

Lima jurus hackers membobol Situs Joomla

Sabtu, 01 November 2008

Last Updated Selasa, 16 Desember 2008

Menjadi site administrator Joomla, banyak suka dan dukanya. Salah satunya adalah situs diusili oleh orang lain. Menangani situs joomla jumlahnya sudah seratusan, ternyata menyisakan pengalaman pahit. Ada rasa takut, kesal, sedih, kecewa campur aduk kayak semen. Apalagi kalau mengalami Joomla attack. Ada sekitar sepuluh situs yang diobrak-abrik. Lima tewas di-deface, 3 abis disusupi spam dan sisanya dikirim sampah bot-shell. Yang mengenaskan adalah di deface. Malu sama BOS,hiks :(.
{jumi[/banner/adscampkotak.html]}

Menjadi site administrator Joomla, banyak suka dan dukanya. Salah satunya adalah situs diusili oleh orang lain. Menangani situs joomla jumlahnya sudah seratusan, ternyata menyisakan pengalaman pahit. Ada rasa takut, kesal, sedih, kecewa campur aduk kayak semen. Apalagi kalau mengalami Joomla attack. Ada sekitar sepuluh situs yang diobrak-abrik. Lima tewas di-deface, 3 abis disusupi spam dan sisanya dikirim sampah bot-shell. Yang mengenaskan adalah di deface. Malu sama BOS,hiks :(.
{jumi[/banner/adscampkotak.html]}

Yang diserang adalah situs yang memiliki pagerank tertinggi dan open security. Semakin banyak backdoor yang terbuka, maka situs akan populer dibajak hacker. Sekali dibajak akan diworo-woro ke IRC room, untuk diperkosa rame-rame. Habislah sudah situs joomla merana? Kok bisa? Apa sih yang tak bisa di dunia ini? Semuanya saling berlawanan. Ada hitam ada putih. Ada baik ada Jahat. Ada FPI ada AKKBB. Ada Islam bener ada AHMADIYAH. Ada Islam benar ada JIL. Semuanya saling melengkapi.

Kembali ke topik. Kenapa situs Joomla dihack? Karena hacker tahu kelemahan situs Joomla. Bagaimana hackers menyerang situs Joomla? Inilah jawabannya. Para hacker menggunakan lima jurus (pertama) untuk menumbangkan situs Joomla.

Lima jurus ini merupakan hasil telusuran, diskusi dan pengalaman pribadi dalam mengelola situs admin. Jadi saya mengundang anda untuk memberikan komentar, kritik dan saran bila jurus yang paparkan ini adalah palsu. Para hackers Joomla dalam menyiapkan serangan ke situs berbasis Joomla akan beberapa strategi. Satu strategi awal dalam menyerang adalah menggunakan Lima jurus. Kelima jurus itu terdiri dari yaitu :

1. Versi Joomla yang digunakan
2. Hostingnya dimana? Jenis hostingnya seperti apa?
3. Jenis Plugin/Extensions yang diinstall
4. File dan folder permissions
5. Ranking situs
6. Jenis situs

Biar lebih mantap dan renyah dinikmati, saya akan membeberkan jurus-jurus mematikan ini pada anda. Mari mas..!

1. Versi Joomla yang digunakan

Semakin lama versi Joomla yang anda gunakan, anda maka semakin banyak lubang kelemahan (vulnerabilities) situs anda. Setiap detik laporan situs Joomla dihack banyak sekali. Laporan tentang hacking itu lalu dilaporkan dan langsung ditambal (patch). Pada Joomla yang sudah di-patch, maka akan muncul versi Joomla terbaru. Itu artinya Kode-skrip joomla anda harus di update. Anda cukup download bagian script yang akan ditambal. Cukup copy-paste, maka patching sudah selesai.

Tapiiiii. Tidak semua orang peduli pada isu ini. Malas dan bosan. Saya juga sudah pernah mengalami ini karena harus menangani situs Joomla yang terlalu banyak. Tapi kalo cuma satu doang mungkin gak masalah. Tapi kalau banyak, penyakit bosan dan CAPEK DEh melanda, maka updating ditinggalkan. Jangan diikuti sifat ini. Karena kalau sudah dibajak, maka anda akan kerja bakti selama seminggu untuk memulai dari awal lagi membangun situs. CEPEK, deh

2. Hostingnya dimana? Jenis hostingnya seperti apa?

Bila ada ISP hosting yang tidak aman, para hackers menyusup di tempat tersebut. Pada beberapa tempat hosting malah jadi sarang penyamun para hackers dalam mencuri data dan menghacking situs. Kerja mereka rapi. Mereka seperi sindikat dan mafia. Mereka sengaja menyediakan jasa hosting murah hanya untuk menjebak client. Hati-hati juga pada free hosting. Tak ada jaminan bahwa situs anda aman. Jadi berhati-hatilah.

Tapi saya pernah punya client yang hosting di tempat murah (an) namun manajemen sekuritinya amburadul. Untuk mencirikannya mudah saja. Pertama, biasanya situs ISP-nya tidak profesional. Harganya murah (an) banget. Secara

logis susah diterima dalam hitungan bisnis. Jadi ada yang dikorbankan. Supportnya kacau dan minim. Sakit hati dan kesal. Kalau ada kesalahan, client yang disalahkan. Site-adminnya kadang-kadang sok tau. Kalau mau detail silakan mampir ke webhostingtalk atau milis web hosting di yahoogroups.

Jadi berhati-hatilah dalam memilih hosting untuk situs Joomla anda. Kalau system keamanan dan support meragukan, cepat-cepatlah anda berpindah. Iklaskan uang anda, daripada anda kehilangan 100 kali lipat nantinya. Nanti akan saya bahas topik memilih hosting yang baik dan benar untuk situs Joomla. Semoga dapat sponsor

3. Jenis Plugin/Extensions yang diinstall

Lobang terbesar penyerangan situs Joomla ada di sini. Semakin banyak yang terinstall plugin/extensions disitus Joomla anda, semakin besar peluang serangan yang dilancarkan. Banyak programmer berhati jahat yang mengubah atau memalsu skrip plugin/extensions Joomla. Hal itu mudah mereka lakukan. Membuat skrip plugin/extensions Joomla bagi programmer merupakan makanan sehari-hari. Para programmer jahat ini juga sering menyusupkan skrip plugin/extensions ke forum joomla untuk didownload secara gratis. Jadi berhati-hatilah.

4. File dan folder permissions

Ini titik kelemahan yang mudah ditemukan dengan bantuan C99 shell atau php shell. Bila ditemukan banyak File dan folder permissions terbuka (666 atau 777) maka kiamat akan tiba. Perbaikilah CHMOD dengan JoomlaXplorer.

Yang default terbuka adalah folder media dan images. Karena memang terbuka untuk umum. Tapi kalau tidak perlu mohon ditutup saja. Karena ini adalah pintu utama menghacking situs anda. Kalau situs anda untuk perusahaan, korporat, yayasan, kelembagaan, lebih baik dimatikan saja fitur user registered berikut folder permissions-nya. Ubah semua CHMOD folder menjadi 644 (koreksi dari Rekan David, adalah 444, tapi saya mengubah menjadi 644. Thanks to david)

5. Ranking situs

Semakin tinggi sebuah pohon, maka semakin kencang angin yang meniupnya. Semakin tinggi ranking situs anda di google, yahoo dan alexa, maka semakin besar situs anda porak-poranda. Menggunakan google, situs anda akan ada diurutan pertama saat akan diserang. Karena situs anda sudah populer. Para hackers tidak punya belas kasih. Pokoknya, HAJAR BLEH.

Jadi dilema. Populer salah, gak populer juga salah. Saya mempunyai situs klien Joomla yang memiliki PR 5 dan alexa bagus. Di logs servernya bertaburan penyusup yang berniat jahat mengobrak-abrik server. heuhhhh, capek deh. That's way administrator site FOR.

sumber: http://webizsolution.do.am/blog/2008-10-05-1_{jumi}/adscamp.html