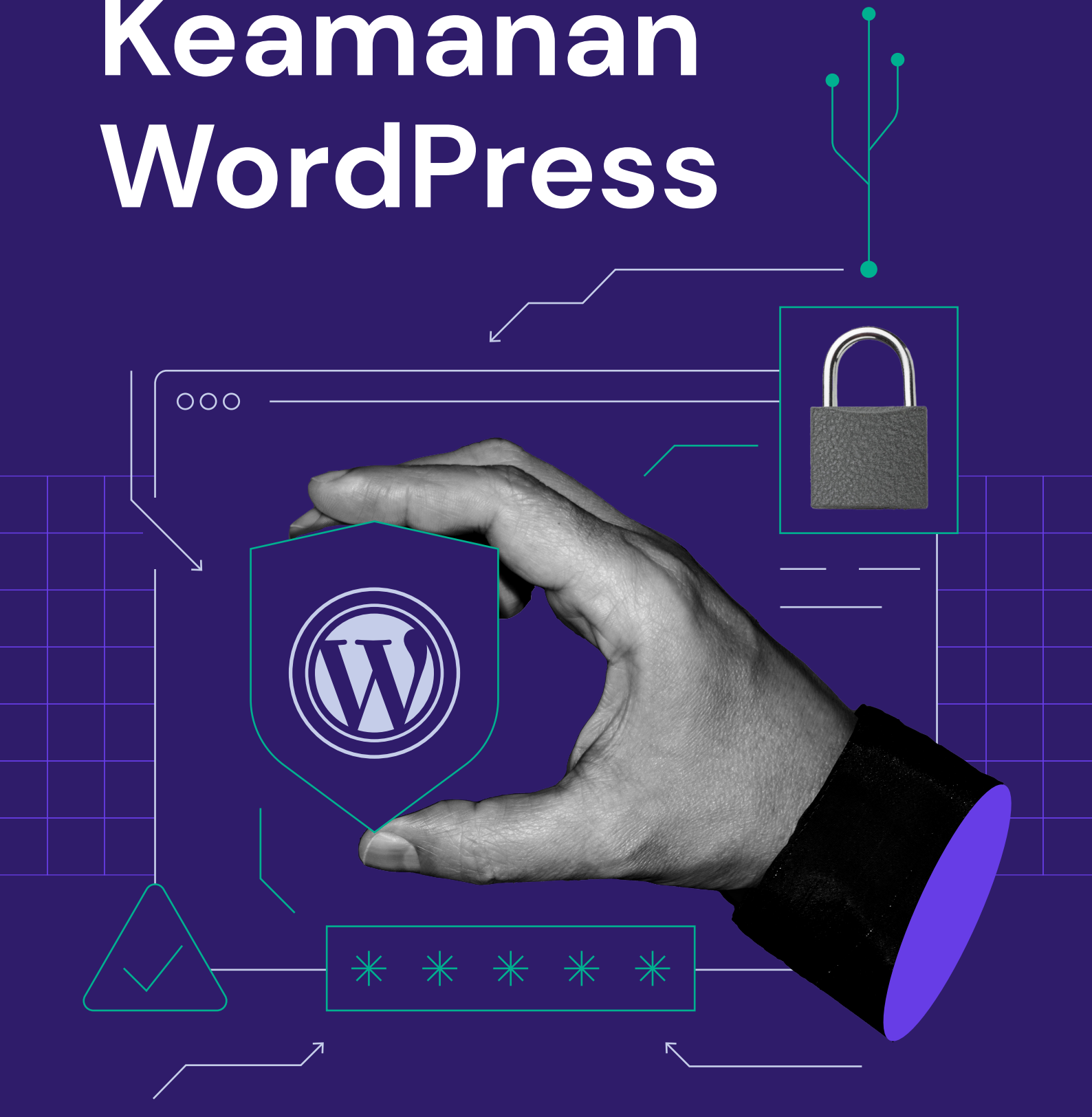
HOSTINGER

Three. Two. Online

Checklist Keamanan WordPress



Checklist Keamanan WordPress

Untuk melindungi website dari serangan cyber, Anda wajib menerapkan langkah-langkah keamanan yang tepat. Meskipun tidak memerlukan skill teknis tingkat lanjut untuk melakukannya, langkah-langkah ini bisa meningkatkan keamanan website WordPress Anda secara signifikan.

Nah, untuk membantu Anda mengamankan website, kami sudah menyiapkan checklist yang menjelaskan langkah-langkah dan tips keamanan WordPress terbaik.

Update software inti WordPress

Setiap update WordPress menghadirkan peningkatan keamanan seperti perbaikan bug dan fitur baru. Dengan versi software terbaru, risiko pelanggaran keamanan di website Anda pun bisa diminimalkan.

Update tema dan plugin

Sama seperti software inti, tema dan plugin WordPress juga mendapatkan update untuk memperbaiki setiap celah keamanan. Segera update keduanya setelah versi barunya tersedia.

Gunakan tema WordPress tepercaya

Instal tema dari repositori WordPress resmi atau developer yang kredibel. Jangan pernah menggunakan tema hasil modifikasi karena mungkin memiliki masalah keamanan.

Gunakan kredensial login WP-admin yang aman

Password yang kuat dan username yang unik membuat informasi login Anda sulit ditebak, sehingga akan melindungi Anda dari serangan brute force.

Aktifkan autentikasi dua faktor

Tambahkan lapisan keamanan ekstra pada proses login. User harus memasukkan kode unik yang dikirimkan melalui pesan teks atau aplikasi autentikasi agar bisa login.

Backup WordPress secara teratur

Salah satu langkah mitigasi yang akan membantu memulihkan data website apabila terjadi insiden, serangan cyber, atau gangguan pada pusat data.

Cek apakah ada malware

Jadwalkan proses scan rutin untuk mencegah terjadinya kerusakan akibat malware, dan kalau terdeteksi, Anda bisa menghapusnya segera.

Hapus plugin dan tema yang tidak digunakan

Cegah serangan backdoor yang disebabkan oleh plugin dan tema yang sudah tidak dipakai dan tidak mendapat update lagi.

Instal sertifikat SSL

Implementasikan protokol transfer data yang aman untuk melindungi informasi yang dikirim dan diterima oleh website Anda dan penggunanya.

Buat whitelist dan blacklist untuk halaman admin

Cegah pembobolan informasi login dan halaman admin website Anda oleh alamat IP yang tidak sah.

Batasi upaya login

Gunakan plugin keamanan untuk memblokir akses dari alamat IP tertentu setelah gagal mencoba login sebanyak waktu yang ditetapkan.

Ubah URL halaman login WordPress

Menggunakan URL khusus akan mempersulit penyerang untuk masuk ke halaman website Anda.

Logout otomatis user yang tidak ada aktivitas

Biasanya, user lupa untuk logout dari website dan membiarkan sesi yang sedang aktif begitu saja. Gunakan plugin keamanan untuk mencegah pihak tidak berwenang mengakses halaman admin di perangkat yang sama.

Sembunyikan versi WordPress

Mengekspos informasi versi WordPress Anda akan memancing penyerang untuk mengeksploitasi celah keamanan, apalagi kalau Anda menggunakan versi lama.

Pantau aktivitas pengguna

Identifikasi aktivitas dan perubahan mencurigakan yang bisa membahayakan website. Hal ini penting kalau Anda memberikan akses kepada beberapa user ke area admin WordPress Anda.

Nonaktifkan pelaporan error

Laporan error PHP menampilkan kerentanan dan informasi lain tentang back-end website Anda yang bisa dieksploitasi oleh pihak tidak berwenang.

Lakukan migrasi ke web host yang aman

Salah satu tugas penyedia hosting adalah memastikan keamanan data dan file website pengguna di server mereka. Pilih penyedia hosting yang menyediakan fitur keamanan canggih, seperti update dan pemantauan.

Matikan pengeditan file

Pihak tidak berwenang bisa mengeksploitasi fitur editor file bawaan di WordPress untuk mengakses website Anda. Tambahkan baris kode sederhana berikut di file **wp-config.php** untuk menonaktifkannya:

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

Batasi akses menggunakan .htaccess

Gunakan file **.htaccess** untuk mengonfigurasi izin eksekusi PHP di folder tertentu dan melindungi file **wp-config.php**.

Ubah prefix database WordPress default

Cegah serangan SQL injection dengan mengganti kata **wp_** pada prefix database default.

Nonaktifkan XML-RPC

Fitur ini memiliki kelemahan yang bisa disalahgunakan penyerang dalam serangan brute force dan DDoS.

Blokir hotlink

Website lain yang menggunakan hotlink ke konten Anda bisa menghabiskan resource server dan memperlambat website Anda.

Kelola izin file

Gunakan FTP client atau file manager web hosting untuk menetapkan user mana yang bisa membaca, menulis, dan mengeksekusi izin pada file dan folder inti WordPress Anda.

Tips Bonus

- Buat password yang kuat untuk login WordPress menggunakan lebih dari 12 karakter, atau gunakan password generator untuk membuatnya.
- Jangan gunakan username umum seperti **admin** atau **administrator**.
- Instal plugin keamanan yang canggih dan lengkap seperti Wordfence. Plugin yang Anda pilih harus menyertakan fitur seperti autentikasi dua faktor, pembatasan upaya login, dan pemindaian malware.
- Gunakan Patchstack untuk mendeteksi kerentanan pada tema dan plugin Anda.
- Simpan data backup website di beberapa lokasi, seperti komputer lokal, flash drive USB, dan penyimpanan cloud.