2023 年网络与信息系统安全月报
（5 月）

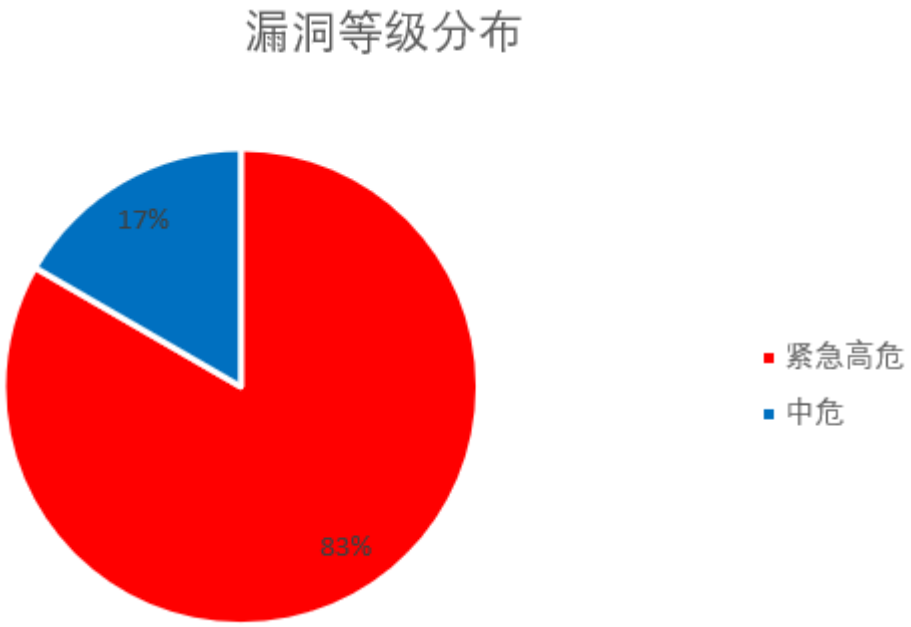
各单位、部门：

为进一步加强校园网络安全管理，保障校园网络安全，现将 5 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 18 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 0 个。其中紧急高危 15 个，中危漏洞 3 个，低危漏洞 0 个，紧急高危占比：83%。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

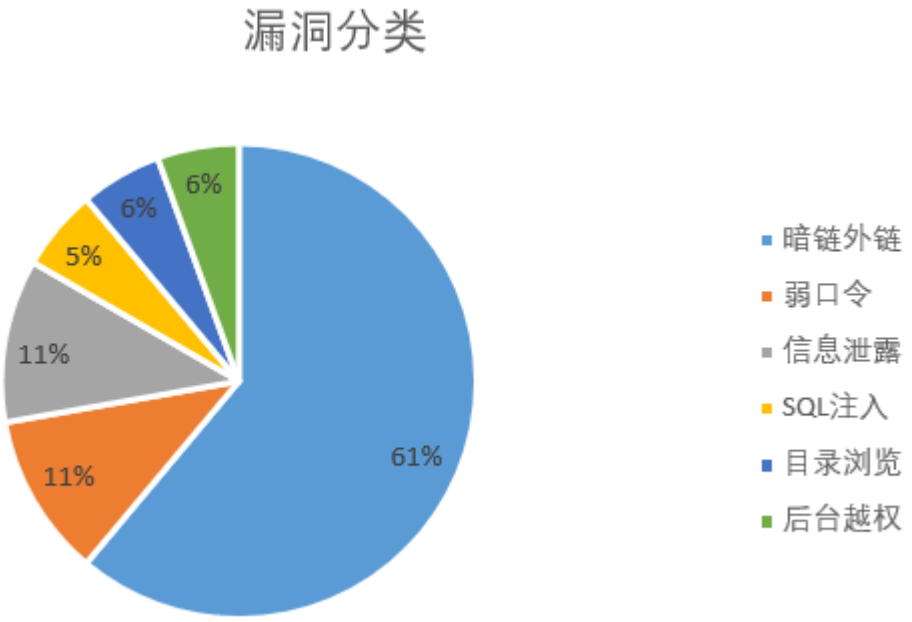
本月检查到 2 家单位所属网站共出现 11 次非法外链，具体情况如下：

网站（系统）	部门	频次	来源
http://spy.njtech.edu.cn/	食品与轻工学院	10 次	通信管理局
https://jwc.njtech.edu.cn	教务处	1 次	通信管理局

二、安全情况分析

(一)漏洞类型统计

本月共发现漏洞 18 个。其中暗链外链 11 个，弱口令 2 个，SQL 注入 1 个，目录浏览 1 个，后台越权 1 个，信息泄露 2 个。漏洞分类占比如下图：



(二)漏洞类型统计

本月共发现漏洞 18 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
网站弱口令较多	加强人员网络安全防范意识，定期修改网站登录密码。
网页存在暗链外链	定期排查网页外链，清除过期链接，避免被恶意抢注为非法网站。
网站配置文件泄露	服务器禁止备份网站文件，禁止将配置文件泄露到公网，加强网站访问目录权限限制。

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。各部门、各单位要严格落实学校网络安全责任制考核的要求，尽力排查存在的网络安全隐患，重点关注本单位系统和网站等信息资产的运行情况，尤其要加强对已经过保信息资产的安全管理，及时下线和关闭不再更新和使用的信息资产。各部门、各单位要层层压实责任，扎实开展工作，加强协同合作，共同维护学校网络安全。

网络与信息系统安全联系电话：58139801。

信息管理中心

2023 年 6 月 5 日