**报告编号：2018-XAFH-SXLT-2**

**互联网新技术新业务信息安全评估复核报告**

|  |  |
| --- | --- |
| **委托单位：** | 中国电信集团有限公司陕西省分公司 |
| **业务名称：** | 智慧乡村 |
| **完成时间：** | 2018年12月 |

**评估单位：国家计算机网络与信息安全管理中心**

**2018年12月**

**声明**

受中国联合网络通信有限公司陕西省分公司委托，国家计算机网络与信息安全管理中心对中国联合网络通信有限公司陕西省分公司移网场景营销平台进行了新技术新业务初评报告的核查。

本次核查主要从系统架构和业务流程分析入手，全面查找智联商城系统配置的不安全因素，查验业务系统是否存在信息安全隐患，保障业务信息安全。

本报告评估结论的有效性建立在被评估单位提供相关证据的真实性基础之上。

本报告中所给出的核查结论仅对被评估业务系统当时的安全状态有效。当评估工作完成后，由于业务系统发生变更而涉及到的系统构成组件（或子系统）都应重新进行评估，本报告不再适用。

本报告中给出的核查情况评估结论不能作为对业务系统内部署的相关系统构成组件（或产品）的评估结论。

在任何情况下，若需引用本报告中的核查结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实。

**评估复核情况确认签字表**

|  |  |
| --- | --- |
| **受评**  **单位** | 中国电信集团有限公司陕西省分公司 |
| **复核**  **业务** | 智慧乡村 |
| **评估**  **复核**  **依据** | 1、《工业和信息化部办公厅关于印发<2018年省级基础电信企业网络与信息安全工作考核要点与评分标准>的通知》（工信厅网安〔2018〕4号）  2、《互联网新技术新业务安全评估指南》（2018年修订版） |
| **复核**  **结果** | 根据工信部相关工作要求和标准，国家计算机网络与信息安全管理中心对移网场景营销平台业务进行了复核，经评估一致认为：   1. 该业务存在部分信息安全风险，可进行改进，总体安全可控，但总体制度建设、制度规范需要进一步加强。 2. 后续需在数据传输管理、登录机制完善、信息内容管理、等多方面进行问题整改，同步配套更新安全保障措施。 3. 该业务评估报告结构较为严谨，但存在部分项目研判依据不准确，技术保障方面仍存在信息安全的薄弱环节 |
| **评估单位**  **复核确认**  **（签字及盖章）** |  |
| **信息安全部门负责人**  **（签字及盖章）** |  |

附件：复核记录

1. **初评报告中部分研判不准确：**

初评报告中存在部分内容研判不准确：

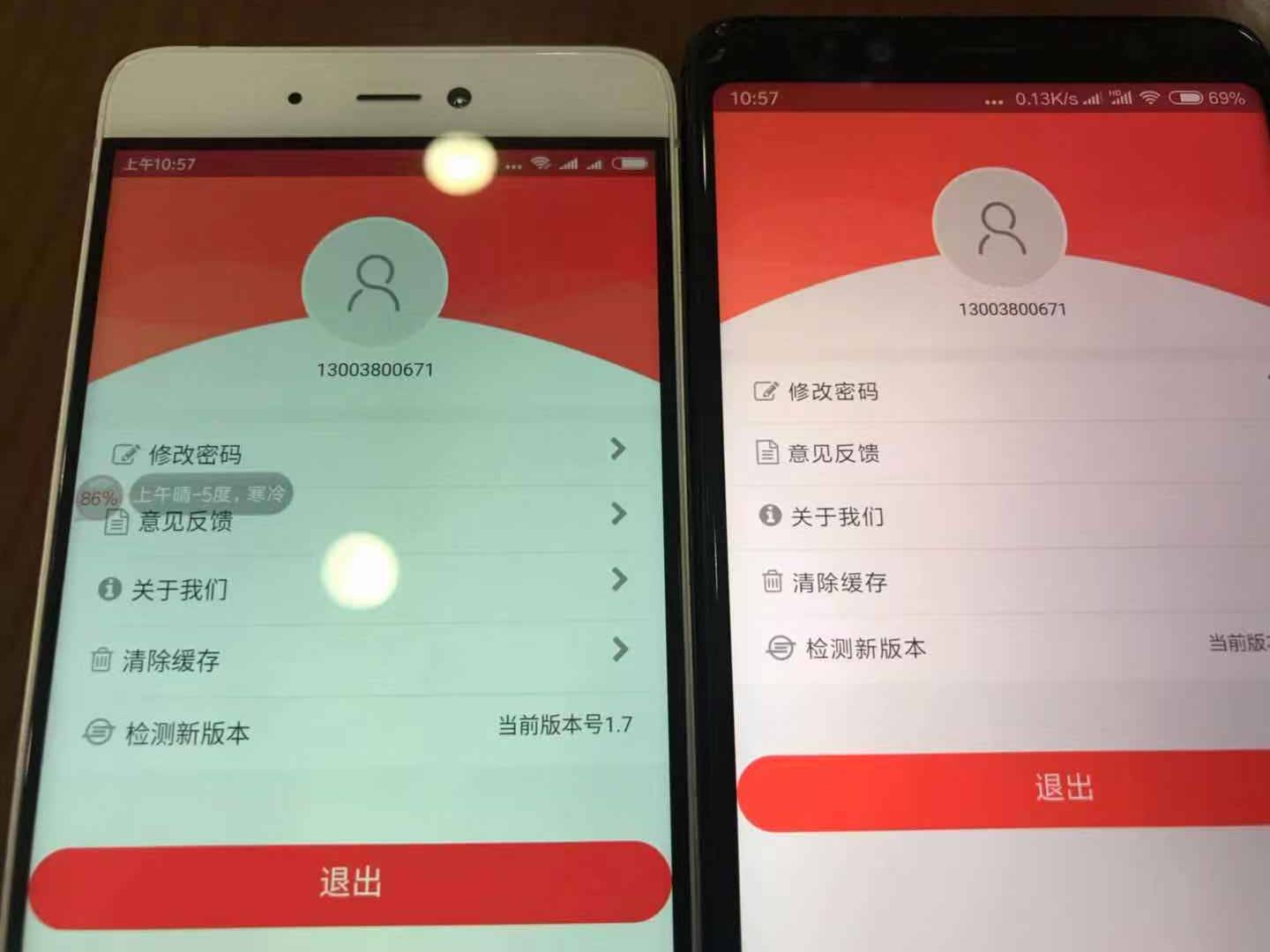
1. 用户真实身份鉴别：该应用采用电话号码+密码、电话号码+短信 两种登陆方式，未强制性采用电话号码+短信的登录方式，无法核对用户的真实身份；
2. 2.2.2-FX-1-1 中存在敏感信息采用明文传输的现象
3. 初评报告业务研判结果出现部分研判结果标注未统一的问题，如：对不涉及的评估意见分别有：不适用、不涉及两种描述。建议对报告内容进行完善统一，加强评估报告的规范性。
4. **复评中新发现的问题：**
5. **业务制度建设存在部分问题**

按照相关管理要求，陕西电信建立了一系列管理办法保障业务安全。该业务平台目前管理制度需按照业务需求，进一步完善相关管理制度，形成制度保障体系。

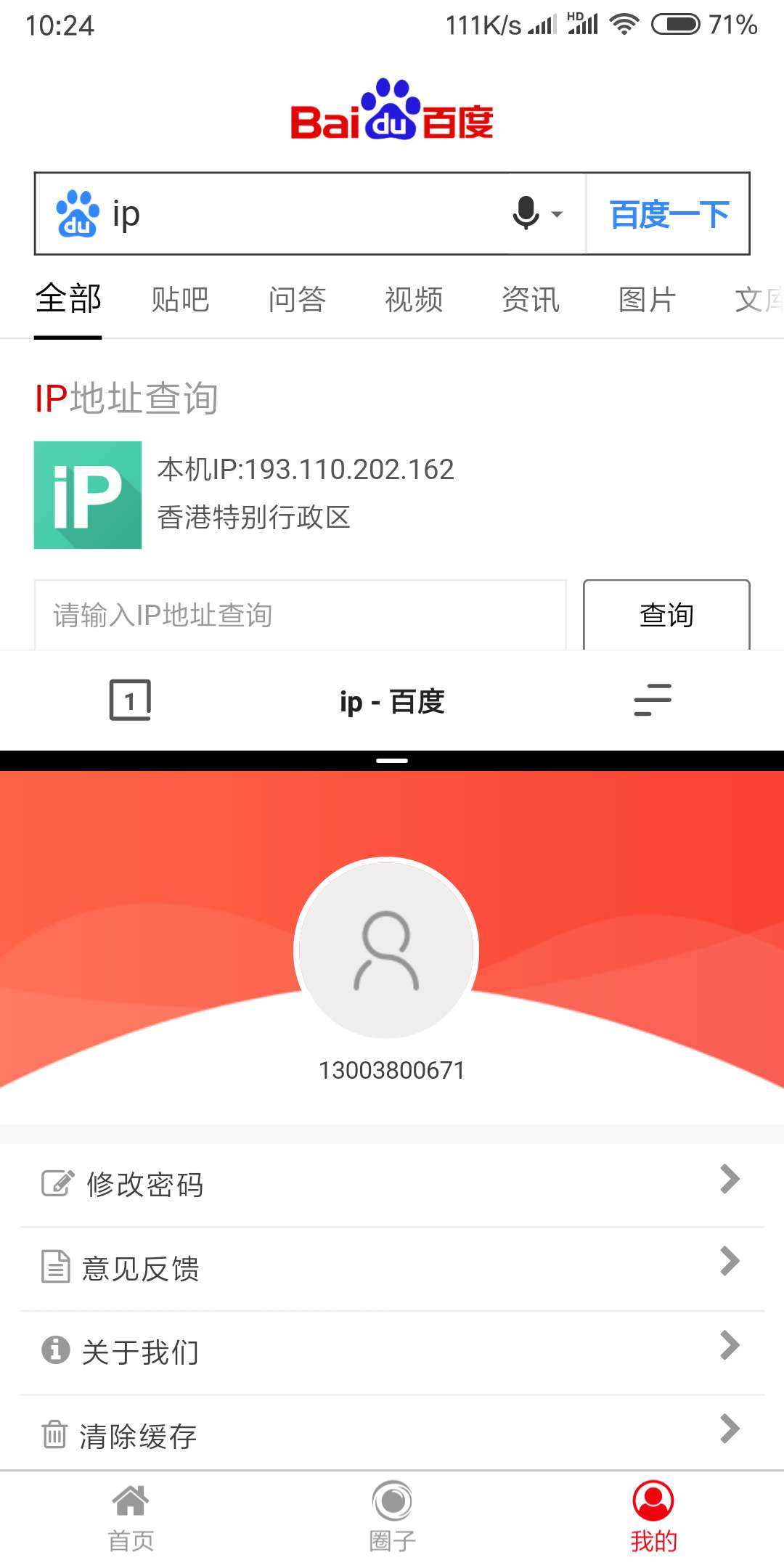
1. **业务保障能力方面，存在部分保障安全风险**

1. **不健全登录机制风险**：**风险程度：高**

* 业务系统存在多点登录风险；



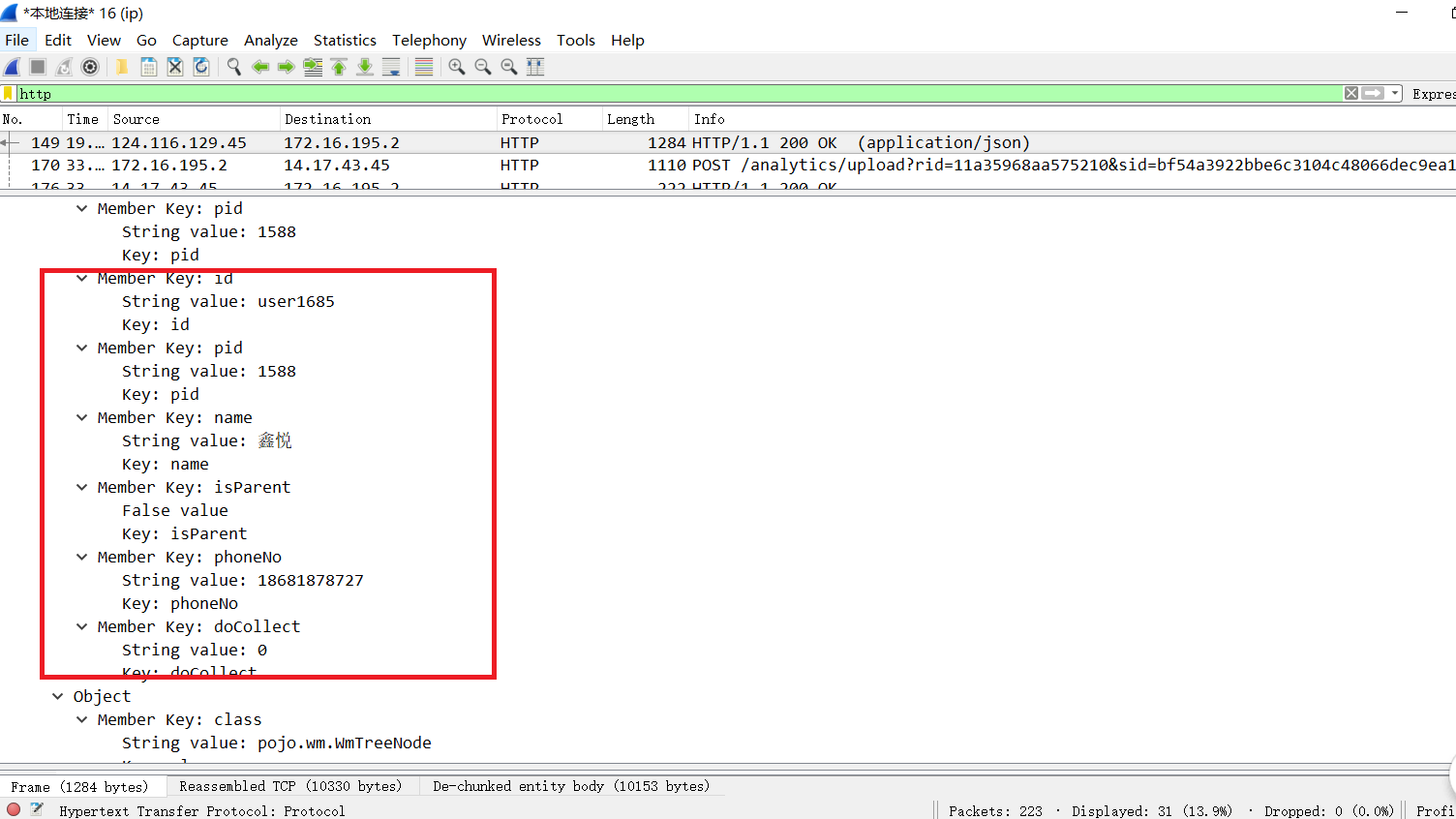
* 异地登录；



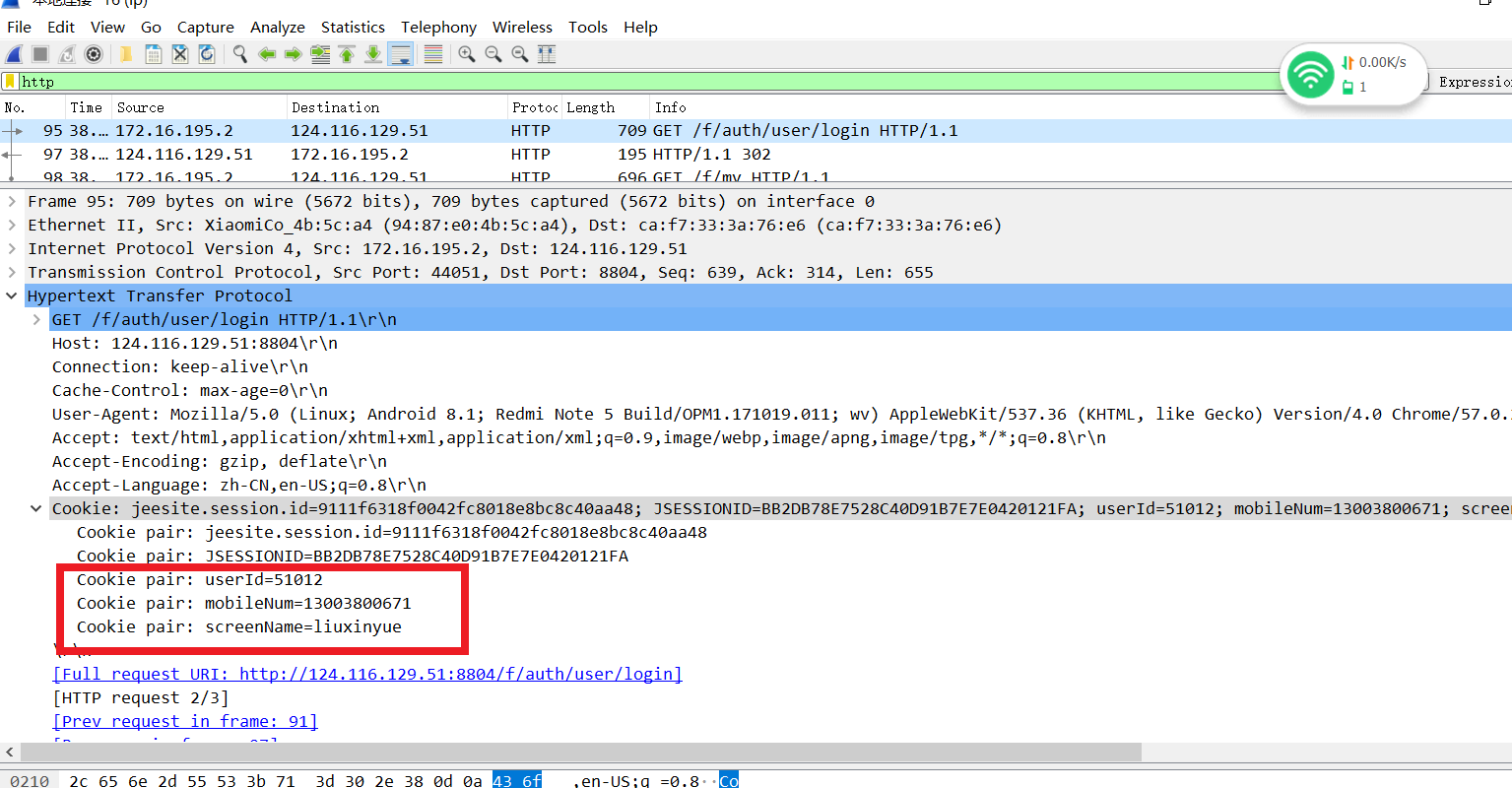
* sessionid未与ip进行绑定

2.**非加密数据传输风险**：**风险程度：高**

* 采用HTTP方式进行数据传输，在通信录模块中明文传输姓名、电话号码等个人信息，存在传输数据被拦截泄露、窃取或篡改，数据传输中断等风险。

****

* 登陆认证后，传输的cookie中存储了用户电话号码、姓名等登录信息。

****