2023 年网络与信息系统安全月报
（3 月）

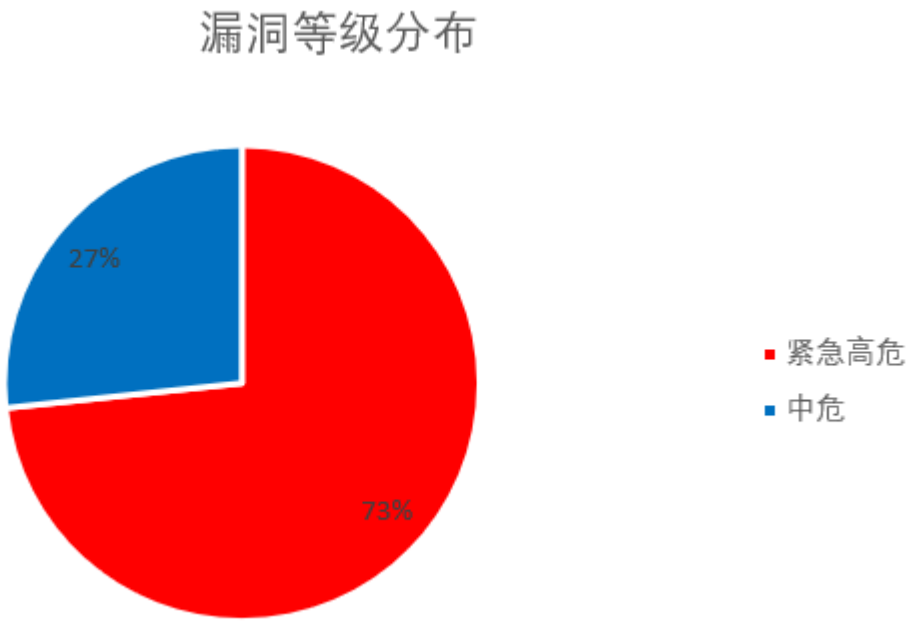
各单位、部门：

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 17 个。通过在校内网站监测、人工挖掘以及安全专项检查共发现漏洞 17 个，校外通报漏洞 0 个。其中紧急高危 13 个，中危漏洞 4 个，低危漏洞 0 个，紧急高危占比：73%。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

本月我校未收到第三方通报漏洞。

(三)非法外链情况

本月检查到 3 家单位所属网站共出现 5 次非法外链，具体情况如下：

网站（系统）	部门	频次	来源
http://tyxy.njtech.edu.cn/	体育学院	1 次	通信管理局
http://chem.njtech.edu.cn	化学与分子工程学院	2 次	通信管理局
http://life-phar.njtech.edu.cn/	生物与制药工程学院	1 次	校内自查
http://tyxy.njtech.edu.cn/	体育学院	1 次	校内自查

（四）重要时期网络安全安全保障

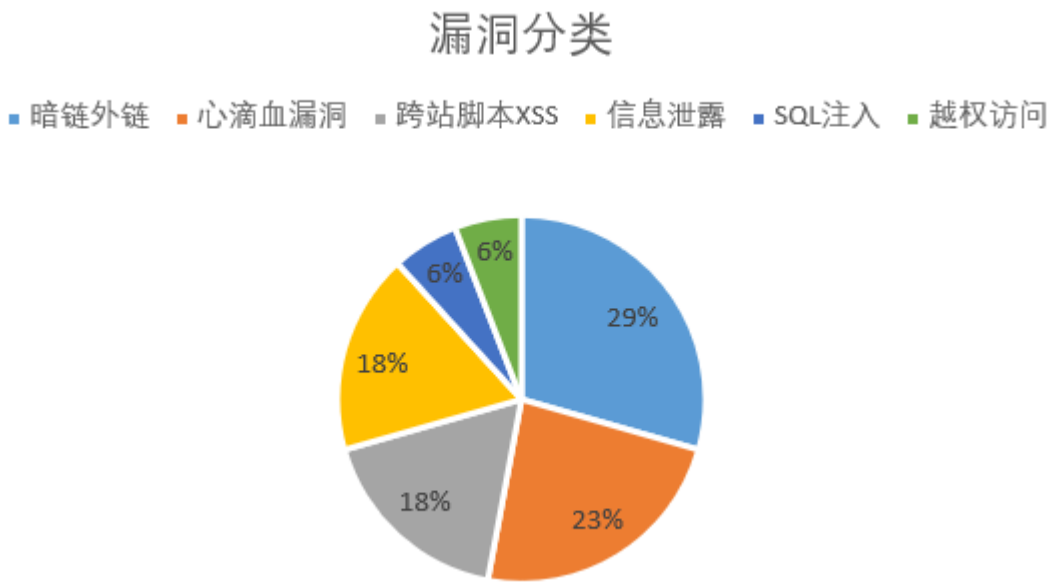
根据上级部门对重要时期网络安全保障工作的有关要求，结合学校实际，为有效保障学校网络信息安全，制订了 2023 年上

半年重要时期网络安全保障工作方案。在 3 月 3 日至 3 月 14 日进行重要时期的网络安全防护、组织人员开展安全值班工作，圆满完成了网络安全保障工作。

二、安全情况分析

(一)漏洞类型统计

本月共发现漏洞 17 个。其中心脏滴血漏洞 4 个，跨站脚本 XSS 漏洞 3 个，暗链外链 5 个，信息泄露 3 个，SQL 注入 1 个，越权访问 1 个。漏洞分类占比如下图：



(二)漏洞类型统计

本月共发现漏洞 17 个，均已修复。

三、安全威胁风险与防范

安全威胁风险	防范措施建议
自建网站存在严重漏洞	未在网站群上部署的自建网站，

	应先进行安全渗透测试，确认无安全漏洞后再开放服务。
系统软件版本过低导致出现严重漏洞	定期维护服务器应用软件，及时升级系统软件版本，避免未及时修复软件漏洞带来的高危风险。

四、网信安全每月小结

本月我校信息系统漏洞总数量较多，因各部门响应处理及时，未造成网络安全事件。本月安全漏洞主要是因为重要系统未及时更新软件而出现。各部门应督促系统开发商定期巡检，升级系统软件版本。各部门要高度重视网络安全工作，严格落实安全管理职责，摸清家底，精准施策，应对当前严峻复杂的国际形势；针对系统漏洞、网站暗外链、“双非”系统，要加强各部门的网站、系统、智能设备等的自查自纠，全流程掌握信息资产使用及管理维护状况，确保全校网络与信息系统持续安全稳定。

网络与信息系统安全联系电话：58139801。

信息管理中心

2023 年 4 月 6 日