Unparalleled Security with Enterprise WordPress

How and why WordPress has become the unlikely hero of enterprise security among WCM platforms

Boris Motusic & United Experts Digital Consultancy, Ltd.

February 2019, version 0.2

UNITED EXPERTS
DIGITAL CONSULTANCY SINCE 1997

WWW.UE.TEAM
TEAM@UE.TEAM

Introduction

WordPress is a dynamic Open Source content management system which is used to power millions of websites and web applications. It is the most widely-used CMS software in the world and it powers more than 33% of the entire Web, giving it an estimated 60% market share of all websites using a CMS. WordPress's usability, extensibility and mature development processes make it also a popular and secure choice for enterprises, such as **CNN, USA Today, Sony, Toyota, Mercedes-Benz and Microsoft**. For such large businesses, according to Forbes, WordPress is the **"**promised land — a standard, easy-to-use, multimedia-friendly platform — after a decade of lurching through clunky, expensive, jerry-rigged content management systems.**"**

Despite the widespread use of WordPress in the enterprise world, a common misconception which persists about the system is that it is insecure. This whitepaper stipulates that WordPress is not only secure but that in fact, it is one of the most secure WCM platforms in the world. To understand the origin of the misconception of WordPress's insecurity, it is important to note that WordPress is the only large-scale software platform whose use spans from the consumer to the enterprise market. Consumer implementations are very different from professional implementations and they greatly contribute to the WordPress security myth. Before digging any deeper, it is important to clarify some WordPress- related concepts and facts.

WordPress "Flavors"

- **WordPress.com** is a website hosting and website management service which is powered by the WordPress.org software. It offers free and paid packages and is mainly used by bloggers, hobbyists and small businesses.

- **WordPress.org,** often called WordPress Core, is a free, Open Source WordPress software which can be installed on a personal web host to create a fully owned and customized website. Here, it is important to elaborate that WordPress is licensed under the General Public License (GPLv2 or later) which provides for four core freedoms, and can be considered as the WordPress "bill of rights":
    1. The freedom to run the program, for any purpose.
    2. The freedom to study how the program works, and change it to make it do what you wish.
    3. The freedom to redistribute.
    4. The freedom to distribute copies of your modified versions to others.

- **Enterprise WordPress** is not an official WordPress version but an assumed customized functionality, configuration and setup, complemented by support and other enterprise-relevant services. There are three fundamentally different approaches to WordPress enterprise implementation:

    - **WordPress as SaaS** – Just as WordPress.com offers hosted service to hobbyists and small businesses, WordPress VIP and WPEngine are known to provide a similar service optimized for enterprise setups.

    - **Custom Enterprise WordPress** – In contrast to the SaaS option, many enterprises opt for the flexibility of a custom solution based on the WordPress Core which can be hosted anywhere and entirely customized in functionality, staging and deployment preferences. Companies like Human Made and Bigbite are leaders in this approach.

    - **Custom Enterprise WordPress Packages** – The ultimate option combining the strengths of Open Source and proprietary software is offered by United Experts. The service comprises a custom-made solution for each client and clearly-defined support, training and core functionality packages.

WordPress Components Related to Security

- **WordPress Core** or WordPress.org as defined above is the free, Open Source WordPress software that you can install on your own web host to create a website that's 100% your own. Given WordPress's popularity, extensibility and interoperability, the WordPress Core can be described as **the operating system of the Web**.

- **WordPress Plugins** – If the core is a Web operating system, you can think about plugins as software applications or **apps that bring targeted functionality**. Yet, some WordPress plugins are so large in complexity and user numbers that they could be considered products on their own. For example, WooCommerce is an e-commerce plugin that powers millions of websites and has dozens of plugins on its own. YoastSEO is another popular plugin with millions of users. Elementor is a popular visual page builder with about one million users.

- **WordPress Hosting** - WordPress can be installed on a multitude of platforms. Though WordPress core software provides many provisions for operating a secure web application, which are covered in this document, the configuration of the operating system and the underlying web server hosting the software are equally important to keep the WordPress applications secure.

The WordPress Security Myth

To understand the origin of the misconception of WordPress's insecurity, it is important to note the fact that WordPress is the only large-scale software platform whose use spans from the consumer to the enterprise market. Consumer implementations are very different from professional implementations and they greatly contribute to the WordPress security myth. The consumer nature of the platform leads to frequent implementations by amateurs who do not follow even basic best practices in the area of security, which is of course completely unrelated to a professional setup.

The top 5 reasons which lead to misconceptions of WordPress's security are:

1. **Amateur WordPress installations which are irrelevant for your enterprise setup**
   WordPress is the only large-scale software platform whose use spans from the consumer to the enterprise market. Amateur installations often do not satisfy even the minimumrequirements of the WordPress best practices in the area of security, and therefore become easy targets for hackers.

2. **Elementary user errors, once again irrelevant for enterprise workflows**
   Many hobbyist sites powered by WordPress do not satisfy elementary password requirements for admin accounts. For example, a lot of site owners use "admin" as a username and "password" as a password. As WordPress powers 1/3 of the web, hackers write scripts that go through WordPress login URLs and try the above login combination.

3. **Outdated WordPress installations**
   As it will be explained in the next whitepaper section, one of the big WordPress advantages is the automatic, background update with security patches. Once again, millions of amateur WordPress installations simply do not tick the simple option in the WordPress configuration to enable automatic updates with security patches. Those websites often do not perform any maintenance after the initial setup and lag few versions behind the latest release. Naturally, they become easy targets for hackers, as would any laptop without an updated antivirus software.

4. **Poor website hosting**
   Many small WordPress sites are hosted on shared hosting environments. While many shared hosting environments are secure, some do not properly separate user accounts which opens an easy door for hackers. Most routine, default enterprise environment configurations prevent common problems caused by poor hosting services or setup. For example, just simply enforcing *https* over *http* would prevent many WordPress exploits.

5. **WordPress versions before 3.x**
   WordPress security has dramatically improved since version 3.x. The current release at the time of writing this whitepaper is 5.02. According to Dre Armeda, Director of Product Security at GoDaddy, co-founder of Securi, Inc., and one of the most respected security experts in the world, WordPress has no major security vulnerabilities: **"**We haven't seen a major vulnerability in WordPress since the pre-3.x days. There have been some minor security bugs and those have been fixed pretty quickly, but in terms of major security vulnerabilities, we haven't seen one in quite a while.**"**

The WordPress Advantage in Security Management

The nature of Open Source and the huge size of the WordPress community and ecosystem, together with the WordPress architecture for automatic background updates, make a key difference in the approach to security management which could never be matched by less popular CMS platforms.

Available Resources for Security Management

WordPress has incomparably larger resources for identifying and resolving security threats compared to any other CMS/WCM platform:

- **Around 50 full-time security experts from the WordPress Security Team**
  The WordPress Security Team is made up of approximately 50 experts including developers and security researchers. The team consults with well-known and trusted security researchers, and collaborates with other security teams to address issues in common dependencies. By comparison, most other CMS platforms have a fewer number of total product developers than is the size of the WP Security Team only.

- **Thousands of contributors and numerous WordPress consultancies**
  In addition to the dedicated team above, thousands of community members and numerous WordPress consultancies all work together to review code and identify potential security threats.

- **Big names like Google, Microsoft, and GoDaddy contribute to WordPress security**
  WordPress basically powers 1/3 of the Web. With numbers like that, WordPress is in a position to influence how the Web works and develops, and therefore to partner with other major web players. For example, improving website speed, crawler readability and security is of interest to Google. By improving WordPress, Google can instantly improve 1/3 of the Web. Thus, it is not surprising that Google is partnering with WordPress and contributing to its improvement.

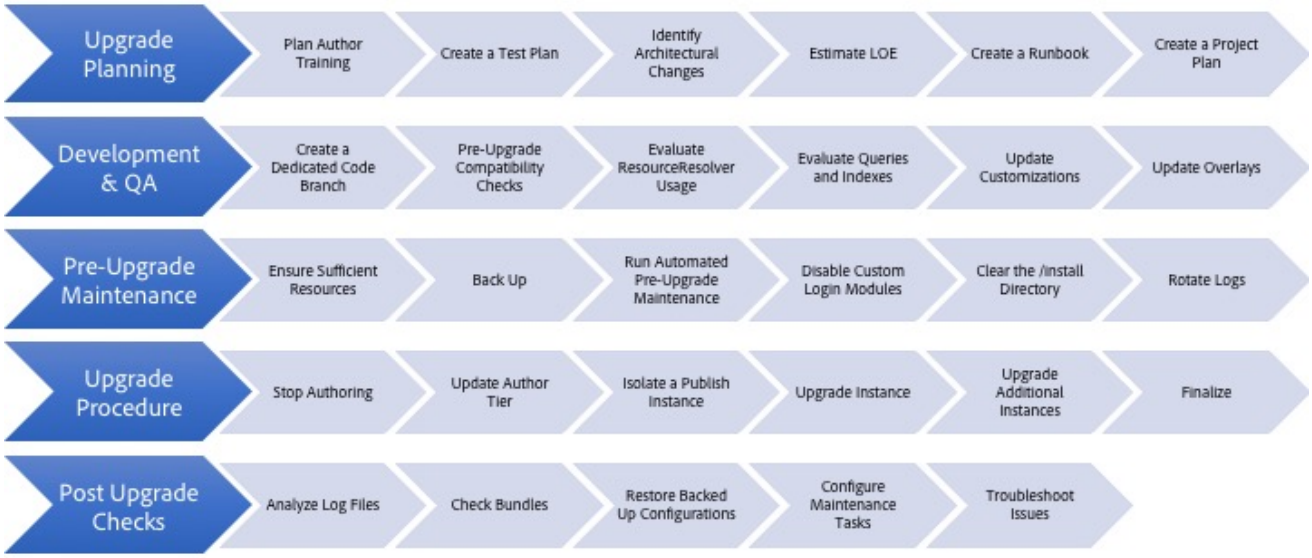
Automatic Updates for Security Releases

The WordPress Security Team can identify, fix and push out automated security enhancements for WordPress without the site owner needing to do anything .The security update will be installed automatically. This is a huge deal for the reasons outlined below. In fact, it is so huge that many enterprises state this aspect as one of the main reasons for migrating to WordPress.

Comparing WordPress Automatic Updates to the Manual Updates of Other Platforms

In comparison to WordPress, the security patches for competing CMS platforms cannot be automatically applied; they are time and resource consuming, and require complex development and deployment workflows. Applying a security patch is in most cases comparable as a procedure to a version update. WordPress updates for security patches are equally simple and automated as security patches!

AEM (Adobe Experience Manager) is another popular option for enterprise WCM. The diagram below taken from the Adobe website (https://helpx.adobe.com/experience-manager/6-3/sites/deploying/using/upgrade.html) illustrates the procedure of **updating Adobe Experience Manager**:



Here is an example related to upgrading the Sitecore CMS as explained by Anurag Agarwal of Edynamic, a Sitecore consultancy:

"While upgrading, there are a number of activities that you need to accomplish manually – missing out on even one of them will render the process incomplete. To be able to fulfill this cycle, and ensure that you're able to fix any issue that may arise in real time, you may have to seek the support of a technical team. So, to minimize any chances of 'something going wrong', it's always recommended that you consider an upgrade plan and follow it to the 'T'. Not only will this prepare you for what lies ahead, it can also help you break the bigger goal into a number of smaller ones to make it convenient."

Anurag outlines the following steps for updating Sitecore:

- Install the upgrade package,
- Handle warnings and collisions,
- Update Solr Assemblies,
- Update the configuration files,
- Install PhantomJS,
- Rebuild search indexes and the link database,
- Upgrade WFFM Module,
- Upgrade DMS,

Security of the WordPress Core

The WordPress Security Team

The WordPress Security Team is made up of approximately 50 experts including lead developers and security researchers — about half are employees of Automattic (makers of WordPress.com, the earliest and largest WordPress hosting platform on the web), and a number work in the web security field. The team consults with well-known and trusted security researchers and hosting companies.

The WordPress Security Team often collaborates with other security teams to address issues in common dependencies, such as resolving the vulnerability in the PHP XML parser, used by the XML-RPC API that ships with WordPress, in WordPress 3.9.24. This vulnerability resolution was a result of a joint effort by both WordPress and Drupal security teams.

WordPress Security Risks, Process, and History

The WordPress Security Team believes in Responsible Disclosure by alerting the security team immediately of any potential vulnerabilities. Potential security vulnerabilities can be signaled to the Security Team via the WordPress HackerOne. The Security Team communicates amongst itself via a private Slack channel, and works on a walled-off, private Trac for tracking, testing, and fixing bugs and security problems.

Each security report is acknowledged upon receipt, and the team works to verify the vulnerability and determine its severity. If confirmed, the security team then plans for a patch to fix the problem which can be committed to an upcoming release of the WordPress software or it can be pushed as an immediate security release, depending on the severity of the issue.

For an immediate security release, an advisory is published by the Security Team to the WordPress.org News site announcing the release and detailing the changes. Credit for the responsible disclosure of a vulnerability is given in the advisory to encourage and reinforce continued responsible reporting in the future.

Administrators of the WordPress software see a notification on their site dashboard to upgrade when a new release is available, and following the manual upgrade users are redirected to the About WordPress screen which details the changes. If administrators have automatic background updates enabled, they will receive an email after an upgrade has been completed.

Automatic Background Updates for Security Releases

Starting with version 3.7, WordPress introduced automated background updates for all minor releases, such as 3.7.1 and 3.7.2. The WordPress Security Team can identify, fix, and push out automated security enhancements for WordPress without the site owner needing to do anything on their end, and the security update will install automatically.

When a security update is pushed for the current stable release of WordPress, the core team will also push security updates for all the releases that are capable of background updates (since WordPress 3.7), so these older but still recent versions of WordPress will receive security enhancements.

Individual site owners can opt to remove automatic background updates through a simple change in their configuration file, but keeping the functionality is strongly recommended by the core team, as well as running the latest stable release of WordPress.

How WordPress handles the OWASP Top 10 security risks

The Open Web Application Security Project (OWASP) is an online community dedicated to web application security. The OWASP Top 10 list focuses on identifying the most serious application security risks for a broad array of organizations. The Top 10 items are selected and prioritized in combination with consensus estimates of exploitability, detectability, and impact estimates.

The following sections discuss the APIs, resources, and policies that WordPress uses to strengthen the core software and 3rd party plugins and themes against these potential risks.

A1 - Injection

There is a set of functions and APIs available in WordPress to assist developers in making sure unauthorized code cannot be injected, and help them validate and sanitize data. Best practices and documentation are available on how to use these APIs to protect, validate, or sanitize input and output data in HTML, URLs, HTTP headers, and when interacting with the database and filesystem. Administrators can also further restrict the types of file which can be uploaded via filters.

A2 - Broken Authentication and Session Management

WordPress core software manages user accounts and authentication and details such as the user ID, name, and password are managed on the server-side, as well as the authentication cookies. Passwords are protected in the database using standard salting

and stretching techniques. Existing sessions are destroyed upon logout for versions of WordPress after 4.0.

A3 - Cross Site Scripting (XSS)

WordPress provides a range of functions which can help ensure that user-supplied data is safe. Trusted users, that is administrators and editors on a single WordPress installation, and network administrators only in WordPress Multisite, can post unfiltered HTML or JavaScript as they need to, such as inside a post or page. Untrusted users and user-submitted content is filtered by default to remove dangerous entities, using the KSES library through the wp_kses function.

As an example, the WordPress core team noticed before the release of WordPress 2.3 that the function the_search_query() was being misused by most theme authors, who were not escaping the function's output for use in HTML. In a very rare case of slightly breaking backward compatibility, the function's output was changed in WordPress 2.3 to be pre-escaped.

A4 - Insecure Direct Object Reference

WordPress often provides direct object reference, such as unique numeric identifiers of user accounts or content available in the URL or form fields. While these identifiers disclose direct system information, WordPress' rich permissions and access control system prevent unauthorized requests.

A5 - Security Misconfiguration

The majority of the WordPress security configuration operations are limited to a single authorized administrator. Default settings for WordPress are continually evaluated at the core team level, and the WordPress core team provides documentation and best practices to tighten security for server configuration for running a WordPress site.

A6 - Sensitive Data Exposure

WordPress user account passwords are salted and hashed based on the Portable PHP Password Hashing Framework. WordPress' permission system is used to control access to private information such an registered users' PII, commenters' email addresses, privately published content, etc. In WordPress 3.7, a password strength meter was included in the core software providing additional information to users setting their passwords and hints on increasing strength. WordPress also has an optional configuration setting for requiring HTTPS.

A7 - Missing Function Level Access Control

WordPress checks for proper authorization and permissions for any function level access requests prior to the action being executed. Access or visualization of administrative URLs, menus, and pages without proper authentication is tightly integrated with the authentication system to prevent access from unauthorized users.

A8 - Cross Site Request Forgery (CSRF)

WordPress uses cryptographic tokens, called nonces, to validate intent of action requests from authorized users to protect against potential CSRF threats. WordPress provides an API for the generation of these tokens to create and verify unique and temporary tokens, and the token is limited to a specific user, a specific action, a specific object, and a specific time period, which can be added to forms and URLs as needed. Additionally, all nonces are invalidated upon logout.

A9 - Using Components with Known Vulnerabilities

The WordPress core team closely monitors the few included libraries and frameworks WordPress integrates with for core functionality. In the past the core team has made contributions to several third-party components to make them more secure, such as the update to fix a cross-site vulnerability in TinyMCE in WordPress 3.5.214.

If necessary, the core team may decide to fork or replace critical external components, such as when the SWFUpload library was officially replaced by the Plupload library in 3.5.2, and a secure fork of SWFUpload was made available by the security team for those plugins who continued to use SWFUpload in the short-term.

A10 - Unvalidated Redirects and Forwards

WordPress' internal access control and authentication system will protect against attempts to direct users to unwanted destinations or automatic redirects. This functionality is also made available to plugin developers via an API, wp_safe_redirect().

Further Security Risks and Concerns

XXE (XML eXternal Entity) processing attacks

When processing XML, WordPress disables the loading of custom XML entities to prevent both External Entity and Entity Expansion attacks. Beyond PHP's core functionality, WordPress does not provide additional secure XML processing API for plugin authors.

SSRF (Server Side Request Forgery) Attacks

HTTP requests issued by WordPress are filtered to prevent access to loopback and private IP addresses. Additionally, access is only allowed to certain standard HTTP ports.

The WordPress Release Cycle

Each WordPress release cycle is led by one or more of the core WordPress developers. A release cycle usually lasts around 4 months from the initial scoping meeting to launch of the version.

A release cycle follows the following pattern:

- **Phase 1**: Planning and securing team leads. This is done in the #core chat room on Slack. The release lead discusses features for the next release of WordPress. WordPress contributors get involved with that discussion. The release lead will identify team leads for each of the features.

- **Phase 2**: Development work begins. Team leads assemble teams and work on their assigned features. Regular chats are scheduled to ensure the development keeps moving forward.

- **Phase 3**: Beta. Betas are released, and beta-testers are asked to start reporting bugs. No more commits for new enhancements or feature requests are carried out from this phase on. Third-party plugin and theme authors are encouraged to test their code against the upcoming changes.

- **Phase 4**: Release Candidate. There is a string freeze for translatable strings from this point on. Work is targeted on regressions and blockers only.

- **Phase 5**: Launch. WordPress version is launched and made available in the WordPress Admin for updates.

Version Numbering and Security Releases

A major WordPress version is dictated by the first two sequences. For example, 3.5 is a major release, as is 3.6, 3.7, or 4.0. There isn't a "WordPress 3" or "WordPress 4" and each major release is referred to by its numbering, e.g., "WordPress 3.9."

Major releases may add new user features and developer APIs. Though typically in the software world, a "major" version means you can break backwards compatibility, WordPress strives to never break backwards compatibility. Backwards compatibility is one of the project's most important philosophies, with the aim of making updates much easier on users and developers alike.

A minor WordPress version is dictated by the third sequence. Version 3.5.1 is a minor release, as is 3.4.23. A minor release is reserved for fixing security vulnerabilities and addressing critical bugs only. Since new versions of WordPress are released so frequently — the aim is every 4-5 months for a major release, and minor releases happen as needed — there is only a need for major and minor releases.

Version Backwards Compatibility

The WordPress project has a strong commitment to backwards compatibility. This commitment means that themes, plugins, and custom code continues to function when WordPress core software is updated, encouraging site owners to keep their WordPress version updated to the latest secure release.

Security of WordPress Plugins

There are approximately 50,000+ plugins listed on the WordPress marketplace. These plugins are submitted for inclusion and are manually reviewed by volunteers before making them available on the repository.

Inclusion of plugins and themes in the repository is not a guarantee that they are free from security vulnerabilities. Guidelines are provided for plugin authors to consult prior to submission for inclusion in the repository, and extensive documentation about how to do WordPress plugin development is provided on the WordPress.org site.

Each plugin and has the ability to be continually developed by the plugin owner, and any subsequent fixes or feature development can be uploaded to the repository and made available to users with that plugin or theme installed with a description of that change. Site administrators are notified of plugins which need to be updated via their administration dashboard.

When a plugin vulnerability is discovered by the WordPress Security Team, they contact the plugin author and work together to fix and release a secure version of the plugin. If there is a lack of response from the plugin author or if the vulnerability is severe, the plugin is pulled from the public directory, and in some cases, fixed and updated directly by the Security Team.

It is important to note that some WordPress plugins are so large in complexity and user numbers that they could be considered products on their own. For example, WooCommerce is an e-commerce plugin that powers millions of websites and has dozens of plugins on its own. YoastSEO is another popular plugin with millions of users. Elementor is a popular visual page builder with about one million users. This kind of plugins are created and maintained by large and serious, often multi-million Dollar businesses that maintain impeccable security records.

Security of WordPress Hosting

Configuration of the operating system and the underlying web server hosting the software is clearly important to keep the WordPress applications secure. WordPress VIP and WPEngine offer SaaS style solution to hosting, deployment and staging. For more flexible setups, it is important to note that all cloud hosting giants like Microsoft Azure, Amazon AWS and Google Cloud provide optimized environments and tools for enterprise-grade WordPress hosting with all the benefits of the Cloud, such as auto-scaling, load balancing, self-healing etc.

For those interested in managing their own enterprise grade hosting infrastructure, United Experts provides sets of optimized plugins and tools for staging, deployment, redundancy and backup along with “recipes” for best practices in the area of security, and related training.

Conclusion

WordPress has become the unlikely hero of digital transformations of enterprises such as CNN, USA Today, Sony, Toyota, Mercedes-Benz and Microsoft. Nevertheless, one of the most common misconceptions about WordPress is that it is insecure. That is predominantly due to the fact that WordPress is the only large-scale software platform whose use spans from the consumer to the enterprise market powering 33% of the entire Web. The consumer nature of the platform leads to frequent implementations by amateurs who do not follow even basic best practices in the area of security, which is completely irrelevant for a professional setup.

WordPress is not only secure but is in fact one of the most secure WCM platforms in the world. It **brings unparalleled security** to some of the **most complex digital projects of some of the world's largest brands**. The outstanding WordPress security is embedded in:

- Mature, polished WordPress Core with an outstanding evaluation for handling OWASP security risks,
- Platform architecture which enables automatic, background updates with security patches which dramatically simplifies and speeds up related maintenance and associated costs,
- Availability of huge resources for security management, including around 50 full-time security experts, thousands of contributors, and big-name partners such as Google and Microsoft

About The Creators

Boris Motusic - Co-Founder & Chief Digital Architect at United Experts, author, and keynote speaker. Boris created WCM system architecture, managed, and consulted world leading brands like Best Western Hotels, BNP Paribas, PwC, and Hitachi with some of the most complex digital projects.
Contact Boris at boris@ue.team

United Experts – digital consultancy since 1997. Digital masterminds from the UE core team join forces with tech and creative talent from companies such as Google, Microsoft, and Amazon to create Digital Project Superteams. Together, they deliver some of the world's most challenging digital projects. But it doesn't end there; valuable experience is shared through training and education, contributions to community events, public speaking, and open source projects. In terms of WCM, United Experts has a narrow focus on enterprise implementations of WordPress and Sitefinity.

Contact United Experts at team@ue.team and www.ue.team