NIAGAHOSTER

25 LANGKAH AMPUH MENGAMANKAN WEBSITE WORDPRESS

Daftar Isi

1

Keamanan Website: Lebih Baik Mencegah Daripada Mengobati

Perkembangan teknologi selalu diibaratkan sebagai pisau bermata dua. Di satu sisi, semakin maju teknologi, semakin banyak juga kemudahan yang didapatkan manusia. Namun, di sisi lain teknologi juga bisa membawa ancaman yang bisa membahayakan penggunanya..

Begitu juga halnya dengan website. Website adalah salah satu produk teknologi yang memudahkan banyak orang, baik itu untuk kepentingan bisnis, organisasi, maupun personal. Ada banyak hal positif yang bisa Anda lakukan menggunakan website.

Sayangnya, seperti yang sudah disebutkan di awal, perkembangan teknologi juga punya konsekuensinya, termasuk website. Orang-orang yang tidak bertanggung jawab melihat perkembangan website sebagai peluang untuk melakukan kejahatan online.

Fakta bahwa banyak kejahatan terjadi di internet bukan berarti Anda perlu berhenti mengembangkan website. Kabar baiknya ada banyak hal yang bisa Anda lakukan untuk melindungi website Anda dari serangan kejahatan di dunia maya.

Ebook ini akan memandu Anda membuat perlindungan yang ampuh dan efektif untuk mengamankan website Anda dari serangan kejahatan online.

Mencegah lebih baik daripada mengobati, bukan?

Mari belajar mengamankan website WordPress Anda dalam 25 langkah!

2

Mengapa Keamanan Website Itu Penting?

Meskipun serangan kejahatan online itu benar-benar nyata, masih ada sebagian pemilik website yang menyepelekan hal ini. Mereka pun tidak memberikan perlindungan lebih untuk website mereka. Akibatnya, ketika website mereka diserang malware atau hacking, tidak banyak yang bisa mereka lakukan.

Untuk menambah pengetahuan Anda soal keamanan website dan meningkatkan kewaspadaan Anda, kami akan membahas lima alasan betapa pentingnya keamanan website terlebih dahulu.

2.1 Ancaman Keamanan Terus Meningkat

WordPress sebagai platform pembuatan website terbesar di dunia menjadi target sasaran empuk para hacker. Menurut riset Sucuri, dari semua kasus serangan online pada 2017, 83 persen di antaranya menyerang WordPress. Angka meningkat dari tahun sebelumnya yang hanya 74 persen.

Fakta di atas tentu menjadi peringatan keras bagi semua pemilik website WordPress untuk meningkatkan perlindungan websitenya. Namun, tidak perlu khawatir karena ebook ini akan memandu Anda mengamankan WordPress secara paripurna!

2.2 Serangan Online Semakin Canggih

Para pembuat malware dan hacker selalu meningkatkan kualitas serangannya. Semakin hari, semakin canggih serangan yang mereka ciptakan. Oleh karena itu, Anda harus selalu memperbarui perlindungan website Anda.

2.3

Reputasi Bisnis Anda Menjadi Taruhannya

Beberapa tahun belakangan ini data privasi konsumen menjadi topik hangat. Kekhawatiran pencurian data membuat konsumen semakin berhati-hati ketika bertransaksi secara online. Hal ini tentu menuntut para pemilik bisnis untuk meningkatkan kualitas keamanan websitenya.

2.4

Website Tidak Aman Berpotensi Terkena Blacklist

Anda tidak hanya menjaga reputasi website di hadapan pelanggan, tetapi juga kepada Google. Google sebagai mesin pencari terbesar di dunia bisa memasukkan website Anda ke blacklist jika memang terbukti sebagai website tidak aman. Berdasarkan data Sucuri, sebanyak 17 persen website yang terinfeksi telah di-blacklist Google pada 2017

2.5

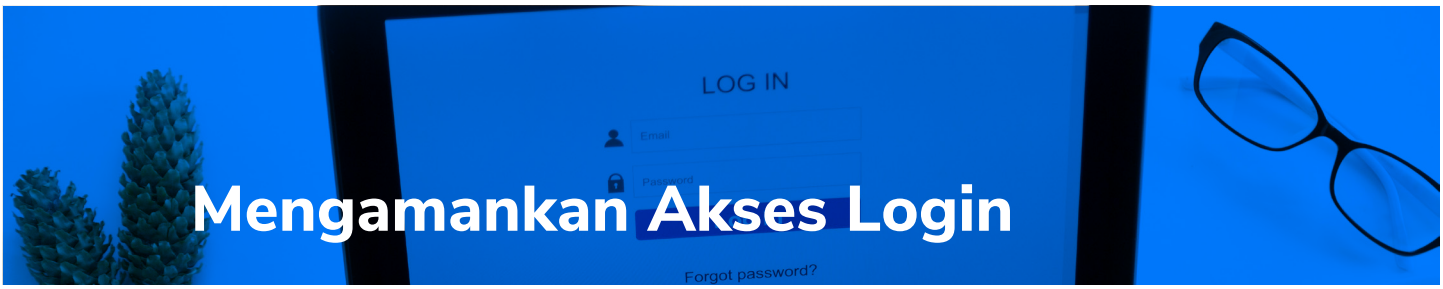
Mencegah Lebih Baik Daripada Mengobati

Perlindungan website memang membutuhkan proses yang panjang dan melelahkan. Namun, lebih baik menjalani proses panjang tersebut daripada merugi jika website diserang. Kerugian dari kejahatan online tidak hanya mencakup materi saja, tetapi juga masalah reputasi dan kepercayaan pelanggan dan pengunjung website.

Intinya, keamanan website bukan hal yang bisa Anda sepelekan. Untuk itu Anda perlu mempelajari cara-cara mengamankan website WordPress yang ampuh dan efektif. Nah, di ebook ini akan mempelajari semua hal soal keamanan website.

3

25 Cara Mengamankan WordPress Anda



Mengamankan Akses Login

Terdapat 25 langkah mengamankan website WordPress yang terbagi menjadi empat bagian, yaitu Mengamankan Akses Login, Menjaga Keamanan Instalasi WordPress, Mengamankan File dan Database, hingga Bonus Tips Keamanan.

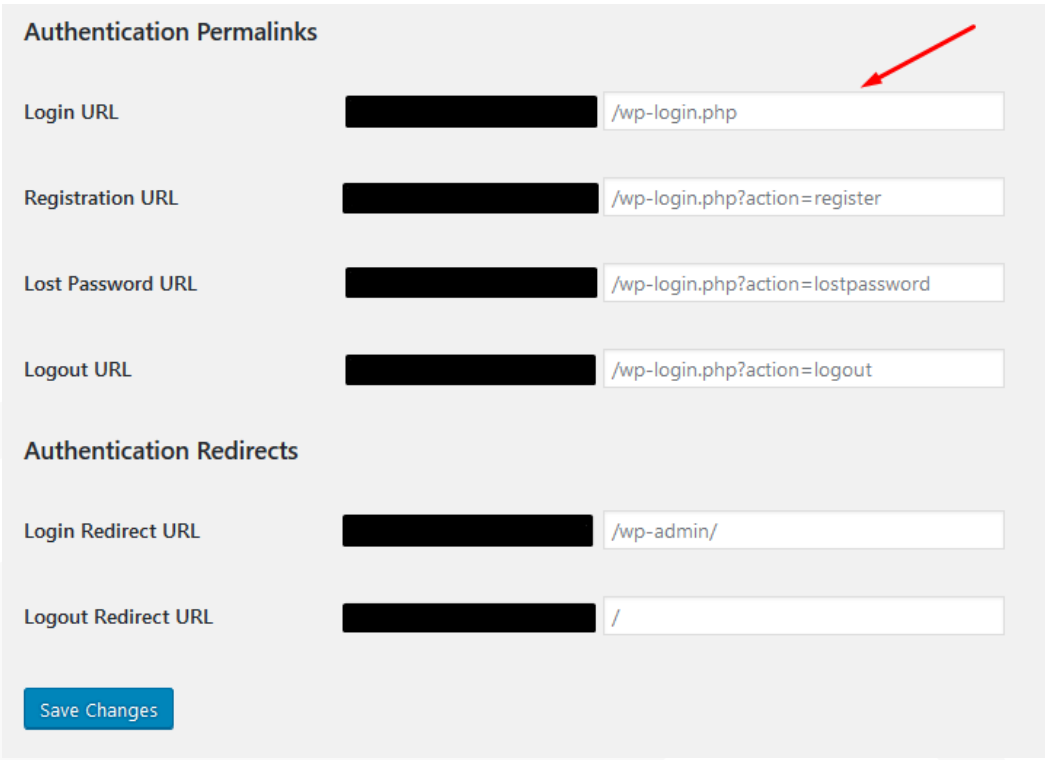
Yuk, mulai langkah pertama Anda mengamankan website!

1. Buat Custom Login URL

Ketika Anda pertama kali menginstall WordPress, link default login administratornya adalah wwww.domainanda.com/wp-login.php. Link default ini tentu memudahkan hacker untuk masuk ke dashboard WordPress Anda.

Anda perlu mengganti link login admin WordPress ke link yang tidak mudah diketahui orang lain. Bagaimana cara melakukannya? Caranya cukup mudah. Anda bisa mengubah link login admin WordPress menggunakan bantuan plugin.

Anda bisa menggunakan plugin gratis Custom Login URL. Install dan aktifkan plugin Custom Login URL melalui dashboard WordPress. Setelah aktivasi selesai, buka **Setting > Permalink** dan Anda akan melihat pengaturan seperti gambar di bawah ini:



Di kolom Login URL, Anda bisa mengganti **/wp-login.php** menjadi link apa pun yang Anda inginkan. Sebagai contoh, Anda bisa menggantinya menjadi **/admin-website**. Buat login URL yang unik dan hanya diketahui oleh Anda agar lebih aman.

2. Ganti Username Default Admin

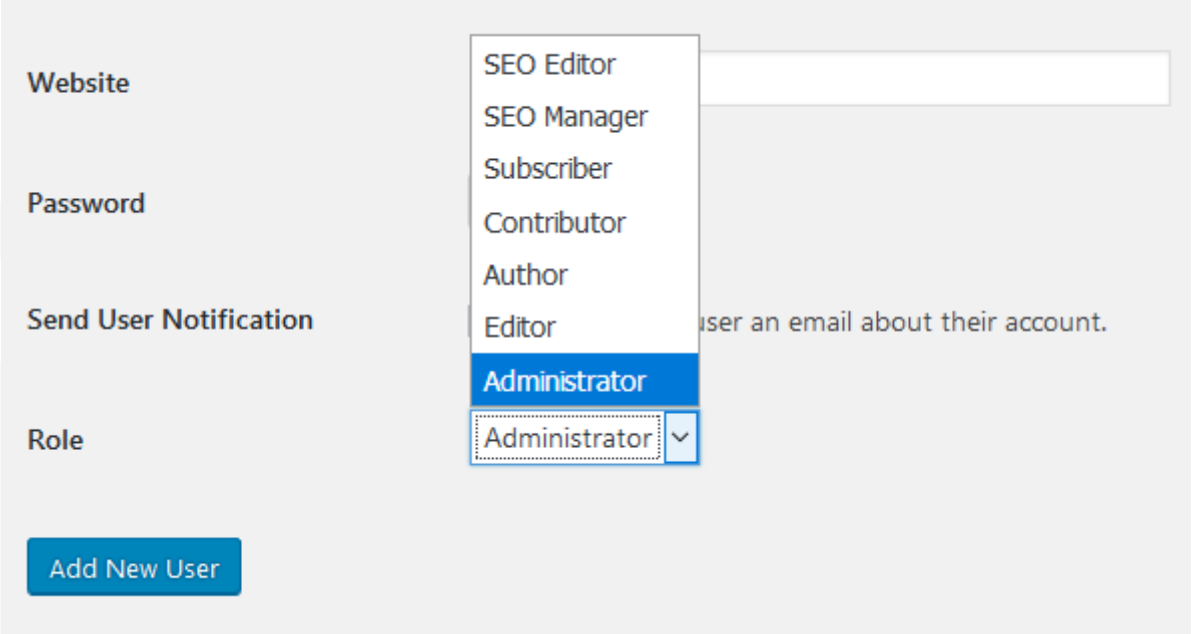
Tidak hanya login URL yang perlu Anda ganti, tetapi juga username admin WordPress. Secara default, username admin WordPress adalah **admin**. Jika Anda masih menggunakan username itu, sebaiknya cepat-cepat diganti karena mudah ditebak.

Cara mengganti username default admin cukup mudah, yaitu melalui menu Users di dashboard WordPress. Anda hanya perlu membuat username baru, berikut langkah-langkahnya:

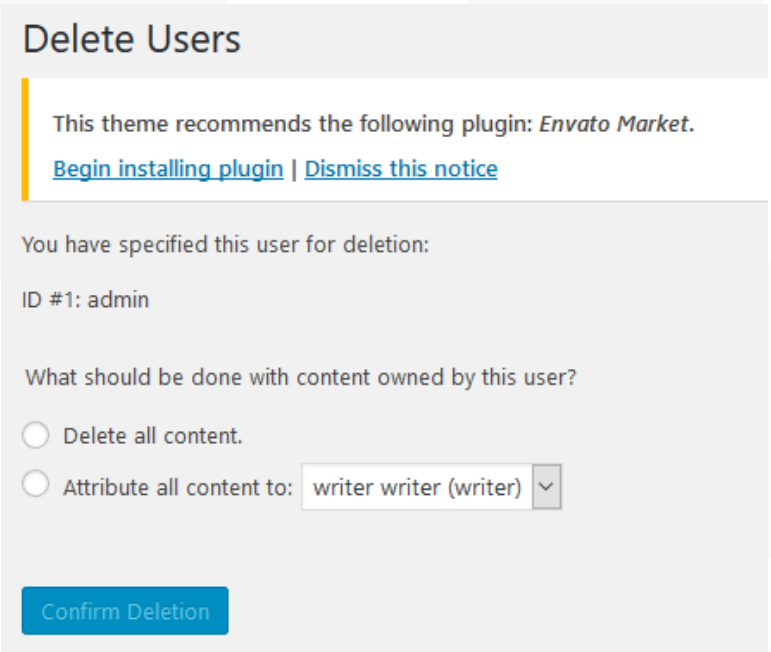
1. Buka dashboard WordPress lalu klik menu **Users > Add New**
2. Buat username yang unik, jangan gunakan **admin** seperti username default sebelumnya.

Catatan: Anda harus menggunakan alamat email yang berbeda dari username sebelumnya.

3. Berikan permission role yang sama dengan username default sebelumnya, yaitu **Administrator.** Kemudian klik **Add New User**



4. Setelah itu logout kemudian login kembali menggunakan username baru. Lalu buka menu **Users** dan hapus username default **admin**
5. Ketika menghapus user lama, pastikan untuk memindahkan semua konten di user lama ke user yang baru saja Anda buat. Pilih **Attribute all content to** [user baru]



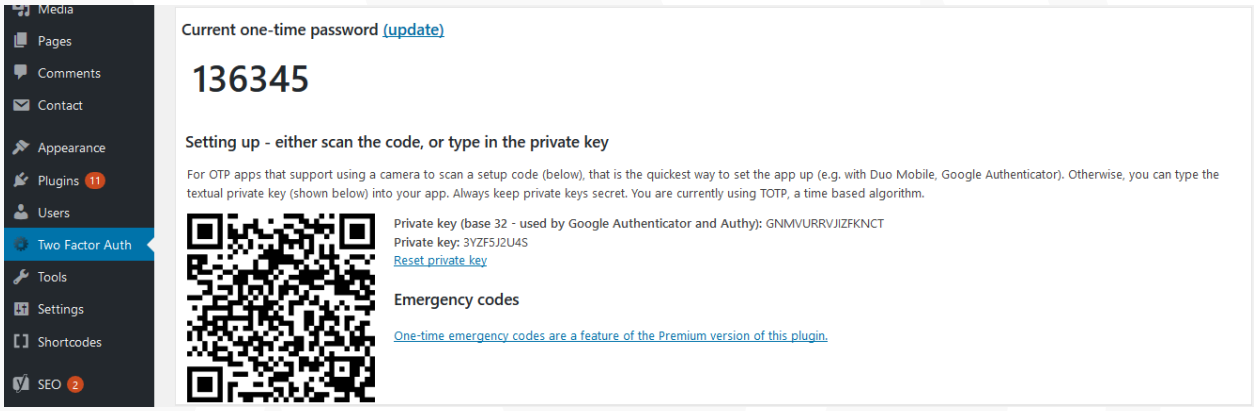
6. Selesai, Anda telah membuat user baru melalui dashboard WordPress

3. Gunakan 2-Factor Authentication

Fitur 2-Factor Authentication memungkinkan Anda untuk memberikan lapisan keamanan lebih di WordPress. Biasanya fitur ini membutuhkan verifikasi dari perangkat lain, baik itu melalui email atau nomor telepon untuk memastikan bahwa penggunanya memang asli.

Anda bisa menemukan fitur ini ketika mendaftar di Facebook, Google, Twitter, atau Instagram. Tidak hanya perusahaan besar saja yang bisa mengaplikasikan 2-Factor Authentication. Anda pun bisa menerapkannya di WordPress Anda.

Caranya cukup mudah, yaitu menggunakan plugin Two Factor Authentication. Setelah install dan mengaktifkan plugin tersebut, klik link 'Two Factor Auth' di sidebar dashboard WordPress.



Kemudian Anda perlu menginstall aplikasi authenticator di handphone Anda. Ada beberapa aplikasi yang bisa Anda gunakan seperti Google Authenticator, Authy, atau LastPass Authenticator.

Di tutorial ini kami menggunakan LastPass Authenticator. Buka aplikasinya di smartphone Anda lalu pilih **Add new account**. Setelah itu, LastPass Authenticator akan memberikan dua pilihan untuk menambahkan akun baru. Anda bisa memilih menggunakan **Scan barcode** atau **Enter security key**. Pilih salah satu metode. Anda bisa mendapatkan barcode atau security code dari plugin yang sudah Anda install sebelumnya. Anda akan mendapatkan notifikasi bahwa aplikasi telah berhasil menambahkan pengamanan two

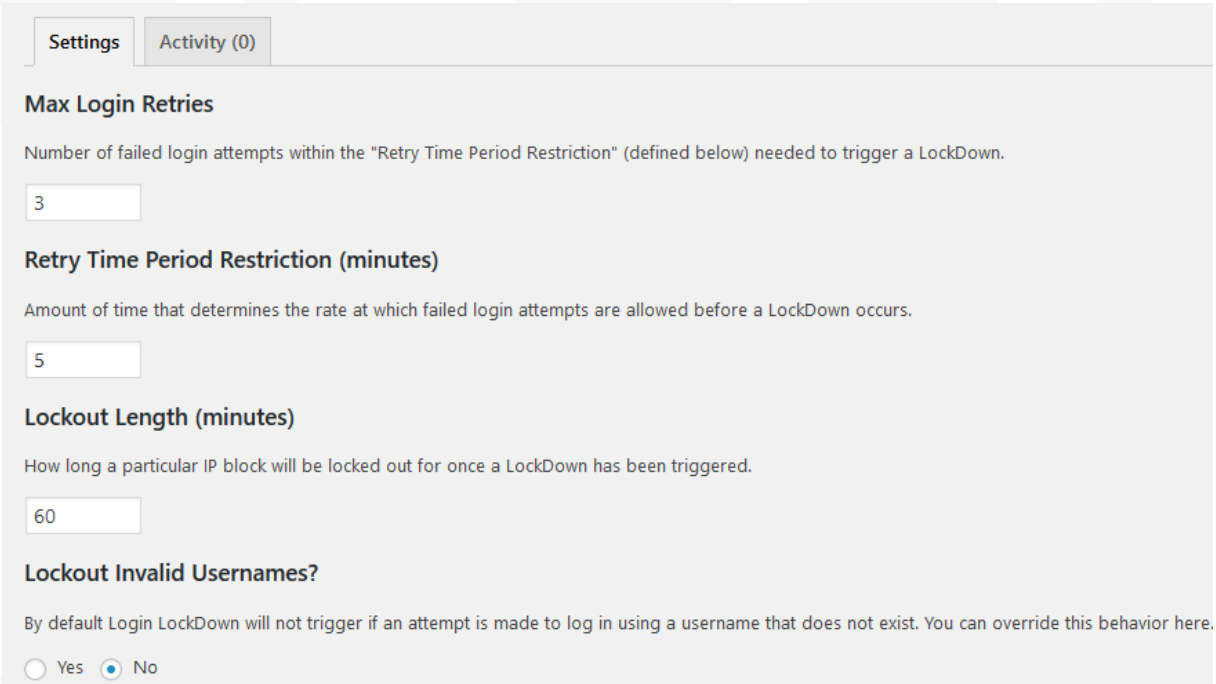
factor authentication untuk website Anda.
Setelah itu, ketika Anda login ke WordPress, Anda akan diminta untuk memasukkan One Time Password (OTP) yang dikirimkan ke aplikasi di smartphone Anda. Jadi halaman login WordPress Anda semakin aman!

4. Batasi Login Attempt

Secara default WordPress tidak membatasi berapa kali login yang bisa dilakukan oleh pengguna. Ini tentu berbahaya karena hacker bisa mencoba login ke admin WordPress Anda berkali-kali sampai menemukan password yang tepat.

Anda tidak mau hal itu terjadi, bukan?

Oleh karena itu, Anda perlu membatasi jumlah login yang bisa dilakukan pengguna. Caranya tidak sulit karena Anda bisa memanfaatkan plugin. Salah satu plugin yang dapat Anda gunakan adalah Login LockDown. Dengan Login LockDown, Anda bisa membatasi jumlah percobaan login yang dilakukan user.
Anda cukup memasang plugin tersebut melalui dashboard WordPress. Setelah melakukan aktivasi, buka menu **Setting > Login LockDown** dan Anda akan melihat pengaturan seperti di bawah ini:



Pertama, Anda perlu menentukan jumlah percobaan login yang bisa dilakukan pengguna. Anda bebas mengatur jumlahnya sesuai kebutuhan Anda. Kedua, tentukan juga rentang waktu yang dibutuhkan pengguna untuk mencoba login lagi setelah mencapai jumlah maksimum percobaan login. Ketiga, Anda juga bisa memblokir sementara alamat IP yang sudah melewati batas gagal login.

5. Aktifkan Logout Otomatis

Risiko keamanan bisa terjadi kapan saja, bahkan ketika Anda sudah berhasil login ke dashboard WordPress. Jika pengguna sudah login ke dashboard WordPress dan tidak melakukan aktivitas apa pun, orang lain bisa membajaknya dengan mengganti password atau pengaturan WordPress.

Jadi lebih baik untuk menerapkan logout otomatis jika pengguna tidak melakukan aktivitas di dashboard WordPress dalam kurun waktu tertentu. Caranya cukup mudah, Anda hanya perlu menginstall plugin Inactive Logout.

Setelah berhasil memasang dan mengaktivasi plugin tersebut, buka menu **Setting > Inactive Logout** untuk melakukan konfigurasi.

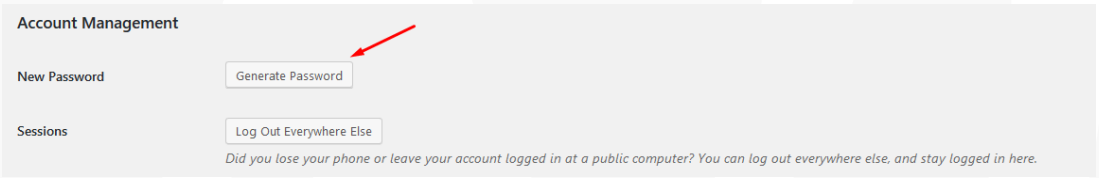
Anda bisa menentukan waktu timeout sesuai dengan kebutuhan Anda. Untuk notifikasi Anda bisa membiarkannya seperti di atas atau Anda juga bisa menggantinya dengan pesan yang Anda buat sendiri.

6. Buat Password yang Rumit

Password adalah komponen penting dalam keamanan WordPress. Membuat password yang sederhana sangat tidak disarankan, terutama untuk website. Ada banyak data dan file penting di website Anda. Jadi jangan pernah membuat password yang terlalu sederhana dan mudah ditebak.

Sekali hacker mendapatkan password admin WordPress Anda, benteng keamanan website Anda sudah roboh. Hacker bisa merusak website Anda dan mengubah pengaturan WordPress Anda.

Solusinya tentu saja adalah membuat password yang rumit. Jika Anda bingung bagaimana membuat password yang rumit dan tidak mudah ditebak, tidak perlu khawatir. Anda bisa memanfaatkan fitur Generate Password dari WordPress.
Untuk menggunakan fitur Generate Password, buka dashboard WordPress. Kemudian buka menu **User** dan pilih user yang ingin Anda ganti passwordnya. Lalu klik Generate Password di bawah kolom **Account Management** seperti di bawah ini:



Setelah itu WordPress akan membuatkan password yang terdiri dari kombinasi angka, huruf, dan tanda hubung. Kombinasinya cukup rumit sehingga akan sulit ditebak oleh siapa pun. Jadi area admin WordPress Anda akan lebih aman.

Jika khawatir tidak bisa mengingat kombinasi password yang sulit, Anda bisa menggunakan aplikasi seperti LastPass untuk menyimpan password Anda. LastPass membantu Anda menyimpan password dengan aman dan Anda bisa menggunakannya secara gratis!

Menjaga Keamanan Instalasi WordPress

7. Nonaktifkan Laporan Error PHP WordPress

Laporan error PHP tentu akan sangat berguna ketika memang ada error terjadi di WordPress sehingga Anda bisa dengan cepat memperbaikinya. Namun, laporan error PHP ini sebaiknya tidak bisa dilihat oleh orang lain.

Jika laporan tersebut bisa dilihat oleh publik, hacker bisa melihat celah error di WordPress Anda. Apalagi laporan error PHP juga sering menampilkan username WordPress Anda. Tentu hal ini sangat berbahaya bagi keamanan WordPress Anda.
Jadi sebaiknya Anda menonaktifkan laporan error PHP. Cara menonaktifkannya pun tidak sulit. Anda hanya perlu menambahkan beberapa baris kode pada file wp-config.php. Untuk mengakses file wp-config.php, Anda memerlukan FTP client seperti Filezilla.

Setelah mengakses file wp-config.php menggunakan FTP client, Anda perlu menambahkan baris kode di bawah ini:

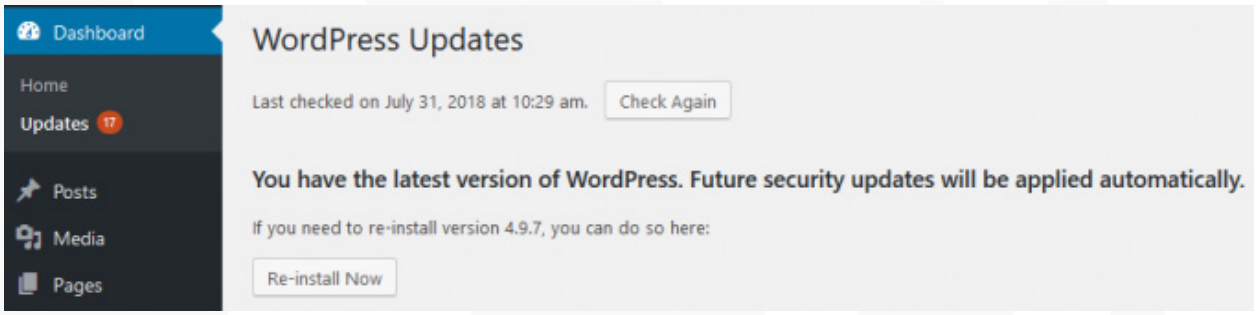
```
ini_set('log_errors','On');
ini_set('display_errors','Off');
ini_set('error_reporting', E_ALL );
define('WP_DEBUG', false);
define('WP_DEBUG_LOG', true);
define('WP_DEBUG_DISPLAY', false);
```

Setelah berhasil menambahkan kode-kode di atas, laporan error PHP Anda sudah otomatis menjadi tidak aktif. Anda telah berhasil menutup satu celah keamanan WordPress!

8. Selalu Update WordPress ke Versi Terbaru

Mungkin ini terlihat sepele. Namun, melakukan update WordPress memiliki dampak yang cukup signifikan terhadap keamanan website Anda. Dengan menggunakan WordPress versi terbaru, Anda sudah membangun pondasi keamanan website yang baik.

Penggunaan WordPress versi terbaru ini sangat penting karena WordPress secara rutin merilis update, baik itu update minor maupun major. Setiap versi terbaru WordPress hadir dengan perbaikan dari versi sebelumnya. Selain itu, Anda juga bisa menggunakan fitur-fitur terbaru bila menggunakan versi WordPress teranyar.
WordPress sendiri selalu mengingatkan penggunanya untuk melakukan update ke versi terbaru. Anda mungkin pernah melihat notifikasi update WordPress di dashboard seperti di bawah ini:



Jika Anda mendapatkan notifikasi seperti di atas, sebaiknya langsung lakukan update segera. Namun, jangan lupa untuk backup data dan file penting terlebih dahulu ya!

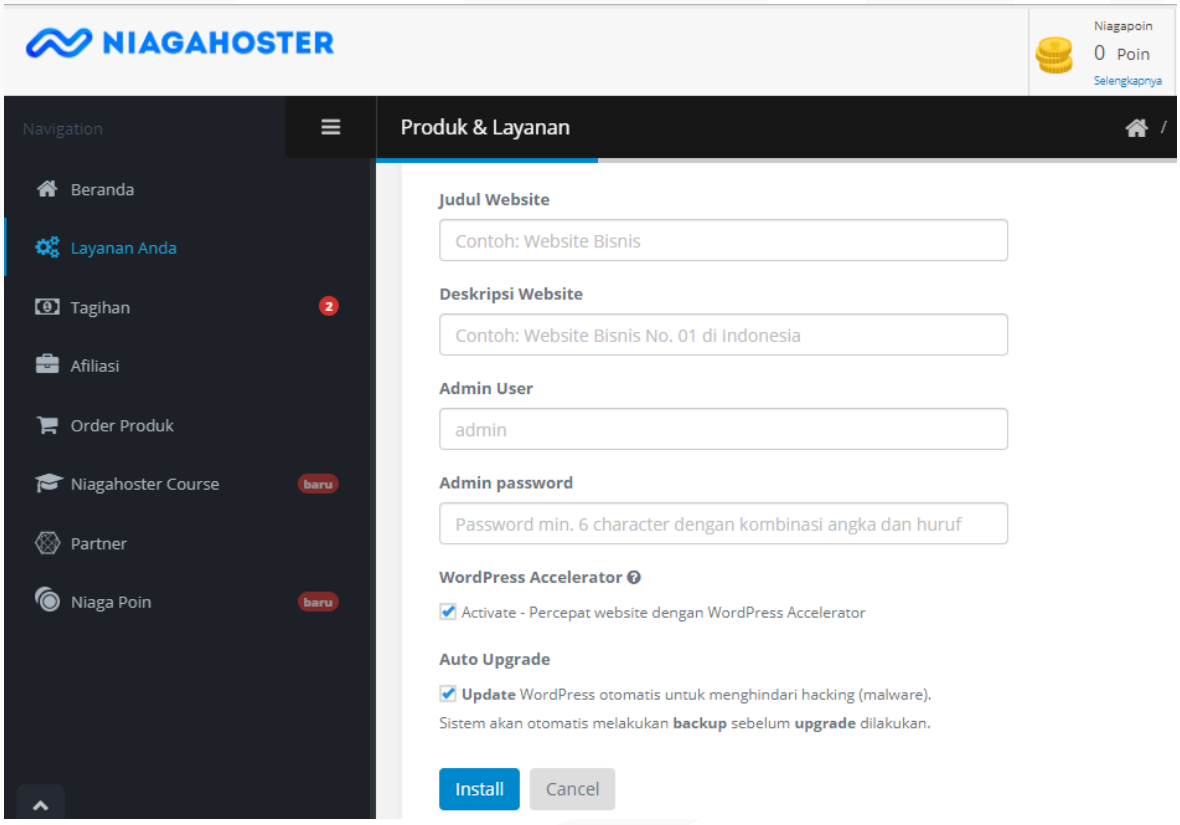
Jika Anda melewatkan notifikasi di atas, masih ada alternatif lain untuk melakukan update WordPress. Alternatif pertama adalah dengan menggunakan plugin. Anda bisa memanfaatkan plugin seperti Easy Update Manager. Plugin ini memungkinkan Anda untuk melakukan update WordPress secara otomatis.

Jika tidak ingin menginstall plugin tambahan dan tetap ingin melakukan update WordPress secara otomatis, Anda bisa menambahkan kode di bawah ini ke file wp-config.php.

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

Selain dua cara di atas, masih ada satu cara lagi untuk mengupdate WordPress, yaitu secara manual. Cara ini biasanya digunakan ketika cara update WordPress otomatis error. Untuk mengupdate WordPress secara manual, Anda perlu mengunduh versi terbaru WordPress di situs resminya dan mengunggahnya menggunakan FTP client. Penjelasan lengkapnya dapat Anda baca di artikel Cara Update WordPress Manual dan Otomatis. Oiya, mengingat betapa pentingnya update WordPress, Niagahoster sendiri menyediakan fitur auto update WordPress.

> *Jika Anda tidak ingin repot-repot menggunakan plugin atau cara update manual, Anda bisa memanfaatkan fitur auto update dari Niagahoster. Anda bisa mengaktifkan plugin ini ketika melakukan order hosting baru atau install WordPress di member area Niagahoster.*



9. Sembunyikan Informasi Server dan PHP

Informasi penting seperti server dan PHP yang Anda gunakan harus disembunyikan. Hacker bisa memanfaatkan dua informasi tersebut untuk menemukan celah keamanan di WordPress Anda.

Untuk menyembunyikan informasi server, Anda bisa menambahkan kode di bawah ini ke file .htaccess di direktori root WordPress Anda:

```
ServerSignature Off
```

Sedangkan untuk menyembunyikan informasi PHP, terdapat dua cara. Cara pertama adalah dengan menambahkan kode di bawah ini ke file .htaccess:

```
Header unset X-Powered-By
```

Cara kedua adalah menambahkan kode di bawah ini ke php.ini:

```
ini_set( 'dispexpose_php = Offlay_errors', 0 );
```

10. Sembunyikan Informasi Versi WordPress

Informasi versi WordPress yang Anda gunakan bisa dimanfaatkan para hacker untuk menemukan celah keamanan di website Anda. Oleh karena itu, sebaiknya informasi ini disembunyikan dari publik.

Terdapat dua cara untuk menghapus informasi versi WordPress yang Anda gunakan. Cara pertama adalah dengan menambahkan kode di bawah ini pada file functions.php tema yang Anda gunakan:

```
/*
Hide scripts and style version
*/
function SG_remove_wp_version_strings( $src ) {
global $wp_version;
parse_str(parse_url($src, PHP_URL_QUERY), $query);
 if ( !empty($query['ver']) && $query['ver'] === $wp_
version ) {
$src = remove_query_arg('ver', $src);
}
return $src;
}
add_filter( 'script_loader_src', 'SG_remove_wp_version_
strings' );
add_filter( 'style_loader_src', 'SG_remove_wp_version_
strings' );
/*
Hide generator tag from the header
*/
function SG_remove_wp_generator() {
return '';
}
add_filter('the_generator', 'SG_remove_wp_generator');
```

Cara kedua adalah dengan menambahkan baris kode di bawah ini ke file .htaccess di direktori root WordPress Anda:

```
#Block WP info
<files readme.html>
Order allow,deny
Deny from all
</Files>
<files license.txt>
Order allow,deny
Deny from all
</files>
```

11. Pasang SSL/TLS

SSL atau Secure Socket Layer adalah protokol yang mengenkripsi transfer data antara website dan browser pengunjung. Enkripsi ini melindungi data-data pengunjung website dari pencurian

Lalu apa itu TLS?

TLS adalah kependekan dari Transport Layer Security. TLS merupakan pengembangan lanjut dari SSL. Kini teknologi SSL sudah tidak lagi digunakan dan sepenuhnya digantikan oleh TLS. Namun, karena kebanyakan orang lebih familiar dengan SSL, istilah ini masih digunakan bersamaan dengan TLS. Fungsi keduanya pun sama. Hanya saja TLS memiliki teknologi yang lebih canggih dibanding SSL.

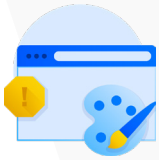
Bagaimana cara mengetahui apakah SSL/TLS website Anda sudah aktif atau belum? Caranya cukup mudah, jika website Anda masih menggunakan protokol **HTTP** di URL, artinya SSL/TLS Anda belum aktif. Website yang SSL/TLS-nya sudah aktif dapat dilihat dari protokol yang digunakan, yaitu **HTTPS**.

SSL/TLS memiliki pengaruh besar terhadap reputasi keamanan sebuah website. Bahkan sejak 2014, Google lebih mengutamakan website yang sudah menggunakan SSL/TLS dibanding yang tidak.

Selain itu, sejak Juli 2018 Google Chrome mulai menandai website tanpa SSL sebagai **not secure**. Google menerapkan aturan tersebut untuk memberikan pengalaman browsing yang lebih aman bagi penggunanya. Ini tentu menjadi peringatan bagi para pemilik website untuk segera menambahkan SSL/TLS di websitenya.

Bagaimana cara mendapatkan SSL/TLS di website Anda?

Caranya cukup mudah, bahkan Anda bisa mendapatkan SSL/TLS secara gratis! Cukup beli hosting di Niagahoster dan Anda bisa mendapatkan SSL gratis selamanya. Setelah membeli hosting paket apa saja di Niagahoster, Anda bisa mengaktifkan SSL/TLS dengan mengikuti langkah-langkah di panduan ini.



12. Hindari Penggunaan Tema dan Plugin Bajakan

Mendapatkan fitur-fitur premium tanpa perlu membayar sepeser pun memang terlihat menggiurkan. Anda bisa saja dengan mudah mendapatkan tema atau plugin bajakan di internet.

Anda mungkin tidak perlu mengeluarkan biaya sama sekali ketika menggunakan tema atau plugin bajakan. Namun, sebenarnya Anda membayar produk bajakan tersebut dengan keamanan website Anda.

Pembuat tema dan plugin bajakan bisa menyebarkan kode-kode berbahaya ke dalam file berbeda untuk menyamarkan diri sehingga sulit dideteksi dan diperbaiki ketika website Anda terserang hack.

Akibatnya Anda bisa kehilangan data-data penting website. Selain itu, yang lebih parah lagi website Anda bisa dihapus dari index Google yang menyebabkan website Anda tidak bisa muncul di hasil pencarian.

Tentu Anda tidak ingin hal itu terjadi, bukan?

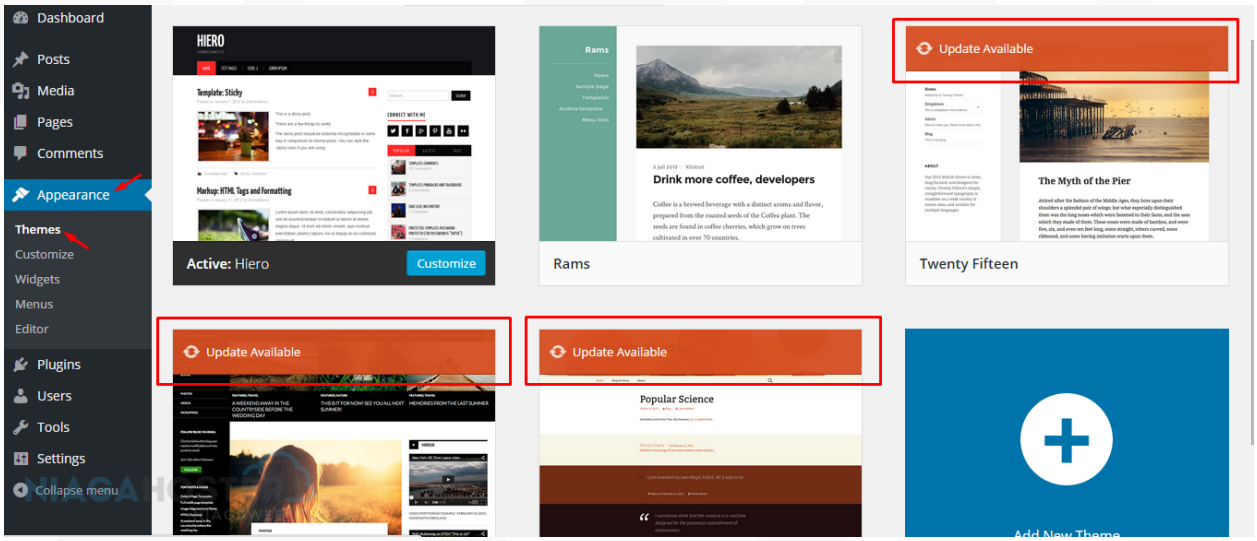
Jangan pernah gadaikan keamanan website Anda hanya untuk tema dan plugin bajakan. Selain berpotensi mengancam keamanan website, Anda juga tidak mengapresiasi pengembang dari tema dan plugin aslinya. Jadi sebaiknya selalu hindari tema dan plugin bajakan ya!

13. Selalu Update Tema dan Plugin yang Anda Gunakan

Menggunakan plugin dan tema resmi saja belum cukup. Anda juga perlu melakukan update tema dan plugin secara rutin. Pengembang selalu memperbaiki bug pada plugin dan tema versi terbaru yang mereka buat. Ini dilakukan untuk menutup celah-celah yang bisa dimasuki oleh hacker.

Jadi pastikan untuk mengupdate plugin dan tema yang Anda gunakan. Agar tidak lupa mengupdate plugin ke versi terbaru, Anda bisa memanfaatkan bantuan plugin seperti Easy Update Managers.

Sayangnya, belum ada plugin yang memungkinkan Anda untuk mengupdate tema WordPress secara otomatis. Anda perlu mengupdatenya secara manual melalui **Dashboard > Appearance > Theme**. Kemudian pilih tema yang akan Anda update. Biasanya akan ada notifikasi seperti di bawah ini ketika tema perlu diupdate:



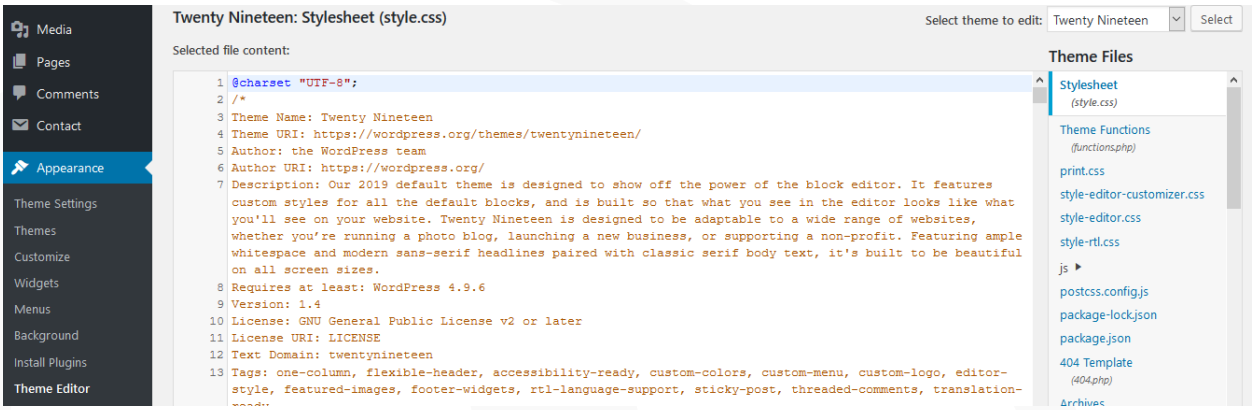
14. Hapus Tema dan Plugin yang Tidak Digunakan

Saat awal menginstall WordPress tentu Anda mencoba banyak plugin dan tema mana yang cocok untuk website Anda. Setelah menentukan satu tema dan beberapa plugin, mungkin Anda lupa untuk menghapus tema-tema dan plugin-plugin yang tidak digunakan.

Kabar buruknya, plugin dan tema yang tidak digunakan bisa menjadi celah hacker untuk menyerang keamanan website Anda. Bagaimana bisa? Hacker bisa melakukan scanning terhadap plugin atau tema yang lama tidak diupdate lalu bisa membuka akses ke admin dashboard WordPress Anda.

Oleh karena itu, untuk menghindari hal-hal yang tidak diinginkan, sebaiknya hapus plugin dan tema yang sudah tidak Anda gunakan. Toh, Anda juga sudah tidak menggunakannya, kan? Jadi selain bisa mengurangi risiko keamanan, Anda juga bisa menghemat space di WordPress Anda.

15. Disable File Editing



WordPress memungkinkan Anda untuk mengedit file tema dan plugin secara langsung melalui fitur code editor. Walaupun berguna, fitur ini juga bisa membahayakan keamanan WordPress Anda.
Jika hacker berhasil masuk ke dashboard WordPress Anda, mereka dapat mengotak-atik file tema atau plugin Anda. Alhasil website Anda bisa menjadi berantakan karena ulah hacker yang merusak file tema atau plugin Anda.

Jadi sebaiknya Anda menonaktifkan izin file editing di WordPress. Caranya cukup mudah. Anda hanya perlu menambahkan baris kode di bawah ini ke file wp-config.php:

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

16. Gunakan .htaccess

Fungsi .htaccess yang umum diketahui adalah untuk memastikan link-link di WordPress agar bekerja dengan benar. Padahal fungsi .htaccess tidak hanya itu. Fungsi lain dari .htaccess adalah untuk meningkatkan keamanan WordPress Anda.

Berikut adalah tiga cara meningkatkan keamanan WordPress menggunakan .htaccess:

1. Menghalangi akses ke halaman administrator

Anda bisa membatasi akses halaman administrator dari alamat IP tertentu menggunakan .htaccess. Anda cukup menambahkan kode di bawah ini ke file XXX:

```
AuthUserFile /dev/null
AuthGroupFile /dev/null
AuthName “WordPress Admin Access Control”
AuthType Basic
<LIMIT GET>
order deny,allow
deny from all
allow from xx.xx.xx.xxx
allow from xx.xx.xx.xxx
</LIMIT>
```

Isi xx.xx.xx.xxx dengan alamat IP yang ingin Anda perbolehkan untuk mengakses halaman admin WordPress. Tidak ada batasan jumlah alamat IP yang bisa Anda tambahkan. Jadi Anda bisa menambahkan alamat IP sebanyak-banyaknya.

Catatan: Metode ini tidak direkomendasikan untuk alamat IP dinamis

2. Menonaktifkan eksekusi PHP di folder tertentu

Hacker sering memanfaatkan fitur upload folder di WordPress untuk mengunggah backdoor scripts. Padahal fitur upload folder seharusnya hanya untuk mengunggah file media. Anda bisa menutup celah ini dengan menonaktifkan eksekusi PHP di folder tertentu.

Caranya adalah dengan menambahkan file .htaccess baru di direktori **/wp-content/uploads** menggunakan baris kode di bawah ini:

```
<Files *.php>
deny from all
</Files>
```

3. Melindungi file wp-config

Di dalam file wp-config terdapat pengaturan inti WordPress dan detail database MySQL. Artinya wp-config adalah file yang sangat penting untuk WordPress Anda. Para hacker seringkali menjadikan file tersebut sebagai target peretasan. Jadi Anda perlu melindungi file tersebut secara ekstra.

Anda bisa melindungi file wp-config dengan menggunakan baris kode .htaccess di bawah ini:

```
<files wp-config.php>
order allow,deny
deny from all
</files>
```

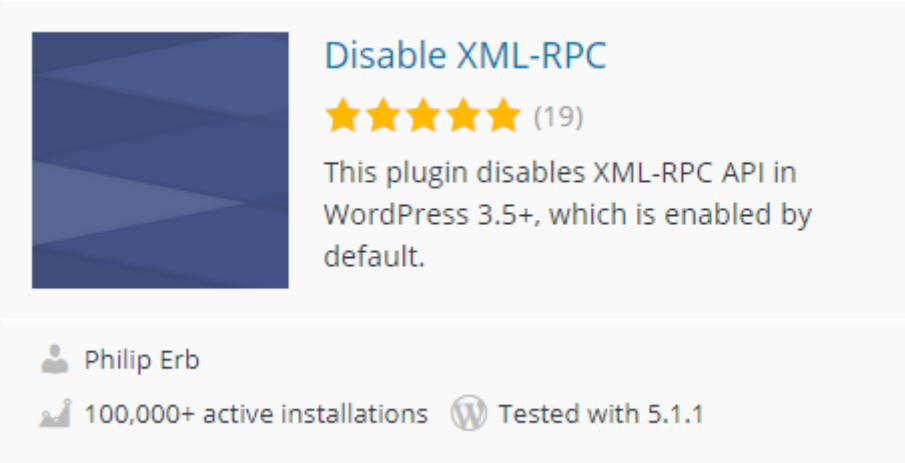
17. Nonaktifkan Fungsi XML-RPC

XML-RPC adalah fitur dari WordPress yang memungkinkan penggunanya untuk mengakses dashboard WordPress secara remote. Dengan XML-RPC, pengguna bisa menerbitkan postingan di WordPress melalui email dengan menjalankan trackback dan pingback.

Meskipun terlihat berguna, sayangnya fitur tersebut juga membuka risiko keamanan untuk WordPress Anda. Risiko keamanan pertama adalah fitur ini dapat dimanfaatkan hacker untuk menjalankan serangan brute force attack ke WordPress Anda. Selain itu, hacker juga bisa lebih mudah mengirimkan serangan DDoS melalui pingback yang dijalankan oleh XML-RPC.

Oleh karena itu, sebaiknya Anda menonaktifkan fitur XML-RPC. Terdapat dua cara untuk menonaktifkannya. Cara pertama adalah menggunakan plugin. Ada beberapa plugin yang bisa Anda gunakan.

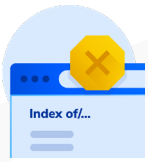
Plugin pertama yang bisa Anda gunakan adalah Disable XML-RPC



Cukup aktifkan plugin di atas dan fitur XML-RPC di WordPress Anda akan otomatis menjadi tidak aktif. Namun, perlu Anda pahami juga bahwa dengan menonaktifkan XML-RPC bisa mempengaruhi kinerja beberapa plugin. Sebab ada beberapa plugin yang kinerjanya berkaitan dengan XML-RPC.
Jika hanya ingin menonaktifkan beberapa elemen XML-RPC, Anda bisa menggunakan plugin Stop XML-RPC Attack atau Control XML-RPC Publishing.

Selain menggunakan plugin, Anda juga bisa menonaktifkan XML-RPC secara manual. Caranya cukup mudah. Anda hanya perlu menyalin kode di bawah ini dan memasukkannya ke file .htaccess Anda:

```
# Block WordPress xmlrpc.php requests
<Files xmlrpc.php>
order deny,allow
deny from all
allow from 123.123.123.123
</Files>
```



18. Disable Directory Browsing

Directory browsing adalah halaman index yang menampilkan informasi penting mengenai plugin, tema, atau bahkan server yang Anda gunakan. Halaman index ini biasanya muncul ketika server tidak bisa menemukan index file seperti index.php atau index.html.

Walaupun terlihat sepele, hacker dapat memanfaatkan informasi penting di directory browsing untuk menemukan celah masuk ke dashboard WordPress Anda. Oleh karena itu, Anda perlu menonaktifkan fitur ini untuk memperkecil celah keamanan WordPress Anda.

Berikut adalah langkah-langkah untuk menonaktifkan directory browsing:

1. Buka file .htaccess di root directory website. Anda perlu menggunakan FTP client seperti FileZilla untuk melakukan langkah ini.
2. Download file .htaccess
3. Buka file tersebut menggunakan text editor. Anda bisa menggunakan Notepad
4. Tambahkan kode `Options -Indexes` di bagian paling bawah file .htaccess
5. Simpan perubahan tersebut
6. Upload file yang sudah diedit menggunakan FTP client

19. Gunakan CDN

Content Delivery Network atau CDN punya banyak manfaat untuk website, salah satunya adalah untuk meningkatkan kualitas keamanan website. Apa saja manfaat CDN untuk keamanan website Anda? Berikut tiga manfaatnya:

- CDN mengaktifkan firewall yang berguna untuk melindungi website dari serangan-serangan online
- CDN mencegah terjadinya brute force attack dan memblokir serangan berbahaya seperti DoS atau DDoS
- CDN juga menyembunyikan alamat IP asli server Anda sehingga mencegah terjadinya serangan langsung ke alamat IP asli server yang Anda gunakan.

Ada banyak perusahaan yang menyediakan layanan CDN, baik gratis maupun berbayar. Jika Anda ingin CDN gratis dengan kualitas yang mumpuni, Cloudflare bisa menjadi pilihan. Beberapa penyedia hosting sudah mengintegrasikan Cloudflare di layanan hostingnya, termasuk Niagahoster.

Jika Anda menggunakan layanan hosting Niagahoster, Anda bisa dengan mengaktifkan Cloudflare dengan mudah melalui cPanel. Untuk cara lengkap bagaimana mengaktifkan Cloudflare dan konfigurasinya, dapat Anda baca di panduan ini.

20. Lakukan Backup Secara Rutin

Tentu tidak ada yang pernah berharap websitenya diretas. Walaupun begitu, setiap pemilik website harus selalu siap jika kemungkinan terburuk terjadi. Sebab siapa pun bisa terkena serangan berbahaya di internet. Baik website pemerintah, website perusahaan besar, maupun website personal sama-sama bisa terkena serangan online.
Oleh karena itu, Anda harus punya backup semua data website. Jadi jika website Anda terkena serangan malware atau diretas, Anda tidak bisa mengembalikan website kembali seperti semula dengan cepat.

Jika Anda menggunakan Niagahoster, semua data website Anda akan di-backup secara rutin setiap minggu. Walaupun begitu, Anda juga tetap perlu melakukan backup secara mandiri. Dengan begitu Anda punya cadangan backup.

Niagahoster sendiri menyediakan fitur Jetbackup yang memudahkan Anda untuk melakukan backup mandiri. Jetbackup mendukung lebih banyak fitur dibanding backup cPanel biasa. Berikut adalah beberapa kelebihannya:

JETBACKUP	VS	cPanel Backup
✔	• Backup seluruh file website	✔
✔	• Self Restore dari Cpanel Client	✘
✔	• Single file restore dari server backup	✘
✔	• Download file dari server backup incremental backups	✘
✔	• Cloudlinux support (put the backup process inside LVE)	✘

Cara penggunaannya pun cukup mudah, Anda hanya perlu mengikuti panduan ini untuk melakukan backup menggunakan Jetbackup. Anda bisa melakukan backup mandiri sesuai kebutuhan Anda.

Saking pentingnya backup, mengandalkan backup dari layanan hosting dan backup mandiri saja belum cukup. Sebagai langkah antisipasi, Anda juga bisa memasang plugin backup untuk menjalankan backup otomatis. Salah satu plugin backup otomatis yang bisa Anda manfaatkan adalah UpdraftPlus.

21. Ganti Prefix Database WordPress

Database WordPress berisi semua informasi dan data penting website sehingga seringkali menjadi target serangan para hacker. Secara default, WordPress menggunakan **wp_** sebagai prefix untuk semua tabel di database WordPress Anda.

Penggunaan prefix default ini tentu cukup berbahaya karena mudah diketahui oleh para hacker. Oleh karena itu, Anda perlu menggantinya. Namun, sebelum memulai penggantian prefix database WordPress, pastikan Anda sudah membuat backup-nya terlebih dahulu.

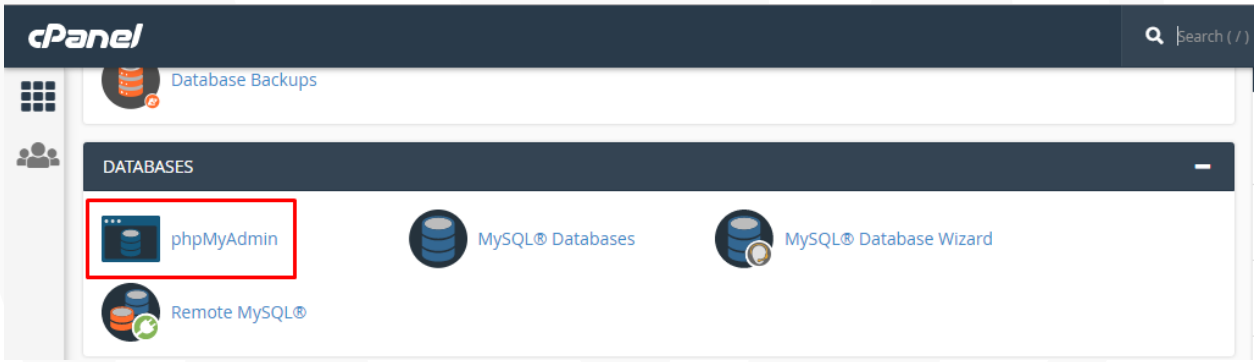
Jika sudah selesai melakukan backup, Anda bisa mulai proses penggantian prefix dengan mengikuti langkah-langkah di bawah ini:

1. Buka file **wp-config.php** yang terletak di root directory WordPress Anda
2. Ubah kode **wp_** menjadi kode lain seperti **wp_a123456_**. Hasilnya akan menjadi seperti di bawah ini:

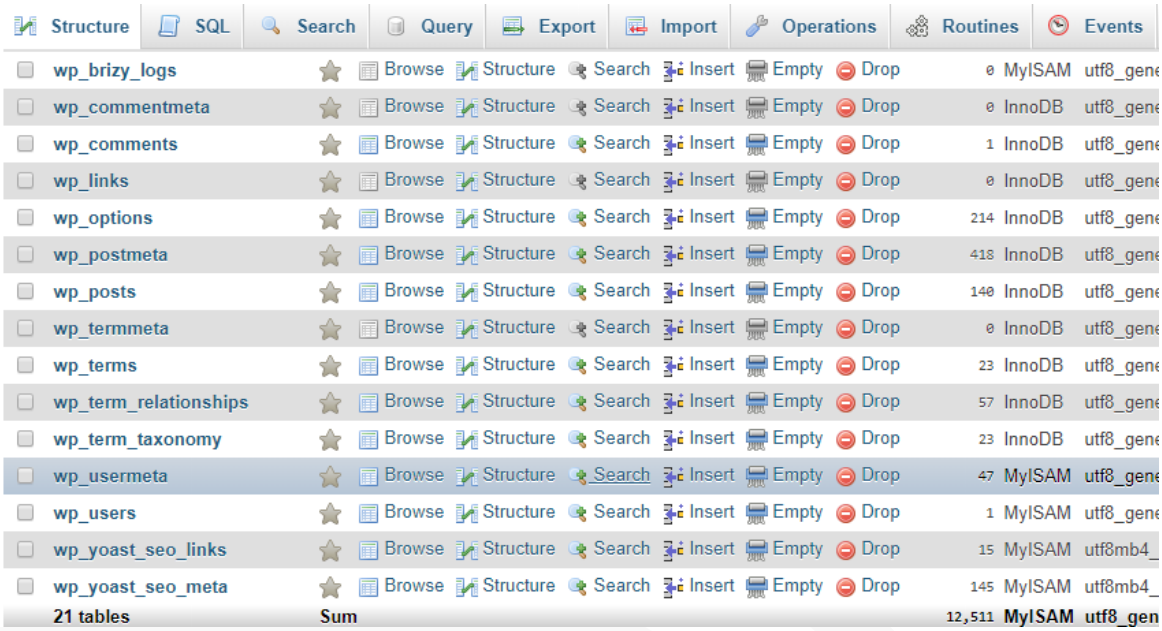
```
$table_prefix  = 'wp_a123456_';
```

> *Catatan: Anda hanya diperbolehkan menggunakan angka, huruf, dan underscore*

3. Setelah itu, buka phpMyAdmin. Anda bisa mengaksesnya melalui cPanel Anda



4. Kemudian buka database WordPress Anda



Structure	SQL	Search	Query	Export	Import	Operations	Routines	Events
wp_brizy_logs	Browse	Structure	Search	Insert	Empty	Drop	0	MyISAM	utf8_gene
wp_commentmeta	Browse	Structure	Search	Insert	Empty	Drop	0	InnoDB	utf8_gene
wp_comments	Browse	Structure	Search	Insert	Empty	Drop	1	InnoDB	utf8_gene
wp_links	Browse	Structure	Search	Insert	Empty	Drop	0	InnoDB	utf8_gene
wp_options	Browse	Structure	Search	Insert	Empty	Drop	214	InnoDB	utf8_gene
wp_postmeta	Browse	Structure	Search	Insert	Empty	Drop	418	InnoDB	utf8_gene
wp_posts	Browse	Structure	Search	Insert	Empty	Drop	140	InnoDB	utf8_gene
wp_termmeta	Browse	Structure	Search	Insert	Empty	Drop	0	InnoDB	utf8_gene
wp_terms	Browse	Structure	Search	Insert	Empty	Drop	23	InnoDB	utf8_gene
wp_term_relationships	Browse	Structure	Search	Insert	Empty	Drop	57	InnoDB	utf8_gene
wp_term_taxonomy	Browse	Structure	Search	Insert	Empty	Drop	23	InnoDB	utf8_gene
wp_usermeta	Browse	Structure	Search	Insert	Empty	Drop	47	MyISAM	utf8_gene
wp_users	Browse	Structure	Search	Insert	Empty	Drop	1	MyISAM	utf8_gene
wp_yoast_seo_links	Browse	Structure	Search	Insert	Empty	Drop	15	MyISAM	utf8mb4_
wp_yoast_seo_meta	Browse	Structure	Search	Insert	Empty	Drop	145	MyISAM	utf8mb4_
21 tables	Sum						12,511	MyISAM	utf8_gen

5. Pada gambar di atas, tampak 21 nama tabel yang perlu diubah. Tentu mengubah nama tabel satu per satu cukup merepotkan. Tidak perlu khawatir, Anda bisa memanfaatkan fitur SQL dan menggunakan template di bawah ini

```
RENAME table `wp_brizy_logs` TO `wp_a123456_brizy_
logs`;
RENAME table `wp_commentmeta` TO `wp_a123456_comment-
meta`;
RENAME table `wp_comments` TO `wp_a123456_comments`;
RENAME table `wp_links` TO `wp_a123456_links`;
RENAME table `wp_options` TO `wp_a123456_options`;
RENAME table `wp_postmeta` TO `wp_a123456_postmeta`;
RENAME table `wp_posts` TO `wp_a123456_posts`;
RENAME table `wp_termmeta` TO `wp_a123456_termmeta`;
RENAME table `wp_terms` TO `wp_a123456_terms`;
RENAME table `wp_term_relationships` TO `wp_a123456_
term_relationships`;
RENAME table `wp_term_taxonomy` TO `wp_a123456_term_
taxonomy`;
RENAME table `wp_usermeta` TO `wp_a123456_usermeta`;
RENAME table `wp_users` TO `wp_a123456_users`;
```

Catatan: Template di atas hanyalah contoh. Anda perlu menyesuaikannya dengan database WordPress Anda sendiri dan prefix database yang sudah Anda buat di awal.

Bonus Tips Keamanan

22. Install Plugin Keamanan

Memasang plugin keamanan adalah sebuah kewajiban bagi semua pemilik WordPress. Plugin keamanan WordPress membantu mengamankan website Anda dari serangan-serangan online. Ada banyak plugin keamanan WordPress dengan fitur berbeda-beda. Ada yang gratis, ada juga yang berbayar.

Kini tersedia banyak plugin keamanan yang tersedia secara cuma-cuma. Salah satu plugin keamanan gratis yang 100% gratis adalah All In One WP Security and Firewall. Plugin ini dikembangkan secara open source sehingga bisa dinikmati banyak orang secara gratis.

Selain plugin di atas, masih ada banyak plugin keamanan lain yang tidak kalah hebat. Beberapa di antaranya adalah Jetpack, Wordfence, dan Sucuri. Ketiga plugin tersebut menyediakan dua versi, yaitu gratis dan berbayar. Jika hanya membutuhkan fitur-fitur dasar keamanan, Anda bisa menggunakan versi gratisnya. Namun, jangan ragu untuk membeli versi berbayarnya kalau Anda memang membutuhkannya! Anggap saja sebagai investasi untuk website Anda.

23. Scan WordPress untuk Mendeteksi Malware

Beberapa plugin keamanan WordPress menyediakan fitur scan malware di WordPress secara rutin. Jetpack, Wordfence, dan Sucuri sama-sama menyediakan fitur scan malware di fitur gratisnya.

Selain memanfaatkan fitur bawaan dari plugin di atas, terkadang Anda juga perlu melakukan scan malware secara manual untuk memastikan kalau WordPress Anda benar-benar aman.

Anda bisa melakukan scan malware secara manual melalui situs-situs pendeteksi malware di bawah ini:

- Security Check & Malware Scanner Sucuri
- IsItWP Security Scanner
- Google Safe Browsing
- WPSec
- UpGuard

24. Aktifkan Firewall

Salah satu langkah pengamanan dasar WordPress adalah dengan mengaktifkan firewall website. Firewall website membantu untuk memblokir trafik berbahaya bahkan sebelum trafik tersebut mencapai website Anda. Selain itu, firewall juga berfungsi untuk melindungi data dari hacker dan pengguna yang tidak punya wewenang.

Maka dari itu, Anda perlu mengaktifkan firewall untuk meningkatkan kualitas keamanan WordPress Anda. Anda bisa mengaktifkan firewall dengan mudah menggunakan bantuan plugin.

Terdapat banyak plugin yang menawarkan fitur ini. Beberapa di antaranya sudah disebutkan di poin sebelumnya, yaitu Sucuri dan Wordfence. Selain dua plugin tersebut, masih tersedia alternatif lain seperti Cloudflare, SiteLock, dan BulletProof Security.

25. Pilih Layanan Hosting Terpercaya

Langkah terakhir dan terpenting adalah memilih layanan hosting terpercaya. Anda tidak bisa memilih hosting asal-asalan karena semua data website Anda akan tersimpan di server hosting tersebut.

Jadi pastikan untuk memilih hosting yang sudah terbukti kualitasnya, terutama pada fitur-fitur keamanan yang ditawarkan. Niagahoster sebagai salah satu penyedia layanan hosting terbesar Indonesia selalu menjadikan keamanan hostingnya sebagai prioritas utama.

Semua website yang Anda hosting di Niagahoster akan dilindungi dengan teknologi keamanan terbaik, yaitu Imunify360. Imunify360 adalah solusi keamanan website terkini yang mampu melindungi website secara sempurna.

Berikut adalah enam fitur utama Imunify360 yang akan melindungi website Anda:

- **Advanced Firewall**

Dengan teknologi *artificial intelligence* (AI) dan imunitas terpadu, firewall canggih Imunify360 mampu mendeteksi ancaman keamanan dan melindungi website Anda secara menyeluruh.

- **Intrusion Detection and Protection System**

Selain mengatasi serangan berbahaya di website, Imunify360 juga mampu mendeteksi potensi-potensi serangan. Imunify360 secara otomatis akan memblokir alamat IP yang terindikasi melakukan aktivitas mencurigakan di website Anda.

- **Malware Detection**

Malware merupakan serangan keamanan yang umum terjadi. Imunify360 melakukan scanning pada semua file di website sehingga potensi serangan malware bisa terdeteksi lebih dini. File-file yang terinfeksi akan dikarantinakan sehingga kerugian bisa terhindari.

- **Proactive Defense**

Proactive Defense mampu menghentikan malware yang bahkan tidak bisa dideteksi oleh scanner sekalipun! Fitur ini akan mengidentifikasi ancaman keamanan di website Anda secara real time dan memblokir potensi-potensi ancaman secara otomatis dalam waktu singkat.

- **Patch Management**

Mengupdate kernel server terbaru adalah kewajiban untuk menjaga kinerja server. Patch Management memungkinkan kernel server Anda tetap terupdate tanpa perlu melakukan reboot dan tidak mengganggu kinerja server sama sekali.

- **Reputation Management**

Reputasi website Anda sangatlah penting. Fitur Reputation Management Imunify360 membantu Anda menjaga reputasi website dengan memberitahu Anda jika website Anda masuk ke dalam blacklist Google atau SBL. Jadi Anda bisa mengatasi masalah tersebut lebih cepat.