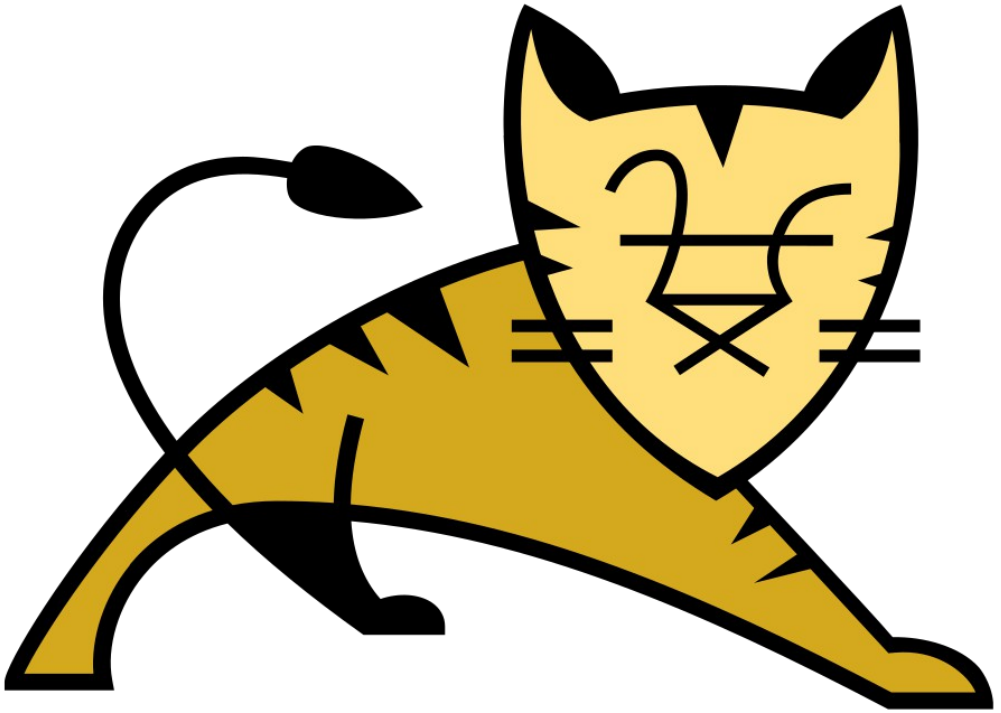
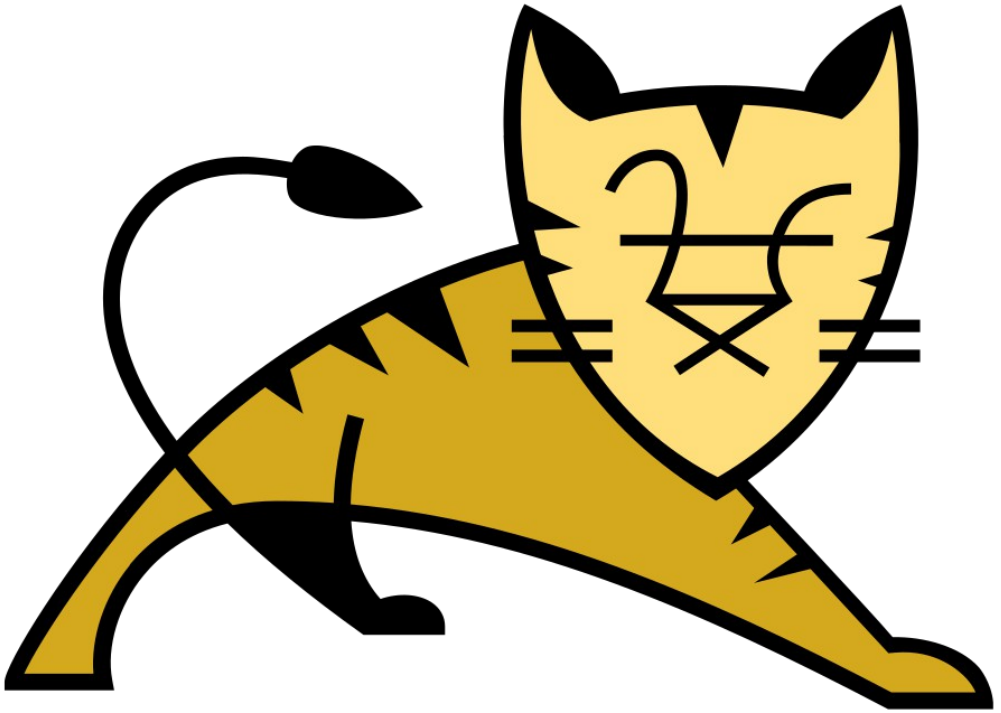
Apache Tomcat (default credentials)



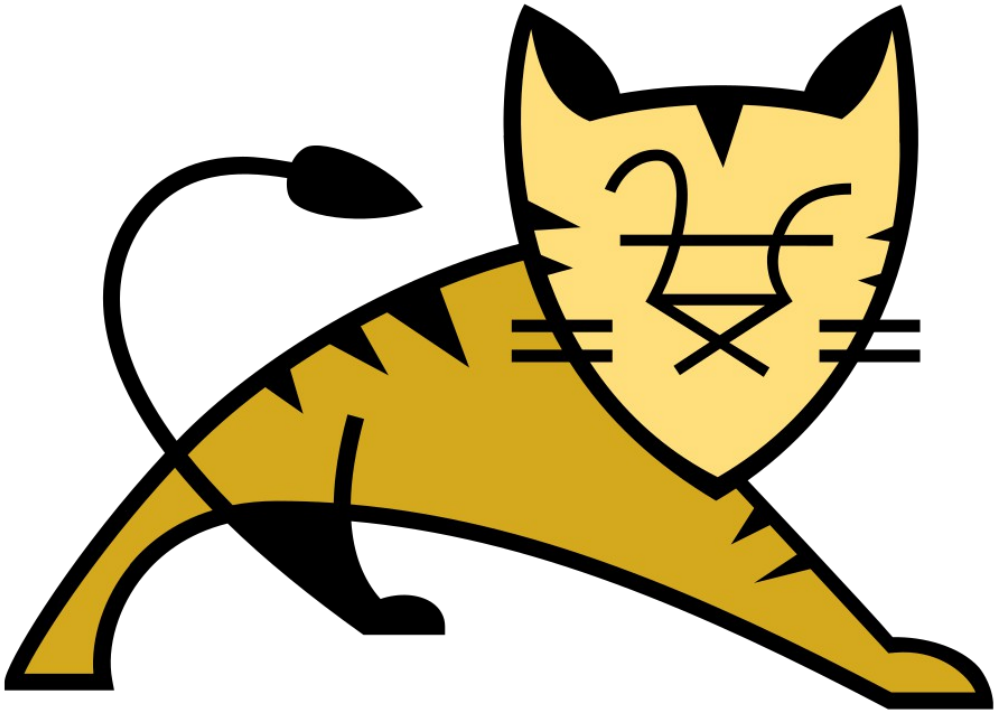
Apache Tomcat is a Java-enabled webserver software which allows Java servlets to be run on webpages

Apache Tomcat (default credentials)



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

Apache Tomcat (default credentials)



In this case, the default credentials for the Tomcat manger page are in place, so we can just login

Privilege Escalation SeImpersonatePrivilege

Privilege Name	Description	State
SeAssignPrimaryTokenPrivilege	Replace a process level token	Disabled
SeIncreaseQuotaPrivilege	Adjust memory quotas for a process	Disabled
SeSystemtimePrivilege	Change the system time	Disabled
SeShutdownPrivilege	Shut down the system	Disabled
SeAuditPrivilege	Generate security audits	Disabled
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeUndockPrivilege	Remove computer from docking station	Disabled
SeImpersonatePrivilege	Impersonate a client after authentication	Enabled

Our user has the Windows SeImpersonatePrivilege, which means they are able to assume the identify of different user in certain cases

Privilege Escalation SeImpersonatePrivilege

Sometimes the SeImpersonatePrivilege can be abused by using a family of Windows exploits called Potato exploits, but modern versions of Windows (Win 10/11) are less likely to be vulnerable

Privilege Escalation PrintSpoofer

A more-modern exploit that takes advantage of the SeImpersonatePrivilege is the PrintSpoofer exploit, which affects Windows 10 / Server 2016 / 2019 operating systems

Privilege Escalation
PrintSpoofer

```
sc query Spooler

SERVICE_NAME: Spooler
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 4  RUNNING
                             (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0×0)
```

In order to conduct a PrintSpoofer attack with SeImpersonatePrivilege, the system must be running the print spooler service, which it is