附件一

DREAD 模型

充分考虑漏洞被利用的难易程度以及对学校网络和系统的 影响情况，采取 DREAD 模型对安全漏洞进行风险等级划分，并对 各级别漏洞进行举例。

（ 一）在量化风险的过程中，对每个威胁进行评分，并按照 如下公式计算风险值：

Risk = D + R + E + A + D

表 1 安全漏洞等级评估模型

|  |
| --- |
| **DREAD** 模型 |
| 类别 等级 | 高（**3**） | 中（**2**） | 低（ **1**） |
| **D**amagePotential潜在危害 | 获取完全权限；执行管理 员操作；非法上传文件等 | 泄露敏感信息 | 泄露其他信息 |
| **R**eproducibility 重复利用可能性 | 攻击者可以随意再次攻击 | 攻击者可以重复攻击， 但有时间或其他条件限制 | 攻击者很难重复攻击过程 |
| **E**xploitability 利用的困难程度 | 初学者在短期内能掌握攻击方法 | 熟练的攻击者才能完成这次攻击 | 漏洞利用条件非常苛刻 |
| **A**ffected users 影响的用户范围 | 所有用户，默认配置，关键用户 | 部分用户，非默认配置 | 极少数用户，匿名用户 |
| **D**iscoverability 发现的难易程度 | 漏洞很显眼，攻击条件很 容易获得 | 在私有区域，部分人能 看到，需要深入挖掘漏 洞 | 发现该漏洞极其困难 |
| 说明：每一项都有 3个等级，对应着权重，从而形成了一个矩阵。 |

（ 二）最后得出安全漏洞风险等级。

表 2 风险等级对应分数

|  |  |
| --- | --- |
| 计算得分 | 安全漏洞风险等级 |
| 0-5 分 | 低风险 |
| 6- 10 分 | 中风险 |
| 11- 13 分 | 高风险 |
| 14- 15 分 | 紧急 |

（ 三） 各级别漏洞案例参考。

表 3 各级别漏洞案例

|  |  |
| --- | --- |
| 风险等级 | 评级标准 |
| 紧急 | 直接获取系统权限的漏洞（服务器权限、客户端权限）。包括但不仅限于远程命令执行、任意代码执行、上传获取 webshell 、SQL注入获取系统权限、缓冲区溢出（包括可利用的ActiveX 缓冲区溢出）。浏览器use after free 漏洞、远程内核代码执行漏洞以及其它因逻辑问题导致的远程代码执行漏洞。 |
| 直接获取重要业务或通用系统权限的漏洞（服务器权限、客户端权限）如： struts。 |
| 严重的敏感信息泄漏。包括但不仅限于核心DB （资金、身份、交易相关）的SQL注入漏洞。 |
| 高 | 直接导致业务拒绝服务的漏洞。包括但不仅限于远程拒绝服务漏洞。 |
| 严重的逻辑设计缺陷和流程缺陷。包括但不仅限于伪造任意号码发送 消息、任意账号资金消费、任意账号密码修改漏洞。 |
| 敏感信息泄漏。包括但不仅限于非核心 DB SQL注入、源代码压缩包 泄漏、可获取大量用户交易信息的接 口、服务器、应用加密可逆或明文的敏感信息泄露。 |

|  |  |
| --- | --- |
| 风险等级 | 评级标准 |
|  | 越权访问。包括但不仅限于绕过认证直接访问管理后台、后台弱密码。 |
| 大范围影响用户的其他漏洞。包括但不仅限于可造成自动传播的存储 型 XSS （包括存储型 DOM-XSS）、涉及交易、资金、密码的 CSRF。 |
| 影响到服务器的本地提权漏洞。 |
| 能直接盗取用户身份信息的漏洞。包括重要业务（如在线、EPOS 、委 托结算、无卡支付等）的重点页面的存储型XSS漏洞、普通站点的SQL 注入漏洞。 |
| 中 | 需交互方可影响用户的漏洞。包括但不仅限于反射型 XSS（包括反射 型 DOM-XSS）、CSRF 、URL跳转漏洞。 |
| 本地拒绝服务漏洞。包括但不仅限于客户端本地拒绝服务（解析文件 格式、网络协议产生的崩溃） 。 |
| 普通越权操作。包括但不仅限于不正确的直接对象引用。 |
| 普通信息泄漏。包括但不仅限于客户端明文存储密码、客户端密码明 文传输以及 web 路径遍历、系统路径遍历。 |
| 普通的逻辑设计缺陷和流程缺陷。 |
| 低 | 轻微信息泄漏。包括但不仅限于路径信息泄漏、文件信息泄露、异常 信息泄露。 |
| 难以利用但存在安全隐患的漏洞。包括但不仅限于可引起传播和利用 的Self-XSS。 |

附件二

安全漏洞整改时效

（ 一）应用系统安全漏洞整改时效要求如下：

|  |  |
| --- | --- |
| 应用系统安全级别 | 整改时效 |
| 紧急风险漏洞 | 高风险漏洞 | 中风险安全漏洞 |
| 高级 | 3 个工作日 | 5 个工作日 | 10 个工作日 |
| 中级 | 5 个工作日 | 10 个工作日 | 10 个工作日 |
| 低级 | 1 个月内 | 1 个月内 | 1 个月内 |

（ 二）操作系统安全漏洞整改时效要求如下：

|  |  |
| --- | --- |
| 所处网络区域 | 整改时效 |
| 紧急或高风险漏洞 | 中风险漏洞 |
| 对外提供服务区域 | Window 操 作 系 统 3 个 月 内 ； Linux&unix 操作系统 6 个月内； 对于影响特别严重，易受攻击的 漏洞，根据网络与信息中心的通告立即整 改完成。 | Window 操作系统 3 个月 内 ；Linux&unix 操作系 统 6 个月内。 |
| 对内提供服务区域 | Window 操 作 系 统 6 个 月 内 ； Linux&unix 操作系统 12 个月内； 对于影响特别严重，易受攻击的 漏洞，根据网络与信息中心的通告立即整 改完成。 | Window 操作系统 6 个月 内 ；Linux&unix 操作系 统 12 个月内。 |

附件三

漏洞处理流程



附件四

|  |
| --- |
| 周口文理职业学院网络安全隐患整改通知书〔20XX〕第 XXX 号XXX 部门：经 XXXX 检测发现，你单位所属 XXXX系统存在高危漏洞和安全 隐患（见附件），请立即组织技术力量进行整改、清理，尽快消除安全隐患，并按照国家信息安全等级保护制度和公安机关政府网站安全监管工作规范的相关要求，对网站/信息系统进行全面检测和安全整改。请于 XXXX年 X月 X日 XX时前，将网络安全隐患整改情况反馈表（见附件）通过学校办公系统发送至网络与信息中心 XXX邮箱。在网络安全隐患整改期间，学校将采取必要的安全保护管理和技 术措施，确保全校网络与信息系统安全。联系人： XXX 联系电话： XXX技术联系人： XXX 联系电话： XXX网络与信息中心XXXX年X月X 日附件： 漏洞检测报告 |

一式两份，一份交被检查单位，一份网络与信息中心留存。

附件五

网络安全隐患整改情况反馈表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 单位名称 |  |  | 联系人 |  |
| 联系电话 |  |  | 电子邮箱 |  |
| 安全隐患网站或信息系统名称 |  |  |
| 域名或 URL |  |  |
| 安全隐患整改情况 |  |  |
| 今后防范措施 |  |  |
| 网络安全分管领导签字： |  |
| 年 月 日（单位盖章） |