POLYSCRIPTING FOR WORDPRESS

Advanced security for the Internet's most popular CMS.

TABLE OF CONTENTS

POLYVERSE

Why Read this Whitepaper

WordPress is by far the world's most popular content management system (CMS). It is used by 37 percent of all websites, which translates into a dominant lead in the CMS market with a share of more than 63 percent.[1] To add some context, it has held onto this commanding position for more than a decade, while its nearest competitor has achieved a market share of less than 5 percent.

However, WordPress is also a victim of its own success. It is now the most targeted and hacked content management system, accounting for 90 percent of all hacked and infected CMS websites in 2018.[2] Keeping WordPress deployments updated, patched and protected is a major dilemma for a broad range of business and IT stakeholders. It will be a particular concern for high-end hosting providers and their customers, or anyone self-hosting their own environment.

This white paper provides a compelling insight into a radically new and innovative approach for protecting and securing WordPress. Polyscripting for WordPress neutralizes and eliminates all of the most dangerous attack vectors, including remote code injection, backdoors and file inclusion assaults.

Balancing the WordPress Benefits Verses Risks Equation

As we mentioned at the outset, WordPress is the outright market leader for CMS solutions. But in our increasingly digitalized global economy, the importance of WordPress has continued to grow. This is because it has also become one of the most popular options for building and operating online stores or e-commerce platforms. It is estimated that it powers around 60 percent[3] of all CMS-based websites and that 28 percent of all e-commerce is transacted through WooCommerce, which is just one of the many e-commerce plugins available for WordPress.

The benefits of using WordPress are easy to understand. It is flexible and highly customizable, with more than 55,000 plugins and more than 3,500 GPL-licenced themes available. This makes it fast and easy to spin up an e-commerce website with just the look and feel needed to appeal to your customers. Additionally, because it is a freely available open source platform written in PHP, costs can be kept under strict control and there is a vast support community available to call on should the need arise.

But strengths can also end up being weaknesses. We've already mentioned that hackers have a well-used playbook for attacking digital storefronts built with WordPress and PHP (the server-side programming language at the heart of WordPress). Of the security vulnerabilities they target, 75 percent are due to WordPress plugins and 11 percent are due to WordPress themes, with 14 percent from the core application code.[4] Hence, the features that make WordPress so adaptable are also the areas of weakness that can be exploited.

This doesn't mean that WordPress is inherently unsafe, but it does show how critically important it is to keep the whole environment up to date and appropriately patched. But this is a complex and time-consuming task. It's a constant headache and you simply have to keep on top of it. Reports suggest only 35 percent[5] of WordPress websites are running on the latest code base and more than 70 percent[6] are vulnerable because of being unsuitably patched.

With all these open vulnerabilities to choose from, the hacker's favorite and most successful attack methodologies now embrace code injection, backdoors and file inclusions. If they can gain access to your WordPress environment and run their own code, then they have free rein to access or change customer data, steal credit card details, or hold organizations to ransom. The stakes couldn't be higher for businesses of all sizes and in all sectors.

Online security is now a shared responsibility, where virtually everyone is a stakeholder. Any cybersecurity solution that delivers rock-solid, impenetrable protection for WordPress and PHP will be highly attractive to a wide audience, but especially for executives, senior IT, or cybersecurity professionals.

That's where Polyscripting technology comes in. It stops all code-injection attacks by making it impossible for any foreign code to be executed. It also removes the overhead of constant monitoring, updating, and patching across the entire WordPress environment. Additionally, it alleviates the stress caused by the threat of unknown zero-day vulnerabilities.

1 Source: W3Techs Web Technology Surveys

2 Source: Securi Hacked Website Report 2018

3 Source: Hostingtribunal.com

4 Source: ithemes.com: 5 Common WordPress Security Issues

5 Source: wordpress.org

6 Source: wpwhitesecurity.com

Polyscripting Technology—Redefining WordPress Security

Polyscripting is a ground-breaking technology that can quickly and easily be applied to the entire WordPress ecosystem for advanced cybersecurity protection. An in-depth technical analysis of how Polyscripting functions can be found in the Polyscripting for WordPress technical whitepaper so below is a high-level summary of its operation intended for business and IT decision-makers.

Polyscripting works by scrambling the syntax and grammar of the entire WordPress software stack. This includes the underlying PHP programming language, the WordPress application code, as well as each of the plug-ins and themes that provide additional features and functionality to the website or webstore. This effectively gives each website a unique and exclusive instance of the programming language and an exclusive application software stack.

Figure 1 below illustrates how this process is accomplished. Following the build phase, all the key components of the WordPress ecosystem are run through an advanced compiler. This randomly transforms the PHP programming language as well as the entire website source code before it goes into production. Everything now uses a one-of-a-kind language dictionary, which has a matching and equally unique interpreter. This new interpreter no longer understands the original PHP syntax, grammar, or command set. It will only run and execute the source code that matches the newly generated instance of PHP.

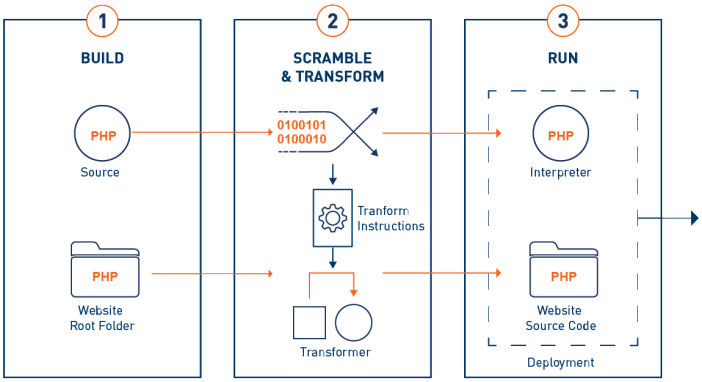

Figure 1: Polyscripting for WordPress process flow

This means that any attempt made by a hacker to carry out script, code, or file injection is doomed to failure. This type of attack relies on two factors to succeed. First, the opportunity to take advantage of a buffer overflow or a similar memory corruption vulnerability to inject the code. Second, the ability to execute the code. Even if a hacker manages to inject foreign code onto the webserver, it's written in the original unscrambled PHP programming language, which will be unrecognizable to the newly randomized interpreter. The result is that the injected code cannot be executed and will immediately be flagged to the system as an error, making the attack instantly visible.

There are several other benefits to highlight:

- Because Polyscripting is carried out after the build stage and before any code is run on the webserver, there is absolutely no impact on existing functionality, performance, or interoperability.
- Servers or websites running older or unpatched software builds are now protected without any additional administrative overhead or costly resources. This removes the stress of constantly monitoring, updating and patching. These tasks can be efficiently carried out via planned maintenance schedules.
- Undiscovered zero-day vulnerabilities are no longer a major concern. Any code injection attacks that exploit them still cannot be executed.
- The Polyscripting process can be repeated at regular intervals or on-demand. This adds an additional layer of defense to the entire WordPress landscape making it virtually impossible to crack.

Polyscripting for WordPress Deployment

Polyscripting for WordPress was designed around two key priorities. For obvious reasons, the first was to deliver the ultimate level of cybersecurity protection. The second was to make sure it has no impact on the usability of WordPress in any way.

Given its level of popularity, installing WordPress is a well-trodden path and there are numerous sources available to help guide you through the process. There are also a variety of options as to how a WordPress environment will be hosted. Numerous high-level hosting providers can handle everything for you. Alternatively, you may choose to self-host either on a cloud platform or in your own data center. The typical deployment time for WordPress will vary depending upon complexity, but you are likely to be up and running in a few hours.

By contrast, applying Polyscripting for WordPress is fast and easy. Everything other than the activation license is packaged into a

single docker container. This includes the advanced Polyscripting compiler, as well as appropriate templates to make the whole process smooth and straightforward. The only prerequisites are suitable user rights to manage WordPress and the ability to modify the underlying PHP code. The Polyscripting process then requires a single change to one environment variable before restarting the container. This triggers the creation of a unique instance of PHP and WordPress ecosystem before binding it to the webserver. A deep copy of all WordPress files is then carried out from the original file store to the container. Only the copy now in the container is scrambled, with the original files left entirely untouched. At that point, the environment is fully protected. To re-scramble the entire environment, it is simply a matter of restarting the containers and the Polyscripting process is repeated.

When it came to deploying Polyverse's own WordPress environment, in addition to security and ease of use considerations, we were also keenly focused on delivering the highest levels of reliability and performance. Although similar results could have been achieved on any of the major cloud platforms, we chose to deploy on the AWS cloud.

Figure 2 below shows the Polyverse high-level WordPress architecture.

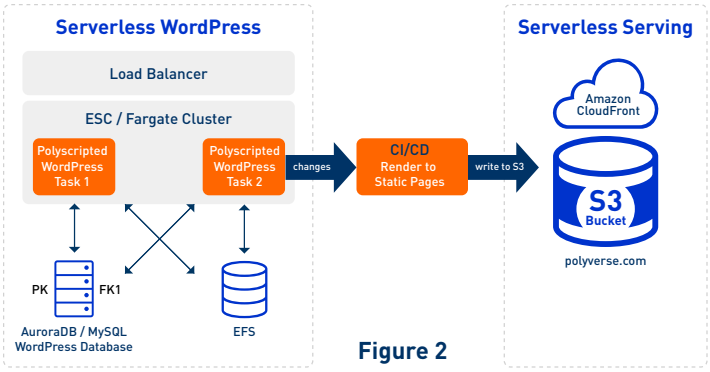

Figure 2

As you can see, this is a serverless design that takes full advantage of the following cloud components:

- Amazon Elastic Container Service (ECS), for high performance and highly-scalable container orchestration.
- The Amazon Fargate compute engine that enables containers to operate in a serverless environment.
- Amazon Elastic File System (EFS), enabling persistently shared storage to be defined and used at the task and container level in ECS.
- The Amazon CloudFront content delivery network for high speed localized content access to consumers of the website content.
- Amazon Simple Storage Service (S3), providing scalable object storage via the web service interface.
- Amazon CloudWatch Synthetics, for monitoring the health of the website content and application endpoints.

While this may appear to be a fairly complicated production-ready blueprint for WordPress, it is incredibly simple to operate and requires very little ongoing management overhead. WordPress authors never need to know about the underlying architecture. They simply carry on doing their work using the world's most popular CMS platform as they would in any other circumstances. From an operational perspective, there are no scalability, load prediction, or performance concerns that need to be addressed.

Most importantly, by applying the Polyscripting technology, cybersecurity protection is raised to an exponentially higher level as verified by independent third-party penetration testing. In common with all deployments, as soon as Polyverse's WordPress website went online, it started to experience attacks from hackers probing for weaknesses. The built-in monitoring and alarm features built into Polyscripting for WordPress detects each of these code injection attempts and records the exact line of code where the attack was attempted. This effectively provides a honeypot capability to capture and analyze any unknown zero-day vulnerability attacks used against the website.

Conclusion and Recommendations

It is self-evident that the suboptimal protection of any website is asking for trouble. The global average cost of a data breach is currently around $4 million per incident. No forward-thinking organization wants to end up as headline news for being the next high-level cybersecurity victim, with all the notoriety and financial impact that will have on their business.

As the outright market leader for CMS and e-commerce webstores, WordPress is a prime target for cybersecurity attacks. Unprotected websites are under attack within a minute of going live. Recent hacking campaigns alone have compromised more

than 2,000 WordPress sites[7] by exploiting vulnerabilities using script injection techniques. It's worth noting that Polyscripting technology would have provided total protection and immunity for every organization that was targeted and compromised.

Building a suitable business case for executive approval for cybersecurity protection remains a vitally important step, especially in the current economic climate. This involves weighing up all available options by evaluating the benefits, risks and costs for each of them.

Traditional basic security measures will always be vital for any WordPress deployment. These should include enforcing strong passwords, two-factor authentication; limiting login attempts; CAPTCHA login pages; strict user and file permissions; adding security plugins along with appropriate security policies; virus and malware scanning.

However, any cybersecurity planning should also include advanced security solutions that will truly make a difference. Polyscripting for WordPress provides that extra layer of state-of-the-art protection by entirely eliminating all code injection, file inclusion or backdoor cybersecurity threats.

Other Resources

- Polyscripting for WordPress Product Brief
- The Business of WordPress Webinar
- Polyscripting for WordPress Technical Webinar
- Polyscripting for WordPress Webpage

Contact us at:
sales-us@polyverse.com
sales-emea@polyverse.com
sales-apac@polyverse.com

or visit our website
https://polyverse.com

7 Source: Techradar