2021 年网络与信息系统安全月报

（4 月）

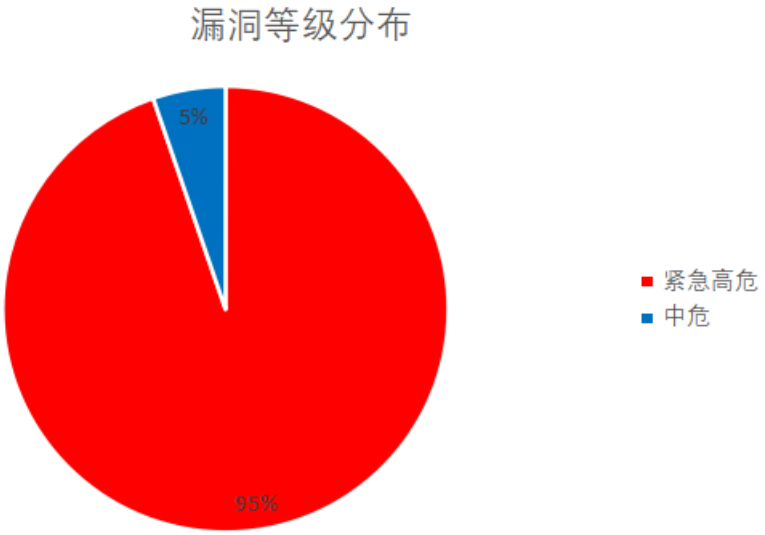
各单位、部门：

为进一步加强校园网络安全管理，保障校园网络安全，现将 4 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 19 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 18 个，校外通报漏洞 1 个。其中紧急高危 18 个，中危漏洞 1 个，低危漏洞 0 个，紧急高危占比：94.7%。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://green.njtech.edu.cn/	信息泄露	已修复	计算机科学与技术学院

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暗链外链，具体情况如下：

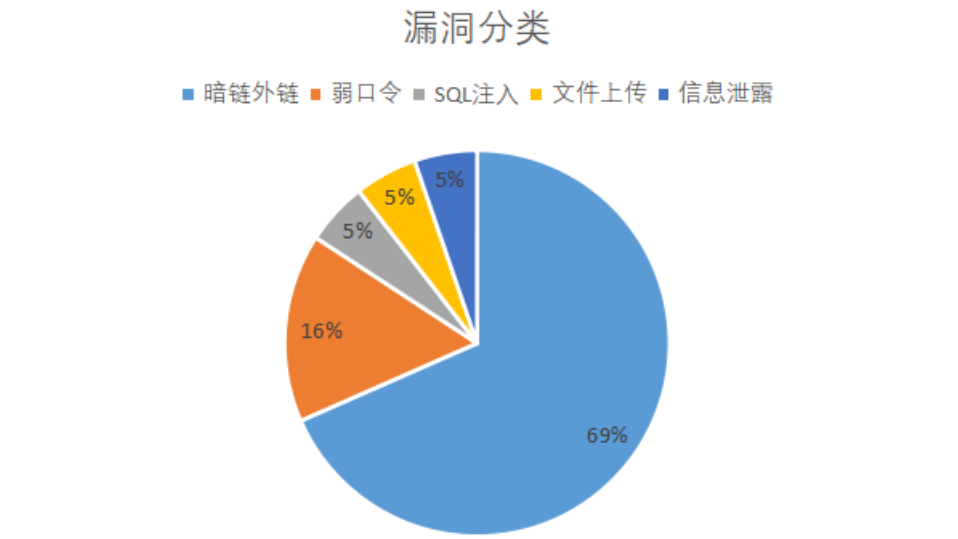
网站（系统）	部门
http://cces.njtech.edu.cn/	安全科学与工程学院
http://csjsxy.njtech.edu.cn/	城市建设学院
http://green.njtech.edu.cn/	计算机科学与技术学院
http://jgy.njtech.edu.cn/	经济与管理学院
http://maker.njtech.edu.cn/	教务处
http://pharm.njtech.edu.cn/	药学院
http://sp.njtech.edu.cn/	大学科技园管理办公室
http://jszy.njtech.edu.cn/	大学科技园管理办公室
http://cce.njtech.edu.cn/	土木工程学院
http://english.njtech.edu.cn/	外国语言文学学院
http://cqt.njtech.edu.cn/old_bak/	党委宣传部

表二：非法外链汇总表

二、安全情况分析

(一)漏洞类型分析

本月共发现漏洞 19 个。其中暗链外链 13 个，弱口令 3 个，SQL 注入 1 个，任意文件上传 1 个，信息泄露 1 个。漏洞分类占比如下图：



(二)漏洞修复情况

本月共发现漏洞 19 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
网站暗链外链问题较多	加强扫描力度，定期清除过期的新闻公告。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》
本月弱口令数量较多	加大运维管理员口令安全意识，定期检查系统密码复杂度。

（二）“双非”信息资产

高校网站为教育网的公网地址，互联网可以直接访问，当出现内容与学校相关或带有学校标识，且未使用学校 IP 地址和 njtech.edu.cn 学校域名后缀的信息系统（网站）为“双非”信息资产，包含以下三种形式：

1. 使用校外 IP，但采用 njtech.edu.cn 学校域名后缀；

2. 使用校内 IP，但采用非 njtech.edu.cn 后缀；

3. 使用校外 IP、非 njtech.edu.cn 后缀，但内容与学校相关。

“双非”信息资产因上线前未做安全检测,极容易存在安全隐患，攻击者可轻易找出漏洞并利用，从而获取网站存在的大量敏感信息。双非系统（网站）多部署在校外或者云端，学校无法第一时间对双非系统（网站）实施技术管理或关停，所以该系统（网站）的安全性尤为需要重视，有双非系统（网站）的单位（部门）务必第一时间备案并签署责任书。我国在 2017 年 7 月 6 日发布关于进一步加强未备案网站管理工作的通知，要求通信管理局加大对未备案接入行为的处罚力度，发现一起，处理一起，采取“零容忍”态度。

针对“双非”信息资产，各单位（部门）需要注意：

1. 增强师生网络安全意识，普及网络安全知识；

2. 新增网站及时到信息管理中心进行备案操作；

3. 新上线系统必须经过安全检测通过才可上线；

4. 发现本单位“双非”信息资产必须及时进行备案，并签订“双非”系统安全责任书。

四、网信安全每月小结

本月我校信息系统漏洞总数量较少，因各部门响应处理及时，未

造成网络安全事件，但我校网站暗链外链问题十分严峻，暴露出我校网站中还存在大量过期的通知公告、网站链接及网站附件等内容。网站管理员需增加清理频率，杜绝僵尸网站的存在， 进一步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 5 月 12 日