



Plugins and Themes Enumeration

We can also find information about the installed plugins by reviewing the source code manually by inspecting the page source or filtering for the information using **cURL** and other command-line utilities.

Plugins

```
Plugins

r! -s -X GET http://blog.inlanefreight.com | sed 's/href=/\n/g' | sed 's/src=/\n/g' | grep 'wp-content/plugins/' | cut -d'"' -f2

t.com/wp-content/plugins/wp-google-places-review-slider/public/css/wprev-public_combine.css?ver=6.1
t.com/wp-content/plugins/mail-masta/lib/subscriber.js?ver=5.3.3
t.com/wp-content/plugins/mail-masta/lib/jquery.validationEngine-en.js?ver=5.3.3
t.com/wp-content/plugins/mail-masta/lib/jquery.validationEngine.js?ver=5.3.3
t.com/wp-content/plugins/wp-google-places-review-slider/public/js/wprev-public-com-min.js?ver=6.1
t.com/wp-content/plugins/mail-masta/lib/css/mm_frontend.css?ver=5.3.3
```

Themes

```
Themes

Avenger666@htb[/htb]$ curl -s -X GET http://blog.inlanefreight.com | sed 's/href=/\n/g' | sed 's/src=/\n/g' | grep 'themes/' | cut -d'"' -f2

http://blog.inlanefreight.com/wp-content/themes/ben_theme/css/bootstrap.css?ver=5.3.3
http://blog.inlanefreight.com/wp-content/themes/ben_theme/style.css?ver=5.3.3
http://blog.inlanefreight.com/wp-content/themes/ben_theme/css/colors/default.css?ver=5.3.3
http://blog.inlanefreight.com/wp-content/themes/ben_theme/css/jquery.smartmenus.bootstrap.css?ver=5.3.3
http://blog.inlanefreight.com/wp-content/themes/ben_theme/css/owl.carousel.css?ver=5.3.3
http://blog.inlanefreight.com/wp-content/themes/ben_theme/css/owl.transitions.css?ver=5.3.3
http://blog.inlanefreight.com/wp-content/themes/ben_theme/css/font-awesome.css?ver=5.3.3
http://blog.inlanefreight.com/wp-content/themes/ben_theme/css/animate.css?ver=5.3.3
http://blog.inlanefreight.com/wp-content/themes/ben_theme/css/magnific-popup.css?ver=5.3.3
http://blog.inlanefreight.com/wp-content/themes/ben_theme/css/bootstrap-progressbar.min.css?ver=5.3.3
http://blog.inlanefreight.com/wp-content/themes/ben_theme/js/navigation.js?ver=5.3.3
http://blog.inlanefreight.com/wp-content/themes/ben_theme/js/bootstrap.min.js?ver=5.3.3
http://blog.inlanefreight.com/wp-content/themes/ben_theme/js/jquery.smartmenus.js?ver=5.3.3
http://blog.inlanefreight.com/wp-content/themes/ben_theme/js/jquery.smartmenus.bootstrap.js?ver=5.3.3
http://blog.inlanefreight.com/wp-content/themes/ben_theme/js/owl.carousel.min.js?ver=5.3.3
background: url("http://blog.inlanefreight.com/wp-content/themes/ben_theme/images/breadcrumb-back.jpg") #50b9ce;
```

The response headers may also contain version numbers for specific plugins.

However, not all installed plugins and themes can be discovered passively. In this case, we have to send requests to the server actively to enumerate them. We can do this by sending a GET request that points to a directory or file that may exist on the server. If the directory or file does exist, we will either gain access to the directory or file or will receive a redirect response from the webserver, indicating that the content does exist. However, we do not have direct access to it.

Plugins Active Enumeration

```
Plugins Active Enumeration

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

HTTP/1.1 301 Moved Permanently
Date: Wed, 13 May 2020 20:08:23 GMT
Server: Apache/2.4.29 (Ubuntu)
Location: http://blog.inlanefreight.com/wp-content/plugins/mail-masta/
Content-Length: 356
Content-Type: text/html; charset=iso-8859-1
```

If the content does not exist, we will receive a **404 Not Found error**.

```
Plugins Active Enumeration

Avenger666@htb[/htb]$ curl -I -X GET http://blog.inlanefreight.com/wp-content/plugins/someplugin

HTTP/1.1 404 Not Found
Date: Wed, 13 May 2020 20:08:18 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Link: <http://blog.inlanefreight.com/index.php/wp-json/>; rel="https://api.w.org/"
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

The same applies to installed themes.

To speed up enumeration, we could also write a simple bash script or use a tool such as **wfuzz** or **WPScan**, which automate the process.

← Previous

Next →

✓ Mark Complete & Next

Cheat Sheet

Table of Contents

Introduction

Intro

WordPress Structure

WordPress User Roles

Enumeration

WordPress Core Version Enumeration

Plugins and Themes Enumeration

Directory Indexing

User Enumeration

Login

WPScan Overview

WPScan Enumeration

Exploitation

Exploiting a Vulnerable Plugin

Attacking WordPress Users

RCE via the Theme Editor

Attacking WordPress with Metasploit

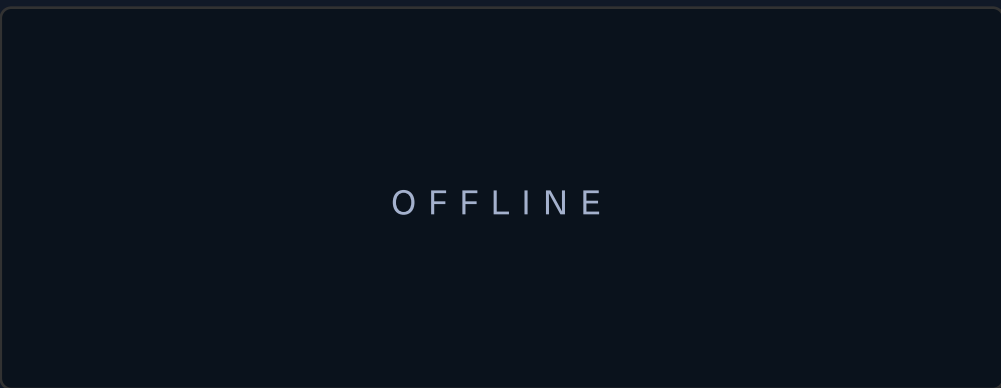
Security Measures

WordPress Hardening

Skills Assessment

Skills Assessment - WordPress

My Workstation



Start Instance

∞ / 1 spawns left

1 Summarize this page

Key Takeaways

- Review the installed plugins by inspecting the page source or using **cURL**.
- Get version numbers from response headers to know specific plugin versions.
- Actively enumerate plugins and themes by sending GET requests to the server.

Summary To gather information about the installed plugins, the page source can be inspected or **cURL** can be used to filter for plugin information. The response headers can contain version numbers for specific plugins. Actively enumerating plugins and themes can be done by sending GET requests to directories or files that may exist on the server. Requests that point to non-existent content would receive a **404 Not Found error**. Tools like **wfuzz** or **WPScan** can automate the enumeration process and speed it up. Plugins and themes are largely enumerated to gather information for further exploitation and attack.

Get Better Answer

Ask a follow-up question

GPT-3.5 GPT-4

