时刻注意WordPress网站的安全

WordPress作为一个很优秀的博客程序，已然被很多人使用，但盛名必然引来注意，更少不了那些不怀好意黑客。因此，加固WP成为个人博客安全防御的工作之一。

1. 升级自己的WP到最新版。
   一般来说，新的WP会修复老版本的一些漏洞，这样升级会使得网站安全。比如很多版本的WP可以使用 pingback
   的远程端口扫描问题，该问题可能导致服务器信息泄露，或被攻击。shortcode
   和文章内容的两处跨站攻击漏洞等。
2. 隐藏安装后WP的版本号。
   默认安装WP之后，会在首页显示安装的WP版本号，建议把那些版本号去掉（进后台，依次选择 外观-->编辑-->footer.php，找到有Wordpress的代码，直接删掉。或者进入functions.php文件，加入

   ```
   function wpbeginner_remove_version() {
       return '';
   }
   add_filter('the_generator', 'wpbeginner_remove_version');
   ```

   保存），因为黑客们很可能利用那个版本号，发现一些漏洞，然后对你网站进行攻击。默认安装WP的时候，它会在你根目录下留下readme.html文件，而这个文件里面有很多关于WP版本信息的介绍，应该删掉。
3. 修改根目录下的.htaccess文件。默认情况下，WP都包含了wp-includes、wp-content以及wp-
   ad
   min
   等文件夹
   ，用户可以在浏览
   器上面输入上面域名加上上面的一些
   目录路径，比如/wp-includes
   ，你会惊讶的发现这个目录下面的文件都显示出来了，这当然不是我们希望的，特别是wp-admin文件夹我们肯定是不想用户直接进入。解决方案：1）如果必须开启该目录的目录列表功能，则应对该目录下的文件进行详细检查，确保不包含敏感文件。2）如非必要，请重新配置WEB服务器，禁止该目录的自动目录列表功能。你可以在www
   目录下修改.htaccess 配置文件，如下：

   ```
   # BEGIN WordPress
   <IfModule mod_rewrite.c>
   RewriteEngine On
   RewriteBase /
   ```

```
RewriteRule ^index₩.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]
Options -Indexes
</IfModule>

# END WordPress
```

然后上传到你服务器所在的根目录下，这样就不可以直接在浏览器上输入文件夹的路径而访问你的文件。或者你有该PHP服务器的控制器，你也可以修改Apache的httpd.conf配置文件，查找 Options Indexes FollowSymLinks，修改为 Options -Indexes；
如果是Tomcat服务器，则可以修改conf/web.xml文件，把listings值改为false，即

```
.....
listings
false
.....
```

ps:修改完httpd.conf后，一定记得重启web服务，才能生效！切忌！

4. 设置robots.txt文件。
   在以前内容里面再添加一行（如果以前有这个文件，没有就直接新建）为：

```
User-agent: *
Disallow: /wp-*
```

意思就是不让所有的搜索引擎抓取根目录下以wp-开头的文件夹下面的所有东西。

5. 不要用WP默认的用户名。
   安装WP的时候，会提供一个默认的用户名admin，尽量不要用，自己取一个，越复杂越好，当然前提是你自己要记得。
6. 减少因为页面异常导致本地路径泄漏。
   如果WEB应用程序自带错误处理/管理系统，请确保功能开启；否则按语言、环境，分别进行处理：1）如果是PHP应用程序/Apache服务器，可以通过修改php脚本、配置php.ini以及httpd.conf中的配置项来禁止显示错误信息：
   修改php.ini中的配置行: display_errors = off
   修改httpd.conf/apache2.conf中的配置行: php_flag display_errors off
   修改php脚本，增加代码行: ini_set('display_errors', false);

2）如果是IIS 并且是
支持aspx的环境,可以在网站根目录新建web.config文件(存在该文件则直接修改),

7. 经常备份你的数据。
上面的设置是有限的。你的网站还是存在各种风险，最好的办法就是经常去备份服务器上面的所有数据，这样当你的网站被黑了，最少你可以把你网站的损失减少到最小，何乐而不为呢！