哈尔滨工程大学信息化处文件

信息化处发〔2022〕 21 号

关于印发《网站、信息系统上线安全检查规范》的通知

各办公室：

《网站、信息系统上线安全检查规范》经 2022 年第 14 次处长办公会讨论通过，现印发给你们，请认真贯彻执行。

哈尔滨工程大学信息化处

2022 年 6 月 8 日

网站、信息系统上线安全检查规范

第一章　总 则

第一条 为加强哈尔滨工程大学网站、信息系统运行的安全性、可靠性和稳定性，在网站、信息系统上线前及时发现和封堵可能存在的安全威胁，制定本规范。

第二条 系统上线需由系统责任单位提交安全测试要求相关信息，由信息化处进行安全测试和评估，测试后反馈系统整改建议，系统责任单位按照整改建议对系统进行整改，并提供详实的整改报告，由信息化处验证整改，系统达到安全条件后，方可上线。在系统进行较大版本升级时，系统责任单位需重新提交测试。

第二章　系统架构安全检查

第三条 系统须为正常上线系统，须更新为最新版本。禁止采用失去技术升级保护的操作系统(如windows 2003等低版本)。禁止采用含有已知漏洞的组件、应用程序、框架（如：Struts2存在安全漏洞的版本）、应用程序服务器、web 服务器、数据库服务器等。以上系统必须执行安全配置，禁止默认安装。所有的软件应该保持及时更新。

第四条 启用本机防火墙，关闭不必要端口。从本机关闭不需要的端口（如：关闭 windows netbios 等服务），原则对外服务端口只开放80、8080、443。

设置本机防火墙如 iptable 对于访问的源地址进行限制，

同时相关服务设置类似 host.allow,host.deny 等策略。

第五条 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，禁止非前端服务器访问数据库网络端口。

第六条 使用最低权限的数据库用户作为 web 应用所需，禁止具有不必要的额外权限。

第七条 使用标准端口提供 http 或 https 服务。保证系统服务正常与上线系统一致,无各种调试、报错信息(如:断点,printf 等调试信息)及注释信息,系统需删除系统默认安装的各种例程、文档及管理程序。删除 Tomcat 的 manager/html 登录页面和相关默认测试页面。

第八条 系统中应禁止暴露配置信息(如数据库连接信息)，源码备份文件，.git 或.svn 仓库等。

第九条 系统中应避免安装不必要的软件。

第三章　网站、信息系统安全检查

第十条 禁止在网站中使用 FCKeditor、eWebeditor 在线文本编辑器。

第十一条 关闭网站所有 Debug 模式，设置友好返回界面。

第十二条 删除网站、信息系统上的所有测试账号，修改网站初始密码。

第十三条 网站登录后的 cookie 需设有 HTTPOnly 属性。

第十四条 禁止在 HTTP 请求中以明文或可逆编码（如：

base64、url 编码等)的形式传递 SQL 语句到后端程序代入执行，禁止由 Web 前端直接生成和传递 SQL 语句到数据库执行，数据库查询必须采用预编译和参数结构化查询。

第十五条 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。禁止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。

第十六条 对于生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感信息禁止在数据库中明文存放。

第十七条 严格控制上传点，尽量禁止让 web 用户直接访问传文件夹，改用程序输出访问。上传目录不能有执行权限，原则上不允许有未经登陆验证的上传点。应对于上传文件类型和目录进行严格控制（禁止用前端的 js 进行控制），文件同时上传目录不能有执行权限。

第十八条 设置有效的身份认证、会话管理及访问控制机制，防止越权及提权，禁止利用 js 进行控制及验证。

第四章 附 则

第十九条 本规范自发布之日起施行。由信息化处网络信息安全办公室负责解释和修订。

哈尔滨工程大学网站、信息系统安全测评信息登记表

填表日期：　　年　月　日

<table>
<tr><td>单位名称</td><td colspan="6"></td></tr>
<tr><td>网站、系统名称</td><td colspan="6"></td></tr>
<tr><td>技术支持/建设公司</td><td colspan="6"></td></tr>
<tr><td>基本信息</td><td>操作系统：</td><td colspan="2"></td><td>版本号：</td><td colspan="2"></td></tr>
<tr><td rowspan="5">开放的网络端口及用途</td><td>端口</td><td colspan="3">开放范围</td><td colspan="2">用途</td></tr>
<tr><td></td><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td></td><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td></td><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td></td><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td rowspan="5">中间件、开发包、数据库</td><td>类型</td><td>版本</td><td>账号</td><td>密码</td><td>备注</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>开源组件</td><td colspan="6"></td></tr>
<tr><td rowspan="4">访问信息</td><td>访问路径</td><td colspan="5"></td></tr>
<tr><td>测试用户名</td><td colspan="2"></td><td>密码</td><td colspan="2"></td></tr>
<tr><td>访问路径</td><td colspan="5"></td></tr>
<tr><td>测试用户名</td><td colspan="2"></td><td>密码</td><td colspan="2"></td></tr>
<tr><td rowspan="4">管理信息</td><td>管理端访问路径</td><td colspan="5"></td></tr>
<tr><td>测试账号</td><td colspan="2"></td><td>密码</td><td colspan="2"></td></tr>
<tr><td>管理端访问路径</td><td colspan="5"></td></tr>
<tr><td>测试账号</td><td colspan="2"></td><td>密码</td><td colspan="2"></td></tr>
</table>

安全配置自查		
序号	项目	自查结果
1	安装各类应用软件时是否遵从最小化安装原则，仅安装需要的组件和应用程序并进行安全配置，避免默认安装，关闭不需要的系统服务、默认共享，避免安装不必要的软件	□是 □否
2	应用所在操作系统自带的防火墙是否启用，不需要对外开放的端口是否已进行限制	□是 □否
3	是否已启用安全审计功能、备份计划，日志保存 180 天以上，具备数据备份与恢复功能	□是 □否
4	是否已设置本机防火墙访问规则，禁止非前端服务器访问数据库网络端口	□是 □否
5	应用系统是否使用最低权限的数据库用户作为 web 应用所需，禁止具有不必要的额外权限，未使用 DBA 权限用户（root sa sys system）连接数据库	□是 □否
6	基础框架是否使用 Apache log4j2、Apache Shiro、Apache Struts2、Oracle Weblogic 框架	□是 □否
7	是否删除系统默认安装的各种例程、文档及管理程序，清理默认测试页面，清理部署过程产生的测试内容、测试用例等，避免源码泄露	□是 □否
8	是否对上传文件重命名，无法进行目录遍历，上传文件所在的目录，是否只允许文件保存，不允许执行脚本	□是 □否
9	检查系统日志记录的时间、来源 IP 是否准确，是否保存 180 天以上	□是 □否
10	是否将各角色用户权限已限制为最小访问权限，部署过程中产生的临时账户、测试账户用后及时清理	□是 □否
11	是否禁止使用弱密码，密码符合 8 位以上、字母数字符号多种组合要求，有密码复杂度检查功能，设置有效的验证码或者滑动等手段防止暴力破解，对于多次错误登录进行封堵，禁止在数据库中明文存放密码	□是 □否
12	是否对于生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息在数据库中明文存放	□是 □否

注：以上信息请填写完整，可另加附页，联系电话 82568222。

哈尔滨工程大学信息化处综合办公室　　2022 年 6 月 8 日印发