2021 年网络与信息系统安全年报

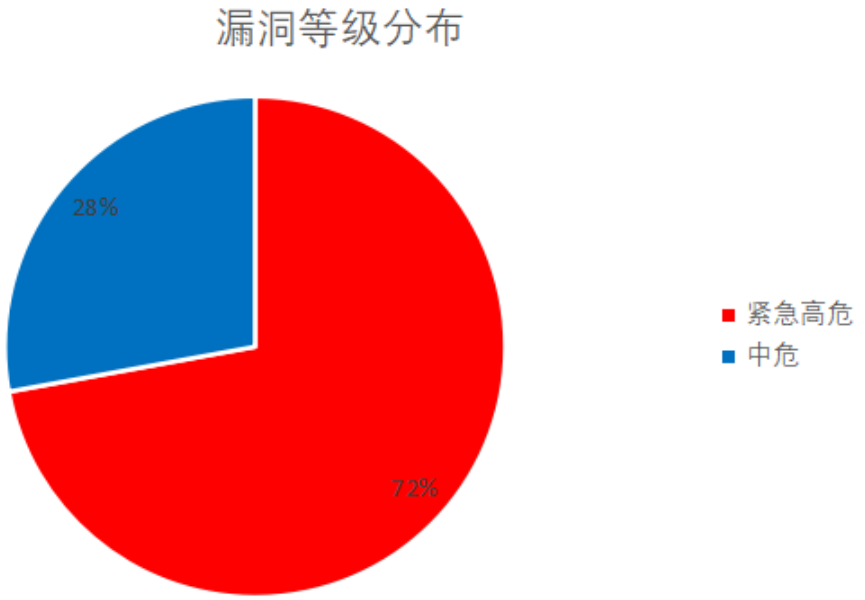
各单位、部门：

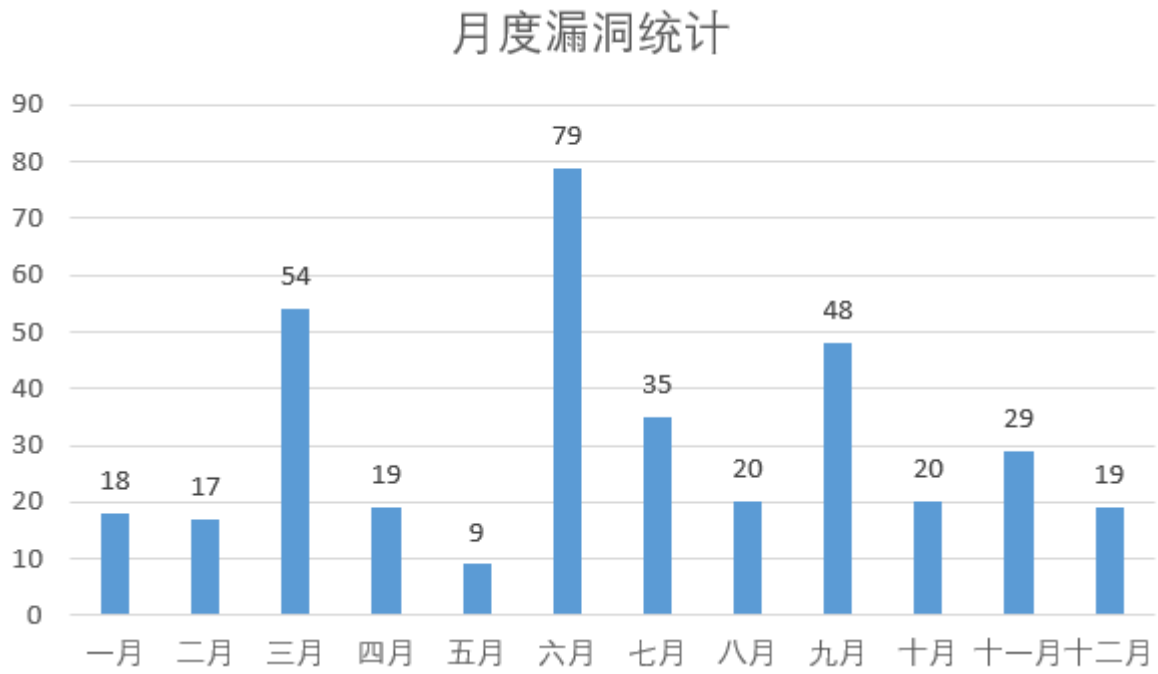
为进一步加强校园网络安全管理，保障校园网络安全，现将 2021 年网络与信息系统安全工作内容通报如下：

一、本年整体安全情况

(一) 漏洞发现情况

本年共发现漏洞 367 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 237 个，校外通报漏洞 94 个，渗透测试漏洞 36 个。其中紧急高危 265 个，中危漏洞 102 个，低危漏洞 0 个，紧急高危占比：72.2%。紧急、高危、中危、低危漏洞统计情况见下图。





注：

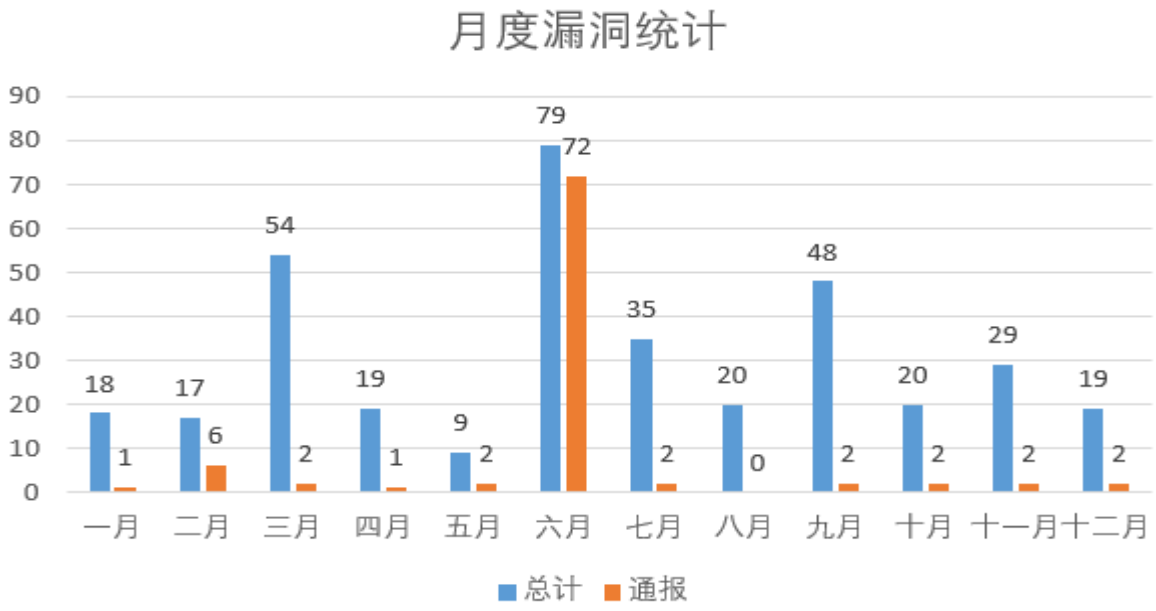
紧急高危漏洞是指可远程利用并能直接获取系统权限（服务器端权限、客户端权限）或者能够导致严重级别的信息泄漏（泄漏大量用户信息或学校机密信息）的漏洞，包括但不仅限于：命令注入、远程命令执行、上传获取 WebShell、SQL 注入、缓冲区溢出、绕过认证直接访问管理后台、核心业务非授权访问、核心业务后台弱密码等。

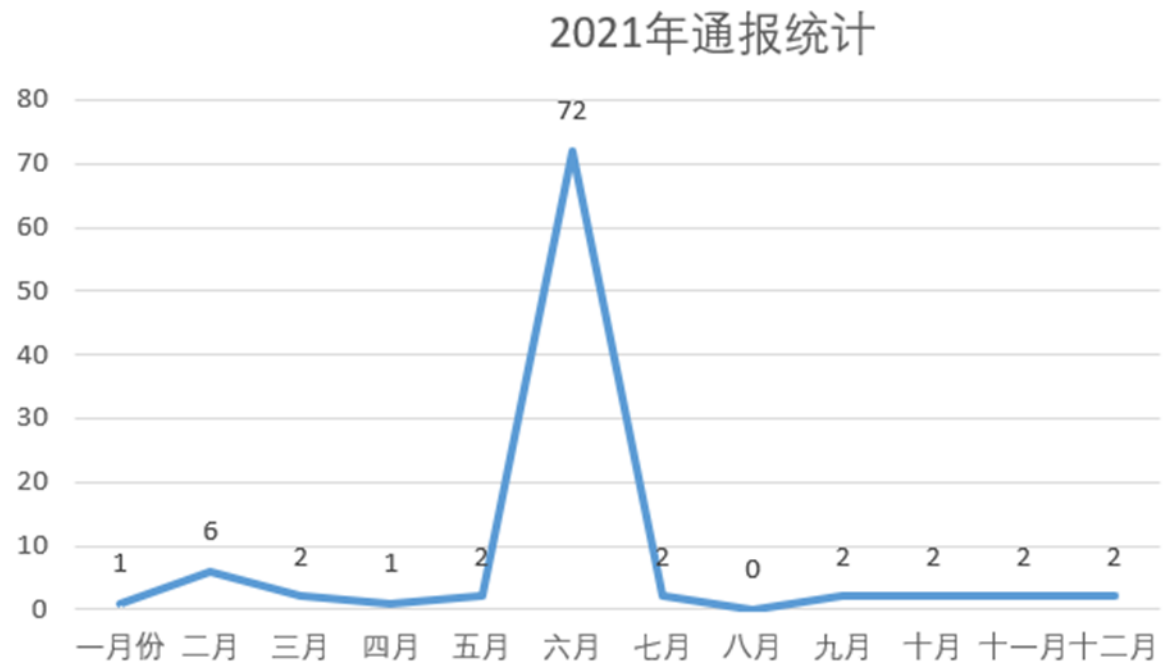
中危漏洞是指能直接盗取用户身份信息或者能够导致普通级别的信息泄漏的漏洞，包括但不限于目录浏览、客户端明文密码存储等。

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

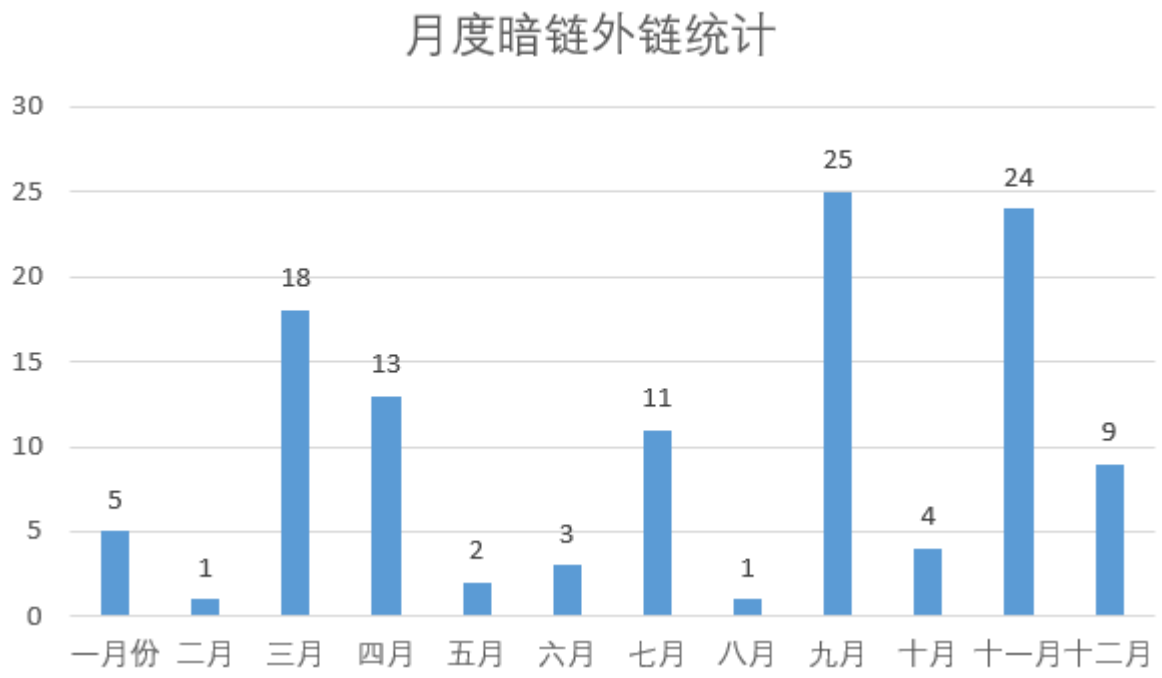
本年所有漏洞通报均在规定时间内完成处理，未造成网络安全事件。漏洞通报如下表所示：





(三)非法外链情况

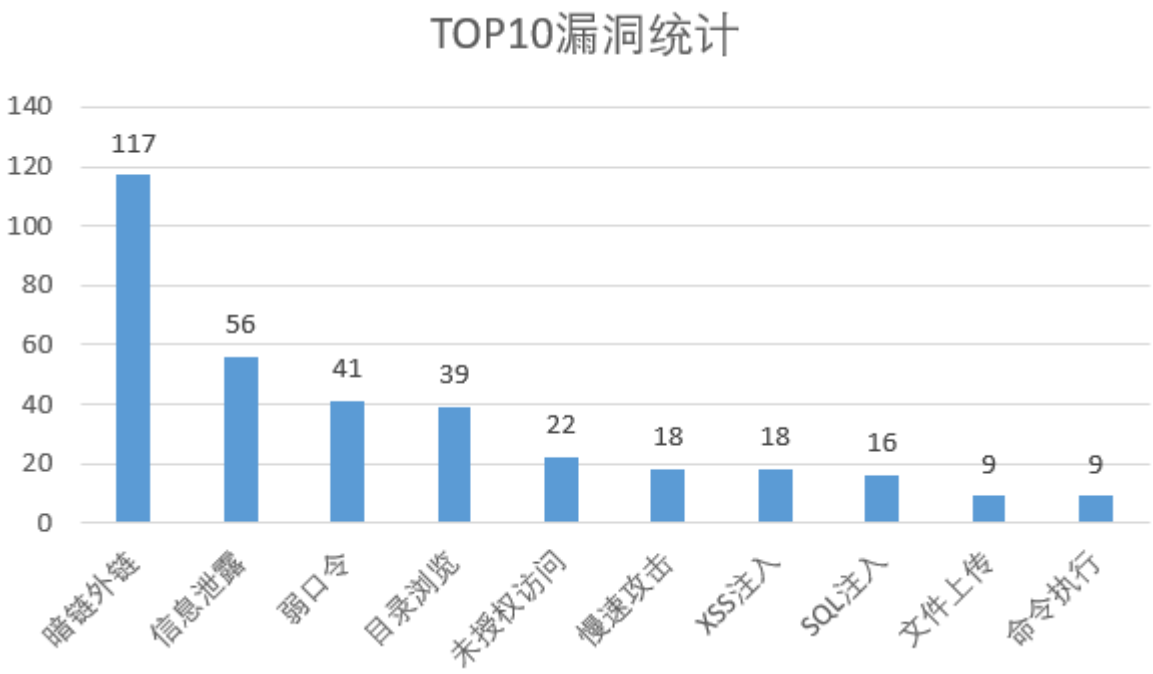
本年检查到 29 家单位所属网站共出现 117 次非法外链，具体月度统计情况如下：



二、安全情况分析

(一)漏洞类型分析

本年度共发现漏洞 367 个。其中暗链外链 117 个，信息泄露 56 个，弱口令 41 个，目录浏览 39 个，未授权访问 22 个，慢速攻击 18 个，xss 注入 18 个，SQL 注入 16 个，文件上传 9 个，命令执行 9 个，其他类漏洞 5 个，文件下载 3 个，身份证泄露 3 个，配置问题 3 个，挖矿木马 3 个，文件包含 1 个，目录遍历 1 个，逻辑漏洞 1 个，后门程序 2 个。漏洞分类占比如下图：



(二)漏洞修复情况

2021 年共发现漏洞 367 个，本年度漏洞均已修复。

三、2021 年网络安全管理与建设

（一）完善网络安全管理体制，提升网络安全管理水平

1．调整学校网络安全和信息化领导小组人员并明确工作职责；召开网络安全和信息化领导小组会议和每季度网络安全工作会议；与各二级单位签订《网络和信息系统安全责任书》；表彰上年度信息化工作先进集体 10 个、先进个人 20 名。

2．制订学校网络信息安全管理规章制度：

（1）《2021 年网络和信息安全工作要点》；

（2）《关于加强网络和信息安全工作的通知》；

（3）《南京工业大学网站群管理办法》；

（4）《南京工业大学电子邮箱用户管理办法》；

（5）《南京工业大学网络安全责任制实施细则》。

3．每月发布《网络与信息系统安全月报》，对本月校园网络安全情况进行梳理分析和总结，对校园网络安全隐患进行排查，积极排查整改，确保全校信息系统（网站）及数据安全。对常见安全漏洞进行科普，提升全校师生网络安全知识素养。

（二）网络与信息化安全项目建设

1．部署上线智能网络信息安全管理平台、安全态势感知平台、web 资产管理平台、WAF 探针系统的建设工作，提高我校网络信息安全管理信息化水平，建立全面的安全防护与应急保障机制，为我校网络信息安全管理提供了重要支撑。

2．完成南京工业大学 OA 办公平台（二级）、南京工业大学统一数据服务平台（二级）和南京工业大学智慧南工平台系统（三级）等保备案和测评工作。提高我校重要信息系统的信息安全防护能力，降低系统被各种攻击的风险。

（三）网络安全宣传培训与教育

1．邀请江苏省公安厅网络安全保卫总队、南京市公安局网络安全保卫支队等网络安全专家为我校各部门网络安全相关人员进行了《当前网络安全形势及有关法律法规政策解读》及《网络安全与自我保护》的培训讲座，提高政治站位，增强忧患意识，以筑牢网络安全屏障为目标，加强组织与制度建设、强化网络安全保障，积极防范化解网络安全风险。

2．以 2021 年网络安全宣传周为契机，组织了各种线上

线下网络安全宣传活动，上线南京工业大学网络信息安全网站,进一步推进网络安全工作融入校园，全面普及网络安全法律法规，营造安全、健康、文明的校园网络环境。

3．2021 年，信息管理中心组织学生团队参加“领航杯”江苏省第六届青少年网络信息安全应用能力竞赛，同学们克服初次参加比赛经验不足等重重困难，沉着应战，顽强拼搏，最终位列第 8 名,获得三等奖,首次参赛即获得历史性突破。

（四）落实网络和信息安全综合治理、筑牢网络安全“防护网”

全面清查学校信息资产，建立相关台账记录，消除网络和信息安全隐患；开展网络攻防演练；开展邮箱、服务器、网络设备安全专项治理。

2021 年 5 月底、6 月上旬，校网络安全和信息化领导小组办公室（信息管理中心）组织专业队伍对全校 300 多个信息系统进行安全检测，对其中 4 个系统开展网络安全应急演练。演练设置信息系统安全、联网设备安全、个人信息安全三个科目，通过系统致瘫、网页篡改、数据泄露、获取联网设备权限等方式，真实展现测试结果，并复盘检验被测单位的监测预警和应急处置能力。通过真操实练发现潜在风险、验证可能危害、检验应急措施。

进一步提升应对网络安全突发事件的组织指挥能力和应急处置能力，提高网络安全工作管理水平，扎实做好网络安全保障工作。

（五）网络信息安全考核成绩创新高

2021 年，信息管理中心按照省委网信办、省教育网信办和校党委要求，深入贯彻落实网络安全责任制，在学校网络安全与信息化领导小组的领导下，认真开展各项工作，圆满完成本年度全省教育系统网络安全责任制考核，考核成绩位居省属高校前列。

本次网络安全责任制考核从领导责任制、队伍建设、工作研究部署、经费保障、信息资产管理、安全威胁监测预警通报、网络安全应急管理、等级保护落实情况、网络安全检查、网络安全宣传教育培训，重要时期网络安全保障工作等 13 个大项、25 个小项对我校网络安全工作进行全方位考核，2021 年累计完成重要时期网络安全保障工作 73 天。在网络信息安全基础考核项目中，我校获得了满分的好成绩。

2021 年，我校主动报送网络安全重要进展信息，积极参与省教育网信办组织的专项工作，学生团队参加“领航杯”江苏省第六届青少年网络信息安全应用能力竞赛获得三等奖，得到考核附加分加分。

（六）恶意程序治理成效明显

1.“挖矿”病毒专项检查。2021 年，信息管理中心在 7 月、9 月、10 月和 12 月进行了“挖矿”病毒专项检查和治理，处理 3 个学院机房用机，受感染的电脑个人终端及服务器超过 100 个。信息管理中心对这些受感染设备进行了紧急网络隔离，并通知设备所属单位及个人，对设备进行全面病毒查杀和修复，避免了校内大规模挖矿病毒感染情况的发生，

确保校内电脑终端及服务器正常运行。

2.“勒索”病毒治理与防范。2021 年，勒索病毒攻击事件频发，传统勒索病毒家族的新变种、新的勒索病毒家族均大量出现。信息管理中心利用态势感知平台等多种工具对校内受“勒索”病毒感染的情况进行分析，及时切断传播途径，并通知相关个人和单位及时处理，并通过南京工业大学网络安全宣传网站，宣传“勒索”病毒的防范和处理方法。

四、存在问题和解决方案

存在问题	解决方案
新模范马路校区流量未纳入态势感知监控，网络安全状况无法及时查看	在创新大楼核心机房部署一台态势感知探针，将监测到的流量发送到态势感知平台，便于两个校区安全态势统一管理。
部分安全审计设备不支持 IPv6 模式	为满足信息系统等保测评基本要求，需要增加支持 IPv6 和 IPv4 的安全审计设备。
原 waf 性能已不能满足要求，且不支持 IPv6 网站	根据等级保护三级要求，新增支持 IPv6 的 waf，且性能满足江浦核心机房所有应用系统防护。
原用于远程调试的 VPN 系统存在安全隐患	建设 VPN 认证系统，满足 IPv6 和 IPv4，支持人脸识别、短信认证、二维码认证等。
2021 年上半年我校被通报 18 起拒绝服务攻击	部署专门的防毒墙，防 DOS 攻击设备，对应用层和网络层 DDOS 攻击进行全

（DOS）事件，拒绝服务器攻击是黑客常用攻击手段之一，	面的检测和过滤，适配对本校 WEB 服务，DNS 业务，移动业务以及代理防护等多个场景
部分数据库信息资产在使用过程中，缺少加密和脱敏措施。	根据《中华人民共和国数据安全法》相关要求，配备相关设备和系统，强制实施数据库加密和脱敏，保护数据库信息资产安全。

五、网信安全年度小结

2021 年，新冠肺炎疫情仍十分严峻。不论是在疫情防控相关工作领域，还是在远程办公与科研、教学信息化等科研教学领域，大量新型互联网产品和服务应运而生，在助力疫情防控的同时也进一步推进校园数字化转型。与此同时，安全漏洞、数据泄露、网络诈骗、勒索病毒等网络安全威胁日益凸显，有组织、有目的的网络攻击形势愈加明显，为校园网络安全防护工作带来更多挑战。

我校将持续完善网络信息安全设施建设和部署，加强网络安全监测和应急处置工作，组织应急演练，持续加强网络安全管理体系建设，出台系列制度，不断夯实网络安全基础。

各单位应全面梳理本单位的信息资产，严格遵守学校网络安全各项工作要求，并做好安全防护工作，安装操作系统防护软件，新建信息系统未经过安全渗透检测，一律不得上线。同时各单位应时刻绷紧安全之弦，高度认识网络安全和信息化工作的极端重要性，从讲政治的高度严格落实网络安全责任制。

信息管理中心

2022 年 1 月 13 日