**报告编号： 2016-LNPG-03-0301**

**中国移动集团辽宁分公司聚和适业务系统信息安全评估报告**

**系统名称：　　　　聚和适**

**委托单位：　　辽宁省通信管理局**

国家计算机网络与信息安全管理中心

目录

[一、 概要 3](#_Toc444847530)

[二、 评估目的 3](#_Toc444847531)

[三、 评估内容 3](#_Toc444847532)

[四、 评估依据 4](#_Toc444847533)

[4.1 政策法规依据 4](#_Toc444847534)

[4.2 安全标准 4](#_Toc444847535)

[4.3 评估方式 5](#_Toc444847536)

[五、 评估组组成 5](#_Toc444847537)

[六、 评估时间 5](#_Toc444847538)

[七、 辽宁移动信息安全管理总体情况 6](#_Toc444847539)

[八、 辽宁移动“聚和适”业务信息安全现状 8](#_Toc444847540)

[8.1 “聚和适”业务基本情况 8](#_Toc444847541)

[8.2 “聚和适”业务功能实现技术原理 8](#_Toc444847542)

[8.3 “聚和适”业务相关的信息安全管理和制度建设情况 10](#_Toc444847543)

[8.4 “聚和适”安全保障措施 11](#_Toc444847544)

[九、 “聚和适”业务评估结果 12](#_Toc444847545)

[9.1 “聚和适”业务管理体系评估结果 12](#_Toc444847546)

[9.2 “聚和适”业务安全评估结果 12](#_Toc444847547)

[9.3 “聚和适”业务安全保障能力评估情况 19](#_Toc444847548)

[十、 整改建议 26](#_Toc444847549)

# 概要

2016年1月26日，国家计算机网络与信息安全管理中心对中国移动集团公司辽宁分公司（以下简称辽宁移动）“聚和适”业务开展了信息安全现场评估工作。

此次信息安全评估主要内容包括管理体系评估、业务风险评估和信息安全保障能力评估三个部分。评估方法包括人员访谈、制度核实、业务功能演示、内容安全测试、测试验证、渗透测试等。

本报告主要给出“聚和适”业务的信息安全评估情况。

# 评估目的

为进一步提升辽宁移动新技术新业务的信息安全防护和处置能力，依据新技术新业务信息安全评估相关政策文件，结合通信安全分级保护、风险评估的基本方法和标准，发现并找出新技术新业务相关的管理制度、业务流程、网络系统、服务器以及应用系统等方面存在的安全漏洞和隐患。目的是为企业健全互联网新技术新业务管理制度、完善业务流程、提早启动保障措施、加固系统和网络漏洞提供参考和依据，进而提高业务系统的安全防护水平，为业务的发展创造安全可靠的环境。

# 评估内容

辽宁移动新技术新业务安全评估工作主要涉及管理、业务和信息安全保障等方面的安全因素。管理方面，主要采用访谈调研、相关文件查阅的方式，查找管理方面存在的漏洞；业务方面，主要采用人员访谈、功能演示、业务试用、流程梳理等方式，查找业务方面存在的漏洞或隐患；信息安全保障能力方面，主要通过内容测试、漏洞扫描、渗透测试等手段，查验现有信息安全技术保障措施是否满足基本要求。各方面的评估重点包括：

* 1. 管理体系方面：重点评估辽宁移动对于各新技术新业务的信息安全管理体系和业务安全管理措施是否满足电信管理机构的安全管理要求，具体包括机构设置、管理制度、信息安全相关要求和技术标准以及具体执行情况；
  2. 业务风险方面：评估辽宁移动新技术新业务的完整业务流程，结合业务功能属性及技术实现，包括内容发布审核、业务边界安全、权限管理、用户信息保护等，评估系统潜在的信息安全风险；
  3. 信息安全保障能力方面：评估辽宁移动现有的安全措施、技术手段等信息安全保障能力是否能够有效控制业务信息安全风险。开展内容过滤机制测试；对业务系统、操作系统、网络设备进行安全检测；通过渗透测试查看系统安全防护情况等。
  4. 其他：评估与辽宁移动新技术新业务相关系统的安全性。

# 评估依据

## 4.1 政策法规依据

《基础电信企业信息安全责任管理办法（试行）》

《互联网新技术新业务信息安全评估管理办法（试行）》

《关于开展基础电信企业网络与信息安全责任考核有关工作指导》

《互联网用户账号名称管理规定》

## 4.2 安全标准

《互联网新技术新业务安全评估指南》（征求意见稿）

《电信网和互联网安全防护管理指南》

《电信网和互联网安全风险评估实施指南》

《电信网和互联网灾难备份及恢复实施指南》

《电信网和互联网物理环境安全等级保护要求》

《电信网和互联网物理环境安全等级保护检测要求》

《电信网和互联网管理安全等级保护要求》

《电信网和互联网管理安全等级保护检测要求》

## 4.3 评估方式

本次信息安全评估的主要方式有：人员访谈、文档材料核查、业务功能验证、内容安全测试和安全测评。

人员访谈从被评估方的业务人员和部门领导直接获取企业信息安全管理、业务应用及平台安全、安全保障措施等方面的现状。

文档材料核查主要是指对企业信息安全、业务安全等相关制度的制定情况进行核实。

业务功能验证通过检查业务功能和流程，对业务应用和系统平台潜在的安全风险做出判断。

内容安全测试主要用于评估企业内容安全相关的保障能力，包括违法不良样本的识别检测、传播扩散控制等方面。

安全测评主要针对业务平台安全和数据安全，涉及漏洞分析、渗透测试等技术手段。

# 评估组组成

|  |  |  |
| --- | --- | --- |
| **姓名** | **职称/职务** | **职责** |
| 王红兵 | 首席工程师 | 评估组长 |
| 段东圣 | 工程师 | 评估测试 |
| 毛洪亮 | 工程师 | 评估测试 |
| 杨□帆 | 工程师 | 评估测试 |
| 孙大鹏 | 工程师 | 评估测试 |
| 贾芳淑 | 工程师 | 评估测试 |

# 评估时间

评估时间：2016年1月26日至2016年1月27日

综合数据分析时间：2016年2月1日至2016年2月29日

评估报告生成时间：2016年3月1日

# 辽宁移动信息安全管理总体情况

辽宁移动成立了专门的信息安全管理部门，配备专职人员23人，其中信息安全中心9人，网管中心下属的网络安全室14人，网络安全室主要为信息安全中心做技术支撑。辽宁移动组建了自主评估队伍，包括业务安全评估组、应用安全评估组、网络安全评估组，由信安中心牵头，建立了辽宁移动信息安全评估制度。技术新业务上线前信息安全评估工作，业务运营主体负责组织开展评估。

中国移动辽宁公司制定了较为完善的网络和信息安全管理办法，具体可以分为三层。

第一层管理办法是《中国移动辽宁公司网络和信息安全工作管理办法》，该办法制定了省内网络和信息安全管理工作整体框架，建立了信息安全责任制落实及管理制度。《中国移动辽宁公司网络和信息安全工作管理办法》是辽宁移动网络和信息安全工作的总体要求，对网络和信息安全各项工作进行了定义，对各项工作目标进行了简要叙述。

第二层管理办法是明确了网络和信息安全各项工作的目标、责任分工、工作流程等，共分为5类33个管理办法。第一类是网络和信息安全责任落实相关管理办法，对基础电信企业网络和信息安全责任考核中所需要落实的各项工作进行了明确，具体包括：

《中国移动辽宁公司信息安全责任管理办法》

《中国移动辽宁公司信息安全工作奖励及责任追究管理办法》

《中国移动辽宁公司信息安全工作报备管理办法》

《中国移动辽宁公司信息安全资金保障管理办法》

《中国移动辽宁公司信息安全检查管理办法》

《中国移动辽宁公司信息安全教育培训管理办法》

《中国移动辽宁公司网络安全“三同步”管理办法》

《中国移动辽宁公司第三方安全管理办法》

《中国移动辽宁公司外包和代维服务安全管理办法》

《中国移动辽宁公司业务安全管理办法》

《中国移动辽宁公司信息安全系统维护管理办法》

《中国移动辽宁公司恶意程序防范管理办法》

《中国移动辽宁公司木马、僵尸网络和恶意程序监测与处置管理办法》

第二类是不良信息治理相关管理办法，明确了垃圾短彩信、骚扰电话、伪基站等治理工作要求，对不良信息治理中组织职责、不良信息发现、处置、上报等进行了重点明确，防止不良信息在网内的产生和传播，具体为《中国移动辽宁公司不良信息发现和处置管理办法》。

第三类是客户信息保护相关管理要求，通过树立安全意识、实行合理授权、进行技术管控等措施，规范客户信息访问流程和用户访问权限，降低客户信息被违法使用风险，具体为《中国移动辽宁公司客户信息安全管理办法》。

第四类是合规管理办法，对非涉密网络保密、储存介质、软件、第三方安全、机房安全管理、网络架构安全和网络资产安全管理等方面进行了说明，并对网络运维工作中信息系统授权原则、网络访问控制、数据备份、日志等网络安全工作提出了明确要求，具体包括：

《中国移动辽宁公司非涉密网络保密管理办法》

《中国移动辽宁公司存储介质管理办法》

《中国移动辽宁公司软件安全管理办法》

《中国移动辽宁公司第三方组件安全管理办法》

《中国移动辽宁公司网络架构安全设计管理办法》

《中国移动辽宁公司信息系统维护授权管理办法》

《中国移动辽宁公司信息系统日志管理办法》

《中国移动辽宁公司信息系统账户安全管理办法》

《中国移动辽宁公司网络与系统安全配置管理办法》

《中国移动辽宁公司机房安全防护管理办法》

《中国移动辽宁公司网络访问控制管理办法》

《中国移动辽宁公司数据备份与恢复管理办法》

《中国移动辽宁公司信息系统变更安全管理办法》

《中国移动辽宁公司系统退服安全管理办法》

《中国移动辽宁公司终端安全管理办法》

《中国移动辽宁公司对外网站安全管理办法》

《中国移动辽宁公司网络和信息资产安全管理办法》

第五类是信息安全应急体系建设相关要求，对应急预案的制定、发布、演练、培训和更新等工作进行了明确，具体为《中国移动辽宁公司信息系统应急预案管理办法》。

第三层管理办法属于实施细则范畴，是对第二层管理办法的补充说明，与第二层文档配合使用。

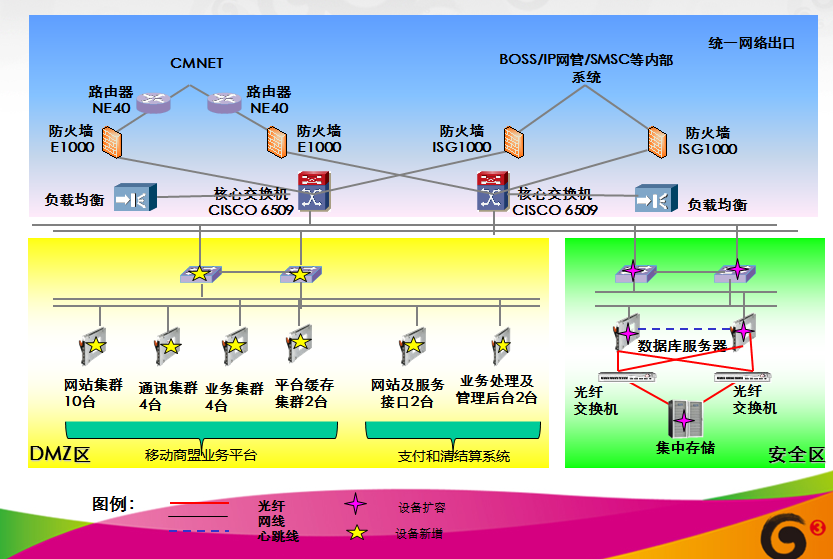
# 辽宁移动“聚和适”业务信息安全现状

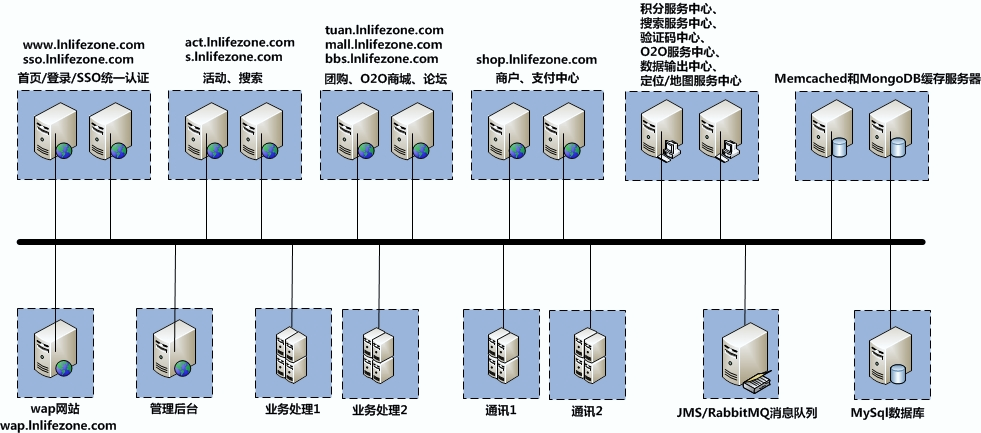
## 8.1 “聚和适”业务基本情况

“聚和适”是中国辽宁移动公司倾力打造的消费类电子商务综合服务平台，旨在成为辽宁地区最大最具权威的生活服务类消费信息指南，结合互联网与无线增值服务的信息传递的即时性和便利性，打造吃、喝、玩、乐、购全方位的互动沟通平台，地址为[www.ln139.com](http://www.ln139.com)。面向用户，聚和适提供信息查询、优惠折扣、用户互动等在内的一站式服务体验。面向商家，聚和适帮助商家达成实现产品电子化，并实现销售环节的流程再造。面向移动，打造一种粘性服务和新的收入增长点，带来客户感知和移动品牌价值的提升。

## 8.2 “聚和适”业务功能实现技术原理

聚和适业务采取典型的**O2O**（Online To Offline）交易模式，商户、商品包装成产品，通过订单串联业务流程，实现一整套下单、支付、下码、消费、结算的电子商务过程。底层架构由三大核心平台组成，外围对接CRM、12580、积分、位置等平台，实现客服支撑、地图展示、二维码机具复用等功能。目前平台主要支付方式为积分支付，月均消耗量在7亿积分左右。为了更好的实现积分消耗平台实现了积分转赠功能以及促销积分派发功能，通过宣传引导及促销活动引导用户进行积分消耗。辽宁移动聚和适平台部署在浑南新业务机房虚拟化平台，业务平台分布在20台虚拟机中，数据库采用无线城市集中数据库，网络拓扑、应用部署情况及业务平台架构如下图所示。





## 8.3 “聚和适”业务相关的信息安全管理和制度建设情况

辽宁移动将电子商务业务，即“聚和适”以及广告发布业务统称为“和生活业务”。为规范“和生活”业务的各项规章制度，促进业务快速健康有序发展，中国移动辽宁公司制定了《“和生活”电子商务业务管理办法》。办法适用于中国移动辽宁公司各市分公司发展“和生活”业务的原则以及对“和生活”商户的管理。在“和生活”电商平台销售商品及有关服务的商户，在“和生活”广告发布平台发布广告的商户应当遵守本办法的规定。

办法确定了各部门的管理职责。市场经营部负责积分业务的统筹管理、制定全年积分生成及使用规划，制定积分兑换总体要求，负责制定消费积分的生成规则及促销积分的使用原则。政企客户部协同市场经营部负责各地市分公司面向政企客户的基于积分、红包、和包电子券派发、二维码等营销活动的审批。审批内容包括但不限于目标客户群选取、派送标准核算、适用商户范围，负责协助广告发布业务运营中的协调沟通工作。数据业务部负责积分业务的日常运营，负责提高客户积分的感知，负责促进客户的积分兑换和积分使用。负责“和生活”电商平台的日常管理维护，管理办法的制定，商户商品审核，营销活动及平台日常运营推广，代理商管理，投诉处理，结算管理，“和生活”电商平台中积分兑换的管理和运营，红包派发、和包电子券派发和二维码支撑等,负责广告产品设计及技术搭建工作。各市分公司负责商户拓展及维系，协议签署、发票收集，商户商品信息录入，活动宣传及部分投诉处理，负责广告发布业务的业务拓展、受理及发票的申领、开具工作。

就“聚和适”业务，在商户管理、电商代理商合作管理、积分兑换、红包及和包电子券管理、支付及清结算管理方面，制定了如下细则：

《“和生活”电子商务业务商户准入资质审核标准》

《“和生活”商户自服务使用手册》

《“和生活”电子商务业务商户商品录入手册》

《“和生活”电子商务业务商户及商品信息上报填写规范》

《“和生活”电子商务业务商户商品信息录入模板》

《“和生活”电子商务业务商品信息管理细则》

《“和生活”电子商务业务商户商品上线相关流程》

《“和生活”电子商务业务代理商管理细则》

《“和生活”电子商务业务积分、红包、和包电子券管理流程》

《“和生活”电子商务业务发票及结算管理实施细则V1.3》。

## 8.4 “聚和适”安全保障措施

前期辽宁移动在“聚和适”的安全防范方面主要参照行业应用支撑中心制定的网络系统安全、主机系统安全、应用系统安全等规章制度，并结合自身业务情况采取了相关安全保障措施，主要包括：

1、制定应急预案：为保证聚和适业务平台的网络与信息安全，增强突发事件的处理能力，辽宁移动制定了聚和适业务平台的专项应急预案。预案适用于负责维护聚和适业务平台的维护组，要求聚和适业务平台专项应急处理工作坚持统一领导、分工负责、及时预警、协作配合、快速处理、确保恢复的原则。网络与信息安全事件处理步骤为按照应急预案要求迅速阻断攻击源，恢复系统正常运行，确保信息内容不被篡改；捕获所有可用信息并备份有关计算机设备；及时通知相关人员和涉及用户；调出所有相关技术文档（安装配置文档、升级更新记录、相关网络配置文档、数据备份记录等）、登记记录以及数据和系统备份；限制受影响的范围，阻止损害进一步扩大；同时继续实行监控并检查冗余数据和系统是否受到同样影响。根据实际情况使用下列手段；消除影响并实行紧急损害恢复。

2、安全事件响应：接到相关部门通报、用户投诉举报的内容违规事件后，应迅速启动应急预案，对违规行为进行核实、处置。已构成业务内容安全事件的，业务运营单位应立即中止其接入，在限定时间内完成整改并提供书面整改报告，进行违规信息取证。

3、人员及权限管理：按照“职责分离、最小化授权”的原则，要求各职能人员权限隔离，业务内容制作、内容审核、内容发送、数据维护、客户信息管理人员等应相互分离，各人之间权限不得重叠。内容制作者和内容审核者负责内容制作、修改和审核，对审核后的内容进行修改的，需由制作和审核人员共同修改确认。内容发送权限者负责将终审后的内容从平台发出，同时不得被分配内容制作和修改权限。内容记录权限者负责对发布内容的来源记录，并保留来源证据。业务运营部门对于发布信息的账号、权限应做好申请、审批管理，一个帐号对应一个用户，并赋予相应的角色权限，严格控制账号使用范围。

# “聚和适”业务评估结果

## 9.1 “聚和适”业务管理体系评估结果

辽宁移动成立了专门的信息安全管理部门，配备专职人员23人，其中信息安全中心9人，网管中心下属的网络安全室14人，网络安全室主要为信息安全中心做技术支撑。

辽宁移动制定了网络与信息安全管理办法、信息安全责任管理办法、信息安全应急预案等一系列网络与信息安全管理制度。2015年对23个业务进行了自评估并已向管局报备，评估报告涵盖了信息内容安全方面的内容。

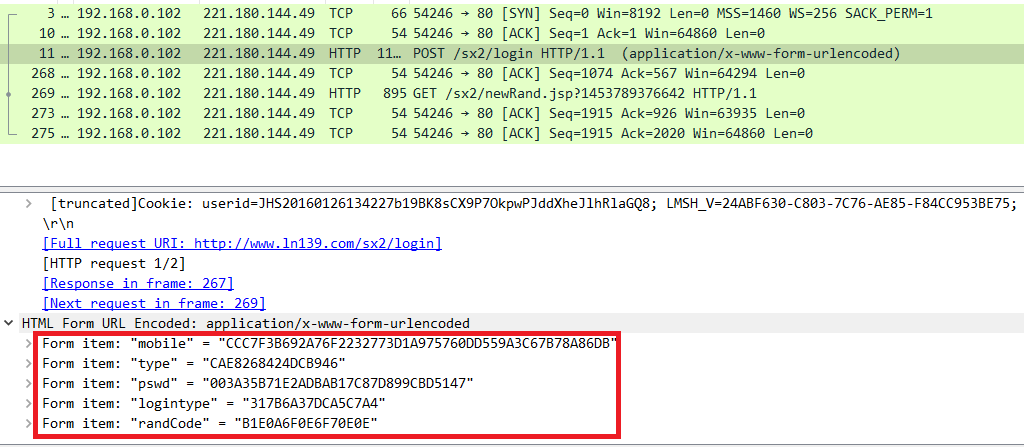
总体上，辽宁移动在网络与信息安全机构设置、人员力量配备，以及管理制度建设等方面基本满足当前的信息安全管理要求，建议辽宁移动后期继续加强安全管理方面的制度建设，根据实际业务的发展情况对网络与信息安全管理方面的制度进行修订，更好的适应业务发展带来的新问题。

## 9.2 “聚和适”业务安全评估结果

1、聚和适业务只支持辽宁移动用户使用，通过手机验证方式即可登录系统，无需用户其他信息，业务后端只有用户的手机信息，需要与网厅对接才能得到姓名、身份证等更多的用户实名信息，建议聚和适业务与网厅服务部门建立工作机制，在相关部门需要调取用户实名信息时能够及时获取用户的准确信息。

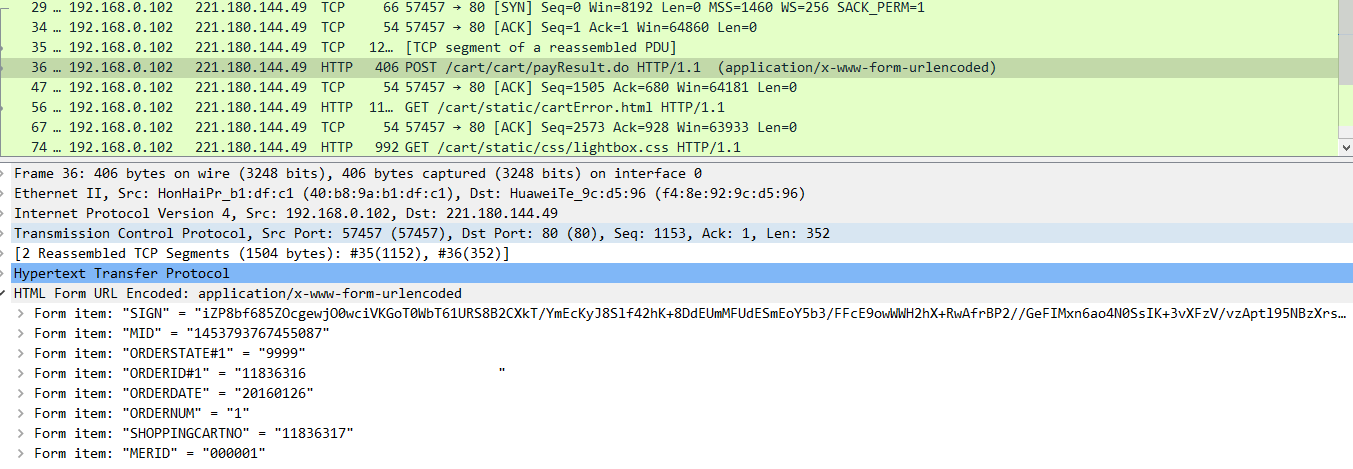


2、在用户登录过程中，聚和适业务对用户的手机号、短信随机码等信息进行了较为严格的加密，保障了用户信息的安全。



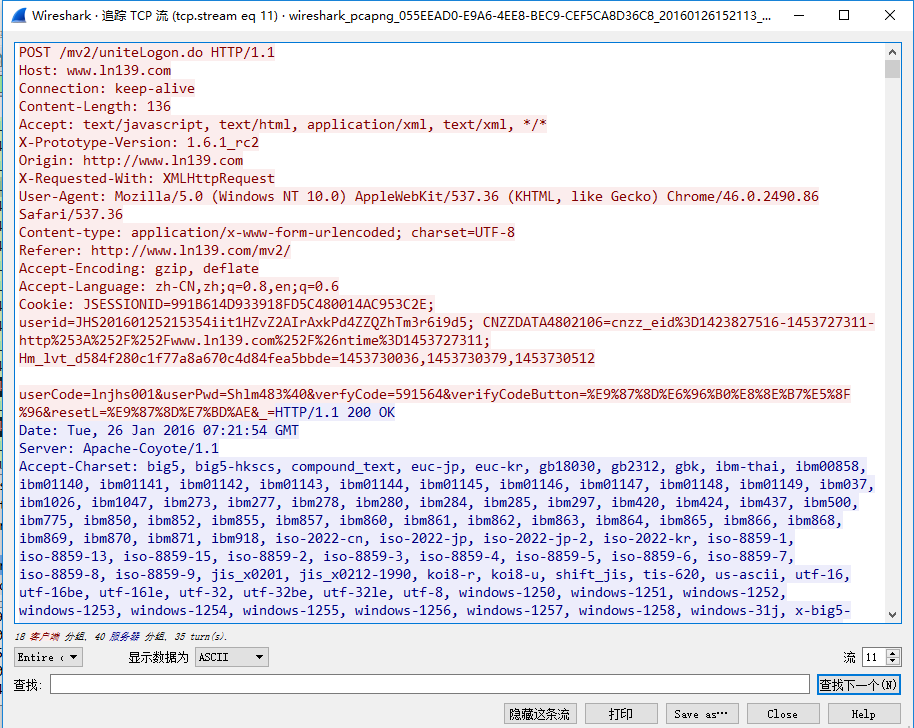
3、用户在聚和适平台购买商品的支付环节中，聚和适业务对用户输入的服务密码进行了严格的加密，保证了用户服务密码的安全。



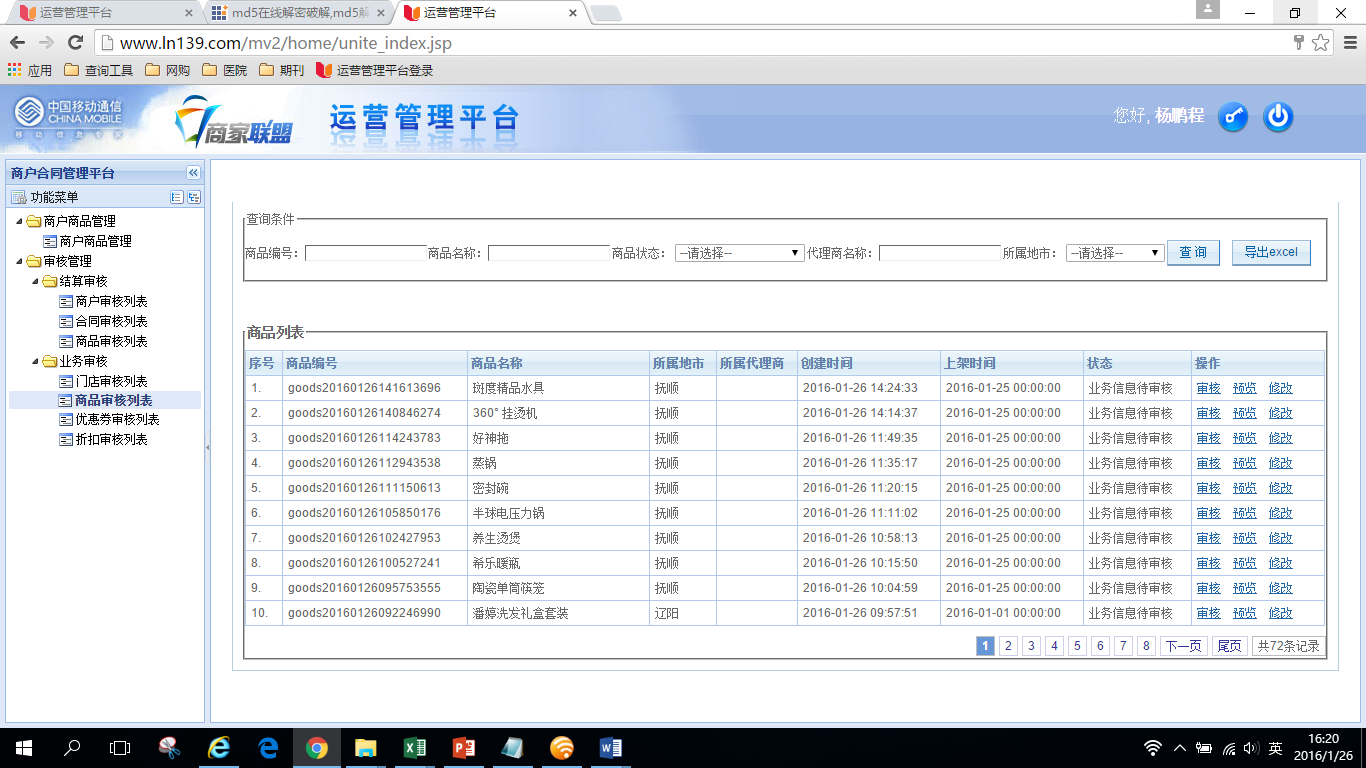


4、聚和适用户登录密码及后台管理系统密码均为明文传输，建议对密码等敏感数据进行加密后再专输或通过HTTPS方面对Web页面进行整体加密传输。

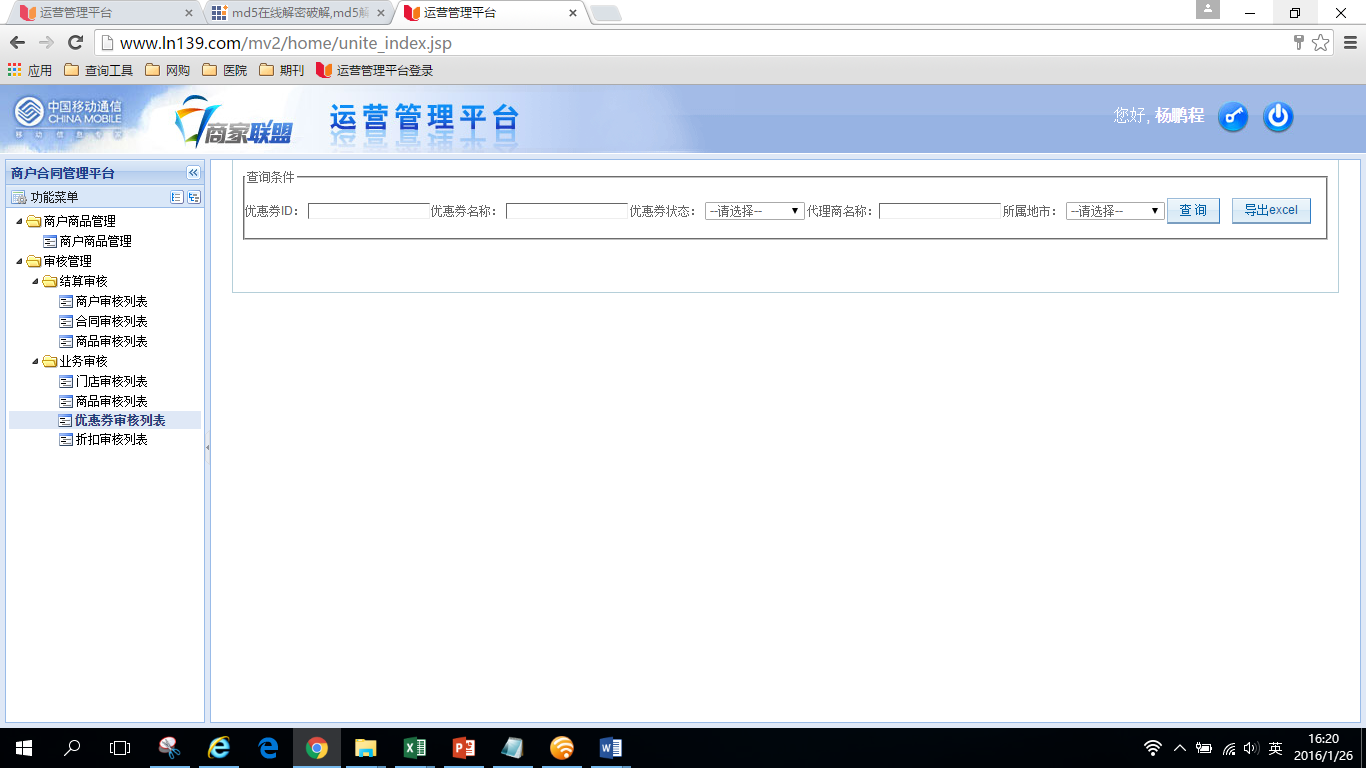




5、聚和适商品、优惠券、折扣需经过发布、结算审核、业务审核等环节才能正式生效，并且发布与审核权限由不同类型的管理账号进行操作，实现了发布与审核功能权限的分离，并且商品信息修改后还需要进行再次审核，信息的发布到生效的流程基本符合信息安全管理要求，建议辽宁移动加强对管理用户权限的管理，确保发布与审核权限对应于不同的管理账号，并且在物理上对应不同的人员，同时加强对相关管理人员的信息安全培训教育，制定相应的培训计划。



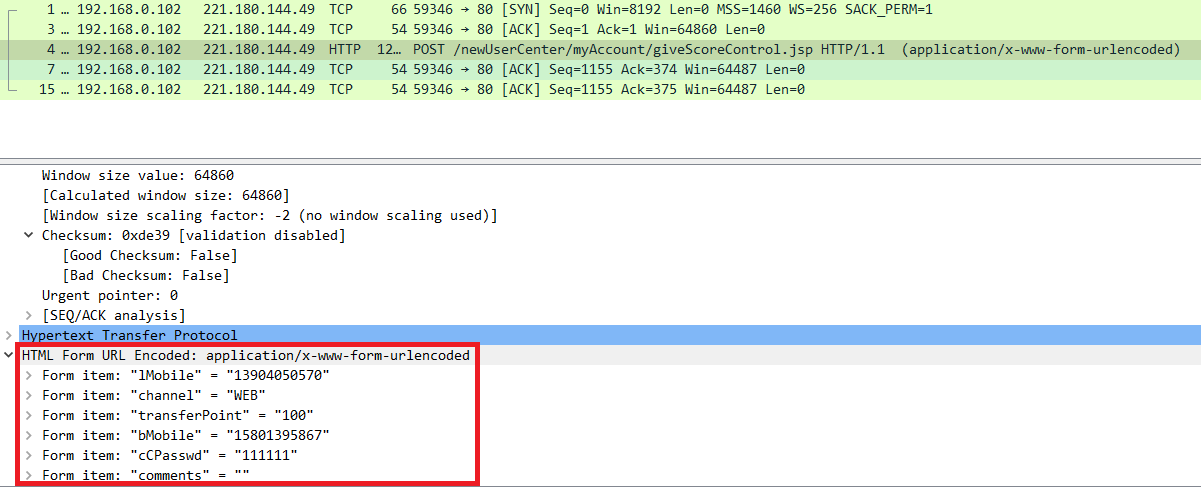






6、聚和适业务提供积分转赠功能，即用户可将积分转赠给其他人。用户在登录后输入要转赠的用户手机号，转赠的积分数额，并输入手机服务密码即可转赠。该部分存在的问题在于用户的服务密码及双方手机号均为明文传输，存在巨大的服务密码泄露的风险。由于手机服务密码是用户极其重要的信息，建议对用户手机号和服务密码进行加密传输，降低用户重要信息被泄露和破解的风险。





7、用户个人信息设置部分，系统对用户的昵称及头像不进行审核和限制，用户可上传敏感及有害信息作为头像。依据《互联网用户账号名称管理规定》的相关要求，互联网信息服务提供者应当落实安全管理责任，完善用户服务协议，明示互联网信息服务使用者在账号名称、头像和简介等注册信息中不得出现违法和不良信息，对互联网用户提交的账号名称、头像和简介等注册信息进行审核，对含有违法和不良信息的，不予注册。建议依据相关规定增加说明信息和审核机制。



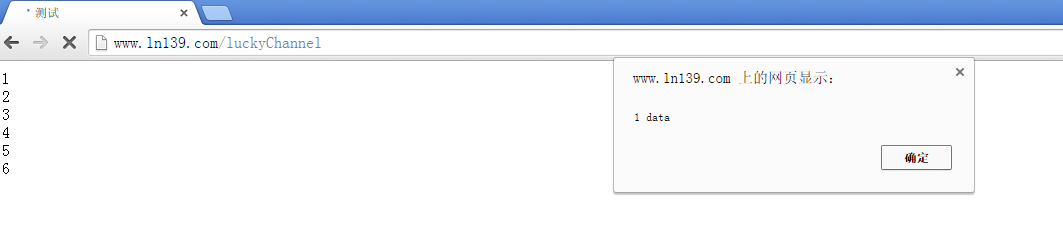
8、聚和适提供商品检索功能，在检索的过程中，没有对检索词进行限制和审核过滤。建议增加检索关键词过滤功能。



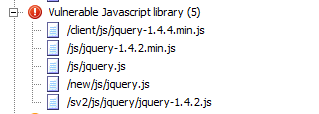
## 9.3 “聚和适”业务安全保障能力评估情况

1、聚和适页面http://www.ln139.com/luckyChannel具有Session固定攻击漏洞，攻击者可直接利用页面的Session信息，建议修复该漏洞，如果上述页面为测试页面，则直接将其从服务器上删除。

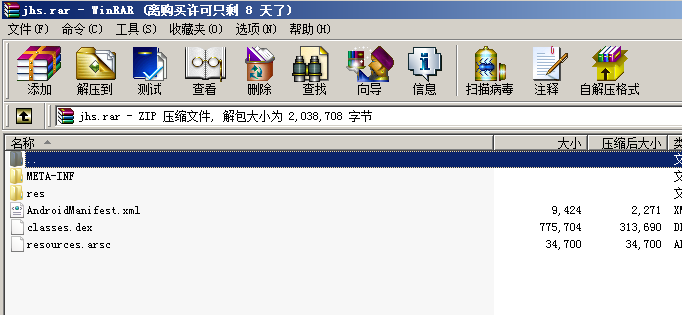


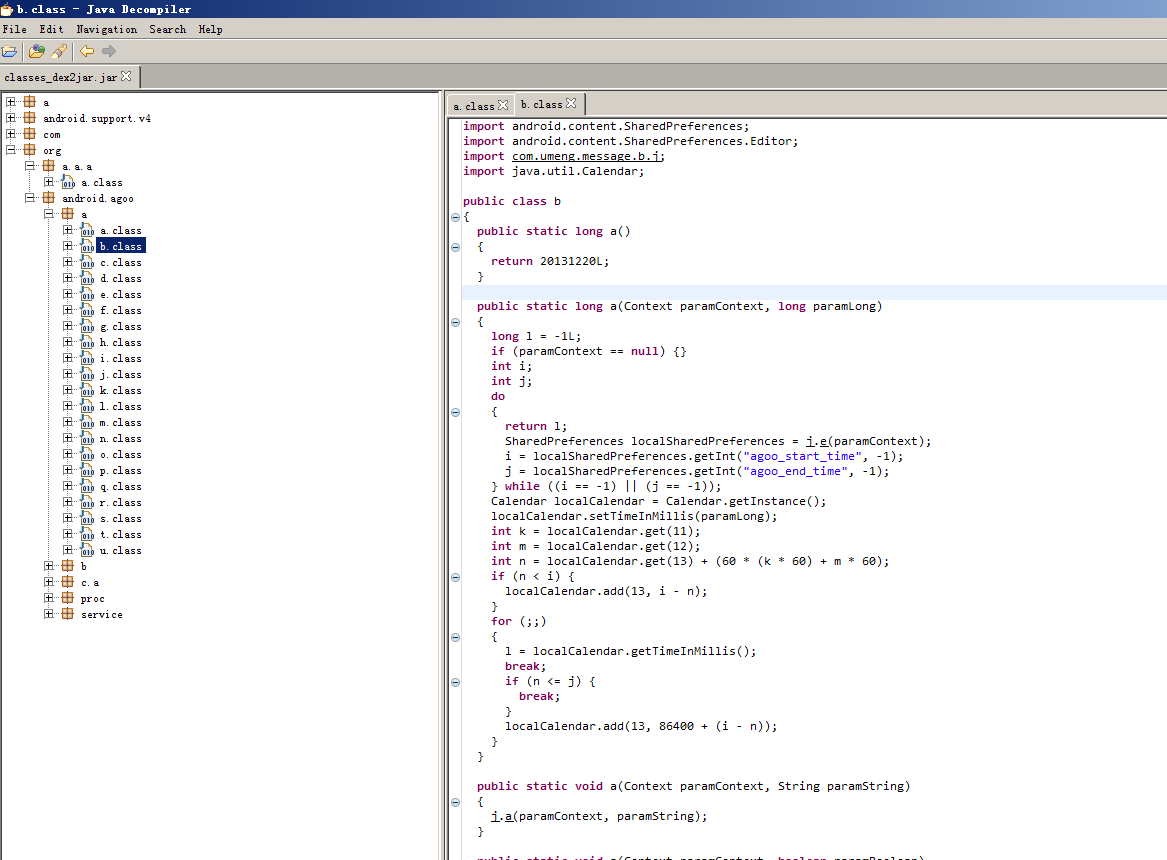


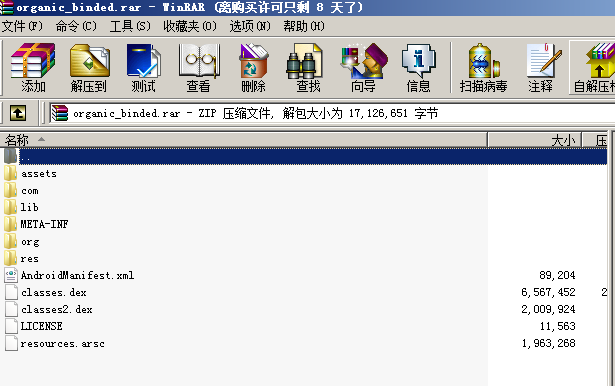
2、聚和适Web的JavaScript的jQuery使用的老版本jQuery1.4.2，但在jQuery 1.6.3之前版本中存在跨站脚本漏洞，当使用location.hash选择元素时，通过特制的标签，远程攻击者利用该漏洞注入任意web脚本或HTML，如果该站点如果没有调用location.hash，则无该漏洞，由于jQuery1.4是五年前的老版本，其功能和安全性都有优待提高，因此建议将jQuery升级到最新版本。

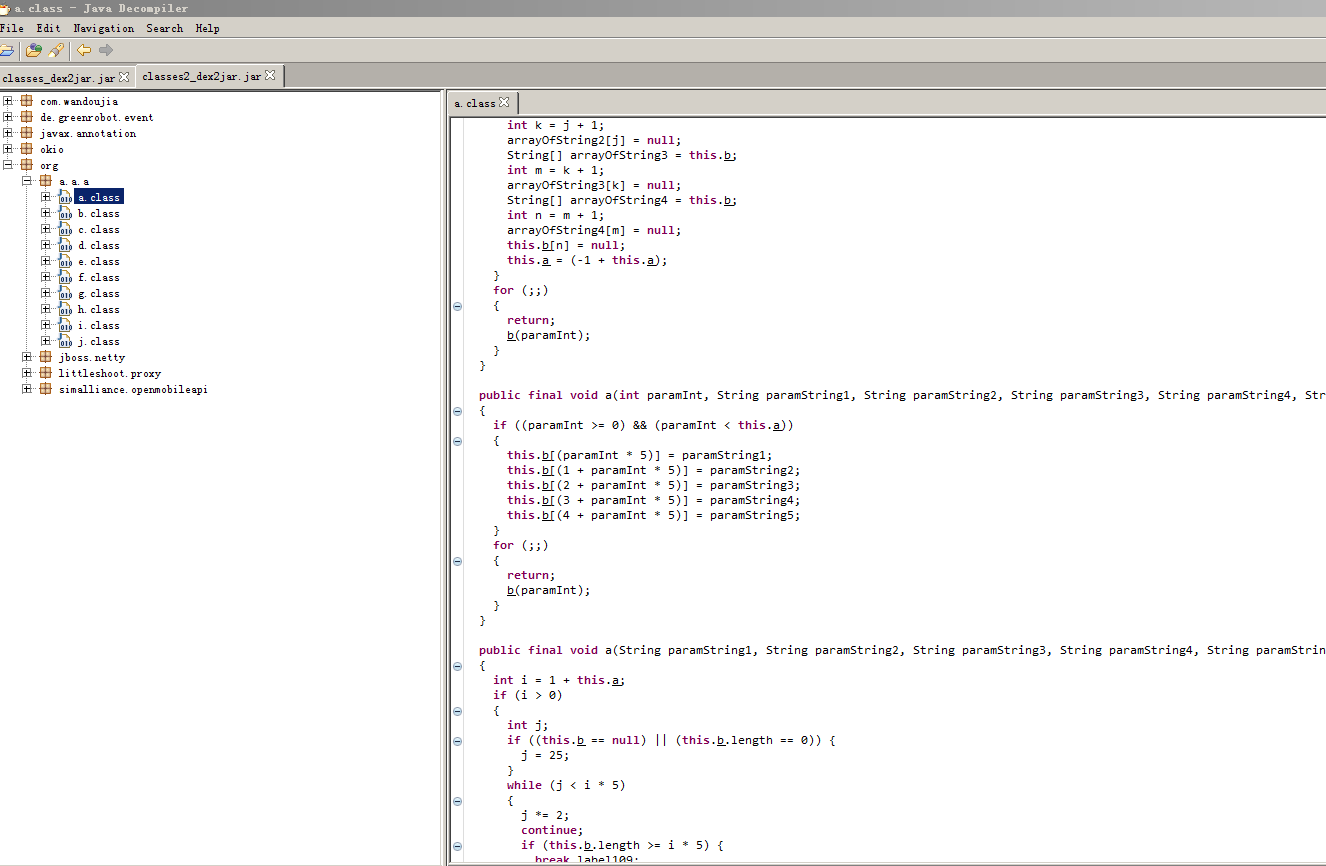


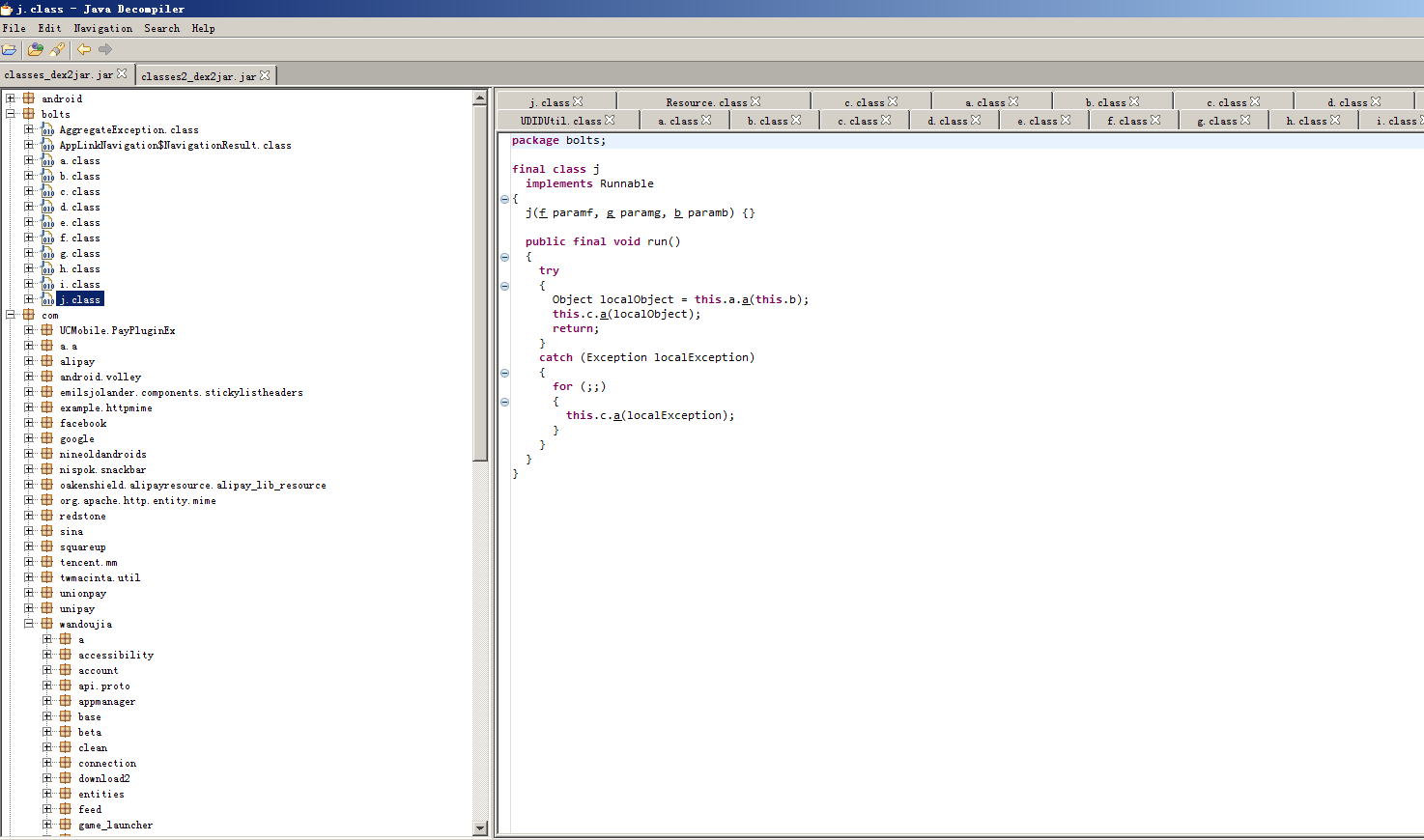
3、[加密不严的Android](file:///C:\\ProgramData\\Acunetix%20WVS%2010\\Data\\Reporter\\SummaryReportItemsTemp.xml" \l "open_new_window_http://blog.gdssecurity.com/labs/2015/3/30/weblogic-ssrf-and-xss-cve-2014-4241-cve-2014-4210-cve-2014-4.html" \o "http://blog.gdssecurity.com/labs/2015/3/30/weblogic-ssrf-and-xss-cve-2014-4241-cve-2014-4210-cve-2014-4.html) APK源码，只对函数及变量名称进行了混淆处理，但不影响攻击者阅读代码，建议更改加密方式。







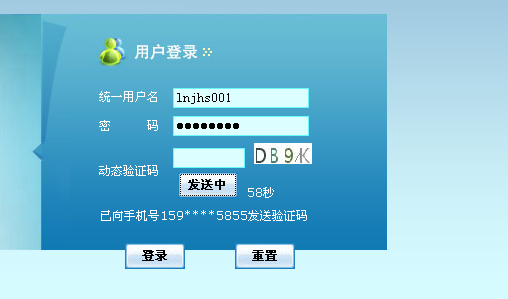


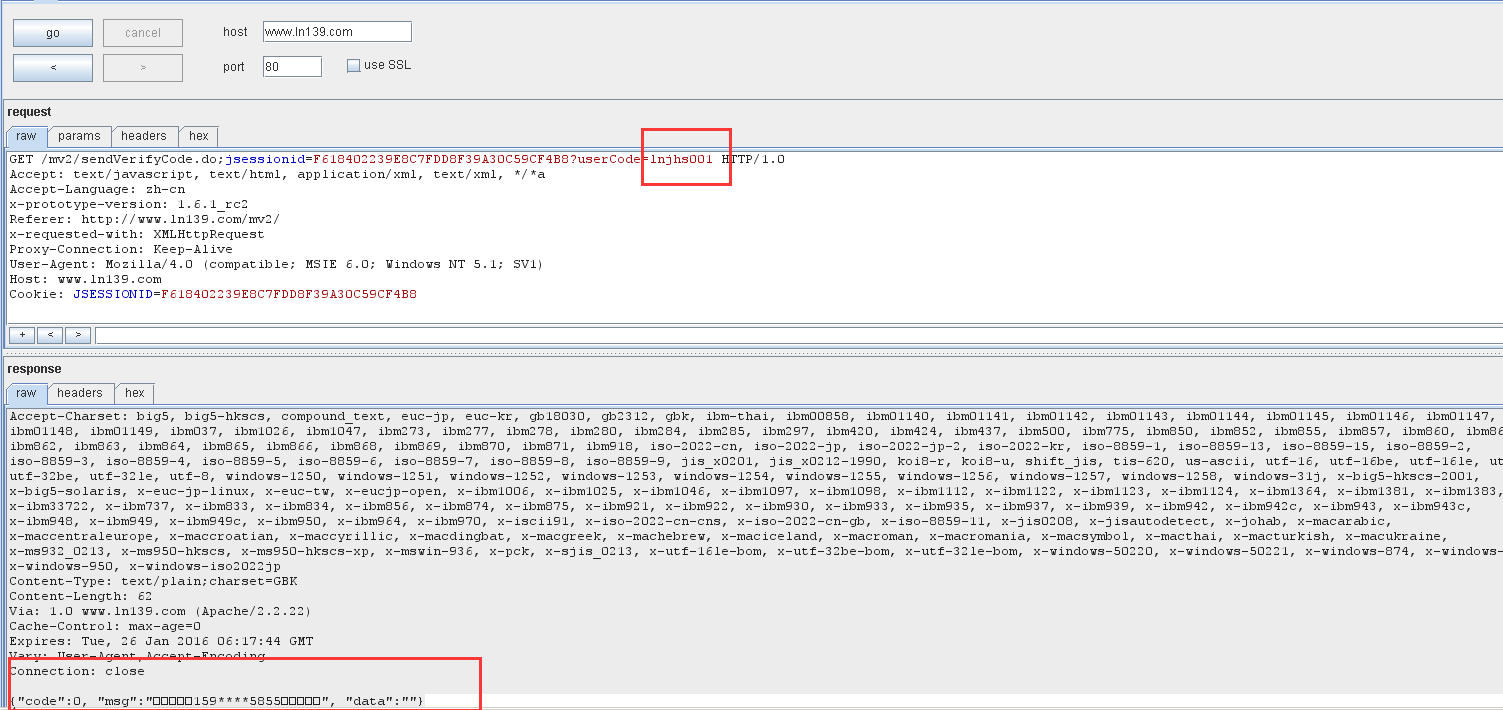


4、页面http://www.ln139.com/sv2/login.do登录缺少验证码及错误次数限制，登录认证方式有待加强，建议增加验证码机制，并增加错误次数限制，当密码错误达到次数时延时登录。



5、后台管理系统<http://www.ln139.com/mv2/>存在短信息重放漏洞，点击登录后，发送账号至数据后台，后台发送短信，只在前台对短信发送次数进行了发送控制，并未在后台进行次数限制,增加后台短信发送控制。





6、发现“辽宁移动聚和适（ln139\_ydsm）”微信账号，但访谈时业务人员不知道该账号是否属于聚和适官方账号，建议辽宁移动对相关账号进行核实，如不是官方账号向腾讯提起申诉，要求关闭。







# 整改建议

业务管理体系方面，辽宁移动基本满足当前的信息安全管理要求，建议辽宁移动后期继续加强安全管理方面的制度建设，根据实际业务的发展情况对网络与信息安全管理方面的制度进行修订，更好的适应业务发展带来的新问题。

业务安全方面，有如下建议。

* 针对聚和适业务后端只有用户的手机信息的问题，建议与网厅服务部门建立工作机制，在相关部门需要调取用户实名信息时能够及时获取用户的准确信息
* 针对聚和适后台管理系统密码明文传输的问题，建议对密码等敏感数据进行加密后再专输或通过HTTPS方面对Web页面进行整体加密传输
* 信息发布审核方面，建议辽宁移动继续加强对管理用户权限的管理，确保发布与审核权限对应于不同的管理账号，并且在物理上对应不同的人员，同时加强对相关管理人员的信息安全培训教育，制定相应的培训计划。
* 针对积分转赠环节用户的服务密码及双方手机号均为明文传输的问题，，建议对用户手机号和服务密码进行加密传输，降低用户重要信息被泄露和破解的风险。
* 用户个人信息设置部分，建议依据《互联网用户账号名称管理规定》的相关要求，增加说明信息和审核机制。

业务安全保障能力方面，建议如下。

* 针对Session固定攻击漏洞问题，建议及时修复或删除测试页面。
* 针对老版本jQuery1.4.2的跨站脚本漏洞问题，建议升级jQuery版本到最新版本。
* 针对[Android](file:///C:\ProgramData\Acunetix%20WVS%2010\Data\Reporter\SummaryReportItemsTemp.xml#open_new_window_http://blog.gdssecurity.com/labs/2015/3/30/weblogic-ssrf-and-xss-cve-2014-4241-cve-2014-4210-cve-2014-4.html) APK源码加密不严的问题，建议更改加密方式。
* 针对登录缺少验证码及错误次数限制的问题，建议加强登录认证方式，增加验证码机制，并增加错误次数限制，当密码错误达到次数时延时登录。
* 针对后台管理系统的短信息重放漏洞，建议增加后台短信发送控制。
* 针对聚和适业务微信账号的问题，建议辽宁移动对相关账号进行核实，如不是官方账号向腾讯提起申诉，要求关闭。