https://www.wpbeginner.com/wordpress-security/:

The Ultimate WordPress SECURITY Guide – Step by Step (2019)

Last updated on March 7th, 2019 by Editorial Staff

Информационната безопасност на WordPress е приоритетна тема за всеки собственик на Web-Сайт. В „Черния списък“ на Google ежедневно биват изброени над 10,000 Web-Сайта за Зловреден софтуер (Malware) и около 50,000 опита за Посегателства над Чувствителна информация (Phishing) всяка седмица.

Като Изрядни владелци на нашия Web-Сайт, редно е да съблюдаваме Добрите WordPress-практики в Информационната безопасност. В настоящото Ръководство ще се запознаем с водещите насоки при Информационната безопасност във WordPress, с оглед да предпазим нашия Web-Сайт от Хакерски атаки и Зловреден софтуер (Malware).

Софтуерът на Ядрото на WordPress е изключително надежден и безопасен и непрестанно се инспектира от стотици Разработчици, но за Сигурността на нашия Сайт, щателни грижи следва да полагаме самите ние.

Във WPBeginner се водим от максима, че Безопасността не касае единствено ПРЕДПАЗВАНЕ от Риска. Тя включва и МИНИМИЗИРАНЕ на Риска. Като собственик на Web-Сайт, редно да предприемем редица мерки за по-добрата Безопасност на нашия WordPress-Сайт (дори когато не сме Tech-експерти).

Разполагаме с богат Арсенал инструменти, които можем да използваме в защита на Уязвимостта и Безопасността на нашия Web-Сайт.

За удобство на Ползвателя, прилагаме Съдържание за по-лесно Търсене в настоящото Ръководство по WordPress Информационна безопасност.

Съдържание

Основи на WordPress Информационната безопасност

Кое прави Информационната безопасност на WordPress така важна?

Злонамерените посегателства по един WordPress-Сайт са в сериозен ущърб на постъпленията от Стопанска дейност и на репутацията ни. Хакери може да се доберат до ценна информация и Пароли, да инсталират Зловреден (Malicious) софтуер и дори да увредят нашите Посетители.

Още по-лош вариант е да се озовем в ситуация да плащаме на хакери пари, за да ни върнат Достъпа до собствения ни Web-Сайт.

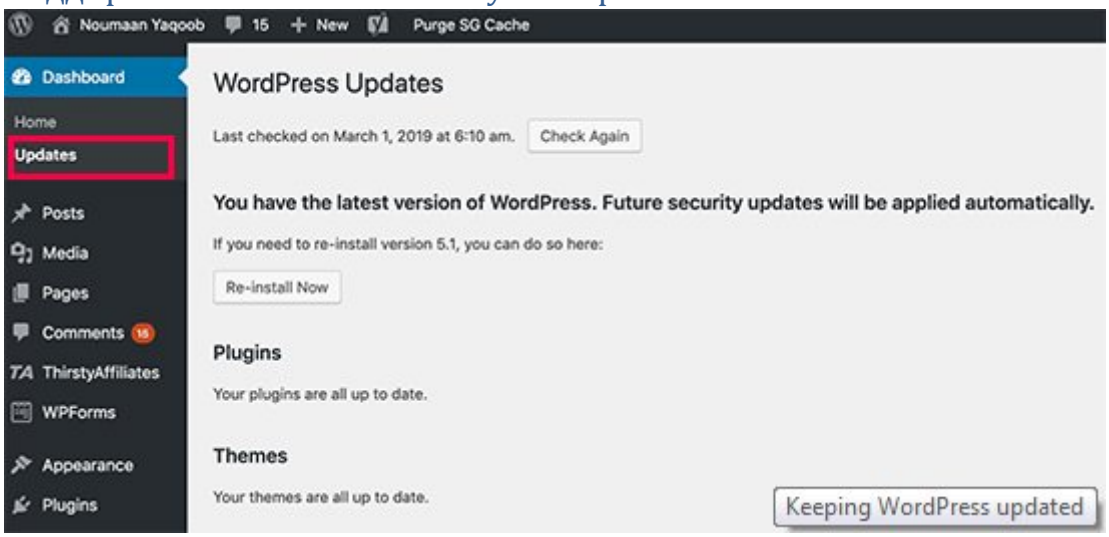
През март 2016 от Google докладваха, че над 50 милиона Посетители на Web-Сайтове са били предупреждавани, че посещаваният от тях Web-Сайт вероятно в заразен с Вируси, че в него присъства Зловреден софтуер или ползва с користни цели тяхна Информация.

В допълнение, Google публикуваха Черен списък с около 20000 Web-Сайта за Зловреден софтуер и около 50000 за Посегателство над Лични данни (Phishing) ежеседмично.

Ако Сайтът ни е със Стопанска цел, трябва да отделяме специално внимание на WordPress Информационната безопасност.

Както собствениците на конвенционален магазин се грижат за безопасността на помещението и сградата, така и ние, като собственик на Online Бизнес, имаме ангажимент относно Защита на нашия Стопански Web-Сайт.

Поддържане на WordPress Актуализиран



В качеството си на Софтуер с Отворен код (Open Source Software), WordPress регулярно се Поддържа и Актуализира. Стандартно, WordPress Автоматично се грижи за по-дребни Update-и, докато Актуализации на Основните версии правим самите ние „на ръка“.

Във WordPress присъстват хиляди Plugin-и и Theme-и, някои измежду които можем да Инсталираме в нашия Web-Сайт. Въпросните Plugin-и и Theme-и се Поддържат от ВЪНШНИ Разработчици и за тях те също Публикуват регулярни Update-и.

Споменатите WordPress Update-и са ключови за Безопасността и Стабилността на нашия WordPress Сайт. WordPress Ядрото, Plugin-ите и Theme-ите ни трябва винаги да са Актуализирани до ПОСЛЕДНА Версия.

Сигурни Пароли и Потребителски правомощия (Strong Passwords and User Permissions)

Най-честите опити за Посегателство (Hacking Attempts) във WordPress, са с използване на чужди Пароли (Stolen Passwords). С цел да ги затрудним, използваме ПО-Сигурни Пароли, строго специфични за нашия Сайт. Не само в Областта за Администриране: WordPress admin area, но и за FTP Акаунти, База-данни, WordPress hosting Абонамент (Account), както и за нашите Обичайни e-mail Адреси (custom email addresses) с Домейн Името на нашия Сайт.

Много често в началото се въздържаме да използваме Сигурни пароли (Strong Passwords), защото са трудни за запомняне. Добрата новина е, че вече не се налага да помним Пароли. Можем да ползваме Password Manager. Направете справка в нашето Ръководство how to manage WordPress passwords.

Друг начин да намалим Риска, е да не предоставяме никому Достъп до нашия WordPress admin Акаунт, освен в случай на крайна необходимост. Ако работим в голям Екип или с външни Автори следва да сме сигурни, че съблюдаваме Правилата за Даване на Потребителски Роли и Правомощия във WordPress, когато добавяме Нови Потребителски Акаунти и Автори в нашия WordPress-Сайт.

Значение на Web-Хостинга

Нашата WordPress Hosting Услуга играе КЛЮЧОВА Роля за Информационната безопасност на нашия WordPress-Сайт. Надеждният shared hosting provider, от типа на: Bluehost или Siteground, полага специални грижи за Защита на своите Сървъри от всякакви Заплахи.

Ето какво регулярно прави добрата Web Hosting компания с цел ЗАЩИТА на нашите Web-Сайтове и Данни.

- Перманентно следи своята Мрежа за нерегламентирани дейности.
- Всички добри Hosting Компании разполагат с Инструменти за Превенция на крупни DDOS Атаки (вж. тук или тук)
- Непрестанно Осъвременяват Software-а и Hardware-а на Сървърите, с цел да лишат Хакерите от възможност да използват прийоми за Увреждане на Уязвими места в Безопасността на познати Стари версии.
- Разполагат с готови Планове за ВЪЗСТАНОВЯВАНЕ след Срив и при Инциденти, и така могат да предпазят Данните ни в случай на съществен инцидент.

При План за Поделен Hosting, ползваме Сървърен ресурс съвместно с множество други Потребители. Това предпоставя Риск от Междусайтова Скриптинг-Атака (Cross-Site Contamination), при каквато Хакерите обикновено ползват друг (Neighbouring) Сайт на Сървъра за Атаки по нашия.

Използването на managed WordPress hosting Услуга предоставя по-сигурна Платформа за нашия Web-Сайт. Компаниите-Доставчици на Managed WordPress hosting осигуряват Автоматично Архивиране (Automatic Backups), Автоматични WordPress Update-и и ПО-Безопасни Конфигурации за ПО-Добра ЗАЩИТА на нашия Web-Сайт.

Авторите ПРЕПОРЪЧВАТ WPEngine като Managed WordPress Hosting Доставчик – техен фаворит. Компанията е сред НАЙ-РЕНОМИРАНИТЕ Участници в Бранша. (вж. нашия специален WPEngine coupon).

WordPress Информационна безопасност в ЛЕСНИ Стъпки (НЕ ИЗИСКВАЩИ Умения по Програмираме)

Наясно сме, че мисълта за подобряване Информационната безопасност на WordPress сигурно притеснява непосветените и особено Hi-Tech неспециалистите. С положителност не сте единствени.

Подпомогнали сме хиляди WordPress-Ползватели да подобрят своята WordPress Информационна безопасност.

Ще ви разясним как можете да подобрите своята WordPress Информационна безопасност със само няколко Click-а (без да трябва да пишете Код).

Предостатъчно е да можете да Позиционирате Мишката и да Щракате с нея!

Инсталиране на WordPress Backup Solution

Архивите (Backups) са наша ПЪРВА Защита срещу всякаква WordPress Атака. Нека сме наясно, че 100%-ва Сигурност е НЕПОСТИЖИМА. Щом Правителствени Web-Сайтове могат да бъдат Hack-вани, значи и нашият може.

Архивите (Backups) ни предоставят Възможност бързо да ВЪЗСТАНОВИМ нашия WordPress-Сайт, в случай на необходимост.

Има множество Свободни и Платени Plugin-и: WordPress backup plugins, които можем да ползваме. Основно Правило при използването на Архиви (Backups) е РЕДОВНО да правим ПЪЛЕН Backup на Сайта на Външен носител (различен от нашия Hosting Account).

Препоръчително е Съхранение да се прави на Cloud Service, от типа на: Amazon, Dropbox или private clouds, от типа на: Stash.

В зависимост от честотата на Промените в нашия Web-Сайт, оптимални може да са Настройки от Архивиране веднъж на ден, до Backup в Реално време.

За щастие, можем да ползваме Plugin-и, като: VaultPress или UpdraftPlus – и двата: надеждни и най-вече: Лесни за използване (не изискват Програмиране).

Най-добър WordPress Security Plugin

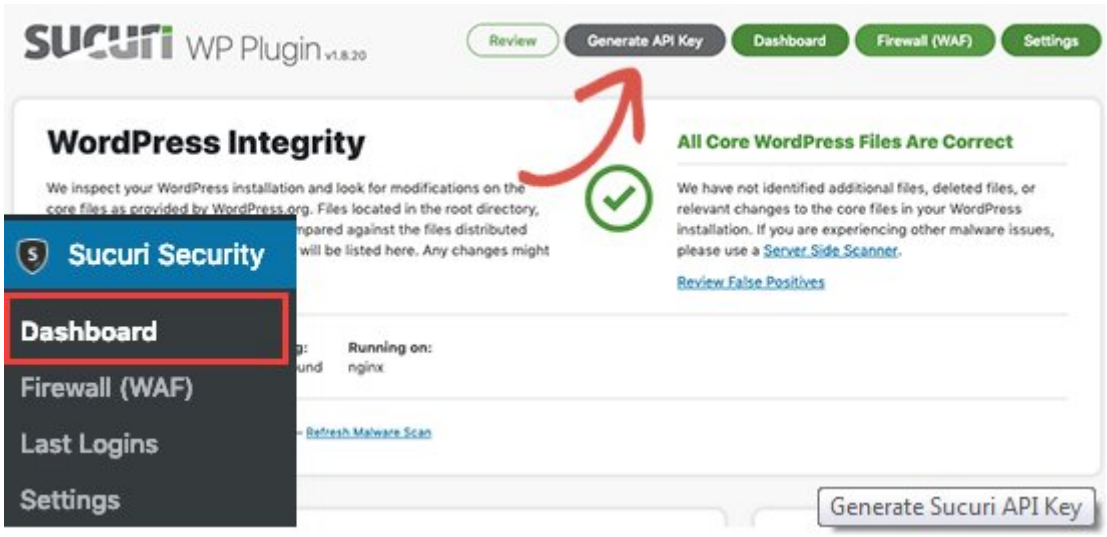
Освен за Архивирания, редно е да се погрижим и за Система за Audit-иране и Monitoring, следяща всичко, което става на нашия Web-Сайт.

Това включва СЛЕДЕНЕ на Файлов ИНТЕГРИТЕТ (File Integrity Monitoring) и на НЕУСПЕШНИ Опити за Влизане, Сканиране за Зловреден софтуер (Malware Scanning) и пр..

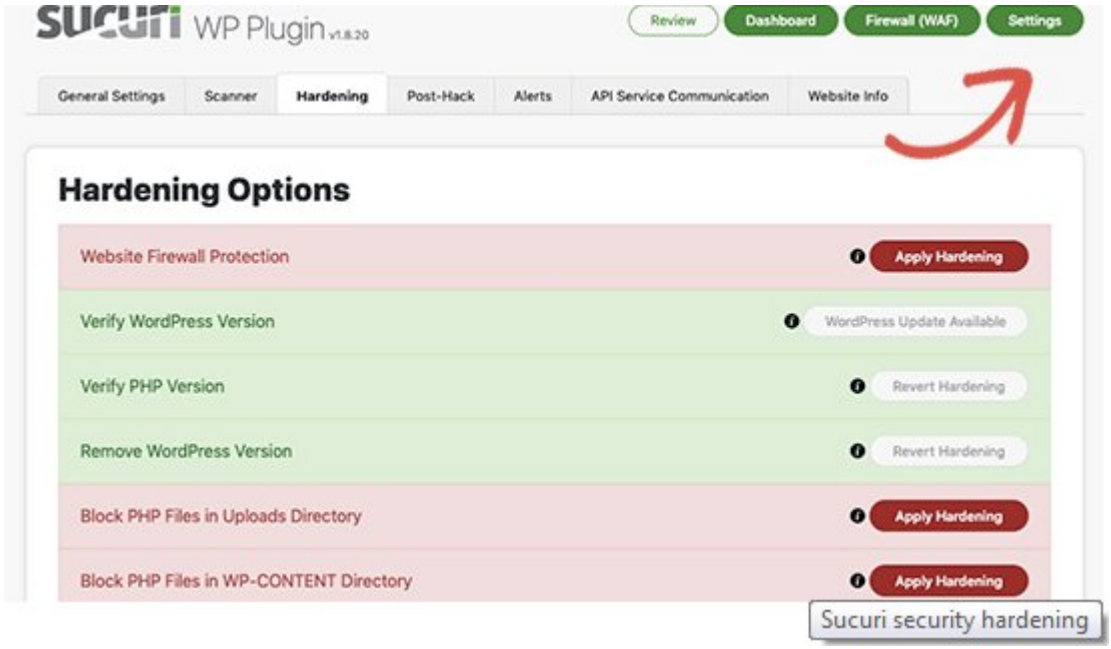
За щастие, за всичко това на помощ ни идва НАЙ-Удачният СВОБОДЕН (Free) WordPress Security Plugin: Sucuri Scanner.

Трябва просто да Инсталираме и Активираме free Sucuri Security plugin. За повече подробности, виж нашето Ръководство „Стъпка по стъпка“ тук: how to install a WordPress plugin.

Когато го Активираме, извикваме Sucuri Меню от нашия WordPress admin. Най-напред ще трябва да Генерираме БЕЗПЛАТЕН API key. Така ще можем да правим Контролни влизания (Audit Logging), Проверка на Интегритета (Integrity Checking), да разпращаме email-Съобщения (email alerts) и други ВАЖНИ Действия.



От Меню „Настройки“ (Settings Menu), Избираме Закладка „По-голяма Сигурност“ (‘Hardening’ Tab). Обхождаме ВСИЧКИ Опции и Избираме Бутон „Прилагане на Засилени мерки“ (“Apply Hardening”).

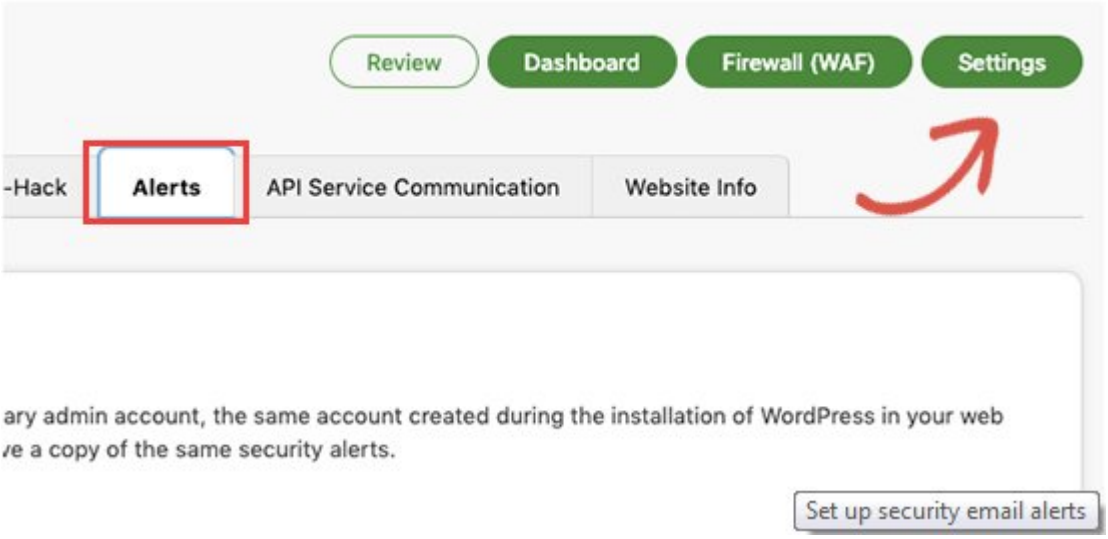


Споменатите Опции ни помагат да „Заключим“ основните Области, които Хакерите обичайно атакуват. Единствената ПЛАТЕНА Надстройка (Upgrade) за ПО-Голяма Безопасност е „Защитна стена на Web-Приложението“ (Web Application Firewall), която ще разгледаме при следващата Стъпка, така че на този етап я прескачаме.

По-нататък в настоящото Ръководство сме изложили множество подобни “Hardening” Опции за Ползвателите, които предпочитат да го направят без помощта на Plugin или за желаещите да предприемат ДОПЪЛНИТЕЛНИ Мерки, като „Смяна Префикса на Базата-данни“ (“Database Prefix change”) или „Промяна в Потребителското име на Admin”.

При вече ЗАСИЛЕНА Информационна безопасност, останалите Plugin-Настройки покриват Изискванията в повечето Web-Сайтове и не предполагат специални Промени. Препоръчваме единствено Персонализиране на „email-Уведомленията“.

Стандартните Настройки за Съобщения може да претрупат Пощенската ни кутия с Електронни съобщения. Съветваме да следите Уведомленията за Ключови събития, като: Промени в Plugin-и, Регистрация на Нови Ползватели и др.под. Уведомленията можем да Конфигурираме на: Sucuri Settings » Alerts.



Конкретният WordPress Security Plugin е изключително мощен: Обхождаме всичко Tab-ове и Настройки (Settings) и проследяваме всички предлагани възможности, като: Сканиране за Зловреден софтуер (Malware Scanning), Журнали при Инспектиране (Audit Logs), Отчетени Неуспешни опити за Влизане (Failed Login Attempt tracking) и др..

Активиране на Защитната Стена на Web-Приложението/Web Application Firewall (WAF)

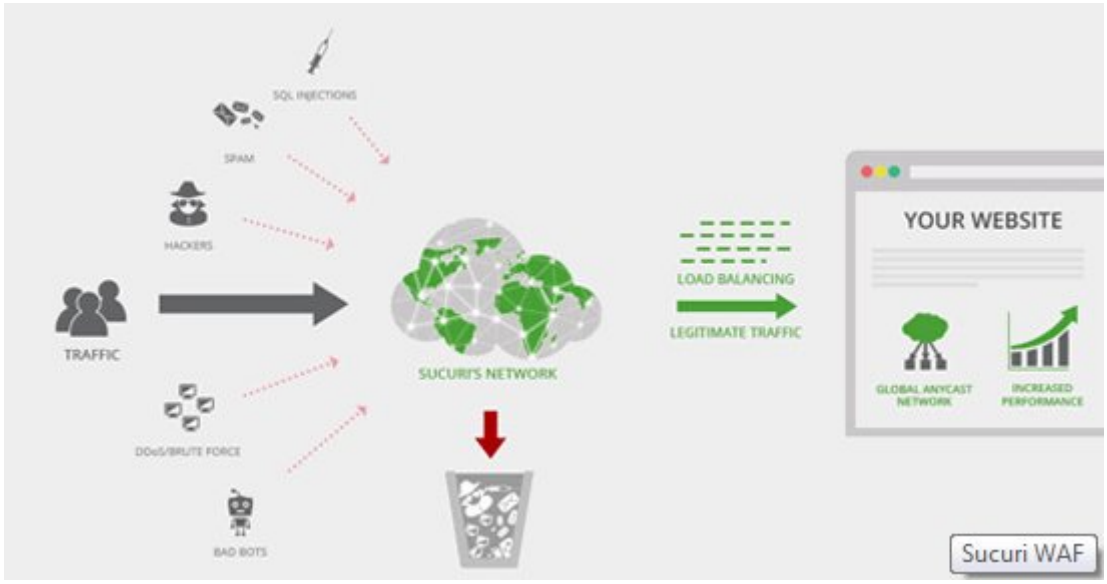
Най-лесният начин да Защитим нашия Сайт и да бъдем уверени в нашата WordPress Информационната безопасност, е като ползваме Web Application Защитната стена/Firewall (WAF).

Website Защитната стена БЛОКИРА всякакъв Злонамерен трафик, още преди да постъпи в нашия Web-Сайт.

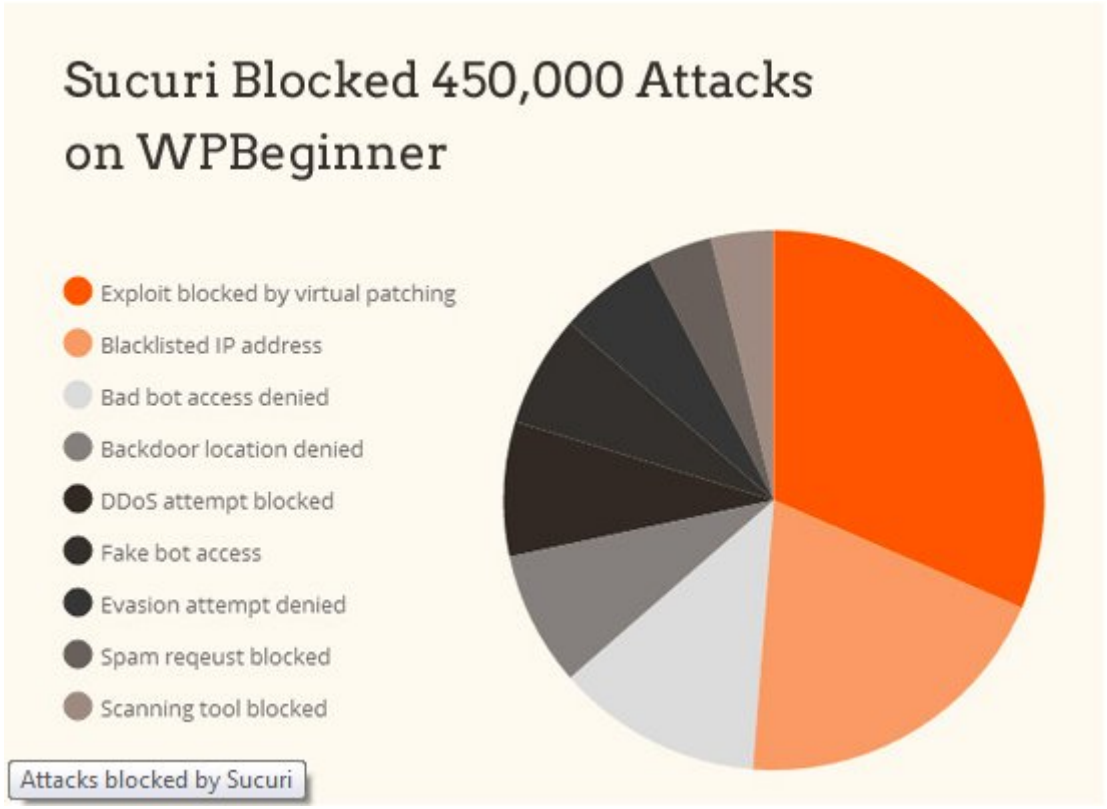
DNS Level Website Firewall – Защитната стена на Ниво: Услуга за Регистрация на Домейн (DNS), Рутира Трафика в нашия Сайт през Proxy Server-ите на Облака (Cloud) на Доставчика; до нашия Web-Сървър достига САМО ДЕЙСТВИТЕЛЕН Трафик.

Application Level Firewall – Plugin-ите за Защитна стена на Ниво „Приложение“ ИНСПЕКТИРАТ Трафика към нашия Server още преди да Зареди повечето WordPress Script-ове. Методът НЕ Е така Ефикасен в Редуциране Натоварването на Server-а, както Защитната стена на Ниво DNS.

Повече подробности вж. в нашия Списък „Най-удачни WordPress Firewall Plugin-и“ (best WordPress firewall plugins).



Персонално ние, **използваме и препоръчваме** Sucuri като НАЙ-ДОБРА Защитна стена на Ниво „Web-Приложение“ за WordPress. „Как с помощта на Sucuri, успяхме да БЛОКИРАМЕ 450000 WordPress Атаки за 1 месец“, можете да разберете на: “How Sucuri helped us block 450,000 WordPress attacks in a month”.



Най-позитивно при Защитната стена на Sucuri е това, че включва Опция за Изчистване на Зловреден софтуер (Malware Cleanup) и ГАРАНТИРАНО Изключване от „Черни списъци“ (Blacklist Removal Guarantee). Принципно, ако станем жертва на Хакери, докато сме под техен надзор, Sucuri Гарантирано ВЪЗСТАНОВЯВАТ Web-Сайта ни (независимо колко Страници съдържа).

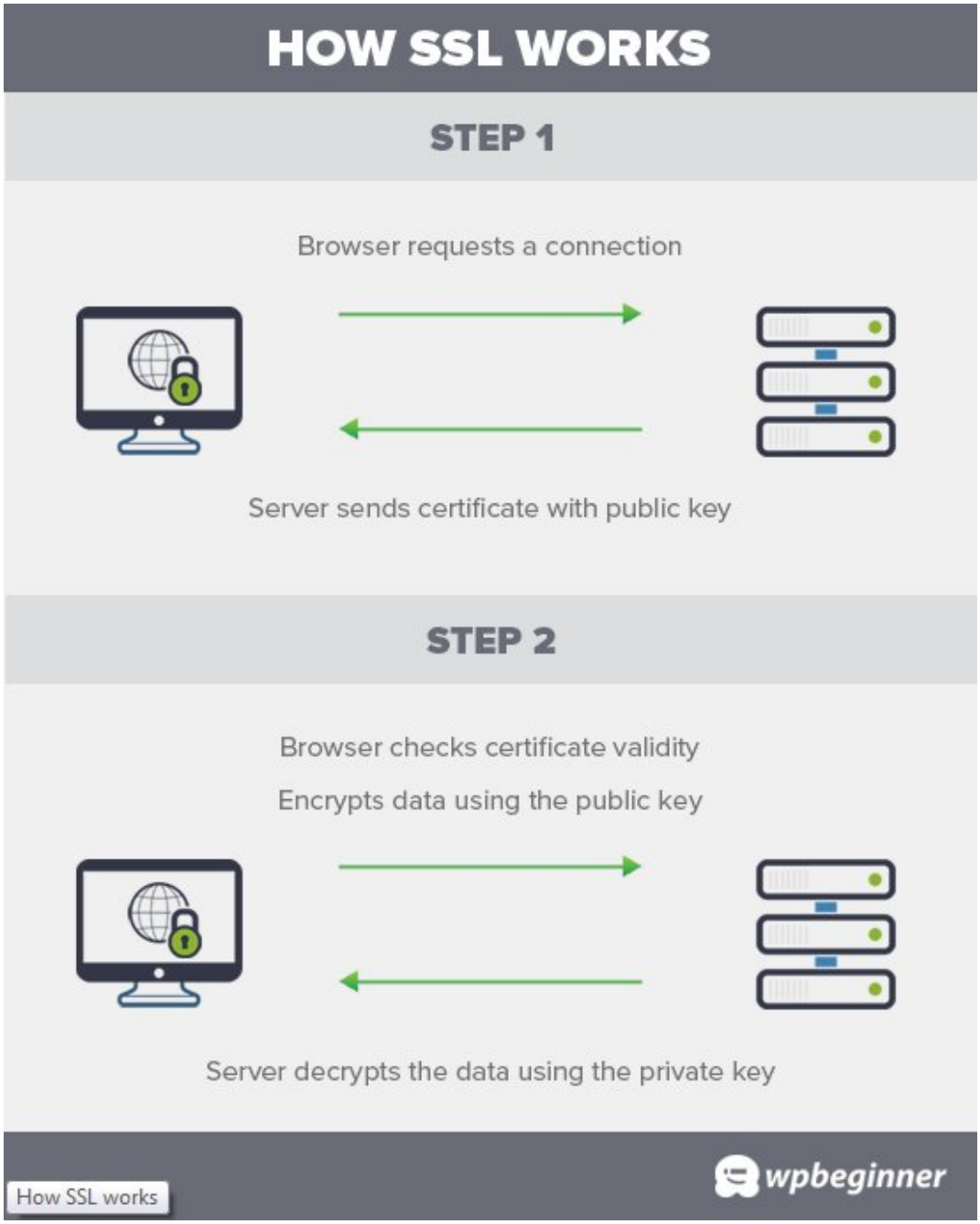
Подобна Гаранция е действително ПЪЛНА, защото включва ресурсоемко Възстановяване на Web-Сайтове и покрива обичайни Такси на Експерти от порядъка на $250 на час. И всичко това, в рамките на Sucuri Security Стека, получаваме срещу $199 на година.

Повишете Информационната безопасност на своя WordPress с Plugin-а Suciri. Improve your WordPress Security with the Sucuri Firewall »

Sucuri не са единствен Доставчик на Защитна стена на Ниво “DNS” на пазара. Друг важен участник в Бранша, са: Cloudflare. Виж Сравнителен анализ на: Sucuri vs Cloudflare (Pros and Cons).

Мигриране на WordPress Сайт към Кодиращ SSL-Слой/HTTPS

Кодиращ SSL-Слой (Secure Sockets Layer) е Протокол за Кодиран Трансфер на Данни между нашия Web-Сайт и Browser-а на Ползвателя. Кодирането възпрепятства Злонамерена намеса и Кражба на Информация.



При Активиран SSL, вместо HTTP, Web-Сайтът ни използва HTTPS и в Browser-а, редом с Адреса на Сайта ни, присъства Знак: 🔒.

SSL-Сертификати доскоро издаваха Сертифицирани служби и цените им варираха от $80 до стотици Долари ежегодно; ето защо, поради допълнителните разходи, множество Собственици на Web-Сайтове продължаваха да ползват досегашния „Несигурен“ Протокол.

В отговор на това, Организацията с Нестопанска цел: Let's Encrypt, започна да предлага Свободни (Free) SSL-Сертификати на Собствениците на Web-Сайтове. Проекта им подкрепят: Google Chrome, Facebook, Mozilla и множество други Компании.

Ето защо в наши дни, по-лесно от когато и да е, можем да използваме SSL за всички наши WordPress Web-Сайтове. Как правим това, вж. в нашето Ръководство „Стъпка по стъпка", на: How to get a free SSL certificate for your WordPress website.

WordPress Информационна безопасност за „Направи си сам" Ползватели (DIY Users)

Ако вече сте изпълнили гореизброените Стъпки, значи сте в подходяща форма.

Както винаги обаче, можем да допринесем с още доста за по-висока WordPress Информационна безопасност.

Възможно е някои от Стъпките по-долу да изискват известни познания по Програмиране.

Промяна на Стандартното Потребителско име: "admin"

В миналото, Стандартното Потребителско име на WordPress admin, бе: "admin". Доколкото, обаче, Потребителските имена предпоставят 50% от Правомощията при влизане, това улесняваше Хакерските опити за Нерегламентирана намеса (*Brute-Force Attacks).

WordPress резонно смениха тактиката и сега при Инсталиране на WordPress (Installing WordPress), трябва да Укажем СОБСТВЕНО (Custom) Потребителско име.

Все пак, някои "1-Click" WordPress Инсталатори, все още установяват Стандартното admin Потребителско име на: "admin". Ако при нас се случи нещо подобно, би било резонно да СМЕНИМ своя WordPress Web-Hosting (switch your web hosting).

Доколкото във WordPress по подразбиране НЕ МОЖЕМ да Променяме Потребителски имена, Usernames ПРОМЕНЯМЕ по някой от следните три начина:

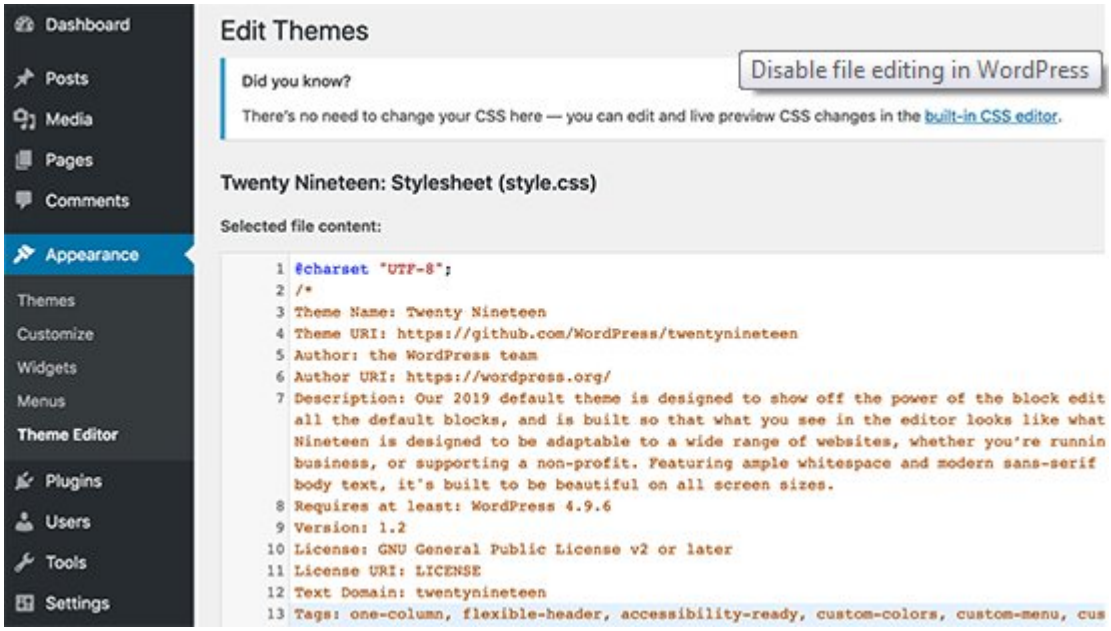
1. Създаваме Ново admin Username и Изтриваме старото.
2. Използваме Username Changer Plugin
3. Променяме Username от phpMyAdmin

Всяка от трите Стъпки сме представили в подробно Ръководство на: how to properly change your WordPress username (step by step).

Бележка: Коментираме Потребителско име: "admin", а НЕ Роля: Администратор.

Деактивиране Редактирането на Файлове (File Editing)

Във WordPress присъства вграден Редактор на Код (Code Editor), с който можем да Променяме нашите Theme- и Plugin-Файлове непосредствено от WordPress admin area. В зложелателни ръце, споменатата Функционална възможност (Feature) може да доведе до Риск в Безопасността и затова ПРЕПОРЪЧВАМЕ нейното Деактивиране.



Лесно можем да сторим това, като добавим следния Код към нашия wp-config.php Файл.

```
// Disallow file edit
define( 'DISALLOW_FILE_EDIT', true );
```

Същото можем да направим и с 1 Click с Мишката, чрез Hardening Опцията в Свободния Sucuri Plugin, за който вече споменахме.

Деактивиране Изпълнението на PHP-Файлове

Друг начин да засилим своята WordPress Информационна безопасност, е като Деактивираме Изпълнението на PHP-Файлове в Директориите, където такова НЕ СЕ НАЛАГА, като: /wp-content/uploads/.

Отварям Текстов редактор (Text Editor), като: Notepad и Paste-ваме следния Код:

```
<Files *.php>
deny from all
</Files>
```

Съхраняваме Файла като: **.htaccess** и го „качваме“ (Upload) в Папки: /wp-content/uploads/ на нашия Web-Сайт с помощта на FTP client.

По-подробни разяснения са изложени в нашето Ръководство, на: how to disable PHP execution in certain WordPress directories

Същото можем да направим и с 1 Click с Мишката, чрез Hardening Опцията в Свободния Sucuri Plugin, който по-горе споменахме.

Лимитирани Опити за Влизане/Login

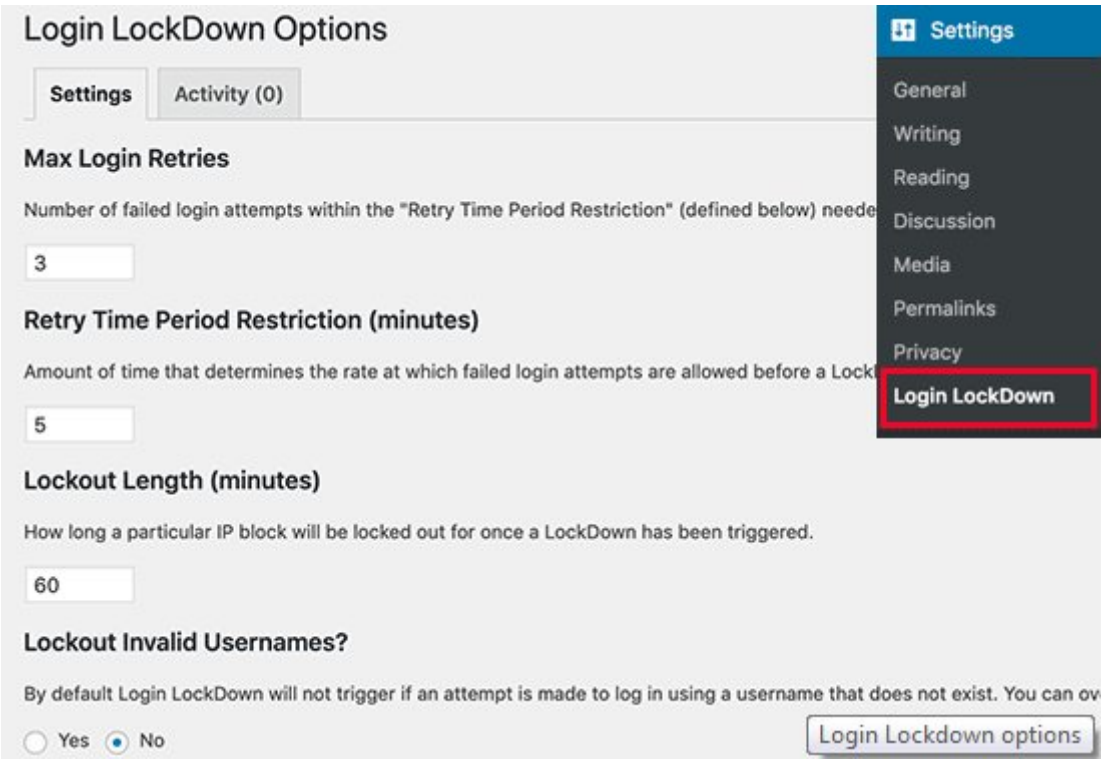
Стандартно, във WordPress на Ползвателите е позволен НЕОГРАНИЧЕН брой Опити за Влизане. Това прави WordPress-Сайта ни УЯЗВИМ от Неправомерни действия. Принципно, Хакерите „разбиват“ Пароли чрез ОПИТИ за Достъп с РАЗЛИЧНИ Комбинации.

Лесно можем да решим Проблема, ОГРАНИЧАВАЙКИ Броя Неуспешни опити за влизане на даден Ползвател. Вече споменатата Защитна стена на Ниво „Web-Приложение“, АВТОМАТИЧНО се грижи за това.

Ако все още не сме Инсталирали и Конфигурирали Защитната стена, сега е моментът да го сторим.

Започваме с Инсталиране и Активиране на Plugin: Login LockDown. Повече детайли сме изложили в нашето Ръководство „Стъпка по стъпка“, на: how to install a WordPress plugin.

При Активиране, отиваме на Страница: **Settings » Login LockDown** и Настройваме (Setup) Plugin-а.



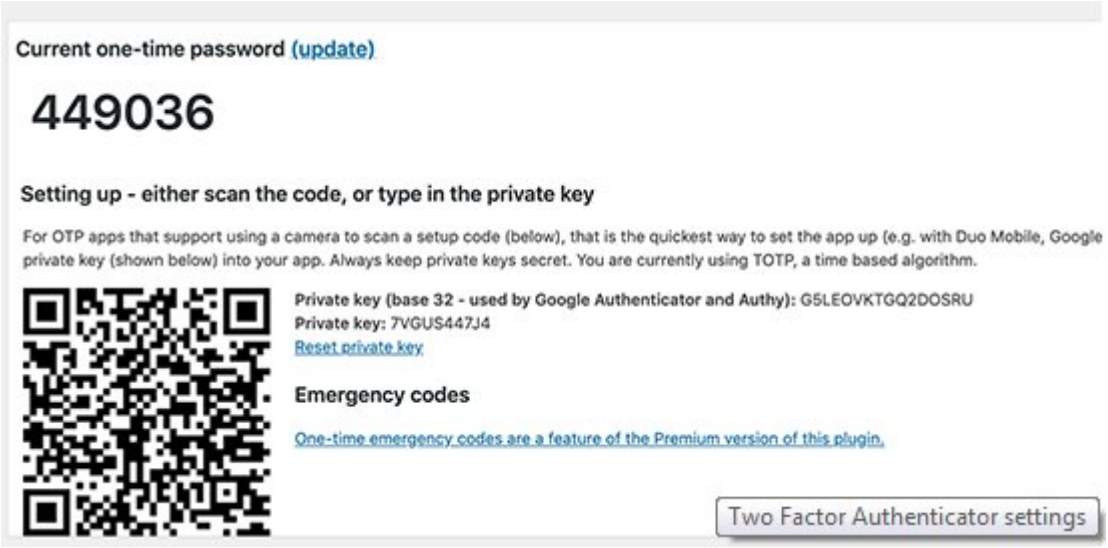
Подробни Инструкции са поместени в нашето Ръководство, на: how and why you should limit login attempts in WordPress.

Добавяне на Двуфакторно Идентифициране (Two Factor Authentication)

Методът: Двуфакторно Идентифициране, изисква Идентификацията при Влизане на Потребители да преминава през ДВЕ Стъпки. Първо са Потребителско име (Username) и Парола (Password), а Втора стъпка изисква УДОСТОВЕРЯВАНЕ на конкретно Устройство или Приложение (app).

Повечето водещи online Web-Сайтове, като: Google, Facebook и Twitter, ПОДДЪРЖАТ такава Опция за нашите Account-и. Въпросната Функционалност можем да добавим и към нашия WordPress Сайт.

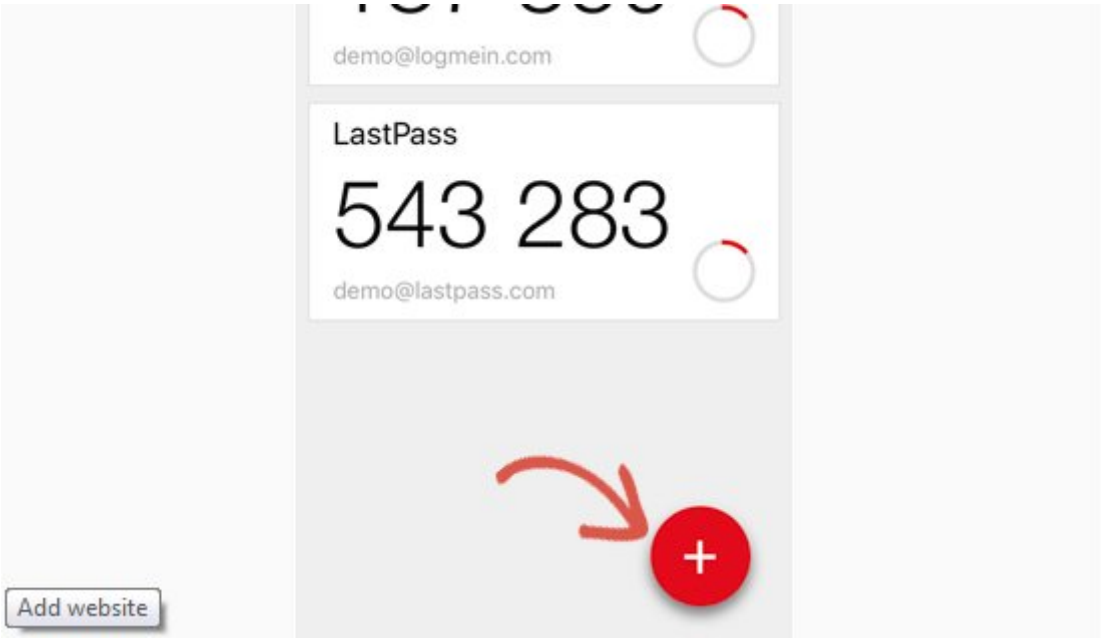
Най-напред, Инсталираме и Активираме Two Factor Authentication Plugin. При Активирането му, „щракваме“ върху ‘Two Factor Auth’ Link в нашия WordPress admin Sidebar.



Вследствие, Инсталираме и Отваряме Приложение за Идентифициране (Authenticator App) на нашия Телефон. Такива Приожения са: Google Authenticator, Authy и LastPass Authenticator.

Препоръчваме да се използва: LastPass Authenticator или Authy, защото и двете позволяват да Backup-ираме нашите Account-и на Облака (Cloud). Това е изключително ПОЛЕЗНО в случай, че Телефонът ни изчезне/изгуби Настройки или си купим нов Телефон. Лесно възстановяваме всички Login-Реквизити на нашия Account.

В Примера тук ще използваме LastPass Authenticator. Действията, обаче, са сходни и при другите Приложения за Идентифициране (Auth Apps). Отваряме нашето Authenticator App и Избираме Бутон: Add.



Следва Въпрос какво предпочитаме: самите ние да Заредим Сайта и или да Сканираме Bar Code-а. Избираме да Сканираме Bar Code-а и насочваме Камерата на нашия Телефон към QRcode-а, изведен на Страницата с Настройки на Plugin-а.

Готови сме. Идентифициращото ни Приложение съхранява Кода. При следващо Влизане в нашия Web-Сайт, след като Въведем Паролата, ще ни трябва и ДВУФАКТОРНИЯТ Идентификационен код.

Тогава отваряме Приложението за ИДЕНТИФИКАЦИЯ (Authenticator app) в нашия Телефон и Въвеждаме показания Код.

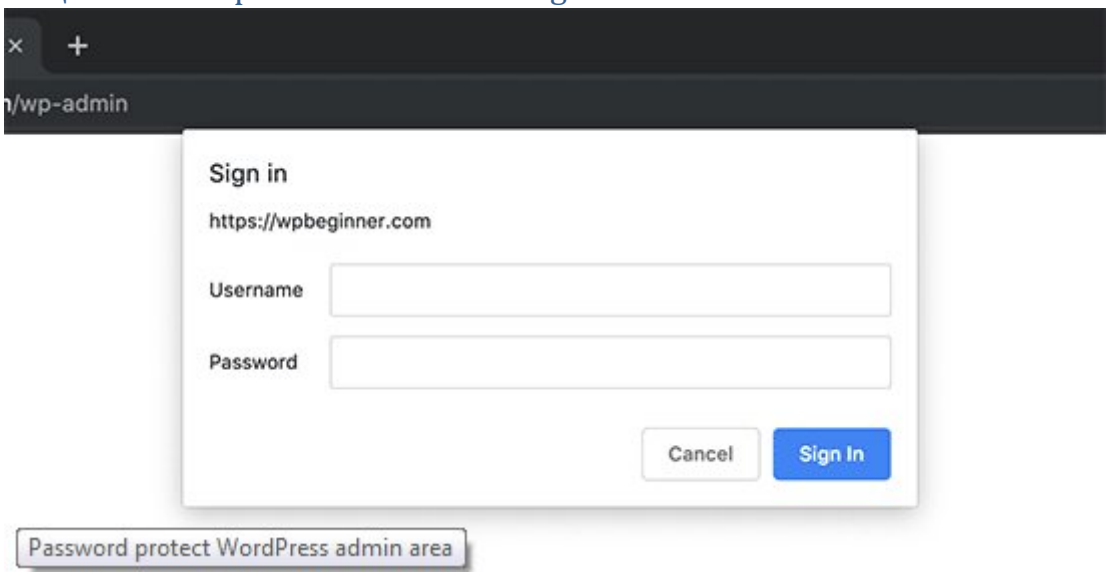
Промяна в Префикса на WordPress Базата-данни

Стандартно, WordPress задава Префикс wp_ на ВСИЧКИ Таблици в нашата WordPress database. Ако WordPress-Сайтът ни използва Стандартен Database Prefix, така улесняваме Хакерите в разкриване Името на наша Таблица. Затова е препоръчително да го променим.

Префикса на нашата База-данни ПРОМЕНЯМЕ, следвайки Ръководството „Стъпка по стъпка“, на: how to change WordPress database prefix to improve security.

Бележка: Споменатото Действие може да Разруши (Break) Сайта ни, ако някъде объркаме нещо. Предприемаме го единствено в случай, че сме сигурни в Уменията си по Програмиране.

Защитени с Парола WP-Admin и Login

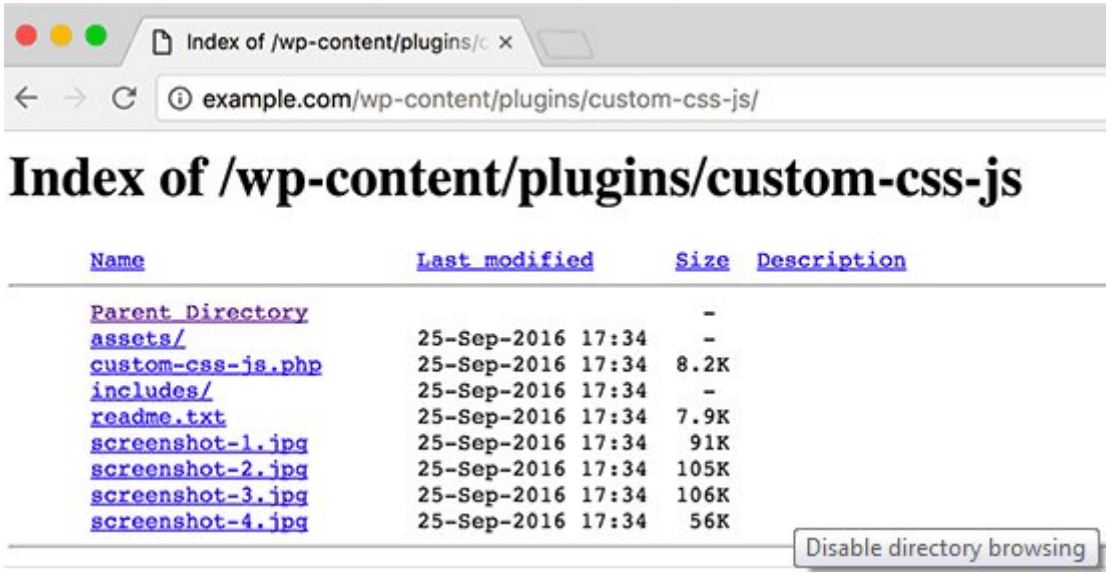


Обичайно, Хакерите имат НЕОГРАНИЧЕН Достъп до нашите wp-admin Папка и Login Page. Това улеснява опитите им за Нерегламентирана намеса и предприемането на DDoS Атаки.

С ДОПЪЛНИТЕЛНА зашита с Пароли на Ниво „Сървър“, ЕФИКАСНО можем да Блокираме подобни опити (Requests).

Следвайте нашите Инструкции „Стъпка по стъпка“, на: how to password protect your WordPress admin (wp-admin) directory.

Деактивиране Индексирането на Директории и Browse-ването



С Проследяване на Директориите (Directory Browsing), Хакерите могат да открият евентуално УЯЗВИМИ Файлове и така да си осигурят достъп.

Като Browse-ва Директориите, всеки може да разглежда Файловете ни, да Копира Изображения, да разбере нашата Структура Директории и друга информация. Поради това, СИЛНО Препоръчително е да ИЗКЛЮЧИМ Опциите за Индексиране на Директориите и Browse-ване.

Достъпваме нашия Web-Сайт с FTP или File Manager на cPanel и намираме .htaccess Файла в Главната Директория на Web-Сайта. Ако не откриваме Файла там, правим справка в Ръководството на: why you can't see .htaccess file in WordPress.

След това, ДОБАВЯМЕ следния Команден ред най-долу в .htaccess Файла:

```
Options -Indexes
```

ЗАДЪЛЖИТЕЛНО Съхраняваме Файл .htaccess и го „качваме" (upload) обратно в нашия Сайт. Повече информация по въпроса е изложена на: how to disable directory browsing in WordPress.

Деактивиране на XML-RPC във WordPress

Отдаленото Извикване на Процедури XML-RPC, бе Активиран ПО ПОДРАЗБИРАНЕ във WordPress 3.5, защото подпомагаше Свързването с Web- и Мобилни Приложения.

Големият Потенциал на XML-RPC може съществено да улесни Нерегламентирани посегателства.

Принципно, ако някой Хакер иска да пробва 500 различни Пароли на нашия Web-Сайт, ще се му нужни 500 отделни Опита за Влизане (Login) и това ще бъде Разкрито и Блокирано от login lockdown plugin-а.

С XML-RPC обаче, Хакерът, с помощта на Функция: **system.multicall**, може да пробва хиляди Пароли с някакви си 20 или 50 Обръщения (Request-а).

Ето защо, при липса на изрична потребност, най-добре е да Деактивираме (Disable) XML-RPC.

XML-RPC във WordPress можем да Деактивираме по 3 Начина, всеки от които е представен в съответно Ръководство „Стъпка по стъпка", на: how to disable XML-RPC in WordPress.

Ориентир: Методът с .htaccess е НАЙ-ДОБЪР, защото Ангажира МИНИМАЛЕН Ресурс.

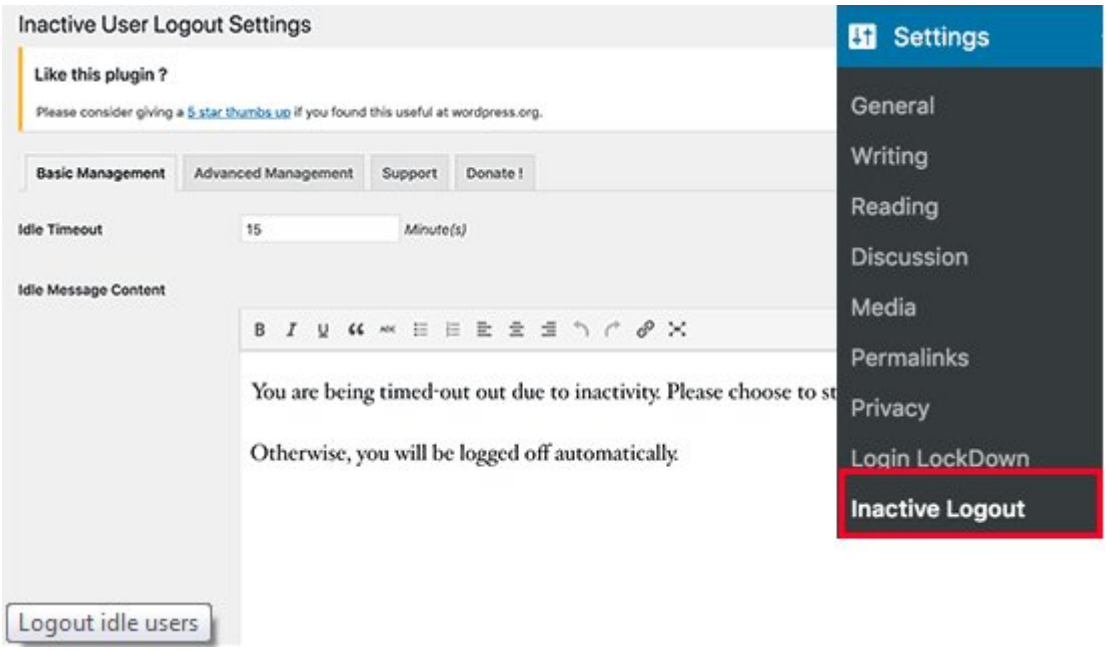
Ако ползваме вече споменатата Защитна стена на Ниво „Web-Приложение“, за същото ще разчитаме на Защитната стена (Firewall).

Автоматично Изключване (Log out) на Неактивните ползватели (Idle Users)

Log-натите Потребители понякога са отвлечени от нещо друго настрани, което поражда Рискове в Безопасността. Някой друг може да седне зад Компютъра им, да СМЕНЯ Пароли или да ПРОМЕНЯ Настройки в техния Account.

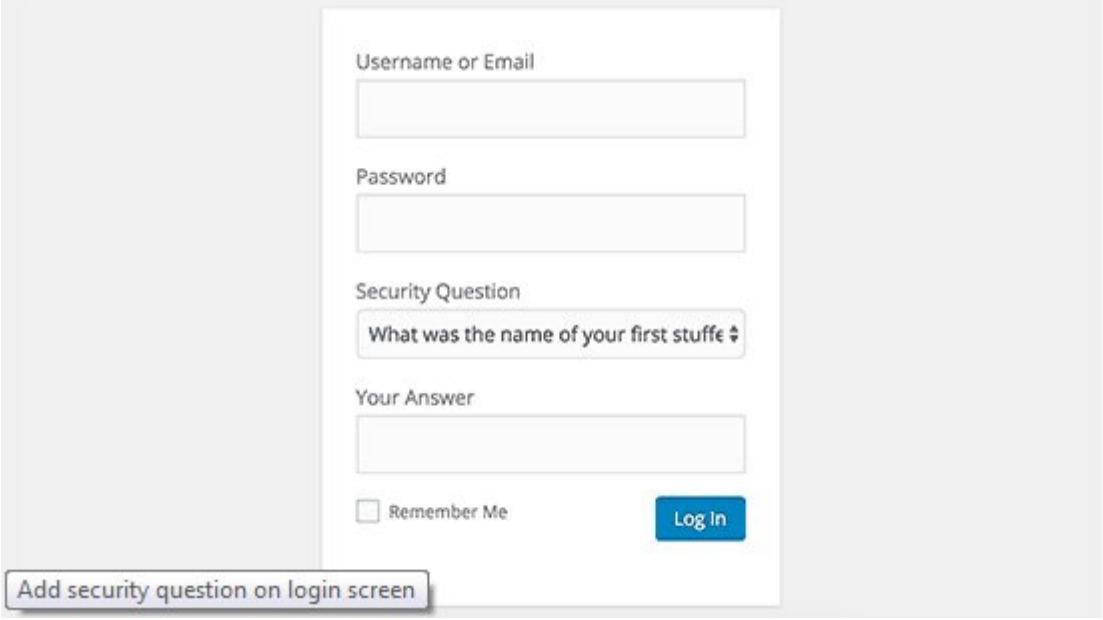
По същата Причина, множество Банкови и Финансови Сайтове АВТОМАТИЧНО „изхвърлят“ (Log out) Неактивен потребител. Подобна Функционалност можем да заложим и ние, в нашия WordPress-Сайт.

Ще трябва да Инсталираме и Активираме Plugin-а: Inactive Logout. За Активиране, отиваме на Страница: **Settings » Inactive Logout** и Конфигурираме Настройките на Plugin-а.



Най-общо, Указваме Времеви интервал и Съставяме „Съобщение, че Сесията се Прекратява“ (Logout Message). ЗАДЪЛЖИТЕЛНО Запомняме Настройките с Избиране на Бутон: „Съхранение“.

Добавяне на Контролен въпрос (Security Questions) при WordPress Login



Добавяйки Контролен въпрос към нашия WordPress Login Екран, допълнително ЗАТРУДНЯВАМЕ Опитите за Неоторизиран достъп.

Контролни въпроси можем да добавим, като Инсталираме WP Security Questions Plugin. Когато го Активираме, трябва да отидем на Страница: Settings » Security Questions и там да Укажем Настройките на Plugin-а.

По-детайлни Инструкции можем да намерим в Ръководството на: how to add security questions to WordPress login screen.

Сканиране на WordPress за Зловреден софтуер (Malware) и Уязвими места (Vulnerabilities)

Ако имаме Инсталиран WordPress Security Plugin, той СТАНДАРТНО Проверява за Зловреден софтуер (Malware) и ни Информира за ПРОБИВИ в Сигурността.

Ако, все пак, констатираме драстичен/-но Срив в Трафика на Web-Сайта/изоставане в Класацията на Търсещите машини (Search Rankings), резонно е да направим Сканиране.

Можем да ползваме нашия WordPress Security Plugin или някой измежду изброените: malware and security scanners.

Подобно online-Сканиране е РУТИНЕН Процес: въвеждаме URL-Адресите на нашия Web-Сайт и техните „Паяци“ (Crawlers) Инспектират Web-Сайта ни за познати Нерегламентиран софтуер и Зловреден код.

Нека не забравяме, че повечето WordPress Security Scanners ЕДИНСТВЕНО Сканират нашия Web-Сайт, но НЕ МОГАТ да Премахнат Нерегламентирания код, нито да Изчистят WordPress-Сайт от Зловредни изменения.

Това ни води до следващия Раздел за Почистване на Зловреден софтуер и Изчистване последствията от Външна намеса във WordPress Сайтове.

Разчистване на Зловредни изменения вследствие Външна намеса във WordPress Сайт

Много WordPress Ползватели не осъзнават ПРИОРИТЕТА на Архивните копия (Backups) и Информационната безопасност на един Web-Сайт, докато Сайтът им действително не пострада.

Профилактиката на един WordPress Сайт може да бъде изключително трудна и времеемка. Непосредственият отговор е: Доверете се на професионалист.

Хакерите Инсталират „Задни врати“ (backdoors) на атакуваните Сайтове, които ако не премахнем радикално и навреме, ги правят уязвими от последващи атаки на Зложелатели.

Привличането на специализирана Компания, като: Sucuri да Възстанови нашия Web-Сайт, е гаранция за текущо изрядното му състояние. Можем да разчитаме на Превенция и при последващи Атаки.

За по-авантюристични и за Ползватели „Направи си сам“, сме предоставили Ръководство „Стъпка по стъпка“, на: fixing a hacked WordPress site.

Това е всичко. Надяваме се Ръководството да ви е запознало с НАЙ-Добрите Практики на WordPress Информационната безопасност, насочвайки ви към най-добрите WordPress Security Plugin-и в конкретния случай.

Ако Материалът ви е бил полезен, Абонирайте се в YouTube Channel за нашите WordPress Видео-уроци (Video Tutorials). Можете да ни намерите и в Twitter и Facebook.

Издателски колектив

Издателски колектив на WPBeginner са група WordPress експерти, ръководен от Syed Balkhi, с над 1300000 читатели в глобален мащаб.