Codex tools: Log in

Home Page
WordPress Lessons
Getting Started
Working with WordPress
Design and Layout
Advanced Topics
Troubleshooting
Developer Docs
About WordPress

Codex Resources

Community portal
Current events
Recent changes
Random page
Help

Interested in functions, hooks, classes, or methods? Check out the new WordPress Code Reference!

bg:Hardening WordPress

Сигурността във WordPress се приема много на сериозно, но както и при всяка друга система има потенциални проблеми със сигурността, които могат да възникнат, ако не се вземат някои основни мерки за сигурност. Тази статия ще премине през някои често срещани форми на уязвимост, и нещата, които можете да направите, за да запази сигурността на вашата WordPress инсталация.

Тази статия не е бързо решение на проблемите, свързани със сигурността. Ако имате конкретни съображения за сигурност или съмнения, трябва да ги обсъдите с хора, на които имате доверие, които имат необходимото познание върху компютърната сигурност и WordPress.

Contents

Какво е сигурност?

Основно сигурността *не се* отнася за изделано сигурни системи. Това понятие може да е непълно или да е невъзможно да се октрие или поддържа. Един сигурен сървър защитава поверителността, цялостта и достъпността на ресурсите си, под контрола на неговия администратор

Качествата на един сигурен хостинг включват:

- С готовност обсъждат твоите притеснения, свързани със сигурността и това кои функции и процеси предлагат на техния хостинг.
- Предлагат най-новата стабилна версия на целия сървърен софтуер.
- Предлагат надеждни методи за създаване на резервни копия и възстановяване от тях.

Решете какви са изискванията ви за сигурност като уточните какви данни трябва да бъдат осигурени. Останалата част от това ръководство ще ви помогне за това.

Теми относно сигурността

Имайте предвид някои основни идеи, докато мислите за сигурността на всяка част от вашата система:

Ограничаване на достъпа
: Вземете съответните решения, с които да ограничите възможните входни точки за злонамерени лица.

Ограничения
: Вашата система трябва да бъде конфигурирана така, че да се намали размерът на щетите, които може да се получат в случай, че бъде компрометирана.

Подготовка и знания
: Поддържайте резервни копия и проверявайте състоянието на вашата WordPress инсталацията на редовни интервали. Имайте план за архивиране и възстановяване на вашата инсталация в случай на катастрофа. Това може да ви помогне да се върнете онлайн по-бързо в случай на проблем.

Уязвимости на вашия компютър

Уверете се, че компютрите, които използвате, нямат шпионски и/или

злонамерен софтуер и вирусни. Не съществува ниво на сигурност, което да защити или гарантира вашият WordPress или вашия уеб сървър, в случай, че имате Keylogger на вашия компютър.

Винаги поддържайте вашата операционна система и инсталиран софтуер актуализирани, особено вашия уеб браузър, за да се предпазите от уязвимости в сигурността.

Уязвимости във WordPress

Както много модерни софтуерни пакети, WordPress се актуализира едовно за да отговори на новите пропуски в сигурността, които могат да изникнат. ПОдобряването на сигурността на софтуера е постоянна грижа, а за тази цел трябва да сте винаги в крак с **най-новата версия на WordPress**. За стари версии на WordPress не се доставят обновления по сигурността.

Актуализиране на WordPress

Основна статия: Updating WordPress.

Най-новата версия на WordPress е винаги достъпна за сваляне от главния сайт, намиращ се на http://wordpress.org. Официалните версии не могат да се свалят от други сайтове -- **никога** не сваляйте или инсталирайте WordPress от друг сайт, раличен от http://wordpress.org.

Версиите след 2.7 включват функция за автоматични обновления. Използвайте тази функция, за да улесните процеса по актуализацията. Също може да използвате контролния панел (WordPress Dashboard), за да се информирате относно актуализациите. Четете новините в контролния панел или в блога на разработчиците на WordPress (WordPress Developer Blog), за ра се информирате относно стъпките за актуализиранете на WordPress и поддържането му сигурен.

Ако бъде разкрита уязвимост във WordPress и се издаде нова версия за да я поправи, информацията, свързана с тази уязвимост също става публично достияние. Това прави старите версии още по-лесни за атака и това е енд от основните причини, порадикоято трявбва винаги да поддържате WordPress актуален.

Ако сте администратор на повече от една инсталация, може да използвате Subversion за да направите поддържката по-лесна.

Докладване на проблеми със сигурността

Ако мислите, че сте намерили уязвимост във WordPress, можете да помогнете, докладвайки въпросния проблем. Погледнете Security FAQ за повече информация относто това, как да докладвате за уязвимост със сигурността

If you think you have found a bug, report it. See Submitting Bugs for how to do this. You might have uncovered a vulnerability, or a bug that could lead to one.

Уязвимости във уеб сървъра

Уеб сървърът,на който се намира WordPress, както и софтуерът на него може да имат уязвимости. Поради тази причина трябва да се убедите, че използвате сигурни, стабилни версии на инсталираните уеб и друг софтуер или се уверете, че използвате доверен хостинг, който се гризи за това вместо вас.

Ако сте на споделен хостинг (на този сървър има и други уеб сайтове) и уебсайт на същия сървър бъде компрометирана, вашият уеб сайт може да също да е потенциално застрашен, дори и да следвате всички упътвания от настоящото ръководство. Попитайте вашият уеб хостинг относно мерките за сигурност, които те взимат.

Уязвимости в мрежата

Мрежата трябва да е сигурна и в двата си края -- от страна на сървъра с WordPress и от страна на клиента --. Това означава да се актуализират настойките на зашитната стена на домашната ви интернет връзка и да сте внимателни от какви мрежи се работите. Интернет кафе в което изпращате пароли, чрез некриптирана връзка, или безжична такава **НЕ** са сигурни мрежи.

Вашият уеб хостинг доставчик, както и вие самите трябва да се уверите, че неговите мрежи на са компрометирани от злонамерени лица. Уязвимости в мрежата биха позволили да бъдат прехванати пароли и друга лична информация.

Пароли

Много потенциални уязвимости могат да бъдат избегнати с добри навици за сигурността. Изборът на сложна парола е важен аспект от тях.

Важно за една парола е да е трудна за отгатване и за brute force атаки. Има много автоматични генератори на пароли, които могат да бъдат използвани а генериране на сигурни пароли

WordPress също предлага измервач за сигурността на всяка парола, който се показва когато си сменяте параолата. Използвайте го, за да се уверите, че пароалта ви е достатъчно сложна.

Какво да избягвате при избора на парола:

- Всякакви пермутаци от вашето истинско име, потребителско име, фирма или уебсайт
- Речникова дума от който и да е език
- Къса парола
- Парола,съставена само от цигри или букви (най-добре комбинация от двете).

Сигурната парола е необходима не само за да защитите съдържанието на своя блог. Ако хакер получи достъп до администраторския ви акаунт може да инсталира всякакви скриптове, които да изложат на риск цялата висистема.

FTP

Когато се свързвате със сървъра си е желателно да използвате SFTP криптиране, ако доставчикът ви поредлага такова. Ако не знаете дали вапият хостинг провайдър предлага тази услуга, просто го попитайте.

Използването на SFTP е същото като FTP, с изключение на това, че паролата и други данни, които се предават между вас и сървъра са в кодиран вид. Това означава, че вашата парола никога няма да бъде изпратена в прав текст, което прави невъзможно прихващането и от хакер.

Файлови права

Някои от характеристиките на WordPress позволяват някои файлове да за бъдат достъпни за запис от уеб сървъра. Въпреки това, даване на достъп за запис на файловете е потенциално опасно, особено на споделен хостинг.

Най-добре е да ограничите файловите права колкото се може повече и да премахвате това ограничение, когато се налага тези файлове да се прометят или да създадете специфични папки с права за запис за строго определни цели, като например качване на файлове.

Ето един пример за файлови права:

Всички файлове трябва да са собственост на потребителския ви акаунт и трябва да имате права за запис. Всички файлове, които трябва да имат права за запис от WordPress, трябва да имат права за запис от уеб сървъра, ако настройките на хостинга го изискват, може да се наложи тези файлове да са собственост на групата на уеб сървъра.

`/`
: Главната WordPress директория: Всички файлове трябва да имат права за записване единствено от вашия потребител, с изключение на `.htaccess`, в случай, че искате WordPress автоматично да пренаписва правилата.

`/wp-admin/`
: Област за администрация на WordPress: Всички файлове трябва да са достъпни за запис само от вашия потребителски акаунт.

`/wp-includes/`
: По-голямата част от работните файлове на WordPress : Всички файлове трябва да са достъпни за запис само от вашия потребителски акаунт.

`/wp-content/`
Съдържание, качвано от потребителите: предназначени за запис от вашия потребителски акаунт, както и от потребителя на уеб сървъра

В `/wp-content/` ще намерите:

`/wp-content/themes/`
Теми. Ако желаете да използвате вградения редактор за теми, всички файлове трябва да са достъпни за запис от потребителя на уеб сървъра. Ако не желаете да използвате вградения редактор за теми, всички файлове може да са достъпниз а запис само от вашия потребителски акаунт.

`/wp-content/plugins/`
Разширения: Всички файлове трябва да са достъпниз а запис самоот вашия потребителски профил.

Други папки, които може да се съдържат в `/wp-content/` е редно да са документирани и правата може да варират.

Смяна на файловите права

Ако имате достъп до сървъра посредством конзола, може да промените правата рекурсивно със следната команда:

За папки:

```
find /път/до/вашата/wordpress/инсталация/ -type d -exec chmod 755 {} \;
```

За файлове:

```
find /път/до/вашата/wordpress/инсталация/ -type f -exec chmod 644 {} \;
```

Относно автоматичните обновления

Когато "казвате" на WordPress да се актуализира автоматично, всички операции се извършват от потребителя, който е собственик на файловете, не от потребителя на уеб сървъра. Всички файлове са с права 0644 и всички директории с 0755, т.е. имат достъп за запис от потребителя и достъп за четене от цялата система, включително и уеб сървъра.

Сигурност на базата данни

Мъдро е, ко имате инсталирани няколко блога на същата система, да ги държите в отделни бази данни, управлявани от разлини потребители. Това е най-лесно, при първоначалната инсталация на WordPress . Това е стратегия за задържане: Ако нарушител успешно кракне едната от инсталациите на WordPress, ще му е много по-трудно да засегне останалите инсталации.

Ако вие самите администрирате MySQL, уверете се, че разбирате конфигурацията му и че излишни функции (като отдалечен TCP достъп) са забранени. Вижте Secure MySQL Database Design за по-добро въведение.

Защита на wp-admin

Добавяне на защита чрез парола (като например BasicAuth) към `/wp-admin/` добавя втори слой защита на администраторския панел на вашия блог, формуляра за вход и вашите файлове. Това кара нарушителите да атакуват този втори слой защита, а не панела за вход на вашия WordPress. Много WordPress атаки се извършват от автономни софтуерни ботове.

Защитата на папката `wp-admin/` може също да блокира някои функции на WordPress, като например AJAX handler на `wp-admin/admin-ajax.php`. Вижте частта с Ресурсите за повече информация и документация относно как правилно да защитите вашата `wp-admin/` директория.

Най-често срещаните атаки към WordPress блоговете най-често се разпределят в две категории:

1. Изпрашане на специфични HTTP заявки към вашия сървър, със специфични експлойти за специфични уязвимости. Тези включват стари/неактуализирани версии на добавки и софтуер.
2. Опит за получаване на достъп до сайта, използвайки "brute-force" атаки за налучкване на паролата.

Най-доброто решение за този "твори слой" е да изисква HTTPS SSL кодирана връзка за администраторския

панел, така, че всички данни сръвзани с администрацията на сайта да са кодирани. *Вижте Administration Over SSL.*

Защита wp-includes

Втори слой зашита може да бъде добавен и там, където до скриптовете няма директен достъп от потребителите. Един от начините да се постигне това е да забраните на тези скриптове да използват mod_rewrite във файлта .htaccess. **Забележка:** да се уверите, че кодът по-долу няма да бъде пренаписан от WordPress, поставсете го извън `# BEGIN WordPress` и `# END WordPress` таговете в .htaccess файла. WordPress може да пренапише всичко между тези два тага.

```
# Block the include-only files.
RewriteEngine On
RewriteBase /
RewriteRule ^wp-admin/includes/ - [F,L]
RewriteRule !^wp-includes/ - [S=3]
RewriteRule ^wp-includes/[^/]+\.php$ - [F,L]
RewriteRule ^wp-includes/js/tinymce/langs/.+\.php - [F,L]
RewriteRule ^wp-includes/theme-compat/ - [F,L]

# BEGIN WordPress
```

Това не работи много добре на Multisite инсталация, тъй като `RewriteRule ^wp-includes/[^/]+\.php$ - [F,L]` би забранило на файла ms-files.php да генерира снимки. Изключвайки тази линия ще направи така, че кодът да работи, но в същото време ще предложи по-слаба сигурност.

Защита на wp-config.php

Можете да изместите файла `wp-config.php` в родителската папка на вашата WordPress инсталация. Това означава, че може да поставите `wp-config.php` файла в папка извън вашето уеб пространство.

> **Забележка:** Някои хора предполагат, че изместването на wp-config.php има минимален принос за сигурността и ако не се извърши внимателно, може на практика да доведе дос ериозни уязвимости. Други не са съгласни.

Забележете, че `wp-config.php` може да бъде разположен ЕДНО ниво над WordPress (където се намират wp-includes) инсталацията. Също така се уверете, че само вие (и уеб сървърът) имат достъп за четене на този файл (това по принцип означава права 400 или 440).

Ако използвате сървър с .htaccess, можете да поставите следния код (в самото начало на файла) за да забраните на всички да го виждат:

```
<files wp-config.php>
order allow,deny
deny from all
</files>
```

Забрана за редакция на файлове

Контролният панел на Wordpress по подразбиране позволява на администраторите да редактират PHP файлове, като добавки и теми. Това често е първият инструмент, който ще използват хакерите, ако успее да получи достъп, тъй като той позволява стартирането на код. Wordpress има опция, с която за забраните редакцията на файловете, посредством контролния панел. Поставяйки следната линия във файла wp-config.php е равносилно на премахването на 'edit_themes', 'edit_plugins' и 'edit_files' възможностите на всички потребители: define('DISALLOW_FILE_EDIT', true);

Това няма да спре хакерите да качат зловреден софтуер на вашия сайт, но би спряло някои атаки.

Добавки

Преди всичко се уверете, че всичките ви добавки са винаги актуализирани. Също така, ако не използвате дадена добавка я изтрийте от вашата система.

Добавки за защитна стена

Има няколко добавки, които претендират че отсяват подозрително изглеждащи заявки, като се базират на правила записани в базата данни или в бели списъци. добавка WPIDS на BlogSecurity's инсталира PHPIDS - общ

слой за защита на WordPress, докато WordPress Firewall използва някои предварително зададени правила на WordPress съвкупно с бял списък без да е необходима конфигурация.

Добавки, които се нуждаят от достъп за запис

Ако добавка изисква достъп за запис на вашите WordPress файлове и папки, моля прочетете кода, за да уверите че е легитимен или попитайте някого, на когото вярвате. Местата, на които може да проверите са форумите по поддръжката и IRC чатовете.

Добавки, които изпълняват код

Както казахме, част от работата по защитата на WordPress е задържане на причинените щети, ако бъде извършена атака.

Plugins which allow arbitrary PHP or other code to execute from entries in a database effectively magnify the possibility of damage in the event of a successful attack.

A way to avoid using such a plugin is to use custom page templates that call the function. Part of the security this affords is active only when you disallow file editing within WordPress.

Сигурност чрез укриване

Сигурност чрез укриване по принцип е ненадеждна стратегия. Въпреки това има области във WordPress, където укриването на информация **може** помогне на сигурнсотта:

1. **Преименуване на администарторския акаунт:** На нова инсталация вие може просто да създадете администраторски акаунт и да изтриете "фабричния" `admin` акаунт. На вече съществуваща инсталация може просто да преименувате фабричния администраторски акаунт, чрез MySQL конзолата,използвайки следната команда `UPDATE wp_users SET user_login = 'newuser' WHERE user_login = 'admin';`, или използвайки друг графичен интерфейс като например phpMyAdmin.
2. **Смяна на представката на таблиците:** Много публикувани SQL-injection атаки, специфични за WordPress допускат, че таблиците започват с `wp_`, което е по подразбиране. Променяйки това, ще спре поне част от тези SQL injection атаки.

Резервни копия

Правете резервни копия редовно, включвайки и вашата MySQL база данни. Вижте следната статия: Създаване на резервни копия на вашата база данни.

Целостта на данните е от изключително значение за надеждни резервни копия. Криптиране на резервните копия,пазене на MD5 ключза всеки файл и/или записването им върху носител само за четене значително увеличават гаранцията, че данните не са манипулирани.

Една надеждна стратегия за резервни копия трябва да включва редовни копия на цялата WordPress инсталация (включвайки файловете на WordPress, както и базата данни) на сигурно място. Представете си,че правите копия един път седмично. Тази стратегия означава, че ако сайтът ви е компрометиран на 1-ви май, но това не е засечено до 12-ти май, собственикът на сайте ще има резервни копия, които ще са от преди 1-ви, които ще помогнат да върнете сайта до нормалното му функциониране, дори резервните копия след заразяването могат да допринесат за това да се установи как сайтът е бил компрометиран.

Логване

Можете да логвате различните заявки, изпращани към WordPress. Стандартните логове на Apache предлагат голяма помощ когато става въпрос за разследване на проблеми със сигурността. Вижте Mod_Security - Логване и предпазване при използване на Apache.

Наблюдение

Понякога прдпазването не е достатъчно и е възможно да бъдете хакнат. Затова мониторинга и откриването на прониквания са много важни. Те ще ви позволят да реагирате по-бързо, да разберете какво се е случило и да възстановите сайта си.

Мониторинг на логовете

Ако сте на частен сървър (където имате администраторски достъп), трябва да следите вашите логове за опити за налучкване на паролите, уеб атаки и т.н. Добро решение с отворен код за наблюдаване на логовете в реално време и блокиране на атакуващия е OSSEC.

Следене на файловете за промени

Когато се осъществи атака,тя винаги оставя следи. Както в логовете, така и на файловата система (създадени нови файлове или модифицирани съществуващи такива). Ако използвате OSSEC той ще наблюдава файловете ви и ще ви извести, когато те бъдат променени

Външно наблюдение на уеб сървъра

Ако хакер опит да заличи сайта ви или да добави зловреден софтуер, може да забележите промените, използвайки уеб базирано мониторинг решение.

Използвана литература*

- MVIS Security Center (Plugin): Идентифицира повечето от темите, описани в това ръководство и предоставя информация за това как да подсигурите WordPress
- e-Book: Подсигуряване на WordPress
- wpsecure.net Има няколко ръководства за това как да подсигурите WordPress.
- Brad Williams: Lock it Up (Video)
- Официална документация за това как да защитите с парола директории с помощта на .htaccess
- Лесен самоучител за защита на контролния панел на WordPress с парола и да поправите грешките 404
- Малко по-сложен самоучител за това как да защитите директории с парола, използвайки .htaccess файла
- whiteWhitelisting the admin-ajax.php handler in password protected directories with apache and lighttpd
- AskApache Password Protection plugin for wp-admin/ and other directories **Caution:** Installing the AskApache Password Protection plugin may lock you out of your WordPress Admin panel. See the comments under the author's plugin home page to read other users' experiences with this plugin.

- реално използваната литература е за оригиналната статия на айглийски език. Тази статия е превод на оригиналната, която се намира тук