Aumente a segurança do seu Joomla!

Apesar do Joomla já ser um sistema relativamente seguro, e ter uma equipe competente que está sempre fazendo correções importantes a fim de aumentar ainda mais sua segurança, ele não é totalmente invulnerável.
Muitos administradores não adotam os devidos cuidados para manterem seus sites Joomla seguros, e acabam sofrendo ataques, ocasionando a perda de horas de trabalho ou até mesmo de dias.

Estes administradores devem sempre ter em mente que, na Internet, a segurança de um site deve estar sempre em constante evolução para os diversos desafios que se apresentam. Não existe um caminho certo e único para dar segurança a um site, sendo que todos os métodos de segurança estão sujeitos a melhorias e revisões, bem como devem estar sempre preparados contra uma possíevel violação.

Felizmente, existem alguns princípios que podem ajudar a evitar essas invasões. São pequenos pormenores extremamente fáceis de implementar e que aumentarão, consideravelmente, a segurança do seu site Joomla. Para isto reuni algumas informações que servirão de orientações para garantir a segurança de seu Joomla.

1 – Realizar backups regularmente.
Os backups dos arquivos e do banco de dados são a nossa última defesa contra a perda dos mesmos. Tais prdas podem acontecer por uma prática qualquer mal executa ou por um inimaginável desastre, devido a ataques hackers aseu site.
Esta tarefa pode ser feita por meio do Cpanel de qualquer conta do seu servidor, com a utilização do FTP Protocolo ou com a utilização de um componente especifico para esta tarefa de backup.

2 – Ficar de olho nas extensões vulneráveis

Não adianta você manter seu Joomla atualizado, se você tem várias extensões instaladas que não estão devidamente atualizadas. A utilização de uma única extensão insegura coloca em perigo todo o seu site.
Para evitar isto você deve tomar as seguintes precauções:

- Faça uma relação de todas as extensões que você utiliza e procure se informar de novas atualizações para elas;

- Procure saber se as extensões que estão sendo utilizadas são seguras e se não são vulneráveis a ataques que comprometam o seu site.

Para isto procure sempre estar bem informado sobre possíveis extensões vulneráveis e verifique se há atualizações corrijam estas vulnerabilidades. Caso não tenha atualização, desinstale esta extensão imediatamente para não comprometer seu site.

Existe uma lista de extensões vulneráveis, a qual está sendo constantemente atualizada, no site oficial do Joomla e no Fórum, as quais podem ser acessadas nos links abaixo:

Fórum contendo a lista de extensões vulneráveis

E lista de extensões vulneráveis dó site oficial do Joomla.

3 – Ter um nome de usuário e senha mais segura.

Não se dê ao trabalho de atualizar constantemente o Joomla, de seguir várias recomendações, para depois colocar tudo a perder com a utilização de uma senha não segura. Par que isto não aconteça, seguem abaixo algumas sugestões:

Senha: Para ter uma senha segura você deve ter letras maiúsculas, minúsculas, números e caracteres especiais. A senha não precisa ser muito extensa. Utilize por exemplo 3

letras maiúsculas, 3 números, 1 letra minúscula e 1 caractere especial. Exemplo: M82+EhY2

Nome de usuário: Sempre que o Joomla é instalado o nome de usuário por padrão é “admin”, e muitos não a modificam, bem como continuam a utilizá-la. Para dificultar a ação de invasores, altere o nome do usuário para alguma coisa mais difícil de adivinhar, você dificultará muito o acesso indevido à sua conta.

4 - Desligar os relatórios de erro

Um das opções que você pode utilizar também é desligar os relatórios de erros. Esses relatórios de erros além de diminuírem a velocidade do site, indicam também aos "hackers" as falhas na segurança do site Joomla.

Os relatórios de erros podem ser desativados no Joomla 1.5 na sua aba de administração, conforme se vê na figura abixo:

site -> Configuração Globais -> Servidor.

Relatório de erros selecionar nenhum.

Depois de desativada esta função, não será mais permitida a visualização dos erros gerados pelo Joomla, o que é uma coisa muito boa, uma vez que o utilizador comum não os vê (o que não era muito profissional) e os “hackers” não poderão forçar erros de forma a descobrirem métodos de comprometer o seu site.

5- Utilizar um componente SEF

De que forma os “hackers” decidem atacar o seu site? O método habitual é simples de explicar. Eles descobrem, por exemplo, que uma determinada versão de uma extensão está vulnerável, bem como a forma de explorar essa mesma vulnerabilidade. Depois

procuram no Google por meio do comando inurl, a assinatura dessa extensão. O resultado é uma lista de sites vulneráveis, e se o seu site estiver nessa lista, adivinhe o que vai acontecer ?

Utilize um componente SEF (Eearch Engine Friendly) de modo a reescrever a sua url. Assim, o seu site não aparecerá mais naquelas listas e você terá mais sucesso nas pesquisas que lhe interessam dado que o seu site ficará mais otimizado para o Google.

.**6- Mover arquivo configuration.php para fora da raiz**
Quando você carregou o seu site para o servidor, teve que efetuar o upload dos arquivos para uma determinada pasta. Nos servidores, estas pastas são chamas de **cpanel** ou pasta **public_html**. Nos servidores com Plesk, é a pasta **httpdocs**. Ora, essa pasta é aquela que está acessível a qualquer utilizador anônimo. Se você colocar um arquivo index.html nessa pasta, qualquer um vai conseguir acessar este arquivo. E qualquer outra pessoa com um browser vai também conseguir.

Essa pasta é a mais vulnerável em qualquer servidor. Portanto, é uma boa idéia mover os arquivos mais sensíveis para uma pasta menos vulnerável. É o caso do arquivo configuration.php.

Vamos fazer estas mudanças, para isto siga as instruções abaixo:

1 - Crie uma pasta no public_html ou httpdocs a qual poderemos chamá-la de **joomla** apenas como exemplo.

2 - Vamos mudar o nome do arquivo **configuration.php** para **joomladoc.php** e, a seguir, vamos movê-la para a pasta joomla a qual acabamos de criar.

3 - Crie um novo arquivo de configuração na raiz com o nome de **configuration.php** contendo o seguinte código:

```
<?php
require( dirname( __FILE__ ) .'/joomla/joomladoc.php' );
?>
```

Observação (Os nomes dados à pasta e ao arquivo é apenas para ilustrar este matéria, você deve dar um nome mais complicado para dificultar ainda mais a sua localização.)
Mude as permissões deste novo arquivo no caso confuguration.php para 444.
Se precisar mudar as configurações, faça-o manualmente no joomla.conf

6 - Mudar o Prefixo da base de dados

Por padrão, ao se instalar o Joomla, o prefixo da base de dados será **jos_.** A maioria dos arquivos “hackers” escritos para comprometer um site Joomla, tentam adquirir informações da tabela **jos_users**. E, desta maneira, podem adquirir a password (senha) e username (nome de usuário) do administrador do website. Mudar o nome do prefixo para algo aleatório ajudará a impedir a maioria dos ataques “hackers”.

O prefixo pode ser escolhido no momento da instalação de um site Joomla mudando o prefixo padrão de jos_ para um que lhe for mais conveniente.

Se você já instalou seu site Joomla e não atentou para a mudança deste prefixo, recomendo que faça esta mudança para aumentar a segurança do seu Joomla.

Para efetuar esta mudança estou disponibilizando o vídeo-tutorial onde é mostrado o passo-a-passo de como fazer a substituição do prefixo do banco de dados por outro.