2023 年网络与信息系统安全月报
（4 月）

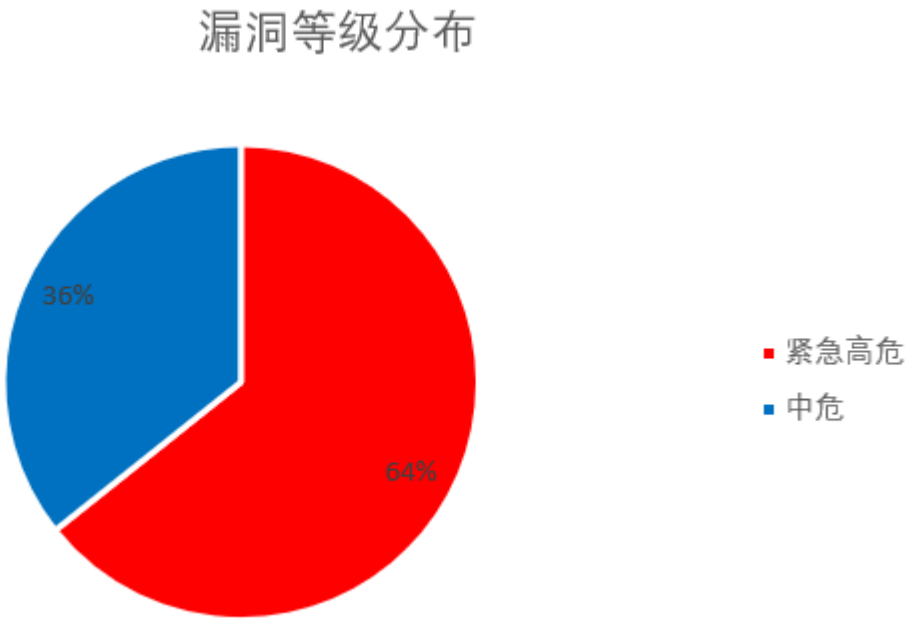
各单位、部门：

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 14 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 14 个，校外通报漏洞 0 个。其中紧急高危 9 个，中危漏洞 5 个，低危漏洞 0 个，紧急高危占比：64%。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 1 家单位所属网站共出现 3 次非法外链，具体情况如下：

网站（系统）	部门	频次	来源
http://life-phar.njtech.edu.cn/	生物与制药工程学院	3 次	通信管理局

(四)校外域名恶意解析

本月我校收到教育部通报：我校所属 IP 地址被校外域名恶意解析定向，违反了《互联网信息服务管理办法》(国务院令第 292 号)第四条规定，我校立即采取措施，对校外域名在边界防火墙采取了阻断访问措施。

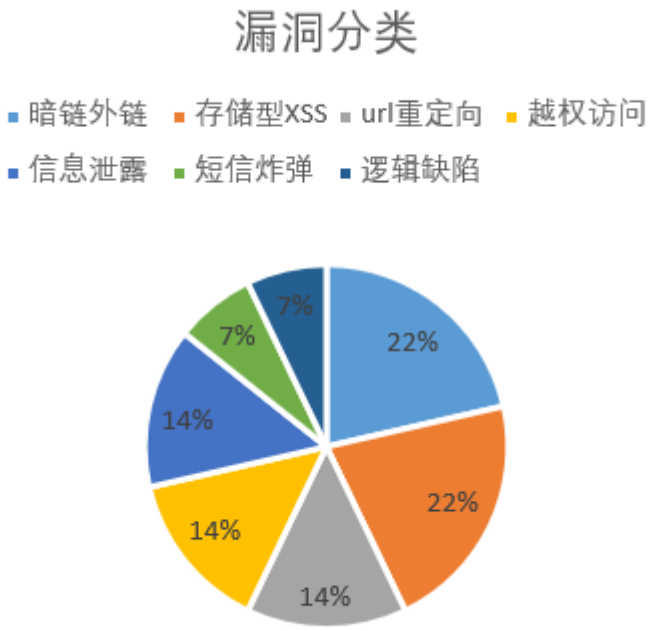
根据前面出现的情况，要求学校所有单位对外申请的域名必

须在信息管理中心进行备案，由信息管理中心统一下发学校子域名，不得私自绑定非学校域名对外提供服务。以免影响我校正常的互联网访问。

二、安全情况分析

(一)漏洞类型统计

本月共发现漏洞 14 个。其中暗链外链 3 个，存储型 XSS 3 个，url 重定向 2 个，越权访问 2 个，信息泄露 2 个，短信炸弹 1 个，逻辑缺陷 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 14 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
网站后台漏洞较多	对外开放系统定期进行漏洞扫描，及

	时处理漏洞避免被恶意利用。
网页存在暗链外链	网页上的外链域名存在过期后未及时续期，域名被抢注后被恶意利用，成为非法网站链接。 解决办法：定期排查网页外链，及时清除过期链接。

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。本月未出现弱口令等漏洞，网页暗链外链情况较上月也明显改善，请各单位继续保持。各部门、各单位要严格落实安全管理职责，摸清家底，精准施策，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 5 月 9 日