# Intro

## WordPress Overview

WordPress is the most popular open source Content Management System (CMS), powering nearly one-third of all websites in the world. It can be used for multiple purposes, such as hosting blogs, forums, e-commerce, project management, document management, and much more. WordPress is highly customizable as well as SEO friendly, which makes it popular among companies. It has a large library of extensions called themes and plugins, both free and paid, that can be added to enhance the website. Some examples of plugins are WPForms, a robust contact form, MonsterInsights that interfaces with Google Analytics, and Constant Contact, a popular email marketing service. However, its customizability and extensible nature make it prone to vulnerabilities through third-party themes and plugins. WordPress is written in PHP and usually runs on Apache with MySQL as the backend. Many hosting companies offer WordPress as an option when creating a new website and even assist with backend tasks such as security updates.

This module will cover a WordPress website's core structure, manual and automated enumeration techniques to uncover misconfigurations and vulnerabilities, and walk through a few common attacks. You will be given the opportunity to perform your own enumeration and attacks against a WordPress instance while working through the material in each section. The module will end with a Skills Assessment to tie together everything you have learned and complete all of the steps necessary to compromise a WordPress website and the underlying web server fully.

Happy hacking, and don't forget to think outside the box!

## What is a CMS?

A CMS is a powerful tool that helps build a website without the need to code everything from scratch (or even know how to write code at all). The CMS does most of the "heavy lifting" on the infrastructure side to focus more on the design and presentation aspects of the website instead of the backend structure. Most CMS' provide a rich What You See Is What You Get (WYSIWYG) editor where users can edit content as if they were working in a word processing tool such as Microsoft Word. Users can upload media directly from a media library interface instead of interacting with the webserver either from a management portal or via FTP or SFTP.

A CMS is made up of two key components:

- A Content Management Application (CMA) - the interface used to add and manage content.
- A Content Delivery Application (CDA) - the backend that takes the input entered into the CMA and assembles the code into a working, visually appealing website.

A good CMS will provide extensibility, allowing you to add functionality and design elements to the site without needing to work with the website code, rich user management to provide fine-grained control over access permissions and roles, media management to allow the user to easily upload and embed photos and videos, and proper version control. When looking for a CMS, we should also confirm that it is well-maintained, receives periodic updates and upgrades, and has sufficient built-in security settings to harden the website from attackers.

Next →
Mark Complete & Next

Cheat Sheet
Summary
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

OFFLINE

Start Instance

∞ / 1 spawns left