

# 2019 年度南京财经大学网络安全 服务 信息安全月报(9 月)



赛尔网络有限公司江苏分公司

二〇一九年十月

## 目 录

|                      |    |
|----------------------|----|
| 目 录 .....            | 2  |
| 相关说明 .....           | 3  |
| 测试人员 .....           | 3  |
| 本月工作内容概况 .....       | 4  |
| 1.1. 网站监测情况 .....    | 5  |
| 1.2. 风险趋势 .....      | 6  |
| 1.3. 第三方漏洞监测情况 ..... | 7  |
| 1.4. 资产信息情况 .....    | 8  |
| 漏洞情况分析 .....         | 9  |
| 1.5. 整体漏洞趋势 .....    | 9  |
| 1.6. 风险修复情况分析 .....  | 10 |
| 1.7. 风险等级分布 .....    | 10 |
| 应急响应事件分析 .....       | 11 |
| 风险预警 .....           | 12 |
| 工作计划 .....           | 14 |

## 相关说明

本文档是由“赛尔网络”于 2019 年 9 月 30 日针对南京财经大学进行安全服务工作所提交的报告资料。

## 测试人员

赛尔网络组成渗透测试小组，由信息资深安全服务工程师主要参与，安全服务部相关工作人员配合。

项目组成人员如下：

| 项目角色 | 姓名  | 职务      | 联系方式        | 项目职责 |
|------|-----|---------|-------------|------|
| 项目经理 | 江东  | 安全服务工程师 | 13260911761 | 安全服务 |
| 安全服务 | 刘巛  | 安全服务工程师 | 15295767969 | 安全服务 |
| 安全服务 | 方文斌 | 安全服务工程师 |             | 安全服务 |
| 安全服务 | 吕翌澍 | 安全服务工程师 |             | 安全服务 |
| 安全服务 | 冯丹  | 安全服务工程师 |             | 安全服务 |
| 安全服务 | 赵军洋 | 安全服务工程师 |             | 安全服务 |

## 本月工作内容概况

综合各类服务项目情况，目前南京财经大学网站安全态势总体评价为良。

除了日常的漏洞扫描和监测工作外，结合上月月报内容，本月与各位老师讨论确定，还重点开展了以下工作：

1. 对 hdmool 网站进行系统预警排查工作并形成漏洞报告输出。
2. 在 9 号至 12 号期间省攻防演练保障学校网站，并对学校部分网站进行抽查工作，未发现相关漏洞。
3. 现场项目启动会展开，提出项目进展过程中所需的相关设备与资料。
4. 部署监测平台并布置监测任务。
5. 通过 dns 的记录对学校资产进行资产梳理工作，形成域名与 ip 的一一对应。

# 本月整体安全情况

## 1.1. 网站监测情况

本月对现梳理的 327 个网站资产进行了 1 轮监测，其中包括可用性监测、敏感词监测、安全事件监测和漏洞监测。



敏感词扫描监测结果：

对现有 327 个资产进行每天监测并人工排查，经过核实未发现真实存在的敏感词。

| <input type="checkbox"/> | 任务名称   | 监测数量 | 监测频率       | 创建时间                 | 更新时间                 | 开关                                  | 任务状态 | 创建者      |
|--------------------------|--------|------|------------|----------------------|----------------------|-------------------------------------|------|----------|
| <input type="checkbox"/> | ▲ 2019 | 327  | 每天23:52:17 | 2019-09-24 08:23:... | 2019-10-10 01:12:... | <input checked="" type="checkbox"/> | 已完成  | operator |

安全事件监测扫描结果：

对现有 327 个网站进行监测并人工进行排查，未发现真实存在的篡改和暗链；

| 网站名称 | 网站地址                        | 篡改 | 暗链 | 网马 | IP地址            | 地理位置 | 更新时间     |
|------|-----------------------------|----|----|----|-----------------|------|----------|
| 59   | http://219.219.191.229:8089 | 1  | 0  | 0  | 219.219.191.229 | 南京   | 2019-10- |
| 173  | http://219.219.191.251      | 1  | 0  | 0  | 219.219.191.251 | 南京   | 2019-10- |
| 72   | http://210.28.81.66:8094    | 0  | 0  | 0  | 210.28.81.66    | 南京   | 2019-10- |
| 327  | http://oldwww.nufe.edu.cn   | 0  | 0  | 0  | 210.28.80.3     | 南京   | 2019-10- |
| 71   | http://219.219.180.166      | 0  | 0  | 0  | 219.219.180.166 | 南京   | 2019-10- |
| 326  | http://mail.stu.nufe.edu.cn | 0  | 0  | 0  | 223.252.214.105 | 杭州   | 2019-10- |

## 1.2. 风险趋势

其中在 2019 年 9 月 1 日到 2019 年 9 月 30 日对全月对学校外网网站进行安全检查工作，未发现篡改事件。

### 1.3. 第三方漏洞监测情况

本月学校未接收到教育 src 的通告，并查看教育 src、补天等第三方漏洞平台，未发现存在南京财经大学的漏洞信息。

## 1.4. 资产信息情况

截止 2019 年 9 月 30 日，根据资产梳理分析南京财经大学的资产情况，现阶段总资产 456 个及对应用系统资产表中 327 个应用系统进行了安全扫描；后期总资产在数量上会有小幅度的变化，此时资产梳理工作将持续进行。

# 漏洞情况分析

## 1.5. 整体漏洞趋势

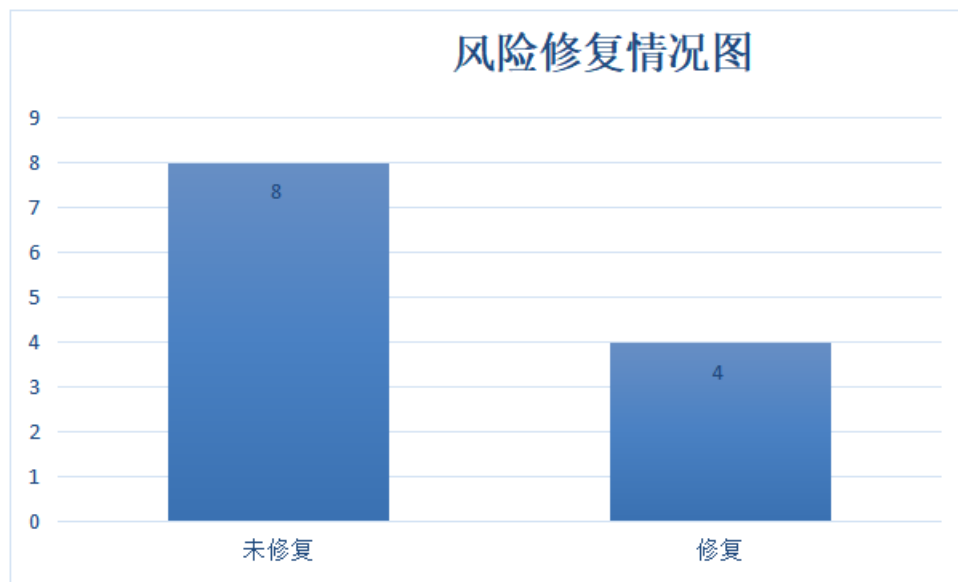
经过长期监测与渗透测试工作，发现南京财经大学存在 12 个漏洞。其中紧急漏洞为 5 个，高危漏洞为 3 个，中危漏洞为 1 个，低危漏洞为 3 个。

下表为本月漏洞简介

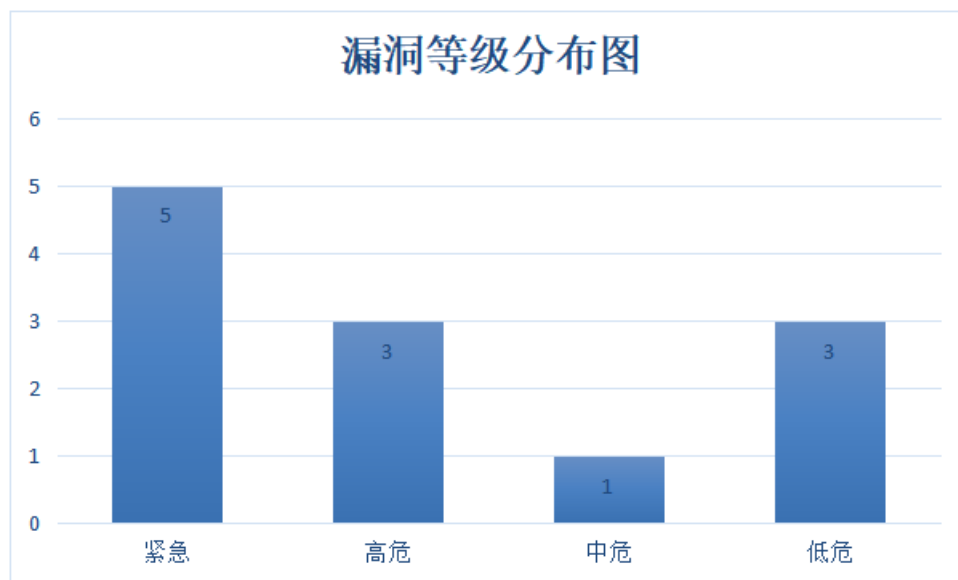
| 域名                      | 应用系统 | 风险名称                | 风险等级 | 发现时间      | 复测时间       | 复测结果 |
|-------------------------|------|---------------------|------|-----------|------------|------|
| http://nufe.hdmoool.com |      | 跨站脚本                | 高危   | 2019/9/2  | 2019/10/10 | 修复   |
|                         |      | 允许任何域的 flash 文件访问资源 | 低危   | 2019/9/2  | 2019/10/10 | 修复   |
| http://lgb.nufe.edu.cn  | 关工委  | 暗链                  | 紧急   | 2019/9/3  | 2019/10/10 | 修复   |
| 219.219.191.228:9988    |      | 链接注入                | 高危   | 2019/9/29 | 2019/10/10 | 未修复  |
|                         |      | 跨站脚本                | 高危   | 2019/9/29 | 2019/10/10 | 未修复  |
|                         |      | 信息泄露                | 低危   | 2019/9/29 | 2019/10/10 | 未修复  |
| 219.219.180.90          |      | 信息泄露                | 低危   | 2019/9/29 | 2019/10/10 | 未修复  |
| 219.219.191.242         |      | Sql 注入              | 紧急   | 2019/9/29 | 2019/10/10 | 未修复  |
|                         |      | 弱口令                 | 紧急   | 2019/9/29 | 2019/10/10 | 未修复  |
|                         |      | 文件上传                | 紧急   | 2019/9/29 | 2019/10/10 | 未修复  |
|                         |      | 信息泄露                | 中危   | 2019/9/29 | 2019/10/10 | 未修复  |
| lib.nufe.edu.cn         |      | 后门                  | 紧急   | 2019/9/29 | 2019/10/10 | 修复   |

## 1.6. 风险修复情况分析

风险数量为 12 个，其中 9 个漏洞在 9 月 29 日以漏洞报告形式输出给学校，其中未修复域名有：219.219.191.228:9988、219.219.180.90、219.219.191.242



## 1.7. 风险等级分布



## 应急响应事件分析

本月无应急响应事件。

# 风险预警

## phpstudy 后门预警

### 1.phpstudy 介绍

Phpstudy 是国内的一款免费的 PHP 调试环境的程序集成包，其通过集成 Apache、PHP、MySQL、phpMyAdmin 不同版本软件于一身，一次性安装无需配置即可直接使用，具有 PHP 环境调试和 PHP 开发功能。

### 2.后门事件

2018 年 12 月 4 日，西湖区公安分局网警大队接报案，某公司发现公司内有 20 余台计算机被执行危险命令，疑似远程控制抓取账号密码等计算机数据回传大量敏感信息。通过专业技术溯源进行分析，查明了数据回传的信息种类、原理方法、存储位置，并聘请了第三方鉴定机构对软件中的“后门”进行司法鉴定，鉴定结果是该“后门”文件具有控制计算机的功能，嫌疑人已通过该后门远程控制下载运行脚本实现收集用户个人信息。

### 3.影响版本

声明 phpstudy 2016 版 PHP5.4 存在后门。

官网下载 phpstudy2018 版 php-5.2.17 和 php-5.4.45 也同样存在后门

### 4.后门检测方法

通过分析，后门代码存在于\ext\php\_xmlrpc.dll 模块中

phpStudy2016 和 phpStudy2018 自带的 php-5.2.17、php-5.4.45

phpStudy2016 路径

php\php-5.2.17\ext\php\_xmlrpc.dll

php\php-5.4.45\ext\php\_xmlrpc.dll

phpStudy2018 路径

PHPTutorial\php\php-5.2.17\ext\php\_xmlrpc.dll

PHPTutorial\php\php-5.4.45\ext\php\_xmlrpc.dll

用 notepad 打开此文件查找@eval，文件存在@eval(%s( '%s' ))证明漏洞存在

### 5.漏洞修复

可以从 PHP 官网下载原始 php-5.4.45 版本或 php-5.2.17 版本，替换其中的 php\_xmlrpc.dll，下载地址：

<https://windows.php.net/downloads/releases/archives/php-5.2.17-Win32-VC6-x86.zip>

<https://windows.php.net/downloads/releases/archives/php-5.4.45-Win32-VC9-x86.zip>

或者去官网下载更新最新的 phpstudy 软件

## 6.技术支持

配合学校进行排查工作

# 工作计划

资产梳理工作