2021 年网络与信息系统安全月报

（6 月）

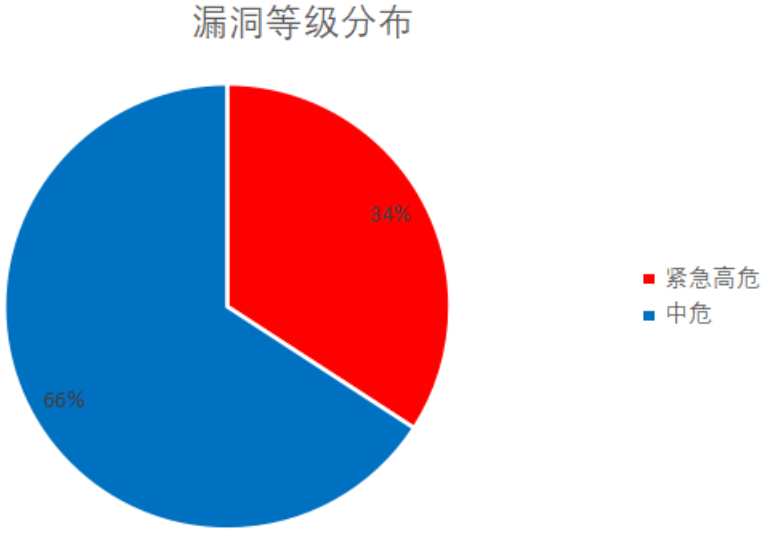
各单位、部门：

为进一步加强校园网络安全管理，保障校园网络安全，现将 6 月份网络与信息系统安全通报如下：

一、本月整体安全情况

(一) 漏洞发现情况

本月共发现漏洞 79 个。通过在校内网站监测、人工挖掘以及安全专项检查测试共发现漏洞 7 个，校外通报漏洞 72 个。其中紧急高危 27 个，中危漏洞 52 个，低危漏洞 0 个，紧急高危占比：34.2%。紧急、高危、中危、低危漏洞统计情况见下图。



注：

紧急高危漏洞是指可远程利用并能直接获取系统权限（服务器端权限、客户端权限）或者能够导致严重级别的信息泄漏（泄漏大量用户信息或学校机密信息）的漏洞，包括但不仅限于：命令注入、远程命令执行、上传获取 WebShell、SQL 注入、缓冲区溢出、绕过认证直接访问管理后台、核心业务非授权访问、核心业务后台弱密码等。

中危漏洞是指能直接盗取用户身份信息或者能够导致普通级别的信息泄漏的漏洞，包括但不限于目录浏览、客户端明文密码存储等。

低危漏洞是指能够导致轻微信息泄露的安全漏洞，包括但不仅限于 web 页面错误、堆栈信息泄露、JSONHijacking、CSRF、路径信息泄露、SVN 信息泄露、phpinfo 等。

(二)第三方漏洞通报

本校 6 月份所有漏洞通报均在规定时间内完成处理，未造成网络安全事件。

漏洞通报的来源包括：中央网信办，江苏省委网信办，教育 SRC。部分存在重大安全隐患的漏洞通报情况如下。

漏洞通报来源	网站（IP 地址）	漏洞类型	修复状态	部门
中央网信办	http://202.119.252.202	信息泄露	已修复	图书馆
江苏省网信办	http://202.119.249.17	越权访问，SQL 注入，XSS 漏洞，文件上传，信息泄露等 11 个漏洞	已关停	材料化学工程国家重点实验室
江苏省网信办	http://202.119.249.191	弱口令，源码信息泄	已关停	经济与管理学院

		露，文件上传等 5 个漏洞		
江苏省网信办	http://202.119.252.179	信息泄露	已修复	图书馆
江苏省网信办	http://202.119.252.183	目录浏览	已修复	图书馆
江苏省网信办	http://202.119.243.22	信息泄露	已修复	图书馆
江苏省网信办	http://hqdt.njtech.edu.cn	弱口令	已修复	后勤保障处
教育 SRC	http://202.119.243.118	信息泄露	已修复	科学研究院

表一：第三方通报漏洞

(三)非法外链情况

本月仍有多个系统及网站存在非法外链，具体情况如下：

网站（系统）	部门
http://tw.njtech.edu.cn/	团委
http://pharm.njtech.edu.cn/	药学院
http://maker.njtech.edu.cn/	教务处

表二：非法外链汇总表

(四)江苏省网信办应急演练

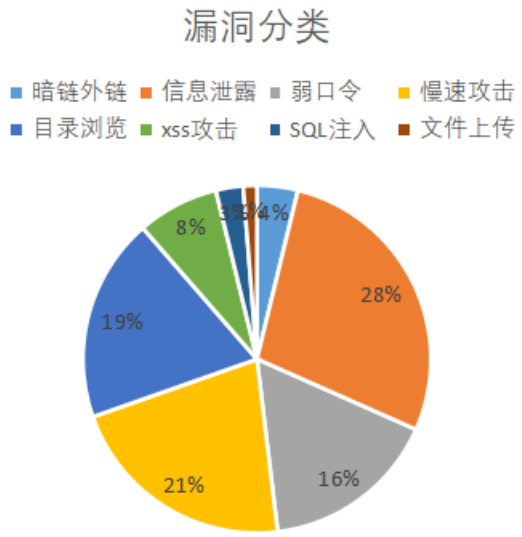
近一个多月江苏省网信办持续进行网络应急演练，在此阶段演练中，发现我校多个信息系统存在安全隐患，共接收到 68 起事件通报，其中弱口令存在 11 处，情况较为严重，其次 XSS 攻击和 SQL 注入也存在较多。针对此情况，各部门信息系统管理员需加强安全意识，及时修改网站后台弱口令，并对系统账号设置

强密码，设置复杂密码规则，系统开发人员禁止私自在服务器搭建管理页面。

二、安全情况分析

(一)漏洞类型分析

本月共发现漏洞 79 个。其中暗链外链 3 个，弱口令 13 个，SQL 注入 2 个，信息泄露 22 个，慢速攻击 17 个，目录浏览 15 个，xss 攻击 6 个，文件上传 1 个。漏洞分类占比如下图：



(二)漏洞修复情况

2021 年 6 月共发现漏洞 79 个，其中 63 个漏洞已修复，16 个漏洞所属系统已关停。

三、安全威胁风险与防范

（一）传统安全威胁风险与防范

安全威胁风险	防范措施建议
暗链外链情况较多	加强扫描力度，定期清除过期的新闻公告。
弱口令数量较多	加大运维管理员口令安全意识，定期检查系统密码复杂度。
多个系统存在软件开发商管理页面，且多存在弱口令	约束系统软件开发商行为，禁止在服务器上搭建私有管理页面。
开放平台 github 存在源码泄露	规范软件开发商和管理员行为，禁止将本校网站源码放到第三方开放平台。
多个服务器存在备份文件	加强服务器管理，禁止在服务器上备份系统信息，禁止在服务器上安装向日葵、Team-viewer 等远程连接工具。

四、网信安全每月小结

本月我校信息系统漏洞总数量较多，暴露的安全问题不容乐观。信息系统弱口令问题仍然较为严重，安全隐患较大，各部门需要重点关注。如果软件系统自身不具备高强度密码限制，须要求信息系统开发商立刻整改，设置高强度密码模块。各信息系统建设完成后必须先按照学校要求完成安全渗透检测，再上线运行。各部门应高度重视，将网络信息安全工作做到位，杜绝网络安全责任事故的发生。

网络与信息系统安全联系电话：58139275,83172363。

信息管理中心

2021 年 6 月 30 日