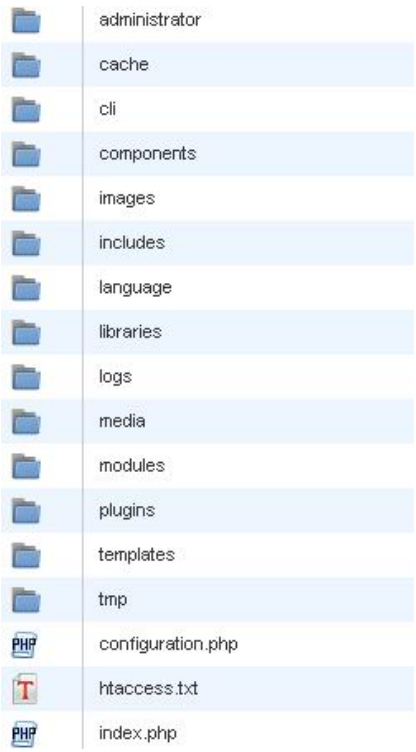
BENARKAH WEBSITE CMS MUDAH DI-HACK?

Untuk melengkapi pengetahuan Anda tentang securitas website, sebaiknya Anda juga membaca buku *Jurus Sakti Amankan Website WordPress*, karena di dalam buku tersebut banyak referensi yang dapat memberikan pemahaman tentang pentingnya securitas website.

Sebuah CMS yang dibuat untuk kebutuhan masyarakat luas, seperti Joomla atau WordPress atau software CMS lainnya, memiliki keunggulan dalam kecepatan dan kemudahan dalam melakukan pembuatan website. Namun, di sisi lain juga memberikan sederet kelemahan. Salah satunya adalah penggunakan sistem folder dan penamaan file yang terstandardisasi, artinya seseorang yang menggunakan Joomla di bilangan Canada maka isi folder dan file website sama dengan seseorang yang menggunakan Joomla di bilangan Asia.

Begitu ada seseorang yang berhasil melakukan pembobolan pada sebuah website berbasis Joomla, orang tersebut dapat melakukan pembobolan dengan cara yang serupa untuk website Joomla lainnya dengan memanfaatkan sistem yang terstandardisasi di dalam CMS tersebut.



Gambar 1.1 Struktur Folder dan File CMS Joomla yang Terstandardisasi

Banyak pemilik website yang tidak menyadari bahwa sebenarnya setiap website memiliki potensi untuk dibobol oleh para orang-orang tak bertanggung jawab. Banyak juga yang tidak terlalu memikirkan tentang keamanan website dan menyangka websitenya aman karena tidak mengandung suatu informasi yang berkaitan dengan keuangan atau informasi pengguna atau informasi berharga lainnya.

Banyak hacker yang melakukan pembobolan ke sebuah website bukan untuk mencuri informasi yang ada di dalam website tersebut, melainkan melakukan pembobolan untuk membobol server di mana website tersebut berada, dengan harapan dapat mencuri informasi dari website lainnya yang berada di dalam satu server tersebut.

Tak aneh jika sebuah server berhasil dibobol, maka banyak website yang ada di dalam server tersebut ikut dibobol juga. Untuk itu sangat penting bagi pemilik website, meski website yang dimiliki tidak mengandung suatu informasi tentang data keuangan, semisal nomor kartu kredit atau data paypal dan lain sebagainya. Tetap harus menaruh perhatian yang serius terhadap keamanan website. Berikut ini beberapa penyebab kenapa sebuah website dapat dibobol dengan mudah.

1.1 Kecerobohan Pemilik Website

Yang paling sering dialami oleh pemilik website berbasis CMS adalah serangan Deface. Deface adalah teknik hacker yang paling tradisional, di mana seorang hacker berhasil melakukan penerobosan ke sebuah website. Dan kemudian mengganti file index website tersebut dengan file index yang dimiliki oleh si hacker, dengan tujuan mengubah tampilan website menjadi seperti yang hacker inginkan.

Gambar 1.2 Sebuah website yang berhasil di-deface oleh R3d ErRor

Biasanya berisikan pesan bahwa website tersebut telah berhasil dibobol oleh hacker tersebut. Si hacker sendiri tidak melakukan perusakan apa-apa bahkan juga tidak menghapus file index asli website, melainkan melakukan rename terhadap file website tersebut.

Dalam kasus yang lebih terselubung lagi, ada seorang hacker yang hanya meninggalkan sebuah file dalam bentuk .txt (yang dibuat dengan notepad) yang berisikan pesan bahwa dia telah berhasil membobol situs. Tentu bagi pemilik yang jarang melihat isi file websitenya tidak mengetahui kalau ternyata diam-diam situsnya sudah berhasil di-hack.

Atau, ada juga yang menempatkan file-file tertentu di dalam hosting dan memanggil file-file tersebut untuk ditampilkan di sebuah website. Dan hal ini akan sangat merugikan pemilik website yang terkena hack karena bandwidth hosting dipergunakan oleh website orang lain.

Tak jarang juga seorang hacker yang berhasil membobol sebuah website, menggunakan hosting website tersebut untuk menyimpan data-data ilegal untuk kebutuhan tertentu, semisal untuk software judi atau malware judi. Tentunya pemilik website tidak curiga karena websitenya berjalan normal, terkecuali jumlah pemakaian bandwidth yang meningkat, meski jika dilihat dari statistik jumlah kunjungan ke website biasa-biasa saja.

Jika Anda mendapati jumlah bandwidth hosting yang meningkat secara signifikan, sementara jumlah kunjungan ke website normal-normal saja, sebaiknya periksa semua file-file website Anda, dan lihat apakah ada folder-folder mencurigakan yang bukan menjadi milik website Anda.

Banyak pemilik website yang mengeluhkan dan kemudian tak sedikit yang menyalahkan sofwatre CMS yang digunakan karena didapati websitenya terkena serangan hacker. “Ah, website-ku dibobol terus

karena aku pake CMS Joomla sih, Joomla murahan sih!" Padahal tidak juga, bisa jadi penyebabnya sebagai berikut.

1.1.1 Tidak Menggunakan Antivirus & Anti Spyware

Banyak faktor yang menyebabkan sebuah website dapat di-hack. Salah satu sebab yang tidak pernah diduga adalah adanya virus atau malware yang menyusup ke dalam komputer sehingga memberikan back door bagi hacker untuk dapat mencuri user dan password FTP. Dan selanjutnya hacker itu menggunakan user dan FTP itu dan digunakan untuk melakukan hacking.

Gambar 1.3 Pentingnya penggunaan antivirus dan anti Spyware di dalam PC

Ada semacam malware yang membidik software FTP dengan tujuan mencuri account untuk login ke dalam hosting yang tersimpan di dalam FTP. Dan setelah mendapatkan user dan password tersebut, pemilik software tersebut menggunakannya untuk login dan melakukan apa saja yang dikehendaki olehnya terhadap website.

Ada juga aplikasi keylogger yang biasanya disisipkan di dalam sebuah software yang dibagikan secara gratis. Untuk itu penting Anda menggunakan antivirus dan anti spyware untuk melindungi komputer dari malware atau aplikasi berbahaya seperti keylogger.

Keylogger adalah sebuah aplikasi yang mampu merekam aktivitas keyboard. Setiap kata yang diketikkan di keyboard dapat terekam dan aplikasi tersebut mengirimkan laporan ke pemiliknya. Sehingga pemilik dapat mengetahui user dan password dari data-data yang terekam.

Pastikan bahwa komputer yang Anda gunakan sudah bebas dari segala macam virus, malware, dan juga spyware. Selalu gunakan anti virus dan anti spyware yang selalu di-update, gunakan update otomatis yang ada pada Anti Virus dan Anti Spyware tersebut.

Jangan menggunakan antivirus bajakan yang banyak dijual di penjual software bajakan, karena tidak akan berguna. Lebih baik gunakan versi gratisan dari Antivirus tersebut daripada menggunakan versi bajakan yang sudah di-crack, yang melumpuhkan kemampuan antivirus tersebut untuk melindungi komputer.

1.1.2 Menggunakan Sembarangan Extension

Salah satu asyiknya menggunakan CMS adalah adanya extension yang dapat diinstal dengan cepat untuk menambahkan suatu fitur tertentu ke dalam website. Namun sayangnya, tidak semua extension itu aman. Banyak extension yang dibuat dengan terburu-buru sehingga menyisakan banyak hole di sana-sini, yang mempermudah seorang hacker untuk melakukan pembobolan.

Salah satu cara mencari jalan masuk untuk pembobolan, seorang hacker akan mencari celah dari sistem pihak ketiga, yaitu dari extension. Khusus

untuk CMS Joomla, ada sebuah tim yang bertugas menguji extension-extension yang terdapat di dalam directory website Joomla.

Bagi pengguna Joomla, wajib mengecek website http://docs.joomla.org/Vulnerable_Extensions_List yang berisikan extension-extension yang bisa menjadi sebab bagi masuknya aksi hacker untuk membobol sebuah website. Lakukan cross check terlebih dahulu sebelum menginstal sebuah extension.

Gambar 1.4 Daftar extension yang mudah direntas - http://docs.joomla.org/Vulnerable_Extensions_List

Selain itu, lihat juga jumlah review sebelum Anda menggunakan sebuah extension. Jika banyak yang me-review maka extension tersebut baik, dan dapat Anda gunakan pada website Anda. Contohnya extension Community Builder yang difavoritkan, banyak diberi rating dan juga banyak dikomentari oleh penggunanya.

Silakan luangkan waktu Anda untuk membaca komentar atau review yang berkaitan dengan extension yang ingin Anda gunakan demi keamanan dan kenyamanan website Anda.

Gambar 1.5 Ada 218 Review untuk Extension Community Builder

1.1.3 Menggunakan Extension atau Theme Nulled

Kebiasaan orang menggunakan sesuatu yang gratis atau membayar murah juga membuka celah untuk membuat pertahanan CMS dapat dijebol. Salah satunya dengan membeli theme nulled atau extension atau plugin nulled.

Gambar 1.6 Jangan menggunakan extension dan theme nulled

Maksudnya nulled di sini adalah sistem validasi license dari provider theme atau extension, atau plugin sudah dimatikan menggunakan script tertentu. Penggunaan script tersebut bisa membuat celah, atau yang disebut dengan hole.

Celah atau hole tersebut kemudian digunakan oleh hacker untuk menyusupi website. Penggunaan theme atau extension atau plugin asli dari provider akan lebih baik meski tentunya lebih mahal, tetapi Anda menggunakan produk asli bukan bajakan.

Selain penggunaan theme nulled, penggunaan theme gratisan juga bisa berpengaruh terhadap kerentanan website karena bisa jadi dibuat secara terburu-buru. Meski tidak semua theme gratisan itu jelek, tidak. Namun berhati-hatilah sebelum menggunakan sesuatu yang gratisan. Selalu cari referensi dan komentar yang sudah pernah menggunakannya.

1.2 Penggunaan Hosting

Bagi website, hosting adalah sebuah rumah bagi file-file website. Sebuah rumah yang dilengkapi dengan sistem pengamanan yang terpadu akan membuat penghuninya dapat tidur dengan nyaman tanpa harus risau dibobol oleh maling.

Seperti itu juga dengan hosting. Agar Anda dapat tidur dengan nyenyak, pastikan provider hosting Anda dapat diandalkan. Setidaknya dapat diajak untuk bekerja sama jika terjadi sesuatu terhadap website. Banyak provider hosting yang lempar tangan, alias tak mau bertanggung jawab memberikan bantuan ketika website berhasil di-hack. Penyelenggara hosting tersebut akan dengan entengnya menyalahkan sistem CMS yang digunakan, padahal tidak juga.

Gambar 1.7 Pilihlah penyelenggara hosting yang berkualitas dan dapat diajak kerja sama

Faktor hosting memberikan peranan atas dibobolnya website. Provider hosting yang mengerti tentang hosting akan mengetahui asalnya serangan dan akan melakukan perbaikan, karena mereka tahu serangan tersebut akan berakibat fatal bagi klien mereka lainnya.

Jika Anda mendapati pernyataan dari provider hosting yang menyalahkan sistem CMS yang Anda gunakan ketika website terkena hacking, sebaiknya Anda pindah hosting ke tempat lain. Untuk panduan bagaimana pindah hosting dan mentransfer file-file dari hosting lama ke hosting baru, dapat dibaca panduannya pada buku *Bengkel Web & SEO Joomla*.

1.3 Penggunaan Strong Password Amat Penting Bagi Keamanan Awal

Satu celah yang paling sering dimanfaatkan oleh para hacker adalah penggunaan password yang mudah ditembus. Banyak pengguna yang

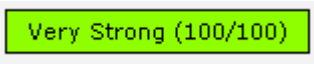
memasukkan tanggal, bulan, dan tahun lahirnya sebagai password, atau memasukkan kata-kata yang mudah diingat.

Pastikan kalau komputer yang Anda gunakan sudah bersih dari segala macam virus, malware dan spyware. Selanjutnya yang harus Anda lakukan adalah mengubah password cPanel Anda dengan Strong Password.

Penggunaan strong password sebagai langkah awal untuk mengamankan website Anda. Percuma juga meski situs web yang Anda miliki sudah dilengkapi dengan scripting (pemrograman) keamanan dan juga firewall, namun Anda menggunakan weak password (password lemah) maka website Anda akan dengan mudah dibobol. Oleh karenanya, gunakanlah strong password! untuk administrator website, FTP dan CMS.

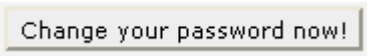
Anda tak perlu menghafal password-nya, catat password tersebut dan simpan di tempat aman. Berikut ini cara mengganti password pada hosting cPanel.

- Masuk ke dalam cPanel hosting Anda.
- Kemudian klik menu 

.
- Pada kolom **Old Password** masukkan password Anda yang sekarang (yang sedang digunakan untuk login).
- Pada kolom **New Password** isi dengan password Anda yang baru yang mengandung unsur strong password.
- Pada kolom **New Password (again)** ulangi password baru Anda.
- Pastikan pada kolom **Strength (why?)** indikator strength password terpenuhi, seperti gambar ini 

.

- Beri tanda centang pada 

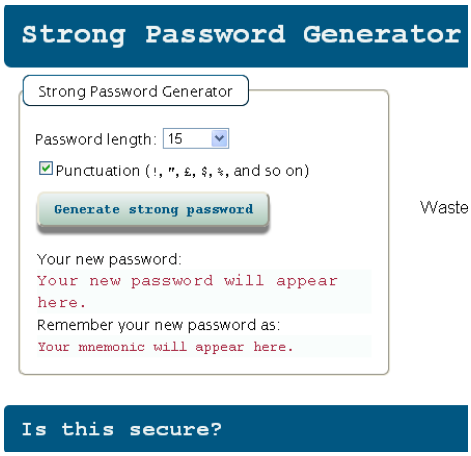
.
- Dan terakhir, tekan tombol 

.

Selalu pastikan bahwa Anda sudah menggunakan strong password. Pengertian Strong Password adalah password yang cukup panjang dan memiliki kombinasi antara huruf, angka, dan karakter unik.

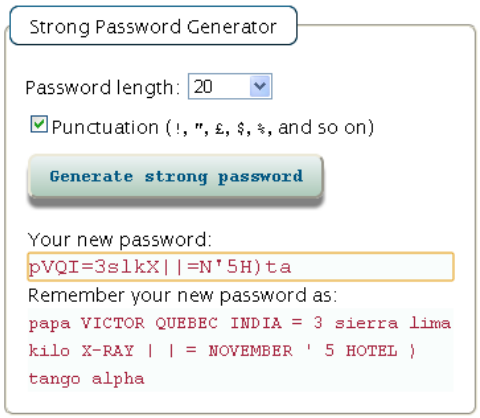
Menurut perhitungan, untuk menjebol password 12 karakter, membutuhkan waktu 17 tahun dengan mencoba-coba setiap kemungkinan karakter yang digunakan.

Untuk memudahkan Anda dalam membuat stong password, silakan membuat strong password dengan strong password generator melalui website http://strongpasswordgenerator.com.



Gambar 1.8 Strong password generator untuk membuat password yang kuat - http://strongpasswordgenerator.com/

Silakan buat sebuah password terlebih dahulu dengan mengisi Password length lebih di atas 15. Artinya, password Anda nantinya memiliki 15 karakter atau lebih, tergantung dari value yang Anda masukkan.



Gambar 1.9 Hasil pembuatan password dengan 20 karakter

Sekarang Anda sudah mengantongi sebuah password yang kuat, yaitu **pVQI=3slkX||=N'5H)ta**. Anda bisa menambahkan karakter atau huruf di dalam password tersebut. Semisal **pVQI=3slkX|c4@$|=N'5H)taZ**. Selanjutnya Anda akan tes kekuatan password tersebut dengan simulasi waktu yang dibutuhkan untuk membobol password tersebut dengan teknik Brute Force.

Brute Force adalah sebuah teknik serangan terhadap suatu sistem securitas, baik komputer atau aplikasi online. Dengan melakukan percobaan-percobaan melalui kombinasi semua kata kunci yang mungkin digunakan sebagai password.

Biasanya serangan brute force sudah tidak lagi dilakukan secara manual, melainkan oleh software berbentuk robot yang dikendalikan dari jauh. Software berbentuk robot ini berkeliaran dari satu server ke server lain, dan begitu mendapati sebuah website yang sesuai dengan kreteria yang dicari oleh pemilik sofware, software ini akan melakukan percobaan login terus-menerus dengan memasukkan kombinasi untuk membobol website. Dan sebuah password yang lemah akan dapat dibobol dalam hitungan menit.

Untuk mengetahui kekuatan password yang Anda gunakan, silakan masuk ke website https://www.grc.com/haystack.htm untuk mencari tahu berapa lama seorang hacker dapat membobol password Anda.

Gambar 1.10 Melakukan test simulasi kekuatan password - https://www.grc.com/haystack.htm

- Setelah masuk ke website https://www.grc.com/haystack.htm, kemudian pada bagian form simulasi, masukkan weak password.
- Sebagai contoh, saya memasukkan password yang biasa digunakan oleh umum (weak password), yaitu berupa kombinasi tanggal dan bulan lahir ditambahi beberapa karakter tertentu yang mudah diingat, contoh: 2201B6.

Gambar 1.11 Mencoba kekuatan password 6 karakter

Hasilnya sungguh mengejutkan. Untuk sebuah massive attack hanya dibutuhkan waktu sekitar kurang lebih 0.0000224 detik. Untuk serangan offline hanya dibutuhkan waktu 0.0224 detik. Sementara untuk serangan online standar dibutuhkan sekitar 3.70 minggu (kurang lebih 1 bulanan).

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	3.70 weeks
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	0.0224 seconds
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	0.0000224 seconds

Sekarang coba masukkan Strong Password yang sudah Anda buat sebelumnya dengan stong password generator ke dalam form simulasi, dan lihat hasilnya.

Gambar 1.12 Mencoba strong password

Hasilnya sungguh mengejutkan, dibutuhkan waktu yang sangat lama sehingga membuat hacker menjadi bosan dan melupakan upaya hacking terhadap penggunaan password Anda.

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	8.91 trillion trillion trillion centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	89.14 thousand trillion trillion centuries

Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	89.14 trillion trillion centuries

Bagaimana? Ternyata mudah bukan untuk membuat strong password itu. Jangan menjadi malas, dengan alasan susah untuk diingat. Buat catatan dan taruh di salah satu folder di komputer atau usb Anda. Anda bisa meng-copas Password tersebut setiap kali akan digunakan.