## 应用上线安全检查申请表

1. 应用基本信息

***以下应用管理员填写***

|  |  |  |  |
| --- | --- | --- | --- |
| 应用名称 |  | | |
| 申请域名 |  | | |
| 所属院系 |  | | |
| IP地址 |  | | |
| 项目负责人 |  | 联系方式 |  |
| 应用管理员 |  | 联系方式 |  |
| 网站扫描方式 | □ 源代码扫描 □ 直接扫描网站（提供网站访问方式） | | |
| 访问范围 | □ 开放 □ 受限 □ 校内 □ 限定 | | |
| 访问对象 | □ 匿名 □ 教师 □ 学生 □ 自定义用户 | | |

1. 应用安全检查情况

***以下应用管理员填写***

1. 手工检查

|  |  |
| --- | --- |
| **检查内容** | **检查结果** |
| 进行代码清理（确保代码中不包含测试、备份、历史等与应用运行无关的文件） | 无 |
| 应用管理用户清理（确保上线系统中不存在无用用户，不存在简单密码用户） | 无 |
| 恶意代码检查（确保代码中不存在已被注入的恶意代码） | 无 |
| 权限检查（确保程序进行了正确的权限控制） | 无 |

项目负责人签字：

1. 应用安全参数

***以下应用管理员填写***

1. 应用使用的第三方控件

|  |  |
| --- | --- |
| 控件名称（版本） |  |
| 控件用途说明 |  |

*（每个控件单独填写）*

1. 用户上传文件（包括第三方控件中用户上传文件的功能）

|  |  |
| --- | --- |
| 上传页面访问地址 | /user\_list/ |
| 上传内容限制 | □ 白名单 □ 黑名单 |
| 页面访问限制 | □ 匿名 □ 登录用户 ☑ 特定用户： 管理员 |
| 上传文件存放方式 | ☑ 数据库 ☑ 本地磁盘，路径： /media/ |

|  |  |
| --- | --- |
| 上传页面访问地址 | /survey/ |
| 上传内容限制 | □ 白名单 □ 黑名单 |
| 页面访问限制 | □ 匿名 □ 登录用户 ☑ 特定用户： 管理员 |
| 上传文件存放方式 | □ 数据库 ☑ 本地磁盘，路径： /media/ |

*（每个上传控件单独填写）*

1. 后台管理程序

|  |  |
| --- | --- |
| 后台管理入口 |  |
| 后台管理用户 |  |
| 访问限制范围 |  |
| 访问限制方式 |  |

1. 用户上传文件访问控制

|  |  |
| --- | --- |
| 用户上传文件的保存路径 | /media/ |
| 访问方式及权限限制（操作系统级文件权限控制或者程序级权限控制） | 程序级权限控制 |

*（每处上传路径单独填写）*

加WAF需要列出的例外URL

|  |  |
| --- | --- |
| 是否启用Web防火墙防护： □ 是 □ 否 | |
| 例外IP地址 |  |
| 例外URL地址 |  |

*（2A、2B级应用必须启用Web应用防火墙，此处针对可能被Web应用防火墙拦截的正常业务提供不检测的IP或页面URL）*

1. 安全检查结果审核

***以下安全管理员填写***

根据上述检查结果，建议应用作如下修改：

修改完成后允许上线运行。

安全管理员签字

1. 应用安全运行方案

***以下安全管理员填写***

|  |  |  |
| --- | --- | --- |
| 应用运行隔离方案 |  | |
| 是否启用Web防火墙防护： □ 是 □ 否 | | |
| 应用访问控制方案 | 端口访问控制 |  |
| 目录访问控制 |  |
| 目录权限控制 |  |