|  |
| --- |
| **老男孩信息系统安全配置基线**  **Tomcat中间件分册（初稿）** |
| **版本 V1.0** |

**二○一九年一月**

|  |  |  |  |
| --- | --- | --- | --- |
| ■版本变更记录 | | | |
| 时间 | 版本 | 说明 | 修改人 |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| 目录 |
| [一. 概述 4](#_Toc408344091)  [1.1适用范围 4](#_Toc408344092)  [1.2规范依据 4](#_Toc408344093)  [1.3实施策略 4](#_Toc408344094)  [二. 安全配置基线标准 5](#_Toc408344095)  [2.1身份鉴别 5](#_Toc408344096)  [2.1.1配置密码并保证复杂度 5](#_Toc408344097)  [2.2访问控制 6](#_Toc408344098)  [2.2.1配置Tomcat运行账户 6](#_Toc408344099)  [2.2.2配置划分用户权限 6](#_Toc408344100)  [2.2.3禁止目录浏览 7](#_Toc408344101)  [2.2.4配置使用安全的HTTP请求 8](#_Toc408344102)  [2.3安全审计 8](#_Toc408344103)  [2.3.1配置安全日志 8](#_Toc408344104)  [2.4资源控制 10](#_Toc408344105)  [2.4.1设置登录超时 10](#_Toc408344106)  [2.4.2设置连接数 10](#_Toc408344107)  [2.5其它安全项 12](#_Toc408344108)  [2.5.1删除缺省文件 12](#_Toc408344109)  [2.5.2配置错误页面处理 12](#_Toc408344110)  [2.5.3更新补丁 13](#_Toc408344111)  [三. 评审与修订 13](#_Toc408344112) |

1. 概述
   1. 适用范围

本配置基线适用于老男孩的Tomcat中间件，主要涉及Tomcat中间件安全配置方面的基本要求，用于指导安全例行工作、新系统入网安全检查等场合。

在未特别说明的情况下，均适用于所有运行Tomcat中间件系统。

* 1. 规范依据

根据老男孩目前Tomcat中间件安全现状，综合参考各信息系统运维部门的意见，结合金融行业等级保护实施指引，制定适合于老男孩的基线配置规范。

主要参考依据如下：

* JR/T0071-2012《金融行业信息系统信息安全等级保护实施指引》（2012年7月发布）
  1. 实施策略

结合网络和信息系统建设情况，考虑安全配置项影响的范围，结合以往工作经验，提出如下安全项目实施策略：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **配置类别** | **安全基线项目名称** | **实施策略** |
| 1 | 身份鉴别 | 配置密码并保证复杂度 | 必须实施 |
| 2 | 访问控制 | 配置Tomcat运行账户 | 必须实施 |
| 3 | 访问控制 | 配置划分用户权限 | 必须实施 |
| 4 | 访问控制 | 禁止目录浏览 | 必须实施 |
| 5 | 访问控制 | 配置使用安全的HTTP请求 | 必须实施 |
| 6 | 安全审计 | 配置安全日志 | 必须实施 |
| 7 | 资源控制 | 设置登录超时 | 必须实施 |
| 8 | 资源控制 | 设置连接数 | 按需实施 |
| 9 | 其它安全项 | 删除缺省文件 | 必须实施 |
| 11 | 其它安全项 | 配置错误页面处理 | 必须实施 |
| 12 | 其它安全项 | 更新补丁 | 按需实施 |

1. 安全配置基线标准
   1. 身份鉴别
      1. 配置密码并保证复杂度

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置密码并保证复杂度（必须实施） |
| **安全基线编号** | 中间件-Tomcat-1 |
| **安全基线项说明** | 口令长度至少8位，并包括数字、小写字母、大写字母和特殊符号四类中至少两类。 |
| **配置方法** | **1、参考配置操作**  在tomcat/conf/tomcat-user.xml配置文件中设置密码  <user username=”tomcat” password=”Tomcat!234” roles=”admin”>  **2、补充操作说明**  口令要求：口令长度至少8位，并包括数字、小写字母、大写字母和特殊符号四类中至少两类。且5次以内不得设置相同的口令。 |
| **检查方法** | 手工检查，查看tomcat/conf/tomcat-users.xml配置文件。 |
| **依据** | 6.2.1.4 应用安全：身份鉴别（S3）：g) 对于系统自动分配或者预设的强度较弱的初始密码，系统应强制用户首次登录时修改初始密码； |
| **备注** | 建议本地方式管理tomcat，不使用远程登录的方式以规避安全问题。若目标tomcat应用必须要远程管理，此项为必须项目。 |

* 1. 访问控制
     1. 配置Tomcat运行账户

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置Tomcat运行账户（必须实施） |
| **安全基线编号** | 中间件-Tomcat-2 |
| **安全基线项说明** | 应按照用户分配帐号。避免不同用户间共享帐号。避免用户帐号和设备间通信使用的帐号共享。  检查是否存在与工作无关的账号。 |
| **配置方法** | **1、参考配置操作**  修改tomcat/conf/tomcat-users.xml配置文件，修改或添加帐号。  <user username=”tomcat” password=” Tomcat!234” roles=”admin”>  **2、补充操作说明**  1、根据不同用户，取不同的名称。  2、Tomcat 4.1.37、5.5.27和6.0.18这三个版本及以后发行的版本默认都不存在admin.xml配置文件。 |
| **检查方法** | 手工检查，查看tomcat/conf/tomcat-users.xml配置文件 |
| **依据** | 6.2.1.4 应用安全：访问控制（S3）：d) 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系； |
| **备注** |  |

* + 1. 配置划分用户权限

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置划分用户权限（必须实施） |
| **安全基线编号** | 中间件-Tomcat-3 |
| **安全基线项说明** | 在设备权限配置能力内，根据用户的业务需要，配置其所需的最小权限。 |
| **配置方法** | **1、参考配置操作**  编辑tomcat/conf/tomcat-user.xml配置文件，修改用户角色权限  授权tomcat具有远程管理权限：  <user username=”tomcat” password=”chinamobile”  roles=”admin,manager”>  **2、补充操作说明**  1、Tomcat 4.x和5.x版本用户角色分为：role1，tomcat，admin，manager四种。  role1：具有读权限；  tomcat：具有读和运行权限；  admin：具有读、运行和写权限；  manager：具有远程管理权限。  Tomcat 6.0.18版本只有admin和manager两种用户角色，且admin用户具有manager管理权限。  2、Tomcat 4.1.37和5.5.27版本及以后发行的版本默认除admin用户外其他用户都不具有manager管理权限。。 |
| **检查方法** | 手工检查，查看tomcat/conf/tomcat-users.xml配置文件  登陆http://ip:8080/manager/html页面，使用tomcat帐号登陆，进行远程管理。 |
| **依据** | 6.2.1.4 应用安全：访问控制（S3）：d) 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系； |
| **备注** | Manager目录为缺省管理目录，若上线后不需要通过web页面管理，可删除（移除）此目录，这样相对更为安全。 |

* + 1. 禁止目录浏览

|  |  |
| --- | --- |
| **安全基线项目名称** | 禁止目录浏览（必须实施） |
| **安全基线编号** | 中间件-Tomcat-4 |
| **安全基线项说明** | 禁止tomcat列表显示文件 |
| **配置方法** | **1、参考配置操作**  (1)编辑tomcat/conf/web.xml配置文件， <init-param>         <param-name>listings</param-name>         <param-value>true</param-value>     </init-param> 把true改成false  (2)重新启动tomcat服务 |
| **检查方法** | 直接访问<http://ip:8800/webadd>，当WEB目录中没有默认首页如index.html,index.jsp等文件时，不会列出目录内容。 |
| **依据** | 6.2.1.4 应用安全：访问控制（S3）：b) 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作； |
| **备注** |  |

* + 1. 配置使用安全的HTTP请求

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置使用安全的HTTP请求（必须实施） |
| **安全基线编号** | 中间件-Tomcat-5 |
| **安全基线项说明** | 禁用PUT、DELETE等危险的HTTP方法 |
| **配置方法** | **涉及系统文件：httpd.conf**  在httpd.conf中，添加如下内容：  <LimitExcept GET POST> Deny from all< /LimitExcept> |
| **检查方法** | 参考安全配置方法查看httpd.conf中是否有相应内容 |
| **依据** | 6.2.1.4 应用安全：访问控制（S3）：a) 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；  6.2.1.4 应用安全：访问控制（S3）：b) 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作； |
| **备注** |  |

* 1. 安全审计
     1. 配置安全日志

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置安全日志（必须实施） |
| **安全基线编号** | 中间件-Tomcat-6 |
| **安全基线项说明** | 启用日志可以回溯事件进行检查或审计，日志详细信息级别如果配置不当，会缺少必要的审计信息。  设备应配置日志功能，对运行错误、用户访问等进行记录，记录内容包括时间，用户使用的IP地址等内容。 |
| **配置方法** | **涉及的系统文件：**server.xml  **涉及参数：**<host>标签  **可加入下面的语句**  <Valve className="org.apache.catalina.valves.AccessLogValve"  directory="logs" prefix="localhost\_access\_log." suffix=".txt"  pattern="common" resolveHosts="false"/>  ------------------------------------------------------------------------------------  className /\*\*必须这样写的参数\*\*/  directory/\*\*这个东西是日志文件放置的目录\*\*/  prefix /\*\*这个是日志文件的名称前缀，我的日志名称为localhost\_access\_log.2007-09-22.txt，前面的前缀就是这个localhost\_access\_log\*\*/  suffix /\*\*这就是后缀名，可以修改\*\*/  pattern /\*\*这个是最主要的参数\*\*/  resolveHosts /\*\*如果这个值是true的话，tomcat会将这个服务器IP地址通过DNS转换为主机名，如果是false，就直接写服务器IP地址。\*\*/ |
| **检查方法** | 以下操作使用root账号或者有Tomcat修改权限账号登陆  1.查看logs目录中相关日志文件内容，记录完整。  2.查看相关日志记录，要求对运行错误、用户访问等进行记录，记录内容包括时间，用户使用的IP地址等内容。 |
| **依据** | 6.2.1.4 应用安全：安全审计（G3）：a) 应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计； |
| **备注** | 必须开启日志审计，但考虑到磁片I/O，不建议开启所有日志记录。 |

* 1. 资源控制
     1. 设置登录超时

|  |  |
| --- | --- |
| **安全基线项目名称** | 设置登录超时（必须实施） |
| **安全基线编号** | 中间件-Tomcat-7 |
| **安全基线项说明** | 应支持账户登录超时锁定功能。超时后用户需再次输入密码登录才能进入系统。 |
| **配置方法** | 编辑tomcat/conf/server.xml配置文件，修改connectionTimeout参数值为300秒，示例如下所示：  <Connector  port="8080" maxHttpHeaderSize="8192"maxThreads="150"  minSpareThreads="25" maxSpareThreads="75"、  enableLookups="false" redirectPort="8443" acceptCount="100"  connectionTimeout="300" disableUploadTimeout="true" /> |
| **检查方法** | 登陆tomcat默认页面http://ip:8080/manager/html ，使用管理帐号登陆  ，300秒自动登出。 |
| **依据** | 6.2.1.4 应用安全：资源控制（A3）：a) 对于有会话或短连接的应用系统，当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话； |
| **备注** | 为保证Tomcat的安全，建议删除默认管理页面（在manager目录），使用本地管理的方式，此条基线适用于在不得不远程管理的情况。  建议本地方式管理tomcat，不使用远程登录的方式以规避安全问题。 |

* + 1. 设置连接数

|  |  |
| --- | --- |
| **安全基线项目名称** | 设置连接数（按需实施） |
| **安全基线编号** | 中间件-Tomcat-8 |
| **安全基线项说明** | 根据机器性能和业务需求，设置最大最小连接数 |
| **配置方法** | **涉及的系统文件：**tomcat配置文件server.xml  **涉及参数：**  minProcessors：最小空闲连接线程数，用于提高系统处理性能，默认值为10  maxProcessors：最大连接线程数，即：并发处理的最大请求数，默认值为75  acceptCount：允许的最大连接数，应大于等于maxProcessors，默认值为100  enableLookups：是否反查域名，取值为：true或false。为了提高处理能力，应设置为false  connectionTimeout：网络连接超时，单位：毫秒。设置为0表示永不超时，这样设置有隐患的。通常可设置为30000毫秒。  其中和最大连接数相关的参数为maxProcessors和acceptCount，如果要加大并发连接数，应同时加大这两个参数。  请参考如下配置：  <Connector port="8080"  maxThreads="150" /\*\*表示最多同时处理150个连接\*\*/  minSpareThreads="25" /\*\*表示即使没有人使用也开这么多空线程等待\*\*/  maxSpareThreads="75" /\*\*表示如果最多可以空75个线程，例如某时刻有80人访问，之后没有人访问了，则tomcat不会保留80个空线程，而是关闭5个空的。\*\*/  acceptCount="100" /\*\*当同时连接的人数达到maxThreads时，还可以接收排队的连接，超过这个连接的则直接返回拒绝连接\*\*/  /> |
| **检查方法** | 参见配置方法给出的参数值，检查其是否负责既定要求，否则建议修改。 |
| **依据** | 6.2.1.4 应用安全：资源控制（A3）：d) 应能够对一个时间段内可能的并发会话连接数进行限制； |
| **备注** | web server允许的最大连接数还受制于操作系统的内核参数设置，通常Windows是2000个左右，Linux是1000个左右。 |

* 1. 其它安全项
     1. 删除缺省文件

|  |  |
| --- | --- |
| **安全基线项目名称** | 删除缺省文件（必须实施） |
| **安全基线编号** | 中间件-Tomcat-9 |
| **安全基线项说明** | 删除缺省安装的无用文件。 |
| **配置方法** | Manager目录为缺省管理目录，若上线后不需要通过web页面管理，可删除（移除）此目录，这样相对更为安全。。 |
| **检查方法** | 检查有无此目录。 |
| **依据** | 6.2.1.4 应用安全：剩余信息保护（S3）：b)应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。 |
| **备注** | 若不需要远程管理时候，建议（临时）移除此目录，避免留下安全隐患。 |

* + 1. 配置错误页面处理

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置错误页面处理（必须实施） |
| **安全基线编号** | 中间件-Tomcat-10 |
| **安全基线项说明** | Tomcat错误页面重定向 |
| **配置方法** | 1. **参考配置操作**   查看并启用tomcat/conf/web.xml文件中下列代码: <error-page> <error-code>404</error-code> <location>/noFile.htm</location> </error-page> …………… <error-page> <exception-type>java.lang.NullPointerException</exception-type> <location>/ error.jsp</location> </error-page> |
| **检查方法** | 判断出错页面是否显示error.jsp页面，并没有包含敏感信息。 |
| **依据** | 6.2.1.4 应用安全：软件容错（A3）：c) 应能够有效屏蔽系统技术错误信息，不将系统产生的错误信息直接反馈给客户。 |
| **备注** |  |

* + 1. 更新补丁

|  |  |
| --- | --- |
| **安全基线项目名称** | 更新补丁（按需实施） |
| **安全基线编号** | 中间件-Tomcat-11 |
| **安全基线项说明** | 在不影响业务的情况下，升级解决高危漏洞，而且该补丁要通过实验测试。 |
| **配置方法** | 访问http://tomcat.apache.org/，查看最新的Tomcat版本，在实验室测试通过的前提下，编译升级Tomcat，以解决高危漏洞。 |
| **检查方法** | 使用安全漏洞扫描工具对Tomcat中间件进行扫描，或通过搜索引擎检索当前版本脆弱性来检查是否存在高危安全漏洞。 |
| **依据** |  |
| **备注** |  |

1. 评审与修订

本标准由老男孩定期进行审查，根据审视结果修订标准，并颁发执行。