2022 年网络与信息系统安全月报

（4 月）

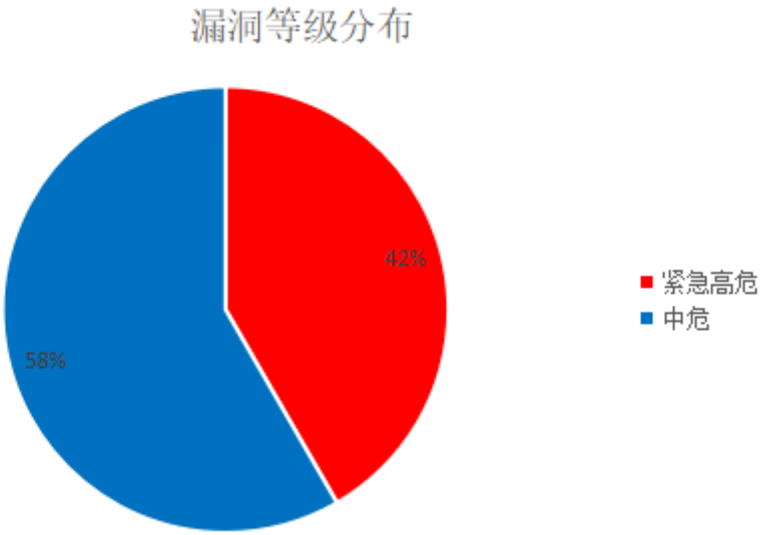
各单位、部门：

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 12 个，均为校内网站监测、人工挖掘以及安全专项检查测试发现，校外通报漏洞 0 个。其中紧急高危 5 个，中危漏洞 7 个，低危漏洞 0 个，紧急高危占比：42%。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

本月未收到第三方漏洞通报。

(三) 非法外链情况

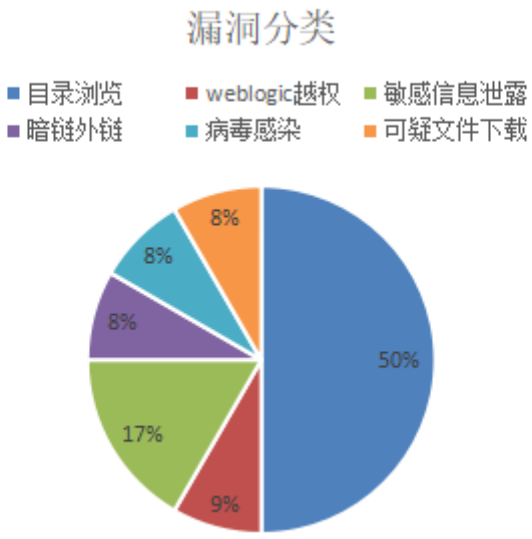
本月检查到 1 家单位所属网站共出现 1 次非法外链，具体情况如下：

网站（系统）	部门	频次
http://202.119.243.15/（实践教学综合管理平台）	教务处	1 次

二、安全情况分析

(一) 漏洞类型分析

本月发现的 12 个漏洞中，目录浏览 6 个，weblogic 越权 1 个，敏感信息泄露 2 个，暗链外链 1 个，病毒感染 1 个，可疑文件下载 1 个。漏洞分类占比如下图：



(二)漏洞修复情况

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
网页存在信息泄露	发布新闻附件中禁止填写身份证信息，如必须填写，必须将出身日期和最后两位模糊化。
部分危险端口对外开放	非常用端口对外开放，需经信息管理中心备案并检查。
系统存在弱口令	系统应设置强密码规则，不要使用简单密码作为初始密码，不要在网页上公布密码。
未完成报备，私自开设信息服务	部门在对外提供信息服务前，一定要确认信息资产完成报备手续，并按照要求完成安全检查。

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。各部门、各单位要严格落实安全管理职责，梳理本单位信息资产，及时清理僵尸系统和网站，做好风险防控，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：58139275。

信息管理中心

2022 年 5 月 4 日