Tomcat 系统加固规范

Opsec.cn

2010 年 9 月

目 录

1 账号管理、认证授权

1.1.1 SHG-Tomcat-01-01-01

编号	SHG-Tomcat-01-01-01
名称	为不同的管理员分配不同的账号
实施目的	应按照用户分配账号，避免不同用户间共享账号，提高安全性。
问题影响	账号混淆，权限不明确，存在用户越权使用的可能。
系统当前状态	记录 tomcat/conf/tomcat-users.xml 文件
实施步骤	**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。
回退方案	还原 tomcat/conf/tomcat-users.xml 文件
判断依据	询问管理员是否安装需求分配用户账号
实施风险	高

重要等级	★★★
备注	

1.1.2 SHG-Tomcat-01-01-02

编号	SHG-Tomcat-01-01-02
名称	删除或锁定无效账号
实施目的	删除或锁定无效的账号，减少系统安全隐患。
问题影响	允许非法利用系统默认账号
系统当前状态	记录 tomcat/conf/tomcat-users.xml 文件
实施步骤	**1、参考配置操作** 修改 tomcat/conf/tomcat-users.xml 配置文件，删除与工作无关的帐号。 例如 tomcat1 与运行、维护等工作无关，删除帐号： <user username=”tomcat1” password=”tomcat” roles=”admin”>
回退方案	还原 tomcat/conf/tomcat-users.xml 文件
判断依据	询问管理员,哪些账号是无效账号
实施风险	高
重要等级	★★★
备注	

1.1.3 SHG-Tomcat-01-01-03

编号	SHG-Tomcat-01-01-03
名称	密码复杂度
实施目的	对于采用静态口令认证技术的设备，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 4 类中至少 2 类。
问题影响	被暴力破解
系统当前状态	记录 tomcat/conf/tomcat-users.xml 文件
实施步骤	**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：长度至少 8 位，并包括数字、小写字母、大写字母和特殊符号 4 类中至少 2 类。
回退方案	还原 tomcat/conf/tomcat-users.xml 文件
判断依据	**判定条件** 查看 tomcat/conf/tomcat-users.xml 文件
实施风险	高
重要等级	★★★
备注	

1.1.4 SHG-Tomcat-01-01-04

编号	SHG-Tomcat-01-01-04

名称	权限最小化
实施目的	在数据库权限配置能力内，根据用户的业务需要，配置其所需的最小权限。
问题影响	账号权限越大, 对系统的威胁性越高
系统当前状态	查看 tomcat/conf/tomcat-user.xml
实施步骤	**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。
回退方案	还原 tomcat/conf/tomcat-user.xml
判断依据	业务测试正常
实施风险	高
重要等级	★
备注	

2 日志配置

2.1.1 SHG-Tomcat-02-01-01

编号	SHG-Tomcat-02-01-01
名称	启用日志记录功能
实施目的	数据库应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的账号、登录是否成功、登录时间以及远程登录时用户使用的 IP 地址。
问题影响	无法对用户的登陆进行日志记录
系统当前状态	查看 server.xml
实施步骤	**1、参考配置操作** 编辑 server.xml 配置文件，在<HOST>标签中增加记录日志功能 将以下内容的注释标记<！-- --->取消 <valve classname=”org.apache.catalina.valves.AccessLogValve” Directory=”logs” prefix=”localhost_access_log.” Suffix=”.txt” Pattern=”common” resloveHosts=”false”/> **2、补充操作说明** classname: This MUST be set to org.apache.catalina.valves.AccessLogValve to use the default access log valve. &<60 Directory:日志文件放置的目录，在 tomcat 下面有个 logs 文件夹，那里面是专门放置日志文件的，也可以修改为其他路径； Prefix: 这个是日志文件的名称前缀，日志名称为 localhost_access_log.2008-10-22.txt，前面的前缀就是这个

	localhost_access_log Suffix: 文件后缀名 Pattern: common 方式时，将记录访问源 IP、本地服务器 IP、记录日志服务器 IP、访问方式、发送字节数、本地接收端口、访问 URL 地址等相关信息在日志文件中 resolveHosts:值为 true 时，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
回退方案	还原 server.xml
判断依据	**判定条件** 登录测试，检查相关信息是否被记录 查看 server.xml 文件
实施风险	低
重要等级	★★★
备注	

3 通信协议

3.1.1 SHG-Tomcat-03-01-01

编号	SHG-Tomcat-03-01-01
名称	HTTPS 协议
实施目的	对于通过 HTTP 协议进行远程维护的设备，设备应支持使用 HTTPS 等加密协议。

问题影响	增加数据库数据传输安全隐患
系统当前状态	查看 tomcat/conf/server.xml
实施步骤	(1)使用 JDK 自带的 keytool 工具生成一个证书 JAVA_HOME/bin/keytool -genkey –alias tomcat –keyalg RSA -keystore /path/to/my/keystore (2)修改 tomcat/conf/server.xml 配置文件，更改为使用 https 方式，增加如下行： Connector classname=”org.apache.catalina.http.HttpConnector” port=”8443” minProcessors=”5” maxprocessors=”100” enableLookups=”true” acceptCount=”10” debug=”0” scheme=”https” secure=”true” > Factory classname=”org.apache.catalina.SSLServerSocketFactory” clientAuth=”false” keystoreFile=”/path/to/my/keystore” keystorePass=”runway” protocol=”TLS”/> /Connector> 其中 keystorePass 的值为生成 keystore 时输入的密码 (3)重新启动 tomcat 服务
回退方案	还原 tomcat/conf/server.xml
判断依据	**1、判定条件** 查看 tomcat/conf/server.xml **2、检测操作** 使用 https 方式登陆 tomcat 服务器管理页面
实施风险	高
重要等级	★★
备注	

3.1.2 SHG-Tomcat-03-01-02

编号	SHG-Tomcat-03-01-02
名称	更改 tomcat 服务器默认端口
实施目的	更改 tomcat 服务器默认端口,增加系统安全性
问题影响	不安全性增加
系统当前状态	查看 tomcat/conf/server.xml
实施步骤	**1、参考配置操作** （1）修改 tomcat/conf/server.xml 配置文件，更改默认管理端口到 8800 <Connector port="**8800**" maxHttpHeaderSize="8192" maxThreads="150" minSpareThreads="25" maxSpareThreads="75"、enableLookups="false" redirectPort="8443" acceptCount="100" connectionTimeout="300" disableUploadTimeout="true" /> （2）重启 tomcat 服务
回退方案	还原 tomcat/conf/server.xml
判断依据	**1、判定条件** **查看** tomcat/conf/server.xml **2、检测操作** 登陆 http://ip:8800
实施风险	高
重要等级	★
备注	

4 设备其他安全要求

4.1.1 SHG-Tomcat-04-01-01

编号	SHG-Tomcat-04-01-01
名称	登录超时
实施目的	对于具备字符交互界面的设备，应支持定时账户自动登出。 登出后用户需再次登录才能进入系统。
问题影响	被恶意攻击者盗用
系统当前状态	查看 tomcat/conf/server.xml
实施步骤	**参考配置操作** 编辑 tomcat/conf/server.xml 配置文件，修改为 30 秒 <Connector port="8080" maxHttpHeaderSize="8192" maxThreads="150" minSpareThreads="25" maxSpareThreads="75"、 enableLookups="false" redirectPort="8443" acceptCount="100" connectionTimeout="**300**" disableUploadTimeout="true" />
回退方案	还原 tomcat/conf/server.xml
判断依据	**1、判定条件** 查看 tomcat/conf/server.xml **2、检测操作** 登陆 tomcat 默认页面 http://ip:8080/manager/html ，使用管理账号登陆
实施风险	高

重要等级	★★
备注	

4.1.2 SHG-Tomcat-04-01-02

编号	SHG-Tomcat-04-01-02
名称	Tomcat 错误页面重定向
实施目的	更改 Tomcat 错误页面重定向页面,增加系统安全性
问题影响	不安全性增加
系统当前状态	查看 tomcat/conf/web.xml
实施步骤	**1、参考配置操作** (1)配置 tomcat/conf/web.xml 文件: 在最后</web-app>一行之前加入以下内容: <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> 第一个<error-page></error-page>之间的配置实现了将 404 未找到 jsp 网页的错误导向 noFile.htm 页面,也可以用类似方法添加其多的错误代码导向页面，如 403,500 等。 第二个<error-page></error-page>之间的配置实现了当 jsp 网页出现 java.lang.NullPointerException 导常时，转向 error.jsp 错误页面，还需要在第个 jsp 网页中加入以下内容: <%@ page errorPage="/error.jsp" %>

	典型的 error.jsp 错误页面的程序写法如下:
	<%@ page contentType="text/html;charset=GB2312"%>
	<%@ page isErrorPage="true"%>
	<html>
	<head><title>错误页面</title></head>
	<body> 出 错 了 ： </p> 错 误 信 息 ： <%= exception.getMessage() %>
	
	Stack Trace is : <pre><%
	java.io.CharArrayWriter cw = new java.io.CharArrayWriter();
	java.io.PrintWriter pw = new java.io.PrintWriter(cw,true);
	exception.printStackTrace(pw);
	out.println(cw.toString());
	%></pre>
	</body>
	</html>
	当出现 NullPointerException 异常时 tomcat 会把网页导入到 error.jsp，且会打印出出错信息。

回退方案	还原 tomcat/conf/web.xml
判断依据	**1、判定条件** 查看 tomcat/conf/web.xml **2、检测操作** URL 地址栏中输入 http://ip:8800/manager~~~
实施风险	高
重要等级	★
备注	

4.1.3 SHG-Tomcat-04-01-03

编号	SHG-Tomcat-04-01-03
名称	禁止 tomcat 列表显示文件
实施目的	禁止 tomcat 列表显示文件,增加系统安全性
问题影响	不安全性增加
系统当前状态	查看 tomcat/conf/web.xml
实施步骤	**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
回退方案	还原 tomcat/conf/web.xml
判断依据	**1、判定条件** 查看 tomcat/conf/web.xml **2、检测操作** 直接访问 http://ip:8800/webadd
实施风险	高
重要等级	★
备注	