**安全测试（初测）报告**

|  |  |
| --- | --- |
| 系统名称 |  |
| 版本号 | V1.0 |
| 送测单位 |  |
| 送测时间 | 2017年12月27日 |
| 复测时间 |  |

有限责任公司

2017年12月29日

**有效性声明**

1、本测试报告封面及结论未盖章无效；

2、本测试报告需经审批和授权签字人签字，否则无效；

3、本测试报告应妥善保存，不得擅自扩大分发范围；

4、本测试报告不得部分复制；

5、本测试报告仅对该系统当前版本有效；

6、本测试报告仅对测试时间段有效；

7、测试报告版权归委托方和技有限责任公司共有，其他任何单位和个人均无权使用本测试报告。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **系统名称** | |  | | **版本** | | V1.0 |
| **送检单位** | **单位名称** |  | | | | |
| **通讯地址** |  | | **联系人** | |  |
| **邮箱** |  | | **电话** |  | |
| **测试单位** | | 有限责任公司网络安全团队 | | | | |
| **测试地点** | |  | | | | |
| **样品内容、数量** | | 光盘【 】 附件【 】 说明书【 】 其他【 √ 】 | | | | |
| **测试依据** | |  | | | | |
| **测试工具** | |  | | | | |
| **测试人员签字** | |  | **日期** | | |  |
| **审核人员签字** | |  | **日期** | | |  |
| **批准人员签字** | |  | **日期** | | |  |
| **测 试 结 论** | | | | | | |
| 测试情况总结如下：  初步测试共计发现网络安全漏洞39个，其中高风险漏洞4项、中风险漏洞12项、低风险漏洞8项。  **声明：**   1. 在不违反国家、行业和公司网络安全与保密要求的前提下，本报告由委托方自行决定使用场合，测试单位不对报告用途作说明或建议。 2. 本次测试仅依据国家、行业及委托单位现有技术标准对信息系统进行安全测试，判定其基本安全防护能力具备情况，不代表不存在安全风险。 3. 由于网络环境的变化、系统部署结构调整、软件版本升级等原因，低（中）安全风险漏洞可转化为中（高）安全风险漏洞，运维单位须注意做好日常安全风险管控。 4. 本报告仅对本次测试涉及的用例和场景负责，运维单位在系统运行过程中发生的网络安全事件自行承担有关责任。 | | | | | | |

目 录

[1. 测试目的 7](#_Toc502671174)

[2. 引用标准及参考资料 7](#_Toc502671175)

[3. 测试范围 7](#_Toc502671176)

[4. 测评结果总结 8](#_Toc502671177)

[5. 入网安测试试结果 9](#_Toc502671178)

[5.1 操作系统 9](#_Toc502671179)

[5.2 数据库 11](#_Toc502671180)

[5.3 中间件 12](#_Toc502671181)

[5.4 应用系统 13](#_Toc502671182)

[6. 系统测试记录 15](#_Toc502671183)

[6.1 测试环境配置 15](#_Toc502671184)

[6.2 网络安全 15](#_Toc502671185)

[6.2.1 整体结构安全 15](#_Toc502671186)

[6.2.2 访问控制 16](#_Toc502671187)

[6.2.3 入侵防范 16](#_Toc502671188)

[6.3 工具 17](#_Toc502671189)

[6.4 主机安全 17](#_Toc502671190)

[6.4.1 身份鉴别 17](#_Toc502671191)

[6.4.2 访问控制 18](#_Toc502671192)

[6.4.3 安全审计 20](#_Toc502671193)

[6.4.4 入侵防范 21](#_Toc502671194)

[6.4.5 恶意代码防范 22](#_Toc502671195)

[6.4.6 资源控制 22](#_Toc502671196)

[6.4.7 数据安全备份与恢复 24](#_Toc502671197)

[6.5 数据库系统安全 24](#_Toc502671198)

[6.5.1 身份鉴别 24](#_Toc502671199)

[6.5.2 访问控制 25](#_Toc502671200)

[6.5.3 安全审计 25](#_Toc502671201)

[6.5.4 入侵防范 26](#_Toc502671202)

[6.5.5 数据安全及备份恢复 27](#_Toc502671203)

[6.6 中间件安全 27](#_Toc502671204)

[6.6.1 身份鉴别 27](#_Toc502671205)

[6.6.2 访问控制 28](#_Toc502671206)

[6.6.3 安全审计 28](#_Toc502671207)

[6.6.4 通信保密性 29](#_Toc502671208)

[6.6.5 资源控制 29](#_Toc502671209)

[6.6.6 入侵防范 30](#_Toc502671210)

[6.6.7 数据安全与备份恢复 31](#_Toc502671211)

[6.7 应用系统安全 32](#_Toc502671212)

[6.7.1 身份鉴别 32](#_Toc502671213)

[6.7.2 访问控制 32](#_Toc502671214)

[6.7.3 安全审计 33](#_Toc502671215)

[6.7.4 通信完整性 33](#_Toc502671216)

[6.7.5 通信保密性 34](#_Toc502671217)

[6.7.6 软件容错 34](#_Toc502671218)

[6.7.7 资源控制 35](#_Toc502671219)

[6.7.8 数据保密性 35](#_Toc502671220)

[6.7.9 代码质量 35](#_Toc502671221)

[6.7.10 后台安全 35](#_Toc502671222)

[6.7.11 页面篡改 36](#_Toc502671223)

[6.8 移动应用安全测评技术要求 36](#_Toc502671224)

[6.8.1 身份鉴别 36](#_Toc502671225)

[6.8.2 访问控制 36](#_Toc502671226)

[6.8.3 重要操作安全 37](#_Toc502671227)

[6.8.4 数据存储安全 37](#_Toc502671228)

[6.8.5 网络通讯安全 37](#_Toc502671229)

[6.8.6 会话安全 37](#_Toc502671230)

[6.8.7 认证安全 37](#_Toc502671231)

[6.8.8 抗抵赖 37](#_Toc502671232)

[6.8.9 客户端保护 37](#_Toc502671233)

[6.9 漏洞扫描 38](#_Toc502671234)

[6.8.10主机风险分布 38](#_Toc502671235)

[6.8.11漏洞风险分布 38](#_Toc502671236)

[6.8.12高危漏洞的主机分布 38](#_Toc502671237)

[6.8.13操作系统主机分布 38](#_Toc502671238)

[6.8.14 操作系统漏洞分布 38](#_Toc502671239)

[6.8.15漏洞详细 38](#_Toc502671240)

[6.10 渗透测试 39](#_Toc502671241)

[渗透测试用例 39](#_Toc502671242)

# 测试目的

为了保障应用系统上线后安全稳定的运行，确保最终应用系统满足产品需求并且遵循系统设计要求，为系统提供有效的安全依据。严格按照测试规范系统开展安全测评。

# 引用标准及参考资料

# 测试范围

|  |  |  |
| --- | --- | --- |
| *序号* | *类别* | *对象* |
| *1* | 主机 | 系统服务器 Red Hat Enterprise Linux Server release 6.4 |
| *2* | 数据库 | mysql 5.5.48 |
| *3* | 中间件 | weblogic 12.2.1.0 |
| *4* | 应用系统 |  |

# 测评结果总结

17年12月28日至17年12月29日，对“系统”应用系统进行了初次测试，共计发现高风险漏洞4项、中风险漏洞12项、低风险漏洞18项。

表4-1 测评分项统计情况

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **风险总数** | 34 | **高风险** | 4 | **中风险** | 12 | **低风险** | 18 |
| **1、操作系统** | | **高风险** | 0 | **中风险** | 4 | **低风险** | 8 |
| **2、数据库** | | **高风险** | 0 | **中风险** | 3 | **低风险** | 1 |
| **3、中间件** | | **高风险** | 0 | **中风险** | 4 | **低风险** | 2 |
| **4、应用系统** | | **高风险** | 4 | **中风险** | 1 | **低风险** | 7 |

（统计图如下）

# 入网安测试试结果

## 操作系统

初次测试发现12个问题，其中高风险问题0个，中风险问题4个，低风险问题8个，具体问题描述见下表。

表 5-1-1 10.92.221.225 系统服务器 Red Hat Enterprise Linux Server release 6.4

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***测试系统*** | ***问题标识*** | ***问题描述*** | ***问题等级*** | ***问题状态*** |
| 系统服务器 Red Hat Enterprise Linux Server release 6.4 | 身份鉴别 | 没有风险 | 无 |  |
| 访问控制 | 存在多个everyone用户具有写权限的目录 | 低 |  |
| 安全审计 | 没有风险 | 无 |  |
| 入侵防范 | 未开启主机防火墙 | 中 |  |
| 恶意代码防范 | 没有风险 | 无 |  |
| 资源控制 | 未加入IT集中监控 | 低 |  |
| 数据安全备份与恢复 | 没有风险 | 无 |  |
| 漏洞扫描 | 没有风险 | 无 |  |

表 5-1-1 10.92.221.226 系统服务器 Red Hat Enterprise Linux Server release 6.4

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***测试系统*** | ***问题标识*** | ***问题描述*** | ***问题等级*** | ***问题状态*** |
| 系统服务器 Red Hat Enterprise Linux Server release 6.4 | 身份鉴别 | 没有风险 | 无 |  |
| 访问控制 | 存在多个everyone用户具有写权限的目录 | 低 |  |
| 安全审计 | 没有风险 | 无 |  |
| 入侵防范 | 未开启主机防火墙 | 中 |  |
| 恶意代码防范 | 没有风险 | 无 |  |
| 资源控制 | 未加入IT集中监控 | 低 |  |
| 数据安全备份与恢复 | 没有风险 | 无 |  |
| 漏洞扫描 | 没有风险 | 无 |  |

表 5-1-1 10.92.221.227 系统服务器 Red Hat Enterprise Linux Server release 6.4

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***测试系统*** | ***问题标识*** | ***问题描述*** | ***问题等级*** | ***问题状态*** |
| 系统服务器 Red Hat Enterprise Linux Server release 6.4 | 身份鉴别 | 没有风险 | 无 |  |
| 访问控制 | 存在多个everyone用户具有写权限的目录 | 低 |  |
| 安全审计 | 没有风险 | 无 |  |
| 入侵防范 | 未开启主机防火墙 | 中 |  |
| 恶意代码防范 | 没有风险 | 无 |  |
| 资源控制 | 未加入IT集中监控 | 低 |  |
| 数据安全备份与恢复 | 没有风险 | 无 |  |
| 漏洞扫描 | 没有风险 | 无 |  |

表 5-1-1 10.92.221.228 系统服务器 Red Hat Enterprise Linux Server release 6.4

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***测试系统*** | ***问题标识*** | ***问题描述*** | ***问题等级*** | ***问题状态*** |
| 系统服务器 Red Hat Enterprise Linux Server release 6.4 | 身份鉴别 | 没有风险 | 无 |  |
| 访问控制 | 存在多个everyone用户具有写权限的目录 | 低 |  |
| 安全审计 | 没有风险 | 无 |  |
| 入侵防范 | 未开启主机防火墙 | 中 |  |
| 恶意代码防范 | 没有风险 | 无 |  |
| 资源控制 | 未加入IT集中监控 | 低 |  |
| 数据安全备份与恢复 | 没有风险 | 无 |  |
| 漏洞扫描 | 没有风险 | 无 |  |

表 5-1-2 操作系统问题汇总表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***测试阶段*** | ***高风险*** | ***中风险*** | ***低风险*** | ***合计*** |
| 初测 | 0 | 4 | 8 | 12 |

（统计图如下）

## 数据库

初次测试发现3个问题，其中高风险问题0个，中风险问题0个，低风险问题3个。具体问题描述见下表。

表 5-2-1 mysql 5.5.48数据库问题汇总表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***测试系统*** | ***问题标识*** | ***问题描述*** | ***问题等级*** | ***问题状态*** |
| mysql 5.5.48数据库 | 身份鉴别 | 没有风险 | 无 |  |
| 访问控制 | 没有风险 | 无 |  |
| 安全审计 | 数据库系统未开启日志进程 | 中 |  |
| 无数据库审计日志 | 中 |  |
| 入侵防范 | 没有风险 | 无 |  |
| 恶意代码防范 | 没有风险 | 无 |  |
| 资源控制 | 最大并发连接数限制 | 低 |  |
| 设置操作超时锁定 | 中 |  |
| 数据安全备份与恢复 | 没有风险 | 无 |  |
| 漏洞扫描 | 无 | 无 |  |

表 5-2-2 数据库问题汇总表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***测试阶段*** | ***高风险*** | ***中风险*** | ***低风险*** | ***合计*** |
| 初测 | 0 | 3 | 1 | 4 |

（统计图如下）

## 中间件

初次测试发现6个问题，其中高风险问题0个，中风险问题4个，低风险问题2个。具体问题描述见下表。

表 5-3-1 weblogic 12.2.1.0问题汇总表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***测试系统*** | ***问题标识*** | ***问题描述*** | ***问题等级*** | ***问题状态*** |
| weblogic 12.2.1.0 | 身份鉴别 | 没有风险 | 无 |  |
| 访问控制 | 没有风险 | 无 |  |
| 安全审计 | 未开启中间件的日志审计功能 | 中 |  |
| 无中间件日志 | 低 |  |
| 通信保密性 | 未配置控制台SSL传输协议 | 中 |  |
| 资源控制 | 没有风险 | 无 |  |
| 入侵防范 | 未对错误页面进行了重定向处理 | 中 |  |
| 未修改中间件默认管理端口7001 | 中 |  |
| 未对控制台console进行重命名 | 低 |  |
| 数据安全备份与恢复 | 没有风险 | 无 |  |
| 漏洞扫描 | 没有风险 | 无 |  |

表 5-3-2中间件问题汇总表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***测试阶段*** | ***高风险*** | ***中风险*** | ***低风险*** | ***合计*** |
| 初测 | 0 | 4 | 2 | 6 |

（统计图如下）

## 应用系统

初次测试发现12个问题，其中高风险问题4个，中风险问题1个，低风险问题7个。具体问题描述见下表。

表 5-4-1 应用系统问题汇总表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***测试系统*** | ***问题标识*** | ***问题描述*** | ***问题等级*** | ***问题状态*** |
| 应用系统 | 身份鉴别 | 没有风险 | 无 |  |
| 访问控制 | 没有风险 | 无 |  |
| 安全审计 | 无日志审计功能 | 中 |  |
| 无审计日志记录 | 低 |  |
| 通信完整性 | 未采用校验码技术保证通信过程中数据的完整性 | 低 |  |
| 通信保密性 | 未采用加密机制加密后传输 | 低 |  |
| 软件容错 | 没有风险 | 无 |  |
| 资源控制 | 未限制单个账户的多重并发会话数 | 低 |  |
| 没有限制应用系统的最大并发会话连接数 | 低 |  |
| 没有限制应用系统对单个帐户的多重并发会话数 | 低 |  |
| 数据保密性 | 未采用加密或其他保护措施实现应用系统敏感信息的存储保密性 | 低 |  |
| 代码质量 | 没有风险 | 无 |  |
| 后台安全 | 没有风险 | 无 |  |
| 页面篡改 | 没有风险 | 无 |  |
| 渗透测试 | 存储性跨站脚本漏洞 | 高 |  |
| 任意文件读取漏洞 | 高 |  |
| 多个反射性跨站脚本漏洞 | 高 |  |
| 多个未授权访问漏洞 | 高 |  |

表 5-4-2 应用系统问题汇总表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***测试阶段*** | ***高风险*** | ***中风险*** | ***低风险*** | ***合计*** |
| 初测 | 4 | 1 | 7 | 12 |

（统计图如下）

# 系统测试记录

## 测试环境配置

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务器名称** | **用途** | **操作系统版本** | **IP** | **软件** |
| 1 | 应用系统服务器 | 部署中间件/应用软件 | Red Hat Enterprise Linux Server release 6.4 |  | weblogic 12.2.1.0 |
| 2 | 系统服务器 | 部署数据库系统 | Red Hat Enterprise Linux Server release 6.4 |  | mysql 5.5.48 |

## 网络安全

### 整体结构安全

1. 应采用冗余技术设计网络拓扑结构，保证信息系统的业务处理能力具备冗余空间，满足业务高峰期需要。

测试记录：网络设备为双机部署。

测试结果：满足要求。

1. 应绘制与当前运行情况相符的系统网络拓扑结构图。
2. 拓扑如下：
3. 应用系统网络拓扑结果应符合公司相关规定要求。

测试记录：网络拓扑符合公司相关规定要求。

测试结果：满足要求。

1. 应保证网络各个部分的带宽满足业务高峰期需要；

### 访问控制

1. 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；

测试记录：已采用远程管理网络设备加密。

测试结果：满足要求。

1. 应限制访问网络设备的用户源；

测试记录：已通过防火墙限制只有IP可以访问网络设备。

测试结果：满足要求。

1. 应检查网络设备针对应用系统开放的端口是否合理。

测试记录：已通过IDC防火墙限制。

测试结果：满足要求。

### 入侵防范

1. 应在网络边界处监视以下攻击行为：强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等；
2. 当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。

## 工具

|  |  |  |
| --- | --- | --- |
| **序号** | **测试名称** | **测试工具** |
| 1 | 漏洞扫描 | 天镜脆弱性扫描与管理系统(V6.0) |

## 主机安全

### 身份鉴别

1. 应采用帐户名密码、生物技术、动态口令等一种或多种相结合的身份认证方式。

**系统**

测试记录：设置了账户名和密码。

测试结果：满足要求。

1. 操作系统口令应有复杂度要求并定期更换，要求帐户口令长度应至少为8位，口令必须从字符（a-z，A-Z）、数字（0-9）、符号（~！@#$%^&\*()\_<>）中至少选择两种进行组合。

**系统**

测试记录：操作系统口令长度至少8位，有复杂度要求并定期更换。

测试结果：满足要求。

1. 应启用用户登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

**应用系统**

测试记录：设置了用户登录失败处理功能。

测试结果：满足要求。

1. 对主机系统进行远程管理应采用加密的方式进行访问。

**系统**

测试记录：通过ssh 2进行远程管理。

测试结果：满足要求。

### 访问控制

1. 应确保用户名唯一性，保证操作系统特权用户权限分离（如：实现操作系统和数据库特权用户的权限分离）。

**系统**

测试记录：满足用户名的唯一性。

测试结果：满足要求。

1. 应重命名系统默认帐户，修改默认帐户口令。

**系统**

测试记录：已修改系统默认帐户及默认口令，口令长度满足复杂度要求。

测试结果：满足要求。

1. 应定期审查操作系统帐户，及时删除或禁用多余、过期的帐户。

**系统**

测试记录：已删除多余用户。

测试结果：满足要求。

1. 应对重要系统文件的访问权限进行限制，windows操作系统 everyone用户应没有访问权限，其它系统设置passwd、group等关键文件和目录的权限，应不超过644，shadow应不超过400。

**系统**

测试记录：已对重要系统文件的访问权限进行了限制。

测试结果：满足要求。

1. 系统禁用不必要服务，并关闭多余的服务端口。

**系统**

测试记录：存在多个everyone用户具有写权限的目录。

测试结果：不满足要求。

**系统**

测试记录：存在多个everyone用户具有写权限的目录。

测试结果：不满足要求。

**系统**

测试记录：存在多个everyone用户具有写权限的目录。

测试结果：不满足要求。

**系统**

测试记录：存在多个everyone用户具有写权限的目录。

测试结果：不满足要求。

1. WINDOWS操作系统应对安全控制选项进行优化，应启用“不允许匿名枚取SAM帐号与共享的匿名枚举”、“不允许SAM帐户的匿名枚举”与“不显示上次的用户名”。

**系统**

测试记录：系统为linux。

测试结果：不适用。

1. WINDOWS操作系统应对控制驱动器和系统在蓝屏之后自动运行提供保护。

**系统**

测试记录：系统为linux。

测试结果：不适用。

1. LINUX、UNIX、SORLARIS操作系统应禁止ROOT用户使用FTP，对允许ROOT远程登陆的地址进行限制。

**系统**

测试记录：未使用FTP服务。

测试结果：满足要求。

### 安全审计

1. 应开启操作系统日志审计功能，或通过第三方审计系统对操作系统进行审计，审计策略应覆盖到所有用户。

**系统**

测试记录：已开启日志审计功能。

测试结果：满足要求。

1. 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。

**系统**

测试记录：审计记录包括了事件的日期、时间、类型、主体标识、客体标识和结果等。

测试结果：满足要求。

1. 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件等；

**系统**

测试记录：审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件等。

测试结果：满足要求。

1. 审计日志记录必须保存六个月以上，应避免日志文件受到未预期的删除、修改或覆盖等。

**系统**

测试记录：审计日志可保存六个月以上。

测试结果：满足要求。

### 入侵防范

1. 操作系统应遵循最小安装原则，仅安装需要的组件，并定期更新补丁。

**系统**

测试记录：已更新补丁。

测试结果：满足要求。

1. 应对系统安全配置参数进行调整，防止操作系统受到攻击（如IPC空连接、SYN FLOOD攻击等）。

**系统**

测试记录：已对系统安全配置参数进行调整，密码口令策略、防攻击策略。

测试结果：满足要求。

1. Windows操作系统应进行关键权限指派，如“从本地登录此计算机”、“从远端系统强制关机”、“关闭系统”、“取得文件或其它对象的所有权” 只指派给Administrators组。

**系统**

测试记录：系统为linux。

测试结果：不适用。

1. 应开启系统自带或第三方防火墙。

**系统**

测试记录：未开启系统防火墙。

测试结果：不满足要求。

**系统**

测试记录：未开启系统防火墙。

测试结果：不满足要求。

**系统**

测试记录：未开启系统防火墙。

测试结果：不满足要求。

**系统**

测试记录：未开启系统防火墙。

测试结果：不满足要求。

### 恶意代码防范

1. 操作系统应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库。

**系统**

测试记录：系统为linux。

测试结果：不适用。

1. 防恶意代码软件应支持统一管理，特征库应支持实时在线更新。

**系统**

测试记录：系统为linux。

测试结果：不适用。

### 资源控制

1. 应通过设定终端接入方式、网络地址范围等方式限制终端登录。
2. **系统**

测试记录：已通过防火墙进行限制，该服务器仅允许通过虚拟化平台进行登陆。

测试结果：满足要求。

1. 应设置登录终端的会话超时锁定功能。

**系统**

测试记录：设置了登陆终端会话超时锁定。

测试结果：满足要求。

1. 应有系统可用性监控措施，对服务器主机用户的磁盘、CPU、内存等使用情况进行监控。

**系统**

测试记录：无系统可用性监控措施对服务器主机用户的磁盘、CPU、内存等使用情况进行监控。

测试结果：不满足要求。

**系统**

测试记录：无系统可用性监控措施对服务器主机用户的磁盘、CPU、内存等使用情况进行监控。

测试结果：不满足要求。

**系统**

测试记录：无系统可用性监控措施对服务器主机用户的磁盘、CPU、内存等使用情况进行监控。

测试结果：不满足要求。

**系统**

测试记录：无系统可用性监控措施对服务器主机用户的磁盘、CPU、内存等使用情况进行监控。

测试结果：不满足要求。

1. 应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。（待定）

### 数据安全备份与恢复

1. 应对重要操作系统进行定期备份。

**系统**

测试记录：厂家对系统进行定期备份。

测试结果：满足要求。

1. 重要操作系统应具备冗余能力。

**系统**

测试记录：系统具有冗余能力。

测试结果：满足要求。

## 数据库系统安全

### 身份鉴别

1. 数据库口令应有复杂度要求并定期更换，要求管理员帐户口令长度应至少为8位，口令必须从字符（a-z，A-Z）、数字（0-9）、符号（~！@#$%^&\*()\_<>）中至少选择两种进行组合，普通帐户口令至少为6位，由非纯数字或字母组成。

测试记录：数据库已设置复杂度要求。

测试结果：满足要求。

1. 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

测试记录：已设置登陆失败处理和自动退出措施。

测试结果：满足要求。

### 访问控制

1. 应启用访问控制功能，依据安全策略控制用户对资源的访问。要求数据库系统的宿主操作系统除提供数据库服务外，不得提供其它网络服务，如：WWW、FTP、DNS 等。限制数据库安装、数据文件、备份等目录的权限。关闭不必要的数据库系统服务。

测试记录：已限制数据库安装、数据文件、备份等目录的权限。

测试结果：满足要求。

1. 应在宿主操作系统中设置本地数据库专用帐号，并赋予该帐户除运行各种数据库服务外的最低权限。

测试记录：宿主操作系统设置本地数据库专用账号。

测试结果：满足要求。

1. 应用系统帐户应按照最小权限的原则，严禁应用系统帐户具有DBA权限。

测试记录：已限制系统账户具有DBA权限。

测试结果：满足要求。

1. 应限制默认帐户的访问权限，修改默认帐户的默认口令。

测试记录：已修改默认账户及口令。

测试结果：满足要求。

1. 应定期审查数据库帐户，及时删除或禁用多余、过期的帐户。

测试记录：已删除或禁用多余用户。

测试结果：满足要求。

### 安全审计

1. 应开启数据库审计功能，或通过第三方审计系统对数据库进行审计，审计范围应覆盖到数据库所有帐户。

测试记录：未开启数据库审计功能。

测试结果：不满足要求。

1. 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件。

测试记录：未开启数据库审计功能。

测试结果：不满足要求。

1. 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。

测试记录：未已开启数据库审计功能，审计记录包括事件的日期、时间、类型、主体标识、客体标识和结果等。

测试记录：未开启数据库审计功能。

测试结果：不满足要求。

1. 应保护审计记录，避免受到未预期的删除、修改或覆盖等，审计记录要求保存6个月以上。

测试记录：未开启数据库审计功能。

测试结果：不满足要求。

### 入侵防范

1. 数据库应遵循最小安装的原则，仅安装需要的组件，并定期更新数据库补丁。

测试记录：数据库遵循了最小安装原则。

测试结果：满足要求。

1. 应加密保存数据库中的敏感字段，如：用户鉴别信息等。

测试记录：有对数据库中的敏感字段进行加密。

测试结果：满足要求

1. 应修改数据库默认端口。(可选)

测试记录：修改数据库默认端口为3308。

测试结果：满足要求。

1. 数据库系统应进行最大并发连接数限制。

测试记录：未进行最大并发连接数限制。

测试结果：不满足要求。

1. 应及时删除数据库默认、多余及测试的数据库实例。

测试记录：已删除多余及测试的数据库实例。

测试结果：满足要求。

1. ORACLE数据库应设置数据库监听口令（注：集群部署不作要求），并设置监听服务空闲连接超时时间。

测试记录：MySQL数据库

测试结果：不适用。

### 数据安全及备份恢复

1. 应提供数据备份与恢复功能，定期对数据库进行备份（安全等级保护拟定级三级及以上系统完全数据备份至少每天一次），重要系统备份数据应异机存放。

测试记录：厂家对数据进行定期备份。

测试结果：满足要求

1. 数据库系统应具备冗余能力。

测试记录：数据库具备冗余能力。

测试结果：满足要求。

## 中间件安全

### 身份鉴别

1. 设置口令安全策略，口令长度至少为8位以上，口令必须从字符（a-z，A-Z）、数字（0-9）、符号（~！@#$%^&\*()\_<>）中至少选择两种进行组合，由非纯数字或字母组成。

测试记录：已设置口令安全策略。

测试结果：满足要求。

1. 如中间件无法配置口令安全策略，应从管理上要求中间件帐户设置口令长度至少为8位以上，口令必须从字符（a-z，A-Z）、数字（0-9）、符号（~！@#$%^&\*()\_<>）中至少选择两种进行组合，由非纯数字或字母组成。

测试记录：已设置口令安全策略。

测试结果：满足要求。

1. 中间件用户鉴别信息应加密存储。

测试记录：鉴别信息应加密存储。

测试结果：满足要求。

1. 应提供登录失败处理功能，限制帐户非法登录次数，设置帐户失败尝试次数、帐户锁定时间等。

测试记录：已设置登录失败处理功能。

测试结果：满足要求。

### 访问控制

1. 应在宿主操作系统中设置本地中间件专用帐号，并赋予该帐户除运行中间件服务外的最低权限。

测试记录：在宿主操作系统设置中间件专用账号。

测试结果：满足要求。

1. 应对中间件的默认管理帐户进行管控，修改默认用户名及默认口令。

测试记录：已修改默认用户名及默认口令。

测试结果：满足要求。

### 安全审计

1. 应设置中间件的日志审计功能，并对审计进程进行保护。

测试记录：未开启日志审计功能。

测试结果：不满足要求。

1. 应设置审计日志容量为50M以上，日志必须保存超过6个月。

测试记录：未开启日志审计功能。

测试结果：不满足要求。

1. 应对安全审计的日志记录文件进行保护，设置记录文件的访问权限，windows操作系统 everyone用户应没有写权限，其他操作系统用户权限应不超过640。

测试记录：未开启日志审计功能。

测试结果：不满足要求。

### 通信保密性

1. Weblogic中间件应配置控制台SSL传输协议。

测试记录：未配置控制台SSL传输协议。

测试结果：不满足要求。

### 资源控制

1. 中间件应启用会话超时功能。

测试记录：启用会话超时功能。

测试结果：满足要求。

1. Tomcat应配置会话连接控制功能。如启用网络连接超时（connectionTimeout）、长连接最大保持时间（keepAliveTimeout）、会话超时（session-timeout）等功能。

测试记录：中间件为weblogic。

测试结果：不适用。

1. IIS中间件应启用会话超时限制及网站连接限制等功能。

测试记录：中间件为weblogic。

测试结果：不适用。

### 入侵防范

1. 中间件应对错误页面进行了重定向处理。

测试记录：中间件未对错误页面进行了404重定向处理。

测试结果：不满足要求。

1. 中间应禁止目录遍历。

测试记录：已禁止目录遍历。

测试结果：满足要求。

1. 中间件应对版本信息进行隐藏。

测试记录：已对版本信息进行隐藏。

测试结果：满足要求。

1. 中间件管理后台操作进行登陆源限制。

测试记录：管理后台已通过IDC防火墙进行登陆源限制。

测试结果：满足要求。

1. Weblogic中间件在通信过程应禁止发送服务标识，防止信息泄露。

测试记录：禁止发送服务标识。

测试结果：满足要求。

1. Weblogic中间件应修改中间件默认管理端口。

测试记录：未修改中间件默认管理端口7001。

测试结果：不满足要求。

1. Weblogic中间件应限制服务器的Socket数量，避免拒绝服务攻击。

测试记录：已限制服务器的Socket数量。

测试结果：满足要求。

1. Weblogic中间件应将控制台console进行重命名，禁止默认方式访问。

测试记录：未对控制台console进行重命名。

测试结果：不满足要求。

1. Tomcat应及时删除管理页面及示例页面。

测试记录：中间件为weblogic。

测试结果：不适用。

1. Tomcat应修改SHUTDOWN字符串。

测试记录：中间件为weblogic。

测试结果：不适用。

1. Tomcat应限制应用服务器Threads数量，避免拒绝服务攻击。

测试记录：中间件为weblogic。

测试结果：不适用。

1. IIS中间件应删除部分安装缺省文件或目录，如sample、help、Data Access及 wwwroot下的默认文件等。

测试记录：中间件为weblogic。

测试结果：不适用。

1. IIS中间件应删除多余的脚本映射和应用程序扩展。

测试记录：中间件为weblogic。

测试结果：不适用。

### 数据安全与备份恢复

1. 应定期对中间件的配置目录文件备份。

测试记录：厂家对中间件定期进行备份。

测试结果：满足要求。

## 应用系统安全

### 身份鉴别

1. 应启用应用系统身份认证功能，提供用户身份标识唯一检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用。

测试记录：已启用身份认证功能。

测试结果：满足要求。

1. 管理员帐户口令长度至少为8位，口令必须从字符（a-z，A-Z）、数字（0-9）、符号（~！@#$%^&\*()\_<>）中至少选择两种进行组合，普通帐户口令至少为6位，由非纯数字或字母组成，密码验证在数据库存储过程中实现。

测试记录：口令长度大于8位，有英文、数字和字符。

测试结果：满足要求。

1. 对于系统默认的初始密码，首次登录时应修改密码，且不允许新设定密码与原密码相同；

测试记录：已修改默认的初始密码。

测试结果：满足要求。

1. 外网应用系统，登录时应附加随机码验证。

测试记录：内网应用系统。

测试结果：不适用。

1. 应提供应用系统登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

测试记录：已设置应用系统登录失败处理功能。

测试结果：满足要求。

### 访问控制

1. 由授权主体配置访问控制策略，并严格限制默认帐户的访问权限。默认帐号应不为admin、supadmin、root等常见管理员帐号。

测试记录：已配置访问控制策略，默认帐号不为admin、supadmin、root等常见管理员帐号。

测试结果：满足要求。

1. 应对不同用户的访问权限进行严格的权限控制，特权帐户权限分离，管理员帐户不参与业务流程。

测试记录：该系统已对账户权限进行分离。

测试结果：满足要求。

### 安全审计

1. 应启用应用系统日志审计功能，审计日志内容应至少包含以下项：
2. 用户登录、登出、失败登陆日志。
3. 管理员授权操作日志。
4. 创建、删除（注销）用户操作日志。
5. 重要业务操作。

测试记录：无日志审计功能。

测试结果：不满足要求。

1. 日志记录应包括：主体、客体、事件类型，日期时间、描述、结果等。

测试记录：无日志审计功能。

测试结果：不满足要求。

1. 应对日志记录进行保护，禁止非授权删除或修改日志记录，日志记录应保存六个月以上。

测试记录：无日志审计功能。

测试结果：不满足要求。

### 通信完整性

1. 采用校验码技术保证通信过程中数据的完整性。

测试记录：未使用校验码技术。

测试结果：不满足要求。

### 通信保密性

1. 在通信双方建立连接之前，应用系统利用密码技术进行会话初始化验证。

测试记录： 通信双方建立连接未利用密码技术进行会话初始化验证。

测试结果： 不满足要求。

1. 敏感信息在传输前应采用加密机制加密后传输。

测试记录：敏感信息在传输未采用加密机制加密后传输。

测试结果：不满足要求。

1. 会话标识应足够随机，防止攻击者猜测标识或依据当前标识推导后续的标识；用户登录后应分配新的会话标识。

测试记录：无会话标识。

测试结果：不满足要求。

### 软件容错

1. 提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。

测试记录： 已提供数据有效性检验功能。

测试结果： 满足要求。

1. 应具备文件上传白名单过滤功能，禁止上传asp、jsp、exe、vbs、com等类型文件。

测试记录：该系统具备文件上传过滤功能。

测试结果：满足要求。

1. 应具备防钓鱼功能，禁止通过用户控制的参数来重定向或包含另外一个网站的内容；

### 资源控制

1. 应用系统应具备空闲超时自动结束会话功能。

测试记录： 应用系统具备空闲超时自动结束会话功能。

测试结果： 满足要求。

1. 应限制应用系统的最大并发会话连接数。

测试记录： 未限制最大并发会话连接数。

测试结果： 不满足要求。

1. 应限制应用系统对单个帐户的多重并发会话数。

测试记录： 未限制单个账户的多重并发会话数。

测试结果： 不满足要求。

### 数据保密性

1. 应采用加密或其他保护措施实现应用系统敏感信息（包括系统管理数据、鉴别信息和重要业务数据）的存储保密性。

测试记录：未对系统敏感信息的存储进行加密保护。

测试结果：不满足要求。

### 代码质量

1. 应严格限制Web目录访问权限，避免路径遍历攻击。

测试记录： 已限制web目录访问权限。

测试结果： 满足要求。

1. 提供下载功能时，需要严格限制用户下载文件的路径，避免用户非法下载应用系统其它文件。

测试记录： 不可下载和读取任意文件。

测试结果： 满足要求。

### 后台安全

1. 应用系统的所有管理或者操作页面均需要进行登录认证，避免恶意攻击者通过绕过登录认证进行非法操作。

测试记录：应用系统的所有管理或者操作页面进行登录认证。

测试结果：满足要求。

1. 应限制应用系统后台的访问源，控制粒度为IP、端口级别。

测试记录：该系统后台的访问源通过防火墙进行限制。

测试结果：满足要求。

1. 应避免使用开源的后台管理程序。

测试记录：后台管理程序不是开源程序。

测试结果：满足要求。

1. 外网应用系统后台管理页面应与应用系统页面分离，并禁止将后台管理权限发布到互联网。

测试记录：已将后台管理页面服务端口与应用系统页面服务端口分离。

测试结果：满足要求。

### 页面篡改

1. 外网应用系统web页面应具有不被恶意篡改的能力。

测试记录：该系统为内网系统，不适用。

测试结果：满足要求。

## 移动应用安全测评技术要求

### 身份鉴别

1. 应启用身份认证功能，并对登陆失败的启用混淆提示及登陆失败处理功能；
2. 应设置密码复杂度策略；

### 访问控制

1. 应禁止请求非必要的权限，限制越权访问；
2. 只开放必要的软件权限，防止扣费风险、隐私泄露风险等；
3. 应启用访问控制功能，设置密码保护以及设置合理的访问控制策略；
4. 应对用户的输入进行有效性校验、认证、授权。

### 重要操作安全

1）应采取有效技术措施保证移动终端处理的敏感信息、移动终端与服务器交互的重要信息的机密性和完整性。

### 数据存储安全

1. 敏感数据应禁止明文存储在移动终端；
2. 本地存储的敏感信息应采用安全的加密算法。

### 网络通讯安全

1. 如使用SSL协议，应使用3.0及以上相对高版本的协议，取消对低版本协议的支持。
2. 应用程序应当有异常保护，应能处理网络异常并及时将异常情况通报用户。

### 会话安全

1. 会话应具有一致性和持续性，会话过程中应维持认证状态，防止信息未经授权访问；
2. 会话标识应唯一、随机、不可猜测；
3. 会话应设置超时时间，当空闲时间超过设定时间应自动终止会话；
4. 应采取措施防止重要数据在传输、存储过程中被窃取；

### 认证安全

1. 在执行口令重置前应认证用户身份；
2. 应用程序与服务器的通信验证若采用证书，应保证证书合法性和一致性；
3. 关键业务应进行二次验证。

### 抗抵赖

1）应实行用户的鉴权登录，通过用户名、密码、手机号、IMSI多重绑定对用户身份进行判断，保证用户登录时身份的不可伪造性。

### 客户端保护

1. 客户端运行时应进行完整性自校验；
2. 应禁止对密码控件内信息进行复制，粘贴；

## 漏洞扫描

### 主机风险分布

### 漏洞风险分布

### 高危漏洞的主机分布

### 操作系统主机分布

### 操作系统漏洞分布

### 漏洞详细

漏洞列表

## 渗透测试

### 渗透测试用例

根据开源web应用安全项目（OWASP）等国际渗透测试标准，对应用系统进行安全评估。评估内容包括如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 测试项 | 详细描述 | 备注 |
|  | 注入 | 注入攻击漏洞，例如SQL，OS以及 LDAP注入。注入攻击发生在将不可信的数据作为命令或者查询语句的一部分，发送给解释器时。攻击者发送的恶意数据可以欺骗解释器，以执行计划外的命令或者在未被恰当授权时访问数据。 |  |
|  | 失效的身份认证和会话管理 | 与身份认证和会话管理相关的应用程序功能往往得不到正确的实现，这就导致了攻击者破坏密码、密匙、会话令牌或攻击其他的漏洞去冒充其他用户的身份。 |  |
|  | 跨站脚本（XSS） | 当应用程序收到含有不可信的数据，在没有进行适当的验证和转义的情况下，就将它发送给一个网页浏览器，这就会产生跨站脚本攻击（简称XSS）。XSS允许攻击者在受害者的浏览器上执行脚本，从而劫持用户会话、危害网站、或者将用户转向至恶意网站。 |  |
|  | 不安全的直接  对象引用 | 当开发人员暴露一个对内部实现对象的引用时，例如，一个文件、目录或者数据库密匙，就会产生一个不安全的直接对象引用。在没有访问控制测试或其他保护时，攻击者会操控这些引用去访问未授权数据。 |  |
|  | 安全配置错误 | 好的安全需要对应用程序、框架、应用程序服务器、web服务器、数据库服务器和平台定义和执行安全配置。由于许多设置的默认值并不是安全的，因此，必须定义、实施和维护这些设置。这包含了对所有的软件保持及时地更新，包括所有应用程序的库文件。 |  |
|  | 敏感信息泄漏 | 许多Web应用程序没有正确保护敏感数据，如身份验证凭据等。攻击者可能会窃取或篡改这些弱保护的数据以进行诈骗、身份窃取或其他犯罪。敏感数据值需额外的保护，比如在存放或在传输过程中的加密，以及在与浏览器交换时进行特殊的预防措施。 |  |
|  | 功能级访问控制缺失 | 大多数Web应用程序在用户使用程序前，验证功能级别的访问权限。但是，应用程序需要在每个功能被访问时在服务器端执行相同的访问控制检查。如果请求没有被验证，攻击者能够伪造请求以在未经适当授权时访问功能。 |  |
|  | 跨站请求伪造（CSRF） | 一个跨站请求伪造攻击迫使登录用户的浏览器将伪造的HTTP请求，包括该用户的会话cookie和其他认证信息，发送到一个存在漏洞的web应用程序。这就允许了攻击者迫使用户浏览器向存在漏洞的应用程序发送请求，而这些请求会被应用程序认为是用户的合法请求。 |  |
|  | 使用含有已知漏洞的组件 | 组件，比如：库文件、框架和其它软件模块，几乎总是以全部的权限运行。如果一个带有漏洞的组件被利用，这种攻击可以造成更为严重的数据丢失或服务器接管。应用程序使用带有已知漏洞的组件会破坏应用程序防御系统，并使一系列可能的攻击和影响成为可能。 |  |
|  | 未验证的重定向和转发 | Web应用程序经常将用户重定向和转发到其他网页和网站，并且利用不可信的数据去判定目的页面。如果没有得到适当验证，攻击者可以重定向受害用户到钓鱼软件或恶意网站，或者使用转发去访问未授权的页面。 |  |

#### 6.9.1.1 存储性跨站脚本攻击（高危）

**[漏洞级别]**

高危漏洞

**[相关链接]**

**[效果及截图]**

Title处未过滤特殊字符导致漏洞

**[危害]**

攻击者可以利用存在XSS漏洞的Web系统攻击浏览相关网页的用户，窃取用户会话中诸如用户名和口令（可能包含在Cookie里）等敏感信息、通过插入恶意代码对用户执行挂马攻击、XSS漏洞还可能被攻击者用于网页篡改。

**[建议措施]**

建议根据系统的具体业务情况对特殊字符进行处理，如果需要输入特殊字符建议对输出的字符进行转义，如果系统业务不需要特殊字符建议在服务器端过滤掉特殊字符，或者对输出的字符进行HTML实体转义。

**[修复截图]**

#### 6.9.1.2 任意文件读取（高危）

**[漏洞级别]**

高危漏洞

**[相关链接]**

**[效果及截图]**

查看图片处未过滤

导致可以查看系统任意文件

**[危害]**

攻击者可利用此漏洞，精心构造字符串攻击语句，浏览本地文件敏感数据信息，并通过数据信息，进一步为后续攻击做准备。

**[建议措施]**

建议在不影响业务的前提下，在服务器端过滤请求参数中的../等特殊字符。

**[修复截图]**

#### 6.9.1.3 多个反射性跨站脚本攻击（高危）

**[漏洞级别]**

高危漏洞

**[相关链接]**

**[效果及截图]**

**[危害]**

攻击者可以利用存在XSS漏洞的Web系统攻击浏览相关网页的用户，窃取用户会话中诸如用户名和口令（可能包含在Cookie里）等敏感信息、通过插入恶意代码对用户执行挂马攻击、XSS漏洞还可能被攻击者用于网页篡改。

**[建议措施]**

建议根据系统的具体业务情况对特殊字符进行处理，如果需要输入特殊字符建议对输出的字符进行转义，如果系统业务不需要特殊字符建议在服务器端过滤掉特殊字符，或者对输出的字符进行HTML实体转义。

**[修复截图]**

#### 6.9.1.4 多个未授权访问（高危）

**[漏洞级别]**

高危漏洞

**[相关链接]**

**基本每个页面都有**

**[效果及截图]**

在未登录情况下可以访问后台管理页面

**[危害]**

通过此漏洞攻击者可以使用系统未授权的模块功能，查看到业务非授权的信息，造成系统信息泄露风险。

**[建议措施]**

建议在不影响业务的前提下，对参数进行模糊化处理，且添加权限验证机制，不仅以返回参数内容作为权限判断依据。

**[修复截图]**