阿里云 | 云盾先知 安全情报

以程序架构探索
移动应用安全的发展历程

先知白帽大会
开放创新 · 先知先行

- WHOAMI？？？

- 残废
- 四叶草安全安全服务部成员，雁行安全团队成员
- 主攻渗透测试，web安全，拥有数百个企业安服实战经验
- 曾多次出现在国内安全顶尖会议
- 多次在甲方安全应急响应中心获得奖项
- Mail：chaihao@seclover.com

- 从互联网到移动应用
- 登陆流程
- 身份认证
- 支付安全
- 用户交互
- 存储机制
- 数据安全
- 客户端缺陷
- 风险控制

从互联网到移动互联——宏观角度

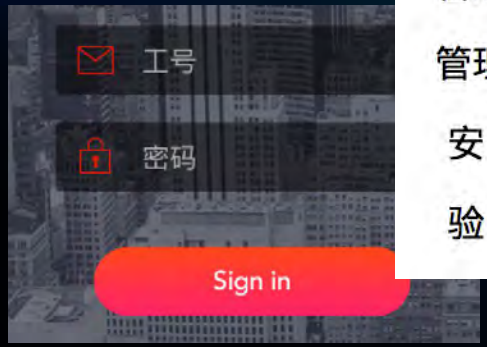
- 互联网到物联网
- 移动设备智能化
- 移动应用多元化
- 移动安全事件的频发
- 移动应用安全检测基准
- 恐怖的移动应用
- 有意识的构建移动应用安全标准体系

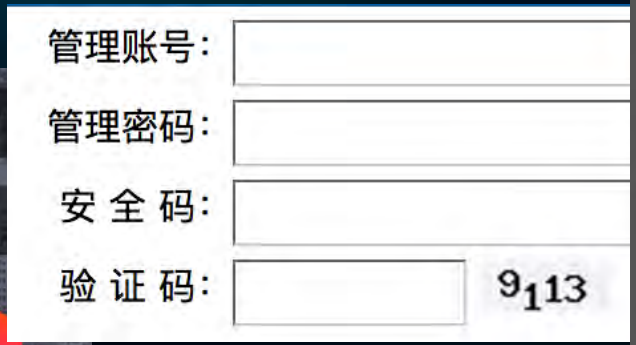
测试者眼中的移动应用——微观角度

? ? ?

登陆流程

- 单因子→多因子→复杂因子→时效因子





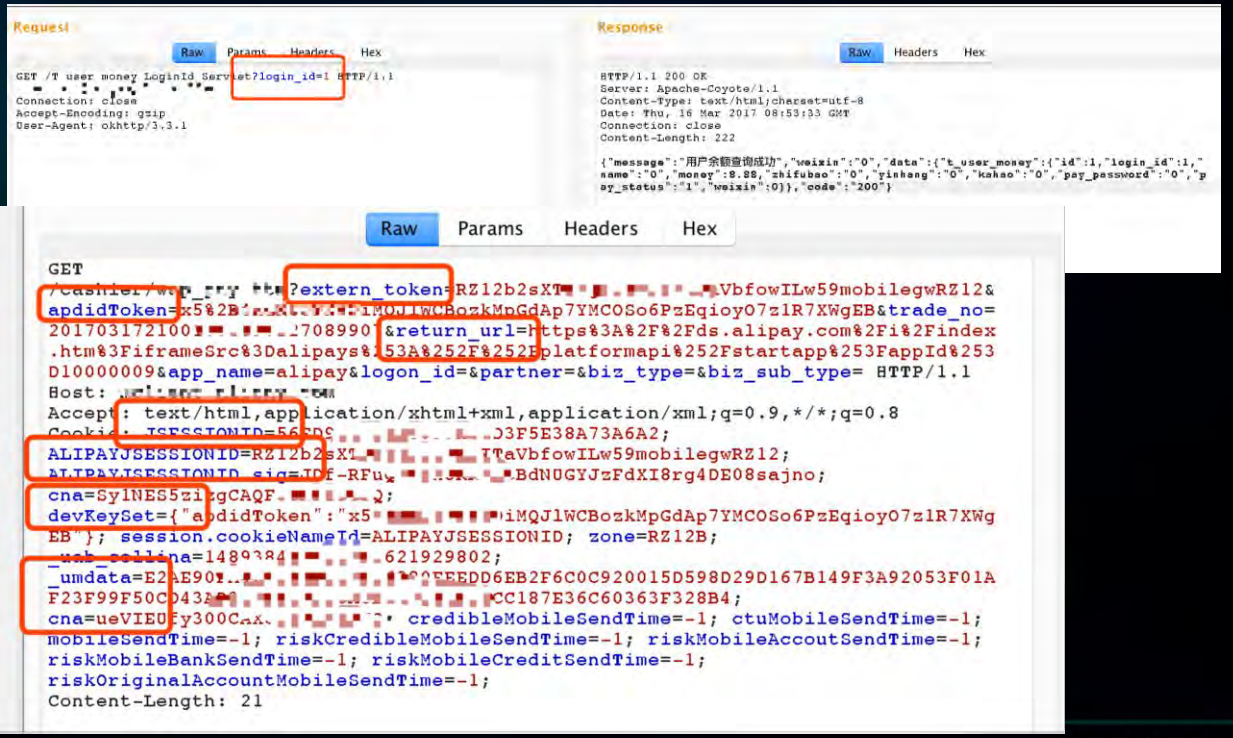
身份识别

- What you know
- What you have
- What are you

- Can i know ?
- Can i have ?
- Can i be you ?

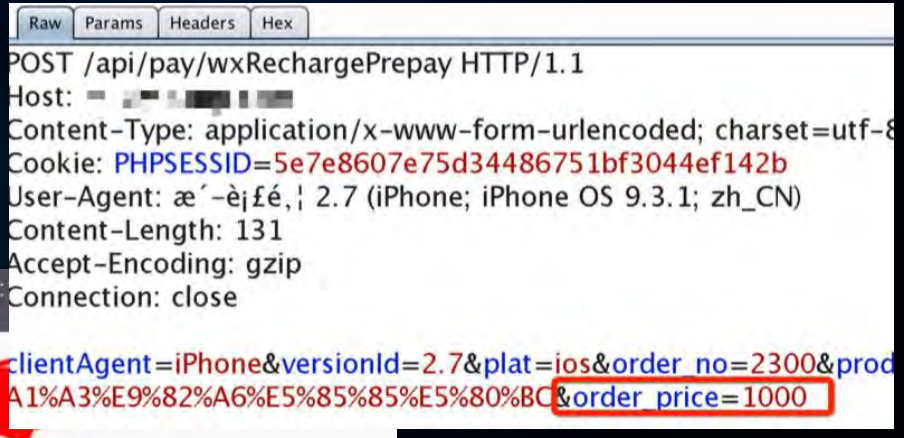
身份认证

- 单一身份标识
- 多重身份检查




我的收银台
正在使用即时到账交易 [?]
好记星学生平板电脑N787，
收款方：上海橡果网络技术...
微信安全支付
¥0.01
收款方
洗衣邦
立即支付
扫一扫付款（元）
0.01

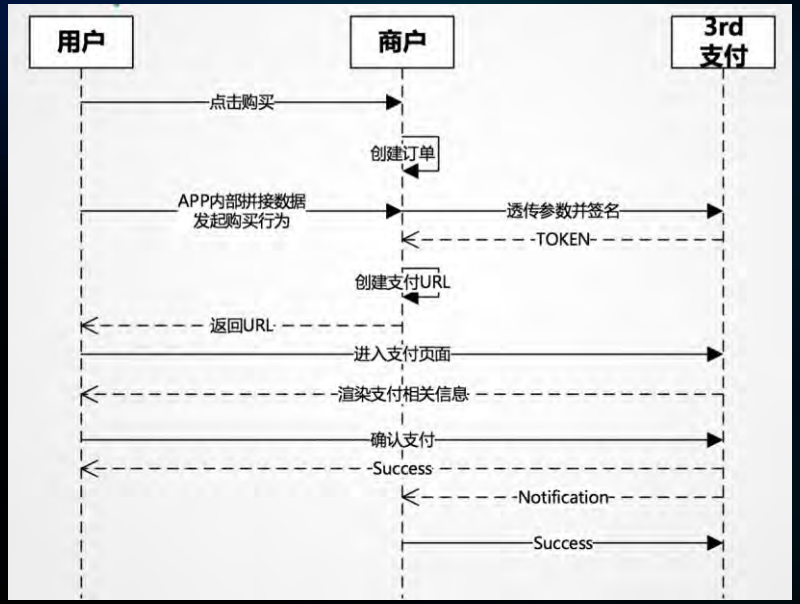
支付业务


Raw
Params
Headers
Hex
POST /api/pay/wxRechargePrepay HTTP/1.1
Host:
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Cookie: PHPSESSID=5e7e8607e75d34486751bf3044ef142b
User-Agent: æ´-è¡£é¸¦ 2.7 (iPhone; iPhone OS 9.3.1; zh_CN)
Content-Length: 131
Accept-Encoding: gzip
Connection: close
clientAgent=iPhone&versionId=2.7&plat=ios&order_no=2300&prod
A1%A3%E9%82%A6%E5%85%85%E5%80%BC&order_price=1000

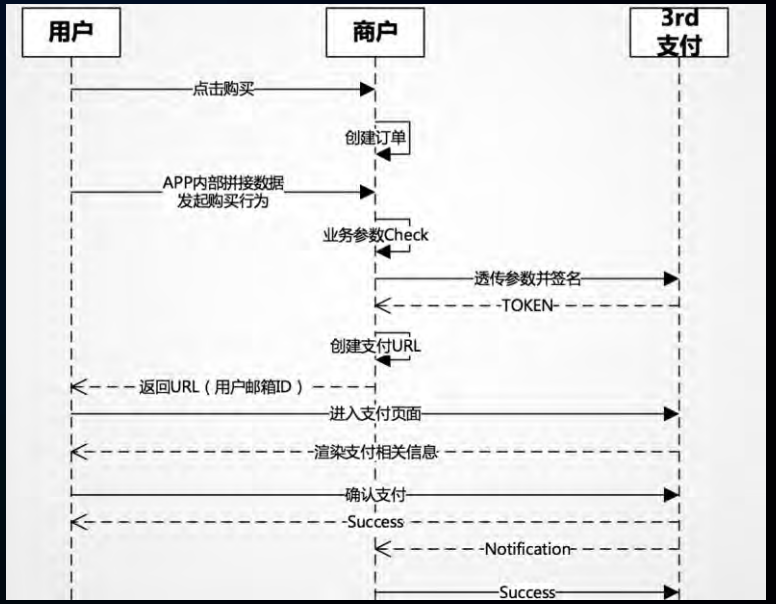

订单号:
Chantal Thomass 巴黎女人 黑色蕾丝褶皱装饰软杯内衣
¥1
2015-03-24
收货人信息

支付业务安全

- 常规支付模型

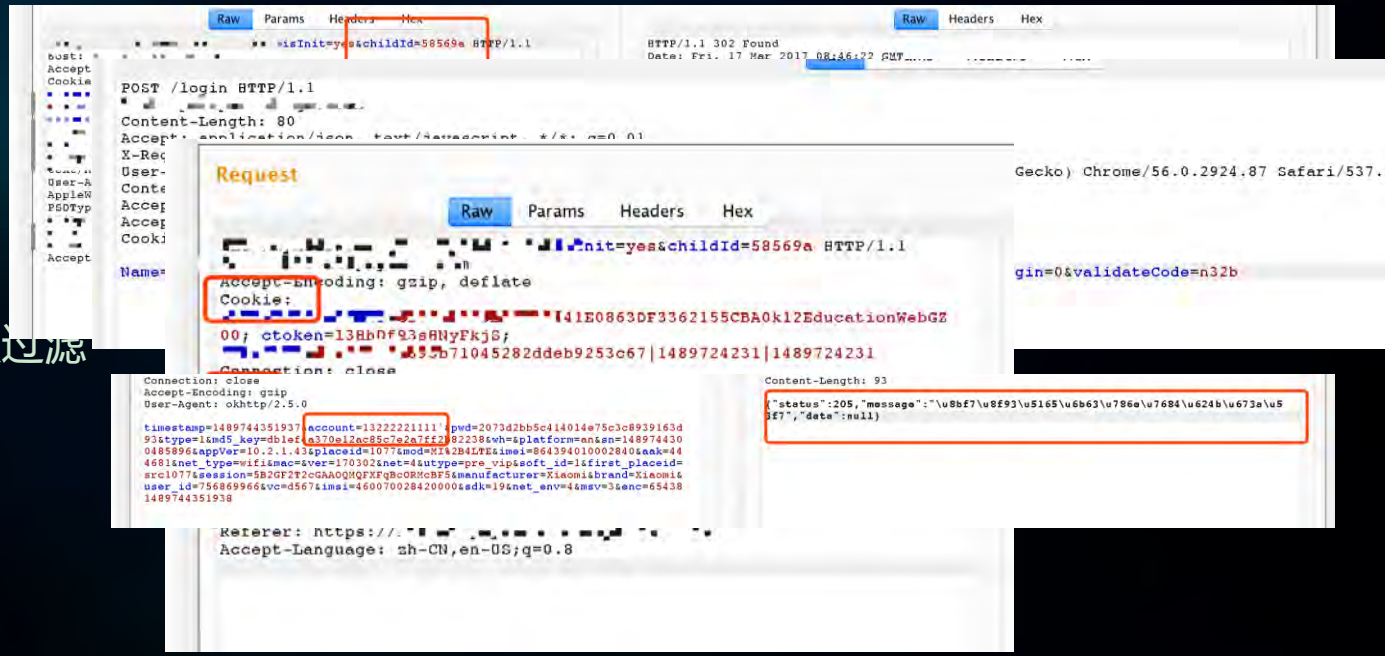


- 低风险支付模型



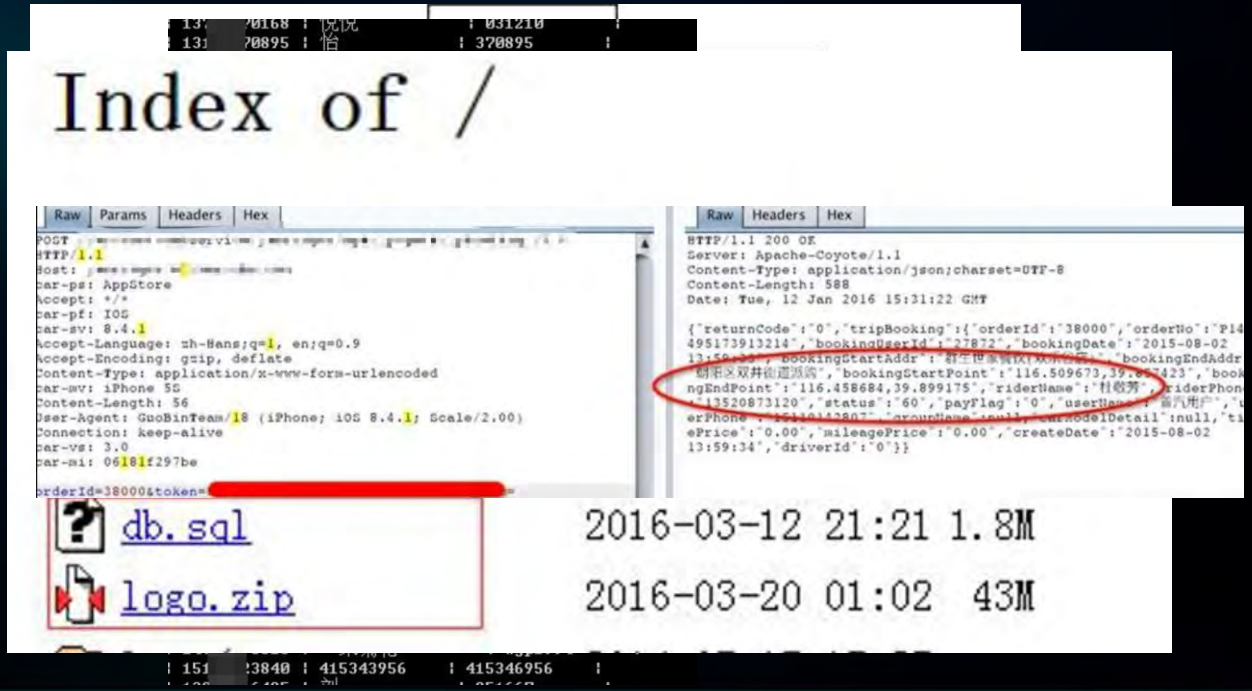
用户交互

- 参数数据类型控制
- 数据传输加密
- 安全认证机制
- 用户输入内容检测及过滤
- 用户权限控制
- 参数值的加密



数据安全

- 数据对称算法加密
- 敏感内容加密
- 权限未明确建立
- 数据备份 / 迁移
- 数据访问控制权限



存储安全

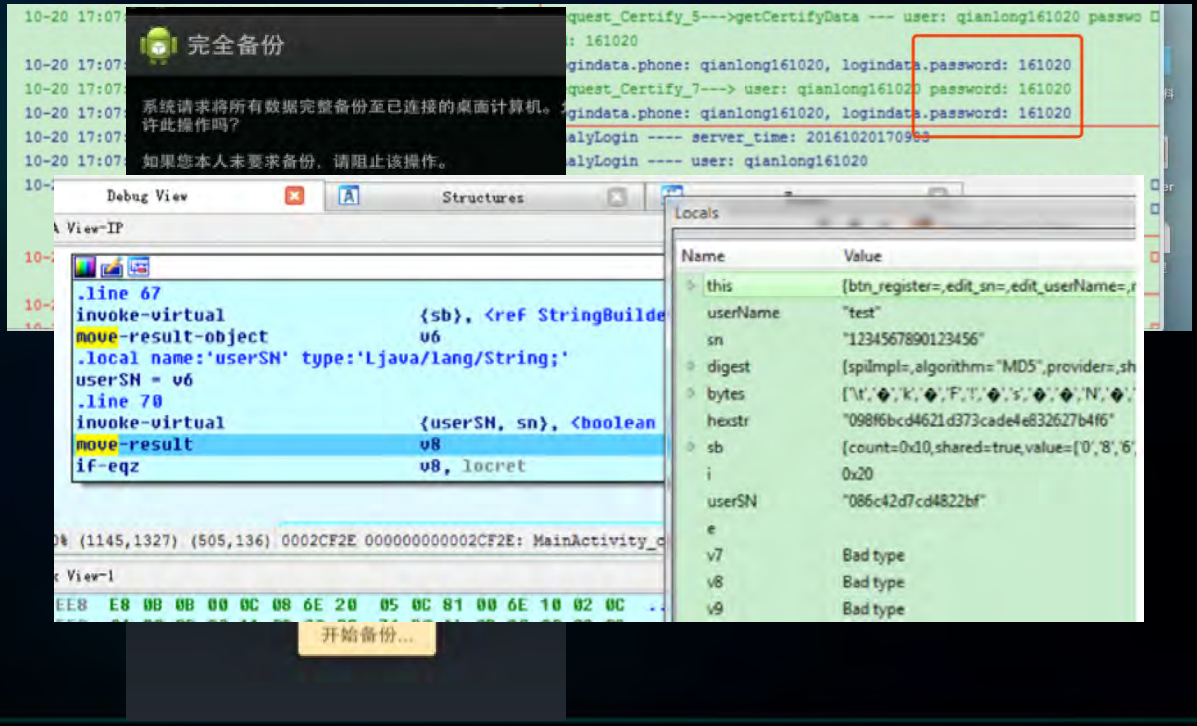
- 配置信息明文存储
- 日志输出明文敏感数据
- 数据传输直传直入
- 敏感信息本地存储

```
<int name="mSystem" value="5" />
<int name="mQSDM_4X" value="0" />
<int name="mProduct" value="256" />
<string name="mUser">qianlong161020</string>
<string name="mDeviceToken">3575161116566245_192.168.30.71_d
<string name="mPassWord">161020</string>
/map>
```

```
10-20 17:07:31.893  1908  1..  Request_Certify_5--->getCertifyData --- user: qianlong161020 passwo
                                rd: 161020
10-20 17:07:31.893  1908  1..  logindata.phone: qianlong161020, logindata.password: 161020
10-20 17:07:32.363  1908  2..  Request_Certify_7---> user: qianlong161020 password: 161020
10-20 17:07:32.363  1908  2..  logindata.phone: qianlong161020, logindata.password: 161020
10-20 17:07:32.493  1908  2..  AnalyLogin ---- server_time: 20161020170955
10-20 17:07:32.493  1908  2..  AnalyLogin ---- user: qianlong161020
10-20 17:07:32.493  1908  2..  Request53--->actionType = 1, user = qianlong161020, date = 0 0, cod
                                e = 01000001,02399001, version = V3.18 B001(20160818), platform = 5
                                , product = 256, qsdm = 0
10-20 17:07:32.603  1908  1..  System_...  MSG_UPDATE_DATA--->mMyApp.mUser = qianlong161020, mMyApp.mPassWord
                                = 161020
10-20 17:07:32.673  1908  1..  System_...  qianlong161020-161020
```

客户端缺陷

- 日志信息的保存
- 程序可被调试
- 任意数据备份
- 全局文件可读写



风险控制

- IP客观属性
- IP主动探测
- 历史行为辅助
- 风控规则
- 传统校验
- ……

怎么变的？

移动应用本身

- 用户
  - 减少记忆内容
  - 简化操作流程
  - 增加认证因子
  - 引入单点登录
  - 内容输入判定
  - 安全级别提醒
  - 行为日志调取
  - 敏感操作验证
- 后端
  - 数据传输保护
  - 后端多重验证
  - 人机检测判定
  - 权限划分清晰
  - 数据安全存储
  - 行为数据分析
  - 运维体系建立
  - 程序自我保护

风险控制


体验
安全

史蒂夫·乔布斯 - 献给疯狂而勇敢的人们

他们是一些与周围格格不入的人，是喜欢自由的人，是那些爱反抗的人，是那些爱惹麻烦的人；

他们以一种不同的方式看待世界。

他们不爱墨守成规，也不乐于接受现状。

你可以认同他们，也可以反对他们；可以赞美他们，也可以贬低他们，但是你唯一做不到的就是忽略他们。因为是他们改变了世界，是他们推动了社会的前进。

也许有些人视他们为疯子，可我们视他们为天才。

因为真正改变了这个世界的，正是那些疯狂到认为自己能够改变世界的人。


阿里云
云盾先知
安全情报
THANKS!