Mengamankan PHP

Mengamankan PHP Apache

Untuk membatasi serangan hacker pada PHP dalam instalasi LAMPP (Linux, Apache, MySQL, PHP, PHPMyAdmin), Anda dapat mengambil beberapa langkah keamanan untuk melindungi aplikasi web Anda dari berbagai jenis serangan. Berikut adalah beberapa konfigurasi dan praktik keamanan umum yang dapat membantu Anda:

Update PHP
Pastikan Anda menjalankan versi PHP yang paling baru dan selalu diperbarui. Setiap pembaruan PHP biasanya mencakup perbaikan keamanan. Anda juga dapat mempertimbangkan untuk menggunakan PHP versi 8.x atau yang lebih baru, karena ini mendukung peningkatan keamanan dan kinerja.

Konfigurasi PHP
Edit file **php.ini** di **/etc/php/8.1/cli/php.ini** dan/atau **/etc/php/8.1/apache2/php.ini** dan terapkan konfigurasi keamanan berikut:

- Batasi maksimum ukuran upload file dengan parameter **upload_max_filesize** dan **post_max_size**.
- Matikan **register_globals**.
- Matikan **allow_url_fopen** dan **allow_url_include** untuk mencegah inklusi dan akses ke URL eksternal.
- Setel **display_errors** menjadi **Off** dalam produksi untuk menghindari menampilkan kesalahan PHP ke publik.
- Aktifkan disable_functions untuk memblokir fungsi-fungsi berbahaya jika Anda tahu apa yang Anda lakukan.
- Aktifkan open_basedir untuk membatasi direktori yang diizinkan PHP untuk mengakses.

Menggunakan opsi **disable_functions** dalam konfigurasi PHP dapat membantu mengurangi risiko keamanan dengan memblokir fungsi-fungsi tertentu yang dapat digunakan oleh penyerang untuk melakukan aktivitas berbahaya. Namun, penggunaan **disable_functions** harus dilakukan dengan hati-hati, karena mematikan fungsi-fungsi tertentu dapat mempengaruhi fungsi normal dari aplikasi PHP Anda. Beberapa fungsi yang sering kali dinonaktifkan karena potensi risiko keamanan termasuk:

1. **exec**: Fungsi exec() digunakan untuk menjalankan perintah shell dari dalam skrip PHP. Ini harus dinonaktifkan untuk mencegah penyerang menjalankan perintah shell di server

Anda.

2. **system**: Sama seperti `exec()`, `system()` juga digunakan untuk menjalankan perintah shell. Ini harus dinonaktifkan.
3. **shell_exec**: Fungsi `shell_exec()` juga digunakan untuk menjalankan perintah shell dan harus dinonaktifkan.
4. **passthru**: `passthru()` adalah fungsi lain yang dapat digunakan untuk menjalankan perintah shell. Ini juga harus dinonaktifkan.
5. **popen**: `popen()` memungkinkan skrip PHP untuk membuka pipe ke proses eksternal. Ini harus dinonaktifkan.
6. **proc_open**: Fungsi ini serupa dengan `popen()` dan juga digunakan untuk menjalankan proses eksternal. Ini harus dinonaktifkan.
7. **eval**: Fungsi `eval()` digunakan untuk mengeksekusi kode PHP dari string. Penyerang dapat memanfaatkannya dengan memasukkan kode berbahaya ke dalam string.
8. **assert:** Fungsi `assert()` juga dapat digunakan untuk mengeksekusi kode PHP dari string. Ini harus dinonaktifkan.
9. **system_popen**: Ini adalah alternatif lain untuk `popen()` dan harus dinonaktifkan.
10. **dl**: Fungsi `dl()` digunakan untuk memuat ekstensi PHP dinamis. Ini dapat membuka celah keamanan jika dinonaktifkan.
11. **proc_close:** Ini adalah fungsi terkait dengan `proc_open()` yang digunakan untuk menutup proses yang telah dibuka dengan `proc_open()`. Dinonaktifkan juga.
12. **pcntl_exec**: Fungsi ini memungkinkan penggunaan fungsi `exec()` dalam lingkungan PHP-FPM. Jika Anda tidak menggunakannya, disarankan untuk dinonaktifkan.

Cari baris yang mengandung **`disable_functions`**. Jika Anda tidak menemukannya, Anda dapat menambahkannya di bagian paling bawah file **php.ini**.

Tambahkan nama fungsi-fungsi yang ingin Anda nonaktifkan, dipisahkan oleh tanda koma. Misalnya, jika Anda ingin menonaktifkan fungsi exec, system, dan eval, tambahkan baris berikut:

```
disable_functions = exec, system, eval
```

Setelah menyimpan perubahan, Anda perlu merestart Apache agar perubahan ini berlaku:

systemctl restart apache2

Catatan:
Pastikan bahwa Anda memeriksa bahwa aplikasi PHP Anda tetap berfungsi dengan baik setelah mengaktifkan disable_functions, karena beberapa fungsi PHP mungkin diperlukan untuk fungsi normal aplikasi Anda. Selalu uji aplikasi Anda dengan cermat setelah mengubah pengaturan ini.

Revisi #2
Dibuat 24 Desember 2025 18:58:14 oleh Friscia Anthony
Diperbaharui 24 Desember 2025 19:06:43 oleh Friscia Anthony