**报告编号：**

**互联网新技术新业务信息安全评估复核报告**

|  |  |
| --- | --- |
| **委托单位：** | 中国移动通信集团山西有限公司 |
| **业务名称：** | 和教育 |
| **完成时间：** | 2019年10月 |

**评估单位：国家计算机网络与信息安全管理中心**

**2019年10月**

**声明**

受中国移动通信集团山西有限公司委托，国家计算机网络与信息安全管理中心对中国移动通信集团山西有限公司和教育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，全面查找和教育配置的不安全因素，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** | 中国移动通信集团山西有限公司 |
| **复核**  **业务** | 和教育 |
| **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和教育业务进行了复核，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. 后续需在数据传输存储、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**（如：3.2.1 信息内容管理制度，信息发布递送功能管理，信息及时交互-信息销毁功能管理，信息社区功能管理）**，对日常管理制度的评估不够全面，建议对报告进行完善统一，精简内容，加强评估报告的规范性。

1. **复评中新发现的问题：**
2. **业务制度建设存在部分问题**

按照相关管理要求，山西移动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为集团公司规范，需进一步按照业务需求，对应制度完善满足本业务保障需要的制度，需形成制度性文件保障业务安全。

1. **业务保障能力方面，存在部分保障安全风险**
2. **业务应用安全保障：**
3. 无先审后发机制，评论、微校园功能缺乏先审后发机制，整个应用缺乏敏感词和敏感图片过滤审核机制；**风险程度：高**

**建议：对应用中涉及到评论、留言、群组聊天功能都进行敏感词、敏感图片的审核；**



1. 可以建立群组，且发消息无过滤机制；**风险程度：高**

**建议：对应用中涉及到评论、留言、群组聊天功能都进行敏感词、敏感图片的审核；**

1. 敏感词库不完善；**风险程度：高**

**建议：实时更新完善敏感词库；**

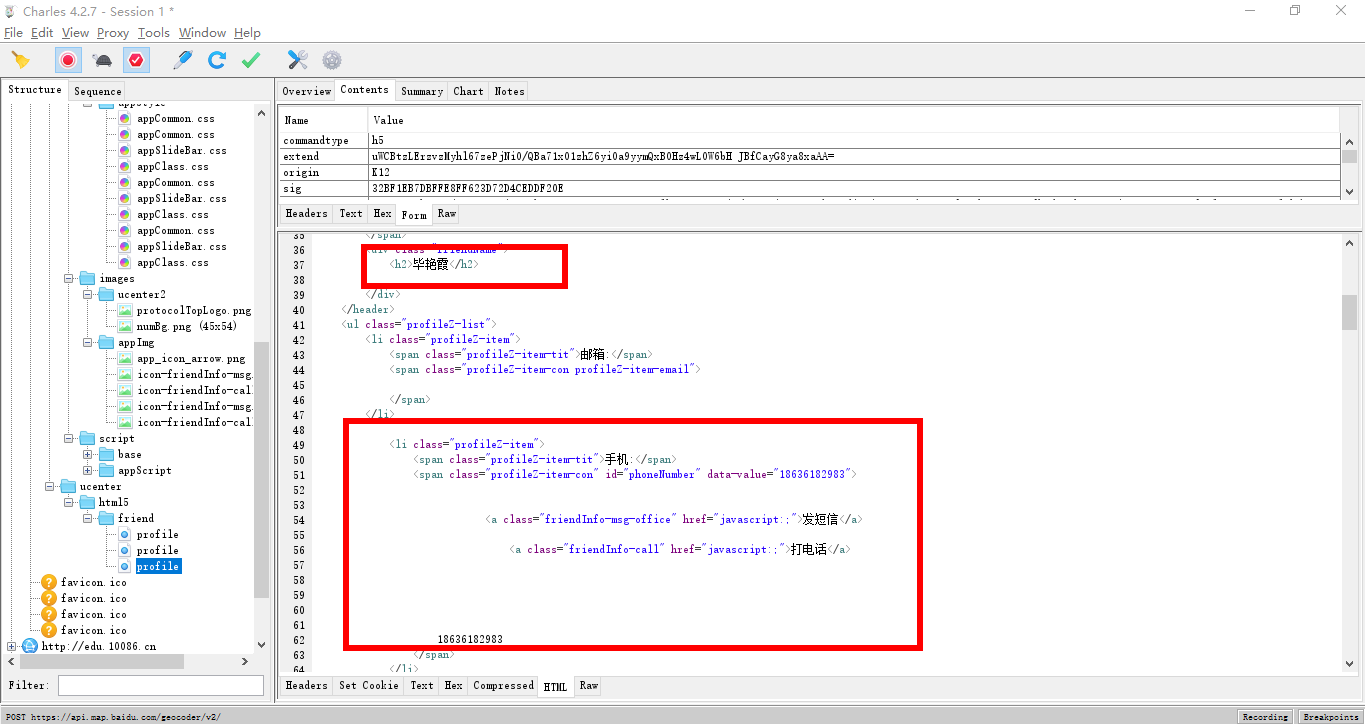
1. 会话失效机制无法有效执行，多点登陆无提示，一个账号登陆可同时登陆不同角色；且一方更改密码时，其他登陆用户无任何提示。**风险程度：中**

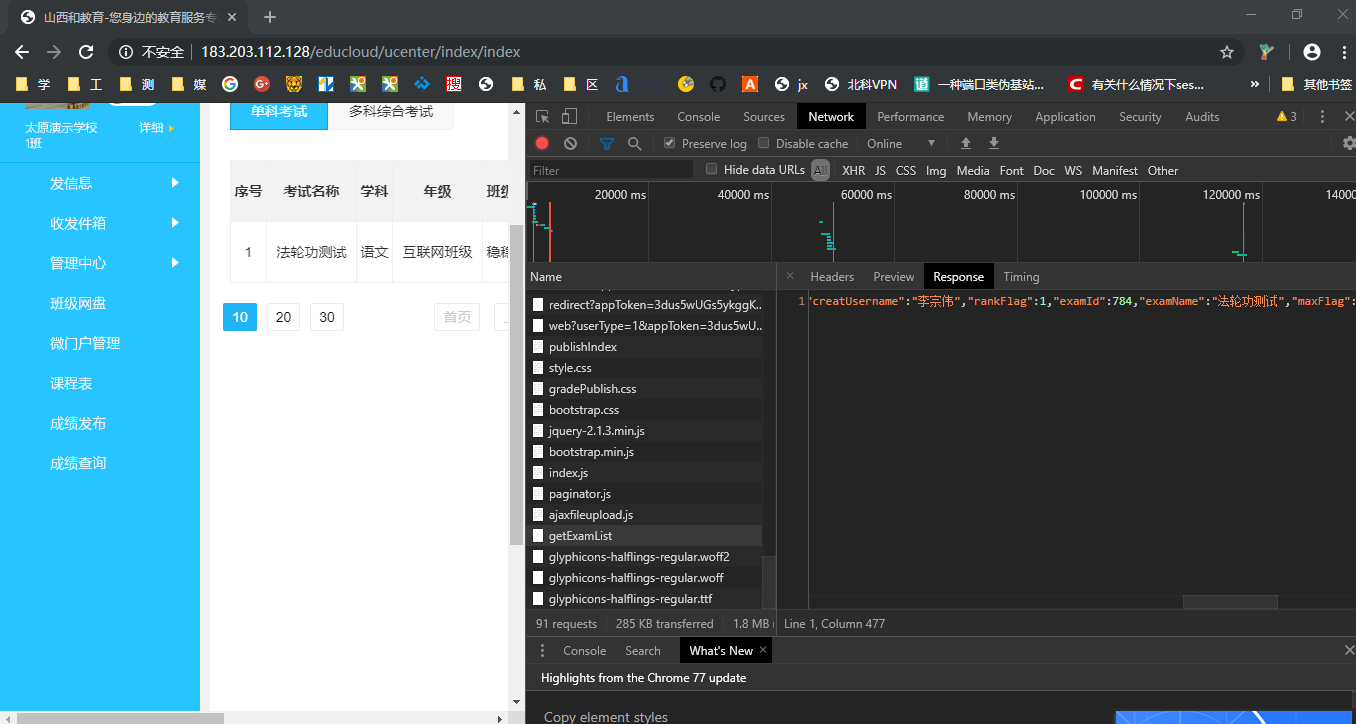
**建议：增加单点登陆校验，如：可采取优化SessionId等方式；**



1. 保障用户身份信息的保密性不够健全：在app端的通信录等页面采用明文传输用户个人信息，容易受篡改劫持;在web端也存在该风险；**风险程度：高**

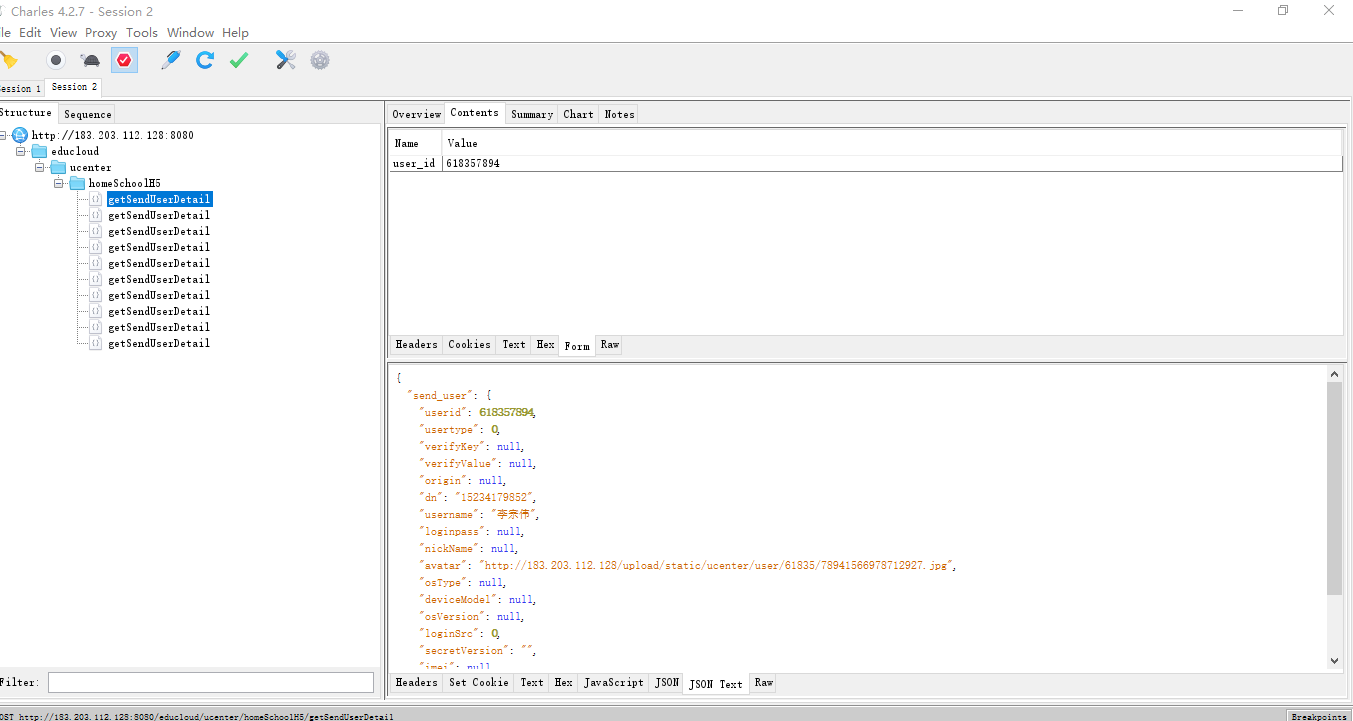
**建议：对涉及敏感个人信息部分进行加密传输；**

****



1. 接口不健全，通过构造请求，修改userid参数，可获取任意个人信息内容，会成个人信息泄露，具有较大的个人信息泄露风险。**风险程度：高**

**建议：优化接口，如：可在该接口中加入随机数校验等方式；**



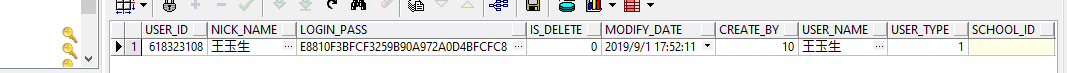
1. 建议显示个人信息时，做适当隐藏，如向好友公开手机号时，建议对中间4位做隐藏。**风险程度：中**

**建议：完善个人信息显示方式，如：可隐藏电话号码中间4位，人名只保留姓氏；**



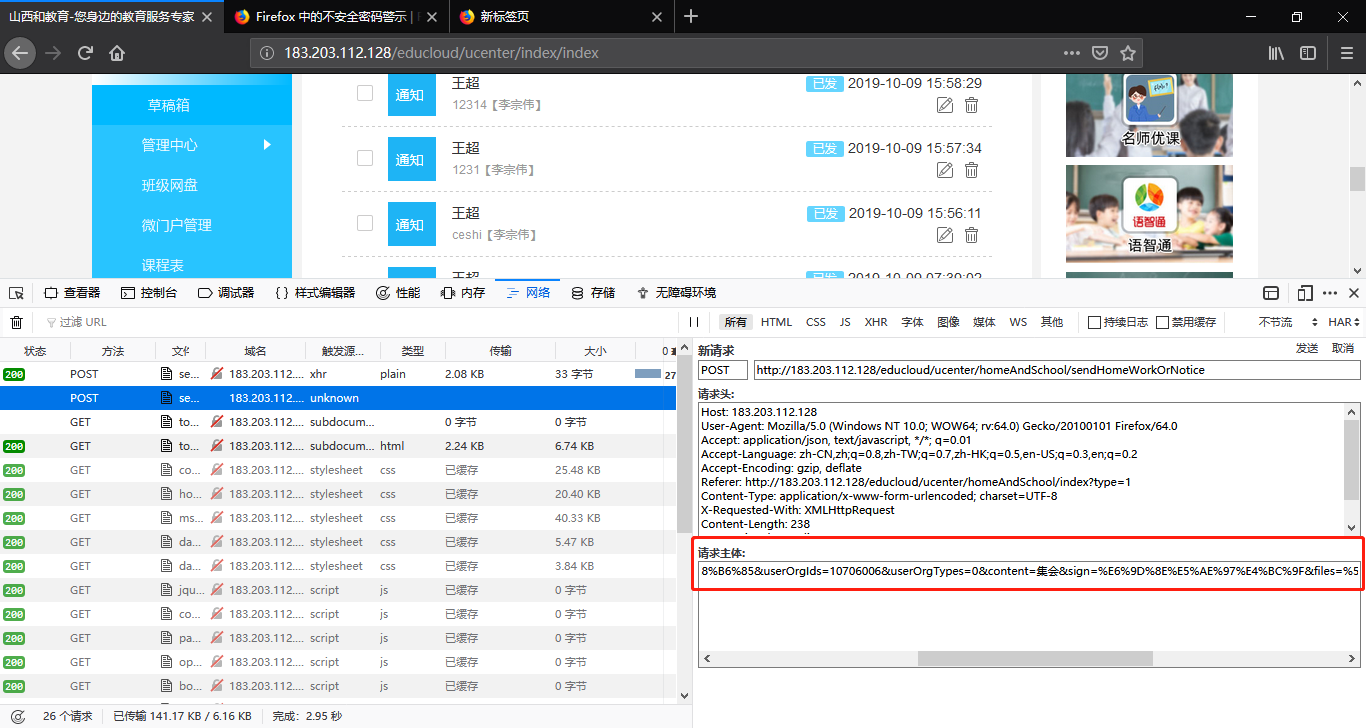
1. 数据库安全风险：数据库明文存储用户个人数据，存在数据泄露的风险。**风险程度：高**

**建议：对人名、电话等敏感信息应采取加密存储；**



1. 存在短信下发接口重大信息安全风险，可任意修改下发参数向任意手机号码或者一组号码群发信息内容，存在垃圾短信轰炸、诈骗等风险，具有违法信息较大范围传播风险；**风险程度：高**

**建议：优化接口，如：可在该接口中加入随机数校验等方式；**



1. 存在短信群发模版数据篡改重大信息安全风险，抽测期间，通过模版修改接口参数设置进行数据篡改，具有违法信息较大范围传播风险。**风险程度：高**

**建议：在短信群发模版中加入先审后发机制；**



1. 用户在自行注销或是毕业后，没有及时删除用户信息。**风险程度：中**

**建议：对注销、已经毕业等用户信息进行及时的销毁；**