Guia definitivo de permissão de arquivos e pastas do WordPress

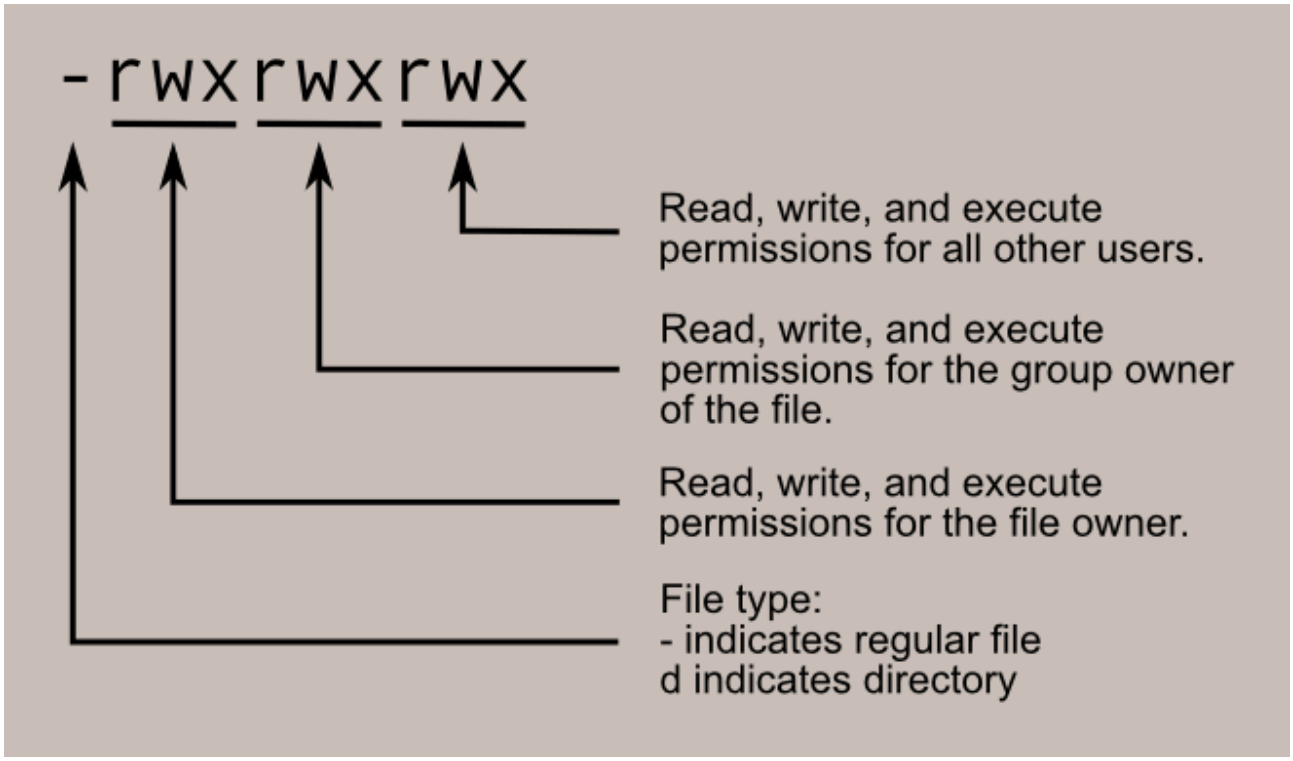
Para segurança da aplicação, as permissões devem ser definidas corretamente e assim definir quem e o que poderá ser lido, escrito, modificado e acessado.

Leandro Vieira 13 de julho de 2015

A correta permissão de arquivos e pastas do WordPress contribuem para uma maior segurança da aplicação, uma vez que as permissões são responsáveis por definir quem e o que poderá ser lido, escrito, modificado e acessado. O assunto é simples e pode ser complexo considerando as variáveis que o envolvem.

De forma básica, você deve compreender três variáveis sobre permissões de arquivos e diretórios:

1. Leitura – permite o acesso para a visualização do seu conteúdo;
2. Escrita – permite que o arquivo seja alterado;
3. Execução – permite a execução de programas e scripts contidos nos arquivos em questão.

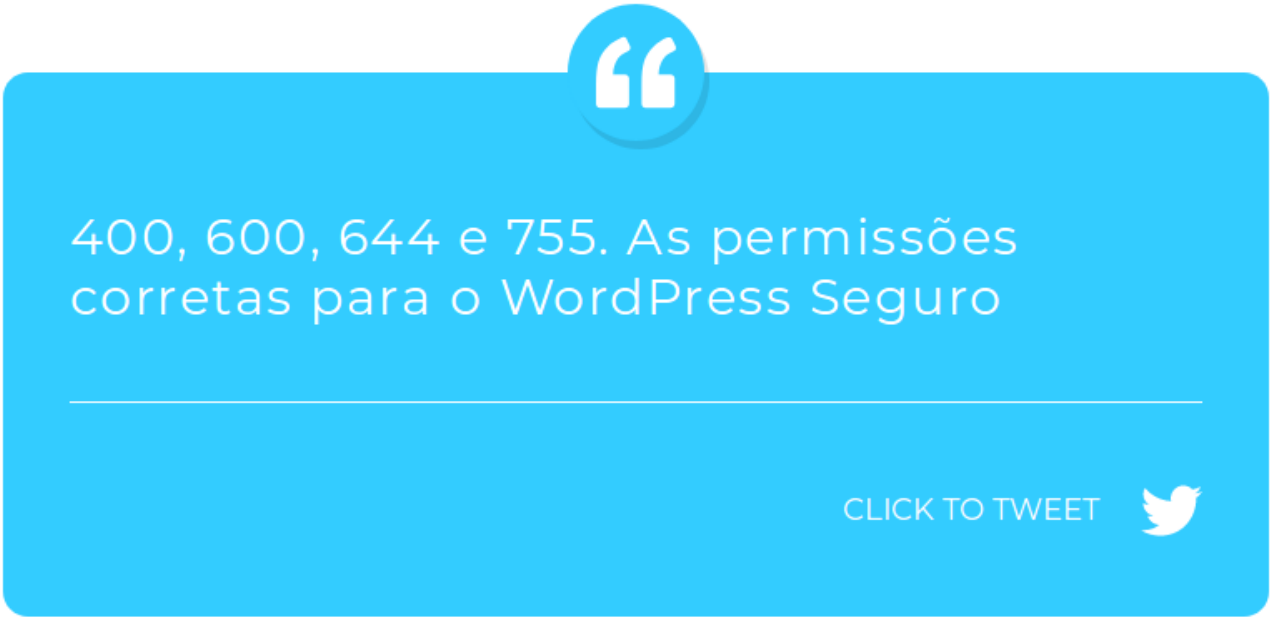


As permissões de arquivos e pastas em números

Segurança para WordPress é possível com uma efetiva permissão dos arquivos e pastas e para isso precisaremos lidar com números e compreender o esquema que o representa. A definição errada dessas permissões, leia-se números, colocará tudo a perder e isso precisa ser levado muito a sério.

Para simplificar e você acertar na mega-sena considere e memorize os números abaixo e siga em frente para conhecer mais sobre a combinação entre 0000 e 0777.

- 0400 – permissão de somente leitura;
- 0600 – permissão de leitura e escrita;
- 0644 – permissão de leitura e escrita para o proprietário e leitura para os demais;
- 0755 – permissão de leitura e escrita para o proprietário, leitura e execução para os demais, evitando a escrita.



As permissões de arquivos e pastas do WordPress para sua segurança

Precisaremos considerar, de uma forma global, todos os arquivos e pastas do core do WordPress, seus plugins e temas e devemos dar uma atenção especial aos arquivos wp-config.php, .htaccess e debug.log.

0644. É a correta **permissão para todos os arquivos**, exceto wp-config.php, .htaccess e debug.log.

A permissão correta para o arquivo wp-config.php

O arquivo wp-config.php deve ter uma tratativa de segurança especial e podemos considerar o uso de duas possíveis permissões.

1. 400. Mais restritiva e permitimos apenas a leitura;
2. 600. Mais branda e além da leitura é permitido a escrita.

A correta permissão para o arquivo .htaccess

Utilizado em servidores web como Apache, .htaccess é a extensão de um arquivo sem nome e sua função é armazenar diretivas de configuração do servidor e assim permitir uma configuração descentralizada das configurações padrão.

644 é a permissão comumente utilizada e recomendada. No entanto, em alguns servidores é possível fazer uso de uma permissão entre 644 à 604 e assim ser mais restritivo ao arquivo. O conselho é começar mais restritivo e aumentar a permissão até que ele funcione, caso tenha sido restritivo demais, mas nunca passe de 644.

A correta permissão para o arquivo debug.log

600. É a permissão correta para o arquivo debug.log gerado pelo mecanismo de depuração de código do WordPress. Além dessa permissão, considere a leitura do artigo A trilogia para um debug seguro e eficaz no WordPress.

O esquema de permissão de arquivos e pastas do WordPress

Permissão	A quem se destina	Considerações
0400	Arquivo wp-config.php	Usar 0600 para permitir escrita além da leitura.
0600	Arquivo debug.log	
0644	Todos os arquivos	Core do WordPress, plugins e temas.
0755	Todas as pastas	Core do WordPress, plugins e temas.

Comandos Shell para definir as permissões de arquivos e pastas do WordPress

```
find /path/to/wp-folder/ type f ! perm 644 exec chmod 644 {} \;

find /path/to/wp-folder/ type d ! perm 755 exec chmod 755 {} \;
```

Diga não ao chmod 0777

Como já falamos inúmeras vezes, considere a permissão 755 para os diretórios e nunca use a permissão 777 para eles, mesmo em diretórios que receberão arquivos enviados via upload. Uma vez que o PHP está sendo processado como proprietário do arquivo, ele recebe a permissão para escrever no diretório mesmo com o uso de 755.

Com o uso da permissão 777 em arquivos ou pastas você permitirá que crackers maliciosos façam upload de arquivos ou modifiquem os existentes e assim tomarão o controle da sua aplicação e poderão até obter informações do seu banco de dados.

Opa! Não conseguimos encontrar o seu formulário.

Fonte: https://blog.apiki.com/permissao-de-arquivos-e-pastas-do-wordpress/