安世加

第二十六期沙龙之
企业安全创新技术（线上）

2020.1.08

业务逻辑安全的攻防思考

安世加

未知攻焉知防

漏洞：正常功能的非正常使用

https://kyfw.12306.cn/otn/view/passenger_edit.html?type=add

火狐官方站点 | 常用网址 | 安全应急响应流程 - ... | 郑州优车安全管理平台 | 三种解密 HTTPS 流... | 专车项目进度统筹-研... | Welcome to [Jenkins]

首页 | 车票 | 团购服务 | 会员服务 | 站车服务 | 商旅服务 | 出行指南 | 信息查

当前位置：个人中心 > 常用信息管理 > 常用联系人

- 个人中心
- 订单中心
  - 火车票订单
  - 候补订单
  - 餐饮·特产
  - 保险订单
- 我的行程
- 会员中心
- 个人信息
  - 查看个人信息
  - 账号安全
  - 手机核验
- 常用信息管理
  - 常用联系人
  - 车票快递地址
- 温馨服务
  - 重点旅客预约

基本信息

* 证件类型：中国居民身份证

(●) 中国居民身份证 ( ) 外国人永久居留身份证 ( ) 港澳台居民居住证

* 姓名：王鹏　姓名填写规则（用于身份核验）

* 证件号码：612501198026034012　用于身份核验，请正确填写。

请输入正确的证件号码！

* 性别：(●) 男 ( ) 女

联系方式

手机号码（+86）：

固定电话：

电子邮件：

地址：

邮编：

52	04	05	200			438
53	05	05	200			438
55	07	05	200			438
56	08	05	200			438

Request | Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Mon, 11 Mar 2019 06:45:04 GMT
Content-Type: application/json;charset=UTF-8
Content-Length: 173
ct: C2_240_45_7
X-Via: 1.1 PShbsjzdx5md98:27 (Cdn Cache Server V2.0)
Connection: close
X-Cdn-Src-Port: 51885
Cdn-Src-Ip: 114.242.122.145

{"validateMessagesShowId":"_validatorMessage","status":true,"httpstatus":200,"data":{"message":"证件号码输入有误!","flag":false},"me
ges":{}}
```

67	07	06	200			399
76	04	07	200			399
85	01	08	200			399
105	09	09	200			399
1	01	01	200			437
2	02	01	200			437
3	03	01	200			437
8	08	01	200			437
9	09	01	200			437

Request | Response

Raw | Headers | Hex

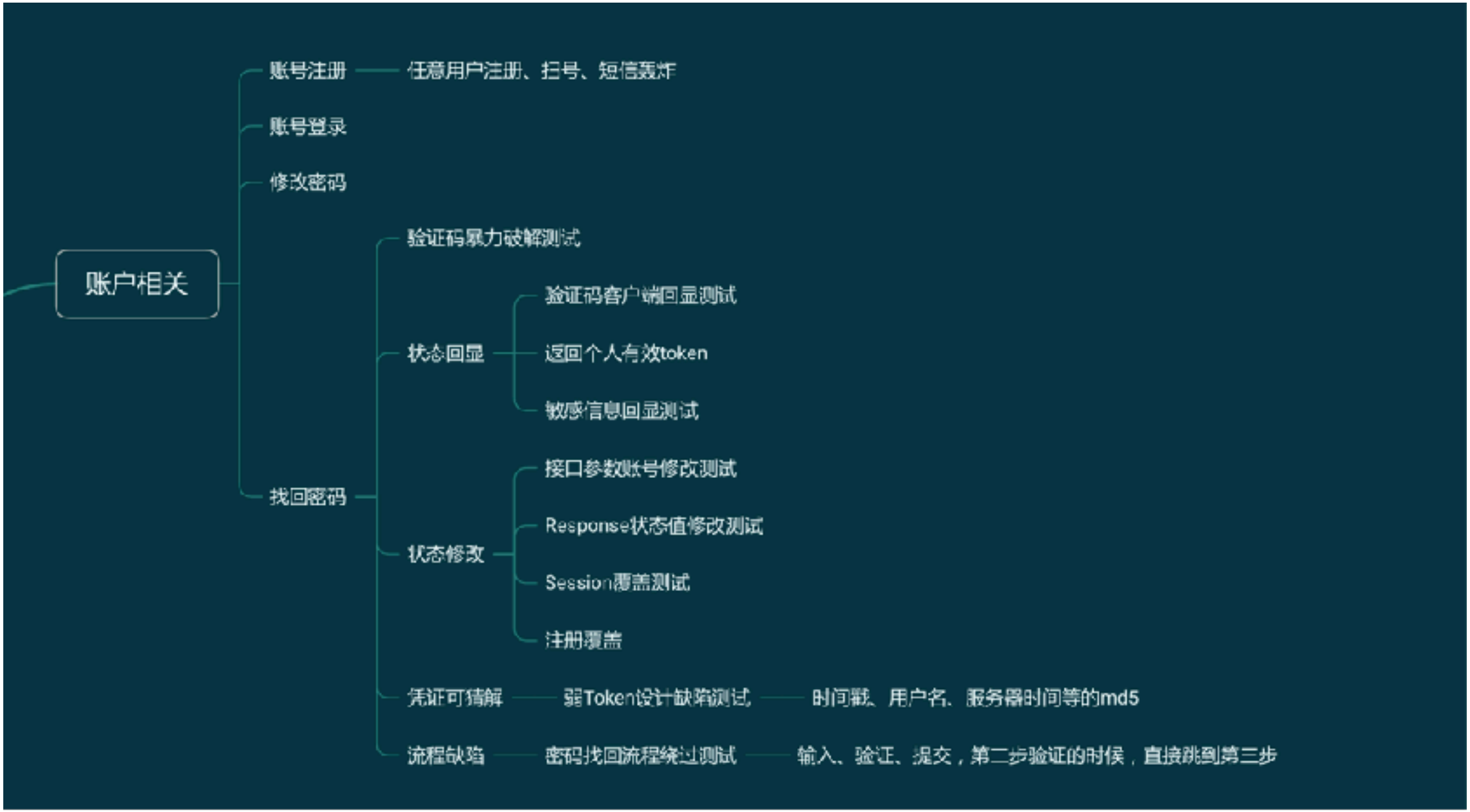
```
HTTP/1.1 200 OK
Date: Mon, 11 Mar 2019 06:45:05 GMT
Content-Type: application/json;charset=UTF-8
Content-Length: 134
ct: C2_240_45_7
X-Via: 1.1 PShbsjzdx5md90:15 (Cdn Cache Server V2.0)
Connection: close
X-Cdn-Src-Port: 51900
Cdn-Src-Ip: 114.242.122.145

{"validateMessagesShowId":"_validatorMessage","status":true,"httpstatus":200,"data":{"flag":true},"messages":[],"validateMessages":{}}
```

产生原因：功能模块复杂度

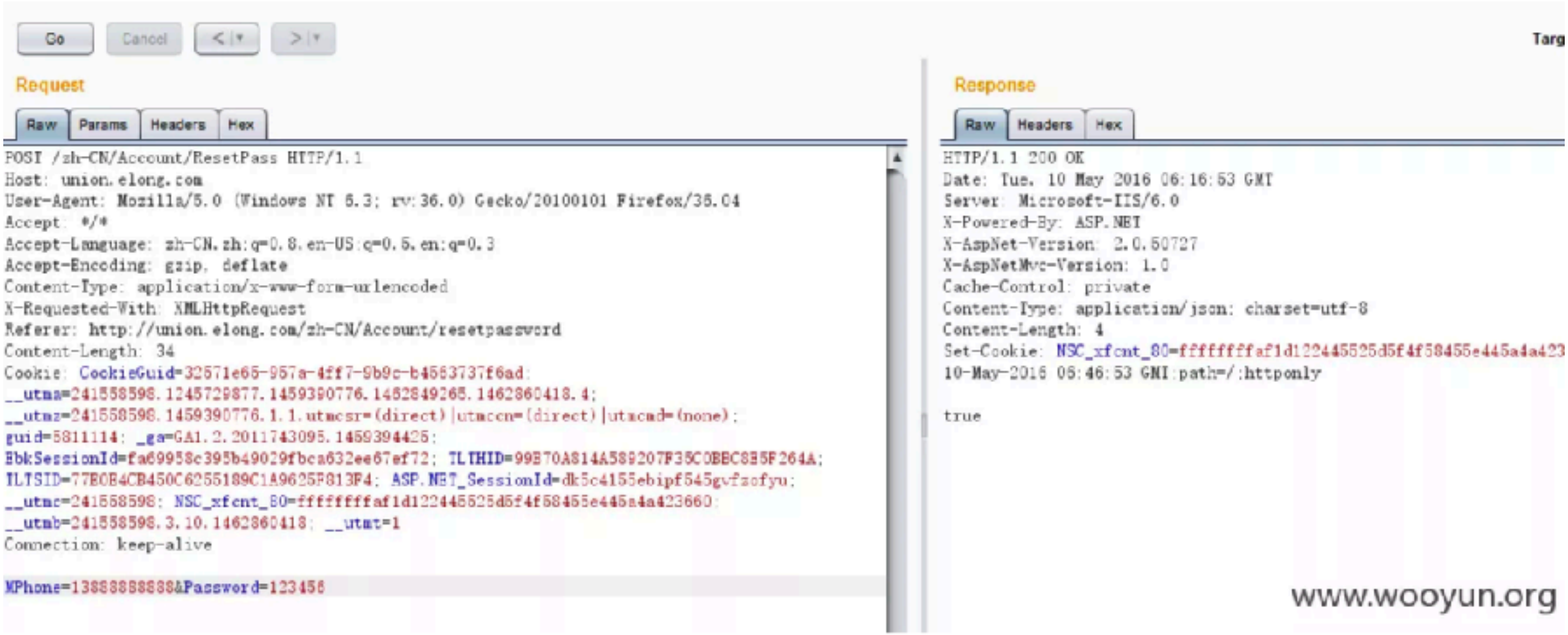

BTV 北京卫视
秀才遇到兵（2）
一件事越复杂


BTV 北京卫视
雷电 黄 LIGHTNING
秀才遇到兵（2）
它会出错的环节越多

账户相关


账户相关
账号注册
任意用户注册、扫号、短信轰炸
账号登录
修改密码
找回密码
验证码暴力破解测试
状态回显
验证码客户端回显测试
返回个人有效token
敏感信息回显测试
状态修改
接口参数账号修改测试
Response状态值修改测试
Session覆盖测试
注册覆盖
凭证可猜解
弱Token设计缺陷测试
时间戳、用户名、服务器时间等的md5
流程缺陷
密码找回流程绕过测试
输入、验证、提交，第二步验证的时候，直接跳到第三步

秒改是一种什么样的体验




●●●●○ 中国移动 09:15 80%
排行
分享
全国排名
月
周
日
我本月的全国排名
第 1000+ 名
本月还没跑步，要加强锻炼啦
秀排名，求点赞
孤独剑
783.16 公里
广东省珠海市
第 1 名
19
月光
673.24 公里
陕西省宝鸡市
第 2 名
13
动态
挑战
发现
排行
我
www.wooyun.org


●●●●○ 中国移动 09:33 77%
我
设置
孤独剑
悦动账号:477120
Lv14
50
动态
1
关注
134
2
粉丝
我的钱包
消息
3
运动记录
05月14日 凌晨0:18
室外跑
7.07 公里
59'17"/公里
418'59"
05月13日 晚上10:31
室外跑
3.73 公里
27'03"/公里
100'49"
动态
挑战
发现
排行
我
www.wooyun.org

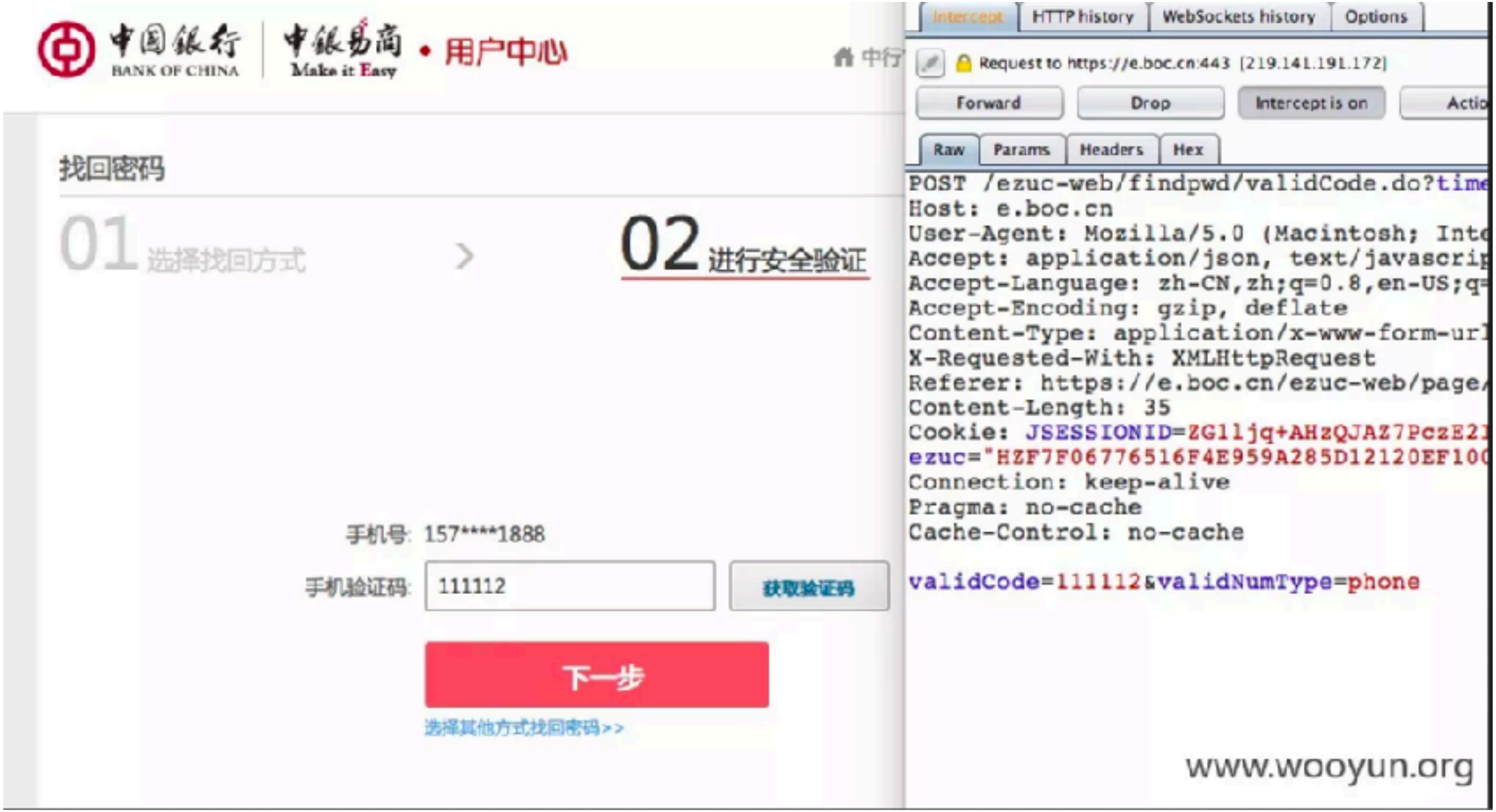
敏感信息回显


union.ceair.com/web/ResetPassWord.aspx?loginuser=1234
中國東方航空
CHINA EASTERN
中国东方航空股份有限公司工会
您可通过昵称或18位身份证号重置密码
返回登陆页面
请输入您的18位身份证号或注册时的昵称，并点击右侧发送按钮，重置密码：
登陆名：
1234
获取信息
电子邮箱：
li*****com
发送密码到此邮箱
手机号：
1386062***4
发送密码到此手机号
www.wooyun.org

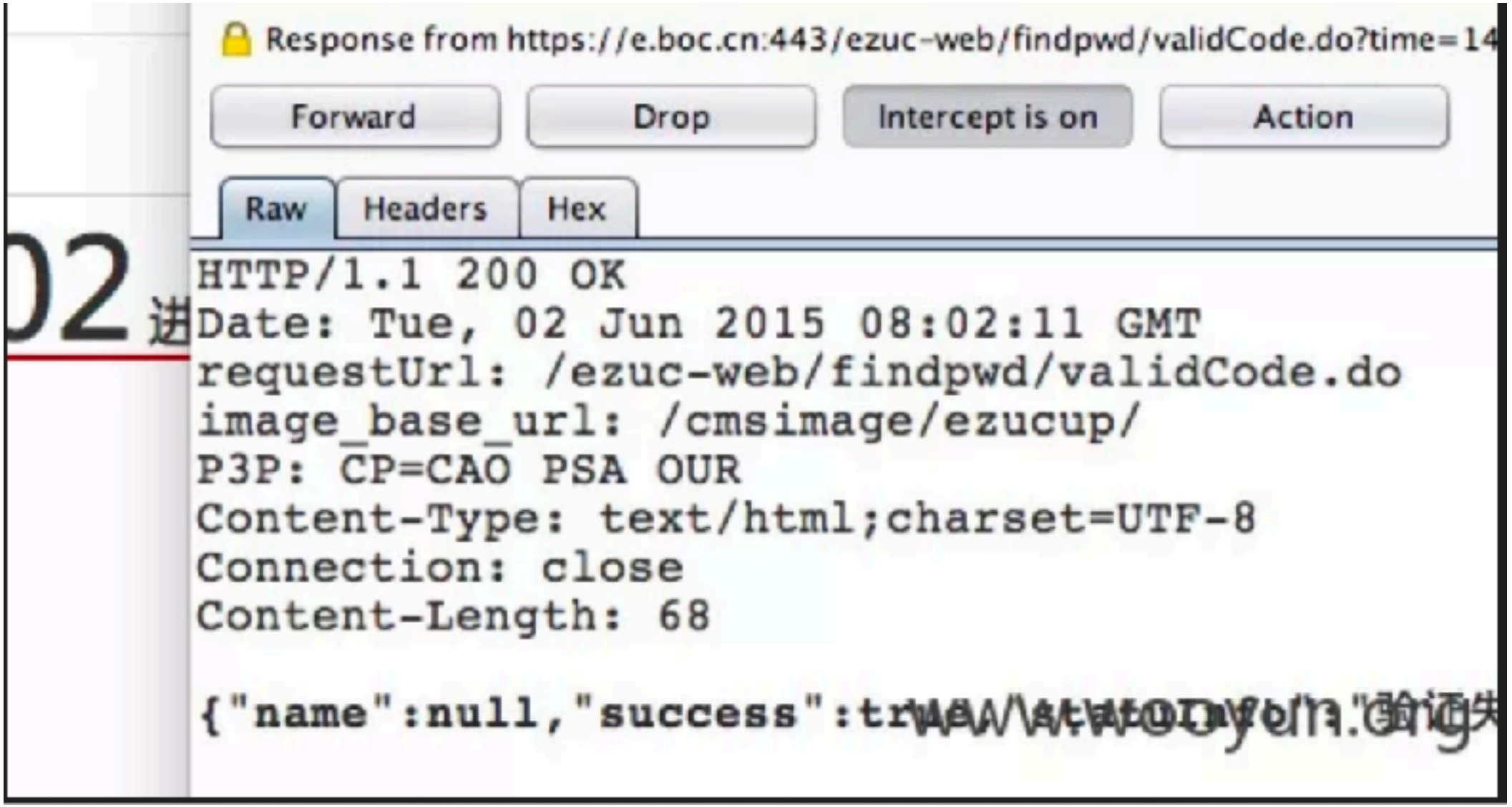
敏感信息回显


147 http://union.ceair.com GET /web/ResetPassWord.aspx?loginuser=0001 200 25024 HTML aspx
Request Response
Raw Headers Hex HTML Render ViewState
899B9A352E4A706CE0437F000001706C 140102196401026233 49A2A8AEB49B1C4F 1980/10/10 13903411600
www.wooyun.org

Response状态值修改

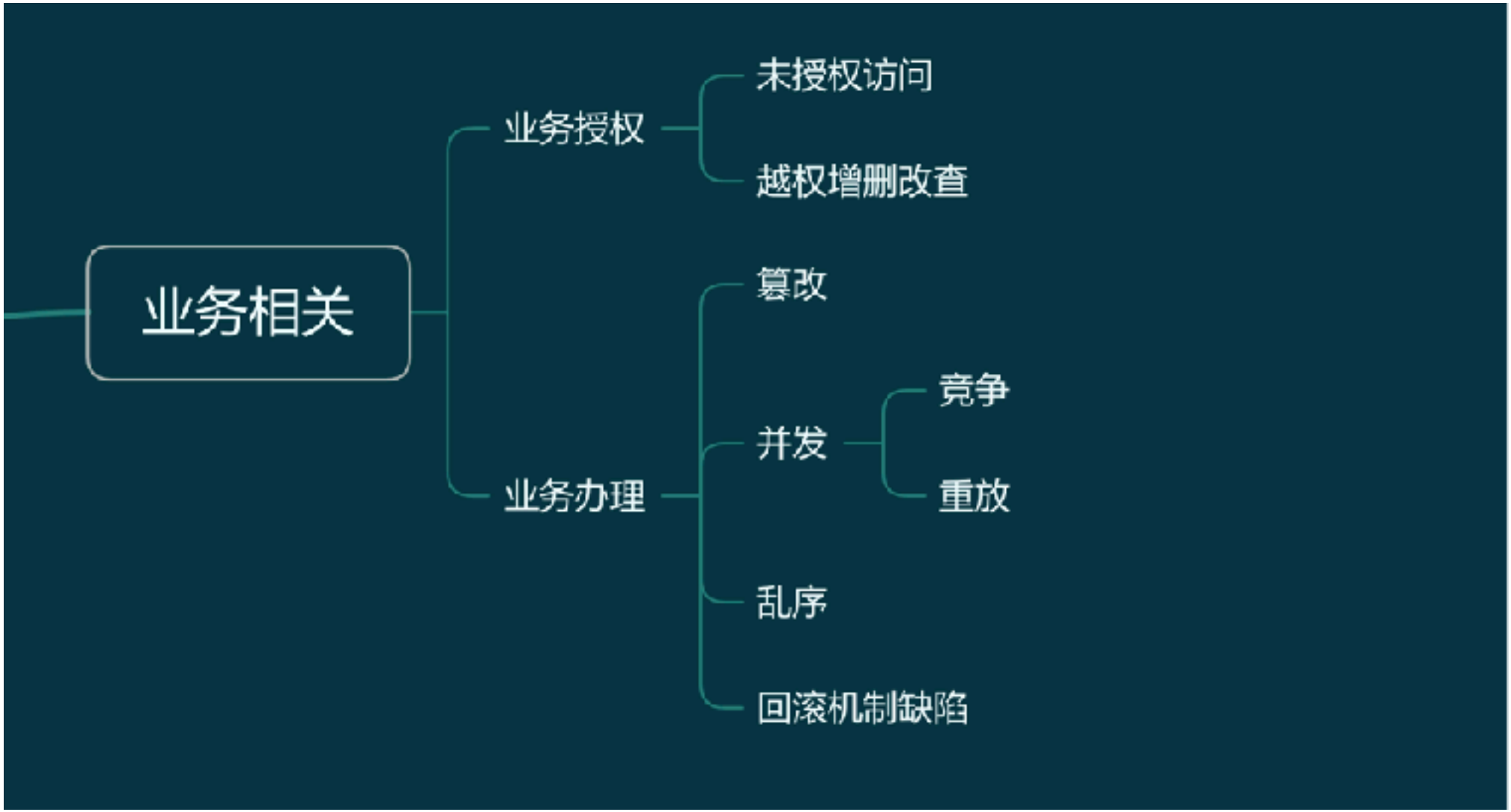


Response状态值修改




https://e.boc.cn/ezuc-web/page/general/home/personal/homepage/personIndex.html
中国银行 BANK OF CHINA
中银易商 Make it Easy
• 用户中心
中行官网 | 中银易商 | 退出 |
talbot
138****9147
| 资料完成 |
登录时间：2015-06-02 16:10:55
个人主页
我的信息
消息
安全中心
绑定账号
我的应用
中银开放平台
应用商店
V钱包
养老宝
出国金融
我的账户
中国银行 BANK OF CHINA
**** **** **** 0522
添加银行卡
www.wooyun.org

业务相关



业务授权

未授权访问

越权增删改查

垂直越权

event.keyingke.com/spec/recruitment/review/?person_id=5549

[个人基本信息]			
姓名：	柏墨尘		
常用名：	柏墨尘		
身份证号码：			
性别：	女		
出生日期：	1995-12-14	手机号：	15340584580
户口所在地：	内蒙古锡林浩特市逸园小区17号楼2单元402	現居住城市：	重庆
电子邮件：	791871948@qq.com	QQ号：	791871948
就业情况：	在校生	应聘渠道来源：	网络
申请职位性质：	校园经纪人	是否接受职位推荐&调剂：	是
家庭住址：	重庆工商大学北区北20宿舍2001		
爱好：	主持，辩论，演讲，声乐，cosplay，策划，除了有专业的法语方面知识外，我在学生会体育部工作一年，多次参加各类比赛的策划活动，积极参与校内的各类辩论与演讲类比赛，锻炼自己的表达能力，同时担任法语与英语主持，锻炼自己的口语，有较强的表演欲，多次参与歌唱比赛与话剧大赛。		
特长：	一：主持 多次担任校园大型晚会法语主持 二：策划 带领团队参加各类创业策划大赛等并取得优异成绩同时在体育部工作期间负责策划各类比赛活动。 三：交际 热情开朗善于交际在校期间加入VAICE(国际交流志愿者协会)负责留学生接待等工作。		
[教育经历]			
入学时间：	2014-09-10	毕业时间：	2016-06-30
所在学校：	重庆工商大学	院系/专业：	国际商学院/法语（国际商务）
学制：	四年制	学历：	本科

[redacted]er/OrderMgr.htm?m=query&f=gotoUpdateOrder&orderId=746

Enable Post data Enable Referrer

3	2015-07-30 15:03:58	订单审核通过,审核人:【焦方刚】	焦方刚
4	2015-07-30 15:04:14	【焦方刚】将订单分配给【李彩彩】	焦方刚
5	2015-07-31 12:38:15	开户成功	李彩彩
6	2015-07-31 12:38:15	订单已发货	李彩彩
7	2015-08-01 14:05:45	已签收	系统
8	2015-08-05 16:49:23	归档成功	李彩彩

物流信息 承运方：顺丰速运 物流单号：991914928985 [修改]

	处理时间	处理信息	处理地点
1	2015-07-31 18:06:00	已收件	济南文东服务点
2	2015-08-01 07:57:00	正在派件..	青岛市北服务点
3	2015-08-01 10:47:00	派送成功	青岛市北服务点

收货人信息 [修改收货地址]

收 货 人：李正本

地　　址：山东省 青岛市 李沧区台柳路278号 保尔馨都3-2-1601

联系电话：13792478759

支付及配送方式

支付方式：在线支付

配送方式：顺丰

运　　费：¥0.00元

发货日期：2015-07-31 12:38:15

入网信息 [修改入网信息]

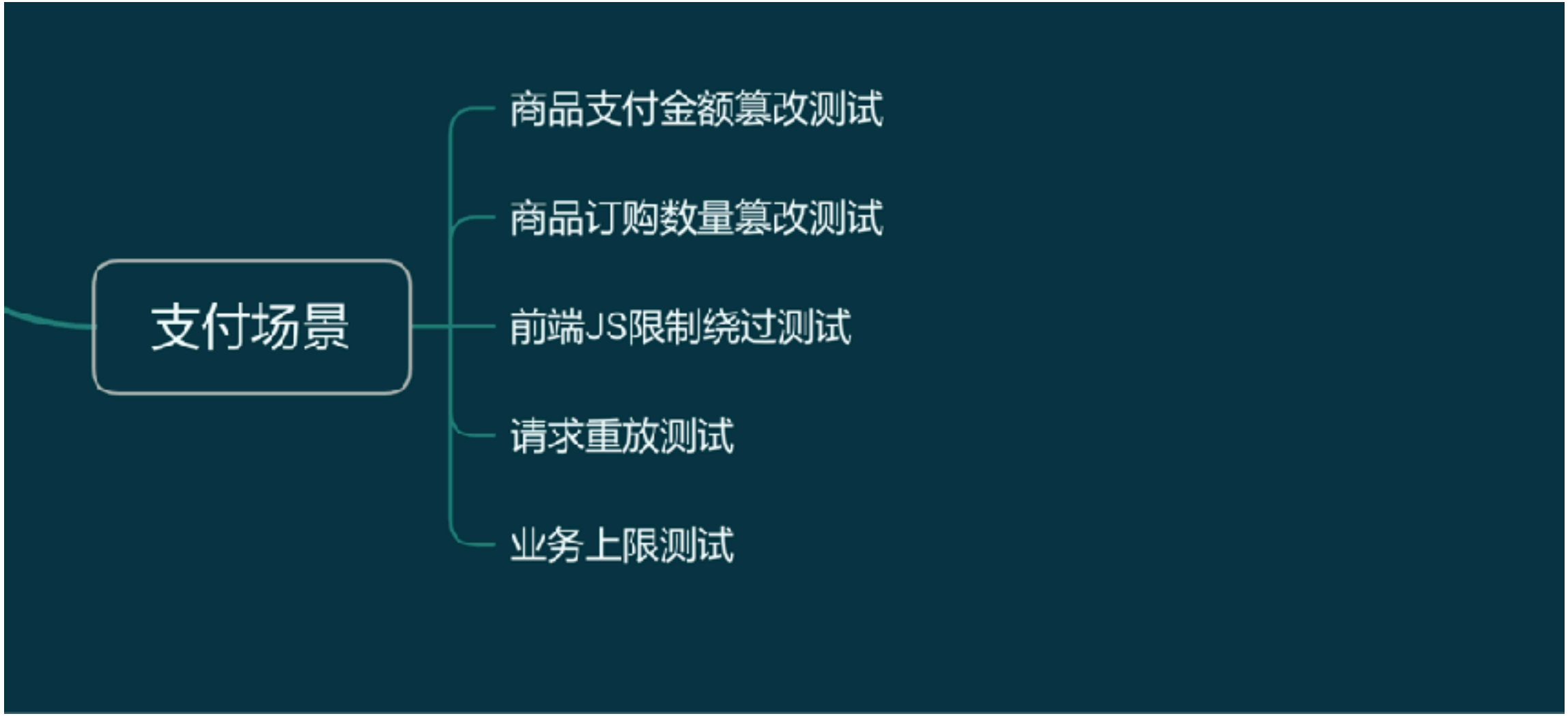
开户卡号：17606399668

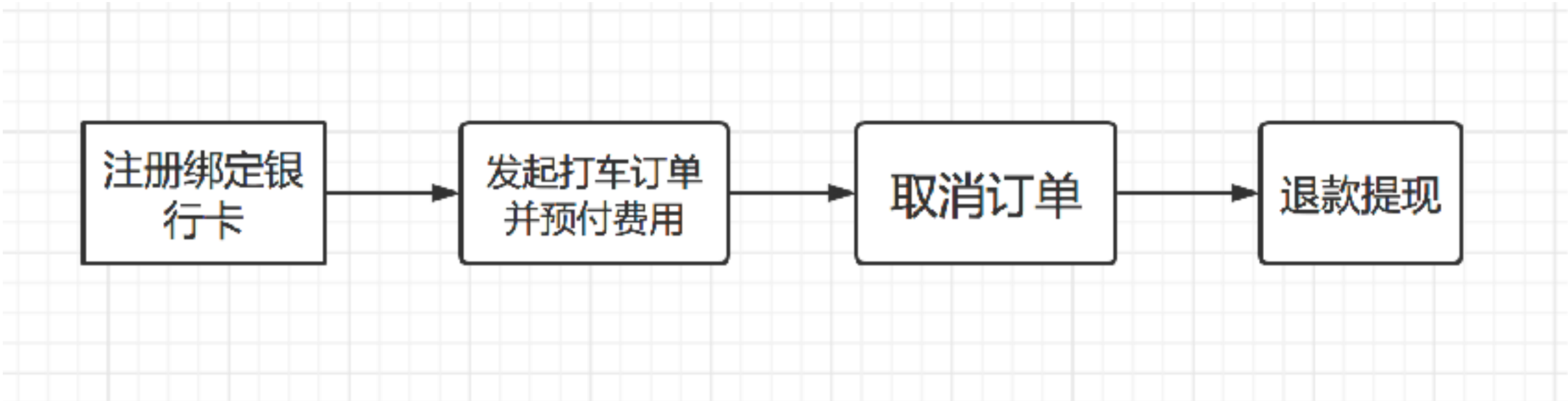
开户姓名：李正本

身份证号：[redacted]

17606399668卡板： Nano卡

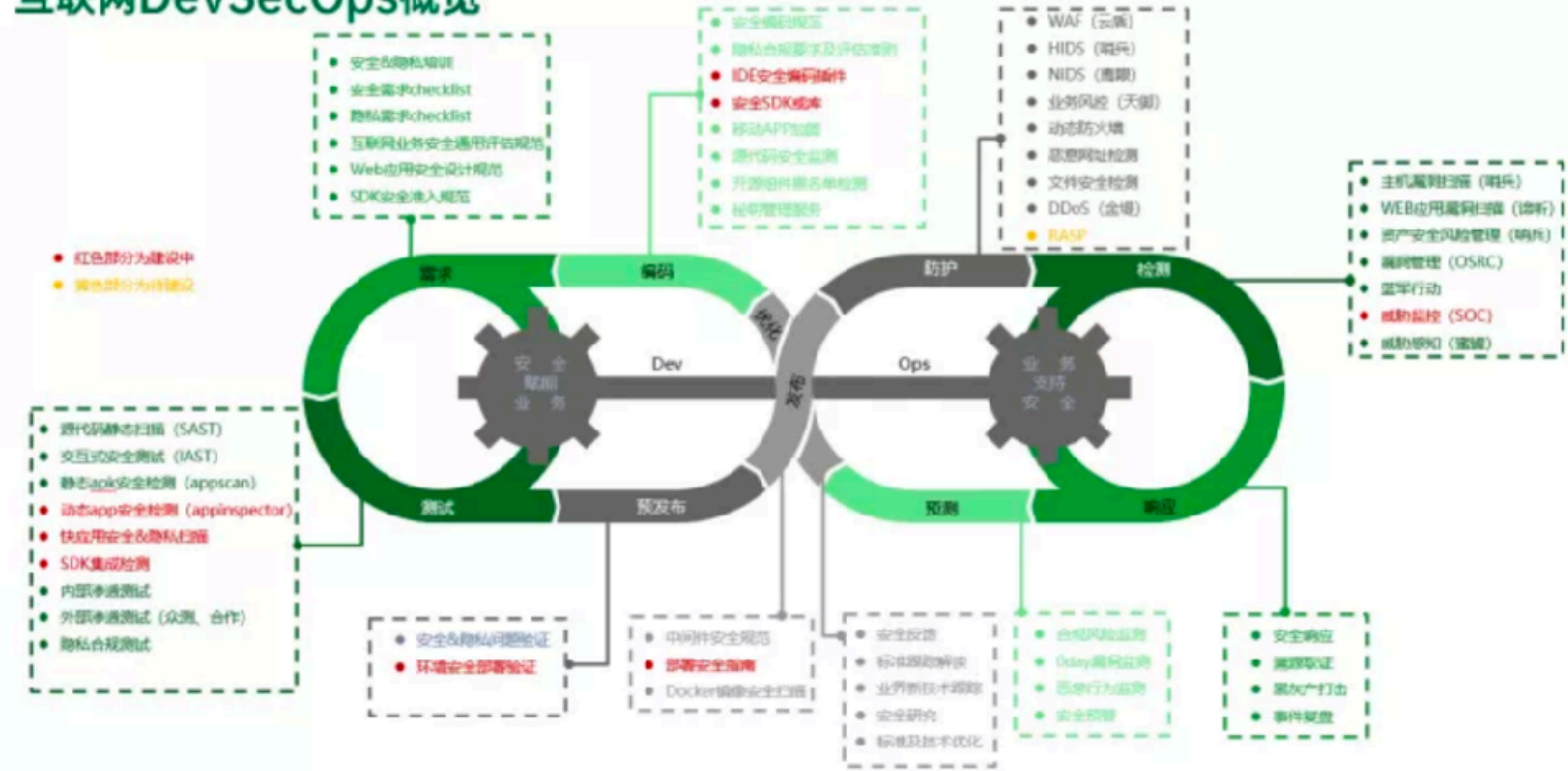
支付场景




注册绑定银行卡
发起打车订单并预付费用
取消订单
退款提现

如何走出此类困境

互联网DevSecOps概览



轻量级SDL实现

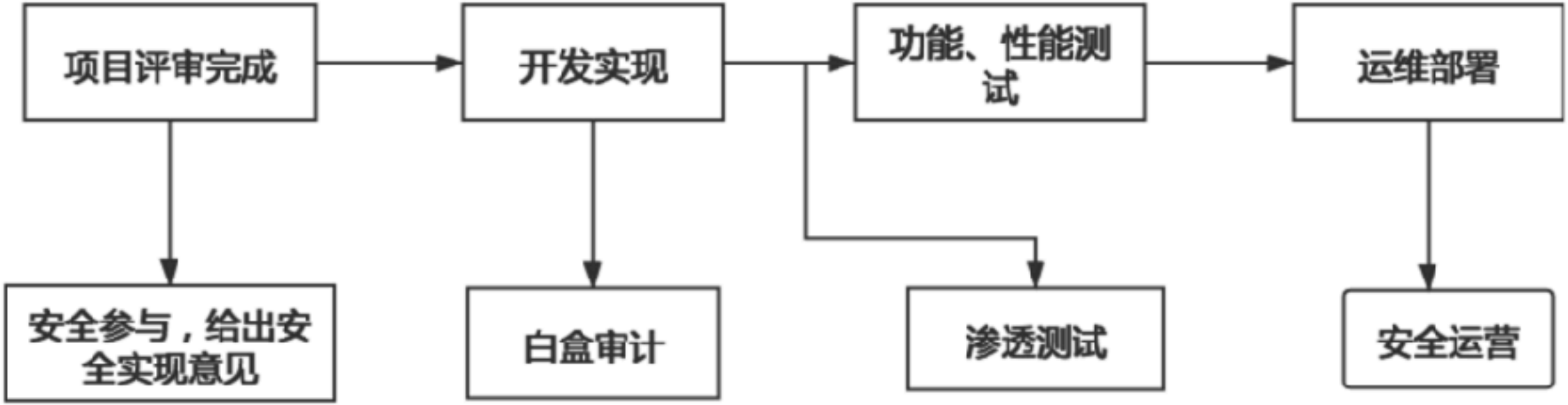
安全设计

白盒审计

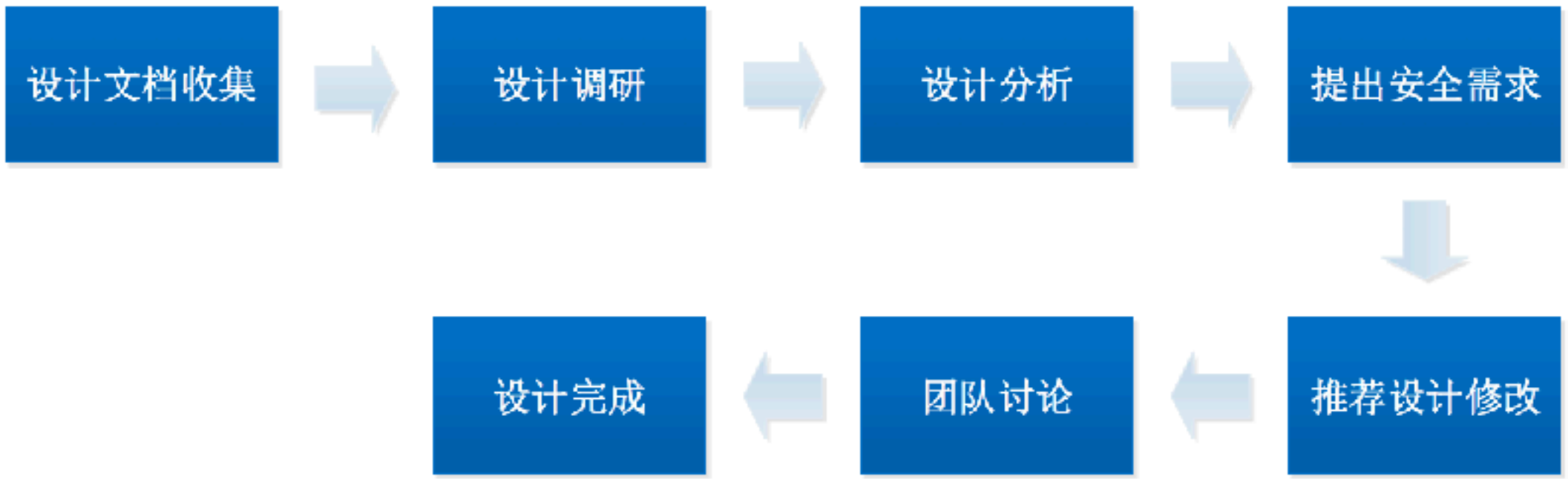
渗透测试

安全运营

轻量级SDL实现



安全设计介入时间与方式



- 数据流：
  - ✧ 用户输入是否被直接用于引用业务逻辑的类或函数？
  - ✧ 是否有一个数据绑定缺陷？
  - ✧ 是否暴露任何后门参数来调用业务逻辑？
  - ✧ 应用程序的执行流程是否正确？
- 身份验证和访问控制：
  - ✧ 是否对所有文件实现访问控制？
  - ✧ 是否安全地处理会话？
  - ✧ 是否存在单点登录？单点登录是否留下后门？
- 已有或内置的安全控制：
  - ✧ 在现有任意安全控制中的弱点；
  - ✧ 安全控制的部署是否正确？
- 架构：
  - ✧ 对所有的输入是否有验证？
  - ✧ 到外部服务器的连接是安全的吗？
- 配置或代码文件和数据存储：
  - ✧ 配置文件中是否含有敏感数据？
  - ✧ 是否支持任何不安全的数据源？

白盒审计

抓大放小

误报与漏报权衡

怎样倾听研发的声音

安全开发规范

创建： 白玉堂 于 三月 25, 2020

1、用户请求传入的任何参数必须做业务有效性验证。

说明：例如账号只允许字母数字和下划线的组合；上传的图片必须是jpg或png格式的，文件大小不能超过1m等，电子邮件、手机号码格式必须正确，确保用户提交的数据、文件合法。

2、用户敏感数据禁止直接展示，必须对展示数据进行脱敏。

说明：个人手机号码显示为:182****6957，隐藏中间4位，防止隐私泄露。

3、用户输入的SQL参数严格使用参数绑定或者METADATA字段值限定，防止SQL注入，禁止字符串拼接SQL访问数据库。

4、用户个人的页面或者功能必须进行权限控制校验。

说明：防止没有做水平权限校验就可随意访问、修改、删除别人的数据，比如查看他人的个人资料、修改他人的订单。

5、禁止向HTML页面输出未经安全过滤或未正确转义的用户数据。

说明：当输出数据格式、长度、内容等不符合输出要求时，必须处理成安全数据才可以输出。

6、在使用平台资源，譬如短信、电话、下单、支付，必须实现正确的防重放限制，如数量限制、验证码校验，避免被滥刷导致资损。

说明：如注册时发送验证码到手机，如果没有限制次数和频率，那么可以利用此功能骚扰到其它用户，并造成短信平台资源浪费。

渗透测试

漏洞的定级：技术难度与业务价值

漏洞的修复周期

安全运营

直观

迅速

可落地

安世加专注于安全行业，通过互联网平台、线下沙龙、培训、峰会、人才招聘等多种形式，
致力于创建亚太地区最好的甲乙双方交流、学习的平台，培养安全人才，
提升行业整体素质，助推安全生态圈的健康发展。

官方网站：https://

www.anshijia.net.cn

微信公众号：

asjeiss