红毯小程序服务器网络安全整改报告

校园信息化办公室：

收到《红毯小程序服务器网络安全高危漏洞通报》后，我们对整个安全事件进行了了解，并对小程序服务器进行了安全排查。现将相关情况报告如下：

一、基本情况

“复旦毕业红毯仪式”小程序主要用来支持2019界毕业生红毯活动的，通过提名候选人，并对其进行投票，筛选出前几名候选人参与红毯活动。该小程序的主要功能在于提名、投票，并在后台网站对提名者进行审核。该校程序的责任部门为共青团复旦大学委员会。开发维护由软件学院15级学生谢思豪、麻俊特完成，服务器在复旦大学信息办托管。

当前改程序的安全防护技术措施：

1. 使用https对访问信息进行加密；

2. 使用nginx进行反向代理，隐藏后端；

3. 前端源码进行了转义，无法阅读；

4. 后端使用JWT与Cookie技术维持会话，保证管理员访问的权限与账号密码的安全；

5. 使用log详细记录每一次数据库的操作；

6. 每隔半小时备份一次数据库，保证数据的高可用。

这次安全事件的发生经过：有同学打开了我们后台管理的网址，进行多次的账号密码尝试，最终将我们的管理账号密码尝试了出来，并在网上流传了开来。这次事件发生的技术漏洞在于两点：1.管理账号的用户名密码过于简单；2.管理网站没有做IP的屏蔽处理。

这次安全事件是由校内同学导致的，经过数据库log的检查，发现并没有对数据库进行改动，并且管理员界面的信息安全，不涉及可能引发舆论的信息泄露。暂未发现损失。

二、整改情况

在经历这次事件后，我们技术部门进行了以下整改：

1. 首先极大的增加了用户名与密码的复杂度，并确保其在有限的时间内无法被暴力破解；

2. 后端增加了关于IP限制代码。管理员登陆与操作只能限制在内网中进行。

3. 对管理员登陆账号密码的尝试进行了更为详细的log记录。

三、后续工作

1. 对所有的数据进行定时备份，确保最坏情况下的数据保留；

2. 定时对log进行查看，确保没有危险的管理员操作；并对出现的危险操作进行原因分析与排查。

共青团复旦大学委员会（加盖公章）

2019年05月08日