# 2021 年网络与信息系统安全月报

# （8 月）

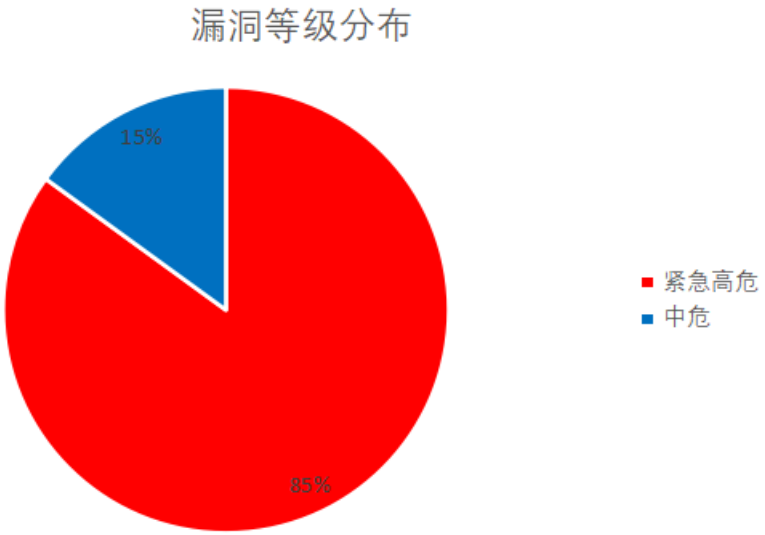
各单位、部门：

为进一步加强校园网络安全管理，保障校园网络安全，现将 8 月份网络与信息系统安全情况通报如下：

## 一、本月整体安全情况

### (一) 漏洞发现情况

本月共发现漏洞 20 个。通过在校内网站监测、人工挖掘以及安全专项检查测试发现漏洞 20 个，校外通报漏洞 0 个。其中紧急高危 17 个，中危漏洞 3 个，低危漏洞 0 个，紧急高危占比：85%。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平台通报漏洞。

## (三)非法外链情况

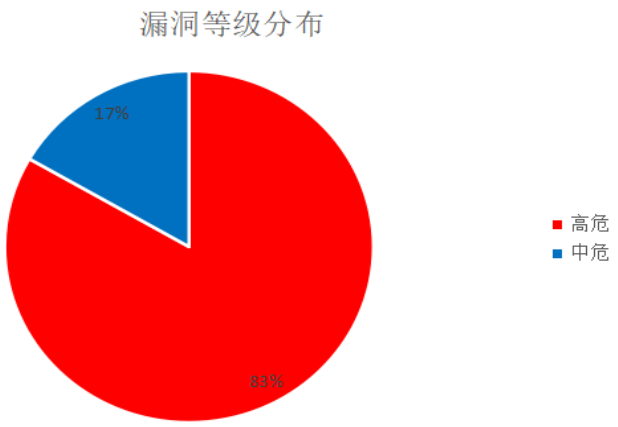
本月检查到 1 个系统及网站存在非法外链，具体情况如下：

| 网站（系统） | 部门 |
| --- | --- |
| http://en.njtech.edu.cn/ | 国际合作处 |

表一：非法外链汇总表

## (三)渗透测试

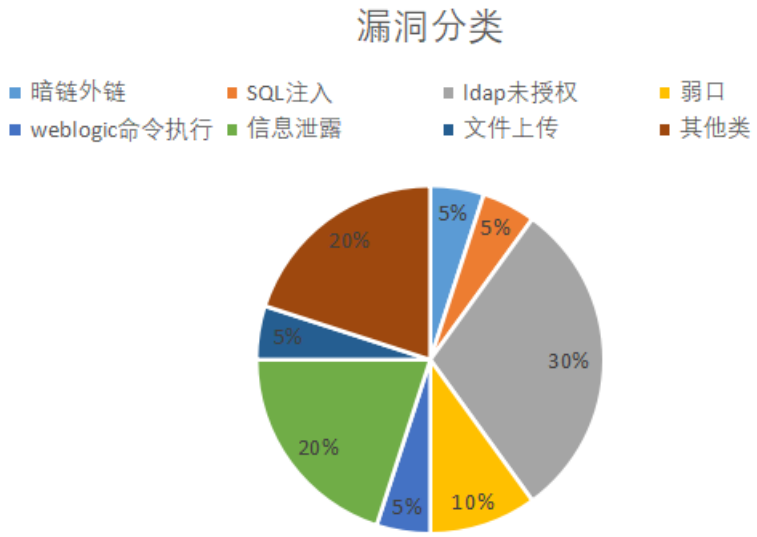
本月进行一个系统（科研管理系统）渗透测试，测试过程中，共发现 6 个漏洞，其中高危漏洞 5 个，中危漏洞 1 个，低危漏洞 0 个，目前漏洞已修复完毕。




## 二、安全情况分析

### (一)漏洞类型分析

本月共发现漏洞 20 个。其中暗链外链 1 个，SQL 注入 1 个，ldap 未授权 6 个，ftp 弱口令 2 个，weblogic 命令执行 1 个，信息泄露 4 个，文件上传 1 个，其他类漏洞 4 个。漏洞分类占比如下图：




### (二)漏洞修复情况

本月漏洞均已修复。

## 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 |
| --- | --- |
| 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。 |
| 不安全端口存在高危漏洞 | 加强运维管理，不必要对外开放的端口限制在本地访问。 |

## 四、网信安全每月小结

本月我校信息系统漏洞总量较少，各部门响应处理及时，未造成网络安全事件。但一些长期强调的网络安全问题，如弱口令，高危端口存在多个未授权漏洞，多个系统存在敏感信息泄露等仍然存在，对信息系统（网站）正常运行造成很大安全隐患，需要重点关注，并积极排查整改，确保全校信息系统（网站）及数据安全。

网络与信息系统安全联系电话：58139275,83172363。

信息管理中心

2021 年 9 月 1 日