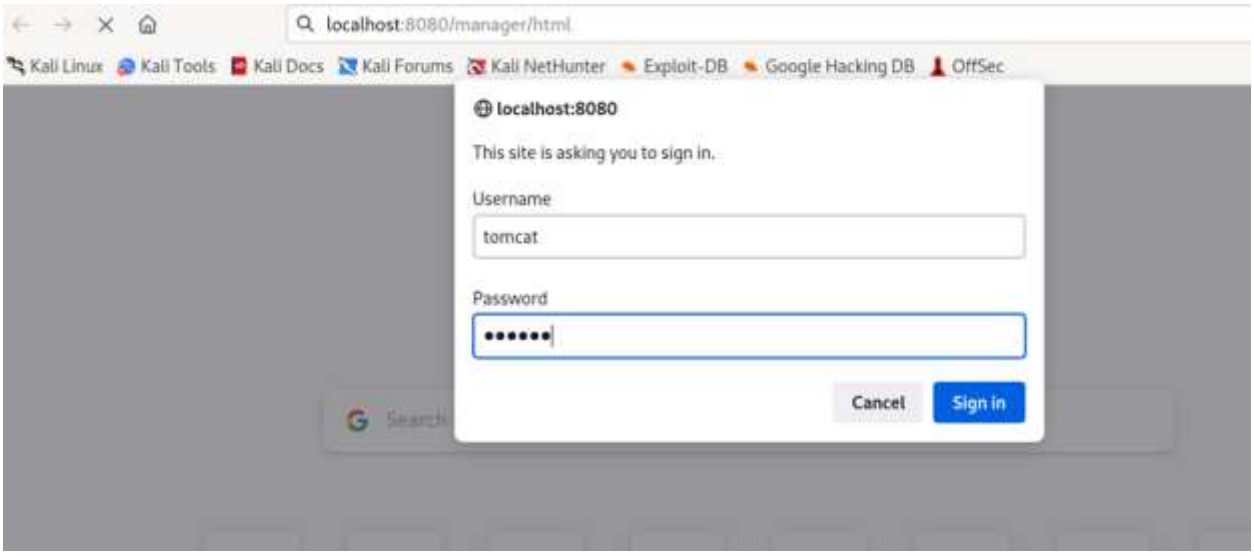
2.3C: Security configurations of Tomcat server

- This document describes the sequence of operations that I performed to hash the password to rectify the problem of clear-text password usage in tomcat-users.xml. Starting with the OWASP Top 10 list, risks include the use of a plain text password (OWASP, 2021). I would not wish to find myself in a situation where details of the admin user of this particular problem at my Tomcat server are disclosed.
- I began by opening the executable./startup.sh in the tomcat folder and starting the Tomcat server.

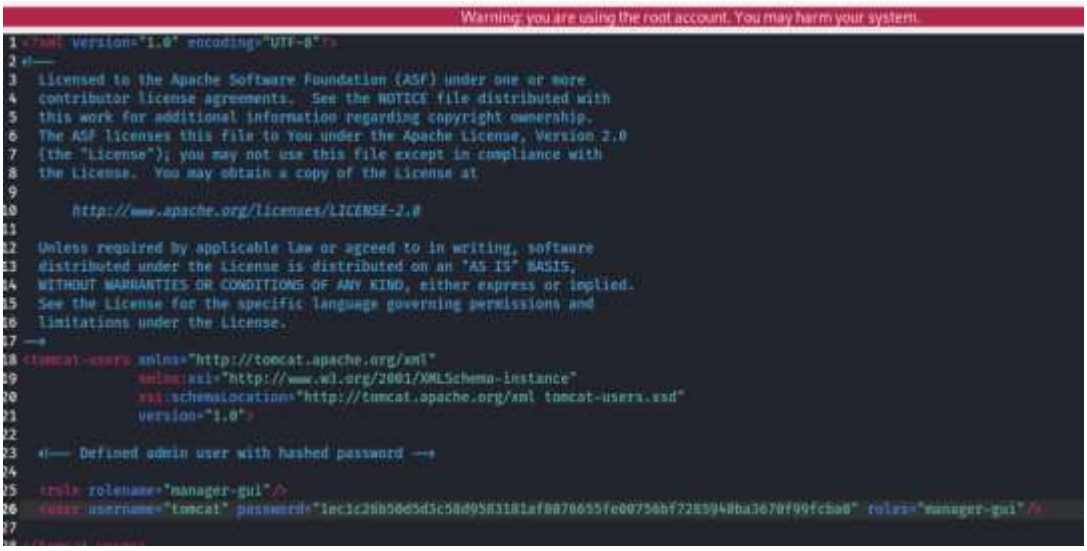
- I then proceeded to clear the text password and replace it with a hashed password by going into the directory of conf/tomcat-user.xml then scanning the code. The file's initial clear-text setup for the admin user was as follows:

I tried the try to login with the credential and was able to gain access.

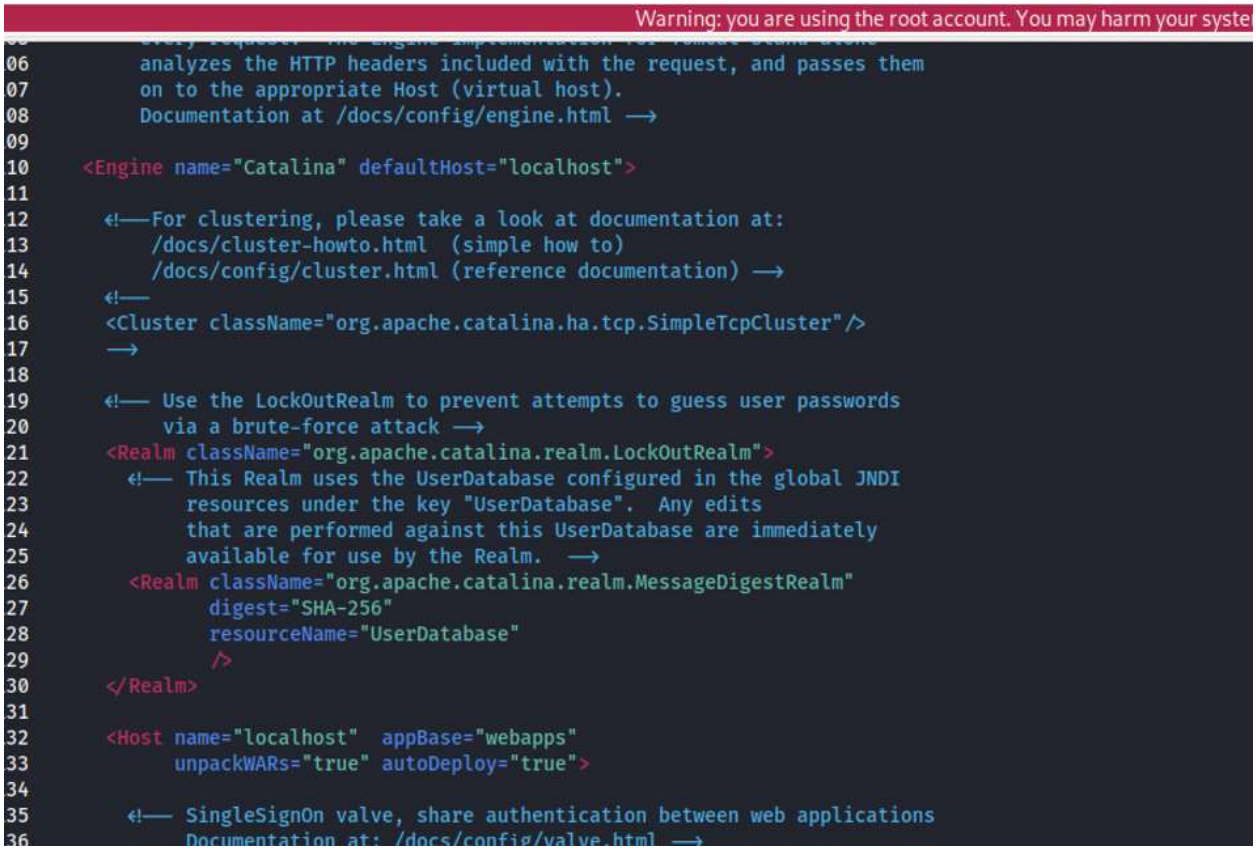



```
┌──(kali㉿kali)-[~]
└─$ echo -n 's3cret' | openssl dgst -sha256
(stdin)= 1ec1c26b50d5d3c58d9583181af8076655fe00756bf7285940ba3670f99fcba0
```

I added the hashed value to the clear text.



- In addition to altering this configuration, I also had to alter the server.xml file so that, when a user tries to sign in, the server will automatically encrypt the plaintext password into the corresponding hashed version.

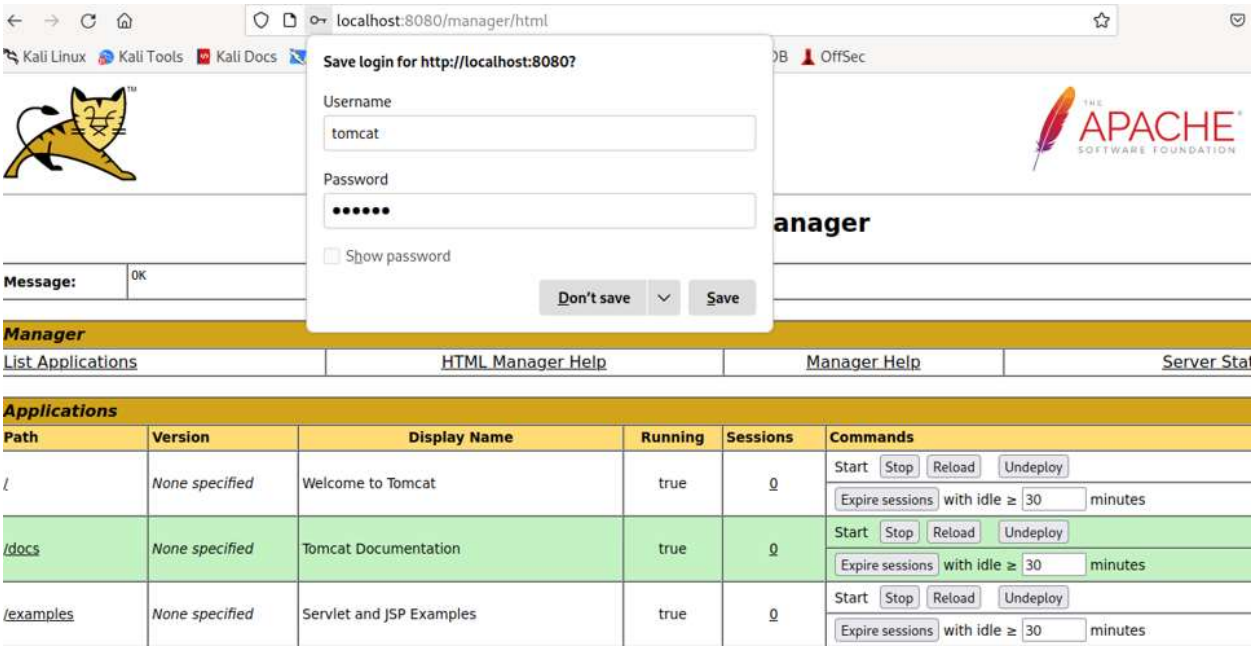


I had to restart the server since the changes I made affected the files of the Tomcat.

```
┌──(root㉿kali)-[/opt/tomcat/apache-tomcat-9.0.75/bin]
└─# chmod +x shutdown.sh

┌──(root㉿kali)-[/opt/tomcat/apache-tomcat-9.0.75/bin]
└─# sudo ./shutdown.sh
Using CATALINA_BASE:   /opt/tomcat/apache-tomcat-9.0.75
Using CATALINA_HOME:   /opt/tomcat/apache-tomcat-9.0.75
Using CATALINA_TMPDIR: /opt/tomcat/apache-tomcat-9.0.75/temp
Using JRE_HOME:        /usr
Using CLASSPATH:       /opt/tomcat/apache-tomcat-9.0.75/bin/bootstrap.jar:/opt/tomcat/apache-tomcat-9.0.75/bin/tomcat-juli.jar
Using CATALINA_OPTS:
NOTE: Picked up JDK_JAVA_OPTIONS:  --add-opens=java.base/java.lang=ALL-UNNAMED --add-opens=java.base/java.io=ALL-UNNAMED --add-opens=java.base/java.util=ALL-UNNAMED --add-opens=java.base/java.util.concurrent=ALL-UNNAMED --add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED

┌──(root㉿kali)-[/opt/tomcat/apache-tomcat-9.0.75/bin]
└─# sudo ./startup.sh
Using CATALINA_BASE:   /opt/tomcat/apache-tomcat-9.0.75
Using CATALINA_HOME:   /opt/tomcat/apache-tomcat-9.0.75
Using CATALINA_TMPDIR: /opt/tomcat/apache-tomcat-9.0.75/temp
Using JRE_HOME:        /usr
Using CLASSPATH:       /opt/tomcat/apache-tomcat-9.0.75/bin/bootstrap.jar:/opt/tomcat/apache-tomcat-9.0.75/bin/tomcat-juli.jar
Using CATALINA_OPTS:
Tomcat started.
```


localhost:8080/manager/html
Kali Linux
Kali Tools
Kali Docs
OffSec
Save login for http://localhost:8080?
Username
tomcat
Password
Show password
Don't save
Save
APACHE
SOFTWARE FOUNDATION
anager
Message:
OK
Manager
List Applications
HTML Manager Help
Manager Help
Server Stat
Applications
Path
Version
Display Name
Running
Sessions
Commands
/
None specified
Welcome to Tomcat
true
0
Start Stop Reload Undeploy
Expire sessions with idle ≥ 30 minutes
/docs
None specified
Tomcat Documentation
true
0
Start Stop Reload Undeploy
Expire sessions with idle ≥ 30 minutes
/examples
None specified
Servlet and JSP Examples
true
0
Start Stop Reload Undeploy
Expire sessions with idle ≥ 30 minutes