**报告编号：**

**中国联通集团公司辽宁省分公司人人通**

**业务系统信息安全评估报告**

**系统名称：　　　　人人通**

**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](#_Toc462735981)

[二、 评估目的 3](#_Toc462735982)

[三、 评估内容 3](#_Toc462735983)

[四、 评估依据 4](#_Toc462735984)

[4.1 政策法规依据 4](#_Toc462735985)

[4.2 安全标准 4](#_Toc462735986)

[4.3 评估方式 5](#_Toc462735987)

[五、 评估组组成 5](#_Toc462735988)

[六、 评估时间 6](#_Toc462735989)

[七、 辽宁联通信息安全管理总体情况 6](#_Toc462735990)

[八、 辽宁联通“人人通”业务信息安全现状 6](#_Toc462735991)

[8.1 “人人通”业务基本情况 6](#_Toc462735992)

[8.2 “人人通”业务功能实现技术原理 7](#_Toc462735993)

[8.3 “人人通”业务相关的信息安全管理和制度建设情况 8](#_Toc462735994)

[8.4 “人人通”安全保障措施 8](#_Toc462735995)

[九、 “人人通”业务评估结果 9](#_Toc462735996)

[9.1 “人人通”业务管理体系评估结果 9](#_Toc462735997)

[9.2 “人人通”业务安全评估结果 9](#_Toc462735998)

[9.3 “人人通”业务安全保障能力评估情况 11](#_Toc462735999)

[十、 整改建议 14](#_Toc462736000)

# 概要

2016年8月9日至10日，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集团有限公司辽宁省分公司（以下简称辽宁联通）“人人通”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“人人通”业务的信息安全评估情况。

# 评估目的

为进一步提升辽宁联通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

辽宁联通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：重点评估辽宁联通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：评估辽宁联通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：评估辽宁联通现有的安全措施、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：评估与辽宁联通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 |
| 程 光 | 工程师 | 评估测试 |
| 钮 艳 | 工程师 | 评估测试 |
| 马宏远 | 工程师 | 评估测试 |
| 贾 恺 | 工程师 | 评估测试 |
| 张 辉 | 工程师 | 评估测试 |
| 高陆云 | 工程师 | 评估测试 |
| 郑晓天 | 工程师 | 评估测试 |
| 贾芳姝 | 工程师 | 评估测试 |

# 评估时间

评估时间：2016年8月9日至2016年8月10日

综合数据分析时间：2016年8月15日至2016年9月23日

评估报告生成时间：2016年9月26日

# 辽宁联通信息安全管理总体情况

辽宁联通公司已成立“信息安全部”，配备了与业务规模相适应的专职信息安全与网络安全管理人员15名。省公司集团客户事业部、市场营销部、产品创新部、电子商务部、信息导航业务中心、网络公司网络建设部、网络公司运行维护部、各市分公司市场营销部各配置1名专职信息安全管理人员。

辽宁联通组建了“新技术新业务信息安全评估工作组”，由信息安全部作为牵头部门，成员单位有产品创新部、市场营销部、网络公司运行维护部、信息化事业部、客户服务部、监管事务部等部门，负责公司的新技术、新业务信息的安全评估工作。

辽宁联通制定了若干网络和信息安全管理办法，包括：

《辽宁联通互联网新技术新业务信息安全责任承诺书》

《辽宁联通新技术新业务信息安全评估管理办法》

《辽宁联通信息安全责任管理办法（2013年修订版）》

《辽宁联通信息安全保障应急预案（修订）》

# 辽宁联通“人人通”业务信息安全现状

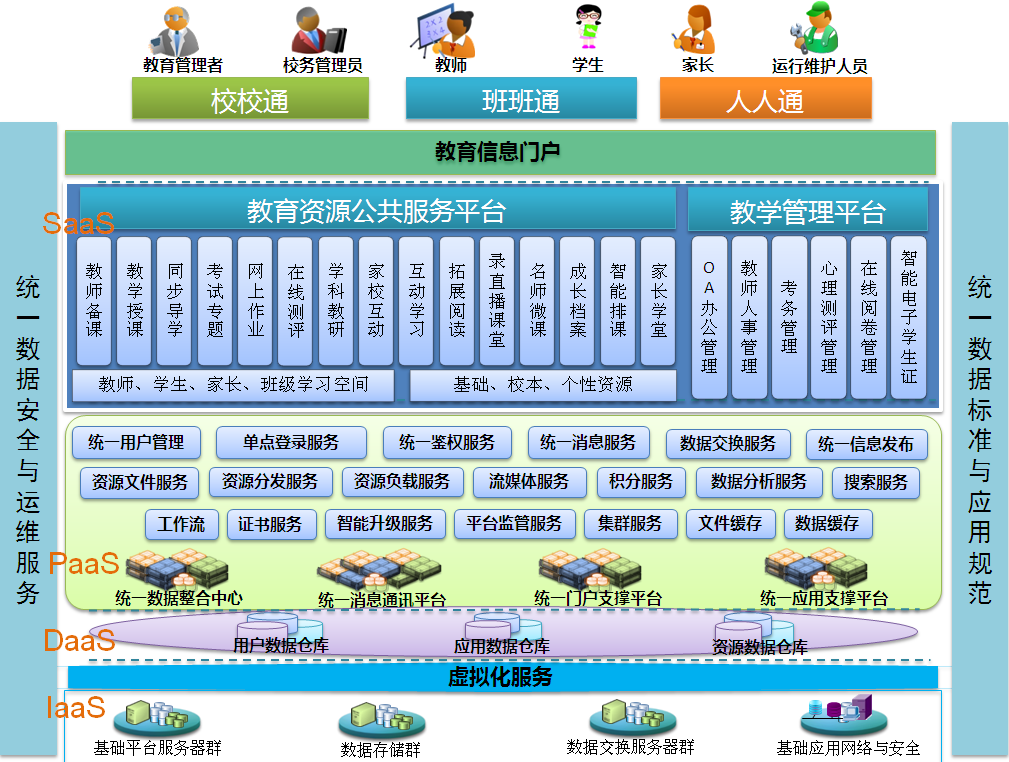
## 8.1 “人人通”业务基本情况

“人人通”业务是中国联通集团公司全国战略落地项目，是以辽宁省教育资源公共服务平台资源为基础，通过多媒体教室、PC、手机、平板等多平台互联网设备，提供教师、学生、家长连接的综合性网络服务。家长、学生可通过手机、平板、电脑等方式，访问教育资源平台，使得家长能及时了解学生学习及作业情况，并对学生进行辅导，学生可网上完成作业并根据老师要求进行课前预习及复习。“人人通”业务为教师提供同步备课、同步导学、网上作业、考试专题、家校互动、课外阅读、学科教研等应用；为学生提供同步学习、互动学习、周练周总结、课外阅读、名师周讲、名师周答、学习加油站等应用；为家长提供同步辅学、家校互动、家长学堂等应用，为班级提供班级圈等应用。

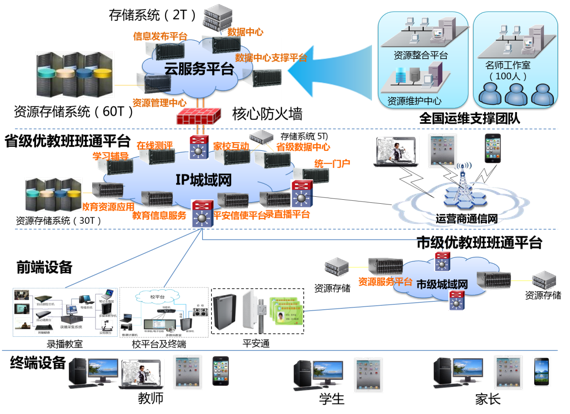
## 8.2 “人人通”业务功能实现技术原理

辽宁教育资源公共服务平台采用虚拟化技术，使教育的多种应用共享服务器、存储等硬件资源，可以帮助用户提升IT基础设施资源的利用效率，提升基础设施的应用和管理水平，实现计算资源的动态优化，使平台应用易维护、易扩充。

在逻辑架构上，整个云平台的应用框架主要由基础设施（IaaS）、数据及资源存储管理层（DaaS）、基础服务层（PaaS）、业务应用层（SaaS）等构成。

****

在网络架构上，辽宁教育资源公共服务平台部署在联通运营商省、市公司IDC机房信息中心机房中，采用一组多台高性能刀片服务器及阵列柜组成硬件平台。辽宁教育资源公共服务平台包括全国运营支撑云资源服务平台、省级集群云平台、市级服务平台、校级服务平台4级平台。



## 8.3 “人人通”业务相关的信息安全管理和制度建设情况

辽宁联通公司未针对“人人通”业务在安全防范方面制定专门的制度性文件，也没有制定专门的业务应急预案。

“人人通”业务系统由郑州威科姆科技股份有限公司开发，辽宁联通公司与威科姆签订了信息安全承诺书，与业务人员签订有保密协议，对运维人员有保密要求。

## 8.4 “人人通”安全保障措施

辽宁联通公司未针对“人人通”业务在安全防范方面制定专门的制度性文件，公司在总体上从日常安全管理和应急管理方面采取了若干保障措施：

日常安全管理方面，网络安全防护措施主要由系统前端部署的2台综合安全网关设备实现，所有访问优教通平台的数据包都要经过安全设备的IPS过滤器，当发现有网络安全隐患时，IPS会阻断恶意访问，保护系统；业务内容安全主要依靠人工审核机制，由审核团队对每日更新内容进行抽帧、全内容观看两种方式审核，保证平台内容的安全性。为保证运维工作有序、正常地开展，还制定了针对运维人员出入管理、设备环境管理、数据保密与备份、计算机病毒防范方面的规范条款。

应急管理措施方面，侧重于网络安全方面内容，如发现系统漏洞时，及时进行版本升级或安装补丁；发现系统病毒时，及时对病毒源端口进行关闭，封锁病毒源IP地址，隔离病毒源文件；必要时使用系统备份对平台系统进行选择性恢复；出现重大事件时，在1小时内进行紧急屏蔽，2小时内资源下线。

# “人人通”业务评估结果

## 9.1 “人人通”业务管理体系评估结果

辽宁联通公司已成立“信息安全部”，配备了与业务规模相适应的专职信息安全与网络安全管理人员15名。辽宁联通制定了信息安全责任管理办法、信息安全保障应急预案等网络与信息安全管理制度。按工信部要求上报了信息安全评估清单，并按要求开展了自评估工作。

总体上，辽宁联通在网络与信息安全管理机构设置和人员配备方面基本满足信息安全管理要求；在管理制度建设方面，缺少针对合作企业、外部人员的安全管理相关的制度性文件或条款，建议信息安全部门牵头制定针对合作企业、外部人员的管理要求和规范，对业务部门提出明确要求，或者在信息安全责任管理办法中增加对合作企业、外部人员信息安全管理相关条款；在自评估工作方面，自评估报告中仅提供了最终的评估结论，没有给出具体的信息安全风险点分析及整改措施，建议对自评估报告中的评估结果部分进行细化，分析业务具体的功能点及信息安全风险点，并提出整改措施建议；在信息安全培训方面，未见到业务人员参加网络与信息安全方面培训的相关证明资料，建议加强对公司全员的的网络信息安全培训，提升全员网络信息安全责任主体意识。

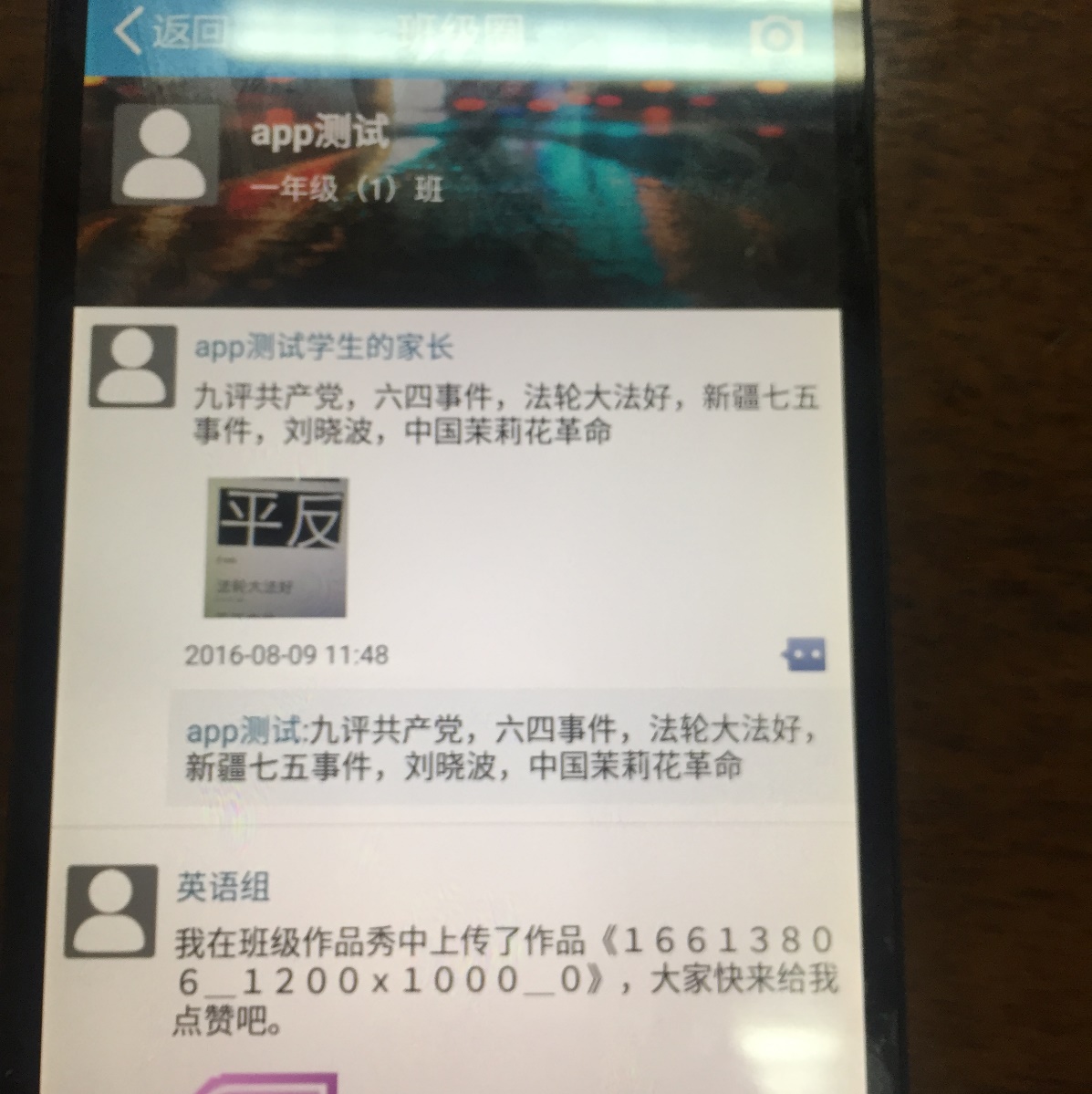
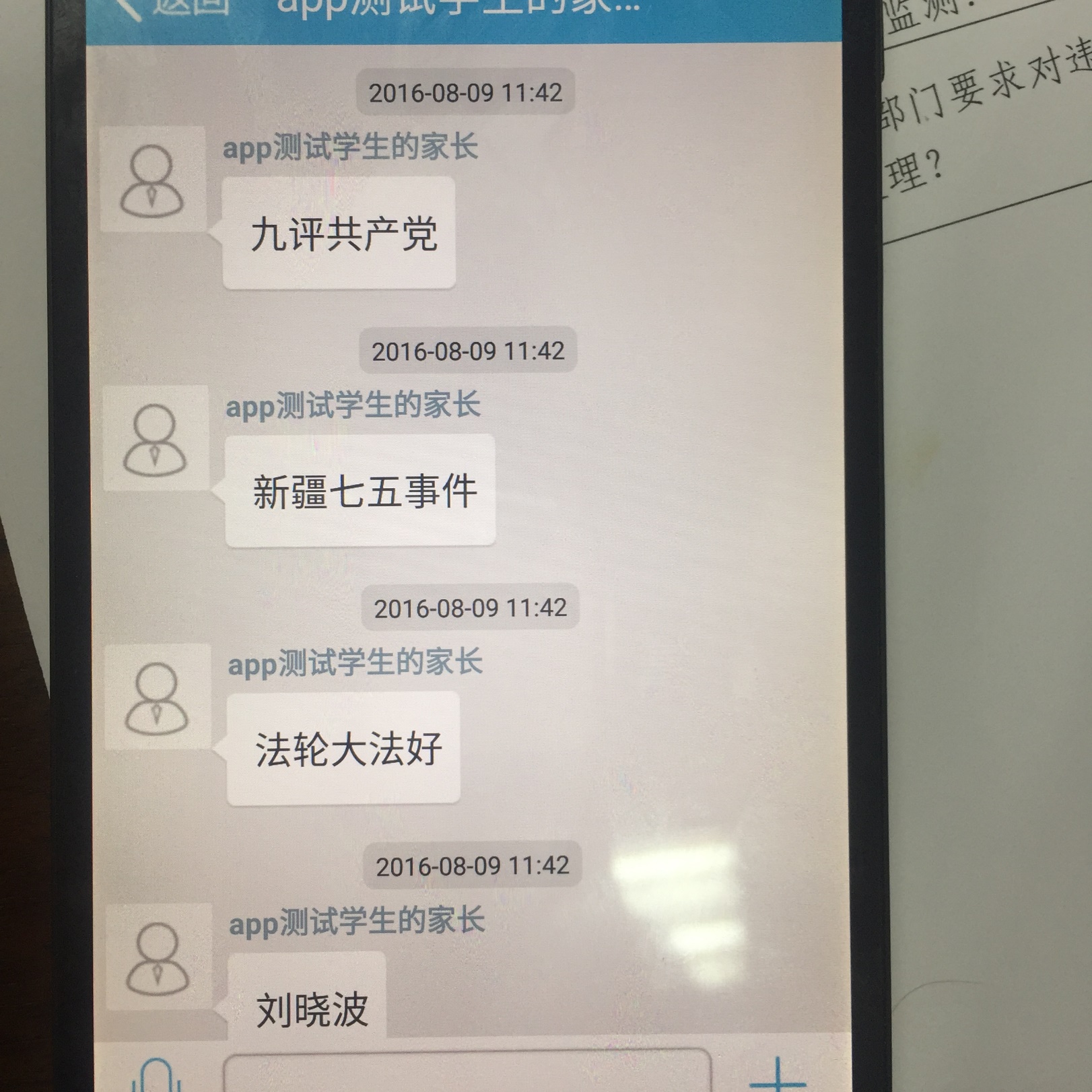
## 9.2 “人人通”业务安全评估结果

1、业务维护手册偏重网络安全方面内容，没有涉及到信息安全方面的内容。建议在维护手册中增加信息安全方面内容，明确对维护人员信息安全方面的要求。

2、人人通业务规模较大，半年内从16000增长至2万多，且面向的是学校教师、家长、学生等群体，建议配套建设与规模相匹配的信息安全技术能力，确保业务安全稳定运行。

3、人人通作业发布、通知、班级圈及其评论等信息发布环节没有信息过滤及审核机制，可发布任意信息。建议增加人工审核或关键词过滤机制。

4、人人通“个人信息”功能没有信息过滤或审核机制，简介可设置违法内容，头像可上传违法图片，建议加强对个人信息的审核，对于包含违法信息的简介或上传的上害图片，不予更新，并进行警示。



5、对教师、家长、学生等的姓名、手机号等敏感个人信息采用明文方式传输，建议进行加密后再传输，或直接利用HTTPS方式传输。

6、评估中，未见到有关信息内容审核标准的相关文件，建议辽宁联通制定信息内容审核标准，作为人工审核的参考依据。

7、未见到违法信息内容监测发现方案，建议制定相应方案。

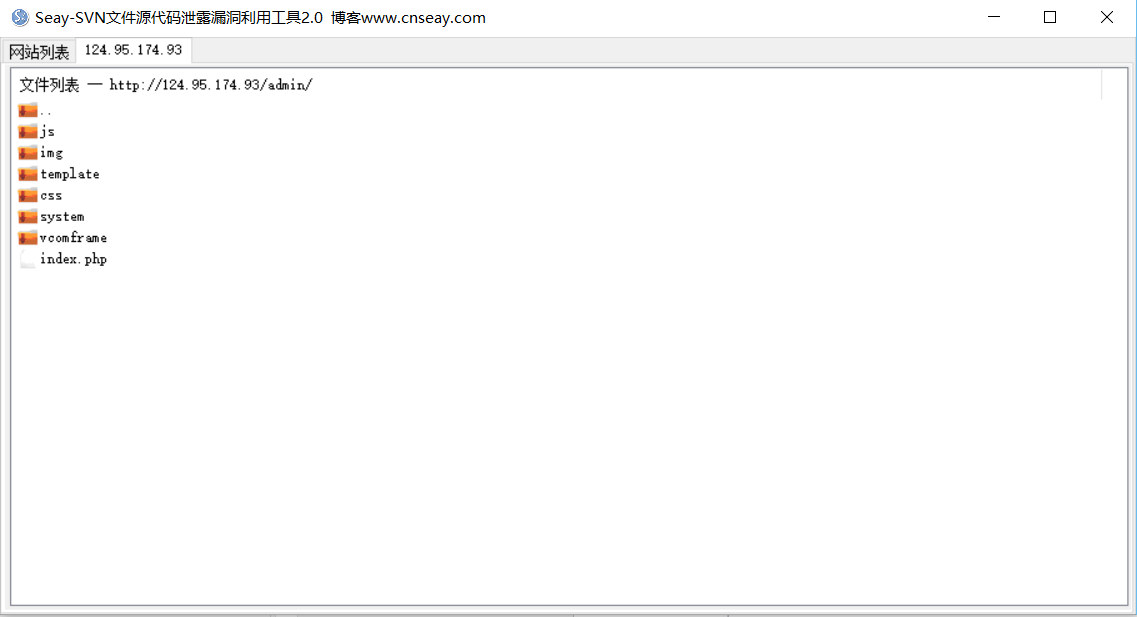
8、没有向群组申请人告知不得传播违法信息，建议向群组申请人明确提示“不得复制、发布、传播违法信息”。

9、管理员和用户密码明文传输，密码仅有长度要求，可以设置弱口令，无手机验证码机制，无登录错误次数限制，登录错误提示信息没有进行模糊处理，建议根据业务实际情况加强管理员和用户登录账户安全认证机制。

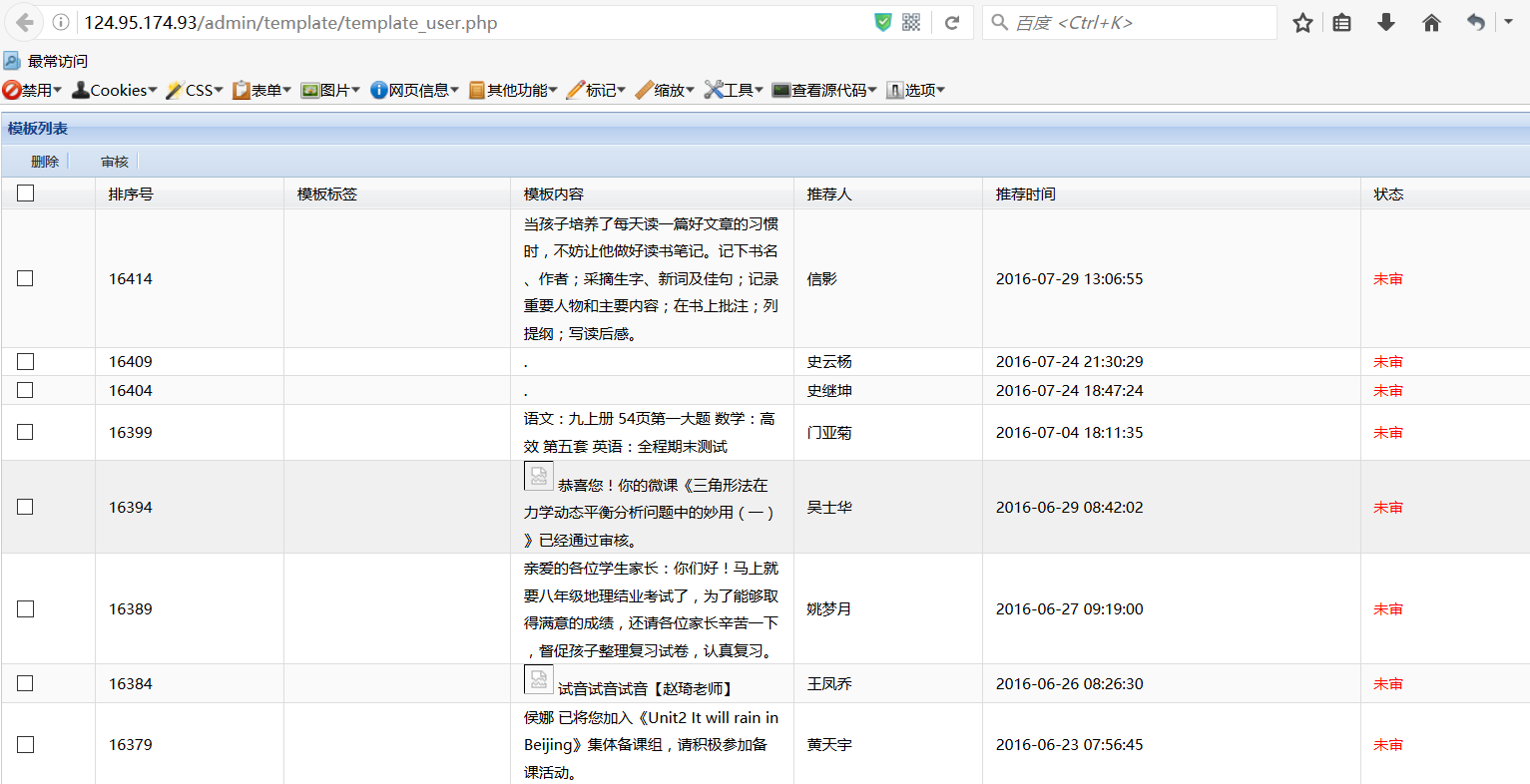
 

## 9.3 “人人通”业务安全保障能力评估情况

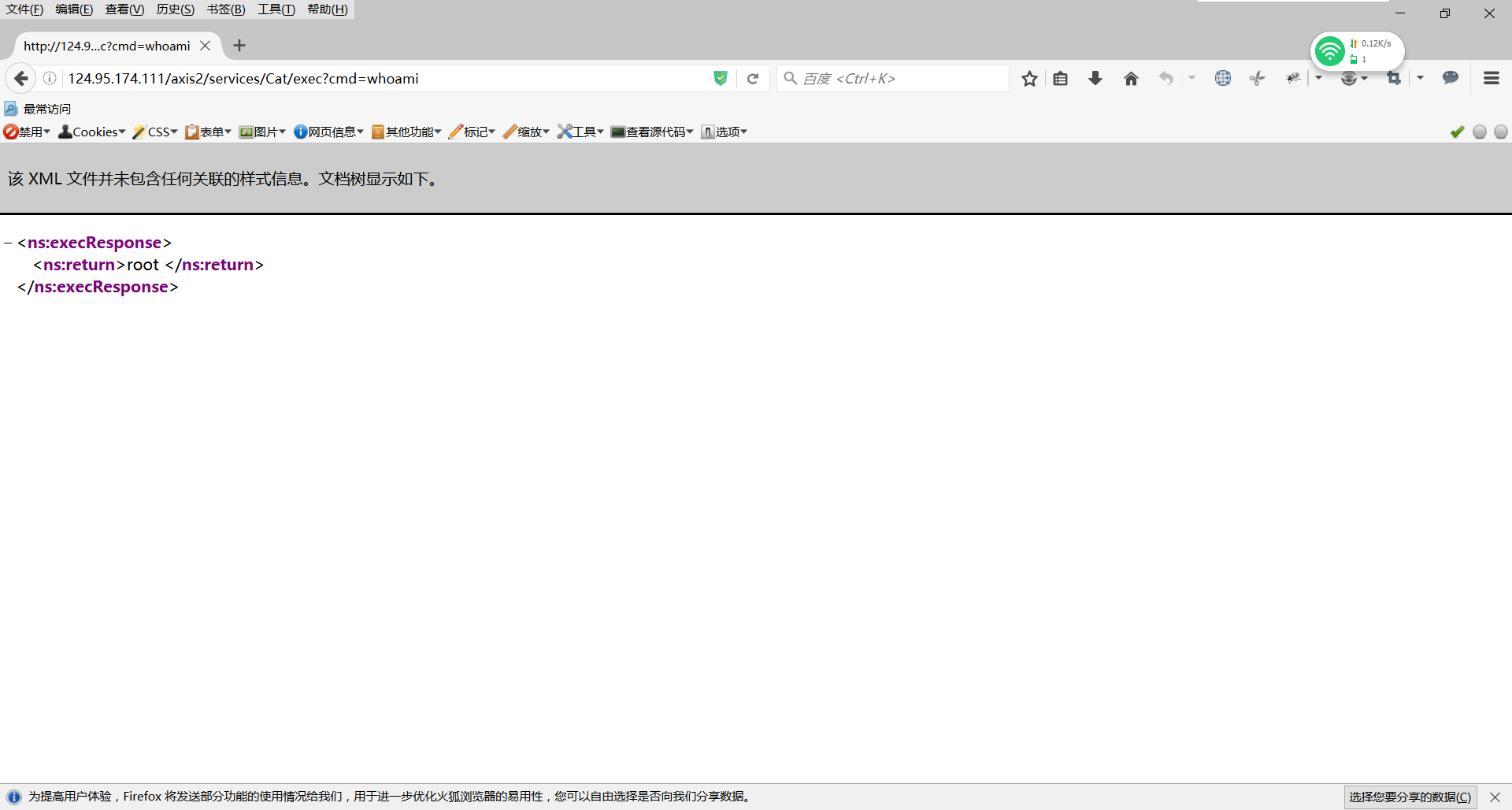
1、可通过直接访问http://124.95.174.93/admin/.svn/entries获取服务器上的备份源代码，建议将所有目录中的SVN文件删除。如果需要这些文件，请将它们放在隔离的位置，并限制它们的访问权限。

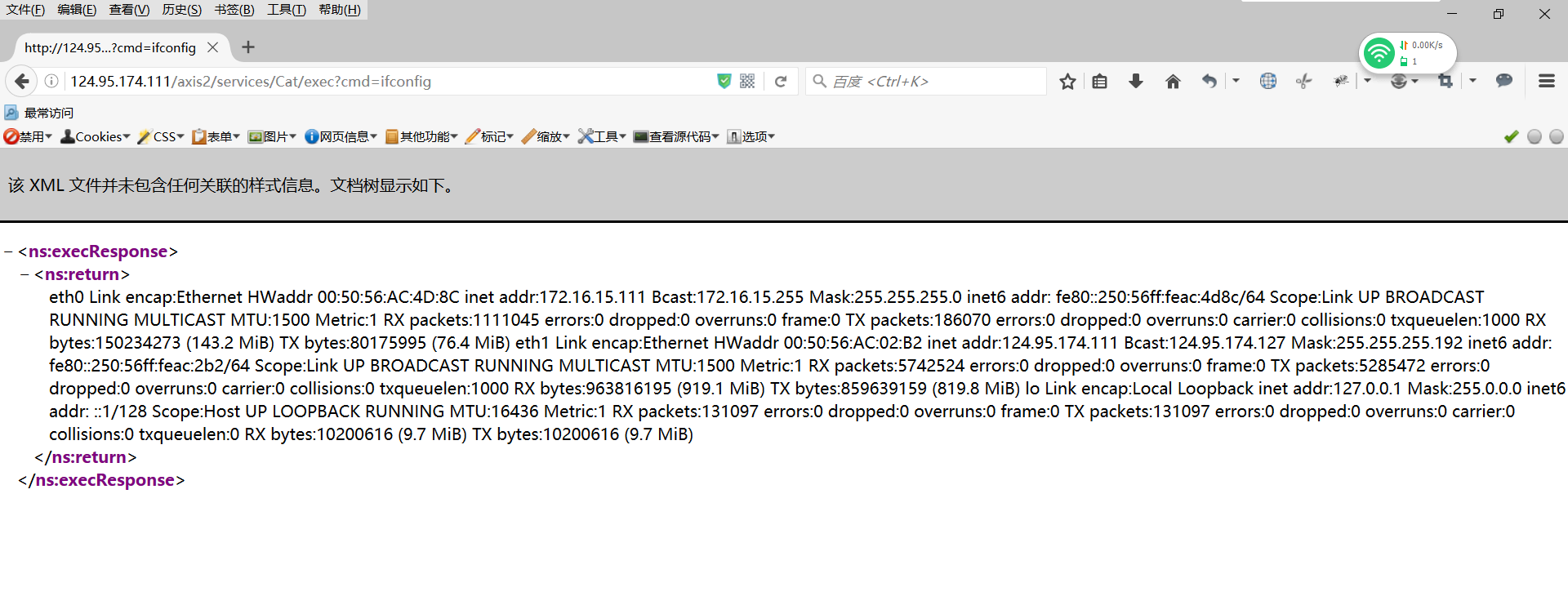


2、直接访问http://124.95.174.93/admin/template/template\_user.php没有进行访问认证，导致网站发生越权访问的漏洞，建议对网站进行访问控制处理。

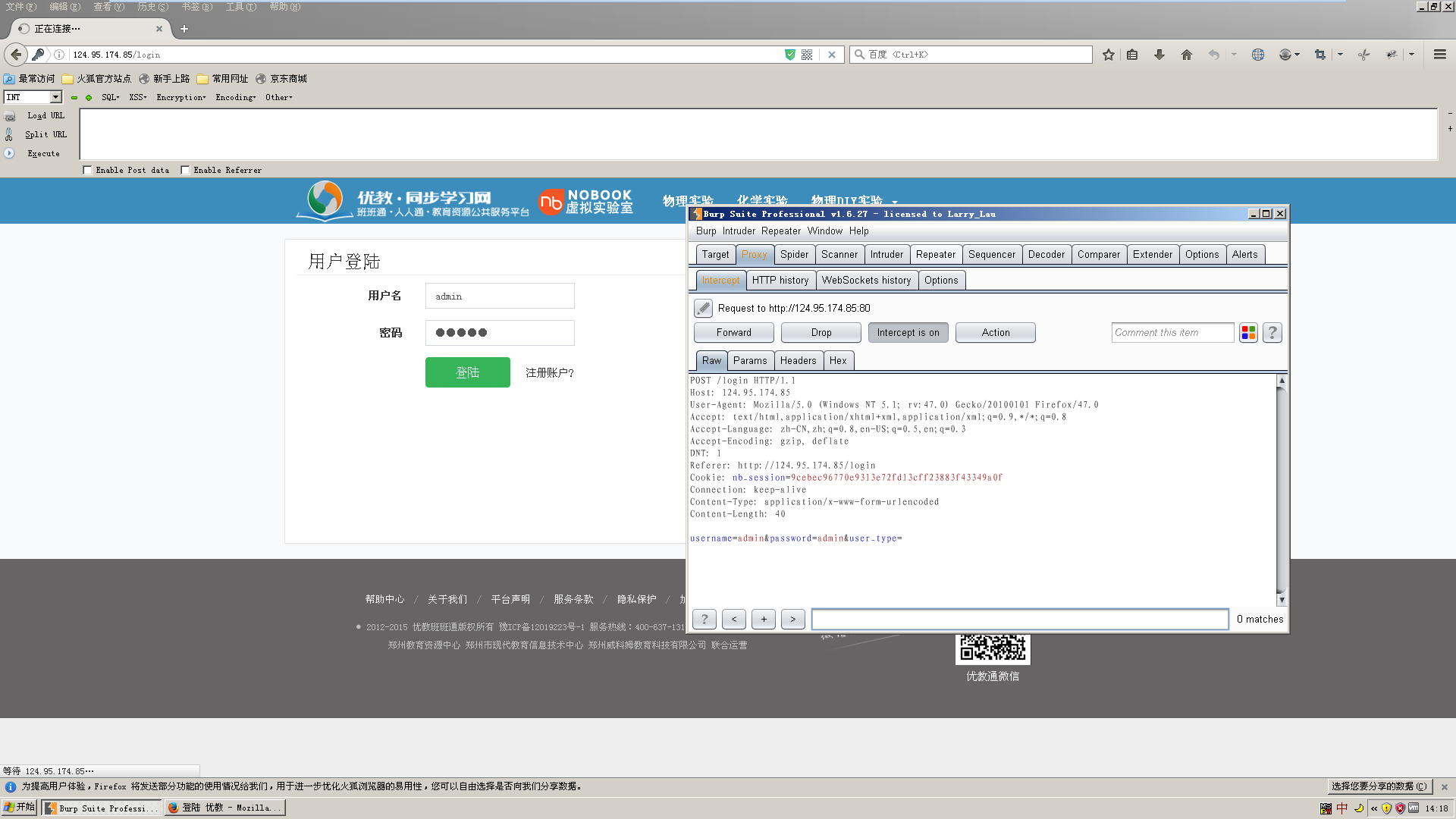


3、网站使用了axis2中间件，并被上传CAT后门，直接访问http://124.95.174.111/axis2/services/Cat/exec?cmd=whoami可获取服务器上当前使用的用户，直接访问http://124.95.174.111/axis2/services/Cat/exec?cmd=ifconfig可获取服务器上当前使用的网卡信息，建议删除网站没有用的中间件，清除网站后门。





4、http://124.95.174.85/login存在默认的用户名和密码，建议修改应用系统默认的弱口令。





# 整改建议

业务管理体系方面，建议辽宁联通公司加强信息安全管理方面的制度建设，制定针对合作企业、外部人员的管理制度或规范性文件，或者在信息安全责任管理办法中增加对合作企业、外部人员的信息安全管理相关条款。建议加强业务人员网络信息安全培训力度。建议根据业务发展情况及时对网络与信息安全管理方面的制度进行修订。

业务安全方面，有如下建议。

* 针对业务维护手册侧重网络安全内容的问题，建议在维护手册中增加信息安全方面内容，明确对维护人员信息安全方面的要求。
* 信息内容审核过滤机制方面，建议针对作业发布、通知、班级圈及其评论等信息发布环节增加人工审核或关键词过滤机制；建议加强对个人信息的审核，对于包含违法信息的简介或上传的违法内容图片，不予更新，并进行警示。建议制定信息内容审核标准，作为人工审核的参考依据。
* 建议制定违法信息内容监测发现方案，增强对违法信息监测发现的能力。
* 建议对教师、家长、学生等的姓名、手机号等敏感个人信息加密后传输，或直接利用HTTPS方式进行传输。
* 建议增加相应的板块或通过弹窗方式，向群组申请人明确提示“不得复制、发布、传播违法信息”。
* 建议根据业务实际情况加强管理员和用户账户登录安全认证机制。

业务安全保障能力方面，建议如下。

* 针对SVN泄露漏洞，建议将所有目录中的SVN文件删除。如果站点操作为了某个原因而需要这些文件，建议将它们放在隔离的位置，并限制它们的访问权限。
* 针对网站越权访问漏洞，建议加强对网站的访问控制。
* 针对网站存在的已知后门漏洞，删除网站没有用的中间件，清除网站后门。
* 针对Web应用的弱口令，建议修改应用系统默认的弱口令。