

## 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.

Plugins

Installed Plugins

Add New

Plugin Editor

☐ Mail Masta

Activate Delete

Mail Masta is email marketing plugin for WordPress.

Version 1.0 | By Mail Masta

☐ Photo Gallery

Deactivate

This plugin is a fully responsive gallery plugin with advanced functionality. It allows having different image galleries for your posts and pages. You can create unlimited number of galleries, combine them into albums, and provide descriptions and tags.

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

http://<target>-wp-content/plugins/mail-masta/

### Index of /wp-content/plugins/mail-masta

Name	Last modified	Size	Description
Parent Directory		-	
amazon_api/	2020-05-13 18:01	-	
inc/	2020-05-13 18:01	-	
lib/	2020-05-13 18:01	-	
plugin-interface.php	2020-05-13 18:01	88K	
readme.txt	2020-05-13 18:01	2.2K	

Apache/2.4.29 (Ubuntu) Server at blog.inlanefreight.com Port 80

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

Directory Indexing

```
MisaelMacias@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

137ms

Terminate Pwnbox to switch location

Start Instance

00 / 1 spawns left

[Cheat Sheet](#)[Go to Questions](#)

### Table of Contents

#### Introduction

- Intro
- WordPress Structure
- WordPress User Roles

#### Enumeration

- WordPress Core Version Enumeration
- Plugins and Themes Enumeration
- Directory Indexing
- User Enumeration
- Login
- WPSan Overview
- WPSan Enumeration

#### Exploitation

- Exploiting a Vulnerable Plugin
- Attacking WordPress Users
- RCE via the Theme Editor
- Attacking WordPress with Metasploit

#### Security Measures

- WordPress Hardening

#### Skills Assessment

- Skills Assessment - WordPress

#### My Workstation

OFFLINE

Start Instance

00 / 1 spawns left

## Questions



Cheat Sheet

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

Target(s): [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

← Previous

Next →

Mark Complete & Next

