WordPress Hardening

Best Practices

Below are some best practices for preventing attacks against a WordPress site.

Perform Regular Updates

This is a key principle for any application or system and can greatly reduce the risk of a successful attack. Make sure that WordPress core, as well as all installed plugins and themes, are kept up-to-date. Researchers continuously find flaws in third-party WordPress plugins. Some hosting providers will even perform continuous automatic updates of WordPress core. The WordPress admin console will usually prompt us when plugins or themes need to be updated or when WordPress itself requires an upgrade. We can even modify the `wp-config.php` file to enable automatic updates by inserting the following lines:

Code: php

```
define( 'WP_AUTO_UPDATE_CORE', true );
```

Code: php

```
add_filter( 'auto_update_plugin', '__return_true' );
```

Code: php

```
add_filter( 'auto_update_theme', '__return_true' );
```

Plugin and Theme Management

Only install trusted themes and plugins from the WordPress.org website. Before installing a plugin or theme, check its reviews, popularity, number of installs, and last update date. If either has not been updated in years, it could be a sign that it is no longer maintained and may suffer from unpatched vulnerabilities. Routinely audit your WordPress site and remove any unused themes and plugins. This will help to ensure that no outdated plugins are left forgotten and potentially vulnerable.

Enhance WordPress Security

Several WordPress security plugins can be used to enhance the website's security. These plugins can be used as a Web Application Firewall (WAF), a malware scanner, monitoring, activity auditing, brute force attack prevention, and strong password enforcement for users. Here are a few examples of popular WordPress security plugins.

Sucuri Security

- This plugin is a security suite consisting of the following features:
  - Security Activity Auditing
  - File Integrity Monitoring
  - Remote Malware Scanning
  - Blacklist Monitoring.

iThemes Security

- iThemes Security provides 30+ ways to secure and protect a WordPress site such as:
  - Two-Factor Authentication (2FA)
  - WordPress Salts & Security Keys
  - Google reCAPTCHA
  - User Action Logging

Wordfence Security

- Wordfence Security consists of an endpoint firewall and malware scanner.
  - The WAF identifies and blocks malicious traffic.
  - The premium version provides real-time firewall rule and malware signature updates
  - Premium also enables real-time IP blacklisting to block all requests from known most malicious IPs.

User Management

Users are often targeted as they are generally seen as the weakest link in an organization. The following user-related best practices will help improve the overall security of a WordPress site.

- Disable the standard `admin` user and create accounts with difficult to guess usernames
- Enforce strong passwords
- Enable and enforce two-factor authentication (2FA) for all users
- Restrict users' access based on the concept of least privilege
- Periodically audit user rights and access. Remove any unused accounts or revoke access that is no longer needed

Configuration Management

Certain configuration changes can increase the overall security posture of a WordPress installation.

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

OFFLINE

Start Instance

∞ / 1 spawns left

- Install a plugin that disallows user enumeration so an attacker cannot gather valid usernames to be used in a password spraying attack
- Limit login attempts to prevent password brute-forcing attacks
- Rename the `wp-login.php` login page or relocate it to make it either not accessible to the internet or only accessible by certain IP addresses