

### 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.

```
(root@kali) ~ [/opt/tomcat/apache-tomcat-9.0.75/bin]
# chmod +x startup.sh

(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.
```

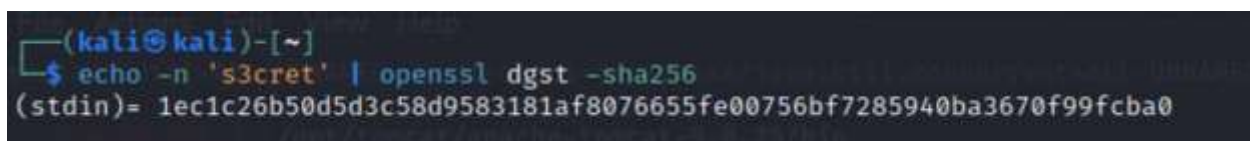
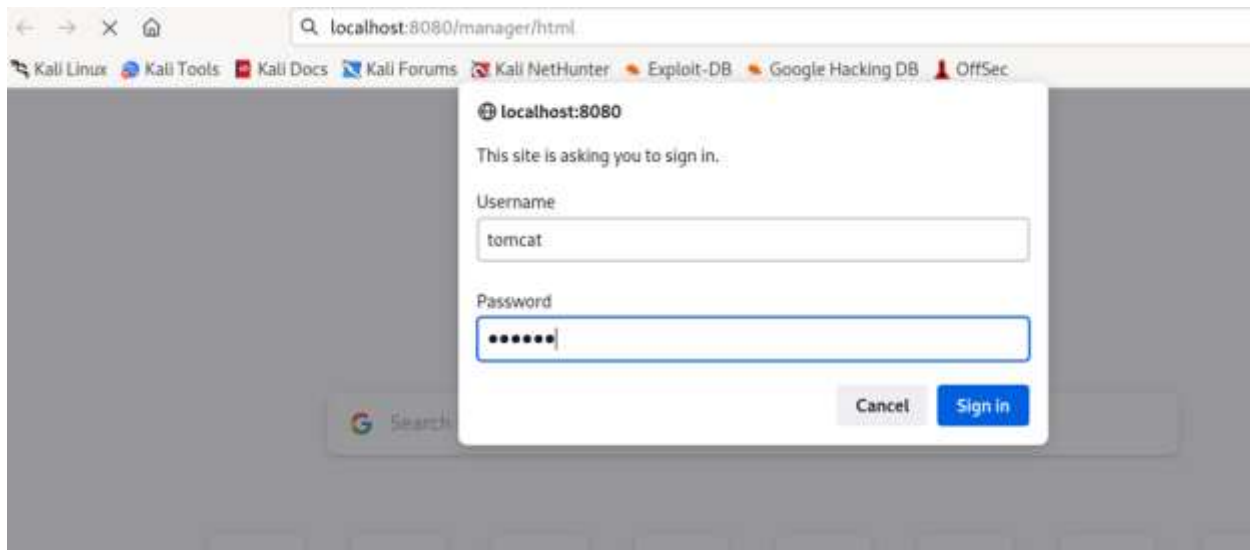
- I then proceeded to clear the text password and replace it with a hashed password by going into the directory of conf/tomcat-user.xml then scanning the code. The file's initial clear-text setup for the admin user was as follows:

```
>
<tomcat-users xmlns="http://tomcat.apache.org/xml"
              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
              xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
              version="1.0">

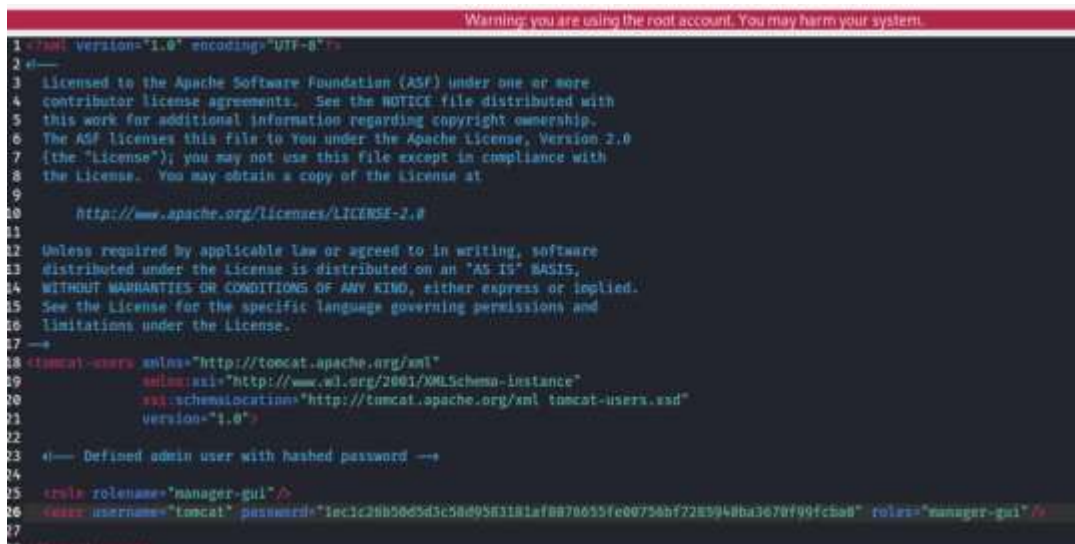
  <role rolename="manager-gui"/>
  <user username="tomcat" password="s3cret" roles="manager-gui"/>
</tomcat-users>

By default, no user is included in the "manager-gui" role required
to operate the "/manager/html" web application.  If you wish to use this app,
you must define such a user - the username and password are arbitrary.
```

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



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.

```

Warning: you are using the root account. You may harm your system
06      analyzes the HTTP headers included with the request, and passes them
07      on to the appropriate Host (virtual host).
08      Documentation at /docs/config/engine.html →
09
10      <Engine name="Catalina" defaultHost="localhost">
11
12          ⚡—For clustering, please take a look at documentation at:
13              /docs/cluster-howto.html (simple how to)
14              /docs/config/cluster.html (reference documentation) →
15          ⚡—
16          <Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
17          →
18
19          ⚡— Use the LockOutRealm to prevent attempts to guess user passwords
20              via a brute-force attack →
21          <Realm className="org.apache.catalina.realm.LockOutRealm">
22              ⚡— This Realm uses the UserDatabase configured in the global JNDI
23                  resources under the key "UserDatabase". Any edits
24                  that are performed against this UserDatabase are immediately
25                  available for use by the Realm. →
26              <Realm className="org.apache.catalina.realm.MessageDigestRealm"
27                  digest="SHA-256"
28                  resourceName="UserDatabase"
29              />
30          </Realm>
31
32          <Host name="localhost" appBase="webapps"
33              unpackWARs="true" autoDeploy="true">
34
35              ⚡— SingleSignOn valve, share authentication between web applications
36              Documentation at: /docs/config/valve.html →

```

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

```

(root@kali)~# cd /opt/tomcat/apache-tomcat-9.0.75/bin
# chmod +x shutdown.sh

(root@kali)~# cd /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)~# cd /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

Save login for http://localhost:8080?

Username  
tomcat

Password  
•••••

☐ Show password

Don't save Save

🐱

THE APACHE®  
SOFTWARE FOUNDATION

anager

Message: OK

Manager

[List Applications](#) [HTML Manager Help](#) [Manager Help](#) [Server Status](#)

Applications

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle ≥ 30 minutes</div>
/docs	None specified	Tomcat Documentation	true	0	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle ≥ 30 minutes</div>
/examples	None specified	Servlet and JSP Examples	true	0	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle ≥ 30 minutes</div>