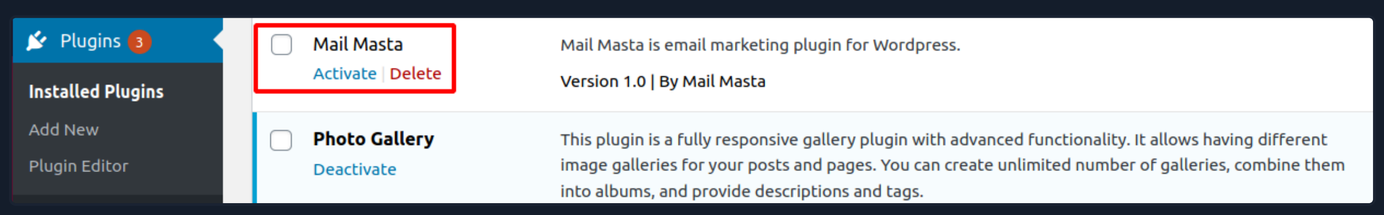
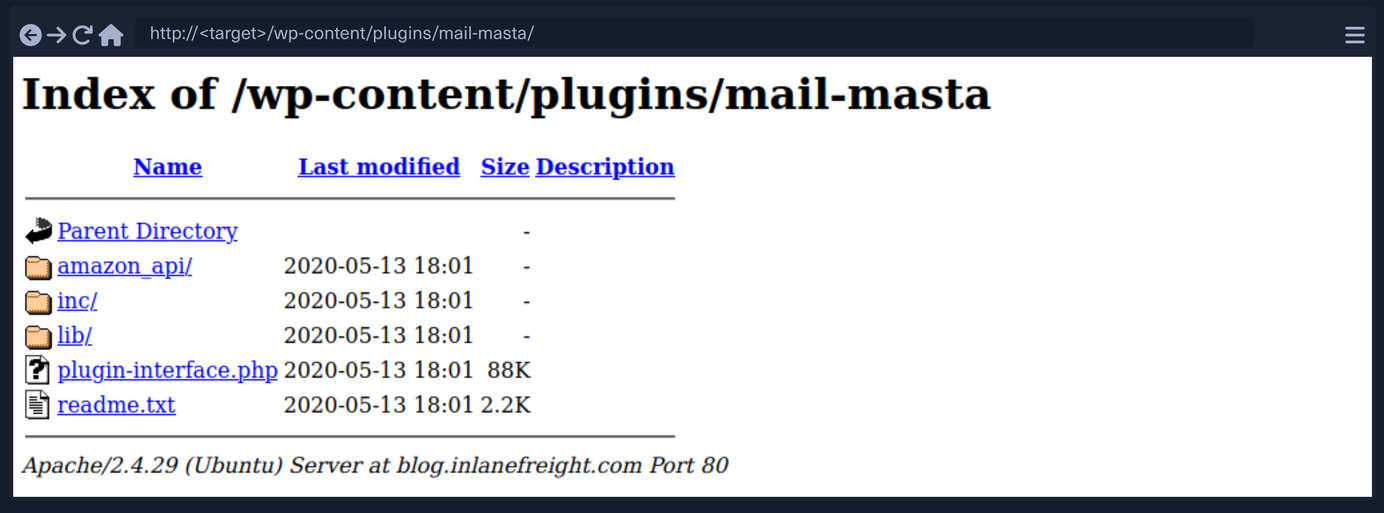
Directory Indexing

Active plugins should not be our only area of focus when assessing a WordPress website. Even if a plugin is deactivated, it may still be accessible, and therefore we can gain access to its associated scripts and functions. Deactivating a vulnerable plugin does not improve the WordPress site's security. It is best practice to either remove or keep up-to-date any unused plugins.

The following example shows a disabled plugin.



If we browse to the plugins directory, we can see that we still have access to the `Mail Masta` plugin.



We can also view the directory listing using cURL and convert the HTML output to a nice readable format using `html2text`.

```
Avenger666@htb[/htb]$ curl -s -X GET http://blog.inlanefreight.com/wp-content/plugins/mail-masta/ | html2text

****** Index of /wp-content/plugins/mail-masta ******
[[ICO]]       Name                Last_modified    Size Description
===============================================================================
[[PARENTDIR]] Parent_Directory                        -
[[DIR]]       amazon_api/         2020-05-13 18:01    -
[[DIR]]       inc/                2020-05-13 18:01    -
[[DIR]]       lib/                2020-05-13 18:01    -
[[   ]]       plugin-interface.php 2020-05-13 18:01  88K
[[TXT]]       readme.txt          2020-05-13 18:01 2.2K
===============================================================================
     Apache/2.4.29 (Ubuntu) Server at blog.inlanefreight.com Port 80
```

This type of access is called `Directory Indexing`. It allows us to navigate the folder and access files that may contain sensitive information or vulnerable code. It is best practice to disable directory indexing on web servers so a potential attacker cannot gain direct access to any files or folders other than those necessary for the website to function properly.

Connect to Pwnbox
Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location
UK 180ms

Terminate Pwnbox to switch location

Start Instance
∞ / 1 spawns left

Waiting to start...

Questions

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

Cheat Sheet

Target: Click here to spawn the target system!

+ 1 Keep in mind the key WordPress directories discussed in the WordPress Structure section. Manually enumerate the target for any directories whose contents can be listed. Browse these directories and locate a flag with the file name flag.txt and submit its contents as the answer.

HTB{3num3r4t10n_15_k3y}

Submit

My Workstation
OFFLINE
Start Instance
∞ / 1 spawns left