**系统上线前安全自查表**

|  |
| --- |
| **南昌大学\_\_\_\_\_\_\_\_\_\_\_\_\_\_系统上线前安全自查表** |
| 网站域名（IP)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（ \_\_\_\_\_\_\_\_\_）  |
| 自评时间 :\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 自评人员:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  |
| **序号** | **测试项目** | **测试内容** | **结果** | **测试概况** |
| 1 | 基础安全 | 双因素认证，确认登陆界面是否使用用户名+密码+复杂验证码等方式认证。 |  |  |
| 2 | 字符过滤，确认对于特殊字符，非法字符是否有基本安全过滤。 |  |  |
| 3 | 安全防护，确认新系统是否有Waf，网站安全卫士等各类型防护手段。 |  |  |
| 4 | 明文传输，设计密码等敏感信息传输是否存在明文传输现象。 |  |  |
| 5 | 敏感数据模糊化，对于身份证，家庭住址，银行卡等各类型敏感信息是否做模糊化处理。 |  |  |
| 6 | 密码策略，涉及密码模块是否是8位以上，有数字，字母，大小写等复杂规则。 |  |  |
| 7 | 弱口令 | 用户弱口令（注册用户，默认用户等其他用户） |  |  |
| 8 | Tomcat，Weblogic，Jboss等各类型中间件管理控制台弱口令 |  |  |
| 9 | 管理后台弱口令 |  |  |
| 10 | 目录分析 | 确认目录中没有测试信息，备份信息，敏感身份等信息页面 |  |  |
| 11 | 端口信息 | 确认开放端口情况，遵守最小化原则。 |  |  |
| 12 | 框架安全 | 确认开发所用框架，中间件为最新安全版本，如STRUCT2，weblogic等 |  |  |
| 请各单位新系统上线前进行基本的安全自查，以上结果中填写：符合，不符合，不确定，不适用。测试情况中可以根据实际情况进行描述，备注。 |