

Въведение

Wordpress е една от най-популярните безплатни платформи за създаване и управление на дневници (или т.н. блогове). За съжаление, никой софтуер не е защитен от възможността за поява на пропуск в сигурността. Екипът на Wordpress се стреми да ги оправя навреме, но от вас зависи дали ще обновявате блога си. Ако забравите или умишлено отлагате обновяването, рискувате някой ден да останете неприятно изненадан зареждайки дневника си и в най-лошия случай откривайки, че всичката ви информация е изчезнала. Не се залъгвайте, че никой не се интересува от вашия малък и скътан дневник. Бъдете подготвени за най-лошото, но се надявайте за най-доброто.

В тази статия ще ви представя 12 съвета как да направите вашия Wordpress блог по-сигурен и защитен. Разбира се, имайте предвид, че нищо не може да ви предпази от пробив чрез нерегистриран проблем в сигурността. Също така, атака може да възникне и от инсталиран плъгин, който има слабости в сигурността.

Преименувайте admin потребителя

Веднага след инсталацията е препоръчително да смените името на администратора. То е *admin* и по подразбиране е такова за всички инсталации. Смяната можете да направите през командния ред на MySQL клиент или ползвайки приложение като PhpMyAdmin, което се предоставя безплатно с повечето хостинг пакети.

Командата, която трябва да изпълните е следната:

```
update tableprefix_users set user_login='newuser' where user_login='admin';
```

tableprefix по подразбиране е *wp*, ако не сте го сменили.

Сменете паролата по подразбиране

Паролата, която Wordpress генерира при първоначалната инсталация е сравнително слаба. Тя се състои от 6 символа и то само от числа и букви. Съществуват [приложения](#) чрез, които може да се направи атака и такава слаба парола да бъде открита сравнително лесно. Направете паролата по-сложна, поне от 10 знака. Освен букви и цифри, използвайте и други знаци.

В тази връзка, за защита от продължителни последователни атаки, инсталирайте плъгина [LoginLock](#), чрез който автоматично можете да блокирате IP адрес при определен брой неуспешни опити за влизане в административната част на вашия блог.

Изтрийте ненужните файлове

След инсталация или обновяване има два файла, които няма да ви трябват повече. Рядко могат да ви създадат проблем, но за всеки случай е добре да ги изтриете. Това са `install.php` и `upgrade.php`. Намират се в папката `wp-admin`.

Използвайте лимитиран потребител

Създайте си отделен потребител с по-ниски права на достъп, който да използвате за публикуване. Този подход не само ще гарантира сигурността на дневника, ако някой се сдобие с името и паролата ви, но ще ви предпази и от самите вас.

Премахване на версията от `header.php`

Ако ползвате стара версия на Wordpress с известни пропуски в сигурността, не е много разумно номерът на версията да се вижда публично.

Кодър в `header.php`, който показва версията е:

```
<meta name="generator" content="WordPress <?php bloginfo('version'); ?>" />
```

За да скриете версията, можете просто да изтриете този ред или да го промените по следния начин:

```
<meta name="generator" content="WordPress" />
```

Забележка: Имайте предвид, че версията се показва не само в `header.php`, а и в rss хранилката например, а и в няколко други файла. За повече информация вижте по-надолу [WordPress Online Security Scanner](#).

Защита на папка `wp-admin`

Ограничаване по IP адрес

Единият вариант да ограничите достъпа до администрацията на вашия блог е да посочите изрично кои IP адреси могат да имат достъп. Това става чрез `.htaccess` файл, който трябва да сложите в директория `wp-admin`. Неговото съдържание трябва да бъде подобно на това:

```
AuthUserFile /dev/null  
AuthGroupFile /dev/null
```

```
AuthName "Access Control"  
AuthType Basic  
order deny,allow  
deny from all  
# домашен IP адрес  
allow from 64.233.169.99  
# работен IP адрес  
allow from 69.147.114.210  
allow from 199.239.136.200
```

Този метод определено е много добър за защита, но е и неудобен, ако нямате статичен IP адрес или ако често пътувате и искате да обновявате блога си в движение. За тази цел, много по-удобен е вариантът със защитата с име и парола.

Ограничаване с име и парола

Защитата с име и парола ви позволява да имате достъп до администрацията от всяко кътче на Земята, но добавя второ, допълнително ниво на сигурност. При този вариант отново се използва .htaccess файл. Но този път имаме и един допълнителен файл .htpasswd.

Създайте .htaccess файл в директория wp-admin и напишете следното:

```
AuthUserFile /home/username/.htpasswd  
AuthGroupFile /dev/null  
AuthName Blog  
AuthType Basic  
require user xxxx
```

Особеностите в този файл са две. Първо, на мястото на xxxx въведете името, с което желаете да влизате (това име НЕ Е името на администраторския ви акаунт). Второ, на реда AuthUserFile виждате, че е зададен път до файла .htpasswd. Тъй като .htpasswd съдържа паролата за достъп, то трябва да сложите този файл извън публичната ви директория (често тя се нарича PUBLIC_HTML, но може и да е с друго име) на хостинга. Ако не сте сигурни, консултирайте се с хостинг доставчика, коя директория е публична и коя не.

Съдържанието на файла .htpasswd е:

```
xxxx:yyyy
```

, където xxxx е името, с което желаете да влизате (същото име, което сте написали и в .htaccess), а yyyy е паролата. Ако всичко е успешно, при опит за вход в администрацията ще се появи диалогов прозорец, който ще ви подкани да въведете име и парола.

Уточнение – тези варианти за защита на wp-admin са приложими само, ако регистрирането на потребители е забранено, тоест само вие (или малък кръг от доверени хора) ползвате администрацията.

И един допълнителен съвет – за да спрете търсачките да обхождат директория wp-admin, в главната директория на вашия блог създайте файл robots.txt и напишете това:

```
Disallow: /wp-admin/
```

Защита на папка wp-content

Защита с празен index.html

Създайте празен файл с име index.html и го сложете в папка wp-content и в папка wp-content/plugins, за да предотвратите разглеждането на съответните папки. Можете да сложите празен файл и в другите подпапки стига там да няма файл със същото име, но с друго предназначение.

Защита с .htaccess

Най-лесният и бърз начин да забраните разглеждането на дадена директория и нейните поддиректории е да използвате .htaccess файл. Създайте такъв файл със следното съдържание:

```
Order Allow,Deny
Deny from all
<Files ~ ".(css|jpe?g|png|gif|js|zip|rar|pdf|xsl|ico)$">
Allow from all
</Files>
```

и го сложете в директория wp-content. Така не само предпазвате текущата директория от разглеждане, но блокирате и всички опити за зареждане на файлове с изключение на тези с упоменато разширение.

Защита на папка wp-includes

Защита с празен index.html

Създайте празен файл с име index.html и го сложете в папка wp-includes, за да предотвратите разглеждането й. Можете да сложите празен файл и в другите подпапки стига там да няма файл със същото име, но с друго предназначение.

Защита с .htaccess

Отново, най-добрият начин за защита на wp-includes е с използване на .htaccess файл. Можете да използвате същия файл както този при wp-content. При мен за съжаление ползвайки същия файл, спря да работи текстовият редактор TinyMCE.

Решението на проблема е вместо да използвате блокиране на заявки за зареждане на файлове, просто да забраните разглеждането на директорията. Това става като в .htaccess напишете следното:

```
Options -Indexes
```

Изключително бърз, лесен и ефективен начин за защита.

Използвайте сигурна връзка към сървъра

По възможност използвайте SSH вместо FTP. Това е може би един от най-трудните за изпълнение съвети, но същевременно един от най-важните. Първо, свържете се с хостинг доставчика си и се уверете, че има включен SSH. Обикновено FTP връзката не е защитена и името и паролата на ftp акаунта ви се предават във вид на чист текст. По този начин, ако някой се добере до тази информация, може да получи достъп до файловете ви и да нанесе достатъчно вреди. Ползвайки SSH, цялата комуникация между вас и сървъра е защитена.

WordPress Online Security Scanner

Този [плъгин](#) от [Blog Security](#) прави проверка на версията и показва възможните уязвимости в даден блог, включително уязвимости в използваната тема и инсталираните плъгини.

Правете редовна профилактика

Редовно правете резервни копия на файловете и на базата от данни, в случай че се наложи да възстановявате информация.

Следете редовно бюлетина на Wordpress

На адрес <http://wordpress.org/development/> се публикува информация свързана с Wordpress, най-новите версии, отстранени пропуски в сигурността и друга полезна информация.

За финал

И накрая – не забравяйте да обновявате редовно.

Надявам се, че този документ не ви е отегчил много, а съветите ще са ви от полза. Ако имате препоръки или забележки, ще се радвам да ги [споделите с мен](#).