TRAINING KIT – HOST2

Hardening web application servers

TLP: WHITE

EXCELLIUM

Your first call when it comes to IT and Security!

Agenda

- Labs objective
- Tomcat and web application installation
- Security issues analysis
- Tomcat hardening
- Q&R

Introduction

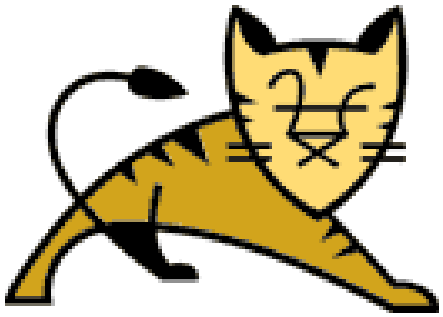
Introduction

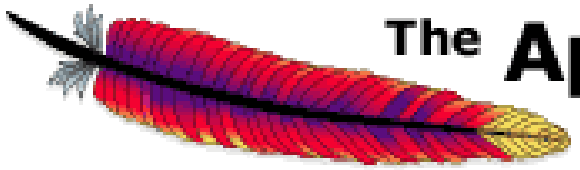
- The labs objective is to discover the impacts of a “default” installation of Tomcat web container and, further, how to harden the installation at differents levels in order to reduce the attack surface.

- The target operating system used will be Windows 2012 R2 because, on Linux environment (ex: Ubuntu / Debian), the package provides a basic hardening level that is not applied into Windows installer of Tomcat.

Introduction

- Tomcat Windows installer version will also be used because, often, Tomcat is provided, as module, of a commercial package and the global installer of the commercial package install Tomcat using default settings.





The Apache Software Foundation
http://www.apache.org/

Tomcat installation

Tomcat installation

Required files are on your working VM:

- **Apache Tomcat 8.0.28 for Windows**
  - C:\Workspace\Courses\trainingkit_host2\apache-tomcat-8.0.28.exe
- **JDK 8 64 bits for Windows**
  - C:\Workspace\Courses\trainingkit_host2\jdk-8u91-windows-x64.exe
- **Vulnerable application**
  - C:\Workspace\Courses\trainingkit_host2\TestVulnApp.war

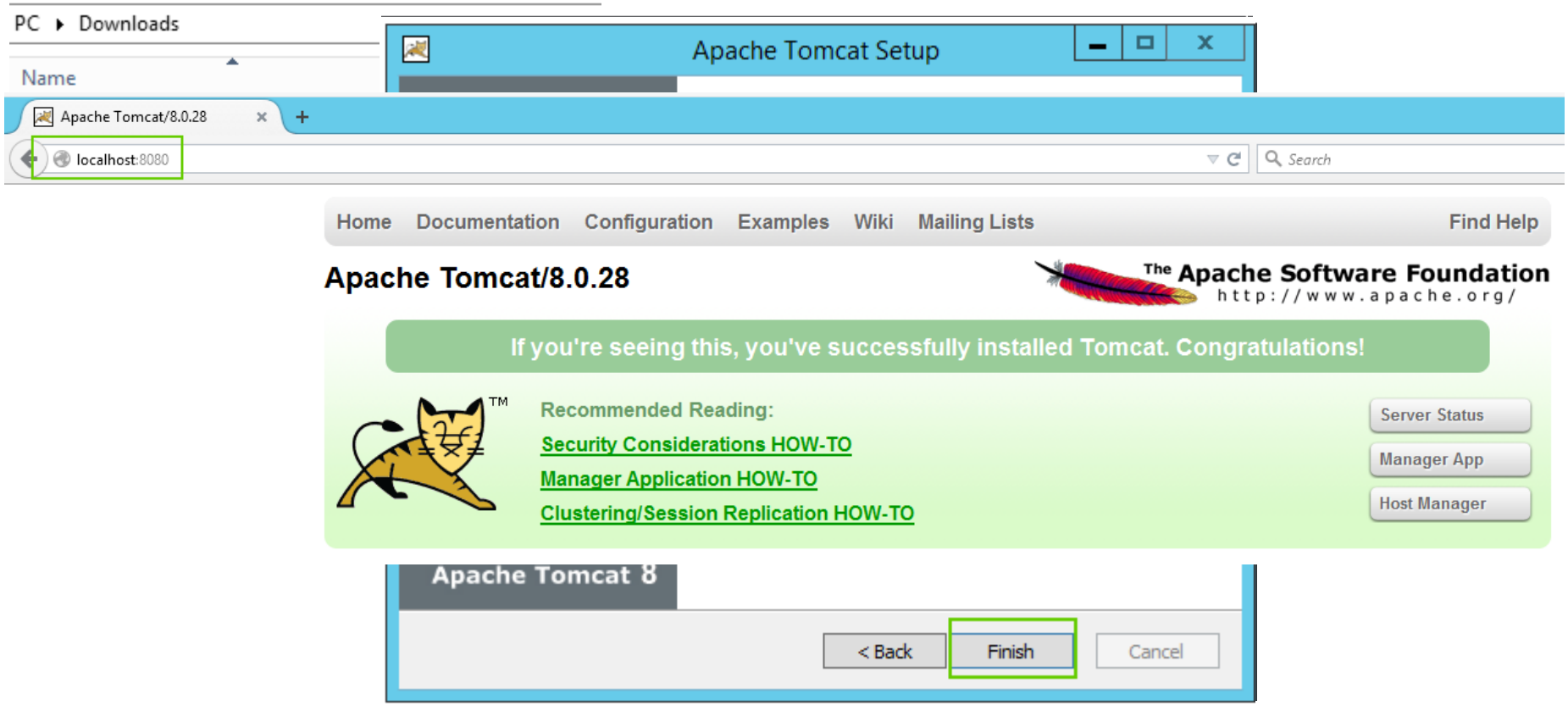
Tomcat installation

- Java JDK installation steps:

EXCELLIUM

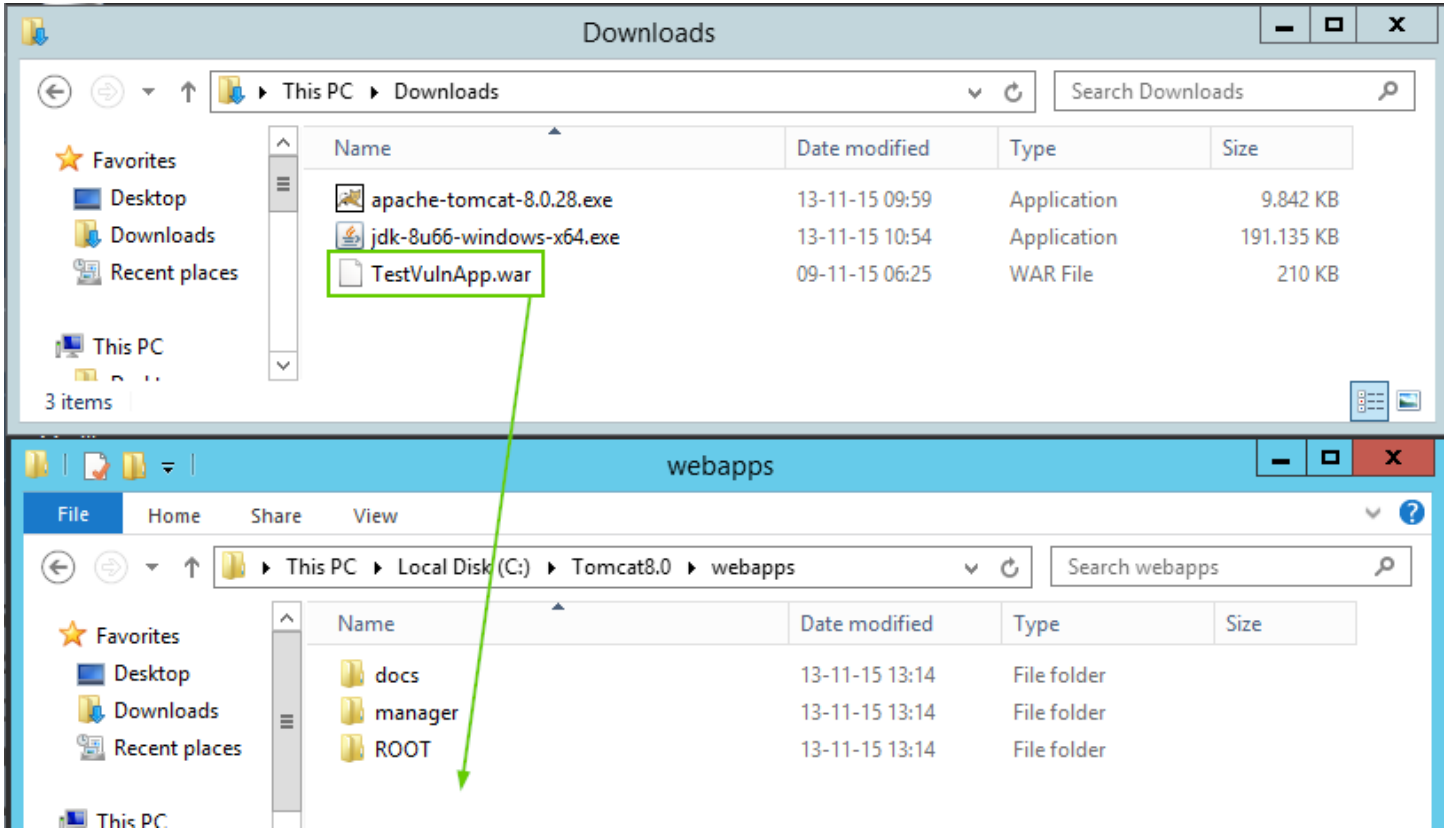
Tomcat installation

- Tomcat installation steps:



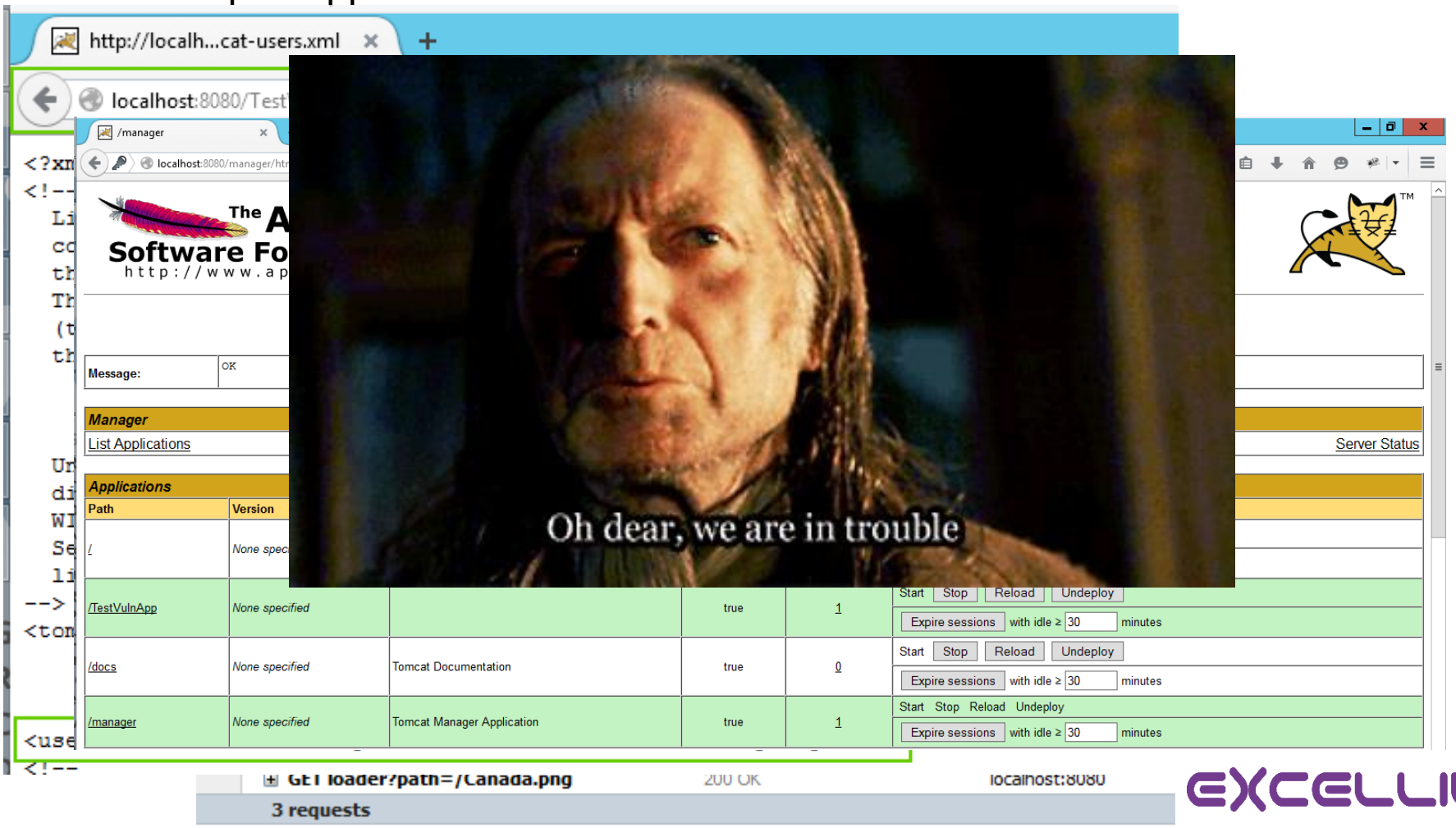
Tomcat installation

- Vulnerable application installation (copy WAR file and wait 5 secs):



Tomcat installation

- Open application access to final users….



Security issues analysis

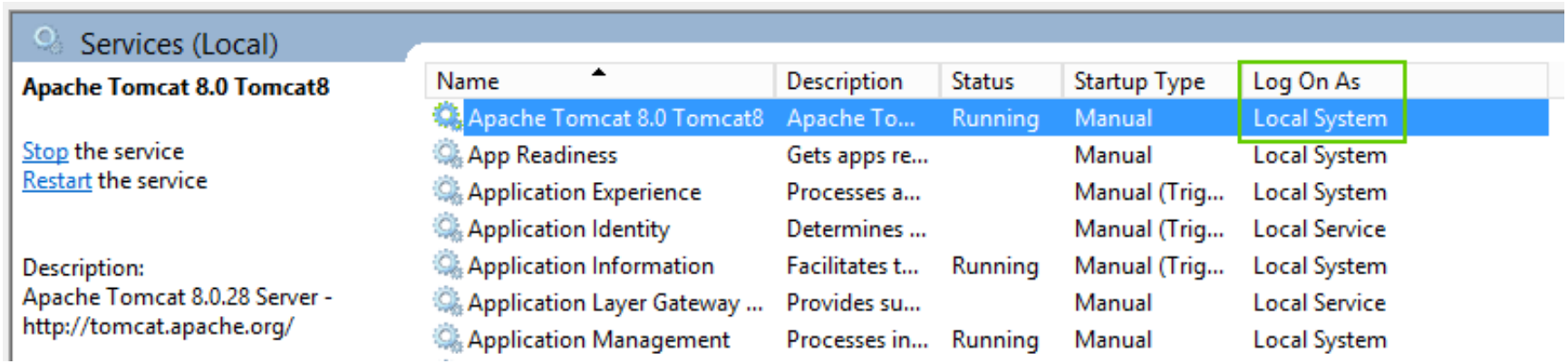
Sec. Issues analysis

- **Cause 1:** Application source code level.

```
@WebServlet("/loader")
public class Loader extends HttpServlet {

    * (non-Javadoc)
    @Override
    protected void doGet(HttpServletRequest req, HttpServletResponse resp) throws ServletException, IOException {
        try {
            String path = req.getParameter("path");
            if (path == null || "".equals(path.trim())) {
                path = "/Luxemburg.png";
            }
            InputStream is = this.getClass().getResourceAsStream(path);
            resp.setContentType("image/png");
            if (is == null) {
                resp.setContentType("text/plain");
                is = new FileInputStream(path);
            }
            IOUtils.copy(is, resp.getOutputStream());
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

Sec. Issues analysis

- **Cause 2:** Windows service credentials configuration level.



EXCELLIUM

Sec. Issues analysis

- **Cause 3:** Tomcat credentials storage protection level.

C:\Tomcat8.0\conf\tomcat-users.xml -

File Edit Selection Find View Goto Tools Project Preferences Help

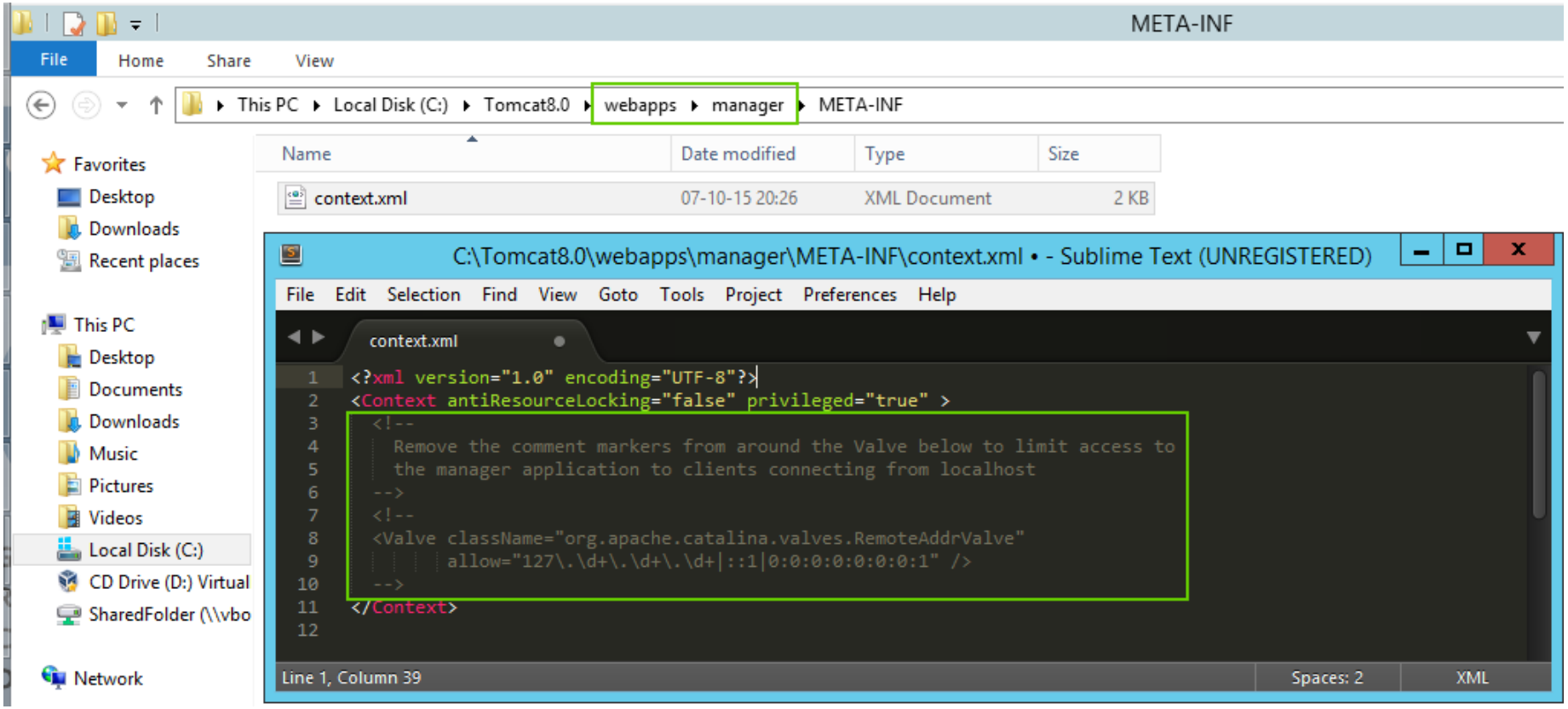
tomcat-users.xml

```
<?xml version='1.0' encoding='cp1252'?>
<!--
  Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<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">
<user username="tomcat" password="tomcat" roles="manager-gui" />
<!--
```

EXCELLIUM

Sec. Issues analysis

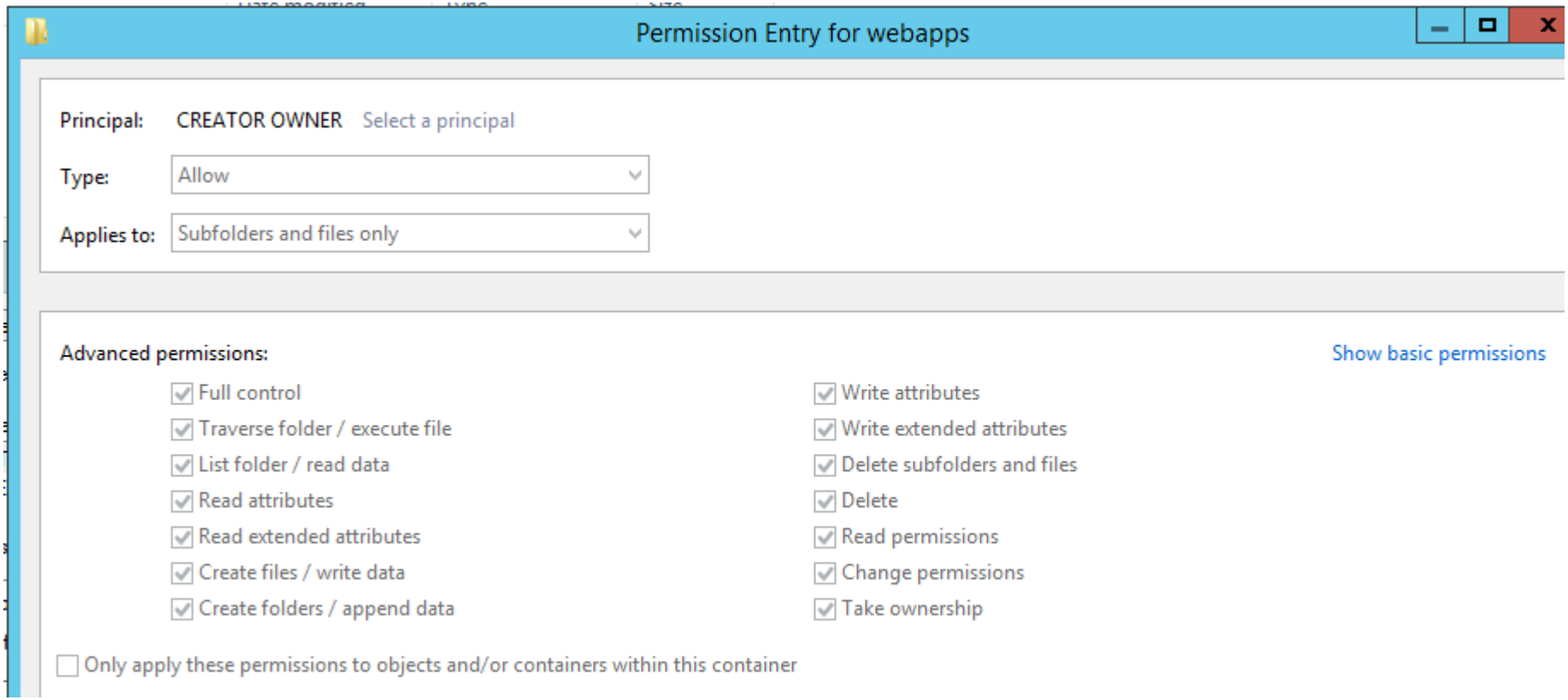
- **Cause 4:** Network access segregation level for access to TC admin app.



EXCELLIUM

Sec. Issues analysis

- **Cause 5:** Access right level for TC owner user on « **webapps** » TC folder.



Sec. Issues analysis

- **Cause 6:** TC JVM Security Manager level.

elp

C:\Tomcat8.0\logs\catalina.2015-11-14.log - Sublime Text (UNREGISTERED)

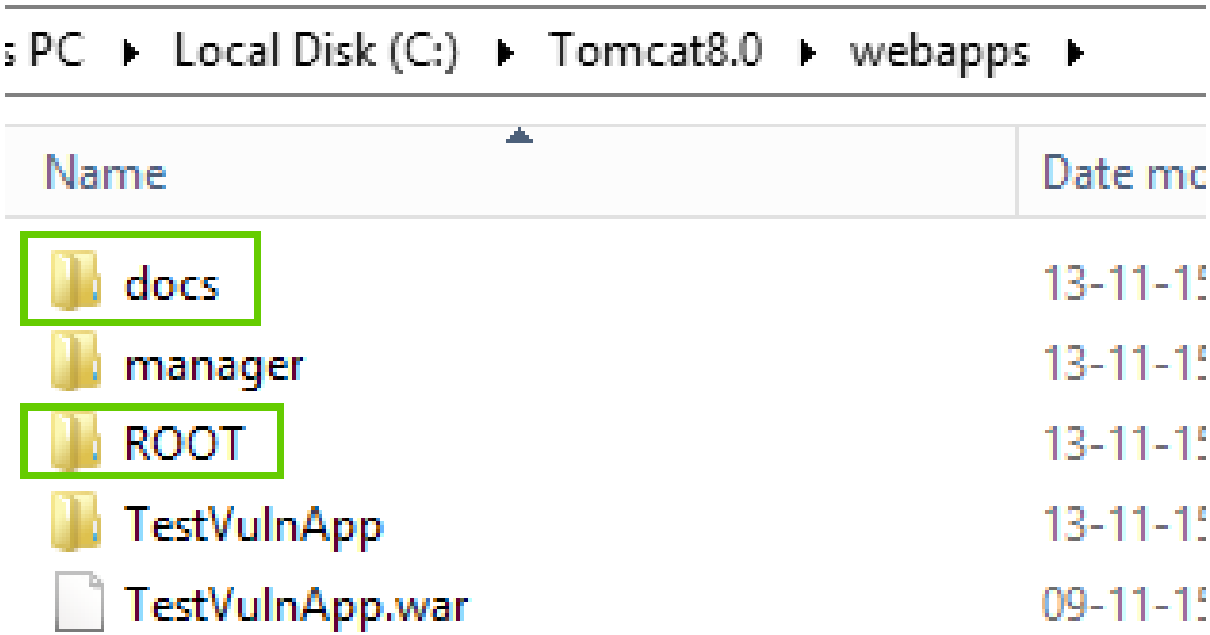
Tools Project Preferences Help

```
[main] org.apache.catalina.startup.VersionLoggerListener.log Server version:        Apache Tomcat/8.0.28
[main] org.apache.catalina.startup.VersionLoggerListener.log Server built:          Oct 7 2015 18:25:21 UTC
[main] org.apache.catalina.startup.VersionLoggerListener.log Server number:         8.0.28.0
[main] org.apache.catalina.startup.VersionLoggerListener.log OS Name:               Windows Server 2012 R2
[main] org.apache.catalina.startup.VersionLoggerListener.log OS Version:            6.3
[main] org.apache.catalina.startup.VersionLoggerListener.log Architecture:          amd64
[main] org.apache.catalina.startup.VersionLoggerListener.log Java Home:             C:\jdk1.8.0_66\jre
[main] org.apache.catalina.startup.VersionLoggerListener.log JVM Version:           1.8.0_66-b18
[main] org.apache.catalina.startup.VersionLoggerListener.log JVM Vendor:            Oracle Corporation
[main] org.apache.catalina.startup.VersionLoggerListener.log CATALINA_BASE:         C:\Tomcat8.0
[main] org.apache.catalina.startup.VersionLoggerListener.log CATALINA_HOME:         C:\Tomcat8.0
[main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Dcatalina.home=C:\Tomcat8.0
[main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Dcatalina.base=C:\Tomcat8.0
[main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djava.endorsed.dirs=C:\Tomcat8.0\endorsed
[main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djava.io.tmpdir=C:\Tomcat8.0\temp
[main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
[main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djava.util.logging.config.file=C:\Tomcat8.0\conf\logging.properties
[main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: exit
[main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Xms128m
[main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Xmx256m
[main] org.apache.catalina.core.AprLifecycleListener.lifecycleEvent The APR based Apache Tomcat Native library which allows optimal performance in product
```

EXCELLIUM

Sec. Issues analysis

- **Cause 7:** TC Documentation and ROOT applications are still online.



Hardening

Hardening

- Based on the security issues analysis, we will apply hardening operations on every security issues, one by one, in order to close as much exploitability path as possible…

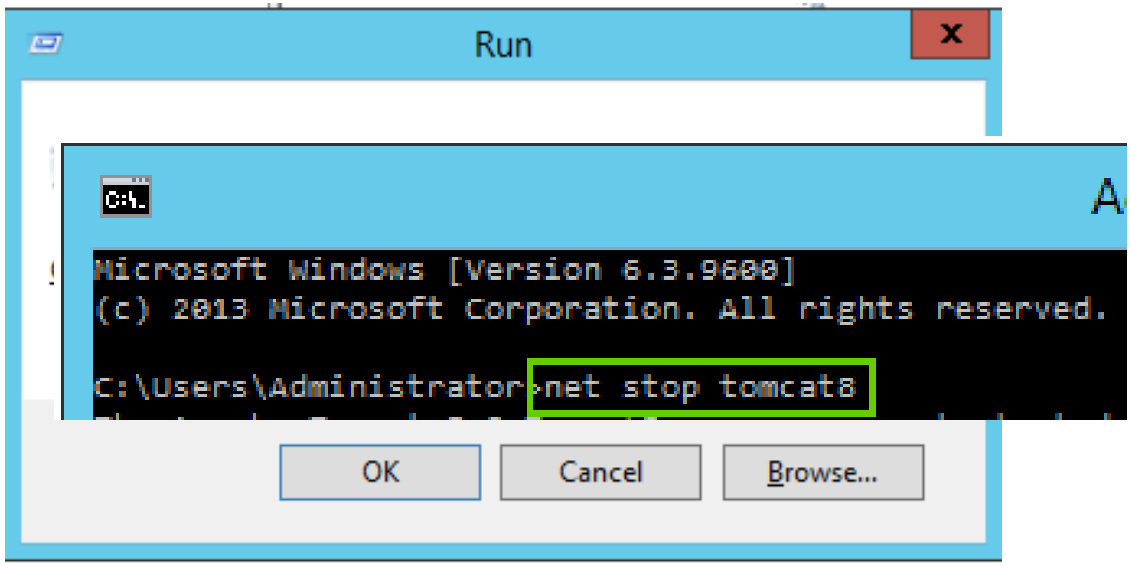
Hardening

As reminder, this is the working areas (**C** = **Cause**):

- **C1:** Application source code level.
- **C2:** Windows service credentials configuration level.
- **C3:** Tomcat credentials storage protection level.
- **C4:** Network access segregation level for access to TC admin app.
- **C5:** Access right level for TC owner user on « **webapps** » TC folder.
- **C6:** TC JVM Security Manager level.
- **C7:** TC Documentation and ROOT applications are still online.

Hardening

!!! Before to start any hardening step, stop Tomcat Windows service !!!



EXCELLIUM

Hardening – C1

→**C1:** Application source code level.

- We assume here that we cannot act on application code because it's a Open Source commercial product and the vendor will provide us a security patch in 6 month !

Hardening – C2

→**C2:** Windows service credentials configuration level.

Objective:

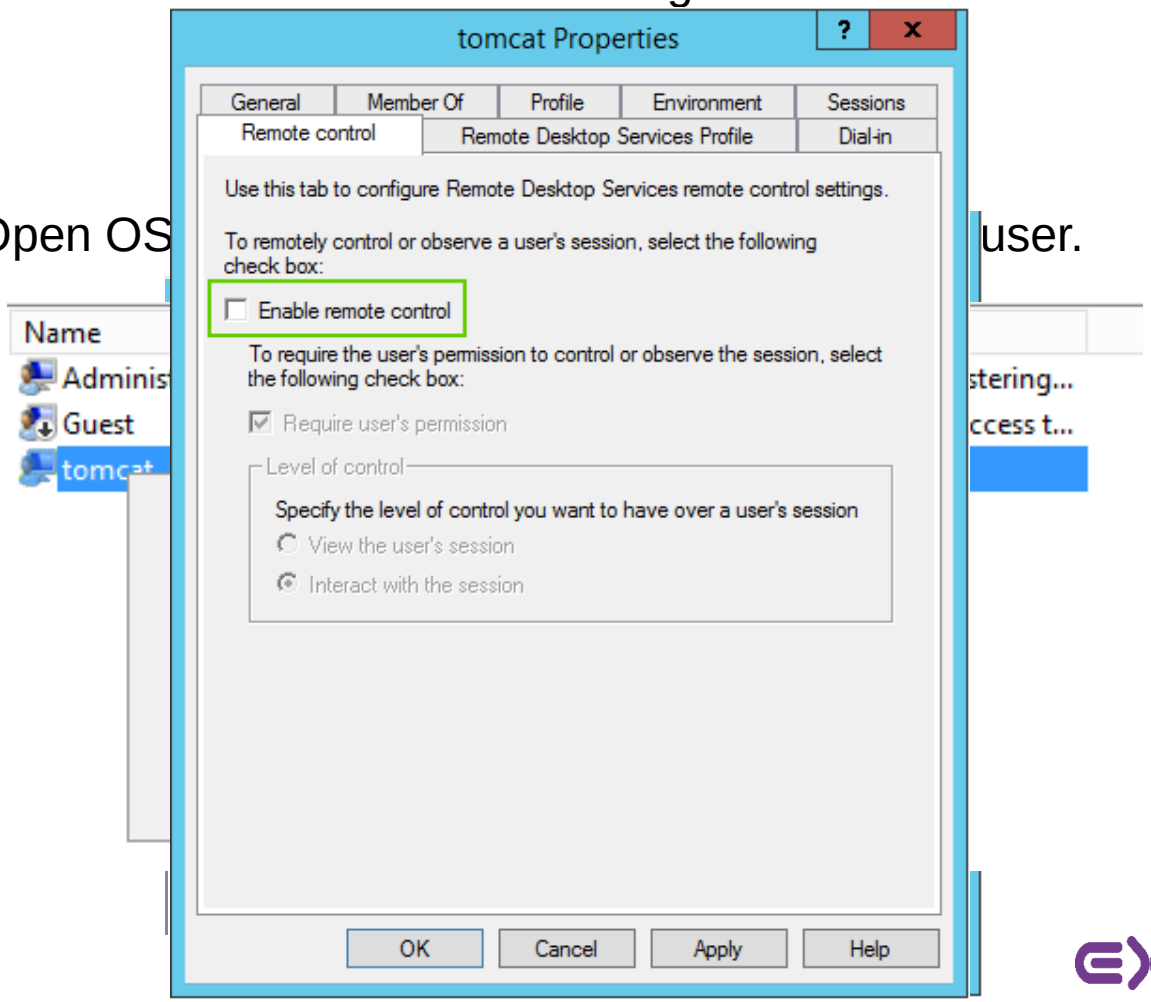
Create a dedicated user for Tomcat in order to avoid that Tomcat application alter Operating System or access to OS sensitive files.

Hardening – C2

→**C2:** Windows service credentials configuration level.

Soluce:

Step 1: Open OS … user.



EXCELLIUM

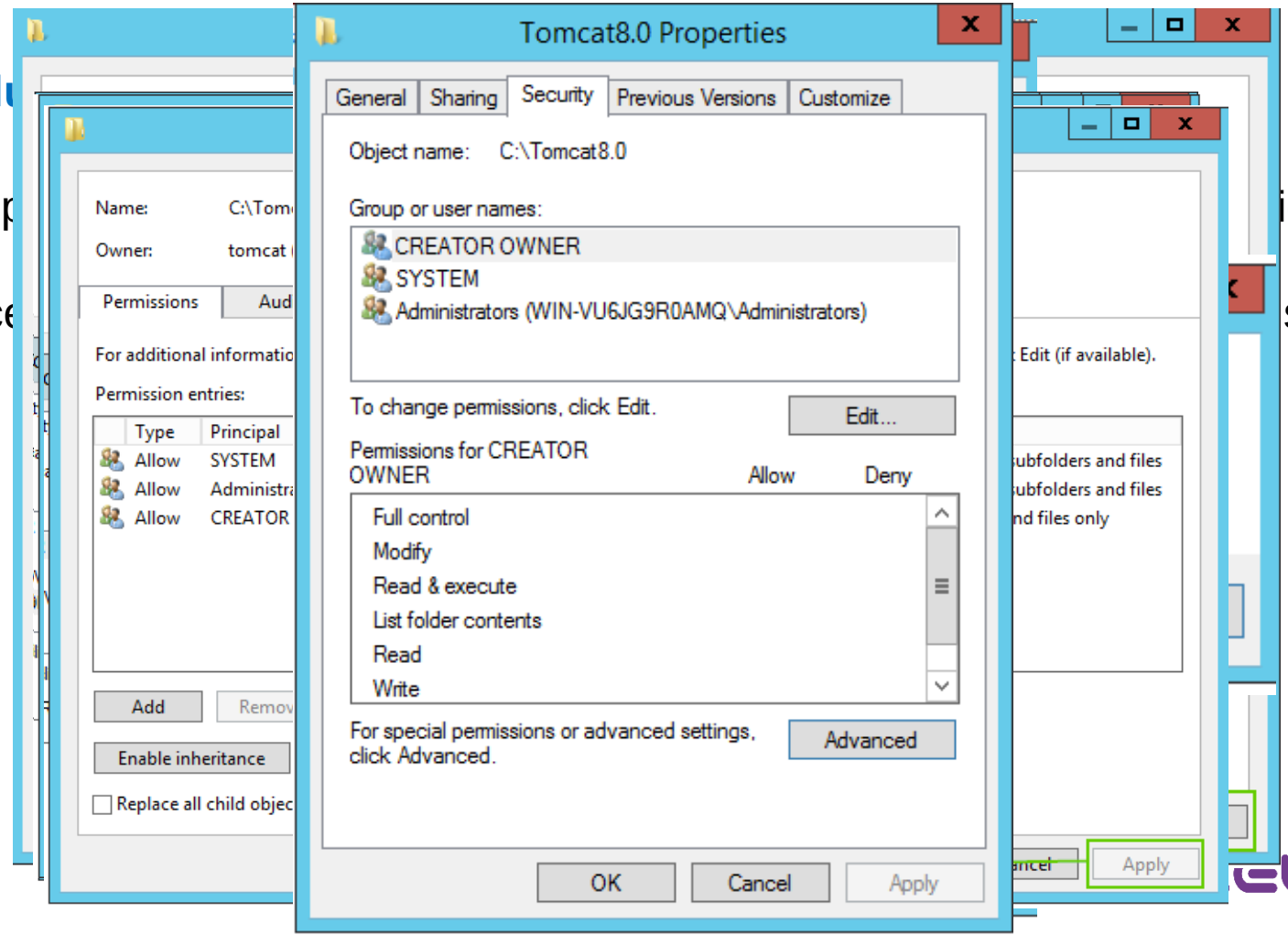
Hardening – C2

→**C2:** Windows service credentials configuration level.

Solu

Step ict

acce ser.

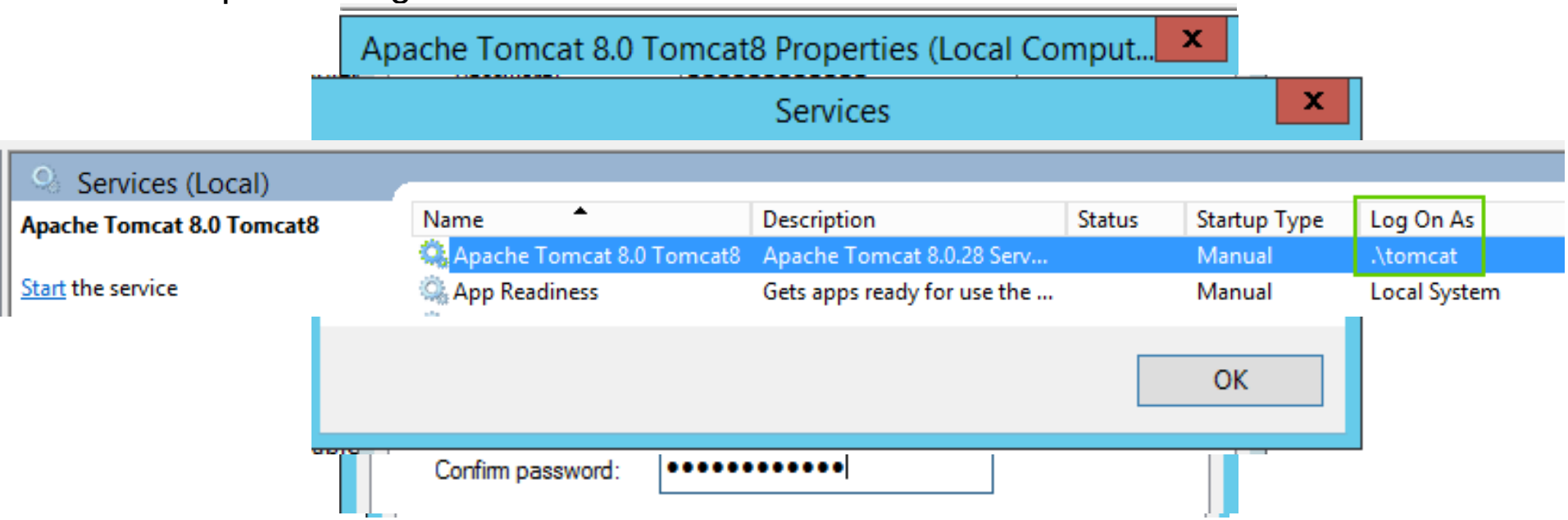


Hardening – C2

→**C2:** Windows service credentials configuration level.

Soluce:

Step 3: Configure Tomcat Windows service to use the Tomcat dedicated user.



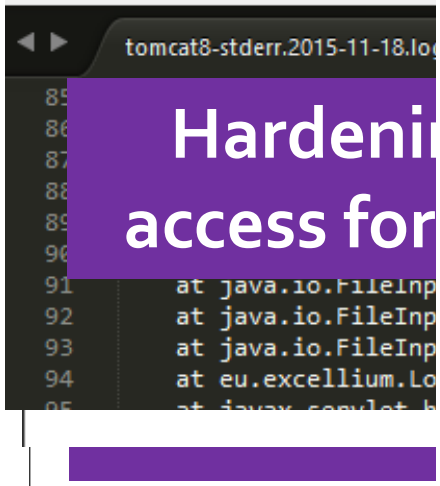
EXCELLIUM

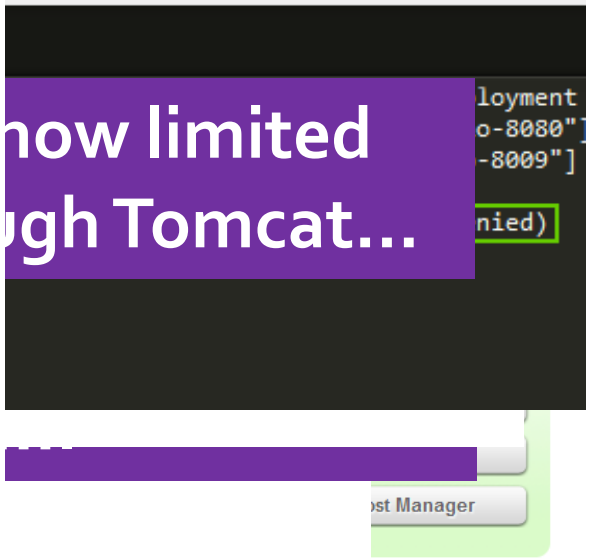
Hardening – C2

→**C2:** Windows service credentials configuration level.

Soluce:

Step 4: Start [illegible] access restriction.





EXCELLIUM

Hardening – C3

→**C3:** Tomcat credentials storage protection level.

Objective:

Protect credentials stored in Tomcat user XML file.

Hints:

https://tomcat.apache.org/tomcat-8.0-doc/realm-howto.html#Digested_Passwords

http://davidghedini.blogspot.lu/2010/07/tomcat-manager-password.html

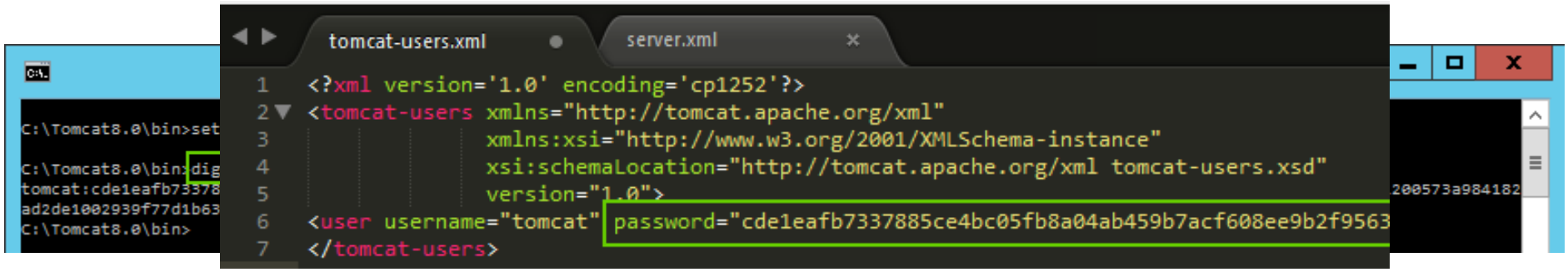
https://tomcat.apache.org/tomcat-8.0-doc/config/credentialhandler.html

Hardening – C3

→**C3:** Tomcat credentials storage protection level.

Soluce:

Step 1: Generate a SHA512 hash of the user password using Tomcat digest script and replace the plain-text password with this hash into the «tomcat-users.xml file». Hash must be salted, use iterations count > 10000 and use a key length of 512 bits.



EXCELLIUM

Hardening – C3

tomcat-users.xml | server.xml

```
<?xml version='1.0' encoding='utf-8'?>
<Server port="8005" shutdown="SHUTDOWN">
  <Listener className="org.apache.catalina.startup.VersionLoggerListener" />
  <Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />
  <Listener className="org.apache.catalina.core.JreMemoryLeakPreventionListener" />
  <Listener className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener" />
  <Listener className="org.apache.catalina.core.ThreadLocalLeakPreventionListener" />
  <GlobalNamingResources>
    <Resource name="UserDatabase" auth="Container"
              type="org.apache.catalina.UserDatabase"
              description="User database that can be updated and saved"
              factory="org.apache.catalina.users.MemoryUserDatabaseFactory"
              pathname="conf/tomcat-users.xml" />
  </GlobalNamingResources>
  <Service name="Catalina">
    <Connector port="8080" protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="8443" />
    <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
    <Engine name="Catalina" defaultHost="localhost">
      <Realm className="org.apache.catalina.realm.LockOutRealm">
        <Realm className="org.apache.catalina.realm.UserDatabaseRealm" resourceName="UserDatabase">
          <CredentialHandler className="org.apache.catalina.realm.MessageDigestCredentialHandler" algorithm="sha-512"/>
        </Realm>
      </Realm>
      <Host name="localhost"  appBase="webapps"
            unpackWARs="true" autoDeploy="true">
        <Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
               prefix="localhost_access_log" suffix=".txt"
               pattern="%h %l %u %t &quot;%r&quot; %s %b" />
      </Host>
    </Engine>
  </Service>
</Server>
```

EXCELLIUM

Hardening – C3

→**C3:** Tomcat credentials storage protection level.

Soluce:

Hardening – C4

→**C4:** Network access segregation level for access to TC admin app.

Objective:

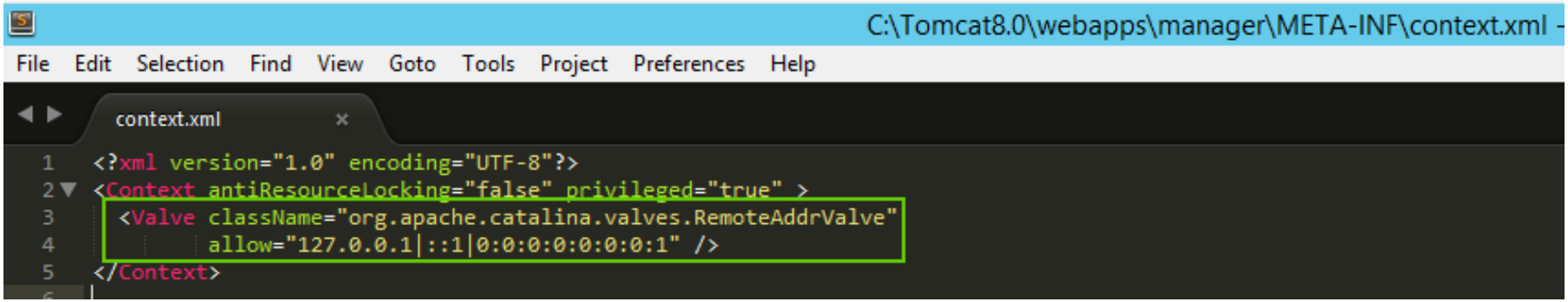
Restrict access to Tomcat admin application only from localhost or 127.0.0.1.

Hardening – C4

→**C4:** Network access segregation level for access to TC admin app.

Soluce:

Step 1: Edit the «context.xml» file of the Tomcat manager application to enable the restriction valve in order to restrict access from specified domain/ip.



EXCELLIUM

Hardening – C4

→**C4:** Network access segregation level for access to TC admin app.

Soluce:

Step 2: Start the Tomcat Windows service and verify the network restriction.

Hardening – C5

→**C5:** Access right level for TC owner user on « **webapps** » TC folder.

Objective:

Update access right in order to avoid that Tomcat dedicated user write into «webapps» application in order to avoid that an application create a webshell through a jsp or a compiled servlet.

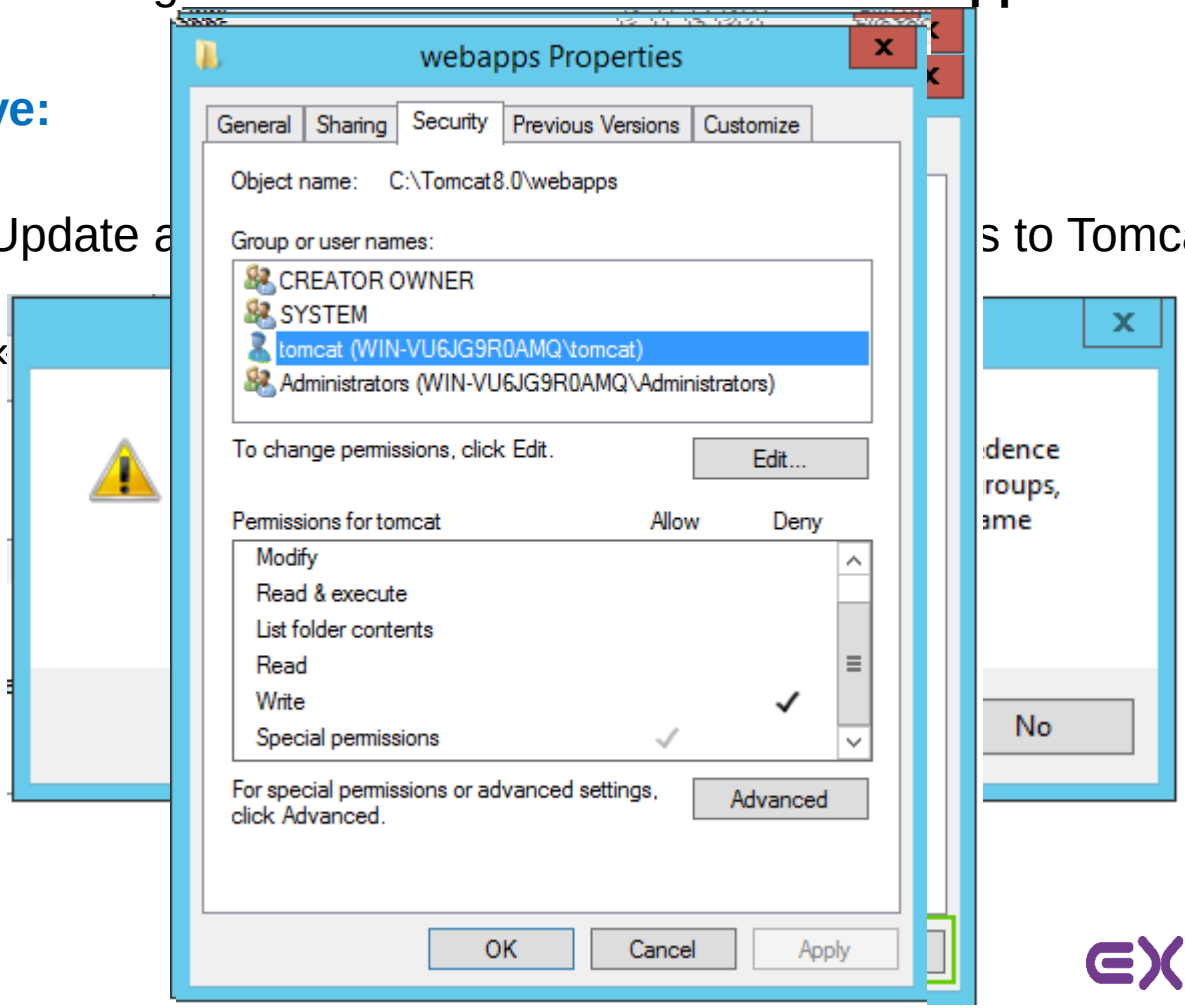
Hardening – C5

→**C5:** Access right level for TC owner user on « **webapps** » TC folder.

Objective:

Step 1: Update a s to Tomcat dedicated

user on «



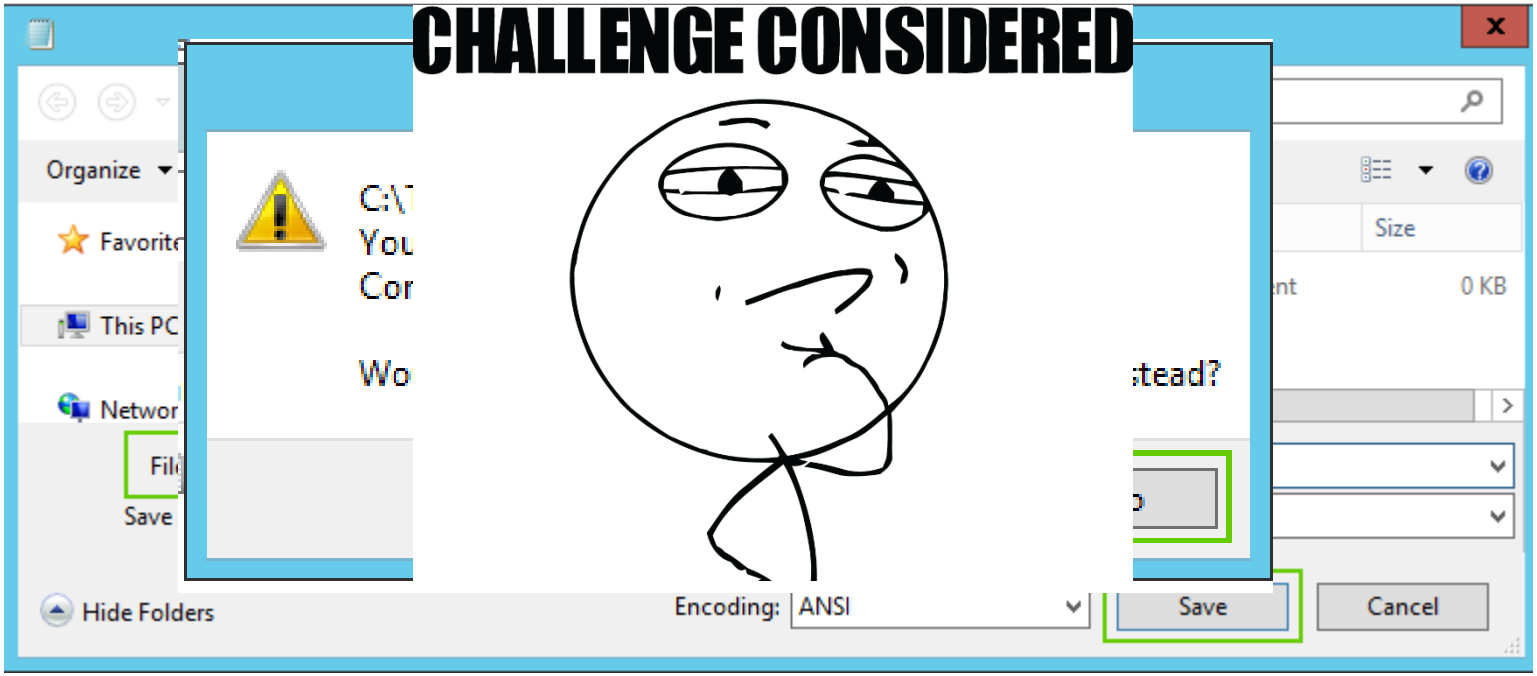
EXCELLIUM

Hardening – C5

→**C5:** Access right level for TC owner user on « **webapps** » TC folder.

Objective:

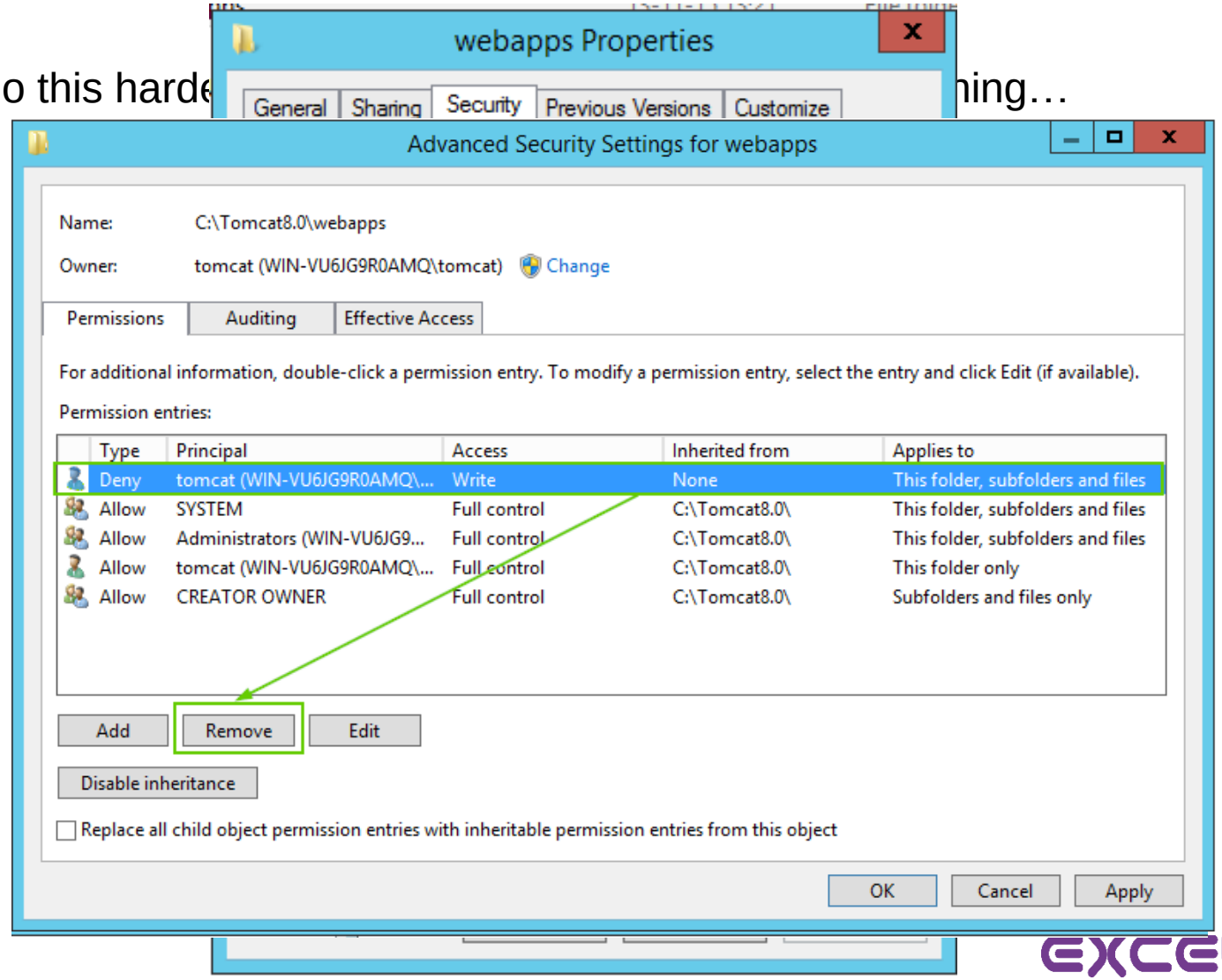
Step 1: Try to write a file into the «webapps» folder as Tomcat dedicated user.



EXCELLIUM

Hardening – C5

Undo this harde…ning…



EXCELLIUM

Hardening – C6

→**C6:** TC JVM Security Manager level.

Objective:

Enable Java Security Manager to restrict action that can be performed by the application deployed on TC server.

Hints:

https://docs.oracle.com/javase/7/docs/technotes/guides/security/PolicyFiles.html

https://docs.oracle.com/javase/7/docs/technotes/guides/security/permissions.html

https://tomcat.apache.org/tomcat-7.0-doc/security-manager-howto.html

http://tomcat.apache.org/tomcat-8.0-doc/config/host.html#Standard_Implementation

Hardening – C6

C:\Tomcat8.0\conf\server.xml

Edit Selection Find View Goto Tools Project Preferences Help

server.xml

```
<?xml version='1.0' encoding='utf-8'?>
<Server port="8005" shutdown="SHUTDOWN">
  <Listener className="org.apache.catalina.startup.VersionLoggerListener" />
  <Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />
  <Listener className="org.apache.catalina.core.JreMemoryLeakPreventionListener" />
  <Listener className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener" />
  <Listener className="org.apache.catalina.core.ThreadLocalLeakPreventionListener" />
  <GlobalNamingResources>
    <Resource name="UserDatabase" auth="Container"
              type="org.apache.catalina.UserDatabase"
              description="User database that can be updated and saved"
              factory="org.apache.catalina.users.MemoryUserDatabaseFactory"
              pathname="conf/tomcat-users.xml" />
  </GlobalNamingResources>
  <Service name="Catalina">
    <Connector port="8080" protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="8443" />
    <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
    <Engine name="Catalina" defaultHost="localhost">
      <Realm className="org.apache.catalina.realm.LockOutRealm">
        <Realm className="org.apache.catalina.realm.UserDatabaseRealm" resourceName="UserDatabase">
          <CredentialHandler className="org.apache.catalina.realm.MessageDigestCredentialHandler" algo
        </Realm>
      </Realm>
      <Host name="localhost"  appBase="webapps"
            unpackWARs="true" autoDeploy="true" deployXML="true">
        <Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
               prefix="localhost_access_log" suffix=".txt"
               pattern="%h %l %u %t &quot;%r&quot; %s %b" />
      </Host>
```

Hardening – C6

→**C6:** TC JVM Security Manager level.

Soluce:

Step 2: Start the Tomcat Windows service and verify the access possibility of the application.

Hardening – C7

→**C7:** TC Documentation and ROOT applications are still online..

Objective:

Undeploy theses applications.

Hardening – C7

→**C7:** TC Documentation and ROOT applications are still online..

Soluce:

Step 1: Remove theses applications from folders « webapps ».

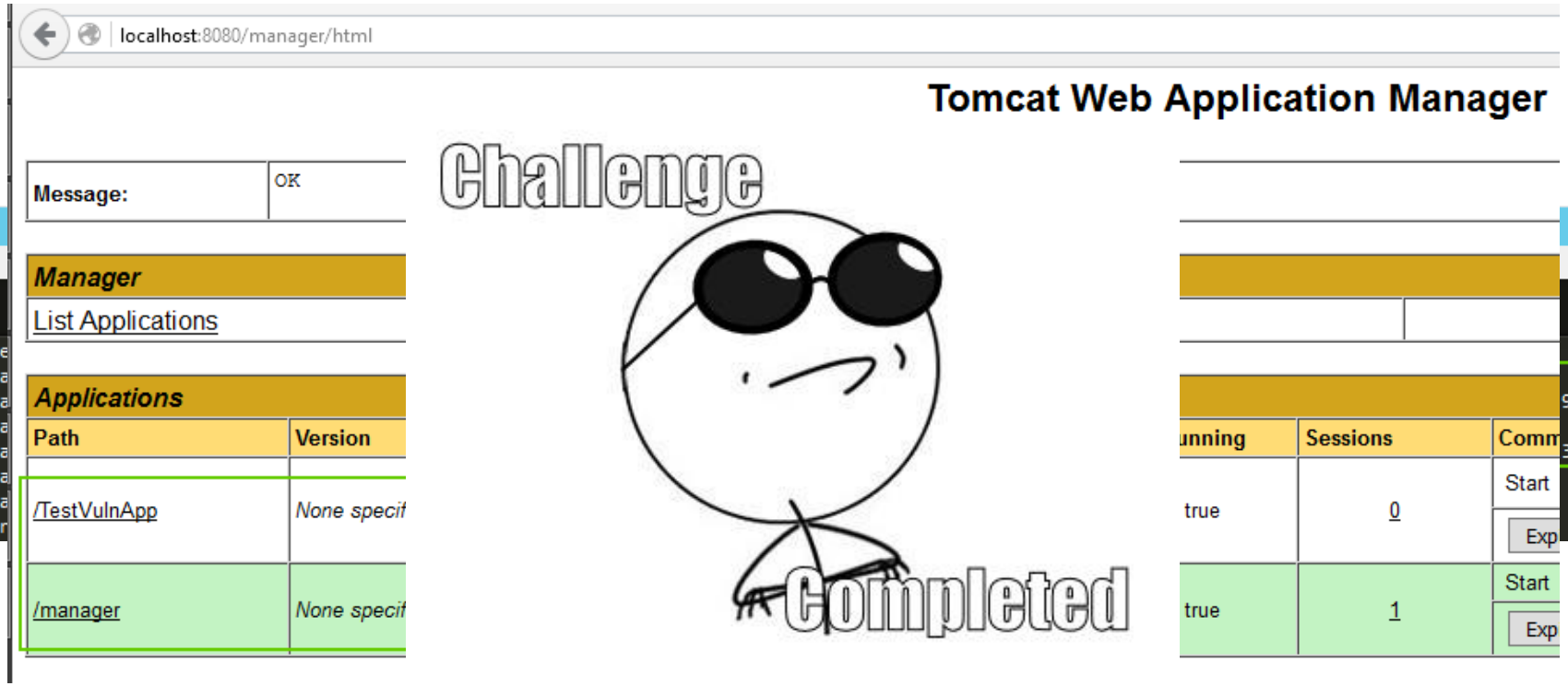
```
C:\Tomcat8.0\work\Catalina\localhost>rmdir /S /Q docs

C:\Tomcat8.0\work\Catalina\localhost>rmdir /S /Q ROOT
```

EXCELLIUM

Hardening – C7

→**C7:** TC Documentation and ROOT applications are still online..

Soluce:



EXCELLIUM

Questions