1. 做好备份

定期进行网站备份时最基本的要求。如果你不能定期备份,一旦出错,网站数据就有可能全部丢失,损失就无法挽回。这样的冒险完全不值得,只要养成良好的备份习惯,即使网站出现问题,也不必担心。

良好的备份习惯有 3 个要点:

1.2.3.备份数据不能保存在服务器上(因为一旦服务器出问题,备份也可能会出问题;使用 vps 的用户尤其要注意这一点)

备份能够自动进行(因为你未必能够记住每天去亲自备份)

有必要保留多个备份(假如说你就保留了过去 3 天的备份,如果你出去度假 5 天,那么你保留的最老版本的备份,可能已经是出了问题的版本了)

因此,我们一般推荐 WordPress Database Backup 这样的插件来进行自动备份,它可以将文件给你自动发送到邮箱中。

2. 保持更新

WordPress 开发社区非常活跃,版本更新速度快,甚至超过了网友们适应的速度。“升级 WordPress 可能会让我的插件/主题无法使用”,基于这样的考虑,是许多 WPer 不愿意及时升级 WordPress 的主要原因。升级 WordPress 确实存在这样的问题。

但是,不及时升级 WordPress 可能会更糟糕。因为 WordPress 每次升级都包含一些安全措施的修补。如果你没有及时更新,你的网站就存在漏洞,这样的网站就处于危险之中。

尤其是 WordPress 小版本的更新,比如从 3.2 到 3.2.1 ,修复了一些安全问题。因此一旦有这样的版本升级,你应该及时进行网站的升级。

对于 WP 网站而言,隐藏版本号或许可以降低一些风险。你可以在你当前所使用的主题的 functions.php 文件中添加如下代码,来隐藏 WordPress 的版本号:

```
remove_action(‘wp_head’, ‘wp_generator’);
```

不过这样并不能代替升级。及时升级仍然是最好的防御措施。

3. 更健壮的密码

或许你已经听无数人这么说了,要选择使用一个更复杂更安全的密码。密码太简单仍然是如何知道你的网站密码是不是很弱呢?容易。如果你的密码有任何的意义,比如说,名字拼音/生日/英文单词等等?如果你能拼出来,基本上就是很差劲的密码。密码应该是真正随机的、毫无意义的字母、数字和符号的组合。

无意义在这里非常重要。将“michael”换成“michae1”并不会更安全一些。因为这样的变换也非常容易猜到。

4. 经常检查你的网站

你的网站经常会在你不知情的情况下受到牵连。比如说,许多令人讨厌的脚本程序会在你的网页上包含一些只有搜索引擎才能查看到的链接。

尽快找到这些代码非常重要。因为一旦 Google 对你的网站进行惩罚,你的排名就要向后靠了,恢复排名的过程异常痛苦。

使用 Google 站长工具或其他类似工具可以帮你尽快查清网页中的链接。

5. 禁止显示目录索引

一般虚拟主机允许显示目录索引。这样,如果有人访问你的网站的某个目录(比如 wp-content/plugins/),就能查看到该目录下的文件名。“ 黑客”可以看到你的服务器上的所有文件名,这非常糟糕。

要修复这个问题很简单,只要使用文本编辑器打开 .htaccess 文件并添加如下代码即可:

#Prevent directory indexing
Options -Indexes

6. 不要使用 FTP

FTP 是向网站上传文件的常用方式,但他并不安全。FTP 传输过程可能会被入侵。如果你的主机允许,建议尽量使用 SFTP 来代替 FTP 。

SFTP 和 FTP 两种工作方式完全不同,但使用上完全一样。如果你不确定你的主机是否支持 SFTP,请联系你的主机商询问(绝大多数都支持 SFTP,包括 我们的主机)。

7. 修改 wp-config.php 文件位置

默认的 wp-config.php 文件存放在网站根目录,但并不是一定要放在这里。你可以将它放到程序的上一级目录中(也就是根本不会出现在网站程序目录中)。

这很做起来很容易,只需要将文件放到上一级目录中。WordPress 会知道去哪儿找到它。

此外,如果你已经使用 WordPress 有段时间,但是却还没有使用安全密钥,我们强烈建议你在 wp-config.php 文件中使用。

WordPress 使用 MD5 来加密用户的密码,加密后的密码很难被破解。但有些黑客用计算机列出了所有 8 位以内密码组合和对应的 md5 码,这样如果获取了加密后的密码,可以直接查出你的密码,非常恐怖。解决这一问题的常用办法就是给密码加“盐”。

你所要做的就是打开 https://api.wordpress.org/secret-key/1.1/salt/ ,将其生成代码复制到 wp-config.php 文件中,然后保存。

8. 小心下载的插件/主题

目前网上可以下载 WordPress 插件和主题的地方非常多,但并非所有的网站都可以相信。根据我们的经验,许多用户网站被黑,大都是使用了带有恶意代码的主题或插件。

在下载 WordPress 主题或插件之前,最好先 Google 一下人们对这个网站的看法。如果有很多的好评和链接,那就不妨去下。否则,还是离开为妙。

对于 WordPress 插件,最好的下载地方是 WordPress 官方插件目录。此外,你也可以去你信得过的地方购买付费插件。

对于 WordPress 主题,WordPress 官方主题目录非常棒。但有很多的优秀的主题开发者都将主题放到自己的网站上。

因此,如果你从第三方的网站上下载 WordPress 主题,强烈建议你立即检查网站(尤其是一些网站会在页脚放一些付费链接,Google 可能会惩罚你的网站)。

9. 通过 ip 限制访问 wp-admin 后台

我们可以通过.htaccess 文件设置,只允许我自己的 ip 访问 wp-admin 目录。这样可以防止暴力破解 WordPress 的密码(除非使用我的电脑),从而轻松保证只有我才可以控制我的网站。当然,这个办法仍然无法阻止数据库被攻击,但是能够有效防止黑客从网站的控制台登录。

将代码放入到 .htaccess 文件中,将红色 ip 地址换成自己的 ip 地址。有一点不方便的是,国内用户的个人用户大多是拨号上网(PPPoE),每次登陆都会随机分配 ip 地址;只有单位里的网络可能会有固定 ip 地址。

你可以登录 ip138 或者 ip.cn 来查询自己的 ip 地址。

```
# 保护 wp-login.php 文件
<Files wp-login.php>
Order deny,allow
Deny from All
Allow from 123.456.789.0
</Files>
```

10. 设置高强度的数据库密码

如果黑客能控制你的数据库,那就基本上就可以为所欲为了。我们强烈推荐用户使用高强度的密码,至少应该包括数字、字母大小写、符号等。使用 cPanel 主机的网友,可以使用密码生成器来帮你自动生成密码。主机上没有密码生成器的其他用户,也可以使用 keepass 这样的软件,来帮你生成高强度密码。

你也可以将数据库的名称设置复杂一些,不要让人一看就能看出是 WordPress 程序。

11. 保护 wp-config.php 文件

wp-config.php 文件里包含的有 WordPress 数据库的重要信息。如果该文件被暴露,再强壮的数据库密码也没有用。 因此,我们可以加一段代码,在 .htaccess 文件里,来保护 wp-config.php 文件:

```
# 保护 wp-config.php 文件
<Files wp-config.php>
Order allow,deny
Deny from All
</Files>
```

12. 防范插件和主题

插件增强了 WordPress 的功能,主题美化了 WordPress 的界面,这是 WordPeress 最吸引用户的资源,但也是容易出问题的地方。有许多不怀好意的插件和主题的开发者,或者插件和主题的下载网站,都被插入了一些恶意代码或后门程序。从我们遇到的许多网友 WordPress 网站的被黑的实际经历看,绝大部分 WordPress 网站被黑,都与使用了暗含后门的主题和插件有关。

因此,我们建议用户尽可能地减少使用的插件数目,并且尽量使用流行的插件,不要使用过于偏僻的和来历不明的插件;通过 WordPress 官方的插件仓库和主题仓库进行下载插件和主题;同时,当插件和主题更新的时候也要及时进行升级更新。

13. 尽量使用 SSL

有许多文章提到了使用 SSL 的重要性,还有许多 WordPress SSL 插件,使用 SSL 并不太麻烦。这里简单解释一下。在你登录 WordPress 网站的时候,你的浏览器需要从你的电脑向服务器传递账户和密码信息。默认情况下,传递过程中数据并不加密,因此存在被黑客截获数据(如账户和密码)的可能性。SSL 就是强制对数据进行加密,减少网站被黑的几率。

如果你的虚拟主机提供 SSL 证书,你可以使用上面的插件来使用 ssl 加密网站。如果没有提供 ssl 证书,建议采用第 1 条中提到的方案,来防止其他用户登录到你的网站后台。

14. 小心你的同事

到此你的网站已经超级安全了,足以防范来自外部的攻击了,现在要防范来自内部的危险了。想象一下,你能否相信你的撰写博客的同事?结果呢,他在你的模板里插入了一个他喜欢的宠物狗的链接,还在你的主机上存放服务器。这种情况很容易防范,你在给你的同事设置用户权限的时候需要慎重。WordPress 默认就提供有用户角色选项,订阅者、投稿者、作者、编辑和管理员。如果你认为你的同事可能会破坏你的博客,要限制其适当的权限。

还有一些插件,如 members 插件和 role manager 插件,可以对用户权限进行更为细致的配置。我们此前在 21 款适合多用户的博客插件一文中,能提到过这些插件。

15. 及时更新

WordPress 新版本发布频繁,经常修复一些安全问题。因此,及时更新你的网站到最新版 WordPress 是非常重要的。当新版的 WP 发布的时候,直接在后台点击更新按钮即可,就可以轻松保持更新。但是需要注意的时候,无论什么时候更新网站,都必须要先备份你的 WordPress。我们推荐使用 WordPress Database Backup 插件,可以轻松进行数据库的自动备份。不仅可以备份到你的

WordPress 主机上,也可以直接备份到你的 email 邮箱。

16. 保护安装文件

在保护程序安装程序方面,WordPress 做的尚不如国内的一些建站程序(如 Discuz!)。WordPress 的安装文件 install.php 可以被任何人访问。如果你的主机宕机,在数据库恢复正常之前,你的网站很有可能被任何人全新安装,给你带来无可挽回损失。非常糟糕。幸运的是,我们有个小技巧可以轻松解决:删除 install.php 文件。你可以通过 FTP 或者主机管理系统里的文件管理系统,删除 WordPress 安装目录下的 /wp-admin/install.php 文件,就彻底消除了隐患。

17. 屏蔽垃圾评论

垃圾评论非常令人讨厌,几乎每个 WordPress 网站都会受到垃圾评论的骚扰。以下这段代码加入到 .htaccess 文件,可以屏蔽掉这些传播广告的垃圾评论:

```
# 屏蔽垃圾评论
<IfModule mod_rewrite.c>
RewriteCond %{REQUEST_METHOD} POST
RewriteCond %{REQUEST_URI} .wp-comments-post\. [NC]
RewriteCond %{HTTP_REFERER} !.*wpchina\. [OR,NC]
RewriteCond %{HTTP_USER_AGENT} ^$
RewriteRule (.*) – [F,L]
</IfModule>
```

当然,这里需要将 wpchina 换成你自己的域名。

18. 移除登录页面里的错误信息

最后,这一条非常重要。在你的主题的 functions.php 文件里添加一行代码,来移除登录错误信息。这样,黑客要进行暴力破解的时候,就不知道是用户名错了,还是密码错了。很聪明!

```
add_filter('login_errors',create_function('$a', "return null;"));
```