安全评测前技术要求

一、系统要求

（一）操作系统

操作系统须保证为正常上线系统，并更新为最新；禁止采用失去技术升级的系统如：windows2003、Windows2008、centos 等；

（二）服务器权限

1. 在本机关闭不需要的端口,设置类似host.allow,host.deny等策略，对于访问的源地址进行限制。参考如下：

```
sudo systemctl status firewalld
# 添加允许的 IP 地址
sudo firewall-cmd --permanent --zone=public --add-source=202.204.*.*
# 开放 HTTP 和 SSH 端口
sudo firewall-cmd --permanent --zone=public --add-port=80/tcp
sudo firewall-cmd --permanent --zone=public --add-port=22/tcp
sudo firewall-cmd --permanent --zone=public
```

--add-port=443/tcp

重新加载防火墙规则

sudo firewall-cmd --reload

查看当前状态

sudo firewall-cmd --state

查看当前配置的规则

sudo firewall-cmd --list-all

sudo systemctl start firewalld

sudo systemctl enable firewalld

2. 数据库和应用系统如在同一台服务器，须采用本机回路进行访问;如前端及数据库分为不同服务器,须设置本机防火墙访问规则,严禁非前端服务器访问数据库网络端口;

3. 使用最低权限的数据库用户作为 web 应用所需，严禁具有不必要的额外权限;

（三）系统配置

1. 对用户输入进行严格有效过滤,防止 sql 注入，xss 跨站脚本,命令执行，crsf 跨站请求伪造等，建议采用白名单过滤策略;

2. 密码复杂度要求：系统必须有密码复杂度检查模块，设置有效的验证码或者滑动等手段防止暴力破解,严格限制密码长度大于8位,含字母（大小写）、数字及符号组合，重要系统须采用二次认证；严禁

在数据库中明文存放用户密码，需进行带 salt 的哈希之后入库；对于多次错误登陆进行封堵;

3. 系统中严禁暴露配置信息（如数据库连接信息），源码备份文件，.git、.svn 仓库等;

4. 个人敏感信息需要做加密存储，不得随意明文传输、明文展示，确需展示应设置密码查看，历史数据应消亡，对于个人信息使用应具有知情协议书，参考《校务数据管理办法》、《个人信息保护法》等。

5. 登录界面不可保留账号密码

6. 关于系统登录入口：方案一：移除系统自身登录入口，接入学校统一身份认证平台，减少单一密码泄露风险；方案二：保留入口，设定密码策略，禁止弱密码登录，并开启多因子身份认证登录。

7. 数据库等设置强密码。

（四）系统运维及上线

1. 系统上线建议安装 edr，日志数据须接入校内日志审计平台。

2. 系统需完成开发后方可进行安全测评，测试系统与正式上线系统一致，无各种调试或报错信息（如：断点，printf 等调试信息），系统需删除系统默认安装的各种例程、文档及管理程序。

3. 接到系统安全评测或渗透报告后须提供详实可行的整改报告，整改没问题后方可上线。

4. 服务器运维需经由堡垒机。

二、系统测评需提供信息

操作系统版本及补丁情况；开放的网络端口及用途；所有第三方的中间件、开发包、数据库、服务版本及管理地址、密码（必须为复杂密码评测后更改）如：tomcat 版本 8.0，apache2.4.2，jquery3.1.0，mysql5.0；系统访问路径；系统的用户登录路径；系统的管理端路径。

备注：如果安装了杀毒软件或者其他防火墙，在评测期间请先行关闭。