HTB ACADEMY

### **WordPress Structure**

### **Default WordPress File Structure**

WordPress can be installed on a Windows, Linux, or Mac OSX host. For this module, we will focus on a default WordPress installation on an Ubuntu Linux web server. WordPress requires a fully installed and configured LAMP stack (Linux operating system, Apache HTTP Server, MySQL database, and the PHP programming language) before installation on a Linux host. After installation, all WordPress supporting files and directories will be accessible in the webroot located at /var/www/html.

Below is the directory structure of a default WordPress install, showing the key files and subdirectories necessary for the website to function properly.

#### File Structure

```
File Structure
 Avenger666@htb[/htb]$ tree -L 1 /var/www/html
   - index.php
    - license.txt
   — readme.html
    wp-activate.php
    — wp-admin
    - wp-blog-header.php
    - wp-comments-post.php
     wp-config.php
    ·wp-config-sample.php
     wp-content
    - wp-cron.php
    · wp-includes
    - wp-links-opml.php
     wp-load.php
     wp-login.php
    - wp-mail.php
     wp-settings.php
     wp-signup.php
     wp-trackback.php
    · xmlrpc.php
```

### **Key WordPress Files**

The root directory of WordPress contains files that are needed to configure WordPress to function correctly.

- index.php is the homepage of WordPress.
- license.txt contains useful information such as the version WordPress installed.
- wp-activate.php is used for the email activation process when setting up a new WordPress site.
- wp-admin folder contains the login page for administrator access and the backend dashboard. Once a user has logged in, they can make changes to the site based on their assigned permissions. The login page can be located at one of the following paths:
  - o /wp-admin/login.php
  - o /wp-admin/wp-login.php
  - ∘ /login.php
  - o /wp-login.php

This file can also be renamed to make it more challenging to find the login page.

• xmlrpc.php is a file representing a feature of WordPress that enables data to be transmitted with HTTP acting as the transport mechanism and XML as the encoding mechanism. This type of communication has been replaced by the WordPress REST API.

## WordPress Configuration File

• The wp-config.php file contains information required by WordPress to connect to the database, such as the database name, database host, username and password, authentication keys and salts, and the database table prefix. This configuration file can also be used to activate DEBUG mode, which can useful in troubleshooting.

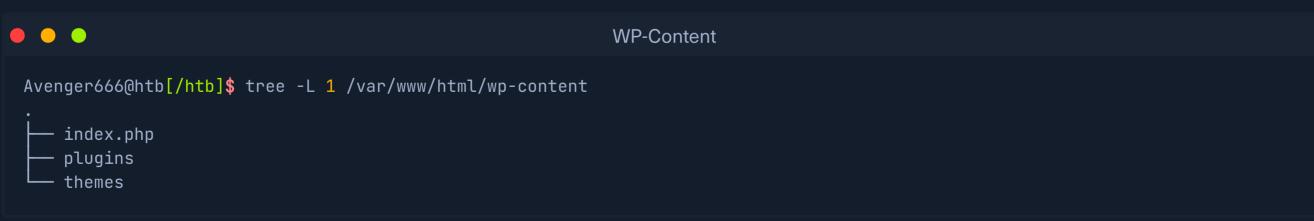
### wp-config.php

```
Code: php
 <?php
/** <SNIP> */
/** The name of the database for WordPress */
 define( 'DB_NAME', 'database_name_here' );
/** MySQL database username */
define( 'DB_USER', 'username_here' );
 /** MySQL database password */
define( 'DB_PASSWORD', 'password_here' );
/** MySQL hostname */
define( 'DB_HOST', 'localhost' );
/** Authentication Unique Keys and Salts */
 /* <SNIP> */
define( 'AUTH_KEY',
                             'put your unique phrase here' );
define( 'SECURE_AUTH_KEY', 'put your unique phrase here' );
define( 'LOGGED_IN_KEY',
                             'put your unique phrase here' );
define( 'NONCE_KEY',
                             'put your unique phrase here' );
define( 'AUTH_SALT',
                             'put your unique phrase here' );
 define( 'SECURE_AUTH_SALT', 'put your unique phrase here' );
 define( 'LOGGED_IN_SALT',
                             'put your unique phrase here' );
 define( 'NONCE_SALT',
                             'put your unique phrase here' );
/** WordPress Database Table prefix */
$table_prefix = 'wp_';
/** For developers: WordPress debugging mode. */
/** <SNIP> */
define( 'WP_DEBUG', false );
/** Absolute path to the WordPress directory. */
if ( ! defined( 'ABSPATH' ) ) {
    define( 'ABSPATH', __DIR__ . '/' );
 /** Sets up WordPress vars and included files. */
require_once ABSPATH . 'wp-settings.php';
```

# **Key WordPress Directories**

• The wp-content folder is the main directory where plugins and themes are stored. The subdirectory uploads/ is usually where any files uploaded to the platform are stored. These directories and files should be carefully enumerated as they may lead to contain sensitive data that could lead to remote code execution or exploitation of other vulnerabilities or misconfigurations.

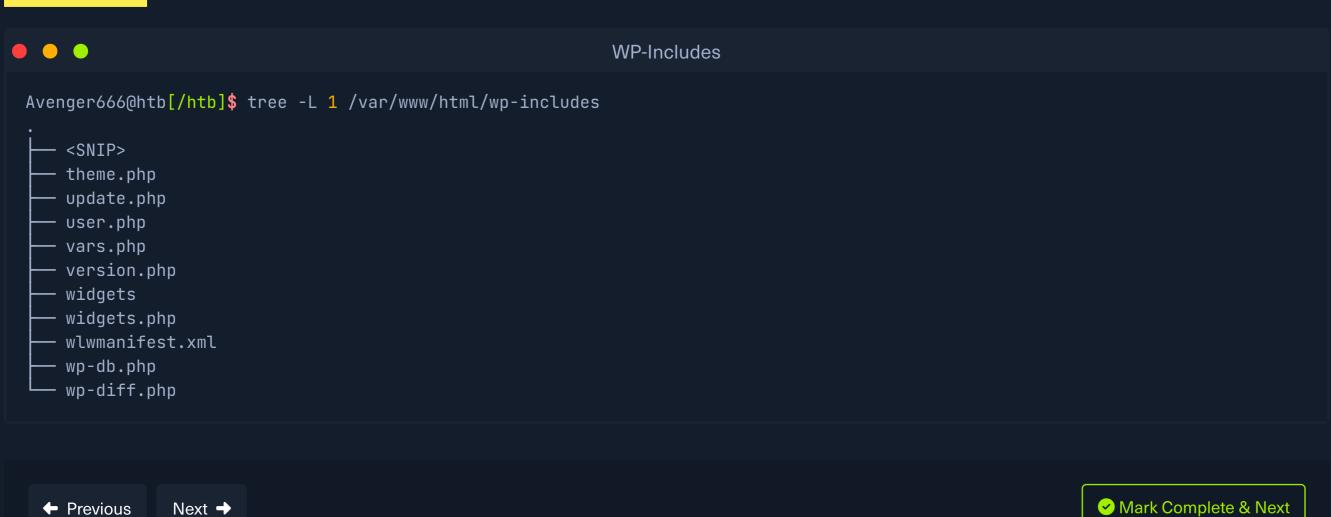
# WP-Content



• wp-includes contains everything except for the administrative components and the themes that belong to the website.

This is the directory where core files are stored, such as certificates, fonts, JavaScript files, and widgets.

# WP-Includes



• WordPress structure: default installation details on a Linux web server. **Cheat Sheet**  Key WordPress files: important files and folders needed for configuration and access. **Table of Contents**  WordPress configuration file: contains sensitive information for connecting to the Introduction database. Intro Summary: The default WordPress installation on an Ubuntu WordPress User Roles Linux web server requires a fully installed and configured LAMP stack. The necessary files and Enumeration directories for the website to function properly can be found in the webroot located at WordPress Core Version Enumeration /var/www/html . Important configurations are Plugins and Themes Enumeration stored in the wp-config.php file, containing database connection information, authentication Directory Indexing keys, and salts. **User Enumeration** Key WordPress files include index.php, 6 Login license.txt , wp-activate.php , wp-admin , and xmlrpc.php. The wp-content directory is WPScan Overview crucial, housing plugins, themes, and other sensitive data, while the wp-includes folder WPScan Enumeration holds core files like certificates and widgets. The wp-config.php file contains information for Exploitation database connectivity and more. **6** Exploiting a Vulnerable Plugin Get Better Answer > Attacking WordPress Users Ask a follow-up question RCE via the Theme Editor GPT-3.5 **◆**GPT-4 Attacking WordPress with Metasploit Security Measures WordPress Hardening Skills Assessment Skills Assessment - WordPress My Workstation OFFLINE

Start Instance

 $\infty$  / 1 spawns left

**Copilot** 

Summarize this page

**Key Takeaways:**