

培训教育  
Training Services



# 中间件安全

主讲：Gnosis

## 4.1.3 tomcat

---

Tomcat 服务器的安全设置

Tomcat 服务器的日志审计方法

# Tomcat 服务器的安全设置

---

了解 Tomcat 服务器启动的权限

了解 Tomcat 服务器后台管理地址和修改管理账号密码的方法

了解隐藏 Tomcat 版本信息的方法

了解如何关闭不必要的接口和功能

了解如何禁止目录列表，防止文件名泄露

掌握 Tomcat 服务器通过后台获取权限的方法

掌握 Tomcat 样例目录 session 操纵漏洞

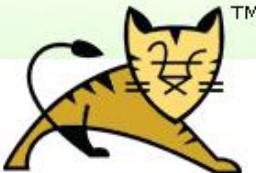
# Tomcat 服务器的安全设置

Tomcat 是一个小型的轻量级应用服务器，在中小型系统和并发访问用户不是很多的场合下被普遍使用，是开发和调试 JSP 程序的首选。

Home Documentation Configuration Examples Wiki Mailing Lists Find Help

## Apache Tomcat/7.0.81

If you're seeing this, you've successfully installed Tomcat. Congratulations!



Recommended Reading:

- [Security Considerations HOW-TO](#)
- [Manager Application HOW-TO](#)
- [Clustering/Session Replication HOW-TO](#)

Developer Quick Start

<a href="#">Tomcat Setup</a>	<a href="#">Realms &amp; AAA</a>	<a href="#">Examples</a>	<a href="#">Servlet Specifications</a>
<a href="#">First Web Application</a>	<a href="#">JDBC DataSources</a>		<a href="#">Tomcat Versions</a>

**Managing Tomcat**  
For security, access to the [manager webapp](#) is restricted. Users are defined in:  
`$CATALINA_HOME/conf/tomcat-users.xml`  
In Tomcat 7.0 access to the manager application is split between different users.  
[Read more...](#)

**Documentation**  
[Tomcat 7.0 Documentation](#)  
[Tomcat 7.0 Configuration](#)  
[Tomcat Wiki](#)  
Find additional important configuration information in:  
`$CATALINA_HOME/RUNNING.txt`

**Getting Help**  
[FAQ and Mailing Lists](#)  
The following mailing lists are available:  
[tomcat-announce](#)  
Important announcements, releases, security vulnerability notifications. (Low volume).  
[tomcat-users](#)  
User support and discussion

Server Status  
Manager App  
Host Manager

# Tomcat 服务器的安全设置 —— 了解 Tomcat 服务器启动的权限

- 1、tomcat启动用户权限必须为非root权限，尽量降低tomcat启动用户的目录访问权限；
- 2、如需直接对外使用80端口，可通过普通账号启动后，配置iptables规则进行转发。
- 备注：避免一旦tomcat服务被入侵，黑客直接获取高级用户权限危害整个server的安全。

基于安全考虑，将tomcat的使用权限赋给admin组， admin用户，只要设置到这个组中，即可以使用tomcat。这样一来可以防止用户误删系统或其他用户的文件；二来即使tomcat中的项目有漏洞遭到攻击，也不至于破坏系统。

**chown -R admin.admin tomcat**

```
drwxr-xr-x. 6 root  root  4096 Jul 28  2015 apr
drwxr-xr-x. 5 root  root  4096 Jul 28  2015 apr-util
drwxr-xr-x. 8 root  root  4096 Apr 11  2015 jdk1.7.0_79
drwxr-xr-x. 6 root  root  4096 Jul 28  2015 nginx
drwxr-xr-x. 9 admin  admin  4096 Jul 13  2015 tomcat6.0.43
drwxr-xr-x  9 root  root  4096 Feb  1  2016 tomcat7.0.61
```

# Tomcat 服务器的安全设置 —— 了解 Tomcat 服务器启动的权限

## 设置启动脚本

```
#!/bin/bash
# Tomcat Settings
export CATALINA_BASE1=/data/Domains/www.123.com/server1
WHO=`whoami`
LOG=`date --date='1 months ago' +%Y-%m`
#####
#####starting#####
start() {
for CATALINA_BASE in $CATALINA_BASE1
do
    echo "*****"
    echo "***      tomcat starting action      ***"
    echo "*****"
    rm -fr $CATALINA_BASE/logs/*$LOG*
    if [[ $WHO == root ]];then
        su - admin -c $CATALINA_BASE/bin/start.sh|awk '{printf'
    elif [[ $WHO == admin ]];then
        $CATALINA_BASE/bin/start.sh|awk '{printf "..."}END{print
    fi
}
```

```
[root@j3_10010003 www.123.com]# ps aux | grep tomcat
admin      1379  0.5 10.9 3967212 209112 ?      Sl  17:02   0:05 /data/server/jdk1.7.0_79/bin/java -Djava.util.logging.config.file=/data/Domains/www.123.com/server1/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -server -Xms2048m -Xmx2048m -Xmn512m -XX:PermSize=512M -XX:MaxPermSize=512M -XX:UseGCOverheadLimit -Djava.awt.headless=true -Dnet.spy.log.LoggerImpl=net.spy.memcached.compat.log.Log4JLogger -Dorg.apache.jasper.compiler.Parser.STRICT_QUOTE_ESCAPING=false -Dorg.apache.el.parser.SKIP_IDENTIFIER_CHECK=true -Djava.library.path=/usr/local/apr/lib -Djava.endorsed.dirs=/data/server/tomcat7.0.61/endorsed -classpath /data/server/tomcat7.0.61/bin/bootstrap.jar:/data/server/tomcat7.0.61/bin/tomcat-juli.jar -Dcatalina.base=/data/Domains/www.123.com/server1 -Dcatalina.home=/data/server/tomcat7.0.61 -Djava.io.tmpdir=/data/Domains/www.123.com/server1/temp org.apache.catalina.startup.Bootstrap -config /data/Domains/www.123.com/server1/conf/server.xml start
root      2147  0.0  0.0 103244    880 pts/0     S+  17:21   0:00 grep tomcat
```

# IIS 服务器的安全设置——了解 Tomcat 服务器后台管理地址和修改管理账号密码的方法

Home Documentation Configuration Examples Wiki Mailing Lists

Find Help

## Apache Tomcat/7.0.81

If you're seeing this, you've successfully installed Tomcat. Congratulations!



Recommended Reading:

[Security Considerations HOW-TO](#)

[Manager Application HOW-TO](#)

[Clustering/Session Replication HOW-TO](#)

Server Status

Manager App

Host Manager

### Developer Quick Start

[Tomcat Setup](#)

[First Web Application](#)

[Realms & AAA](#)

[JDBC Data Sources](#)

[Examples](#)

[Servlet Specifications](#)

[Tomcat Versions](#)

### Managing Tomcat

For security, access to the [manager webapp](#) is restricted. Users are defined in:

### Documentation

[Tomcat 7.0 Documentation](#)

[Tomcat 7.0 Configuration](#)

### Getting Help

[FAQ and Mailing Lists](#)

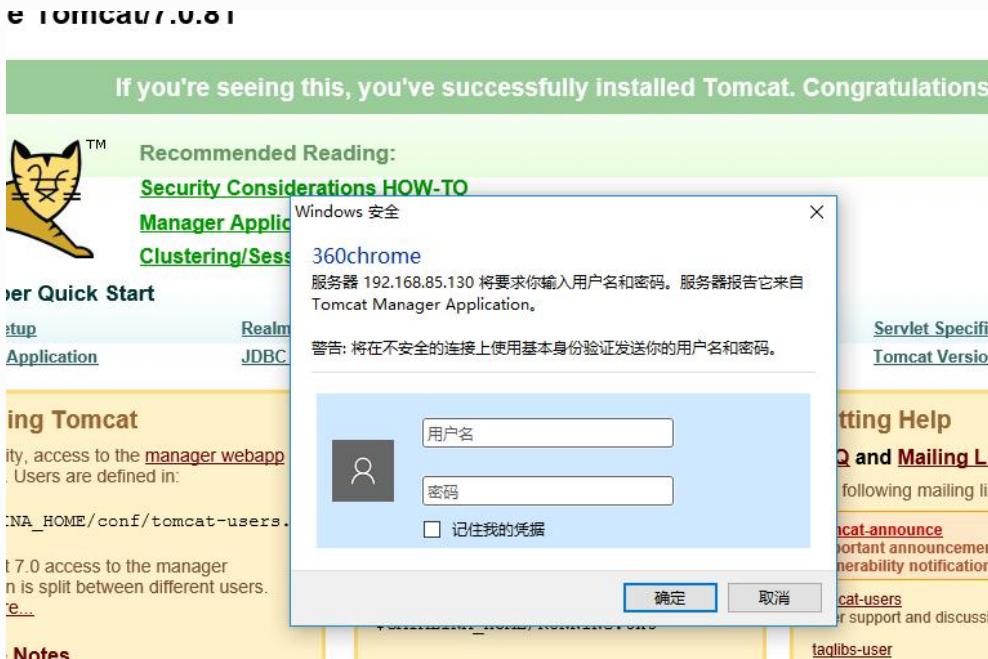
The following mailing lists are available:

tomcat服务器http://localhost:8080/

这样访问，点击Manager App后要求输入用户名和密码才能进入管理应用界面

# IIS 服务器的安全设置——了解 Tomcat 服务器后台管理地址和修改管理账号密码的方法

## 弹出



打开tomcat-users.xml这个文件  
进行如下配置  
在</tomcat-users>节点的前面

```
<role rolename="manager-gui"/>
    <user username="admin" password="admin" roles="manager-gui"/>
<!--

<role rolename="tomcat"/>
    <role rolename="role1"/>
    <user username="tomcat" password=<must-be-changed> roles="tomcat"/>
    <user username="both" password=<must-be-changed> roles="tomcat,role1"/>
    <user username="role1" password=<must-be-changed> roles="role1"/>
-->
</tomcat-users>
```

# IIS 服务器的安全设置——了解 Tomcat 服务器后台管理地址和修改管理账号密码的方法

进行这样的配置后保存，重启tomcat服务器  
再进行访问http://localhost:8080/  
点击Manager App后输入用户名为admin和密码为admin即可进入管理应用界面

**Tomcat Web Application Manager**

Message:	OK
----------	----

**Manager**

<a href="#">List Applications</a>	<a href="#">HTML Manager Help</a>	<a href="#">Manager Help</a>	<a href="#">Server Status</a>
-----------------------------------	-----------------------------------	------------------------------	-------------------------------

**Applications**

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	<a href="#">Start</a> <a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Undeploy</a> <a href="#">Expire sessions</a> with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	<a href="#">Start</a> <a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Undeploy</a> <a href="#">Expire sessions</a> with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	0	<a href="#">Start</a> <a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Undeploy</a> <a href="#">Expire sessions</a> with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	<a href="#">Start</a> <a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Undeploy</a> <a href="#">Expire sessions</a> with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	1	<a href="#">Start</a> <a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Undeploy</a> <a href="#">Expire sessions</a> with idle ≥ 30 minutes

**Deploy**

# Tomcat服务器的安全设置——了解隐藏 Tomcat 版本信息的方法

---

1、首先备份tomcat

2、进入tomcat的lib目录找到catalina.jar文件

```
[root@localhost lib]# ll catalina.jar  
-rw-r--r--. 1 root root 1676596 8月 11 18:23 catalina.jar
```

3、unzip catalina.jar之后会多出两个文件夹

```
r META-INF  
org
```

4、cd org/apache/catalina/util/ | 编辑配置文件ServerInfo.properties

# Tomcat服务器的安全设置——了解隐藏 Tomcat 版本信息的方法

## 5、编辑配置文件ServerInfo.properties

```
server.info=Apache Tomcat/7.0.81  
server.number=7.0.81.0  
server.built=Aug 11 2017 10:21:27 UTC  
~
```

```
server.info=Apache Tomcat  
server.number=0.0.0.0  
server.built=Aug 11 2017 10:21:27 UTC  
~
```

## 6、将修改后的信息压缩回jar包

```
jar uvf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

## 7.重启服务

The screenshot shows the Apache Tomcat homepage. At the top, there is a navigation bar with links: Home, Documentation, Configuration, Examples, Wiki, and Mailing Lists. To the right of the navigation bar is a 'Find Help' search bar. Below the navigation bar, the text 'Apache Tomcat' is displayed. A green banner at the top of the main content area says 'If you're seeing this, you've successfully installed Tomcat. Congratulations!'. To the left of this banner is the iconic yellow cartoon cat logo. To the right of the banner are three buttons: 'Server Status', 'Manager App', and 'Host Manager'. In the center of the page, under the heading 'Recommended Reading:', there are four links: 'Security Considerations HOW-TO', 'Manager Application HOW-TO', and 'Clustering/Session Replication HOW-TO'. At the bottom of the page, there are several navigation links: 'Developer Quick Start', 'Tomcat Setup', 'Realms & AAA', 'Examples', and 'Servlet Specifications'.

# Tomcat服务器的安全设置——了解如何关闭不必要的接口和功能

---

## ➤ 禁用管理端

- 1、删除默认的 {Tomcat安装目录} /conf/tomcat-users.xml文件，重启tomcat后会自动生成新的文件；
- 2、删除 {Tomcat安装目录} /webapps下默认的所有目录和文件；
- 3、将tomcat应用根目录配置为tomcat安装目录以外的目录。
- 配置样例：

```
<Context path="" docBase="/home/work/local/tomcat_webapps"  
debug="0" reloadable="false" crossContext="true" />
```
- 备注：

对于前端web模块，Tomcat管理端属于tomcat的高危安全隐患，一旦被攻破，黑客通过上传 web shell的方式将会直接取得服务器的控制权，后果极其严重

# Tomcat服务器的安全设置——了解如何关闭不必要的接口和功能

---

- telent管理端口保护
- 1、修改默认的8005管理端口为不宜猜测的端口（需要大于1024）；
- 2、修改SHUTDOWN指令为其他字符串。
- 配置样例：
- <Server port="8527" shutdown="dangerous">
- 备注：
- 以上配置想的配置内容只是建议配置，可以按照服务实际情况进行合理配置，但要求端口配置在8000 ~ 8999之间

# Tomcat服务器的安全设置——了解如何关闭不必要的接口和功能

---

- ajp连接端口保护
- 1、修改默认的ajp的8009端口为不以冲突的大于1024的端口；
- 2、通过iptables规则限制ajp端口的访问权限仅为线上机器。
- 配置样例：
- <Connector port="8528" protocol="AJP/1.3" />
- 备注：
- 以上配置项的配置内容仅为建议配置，请按照服务实际情况进行合理配置，但是要求端口配置在8000 ~ 8999之间；
- 保护此端口的目的在于防止线下的测试流量被mod\_jk。

## 文件列表访问控制

- 1、conf/web.xml文件中default部分listings的配置必须为false。
- 配置样例：
- <init-param>
- <param-name>listings</param-name>
- <param-value>false</param-value>
- </init-param>
- 备注：
- false为不列出目录文件，true为允许列出，默认为false

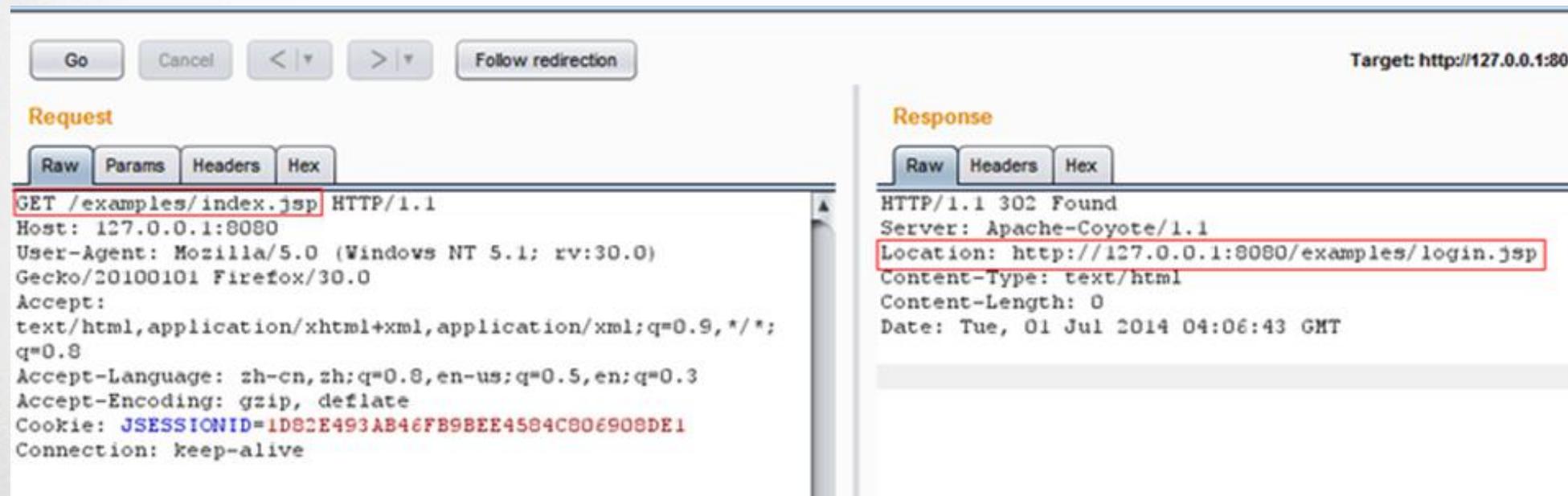
## 利用Tomcat管理后台配置弱点渗透网站实例

- Tomcat 默认存在一个管理后台，默认的管理地址是http://IP或域名:端口号 /manager/html。通过此后台，可以在不重启Tomcat服务的情况下方便地部署、启动、停止或卸载WEB应用。但是，如果配置不当的话就存在很大的安全隐患。

<https://mp.weixin.qq.com/s/eD8B3yCqP38KN8tEd9p7Kg>

# Tomcat服务器的安全设置——掌握 Tomcat 样例目录 session 操纵漏洞

Apache Tomcat默认安装包含“/examples”目录，里面存着众多的样例，其中 session样例(/examples/servlets /servlet/SessionExample)允许用户对 session进行操纵。因为session是全局通用的，所以用户可以通过操纵 session 获取管理员权限。



<http://www.moonsec.com/post-446.html>

# Tomcat 服务器的日志审计方法——了解 Tomcat 的日志种类

---

Catalina引擎的日志文件，文件名catalina.日期.log

Tomcat下内部代码丢出的日志，文件名localhost.日期.log (jsp页面内部错误的异常，  
org.apache.jasper.runtime.HttpJspBase.service  
类丢出的，日志信息就在该文件！)

Tomcat下默认manager应用日志，文件名manager.日期.log

控制台输出的日志，Linux下默认重定向到catalina.out

Access日志（Servlet.xml配置）

应用程序通过log4j.properties: \${catalina.base}/logs/probe.log重定向过来的日志

# Tomcat 服务器的日志审计方法——了解 Tomcat 的日志种类

Tomcat使用的日志配置文件：  
\$CATALINA\_BASE/conf/logging.properties

```
# Unless required by applicable law or agreed to in writing, software
# distributed under the License is distributed on an "AS IS" BASIS,
# WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
# See the License for the specific language governing permissions and
# limitations under the License.

handlers = 1catalina.org.apache.juli.FileHandler, 2localhost.org.apache.juli.FileHandler, 3manager.org.apache.juli.FileHandler, 4host-manager.org.apache.juli.FileHandler, java.util.logging.ConsoleHandler

.handlers = 1catalina.org.apache.juli.FileHandler, java.util.logging.ConsoleHandler
```

catalina.2017-08-02.log	host-manager.2016-12-16.log	localhost.2016-12-21.log	localhost.2017-08-16.log
catalina.2017-08-03.log	host-manager.2016-12-19.log	localhost.2016-12-22.log	localhost.2017-08-17.log
catalina.2017-08-04.log	host-manager.2016-12-22.log	localhost.2016-12-23.log	localhost.2017-08-18.log
catalina.2017-08-06.log	host-manager.2016-12-23.log	localhost.2016-12-24.log	localhost.2017-08-21.log
catalina.2017-08-07.log	host-manager.2017-08-01.log	localhost.2016-12-26.log	localhost.2017-08-22.log
catalina.2017-08-08.log	host-manager.2017-08-22.log	localhost.2016-12-28.log	localhost.2017-08-23.log
catalina.2017-08-09.log	host-manager.2017-08-23.log	localhost.2016-12-29.log	localhost.2017-08-24.log
catalina.2017-08-10.log	jjjjjxin	localhost.2016-12-30.log	localhost.2017-08-25.log
catalina.2017-08-14.log	lasun	localhost.2017-08-01.log	logs
catalina.2017-08-15.log	localhost.2016-12-02.log	localhost.2017-08-02.log	manager.2016-12-16.log
catalina.2017-08-16.log	localhost.2016-12-05.log	localhost.2017-08-03.log	manager.2016-12-19.log
catalina.2017-08-17.log	localhost.2016-12-06.log	localhost.2017-08-04.log	manager.2016-12-22.log
catalina.2017-08-18.log	localhost.2016-12-08.log	localhost.2017-08-06.log	manager.2016-12-23.log
catalina.2017-08-21.log	localhost.2016-12-09.log	localhost.2017-08-07.log	manager.2017-08-01.log
catalina.2017-08-22.log	localhost.2016-12-12.log	localhost.2017-08-08.log	manager.2017-08-22.log
catalina.2017-08-23.log	localhost.2016-12-13.log	localhost.2017-08-09.log	manager.2017-08-23.log
catalina.2017-08-24.log	localhost.2016-12-15.log	localhost.2017-08-10.log	
catalina.2017-08-25.log	localhost.2016-12-16.log	localhost.2017-08-11.log	
catalina.out	localhost.2016-12-19.log	localhost.2017-08-14.log	

# Tomcat 服务器的日志审计方法——掌握 Tomcat 日志的审计方法

pattern表示日志生产的格式，common是tomcat提供的一个标准设置格式。其具体的表达式为

%h %l %u %t "%r" %s %b

但本人建议采用以下具体的配置，因为标准配置有一些重要的日志数据无法生成。

%h %l %u %t "%r" %s %b %T

具体日志产生样式说明如下(从官方文档中摘录)：

安全基线项目名称	Tomcat 审核登录安全基线要求项
安全基线编号	编号 SBL-Tomcat-03-01-01 重要
安全基线项目说明	设备应配置日志功能，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。
检测操作步骤	<p><b>1、参考配置操作</b></p> <p>编辑 server.xml 配置文件，在&lt;HOST&gt;标签中增加记录日志功能</p> <p>将以下内容的注释标记&lt;!-- --&gt;取消</p> <pre>&lt;valve classname="org.apache.catalina.valves.AccessLogValve"&gt;     Directory="logs" prefix="localhost_access_log." Suffix=".txt"     Pattern="common" resolveHosts="false"/&gt;</pre> <p><b>2、补充操作说明</b></p> <p>classname: This MUST be set to org.apache.catalina.valves.AccessLogValve to use the default access log valve.</p> <p>&amp;&lt;60&gt;</p> <p>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；</p> <p>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</p> <p>Suffix: 文件后缀名</p> <p>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</p> <p>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</p>

# Tomcat 服务器的日志审计方法——掌握 Tomcat 日志的审计方法

---

- \* %h 访问的用户IP地址
  - \* %l 访问逻辑用户名，通常返回'-'
  - \* %u 访问验证用户名，通常返回'-'
  - \* %t 访问日时
  - \* %r 访问的方式(post或者是get)，访问的资源和使用的http协议版本
  - \* %s 访问返回的http状态
  - \* %b 访问资源返回的流量
  - \* %T 访问所使用的时间
- 有了这些数据，我们可以根据时间段做以下的分析处理
  - \* 独立IP数统计
  - \* 访问请求数统计
  - \* 访问资料文件数统计
  - \* 访问流量统计
  - \* 访问处理响应时间统计
  - \* 统计所有404错误页面
  - \* 统计所有500错误的页面
  - \* 统计访问最频繁页面
  - \* 统计访问处理时间最久页面
  - \* 统计并发访问频率最高的页面

# Tomcat 总结

---

## 知识子域：Tomcat 服务器的安全设置

了解 Tomcat 服务器启动的权限

了解 Tomcat 服务器后台管理地址和修改管理账号密码的方法

了解隐藏 Tomcat 版本信息的方法

了解如何关闭不必要的接口和功能

了解如何禁止目录列表，防止文件名泄露

掌握 Tomcat 服务器通过后台获取权限的方法

掌握 Tomcat 样例目录 session 操纵漏洞

## 知识子域：Tomcat 服务器的日志审计方法

了解 Tomcat 的日志种类

掌握 Tomcat 日志的审计方法

THANK YOU 感谢观看  
FOR YOUR ATTENTION!

北京谷安天下科技有限公司

谷安天下公司主页：[www.gooann.com](http://www.gooann.com)

谷安培训教育网页：<http://px.gooann.com>

安全意识产品网页：<http://sectv.gooann.com>

产品解决方案网页：<http://product.gooann.com>

谷安信息安全商城：<http://gooannpx.taobao.com>