POLYSCRIPTING FOR PHP

ERADICATE CODE INJECTION THREATS

For the past decade, PHP has maintained its status as the most popular server-side scripting language. Today, 4 out of 5 websites rely on PHP for running critical web applications. At the same time, code injection remains the top security risk for web applications, with hackers specifically targeting known PHP vulnerabilities. Polyscripting for PHP represents a paradigm shift in cybersecurity protection. It completely eradicates all code-injection hazards by making it impossible for any injected code to be executed on the server.

At a Glance

Key Benefits

+ *Neutralizes 100% of PHP code-injection attacks*
+ *Entails no change to functionality or performance*
+ *Makes it possible to patch for hygiene, not security*
+ *Provides high return on security investment*
+ *Maintains security compliance*

Product Overview

Polyscripting for PHP is a powerful new technology designed to completely neutralize code-injection attacks. It eliminates the stress of having to constantly track and hastily patch weaknesses and flaws. This is important because, despite the popularity and widespread use of PHP, some vulnerabilities have gone unreported and unpatched for over a year, leaving millions of systems open to exploitation.

Polyscripting for PHP removes the mechanism that could otherwise enable hackers to execute injected code on a web server, making this entire threat category futile. This is achieved by scrambling the syntax and grammar of the programming language, effectively giving each website a unique instance of the language. The result is that any injected code written in the standard language format is no longer recognized and simply cannot run. Furthermore, any attempt to execute rogue injected code is instantly detected and flagged by triggering a syntax error.

Polyscripting for PHP is the most powerful and innovative way to safeguard against PHP code-injection attacks without impacting program functionality or interoperability in any way. It's available on GitHub under the MIT open source license, which means it is free to download and you can begin reaping the benefits immediately in your own PHP environment.

Key Benefits

Neutralizes 100% of PHP code-injection attacks. Creating a randomized and unique implementation for each website safeguards against 100% of code-injection cyberattacks, the top security threat for PHP-based web applications.

Removes the stress and urgency to apply security patches. Unpatched servers and websites are safeguarded without additional administration overhead or costly resources. Patches can be efficiently and pragmatically applied when it is most

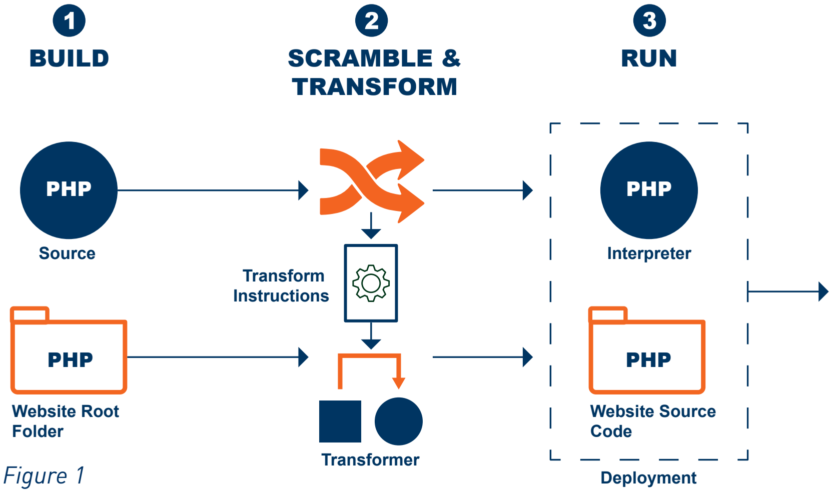

Figure 1

convenient for the business, freeing up valuable IT resources to focus on innovation.

Maintains security compliance. Polyscripting for PHP facilitates adherence to strict security-compliance frameworks enabling an incremental, robust and innovative cybersecurity barrier.

Provides outstanding Return on Security Investment (ROSI). Polyscripting for PHP delivers superior, high-caliber, code-injection protection at a substantially lower cost than more traditional solutions. It's easier for each organization to balance its specific security-risk profile and budget.

Key Features

- **The only way to avoid code-injection** when running production code with known and unknown vulnerabilities.
- **Zero changes to anything that matters.** Polyscripting for PHP entails no changes to program functionality or interoperability; no impact on developers, the development process or users; and no runtime performance overhead.
- **Early detection of malicious activity.** Any attempts to run injected code are instantly detected by triggering a syntax error.
- **Freely available to download on GitHub under the MIT open source license.**

How it Works

Code injection is an incredibly powerful kind of cyberattack that enables malicious actors to run their code on servers or websites belonging to others. It has often been used as a backdoor to access, steal, change or corrupt data. Some of the most damaging security breaches have relied on code-injection techniques.

Polyscripting is a beautifully simple but amazingly effective tool that eliminates the danger of code-injection threats. It works by randomizing the syntax and grammar within the PHP interpreter source code before the interpreter is compiled. This creates a unique instance of a language, as well as a matching interpreter. The new interpreter no longer understands the syntax and grammar of the original language. It will only run application source-code that matches the newly generated and unique interpreter, which remains a mystery to any hacker seeking to activate a code-injection assault. (figure 1)

Even better, the Polyscripting process can be repeated on demand at regular intervals to add yet another layer of defense. This makes even an individually crafted and targeted code-injection attempt a hopeless task because it will no longer work once the PHP interpreter and server-side web source-code is rescrambled.

To implement Polyscripting in your environment, contact us.

> "Polyverse is recognized for creating unprecedented resilience against cyberattacks by making the software on every computer unique and diverse. Polyverse's ability to eliminate zero-day threats, employ moving target defense, and eliminate code injection with Polyscripting makes the company a leader in preventative cybersecurity."

David Campbell
CEO
Tech Ascension Awards

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

or visit our website
https://polyverse.com

POLYVERSE