

64MB.win

又一个WordPress站点, 运行在64MB内存的VPS

Nginx中WordPress安全配置规则

在Nginx的配置文件中, 通过禁止一些文件和目录的访问, 可以提高站点的安全性。

我这里采用的是Centmin Mod (CentOS上的LNMP一键包) 中教程安装WordPress时候引用的一个安全配置规则; 额外在禁止文件中增加了 `wp-comments-post.php`, 一定程度上可以防范垃圾评论, 客官们可以根据自己的需求决定是否保留。

IMPORTANT!! 如有需要, 注意请务必在 WordPress 安装之后再添加下面的安全配置规则。

```
wget -P /etc/nginx/sites-available http://x.weishimi.com/64mb/conf/wpsecure.conf
```

往虚拟主机配置文件 (E.G. `64mb.wp.conf`) 添加:

```
vi /etc/nginx/sites-enabled/64mb.wp.conf
```

在 `location /` 块的最下面, 添加如下一行:

```
include /etc/nginx/sites-available/wpsecure.conf;
```

```
nginx -t  
nginx -s reload
```

这样子就可以了, 重要的事情再说一遍吧! 注意在WordPress安装之后, 可以打开首页之后, 再操作上面的。

解说一下Nginx站点安全配置规则

```
#  
# uploads和files文件夹里php格式的文件, 不允许  
location ~* /(?:uploads|files)/.*\.php$ {  
    deny all;  
}  
  
# 一些文件可能会显示密码等信息, 不允许  
location ~* \.(engine|inc|info|install|make|module|profile|test|po|sh|.*sql|theme|tpl(\.php)?|xhtml|  
{  
    return 444;  
}  
  
# nocgi cgi等可执行的, 不允许  
location ~* \.(pl|cgi|py|sh|lua)\.$ {  
    return 444;  
}
```

```
# disallow 一些通信协议，不允许
    location ~* (roundcube|webdav|smtp|http\|:|soap|w00tw00t) {
        return 444;
    }

# 一些文件不允许，其中添加 wp-comments-post.php 可以一定程度上防范垃圾评论，这，注意就好了，如果有特别需要的
location ~ /\.(|wp-config.php|wp-comments-post.php|readme.html|license.txt) { deny all; }
```

基本上就这样子，当然你也可以根据自己的需要，添加或删除。

本条目发布于2016年1月5日 [<https://64mb.win/how/wpsecure/>]。属于INFO分类，被贴了 Nginx、WPSecure、WordPress 标签。