通付盾

移动互联网数据隐私对抗

通付盾

撞库攻击

密码找回漏洞

数据篡改

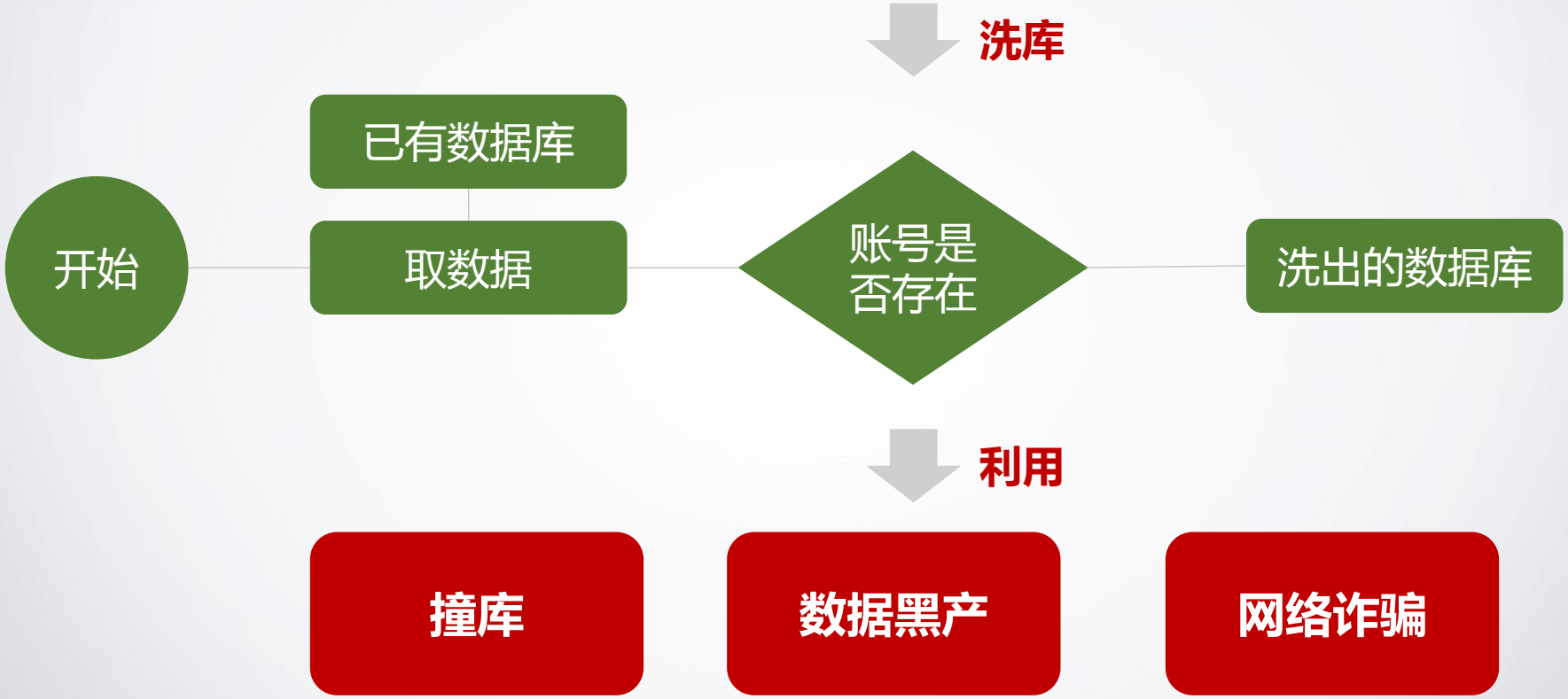
越权漏洞

01 撞库攻击

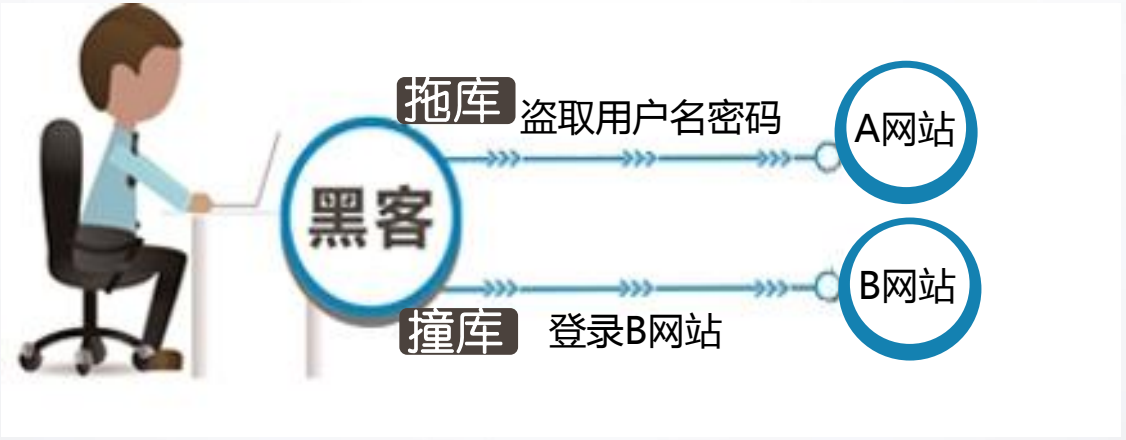
案例

通付盾
保护您的网络财产

2016年12月10日，12GB京东账户数据在暗网流通，数据多达数千万条。据说本次泄露的账户数据包括了用户名、密码、邮箱地址、QQ号、电话号码、身份证等信息。京东回应称这部分数据泄露是缘于2013年的Struts 2安全漏洞，并表示京东很早就已经修复了此漏洞



撞库攻击



验证码的前世今生

通付盾
保护您的网络财产

验证码作用：区分普通人与恶意攻击者、垃圾邮件、广告、撞库登录、暴力破解、暴力注册、投票刷票、恶意抢购、论坛灌水

传统验证码

- **识别率高**

有多种方式破解传统验证码，如抢票软件、OCR技术识别验证码、打码平台+机器学习，据360公布的12306验证码大数据显示，其图形验证码数量已经达到581种，但是借助各种识图技术破解图形验证码的成功率已经达到85%

- **用户体验差**

背景混淆识、文字扭曲、粘连等方法增加破解难度的同时，极大伤害用户体验

- **网站运行效率低**

一次验证成功的用户极低，过多的用户请求极大降低网站运行效率

传统验证码风险

- 验证码客户端校验
- 验证码客户端生成
- 验证码返回在客户端
- 验证码重复使用

…

验证码的突破

通付盾
保护您的网络财产

通付盾
保护您的网络财产

完善的滑动验证产品

人机识别
采集客户滑动过程轨迹，与服务器端海量数据样本对比，区分人和机器

防重放
验证被使用过一次就失效，不存在“一次成功，反复重复验证”的情况

防人工打码
验证码失效控制提高人工打码成本，referer绑定控制导致打码平台验证不通过

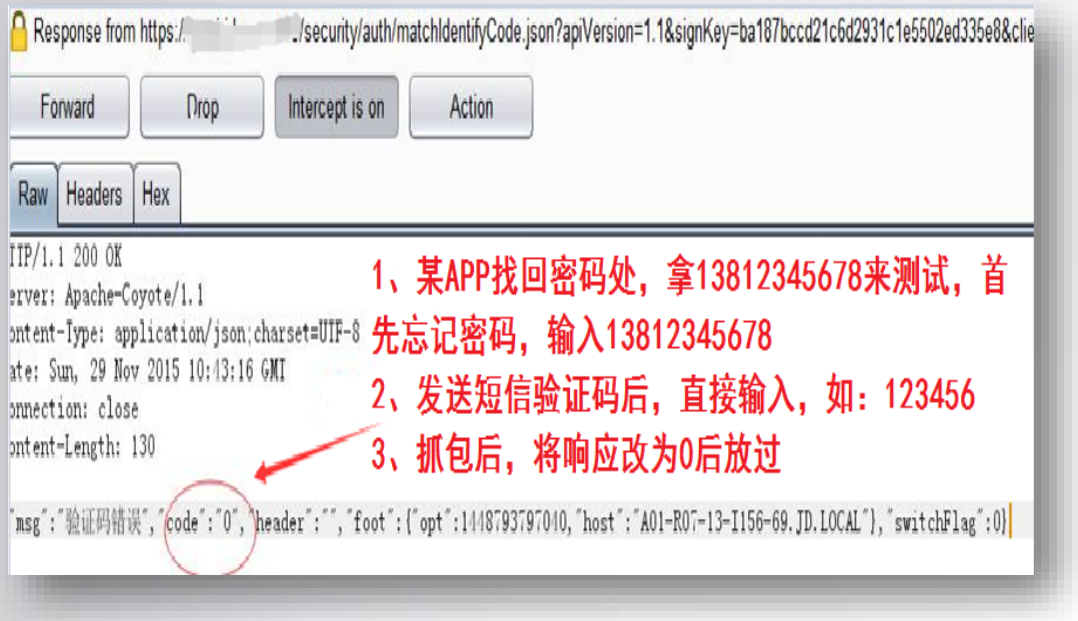
防绕过
基于强大的后台分析引擎，对比人机特征，避免破解程序绕过验证模块

密码找回漏洞

密码找回漏洞类型

通付盾
保护您的网络财产

密码找回漏洞


Response from https:/ ./security/auth/matchIdentifyCode.json?apiVersion=1.1&signKey=ba187bccd21c6d2931c1e5502ed335e8&clie
Forward
Drop
Intercept is on
Action
Raw
Headers
Hex
TTP/1.1 200 OK
erver: Apache-Coyote/1.1
ontent-Type: application/json;charset=UTF-8
ate: Sun, 29 Nov 2015 10:13:16 GMT
onnection: close
ontent-Length: 130
"msg":"验证码错误","code":"0","header":"","foot":{"opt":1441879379040,"host":"A01-R07-13-I156-69.JD.LOCAL"},"switchFlag":0}
1、某APP找回密码处，拿13812345678来测试，首先忘记密码，输入13812345678
2、发送短信验证码后，直接输入，如：123456
3、抓包后，将响应改为0后放过


中国移动
下午6:41
100%
关于我的
1、各种下一步，将新验证码修改为1381234
2、修改成功后，验证登录成功
bjzhouminh
点击此处去绑定
下班
我的账户
我的收成
消息中心
我的活动

解决方案

通付盾
保护您的网络财产

- 限制错误登录次数
- 不要将验证码放在客户端，验证码应进行单次有效校验
- Token生成随机且服务端对token进行校验
- 最终重置密码环节同时校验手机号和短信验证码
- …

数据篡改

业务数据篡改漏洞类型

通付盾
保护您的网络财产

0元购车

通付盾
保护您的网络财产

我的订单　交易提醒：所有订单（2）待付款（2）待收货（0）待评价（0）

下单时间(开始)　下单时间(结束)　关键字　商品名称/订单号　查找

查看订单详细

宝马X5(进口) 2014款 防弹车升级版

（定金购买）　订单编号：10000000266

预付定金 ¥1　未付款

当前状态：新订单　查看流程　去付款

关闭交易

订单总价

¥1

下单时间：2016-02-15 13:26:52

确认收货　我要投诉

查看订单详细

宝马4系车款 2014款 双门轿跑车 435i 风尚设计套装

（定金购买）　订单编号：10000000264

预付定金 ¥1　未付款

当前状态：新订单　查看流程　去付款

订单总价

¥2

下单时间：2016-02-14 17:51:24

确认收货　我要投诉

此处是价格

解决方案

通付盾
保护您的网络财产

服务端对支付金额进行校验

服务端对商品数量类型做校验，必须为正整数

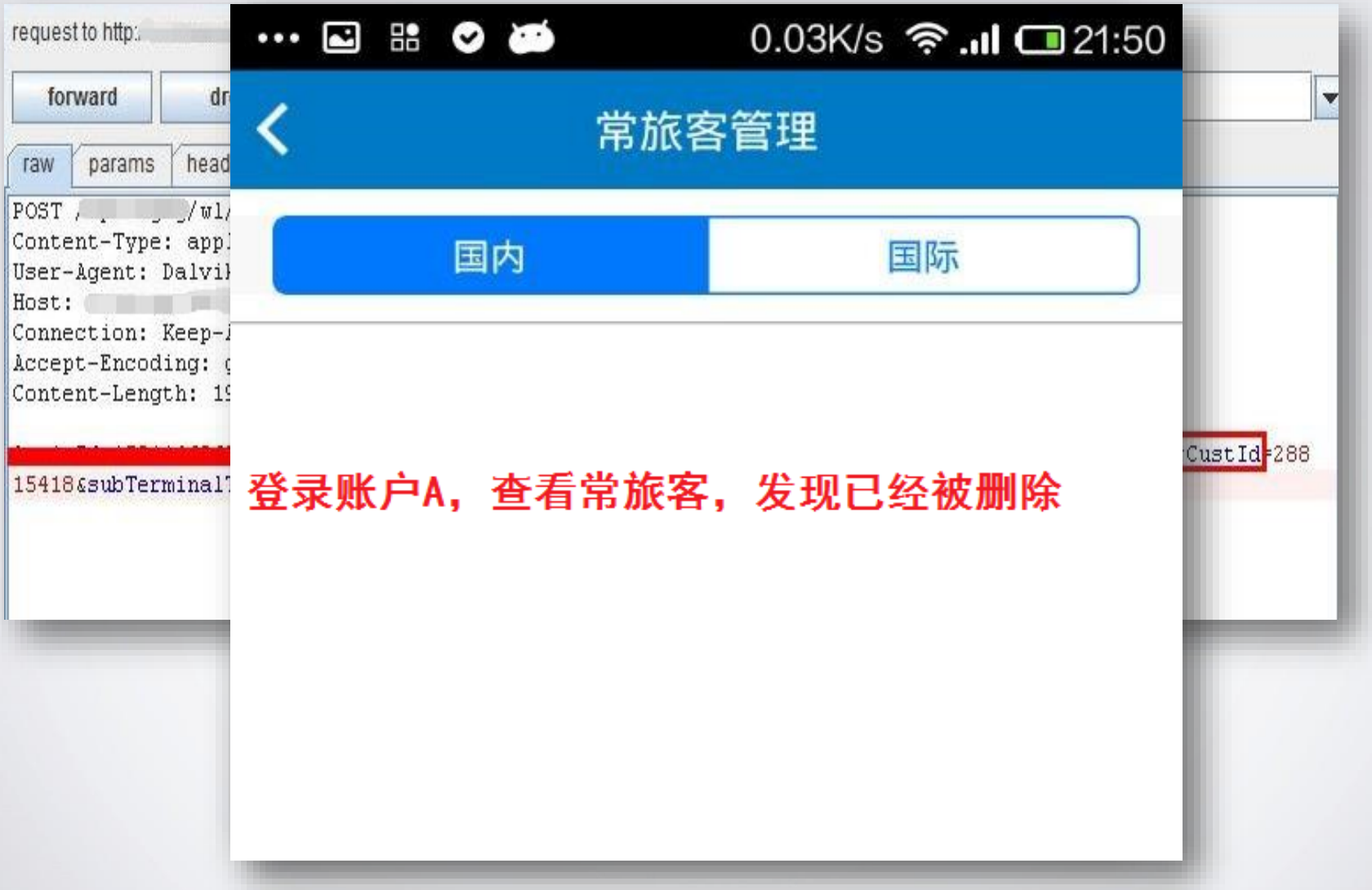
服务端校验用户提交的数据，如果大于限制的阀值不予通过

越权漏洞

越权漏洞类型

通付盾
保护您的网络财产

越权删除他人信息


request to http:
forward
raw
params
POST
Content-Type:
User-Agent:
Host:
Connection:
Accept-Encoding:
Content-Length:
15418&subTerminal
CustId=288
0.03K/s
21:50
常旅客管理
国内
国际
登录账户A，查看常旅客，发现已经被删除

解决方案

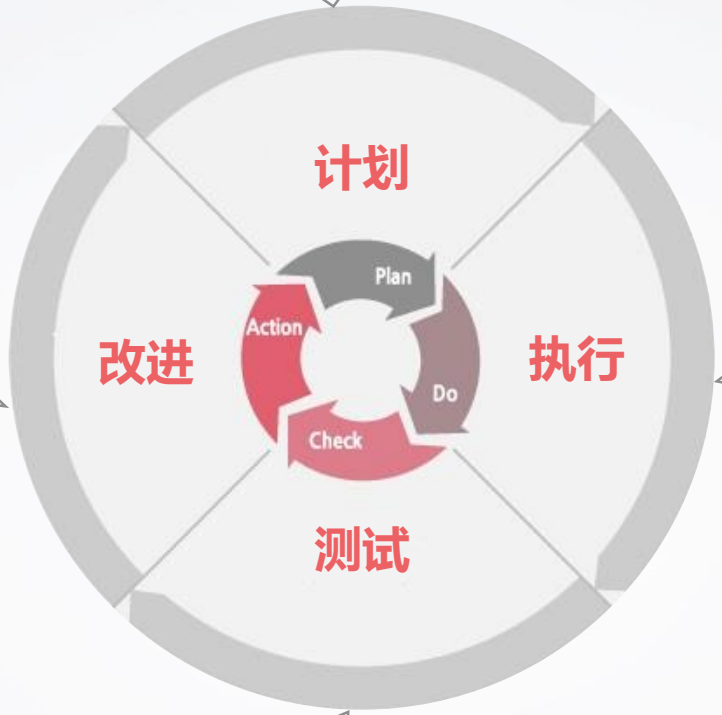
通付盾
保护您的网络财产

服务器端校验增删改查信息的操作是否属于当前用户

判断当前请求用户是否有相应权限

数据保护整体方案

产品设计阶段应遵循SDL，把安全要素融入到软件开发各个阶段



开发阶段应遵循安全开发规范，完成该阶段的安全任务，安全任务未完成不允许进入下一阶段

对于发现的漏洞应及时整改。安全是一场博弈，后续应持续检测及整改发现的漏洞，不断完善

开发完成应进行渗透测试，及时发现隐藏漏洞风险

客服电话：400-831-8116
官方网址：www.tongfudun.com
商务合作：info@tongfudun.com
售后服务：service@tongfudun.com

北 京 · 上 海 · 广 州 · 深 圳 · 苏 州 · 杭 州 · 成 都