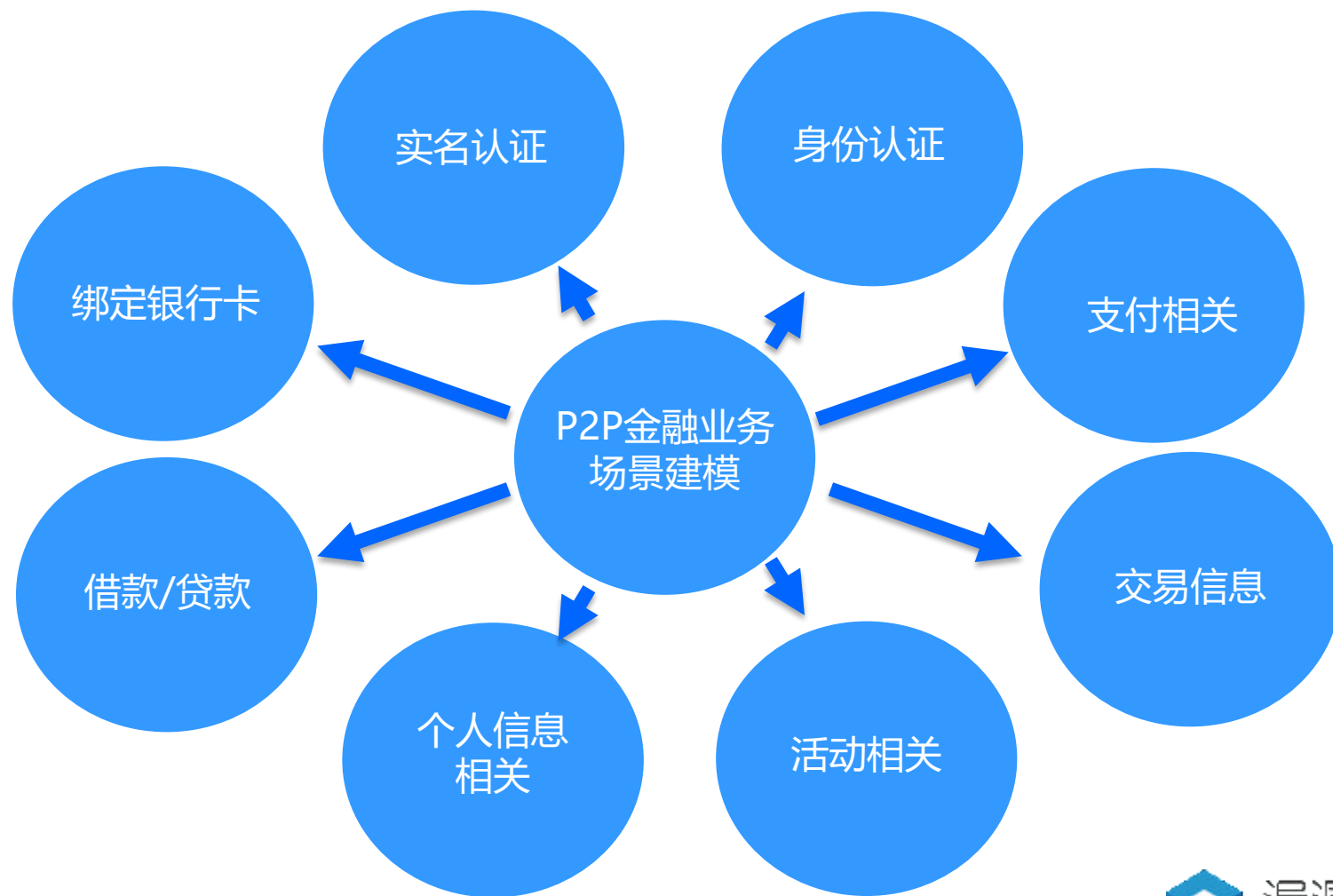
白盒：开发文档

黑盒：主动识别

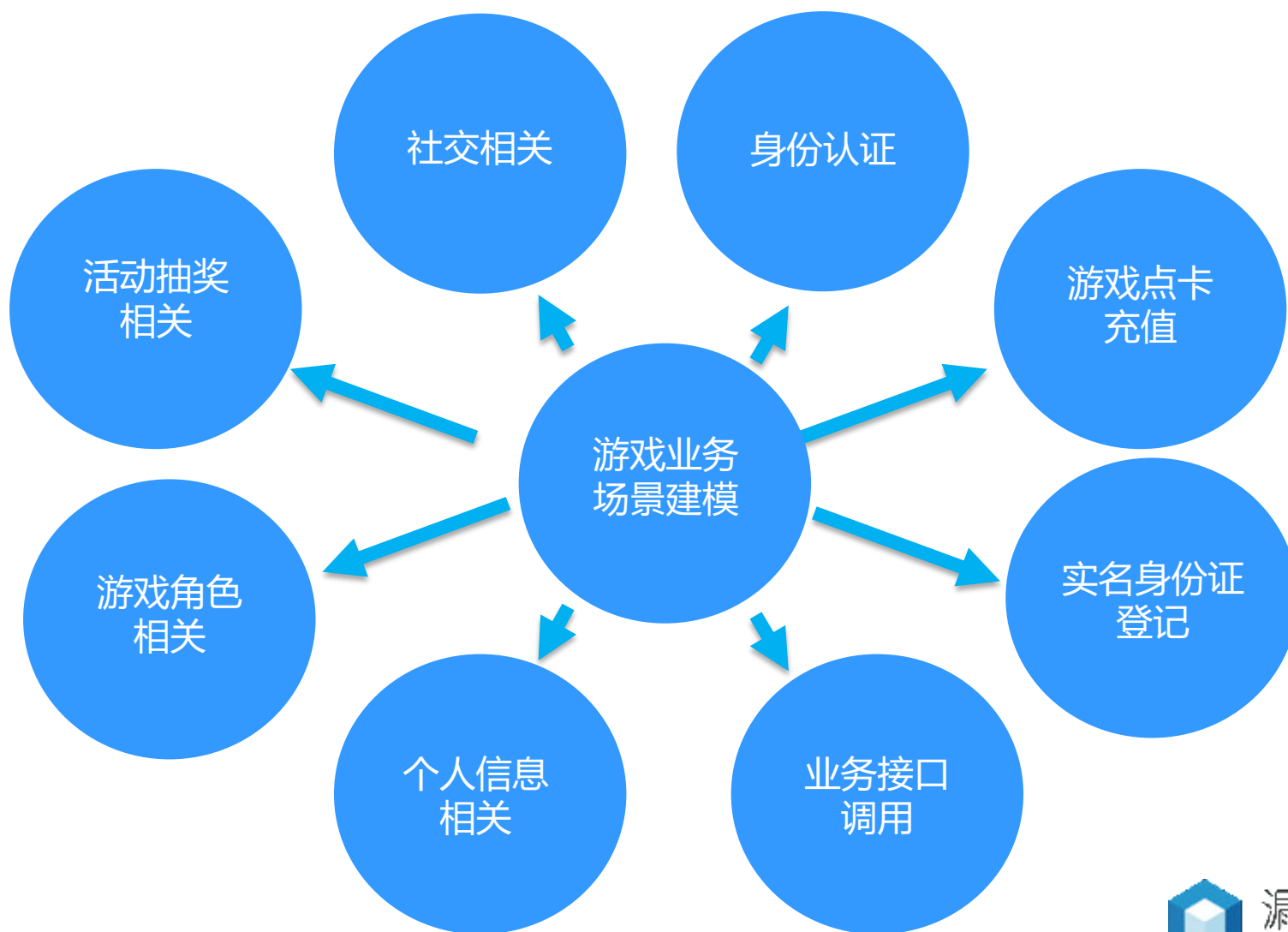
业务场景建模-1 | 电商



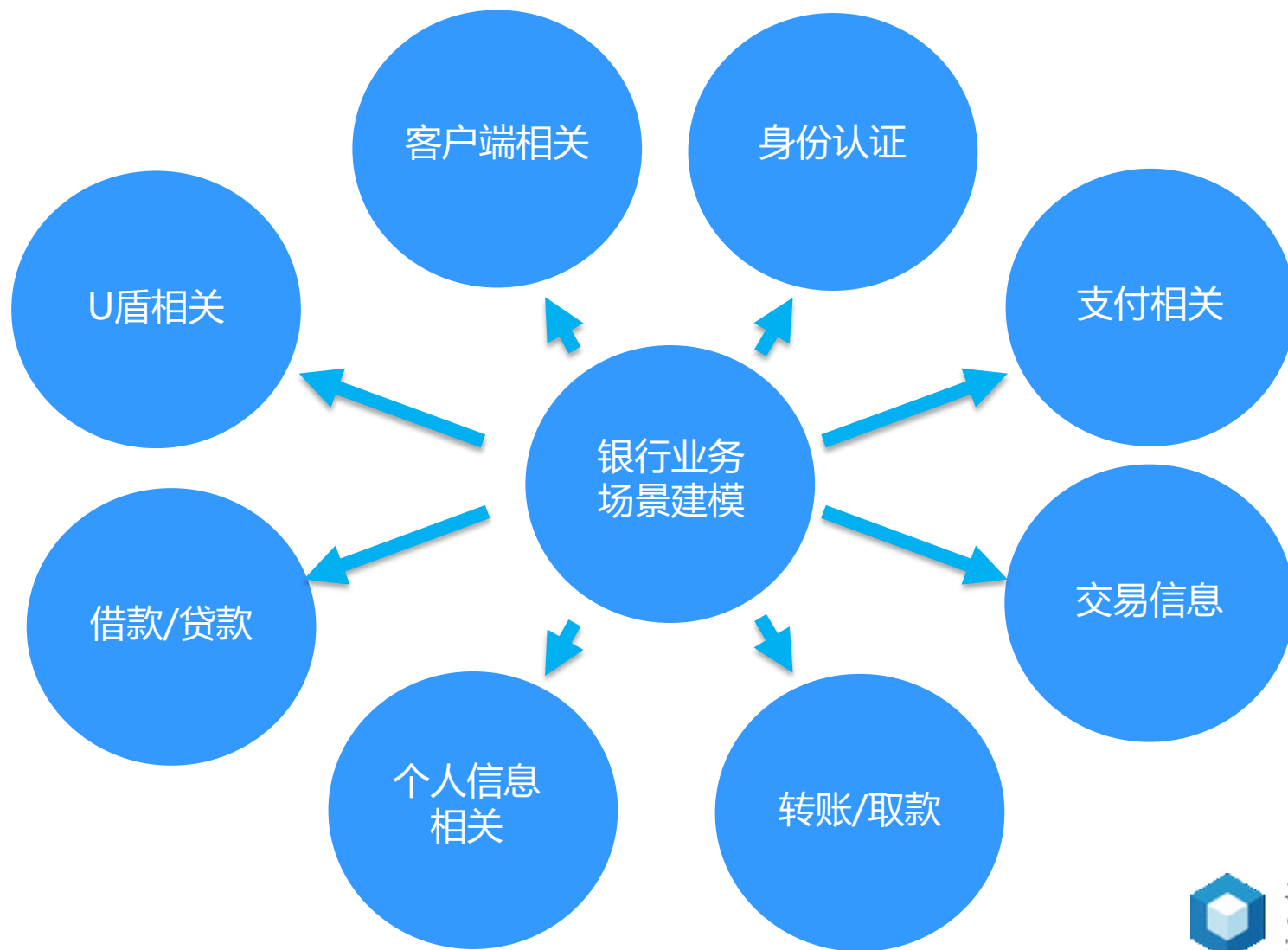
业务场景建模-1 | P2P金融



业务场景建模-1 | 游戏



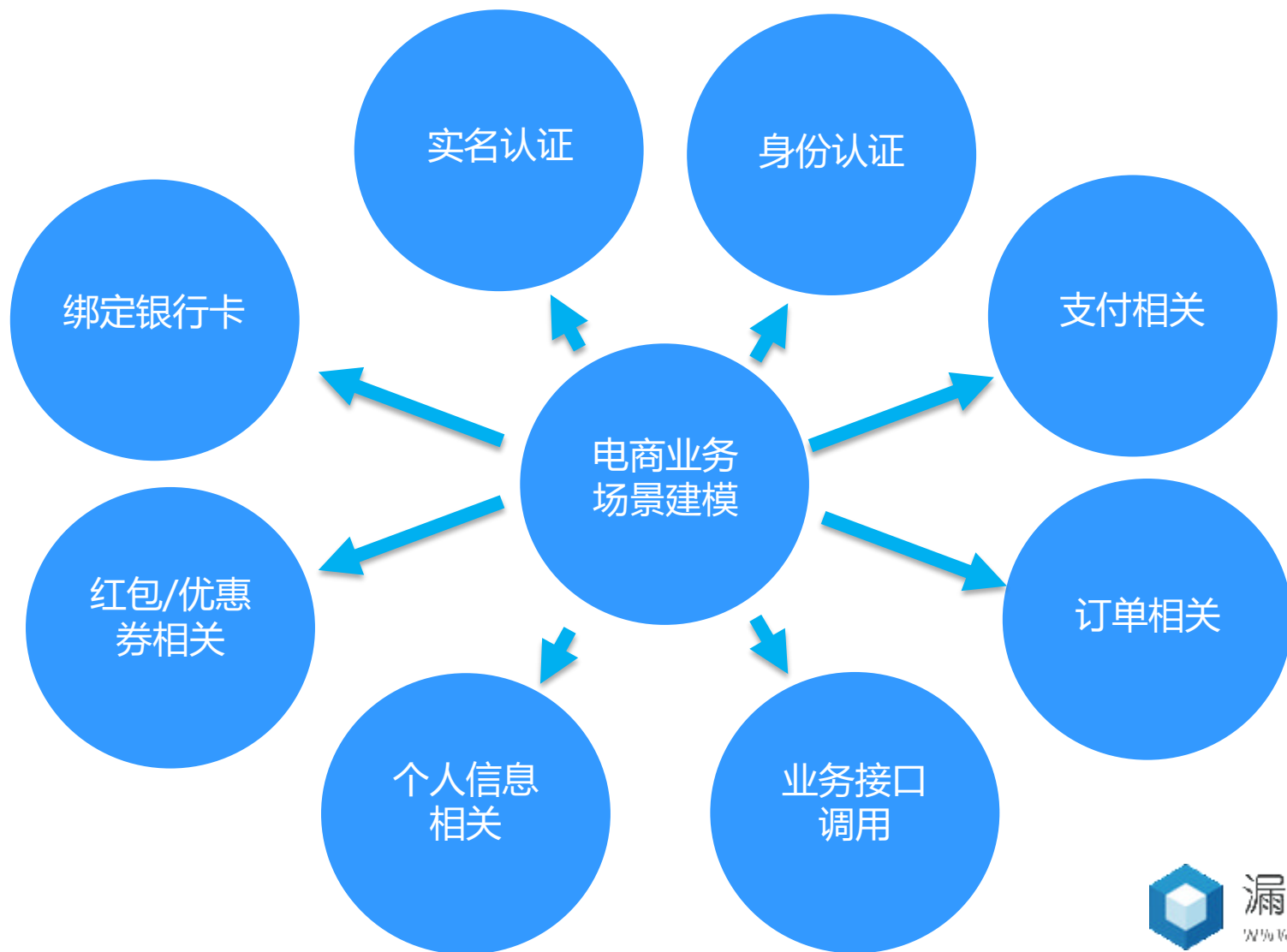
业务场景建模-1 | 银行



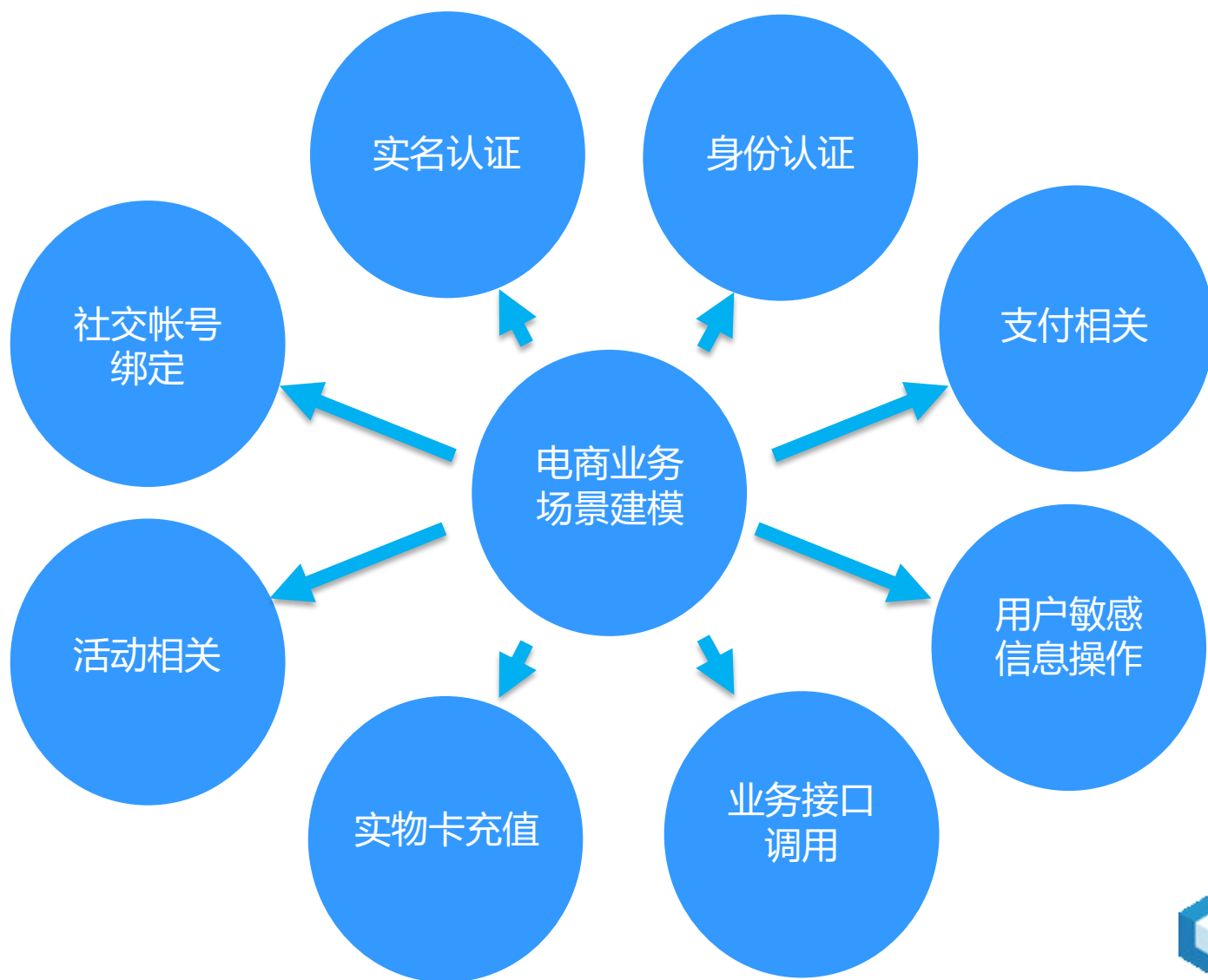
业务场景建模-2

- ✓ 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

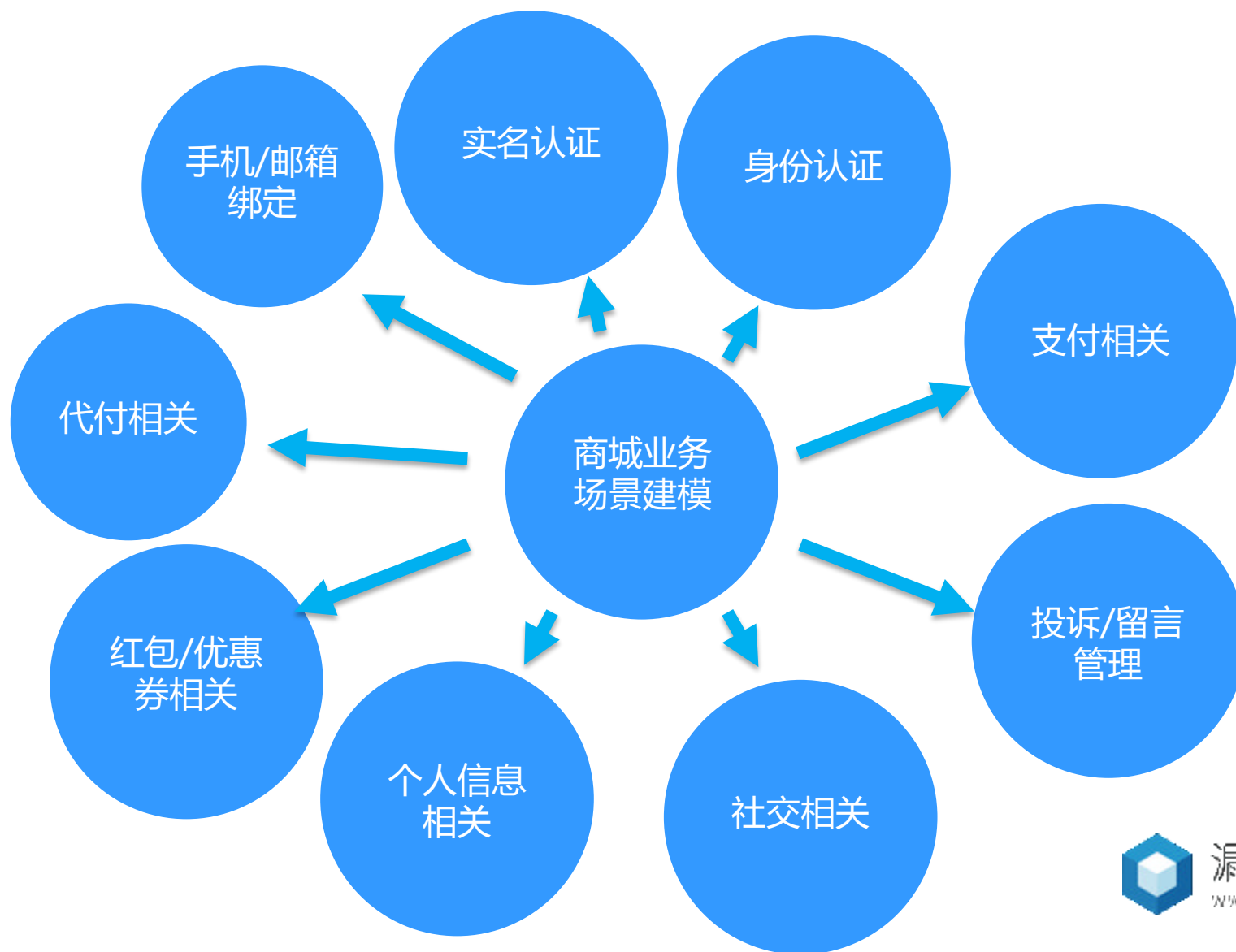
业务场景建模-2 | Plan-A



业务场景建模-2 | Plan-B



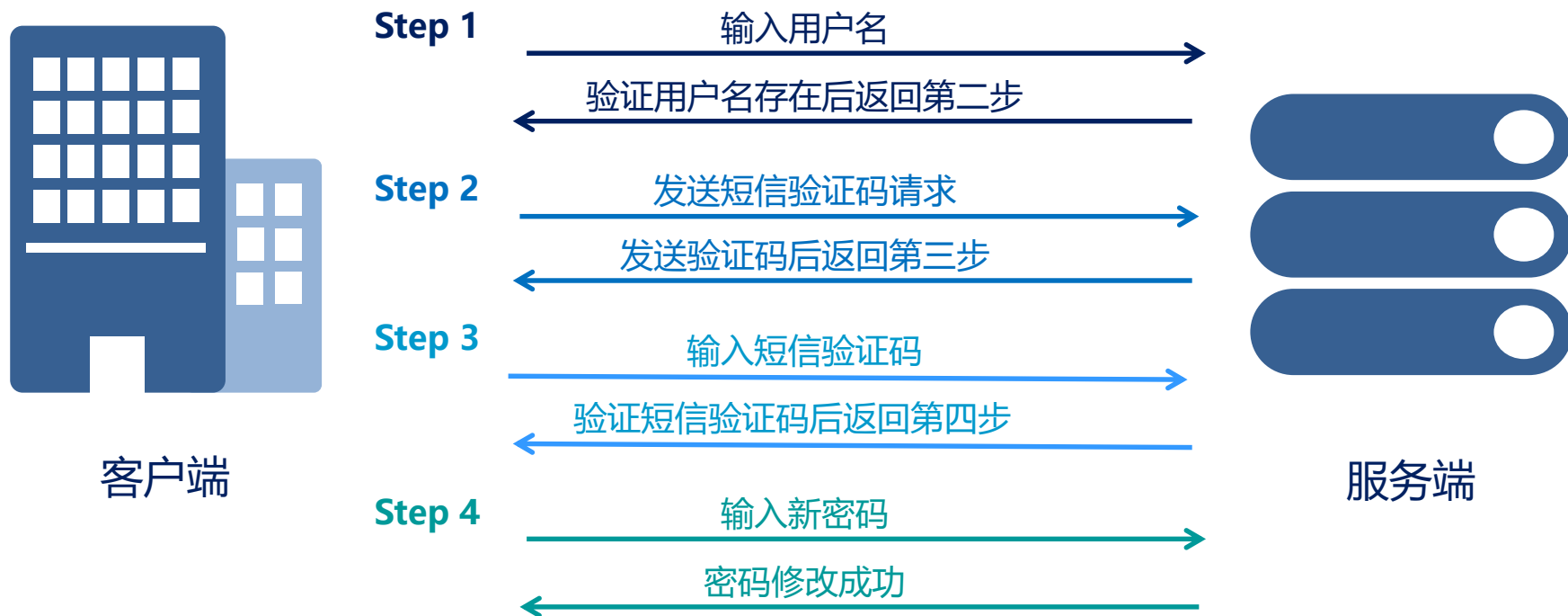
业务场景建模-2 | Plan-C



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

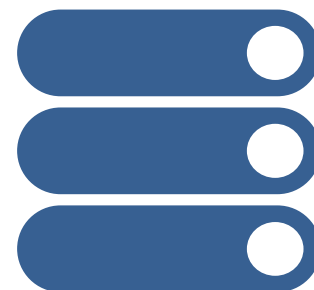
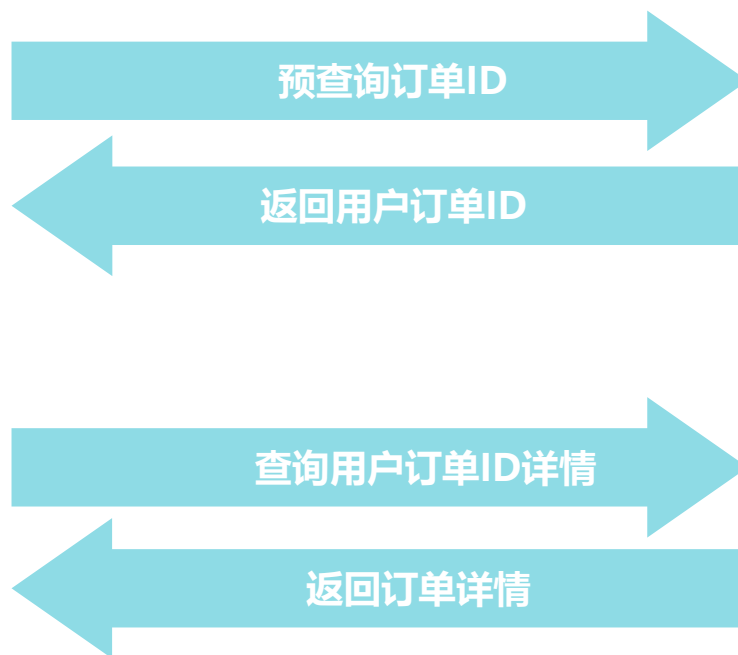
密码重置



订单查询



客户端

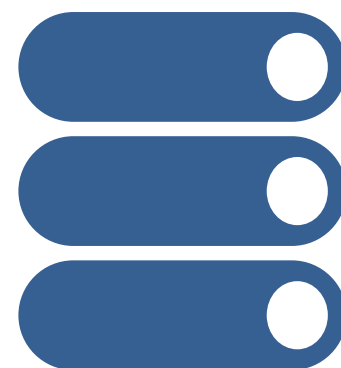


服务端

支付交易



客户端



服务端

- ✓ 已知风险对照
- ✓ STRIDE分析方法

风险点识别



分期付款

快捷支付

网银支付

快捷支付

网银支付

电子券

案例流程测试

程序乱序测试

欲购天下菜鳥品

請到天天上菜館品

积分兑换，低积分起换兑降高积分商品

购买数量负数

突破购买最大数限制

地址填寫

发票填写

测试项目	备注填写
------	------

其他输入字符	
--------	--

重慶博文印務

1, 账号余额为负数

行充值



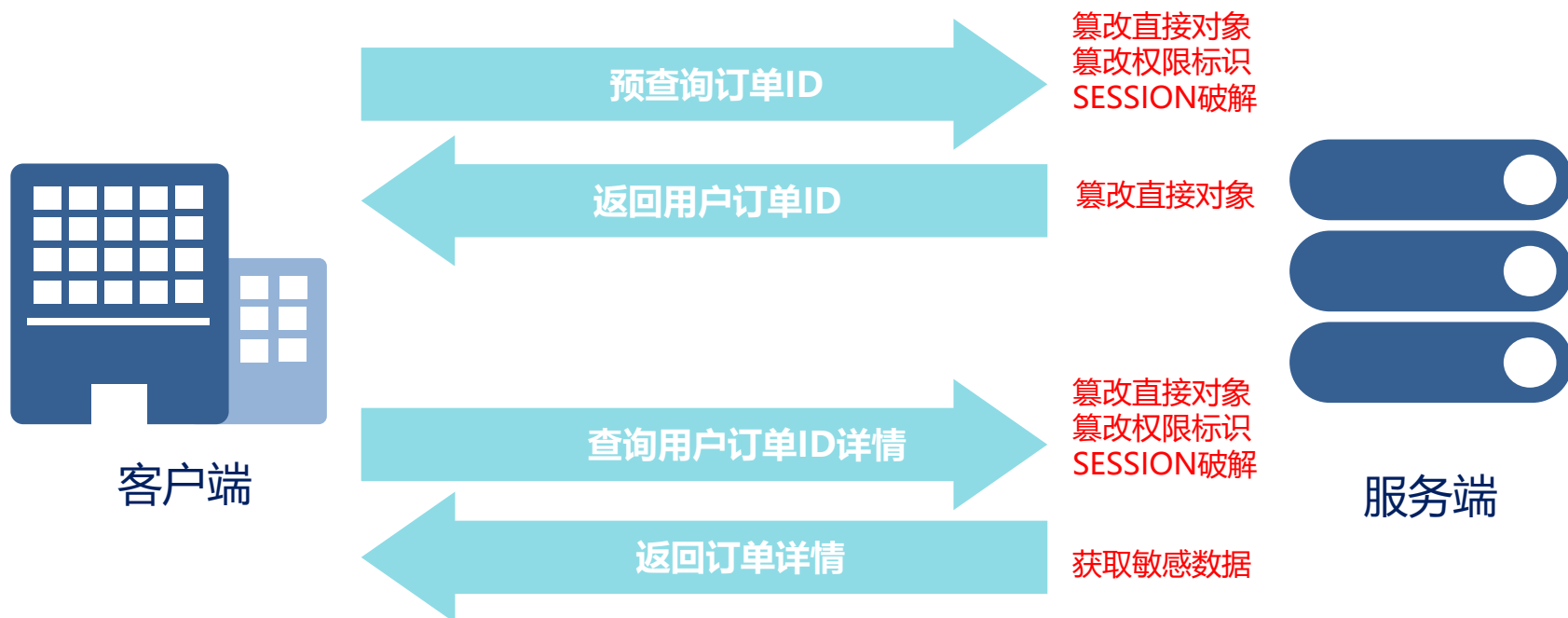
漏洞盒子

WWW.VULGOR.COM

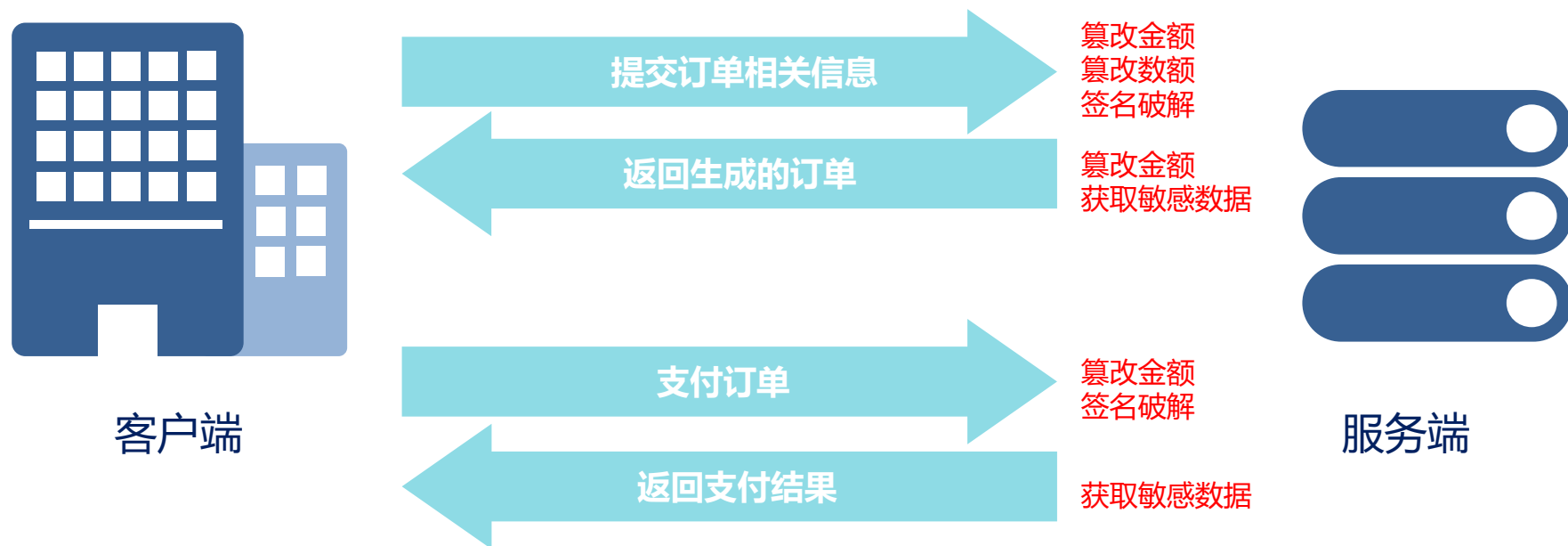
密码重置



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 | 漏洞盒子

crs.vulbox.com | 网藤风险感知

www.freebuf.com | FreeBuf