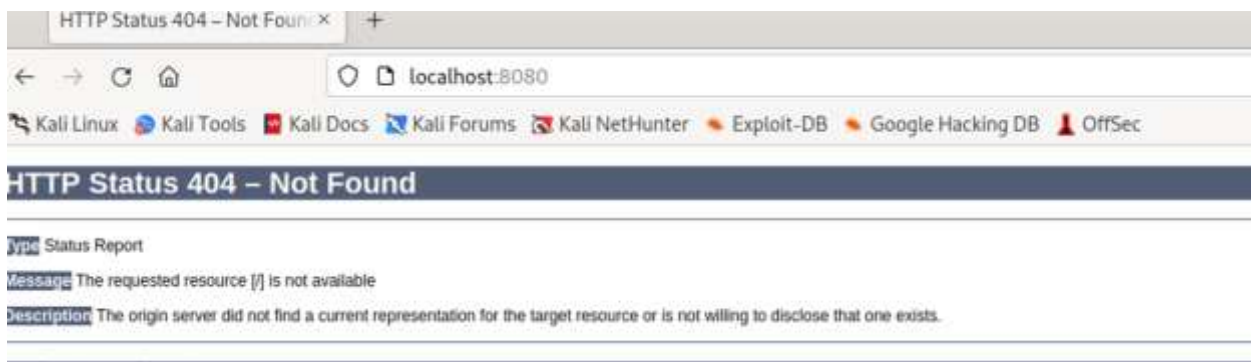## 2.2C: Security configurations of Tomcat server

- In this category, I focused on configurations which act to guard the Tomcat server against two particular threats. In order to prevent access to the Tomcat managers page we need to change a couple of the default Tomcat parameters. Second, I ensured that they existed but were hard to detect with other tools such as NMap through which you can find out the type of the server and its version number. Because of the adjustments' exclusion of some threats that the server will inevitably face, security on the servers is also enhanced.

- First, I fixed the issue preventing access from the root path (http:Our web application map is to: http://localhost:8080 using the Tomcat manager page. It is important particularly because if they are hacked, the basic server pages include some extremely secure information. To do this, I made the following changes: Modifying the ROOT folder: I then navigated to the root > subfolder and then/into the web apps folder found in the Tomcat installation directory. Here, the default page is managed by index.jsp file, which was changed in this case. Using the file, I made it so that if anyone tried to visit the root URL, they would be shown the HTTP 404 page. This means that anybody who is not directly involved will automatically have less ways to know anything about them that should not lay their hands on.

- Custom Error Page: In order to have a better looking result, I created the custom 404 error page using the site's HTML prototyping recommendation. For this reason, this page informs the user that the requested web page is not available and the he should contact the administrator. Therefore, it was necessary to locate our custom page to the ROOT folder so it could launch when accessing the root URL.

```html
1 <html>
2
3 <head>
4 <title>Page not found</title>
5 <link rel="icon" type="image/x-icon" href="favicon.ico">
6 </head>
7 <body>
8
9 <h1>
10     <center>The Page You looking for is not available, please connect with administrator.</center>
11 </h1>
12
13 </body>
14 </html>
15
```

```xml
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!--
3  Licensed to the Apache Software Foundation (ASF) under one or more
4  contributor license agreements.  See the NOTICE file distributed with
5  this work for additional information regarding copyright ownership.
6  The ASF licenses this file to You under the Apache License, Version 2.0
7  (the "License"); you may not use this file except in compliance with
8  the License.  You may obtain a copy of the License at
9
10     http://www.apache.org/licenses/LICENSE-2.0
11
12  Unless required by applicable law or agreed to in writing, software
13  distributed under the License is distributed on an "AS IS" BASIS,
14  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
15  See the License for the specific language governing permissions and
16  limitations under the License.
17 -->
18 <web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
19  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
20  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
21                  http://xmlns.jcp.org/xml/ns/javaee/web-app_4_0.xsd"
22  version="4.0"
23  metadata-complete="true">
24
25  <display-name>Welcome to Tomcat</display-name>
26  <description>
27    Welcome to Tomcat
28  </description>
29
30  <error-page>
31    <error-code>404</error-code>
32    <location>/404.html</location>
33  </error-page>
```

- Verifying the Modifications: About these changes I tested the server using the link http://localhost:8080. Sometimes this would take me to the website's 404 error page which stated that the management page could not be accessed through ''. I then verified that the admin page was forwarded to http://localhost:8080/manage-tomcat.jsp, www.google.com/manage-tomcat.jsp and http of that same input.

How to Stop Nmap from Detecting the Server

- I then encountered an issue, where Nmap scans revealed information about the version of Tomcat servers. Should all these features be exposed to public domain, the attackers looking for a specific chink in the armor will enjoy attacking the server. To put an end to this, I did the following:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV localhost
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2024-09-28 15:28 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 999 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.75 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

- The file was identified as web.xml in the Tomcat7 server in the conf directory. This file keeps Tomcat's settings and alters its behavior in accordance with the received requests. This file also contained server details which I however ensured that they were not revealed to http responses such as the kind of server as well as version. This largely wards off tools such as Nmap to get the server information.

Preceding web.xml file


```
Warning: you are using the root account. You may harm your system.
                server.xml          ×              web.xml
20  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
21                      http://xmlns.jcp.org/xml/ns/javaee/web-app_4_0.xsd"
22  version="4.0">
23
24  <!-- Custom display name to hide Apache Tomcat information -->
25  <display-name>Apache Tomcat</display-name>
26
27  <!-- Custom error page to prevent information leakage -->
28  <error-page>
29    <error-code>404</error-code>
30    <location>/404.html</location>
31  </error-page>
32
33  <!-- Optional: Add init-param to hide server details -->
34  <init-param>
35    <param-name>server</param-name>
36    <param-value>Unknown</param-value>
37  </init-param>
38
```

Preceding Server.xml file


```
Warning: you are using the root account. You may harm your system.
                server.xml                          web.xml
21  -->
22  <Server port="8005" shutdown="SHUTDOWN">
23    <Service name="Catalina">
24      <Connector port="8080" protocol="HTTP/1.1"
25                 connectionTimeout="20000"
26                 redirectPort="8443" />
27      <Engine name="Catalina" defaultHost="localhost">
28        <Host name="localhost" appBase="webapps"
29              unpackWARs="true" autoDeploy="true">
30          <Valve className="org.apache.catalina.valves.AccessLogValve"
31                 directory="logs" prefix="localhost_access_log" suffix=".txt"
32                 pattern="%h %l %u %t &quot;%r&quot; %s %b" />
33        </Host>
34      </Engine>
35    </Service>
36  </Server>
```

After-change file Web.xml


```
Warning: you are using the root account. You may harm your system.
```

```
                server.xml              ✕                    web.xml

xsI:schemaLocation= http://xmlns.jcp.org/xml/ns/javaee
                    http://xmlns.jcp.org/xml/ns/javaee/web-app_4_0.xsd"
version="4.0">

<!— Custom display name to hide Apache Tomcat information →
<display-name>Unknown Server</display-name>

<!— Custom error page to prevent information leakage →
<error-page>
  <error-code>404</error-code>
  <location>/404.html</location>
</error-page>

<!— Optional: Add init-param to hide server details →
<init-param>
  <param-name>server</param-name>
  <param-value>Unknown</param-value>
</init-param>
```

After-change file Server.xml


```
Warning: you are using the root account. You may harm your system.
6    limitations under the License.
7  →
8 <!— Note:  A "Server" is not itself a "Container", so you may not
9       define subcomponents such as "Valves" at this level.
0       Documentation at /docs/config/server.html
1  →
2 <Server port="8005" shutdown="SHUTDOWN">
3   <Service name="Catalina">
4     <Connector port="8080" protocol="HTTP/1.1"
5               connectionTimeout="20000"
6               redirectPort="8443"
7               server="web-server" />
8     <Engine name="Catalina" defaultHost="localhost">
9       <Host name="localhost" appBase="webapps"
0             unpackWARs="true" autoDeploy="true">
1         <Valve className="org.apache.catalina.valves.AccessLogValve"
2               directory="logs" prefix="localhost_access_log" suffix=".txt"
3               pattern="%h %l %u %t &quot;%r&quot; %s %b" />
4       </Host>
5     </Engine>
6   </Service>
```

- Nmap testing: Before, the changes I made, I located and determined the version of the Tomcat server using Nmap. As such, after making those changes I repeated the scan to carry out the next steps. This time around there was no detail in the server information that would suggest that it had changed to show that the information has been well hidden as required.

- With the help of these adjustments I was able to successfully raise the level of the security in the Tomcat server. Other users can never find other information on the server if the default page is set to be in the hidden state. If the specific details of the server are not visible to the scanning method of the Nmap they will also not attempt to attack with aim. In other words, these settings must be set on in order to ensure the protection of a given production web server.