CFCA

Handbook For Testing

（版本：3.0.1.1）

中国金融认证中心

文档修订记录

本文档会随时保持更新，请与中国金融认证中心索要最新版本

版本	内容	日期	编写	审核
1.0.0.1	创建	2019-11-27	王烁	林峰
2.0.0.1	增加错误定位机制	2020-6-26	许红梅	林峰
3.0.0.1	增加安全测试内容	2020-9-27	许红梅	林峰
3.0.1.0	1.增加 5.web 类产品 2.增加 2.3 当前用户非 root 权限检查	2021-1-25	许红梅	林峰
3.0.1.1	增加一体机产品 3.5 安全加固	2021-6-7	许红梅	林峰

注：对该文件内容增加、删除或修改须填写此修订记录，详细记载变更信息，以保证其可追溯性。

目录

1. 文档

1.1 入口文档

提交测试的版本必须具备以下文档，否则可直接退回

1. 产品/用户需求说明书；
2. 软件需求说明书；
3. 安装部署手册或用户操作手册；
4. 如果涉及版本升级，必须提供升级手册。

1.2 需求文档

需求文档在检查时应包含如下信息

1. 用户使用场景：需要解决什么问题；
2. 用户生产环境信息：如 OS，JDK，中间件，数据库等版本；
3. 环境配置信息：CPU，内存，硬盘大小等；
4. 系统架构图；
5. 性能需求：包含 TPS，响应时间，并发用户数等；
6. 开发人员、测试人员签名；
7. 如果产品在运行部上线，则还需要运行部相关人员签名。

1.3 接口文档

1. 文档包含接口名以及接口参数信息；
2. 接口描述包含输入输出参数类型、是否必输、长度、取值范围等；
3. 检查输入输出参数类型、参数个数、参数大小写与实际一致；
4. 服务端通过报文与客户进行业务交互时，应提供空转报文和心跳报文；
5. 对外提供的接口文档中的输入输出字段、错误码等不能随意改动。

1.4 操作手册

操作手册必须详细写明需要修改的配置项，以免遗漏。

2. 服务类产品

2.1 日志

1. 服务端、客户端日志中应打印本地以及远端 IP 地址及端口，以便能够快速从回溯包中找到对应的网络日志；
2. info 级别的日志应该包含各个步骤的关键信息，debug 级别的日志中应包含详细信息以及与数据库交互的 sql 语句；
3. 服务类产品在启动时应该打印环境信息，如主要配置信息、JDK、操作系统、中间件版本、当前用户是否有 root 目录权限等，并且将环境信息日志单独存放；
4. 服务类产品在调用工具包和其它系统（如时间戳、CA 等）进行交互时，工具包的日志要在单独的日志文件中打印；
5. 如果有超时报警日志时，超时阈值要求可通过配置文件修改，响应时间超过超时阈值的业务要记录到超时报警日志中，方便反查 info 日志；
6. 对于交易的业务报文，无论堆栈信息多大都应完整记录至 Error 日志中。

2.2 数据库

1. 项目立项时，应该对日交易量有大致估算，以便选择适合的数据库。尤其对于托管在 CFCA 的服务类产品，如果交易量超过千万，则优先考虑 oracle 数据库，并提前规划好分表分库策略，以及数据定期备份、清理等策略。
2. 使用 Mysql 数据库时，如果记录中包含中文字段，则必须使用 UTF8Mb4 的编码格式，否则 4 字节的偏僻字将无法插入至数据库中。
3. 已上线服务类产品修改表结构时，如果没有明确告之会停服务进行表结构的修改，则应该在超过生产压力业务量的时候进行数据库脚本的更新验证，而不能只在无业务的情况下执行数据库更新脚本。
4. 对于已上线服务类产品，库表中新增列操作时，如果新增列字段属性非空，并且有默认值，必须添加 Not Null 关键字，否则会出现排他锁，不仅影响正常业务，而且更新的非常慢，对于数据量大的表影响尤其明显。

2.3 测试环境

1. 使用与生产环境一致的环境配置进行测试，如果需求文档中未指明生产环境，则要求需求人员进行补充，如 JDK，中间件，数据库，操作系统等环境信息，版本号等。
2. 程序在 linux 环境启动时需检查当前用户是否具有 root 目录权限，如果有则程序启动失败。

2.4 UI 审核

存在经过 UI 组设计页面的产品时，在发版前需要通过 UI 组的审核。

3. 一体机产品

3.1 自检

一体机产品需包含自检机制，可通过自检功能检测主要服务及功能的工作状态，并输出详细自检报告。

3.2 端口

1. 检查端口的占用情况。端口作为重要资源之一，除非服务需求，否则不得占用；
2. 如果服务必须占用端口，那么不要使用 10000 内的常用端口，尽量使用 65500 后的端口；
3. 被占用的端口如果被用户使用，需给予友好提示。
4. 禁用 SSH 端口，避免一体机远程连接，尽量不要开放不使用的端口。

3.3 异常场景

应覆盖断网，断电，硬盘满，数据库占满，非标准报文处理等异常场景。

3.4 高可用

一体机产品如果有多主、热备等高可用机制，需要测试在主机出现异常时，是否能够正确切换，数据存储是否会出现脑裂。

3.5 安全加固

1. 禁用系统单用户模式或其他禁止修改 root 密码的方案，使用动态 root 密码方案；
2. 使用经过精简和安全加固的 tomcat 版本；
3. 一体机产品如需要集成密码卡，硬件问题定位机制必须有。

4. 工具类产品

1. 需定时（如每隔 5 分钟）输出软件执行信息，包括软件已经完成了哪些操作，完成百分比，已运行时间等。
2. 需明确标注要修改的配置项，以免操作时遗漏。

3. 需要在上线前进行演练，以评估上线时运行时间。

5. WEB 类产品

1. WEB 应用包应与配置文件分离；web.xml 文件中配置禁止用户下载文件；
2. 对请求报文进行过滤，禁止传入“./ ”、“<”、“>”、“<Script”等非法字符；
3. 输入输出参数禁止传递路径，后台文件名与系统路径应进行映射。

6. 偏僻字覆盖

发版产品尽量覆盖以下 5 个区域的偏僻字

A 区：

丠乇㐮峎㠉泗阳䧅靐奍𪛊

B 区:

匸𠀀𠁥𤬫𪚥𪛖

C 区：

𪜀𪜁𪣻𪰼𫄃𫌆𫗁𫜴

D 区：

𫝀𫝄𫝑𫝜𫝢𫠝

E 区：

𫠠

7. 安全性测试

7.1 越权漏洞

1. 水平越权

Web 应用程序在接收到用户的操作数据请求时，没有判断数据所对应的用户，或者通过从用户表单参数中获取 userId 来实现的，通过修改 userId 实现水平越权。

2. 垂直越权

当 web 应用没有做用户权限控制，或者只在菜单上做了权限控制，通过修改 URL，就可以访问或者控制其他角色拥有的数据或者页面，达到权限提升的目的。如低权限用户通过修改 url 可直接访问高权限用户的操作。

3. 越权修改密码

在登录用户 A 进行密码修改时，使用抓包工具设置断点，进行抓包，修改抓取到的用户名为 B，旧密码为 B 的旧密码，成功运行。

7.2 密码明文传输

在登录时使用抓包工具可查看用户账号及密码是否为明文。

7.3 SQL 注入

根据“外部数据不可信任”原则，如果程序要使用用户输入的变量或 URL 传递的参数来组成 SQL 语句，程序应对用户输入的内容或传递的参数进行数据类型及格式的检查，过滤特殊符号，或采用 SQL 预编译以防止 SQL 注入。

7.4 XSS 跨站攻击

XSS 主要原因是过于信任客户端提交的数据，没有对客户端提交的数据进行转义处理或者过滤。程序应限定客户端提供的数据类型，并对客户端提交的数据类型进行转义，过滤、移除敏感字符及特殊标签。

7.5 安全扫描

服务端产品需要使用 OpenVas、Nessus 进行安全扫描。

8. 错误定位机制

软硬件产品必须具备完整的错误定位机制，包含 trace 以及 dump 信息，以便定位问题。