业务视角下的逻辑安全

陆文举（土夫子）

关于我：

- 会分期运维总监、白帽子
- DSRC（滴滴安全应急响应中心）TOP白帽
- 帮助滴滴、百度、阿里、京东发现多个严重安全漏洞
- 8年运维经验，3年安全渗透经验
- 曾就职于58同城、碧生源等多家上市公司

业务，安全的基石

绑卡 | passport | 支付 | 订单

钱包 | 优惠券 | 认证中心 | 短信下发

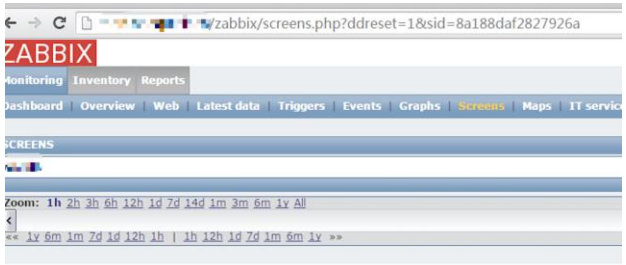
评价 | 修改密码 | 会员中心 | 提现

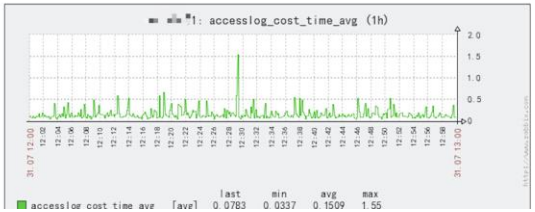
商家上传 | 商家导出 | 运营中心

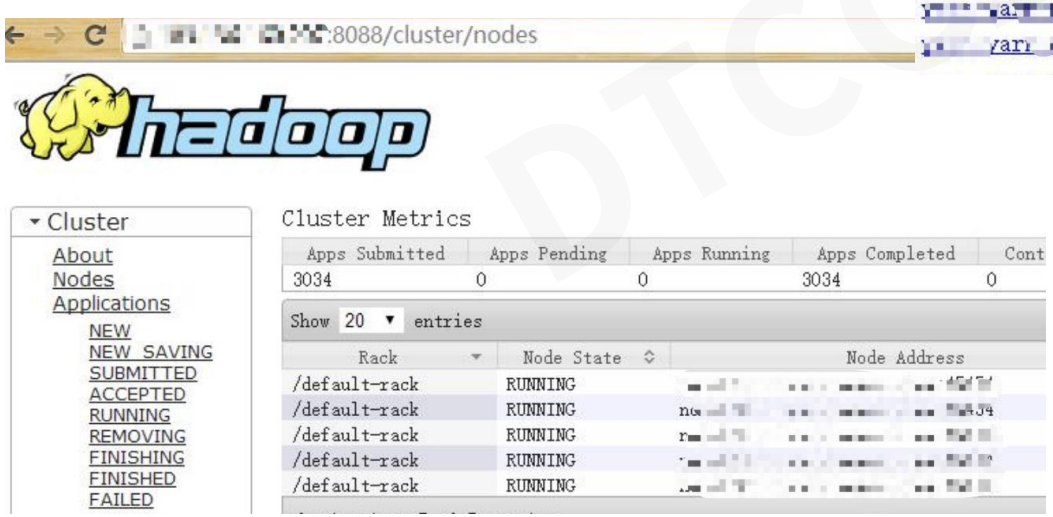
当前安全产品

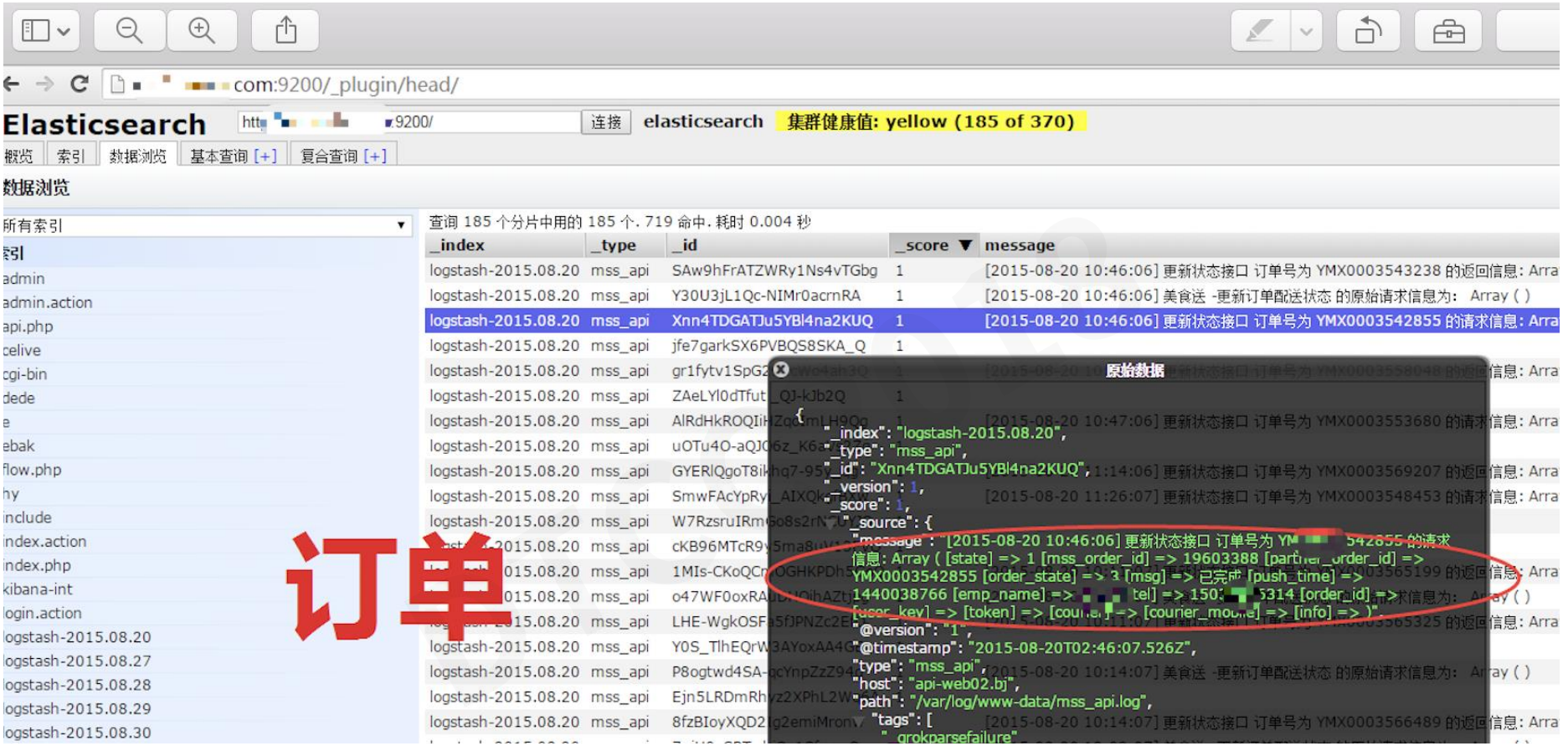
买了这么多安全产品，就安全了吗？

1、未授权访问









2、信息泄露

20000 元/月　面议

租赁方式：　整租

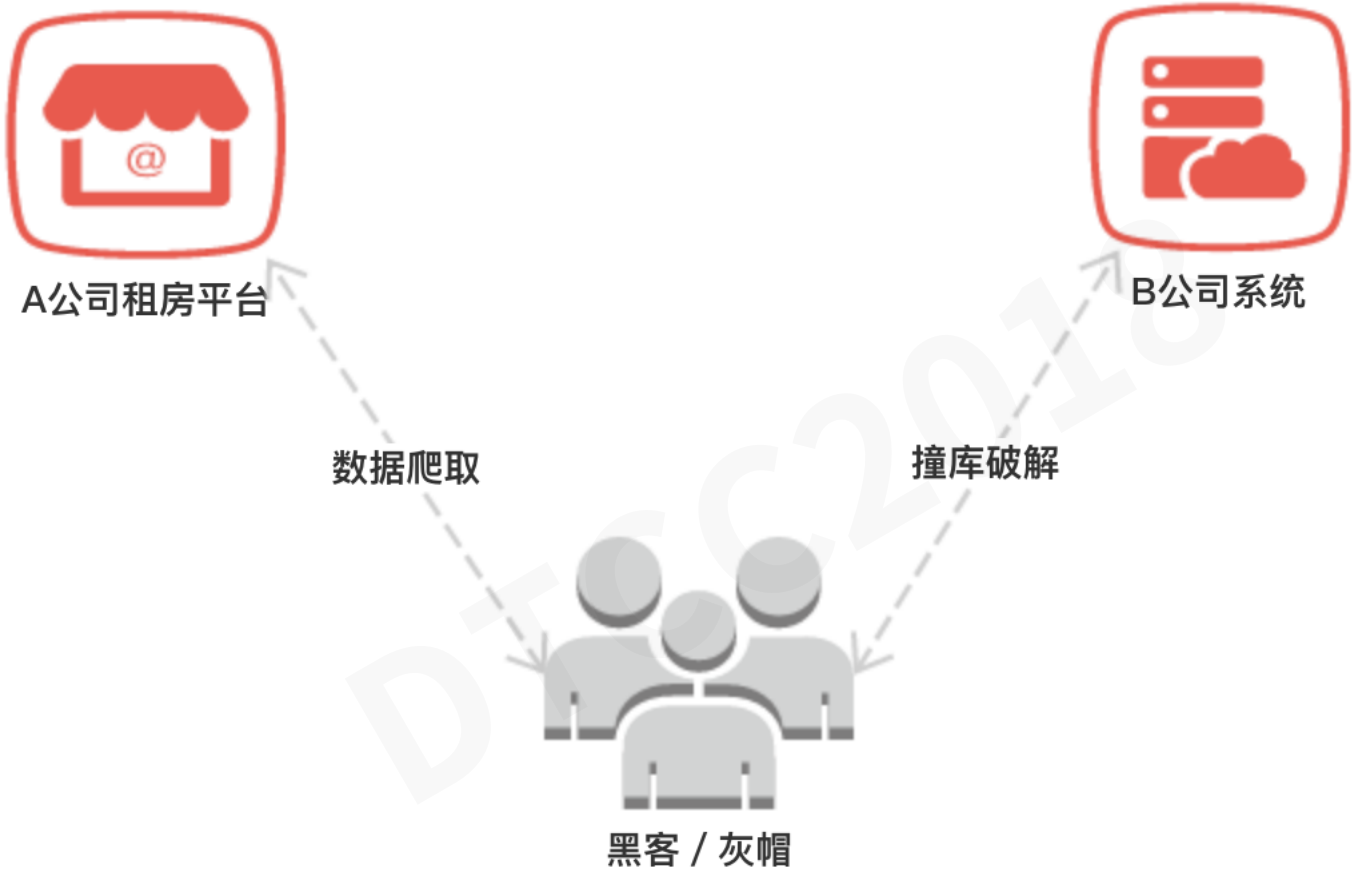
房屋类型：　3室2厅3卫　208 平　精装修

朝向楼层：　南　共3层

所在小区：

所属区域：

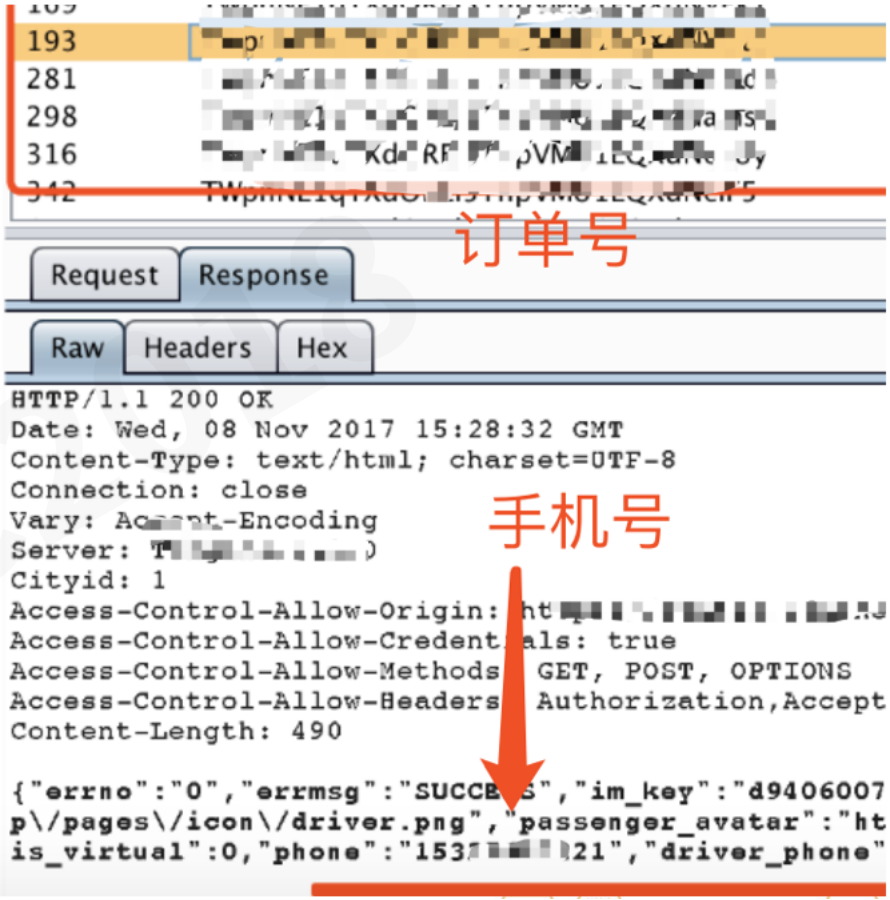
详细地址：



Raw | Headers | Hex

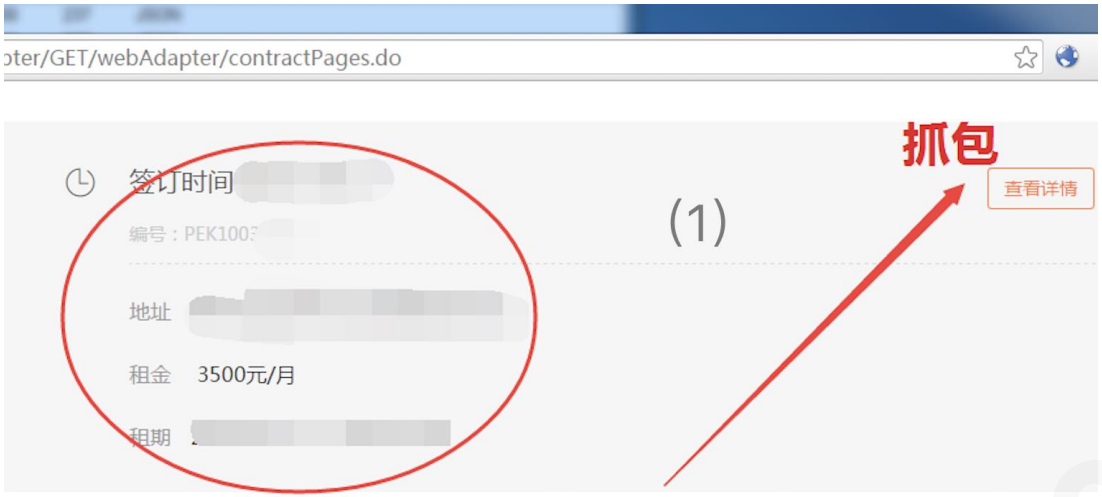
```
HTTP/1.1 200 OK
Date: Sat, 21 Oct 2017 07:35:36 GMT
Content-Type: application/json;charset=UTF-8
Connection: close
Server: nginx/1.6.2
Content-Length: 559

{
  "status" : 0,
  "data" : {
    "order" : {
      "orderId" : "[redacted]",
      "fromAddress" : "北京市朝阳区来广营东路融创动力文化创意[redacted]",
      "toAddress" : "[redacted]",
      "createTime" : [redacted],
      "st[redacted]s" : [redacted],
      "businessType" : [redacted],
      "[redacted]tName" : [redacted],
      "inne[redacted]" : "[redacted]e",
      "d[redacted]" : "[redacted]",
```

订单id、地址



订单id、地址、手机号 = 完整订单信息

3、越权遍历

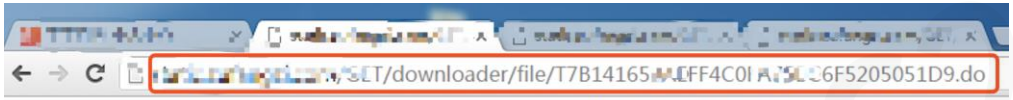



```
_ga=GA1.2.179097[redacted]123937;
Hm_lvt_09ee6c22fe881215ea09e54c879d08b1=1456123937,1456[redacted]
Hm_lpvt_09ee6c22fe881215ea09e54c879d08b1=1456125[redacted]

param=%7B%22contractId%22%3A%2231016%22%7D&base=%7[redacted]accou
n[redacted]%22%2C%22account[redacted]%22%3A%22%22%2C%22token%22%3A%22eyJ0eXA[redacted]IU
z[redacted]1NiJ9.eyJleHBpcmU[redacted]nBJ2CI6bn[redacted]3Vu
d[redacted]Ip
l[redacted]%22%3C%22[redacted]%224b534c46-166[redacted]-f04f-145[redacted]%22%2C%22ba
s[redacted]
```

遍历此处id

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 22 [illegible] 07:22:28 GMT
Content-Type: application/[illegible]; charset=UTF-8
Connection: [illegible]
Expires: Mon, 22 Feb [illegible] 07:22:27 GMT
Cache-Control: [illegible] cache
Access-Control-Allow-Origin: *
Content-Length: 508

{"message":"□□□□","data":{"title":"□□□□□□□□□□24□□□□","fileFetchUrl":"http://s[illegible].com/GET/do
wnloader/file/T7B1416[illegible]4C0.[illegible]75B[illegible]F5205051D9.do","hasAgreement":false,"description":"□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□B1-2-3,B1-2-4□□□□□□□□□□6□□□□□□8□3□□-822□1600.00□/□","icon[illegible]}
```

获取到的合同链接



北京市房屋租赁合同

出租人（甲方）：[illegible]　　身份证：[illegible]

承租人(乙方)：[illegible]　　身份证：[illegible]

居间人(丙方)：[illegible]

依据《中华人民共和国合同法》及有关法律、法规的规定，甲乙双方在丙方的居间服务下，在平等、自愿的基础上，就

第一条 房屋基本情况

(一)房屋坐落于 通州区马驹[illegible]

(二)户型 1室1厅1卫 ，房屋建筑面积 57.31 平方米。

(三)房屋权属状况：甲方持有(□房屋所有权证/ □公有住房租赁合同/ √房屋买卖合同/ □其他房屋来源证明文件)，房明名称：____，房屋(□是 √否)已设定了抵押。

(四)甲方身份：(√房地产权利人□代管人□转租人□其他____/____)。

后台越权，人人都是admin


```
eb\uff08\u5fd7\u65b0\u8def\u5e97\uff09#1","aoiname":"\u4e94\u9053\u53e3","business_status":null,"takeout_oncall_type":null,"shop_phone":"010-
38140.95","pass_uid":"1274322838","user_phone":"1    3","pass_phone":"","user_name":"\u7    \u58eb","user_address":"\u4    84\u5c
rder_time":"09:44","expect_time":"11:00","total_price":0,"total_real_price":"0.00","user_real_price":"0.00","user_price":43.01,"real_diff_price":0,"pay_sta
t":0.85},{"name":"\u9ebb\u9171","number":1,"current_price":2,"total":2,"discount_price":1.7,"shop_discount":0.85},
name":"\u6cb9\u9ea6\u83dc","number":1,"current_price":1,"total":1,"discount_price":0.85,"shop_discount":0.85},
"\u849c\u6ce5","number":1,"current_price":0.01,"total":0.01,"discount_price":0.01,"shop_discount":0.85},
ame":"\u5e7f\u5473\u9999\u80a0","number":3,"current_price":2,"total":6,"discount_price":5.1,"shop_discount":0.85},
\u5706\u751f\u83dc","number":1,"current_price":1,"total":1,"discount_price":0.85,"shop_discount":0.85},
\u9c7c\u4e38","number":1,"current_price":2,"total":2,"discount_price":1.7,"shop_discount":0.85},
ame":"\u8c46\u76ae","number":1,"current_price":2,"total":2,"discount_price":1.7,"shop_discount":0.85},
ame":"\u6728\u8033","number":1,"current_price":2,"total":2,"discount_price":1.7,"shop_discount":0.85},
\u6d77\u5e26\u7247","number":1,"current_price":2,"total":2,"discount_price":1.7,"shop_discount":0.85},
ame":"\u51ac\u74dc","number":2,"current_price":1,"total":2,"discount_price":1.7,"shop_discount":0.85},
```

4、支付

支付99元订金即可开团并邀请3人参团.
(详见下方活动流程)

选择外观:

冰晶白 苹果绿 珊瑚红 活力橙 宝石蓝 流光金

选择车型:

萌动版1.0L-5MT | 帅真版1.0L-5MT

酷趣版1.0L-5MT | 酷趣版1.5L-4AT

个人信息:

姓 名 参[redacted]

手 机 1[redacted]

验证码 1[redacted] 获取短信验证码

省 份 [redacted]区

城 市 [redacted]

经销商 [redacted]司

选择团购[redacted]餐(可选填):

团购专享套餐(套餐价：1元)

[redacted]

酷趣版1.0L-5MT指导价：

¥ 45,900

实际付款金额:

¥ 100 (订金)

立即拼团 我的团

* 团名：填写购车信息后可见

QQ炫舞 好友 辛爱的单身情歌

www.woovun.org

www.wooyun.org

5、密码重置

手机登录　　密码登录

手机号码未注册，请更换或 立即注册

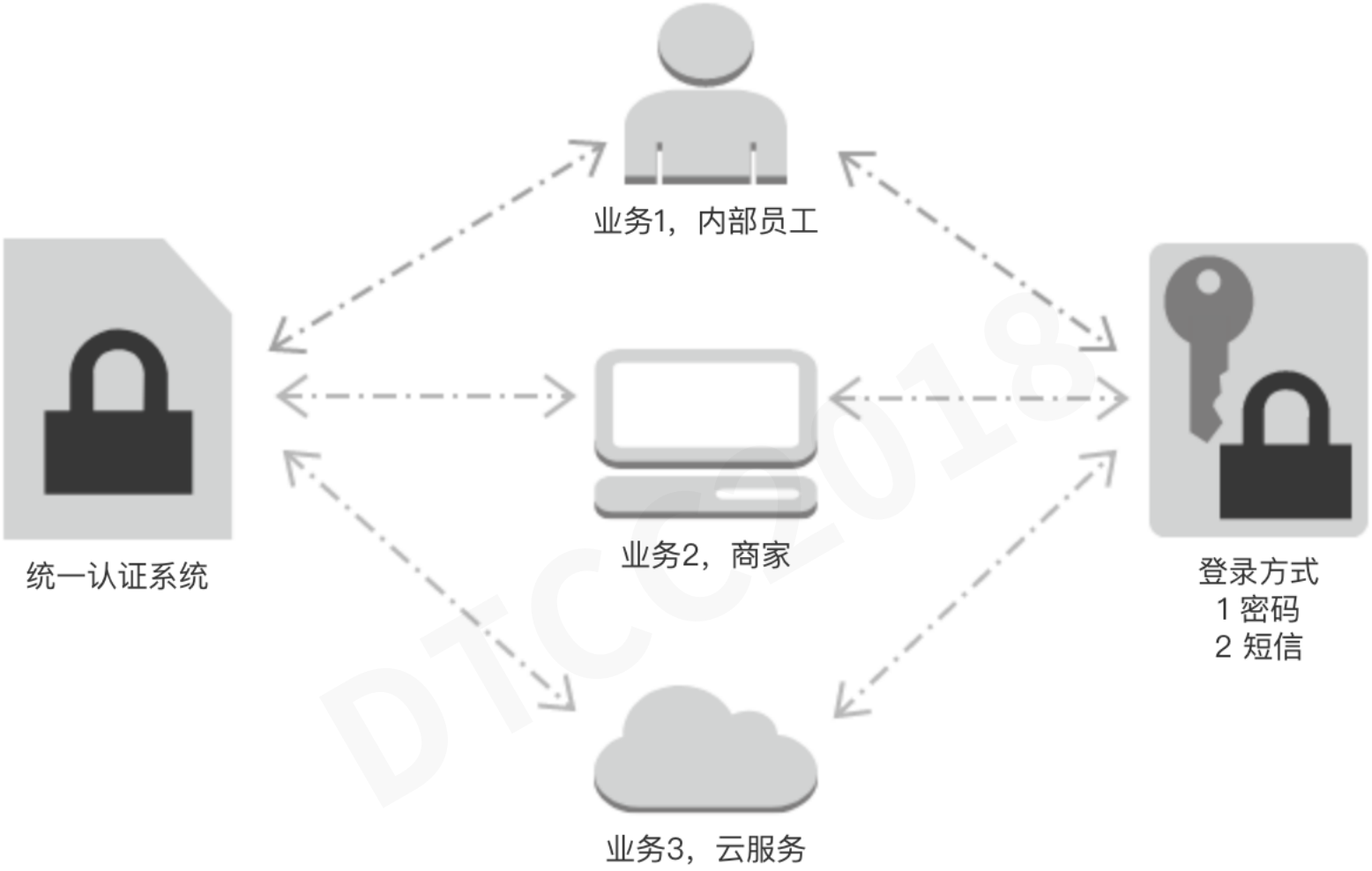
13344551123

短信验证码　　获取验证码

登录

2万次请求便可成功碰撞登录1个账号

6、API调用



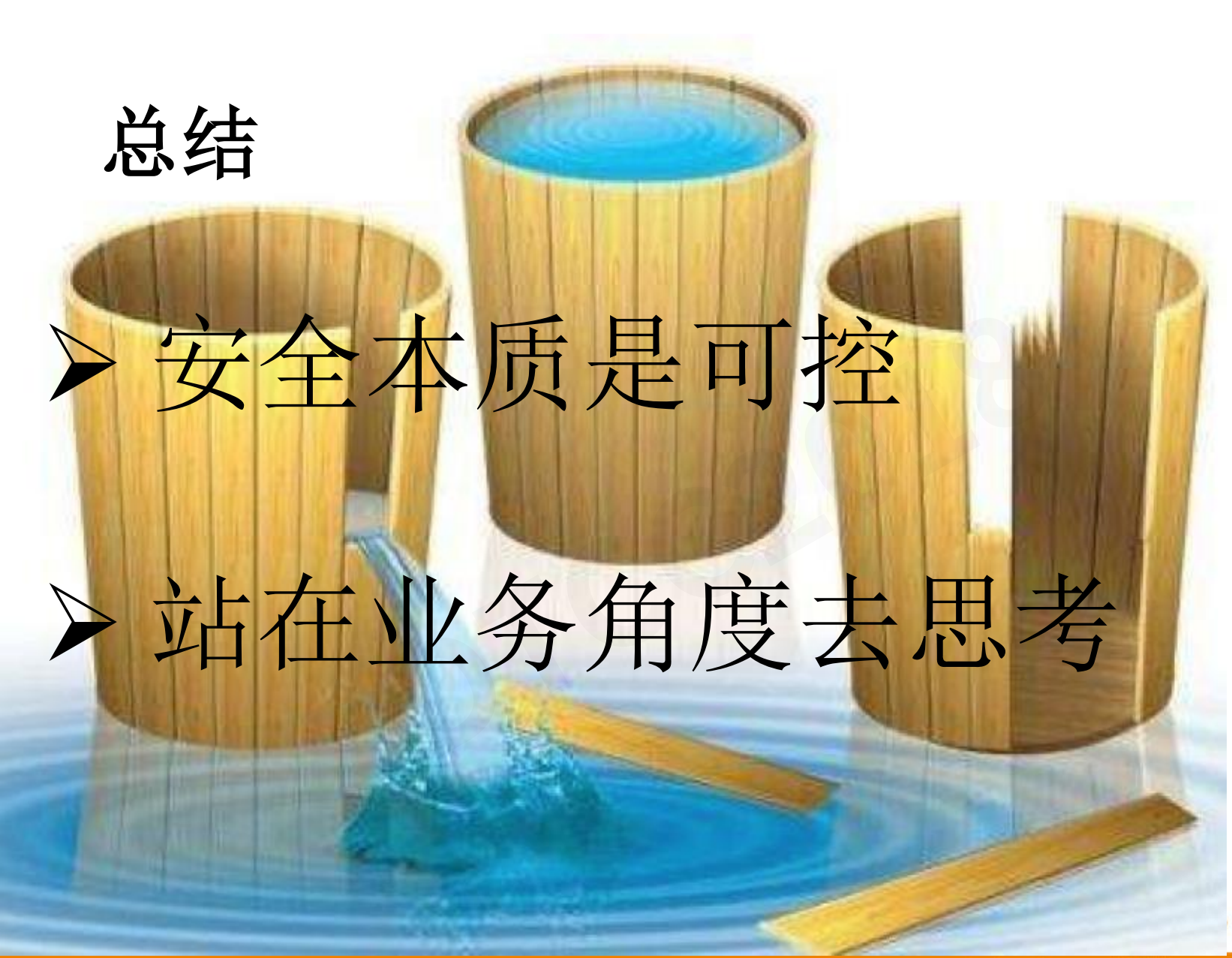
Attack type: Sniper

```
POST /passport/login HTTP/1.1
Host: auth.********.com
Content-Type: application/x-www-form-urlencoded
Origin: https://********.com
Connection: close
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 11_2_1 like Mac OS X) AppleWe
Referer: https://********.com/
Content-Length: 56
Accept-Language: zh-cn

r={"r":1,"cell":"13311221122","password":"123456","s":"1","code":"123123"}
```

r 代表业务线，1用户，2商家

s 代表登录方式，1密码，2短信

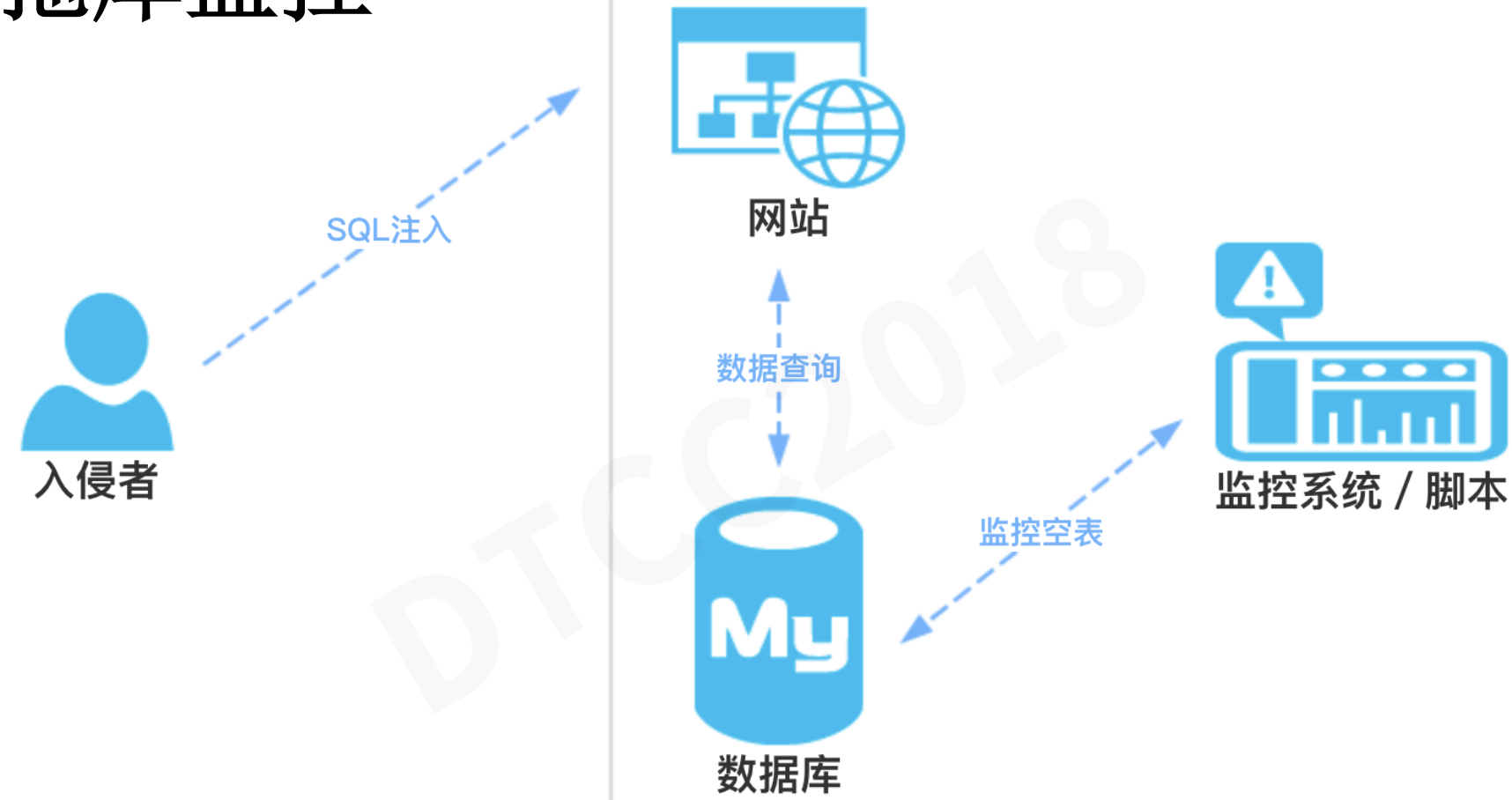
总结



- 安全本质是可控
- 站在业务角度去思考

SQL注入扫描检测

拖库监控



数据库加密存储

加盐法

多数应用在数据库存储数据的时候，对账号、，密码、银行卡等敏感数据可采用salt方法加密，防止数据被拖库后破解

混淆法

在存储数据时，可将a用户密码对应b用户密码，增加黑客破解难度

Java技术经理

资深数据建模工程师

资深／高级java开发工程师

高级数据爬虫工程师

数据挖掘工程师

测试工程师

支付技术总监

架构师／技术经理

THANKS


HANA
Hadoop
SQL
MySQL
DB2
BigData
Spark
SQL Server
NewSQL
Oracle
MPP
NoSQL
OLAP

讲师申请
联系电话（微信号）：18612470168

关注“ITPUB”更多
技术干货等你来拿~

与百度外卖、京东、魅族等先后合作系列分享活动

微学堂

让学习更简单

微学堂是以ChinaUnix、ITPUB所组建的微信群为载体，定期邀请嘉宾对热点话题、技术难题、新产品发布等进行移动端的在线直播活动。

截至目前，累计举办活动期数60+，参与人次40000+。

ITPUB学院

ITPUB学院是盛拓传媒IT168企业事业部（ITPUB）旗下
企业级在线学习咨询平台
历经18年技术社区平台发展
汇聚5000万技术用户
紧随企业一线IT技术需求
打造全方式技术培训与技术咨询服务
提供包括企业应用方案培训咨询（包括企业内训）
个人实战技能培训（包括认证培训）
在内的全方位IT技术培训咨询服务

ITPUB学院讲师均来自于企业
一些工程师、架构师、技术经理和CTO
大会演讲专家1800+
社区版主和博客专家500+

培训特色

无限次免费播放
随时随地在线观看
碎片化时间集中学习
聚焦知识点详细解读
讲师在线答疑
强大的技术人脉圈

八大课程体系

基础架构设计与建设
大数据平台
应用架构设计与开发
系统运维与数据库
传统企业数字化转型
人工智能
区块链
移动开发与SEO

联系我们

联系人：黄老师
电　话：010-59127187
邮　箱：edu@itpub.net
网　址：edu.itpub.net
培训微信号：18500940168