2021 年网络与信息系统安全月报
（3 月）

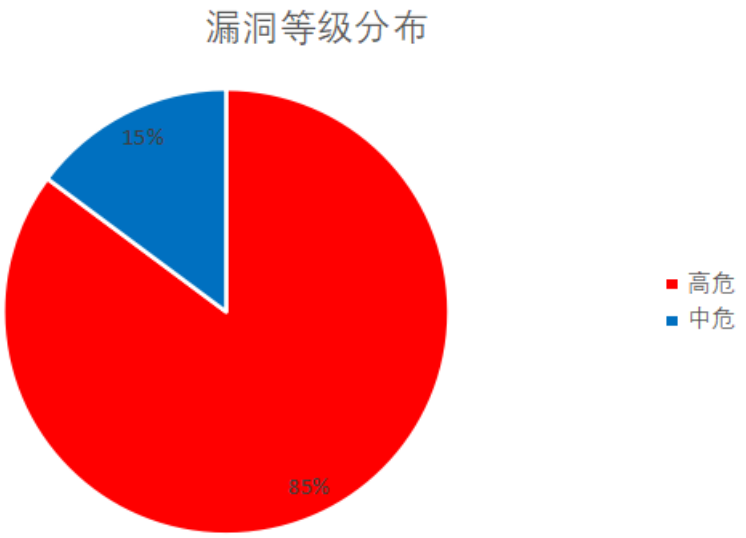
各单位、部门:

为进一步加强校园网络安全管理，保障校园网络安全，现将 3 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 54 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 52 个，校外通报漏洞 2 个。其中紧急高危 46 个，中危漏洞 8 个，低危漏洞 0 个，紧急高危占比：85.1%。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

本月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：教育 SRC。具体情况如下。

漏洞通报来源	网站（IP 地址）	漏洞类型	修复状态	部门
教育 SRC	http://202.119.249.101:8080/	SQL 注入	已修复	后勤保障处
教育 SRC	http://yjsxt.njtech.edu.cn/	文件上传	已修复	研究生院

表一：第三方通报漏洞

(三)非法外链

本月查到多个系统及网站存在非法暗链外链，具体情况如下:

网站（系统）	部门
http://arch.njtech.edu.cn/	建筑学院
http://cly.njtech.edu.cn/xtcx/	材料科学与工程学院
http://english.njtech.edu.cn/	外国语言文学学院
http://cqt.njtech.edu.cn/old/	党委宣传部
http://sp.njtech.edu.cn/	大学科技园管理办公室
http://jgy.njtech.edu.cn/	经济与管理学院
http://jkjy.njtech.edu.cn/	后勤保障处

表二：非法暗链外链汇总表

(四)渗透测试

本月共进行三个网站（系统）的渗透测试。渗透测试是通过模拟

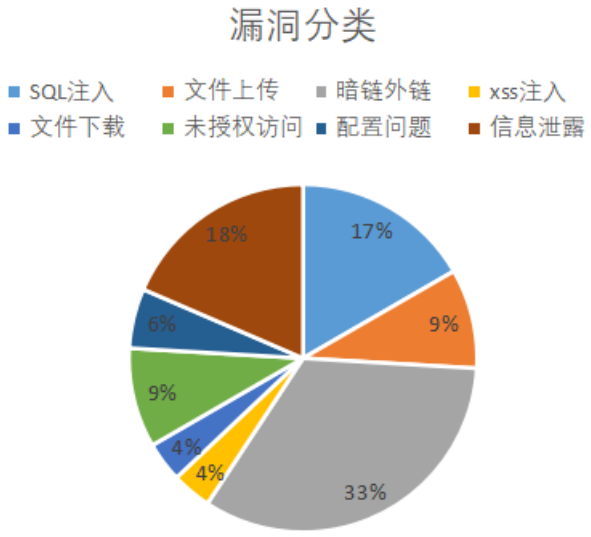
恶意黑客的攻击方法，来评估计算机网络系统安全的一种评估方法。这个过程包括对系统的任何弱点、技术缺陷或漏洞的主动分析，这个分析是从一个攻击者可能存在的位置来进行的，并且从这个位置有条件主动利用安全漏洞。

本次渗透测试共发现漏洞 22 起，其中高危紧急漏洞 15 起，包括 5 起可获取服务器权限的漏洞，中危漏洞 7 起。

二、安全情况分析

(一) 漏洞类型分析

本月共发现漏洞 54 个。其中 SQL 注入 9 个，文件上传 5 个，暗链外链 18 个，xss 注入 2 个，文件下载 2 个，未授权访问 5 个，配置问题 3 个，信息泄露 10 个。漏洞分类占比如下图:



(二) 漏洞修复情况

本月共发现漏洞 54 个，均已全部修复。

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
网站后台威胁严重	控制网站登录账号密码，制定网站后台测试计划。
网站暗链外链问题较多	加强扫描力度，定期清除过期的带有校外域名链接的新闻公告，重点排查网页中非本校域名链接。详见南工校信〔2020〕3 号《关于加强我校网站中外部链接管理的通知》。
网站压缩文件可直接访问并下载	网站避免压缩文件，压缩文件控制权限，禁止下载。

四、网信安全每月小结

本月我校发现的网站暗链外链问题数量较多，因各部门响应处理及时，未造成网络安全事件。因我校网站暗链外链问题多次存在，请各单位（部门）网站管理员务必定期清查网站页面内容、网站链接及网站附件内容，进一步加强部门网站建设和管理，确保我校网络信息发布环境安全稳定。

网络与信息系统安全联系电话：58139275,83172363。

信息管理中心

2021 年 4 月 2 日