Apache Reverse Proxy & AJP

Luckily, Apache has the AJP module precompiled for us. We will need to install it, though, as it doesn't come in default installations. Configuring the AJP-Proxy in our Apache server can be done as follows:

- `Install the libapache2-mod-jk package`
- `Enable the module`
- `Create the configuration file pointing to the target AJP-Proxy port`

Note: As mentioned in the previous section, port 80 is in use in Pwnbox, and Apache also uses it as its default port. You can change Apache's default port on "/etc/apache2/ports.conf" to any other port. If you use port 8080, don't forget to stop nginx beforehand with `sudo nginx -s stop.` In the following configuration, we are using 8009, which is Tomcat's default port for AJP, and this is how we would use it in a real environment. However, to complete the exercise at the end of the previous section, this time using Apache, you should specify the IP and port of the target you will spawn (they will both be visible right next to "Target:"). The port you will see is essentially mapped to port 8009 of the underlying Docker container.

The required commands and configuration files are the following:

```
Govardhan Gujji22@htb[/htb]$ sudo apt install libapache2-mod-jk
Govardhan Gujji22@htb[/htb]$ sudo a2enmod proxy_ajp
Govardhan Gujji22@htb[/htb]$ sudo a2enmod proxy_http
Govardhan Gujji22@htb[/htb]$ export TARGET="<TARGET_IP>"
Govardhan Gujji22@htb[/htb]$ echo -n """<Proxy *>
Order allow,deny
Allow from all
</Proxy>
ProxyPass / ajp://$TARGET:8009/
ProxyPassReverse / ajp://$TARGET:8009/""" | sudo tee /etc/apache2/sites-available/ajp-proxy.c
Govardhan Gujji22@htb[/htb]$ sudo ln -s /etc/apache2/sites-available/ajp-proxy.conf /etc/apac
Govardhan Gujji22@htb[/htb]$ sudo systemctl start apache2
```

Note: The below cURL command is the one you would normally use, since Apache is listening on port 80 by default. Remember that you had to change port 80 to another one of your choosing. So, to complete the exercise of the previous section, next step would be to specify the port of your choosing while using cURL, "curl http://127.0.0.1:8080" for example.

Accessing the "hidden" Tomcat page

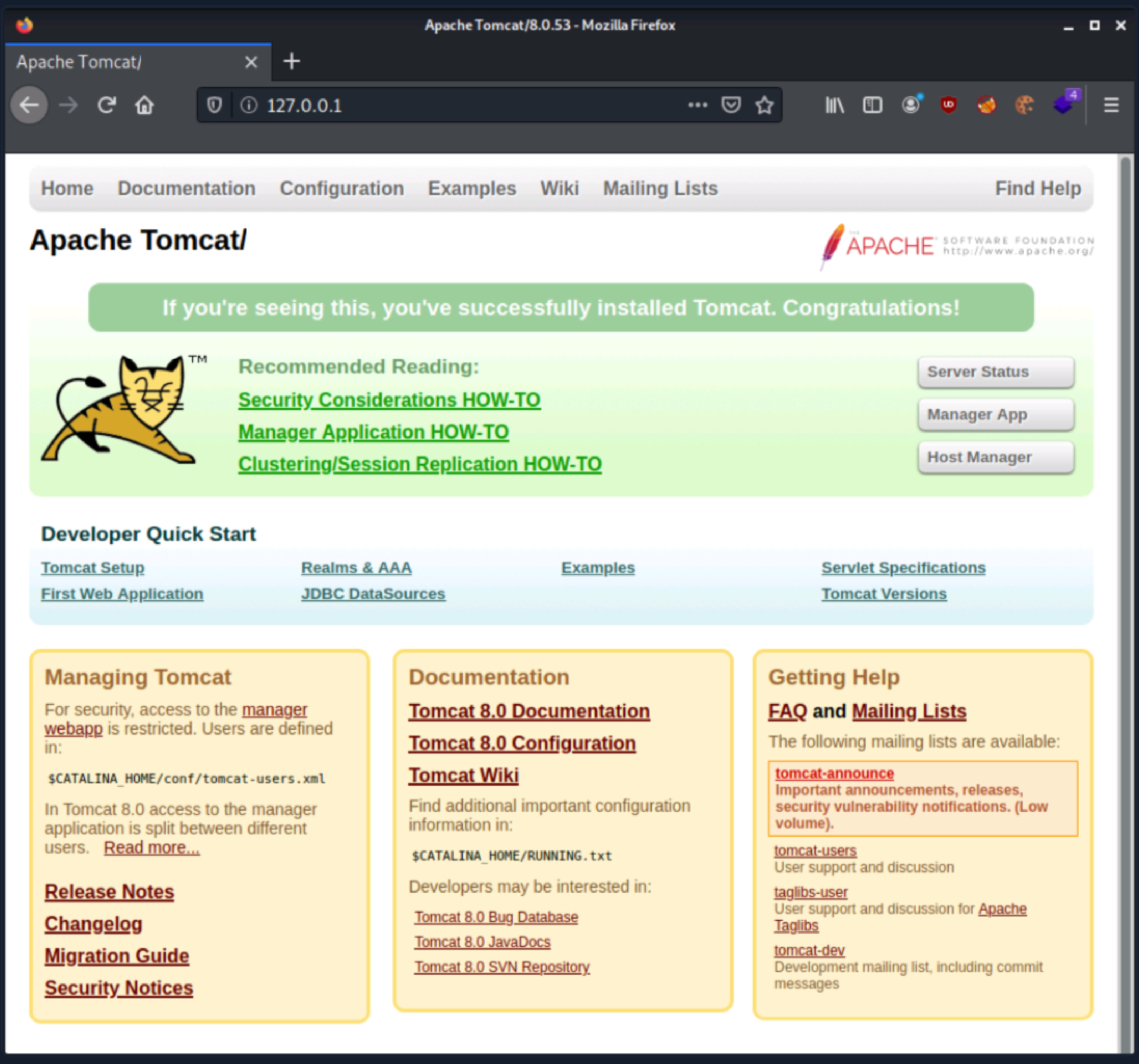
Accessing the "hidden" Tomcat page

```
Govardhan Gujji22@htb[/htb]$ curl http://127.0.0.1

<SNIP>
<!DOCTYPE html>
<html lang="en">
    <head>
        <meta charset="UTF-8" />
        <title>Apache Tomcat/X.X.XX</title>
        <link href="favicon.ico" rel="icon" type="image/x-icon" />
        <link href="favicon.ico" rel="shortcut icon" type="image/x-icon" />
        <link href="tomcat.css" rel="stylesheet" type="text/css" />
    </head>

    <body>
        <div id="wrapper">
            <div id="navigation" class="curved container">
                <span id="nav-home"><a href="https://tomcat.apache.org/">Home</a></span>
                <span id="nav-hosts"><a href="/docs/">Documentation</a></span>
                <span id="nav-config"><a href="/docs/config/">Configuration</a></span>
                <span id="nav-examples"><a href="/examples/">Examples</a></span>
                <span id="nav-wiki"><a href="https://wiki.apache.org/tomcat/FrontPage">Wiki</
                <span id="nav-lists"><a href="https://tomcat.apache.org/lists.html">Mailing l
                <span id="nav-help"><a href="https://tomcat.apache.org/findhelp.html">Find He
                <br class="separator" />
            </div>
            <div id="asf-box">
                <h1>Apache Tomcat/X.X.XX</h1>
            </div>
            <div id="upper" class="curved container">
                <div id="congrats" class="curved container">
                    <h2>If you're seeing this, you've successfully installed Tomcat. Congratu
                </div>
<SNIP>
```

If we configure everything correctly, we will be able to access the Apache Tomcat manager using both cURL and our web browser.


Apache Tomcat/8.0.53 - Mozilla Firefox
Apache Tomcat/
127.0.0.1
Home Documentation Configuration Examples Wiki Mailing Lists Find Help
APACHE SOFTWARE FOUNDATION http://www.apache.org/
Server Status
Manager App
Host Manager

Apache Tomcat/

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
Tomcat Setup
First Web Application
Realms & AAA
JDBC DataSources
Examples
Servlet Specifications
Tomcat Versions

Managing Tomcat
For security, access to the manager webapp is restricted. Users are defined in:
$CATALINA_HOME/conf/tomcat-users.xml
In Tomcat 8.0 access to the manager application is split between different users. Read more...
Release Notes
Changelog
Migration Guide
Security Notices

Documentation
Tomcat 8.0 Documentation
Tomcat 8.0 Configuration
Tomcat Wiki
Find additional important configuration information in:
$CATALINA_HOME/RUNNING.txt
Developers may be interested in:
Tomcat 8.0 Bug Database
Tomcat 8.0 JavaDocs
Tomcat 8.0 SVN Repository

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
taglibs-user
User support and discussion for Apache Taglibs
tomcat-dev
Development mailing list, including commit messages

Previous Next Mark Complete & Next

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left