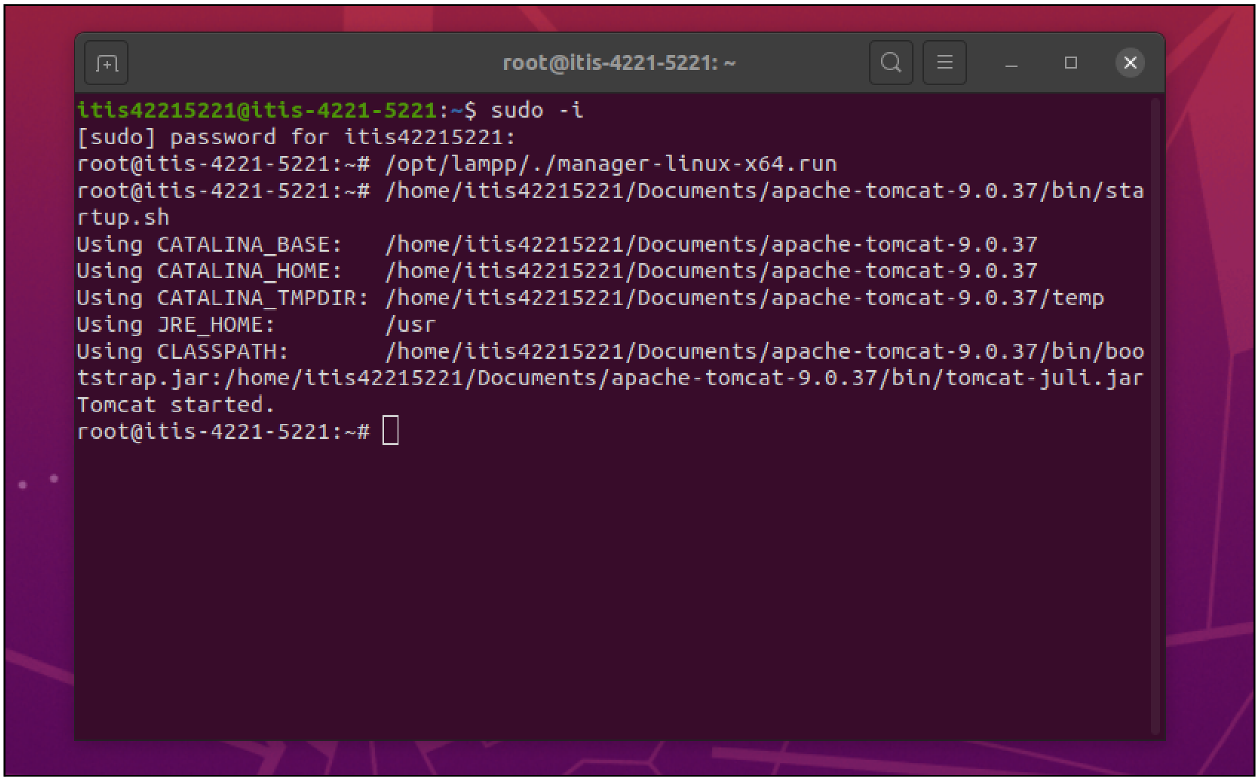
Tunestore 2 - Hosting your Attack Pages

This document shows you how to host your attack pages, which you may want to do in order for some of the attacks to work properly.

Start the Tomcat server like you usually would:

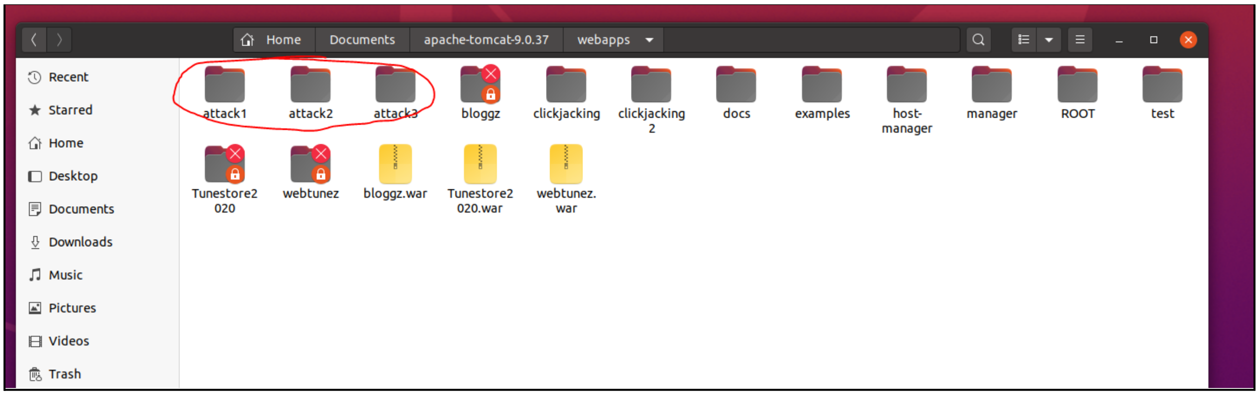


```
itis42215221@itis-4221-5221:~$ sudo -i
[sudo] password for itis42215221:
root@itis-4221-5221:~# /opt/lampp/./manager-linux-x64.run
root@itis-4221-5221:~# /home/itis42215221/Documents/apache-tomcat-9.0.37/bin/sta
rtup.sh
Using CATALINA_BASE:   /home/itis42215221/Documents/apache-tomcat-9.0.37
Using CATALINA_HOME:   /home/itis42215221/Documents/apache-tomcat-9.0.37
Using CATALINA_TMPDIR: /home/itis42215221/Documents/apache-tomcat-9.0.37/temp
Using JRE_HOME:        /usr
Using CLASSPATH:       /home/itis42215221/Documents/apache-tomcat-9.0.37/bin/boo
tstrap.jar:/home/itis42215221/Documents/apache-tomcat-9.0.37/bin/tomcat-juli.jar
Tomcat started.
root@itis-4221-5221:~#
```

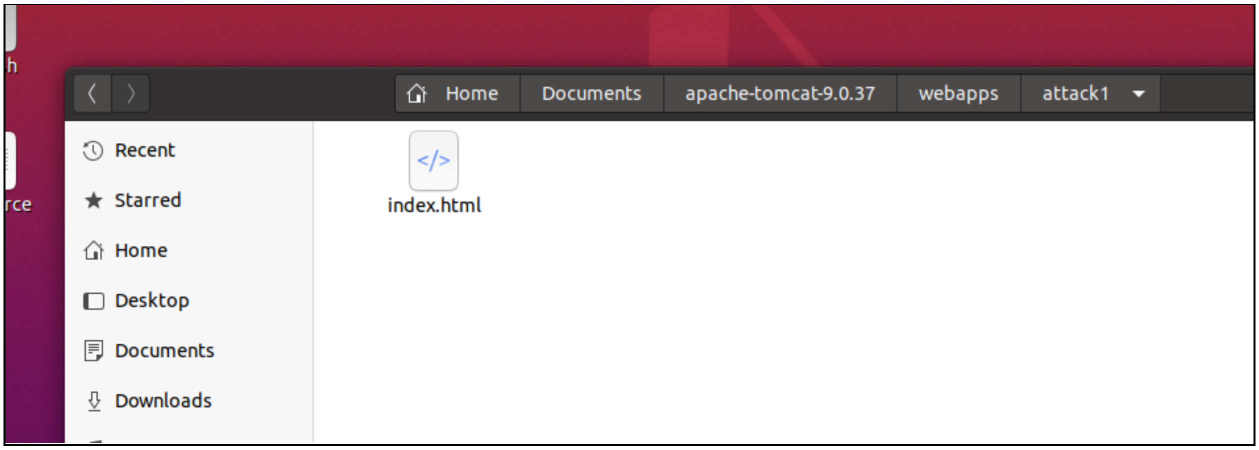
Open up “Files” and navigate to the following folder:

a. Documents > apache-tomcat-9.0.37 > webapps

This is the folder you will put your attack pages in. For instance, if I needed to create three CSRF attack pages for Tunestore II, I would create three different folders like so:



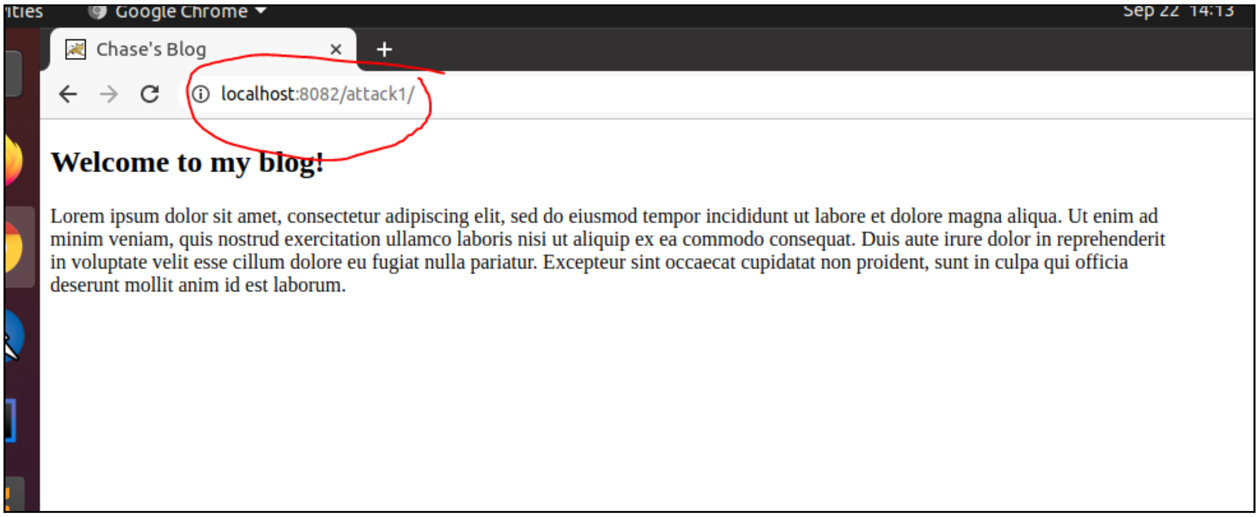
Inside each of these folders, you will need a page called index.html. Here is my attack1 folder:



Now, if I wanted to visit this attack page, I could do so with the following link:

http://localhost:8082/attack1/

Notice that this link is similar to the Tunestore link, except you replace Tunestore2020 with the folder name that your attack page is inside of.



Welcome to my blog!

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Now, your page is hosted, and you can edit your *index.html* file to carry out a CSRF attack when a victim visits the page.