



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

Last updated on March 7th, 2019 by [Editorial Staff](#)

BEGINNER'S GUIDE FOR WORDPRESS

Start your WordPress Blog in minutes



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 владетели 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 следват максима, че Безопасността не касае единствено ПРЕДПАЗВАНЕ от Риска. Тя касае и МИНИМИЗИРАНЕ на Риска. Като собственик на Web-Сайт, следва да предприемем редица мерки за по-добрата Безопасност на нашия WordPress-Сайт (дори и в случай, че не сме Tech-експерти).

Разполагаме с богат Арсенал инструменти, които можем да използваме в защита на Уязвими места/Безопасността в/на нашия Web-Сайт.

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

Съдържание

Основи на WordPress Информационната безопасност	4
Кое прави Информационната безопасност на WordPress така важна?.....	4
Поддържане на WordPress Актуализиран.....	5
Сигурни Пароли и Потребителски правомощия (Strong Passwords and User Permissions).....	5
Значение на Web-Хостинга	6
WordPress Информационна безопасност в ЛЕСНИ Стъпки (БЕЗ да се нуждаем от Умения по Програмиране).....	6
Инсталиране на WordPress Backup Solution	7
Най-добър WordPress Security Plugin.....	7
Активиране на Защитната Стена на Web-Приложението/Web Application Firewall (WAF)	9
Мигриране на WordPress Сайт към Кодиращ SSL-Слой/HTTPS	11
WordPress Информационна безопасност за „Направи си сам“ Ползватели (DIY Users)	12
Промяна на Стандартното Потребителско име: “admin”	12
Деактивиране Редактирането на Файлове (File Editing)	12
Деактивиране Изпълнението на PHP-Файлове	13
Лимитиране Опитите за Влизане/Login.....	13
Добавяне на Двухфакторно Идентифициране (Two Factor Authentication)	14
Промяна в Префикса на WordPress Базата-данни	16
Защитени с Парола WP-Admin и Login.....	16
Деактивиране Индексирането на Директории и Browse-ването.....	17
Деактивиране на XML-RPC във WordPress.....	17
Автоматично Изключване (Log out) на Неактивните ползватели (Idle Users).....	18
Добавяне на Контролен въпрос (Security Questions) при WordPress Login.....	19
Сканиране на WordPress за Зловреден софтуер (Malware) и Уязвими места (Vulnerabilities).....	19
Ликвидиране на Зловредни изменения вследствие Външна намеса във WordPress Сайт	20
Разяснителни бележки	21
Що е Security Activity Auditing?	21
Що е File Integrity Monitoring?	22
Що е Remote Malware Scanning?.....	22
Що е Blacklist Monitoring?	22

Що е Effective Security Hardening?	23
Какво включват Post-Hack Security Actions?.....	23
Що са Security Notifications?	23
Що е Website Firewall (premium)?	23
Кое е това , което нашият Plugin прави, а другите Security Plugin-и - не?.....	24
Ако Инсталираме Sucuri Security Plugin, имаме ли право на Sucuri Account?	24
Ако имаме Premium Plugin-а, ще ни трябва ли Свободният (Free) Plugin?	24
Ще ни трябват ли други Sucuri-Продукти, ако имаме Sucuri Security Plugin?	24
Откъде получаваме Поддръжка за въпросния Plugin?.....	24
В КОНФЛИКТ ли е Plugin-ът ни с WordFence?	24
Какви са Ограниченията на Remote Malware Scanner при Отдалечено Сканиране за Зловреден софтуер?	25
Plugin-ът ни НЕ ИДЕНТИФИЦИРА Зловреден софтуер	25
Безплатно ли е Активирането на Защитната стена?.....	25
Ще Повлияе ли Plugin-ът на Поведението и Производителността (Performance) на нашия Web-Сайт?.....	25
Log-овете в моята База-данни ли се Съхраняват?	25
Възможни ли са Проблеми с Инсталирането на Plugin-и при някои Host-ове?.....	25
Нужен ли ни е този Plugin, за да ползваме Услуга Website Firewall?	25
Каква Информация събира Sucuri?	26

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 навредят на 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.



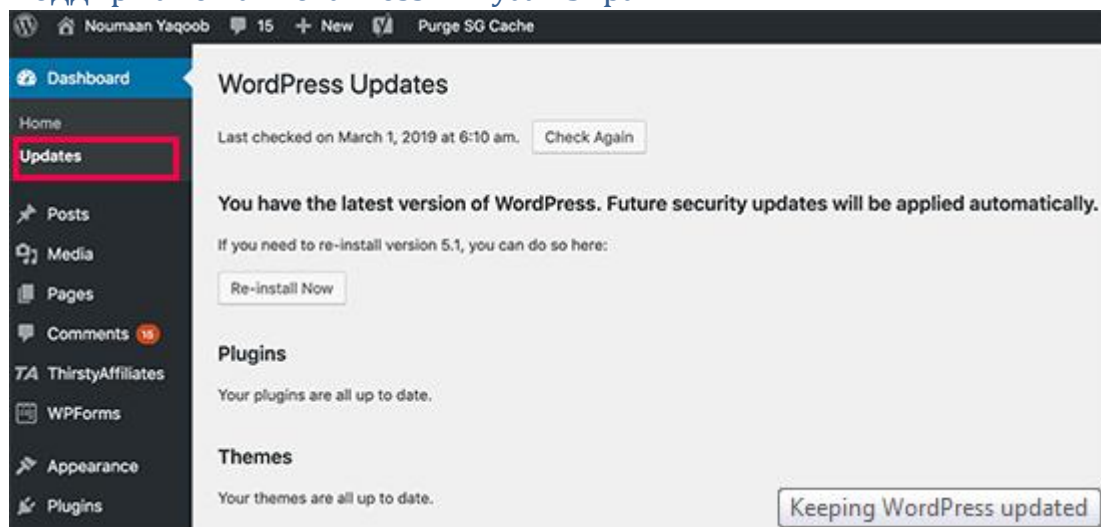
През март 2016 от Google докладваха, че над 50 милиона Посетители на Web-Сайтове са били предупреждавани, че посещаваният от тях Web-Сайт вероятно е заразен с Вируси, че в него присъства Зловреден софтуер или ползва с корисни цели тяхна Информация.

В допълнение, Google публикуват Черен списък с около 20,000 Web-Сайта за Зловреден софтуер и около 50,000 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 владеец на Online Бизнес, имаме ангажимент по 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-древни Update-и, докато Актуализации на Основните версии правим самите ние: „на ръка“.

Във WordPress присъстват хиляди Plugin-и и Theme-и, подходящи 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 въздържахме 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. Справка: в нашето Ръководство [how to manage WordPress passwords](#) [тук](#).

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

Предоставяната ни [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 какви регулярни Мерки предприема 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.
- Имат готови Планове за ВЪЗСТАНОВЯВАНЕ след Срив и при Инциденти, с цел да могат да предпазят Данните ни в случай на крупна злополука.

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

Използването на [managed WordPress hosting](#) Услуга предполага в по-сигурна Платформа за нашия Web-Сайт. Компаниите-Доставчици на Managed WordPress hosting провеждат Автоматично Архивиране (Automatic Backups), Автоматични WordPress Update-и и предоставят ПО-Безопасни Конфигурации за СИГУРНА Защита на нашия Web-Сайт.

Авторите ПРЕПОРЪЧВАТ [WPEngine](#) като Managed WordPress Hosting Доставчик – техен фаворит. Компанията е сред НАЙ-РЕНОМИРАНИТЕ Представители на Бранша. (вж. нашия специален [WPEngine coupon](#)).

WordPress Информационна безопасност в ЛЕСНИ Стъпки (БЕЗ да се нуждаем от Умения по Програмиране)

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

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

Ще разясним как можем да подобрим WordPress Информационната безопасност със само няколко Click-а (без да трябва да пишете Код).

Предостатъчно е да можем да Позиционираме Мишката и да Щракаме 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 Архивите (Backups) е РЕДОВНО да правим ПЪЛЕН Backup на Сайта на Външен носител (различен от нашия Hosting Account).

Препоръчително е Съхранението да става 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.

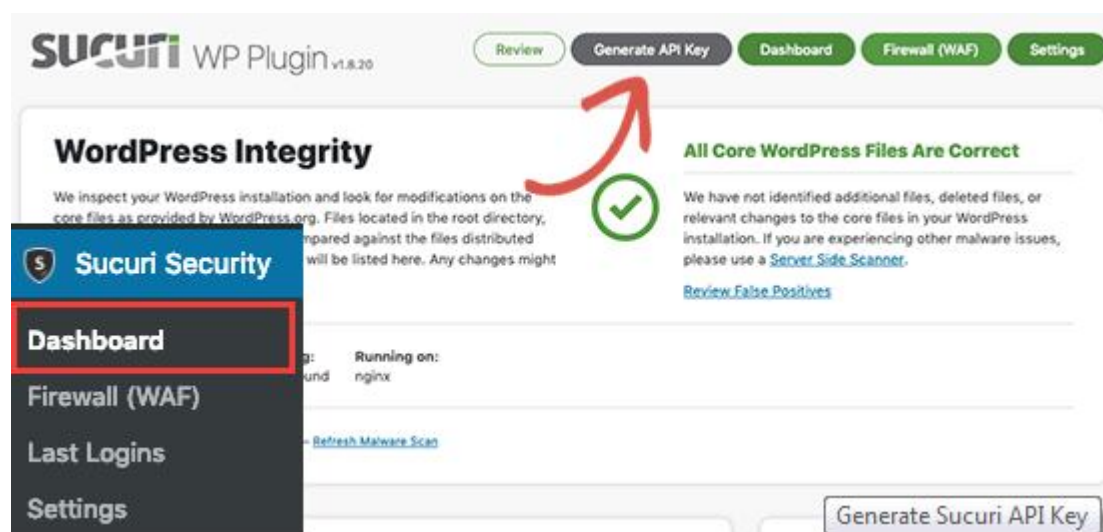
Това включва СЛЕДЕНЕ за Файлов ИНТЕГРИТЕТ (File Integrity Monitoring) и на НЕУСПЕШНИ Опити за Влизане, Сканиране за Зловреден софтуер (Malware Scanning) и пр..

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

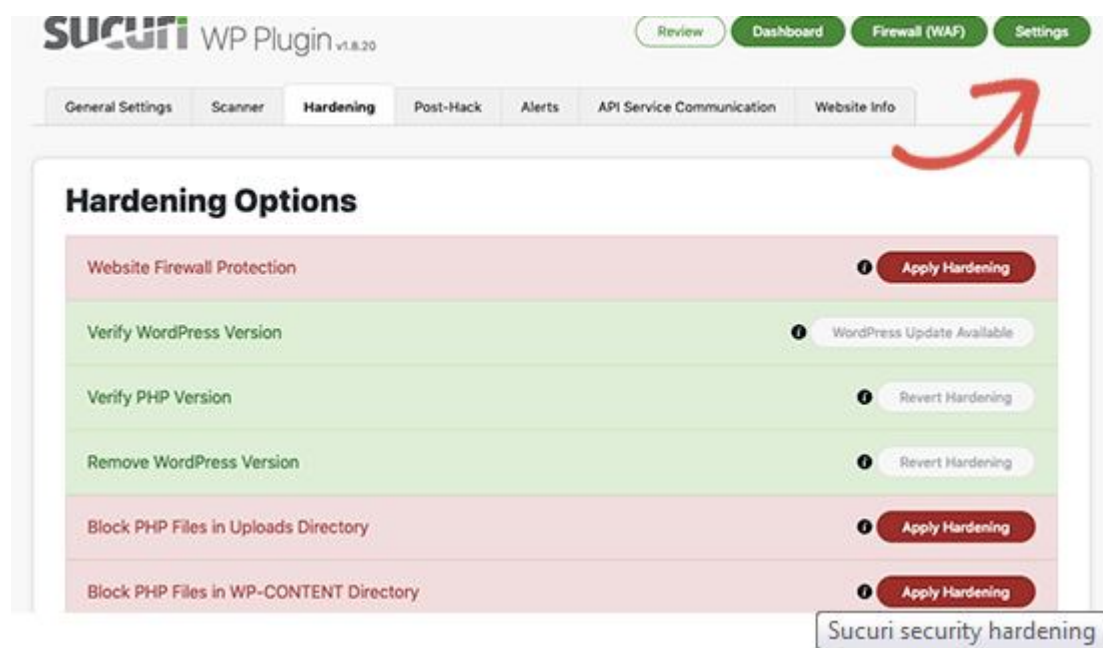
Трябва просто да Инсталираме и Активираме [free Sucuri Security plugin](#). За повече подробности, виж нашето Ръководство „Стъпка по стъпка“ тук: [how to install a WordPress plugin](#).

При неговото Активиране, извикваме Sucuri Меню от нашия WordPress admin. Най-напред трябва да Генерираме БЕЗПЛАТЕН [API key](#). Така ще можем да правим

ПРОСЛЕДЯВАНЕ на Промените (Audit Logging/[Activity Auditing](#)), да провеждаме Проверки за Интегритет (Integrity Checking/[Integrity Monitoring](#)), разпращане на Уведомления по email (email alerts) и други ВАЖНИ Дейности.



От Меню „Настройки“ (Settings Menu), Избираме Закладка „[По-голяма Безопасност](#)“ (‘Hardening’ Tab). Обхождаме една по една Опциите и за ВСЯКА, Избираме Бутон „Засилени мерки“ (“Apply Hardening”).

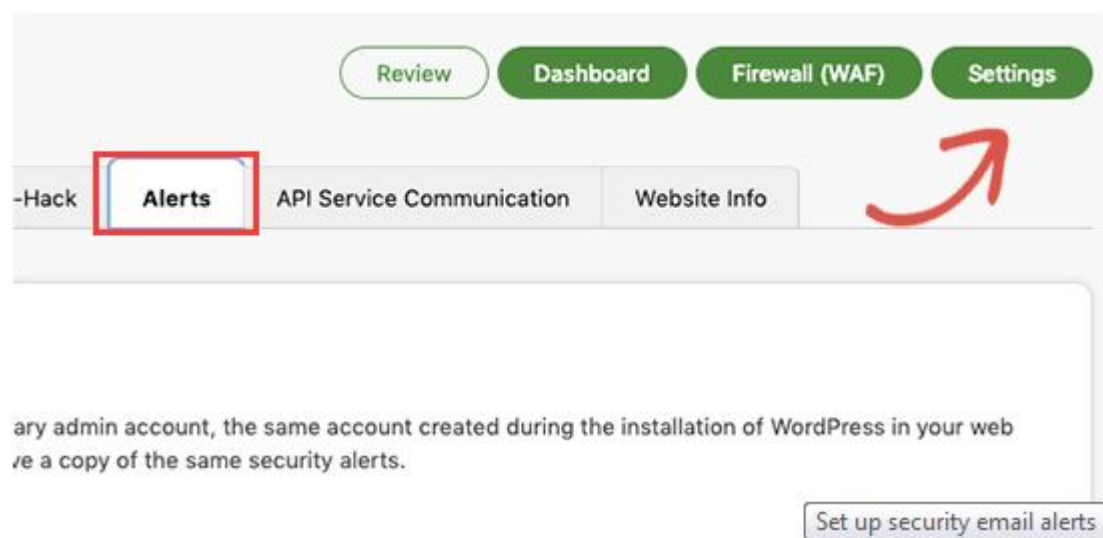


Споменатите Опции ни помагат да „Заклучим“ основните Области, които Хакерите обичайно атакува. Единствената ПЛАТЕНА Надстройка (Upgrade) за ПО-Голяма Безопасност е Защитна стена на Ниво „Web-Приложение“ (Web Application Firewall), която разглеждаме при следващата Стъпка, така че тук ще я пропуснем.

По-нататък в настоящото Ръководство сме изложили множество сходни “Hardening” Опции за Ползватели, предпочитащи да не ползват 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 при 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: Изменения 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 всички Tab-ове и Настройки (Settings), проследяваме и избираме всички предоставяни ни Опции, като: Сканиране за Зловреден софтуер (Malware Scanning), Журнали „Промени“ (Audit Logs), Проследени Неуспешни опити за Влизане (Failed Login Attempt tracking) и др..

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

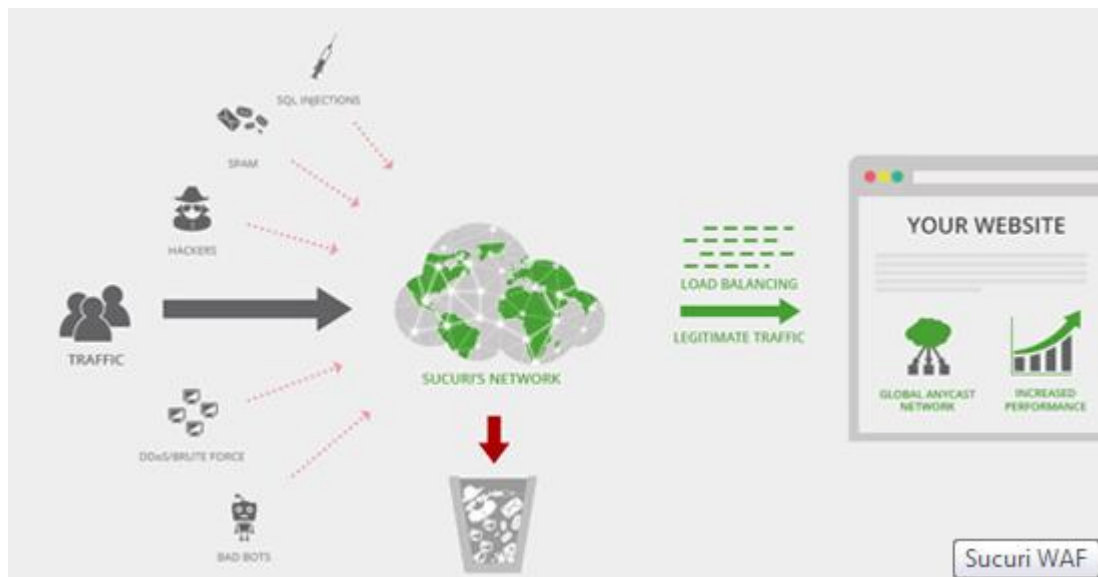
Най-удобен прием да Защитим нашия Сайт и да сме спокойни за нашата WordPress Информационна безопасност, е като ползваме Защитната стена на Ниво „Web-Приложение“ Web Application Firewall (WAF).

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

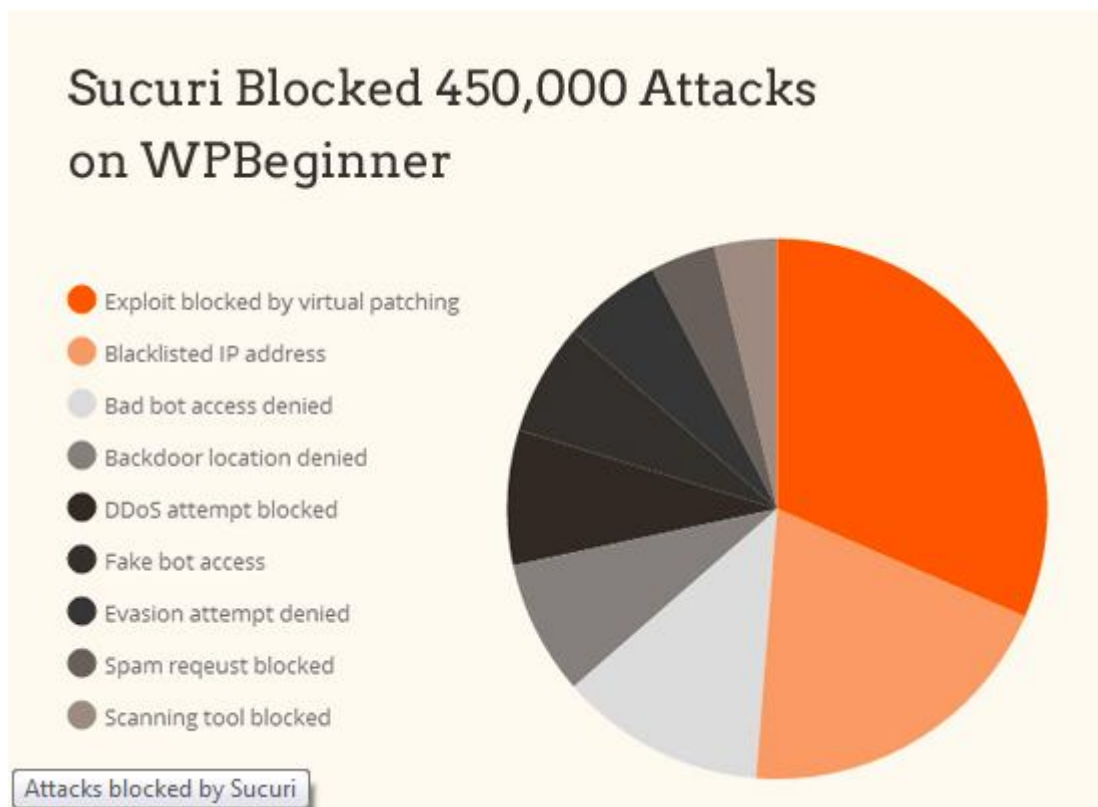
DNS Level Website Firewall – Защитната стена на Web-Сайт на Ниво: Услуга за Регистрация на Домейн (DNS), Рутира Трафика в нашия Сайт през Proxy Server-ите на Облака (Cloud) на Доставчика; до нашия Web-Сървър достига САМО ДЕЙСТВИТЕЛЕН Трафик.

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”.

За повече подробности, вж. нашия Списък с „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 450,000 WordPress Атаки за 1 месец“, можете да разберете на: “How [Sucuri helped us block 450,000 WordPress attacks in a month](#)”.



Най-съществено при Защитната стена на Sucuri е това, че предоставя 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).

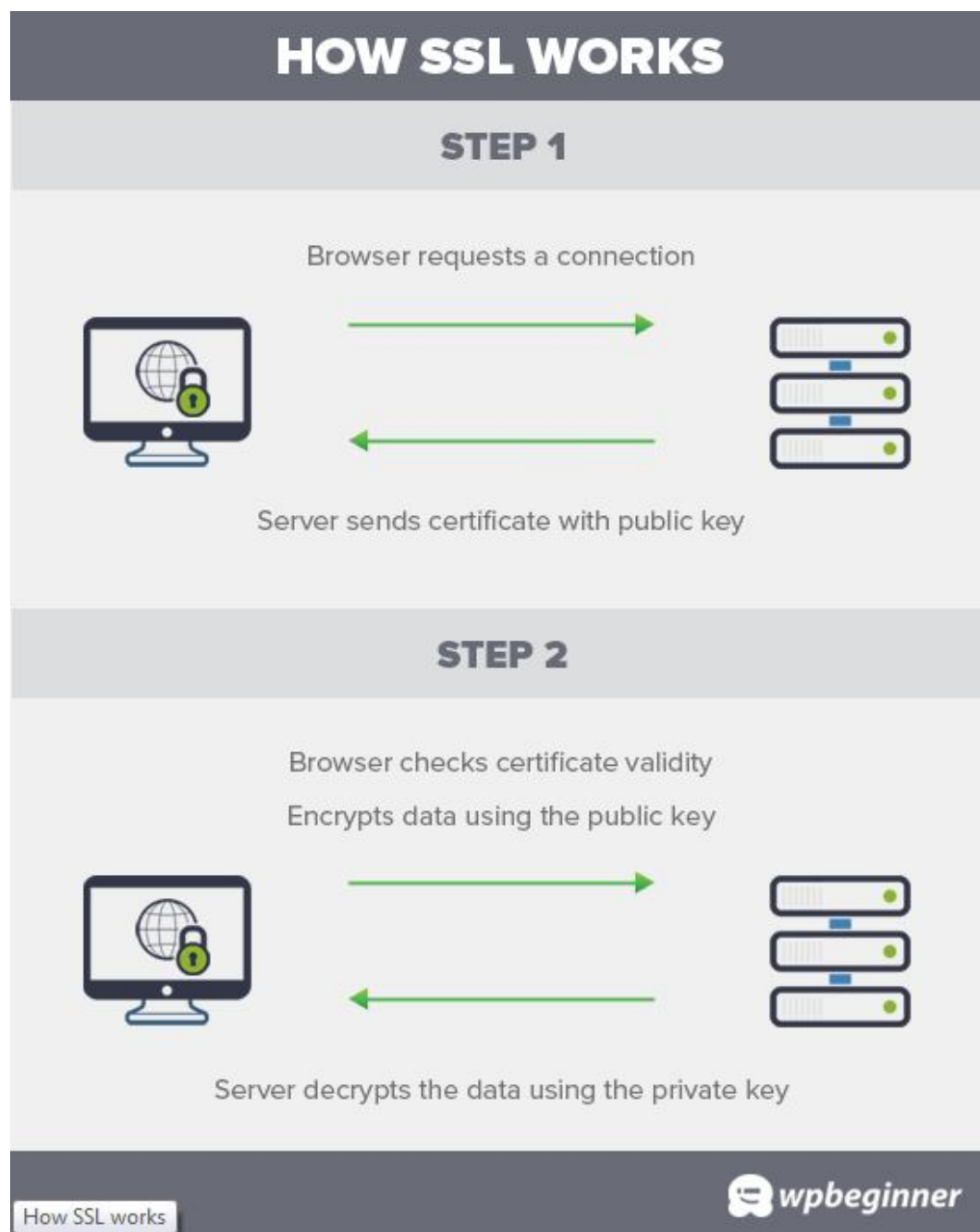
Подобна Гаранция е действително ПЪЛНА, защото касае ресурсоемко Възстановяване на Web-Сайтове и покрива обичайни Такси на Експерти от порядъка на \$250 на час. И всичко това, в рамките на Sucuri Security Стека, получаваме срещу \$199 на година.

Повишете Информационната безопасност на своя WordPress с Plugin-a Sucuri. [Improve your WordPress Security with the Sucuri Firewall »](#)

[Sucuri](#) не са единствен Доставчик на Защитна стена на Ниво “DNS” на пазара. Друг важен представител на 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. Проектът им е подкрепян от: [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“: 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, резонно би било да предприемем СМЯНА на настоящия 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:

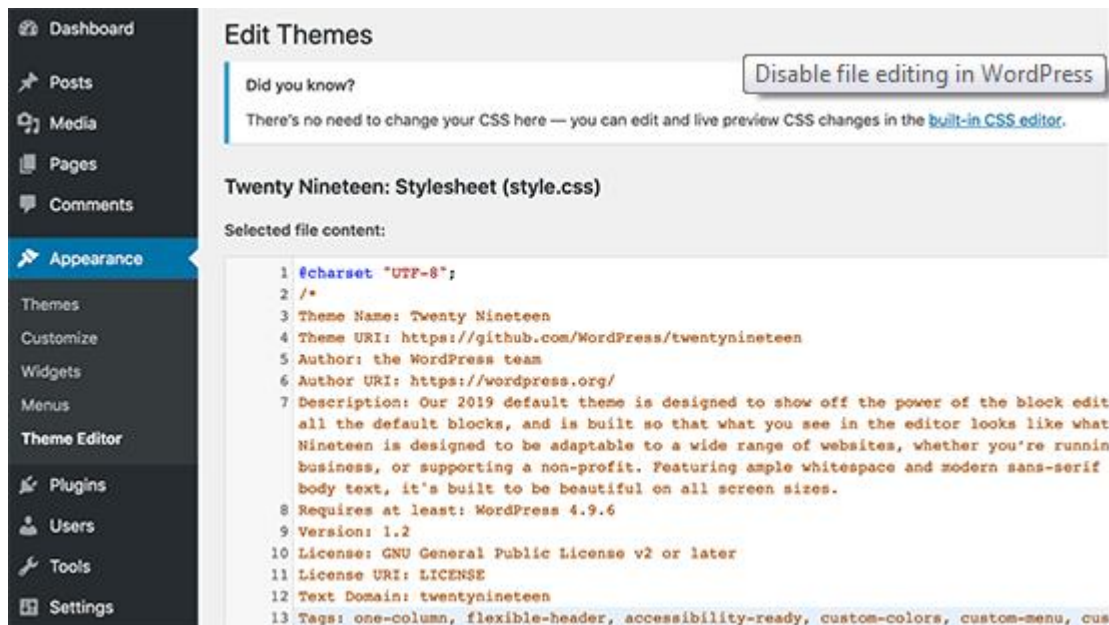
1. Създаваме Ново admin Username и Изтриваме старото.
2. Използваме [Username Changer](#) Plugin
3. Променяме Username от phpMyAdmin

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 нейно Деактивиране.



Лесно можем да сторим това, като добавим следния Код към нашия [wp-config.php](#) Файл:

```
1 // Disallow file edit
2 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

Допълнителна мярка за повишаване на WordPress Информационната ни безопасност, е да Деактивираме Изпълнението на PHP-Файлове в Директориите, където такова НЕ СЕ НАЛАГА, от типа на: /wp-content/uploads/.

Отваряме Текстов редактор (Text Editor) , например: Notepad и Paste-ваме следния Код:

```
1 <Files *.php>
2 deny from all
3 </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: [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.

Лимитиране Опитите 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-a.

Login LockDown Options

Settings Activity (0)

Max Login Retries
Number of failed login attempts within the "Retry Time Period Restriction" (defined below) needed to trigger a LockDown.

Retry Time Period Restriction (minutes)
Amount of time that determines the rate at which failed login attempts are allowed before a LockDown is triggered.

Lockout Length (minutes)
How long a particular IP block will be locked out for once a LockDown has been triggered.

Lockout Invalid Usernames?
By default Login LockDown will not trigger if an attempt is made to log in using a username that does not exist. You can override this.
☐ Yes ☒ No

[Login Lockdown options](#)

Settings
General
Writing
Reading
Discussion
Media
Permalinks
Privacy
Login LockDown

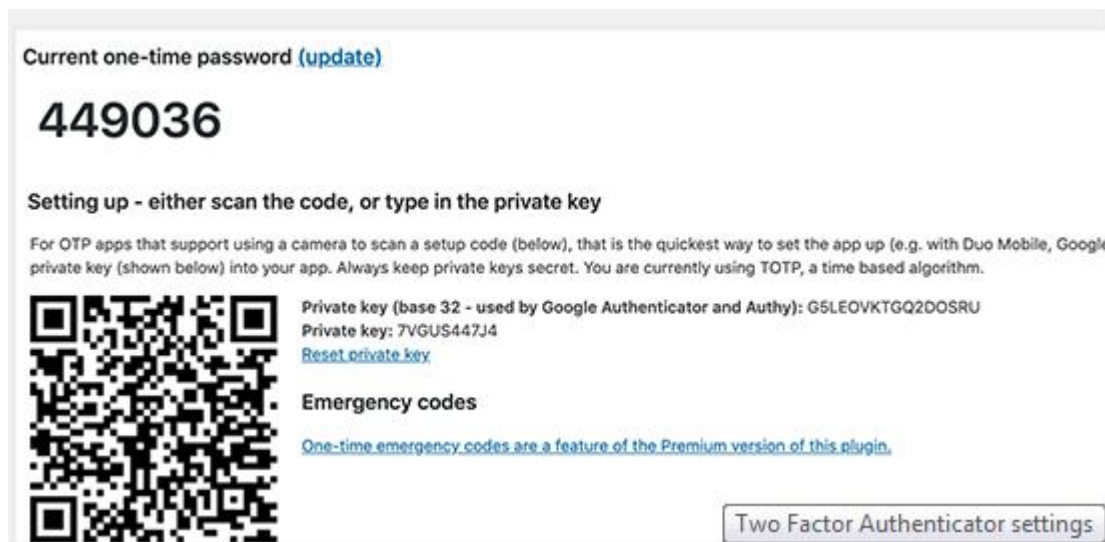
Подробни Инструкции са поместени в нашето Ръководство, на: [how and why you should limit login attempts in WordPress](#).

Добавяне на Двухфакторно Идентифициране (Two Factor Authentication)

Методът: Двухфакторно Идентифициране, изисква Идентификацията при Влизане на Потребители да преминава през ДВЕ Стъпки. Първо: Потребителско име (Username) и Парола (Password), а на 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. Такава Функционалност можем да добавим и към нашия WordPress Сайт.

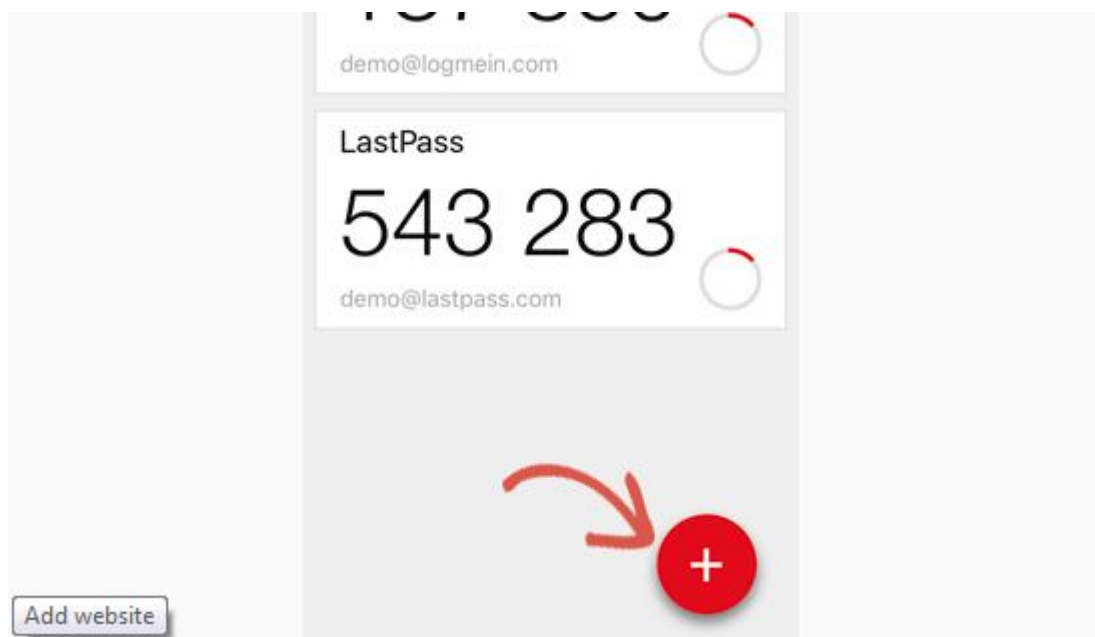
Най-напред, Инсталираме и Активираме [Two Factor Authentication](#) Plugin. При Активирането му, „щракваме“ върху ‘Two Factor Auth’ Link в нашия WordPress admin Sidebar.



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

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

В Примера тук ще разгледаме 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.

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



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

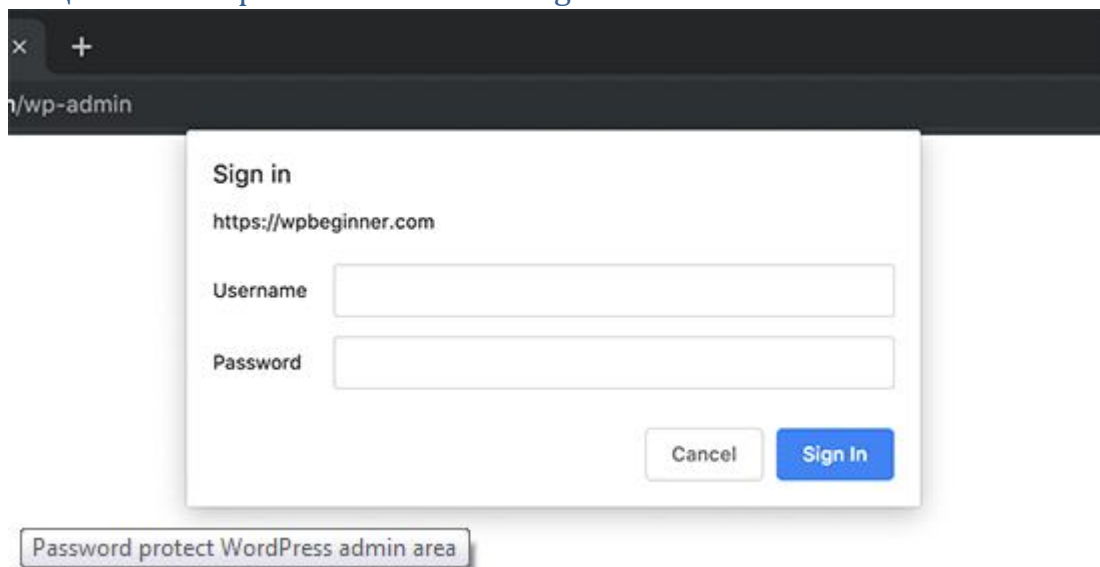
Промяна в Префикса на WordPress Базата-данни

Стандартно, WordPress задава Префикс `wp_` на ВСИЧКИ Таблицы в нашата [WordPress database](#). Ако WordPress-Сайтът ни използва Стандартен Database Prefix, с това 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

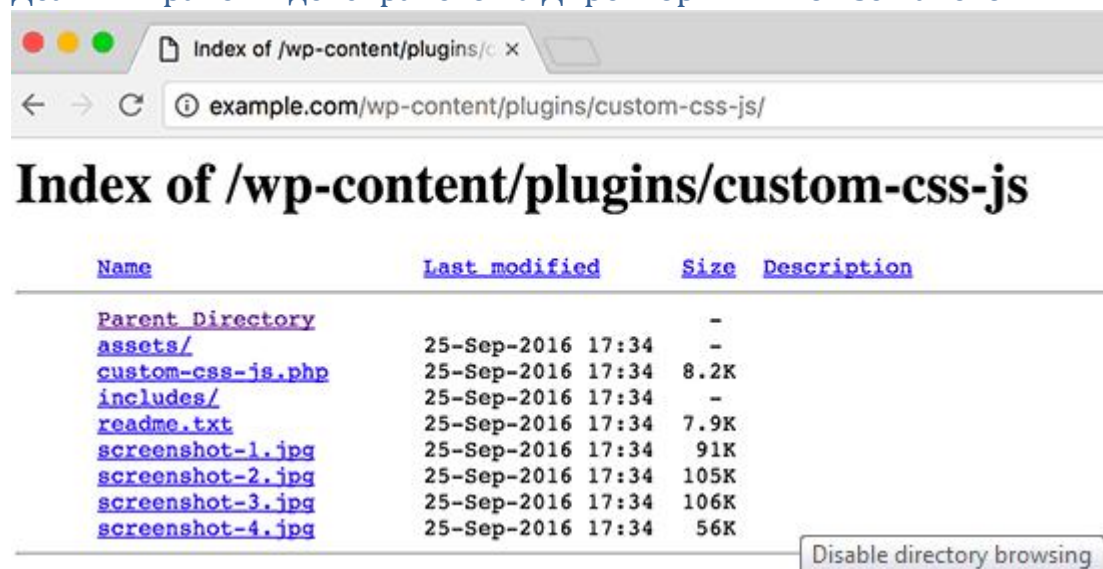


Обичайно, Хакерите имат НЕОГРАНИЧЕН Достъп до нашите `wp-admin` Папка и Login Page. Това улеснява опитите им за Нерегламентирана намеса и предприемането на DDoS Атаки.

С ДОПЪЛНИТЕЛНА защита 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 Обхождане 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 можем да открием 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

Отдалеченото Извикване на Процедури [XML-RPC](#), бе Активирано 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 за нашия Web-Сайт, ще са му нужни 500 отделни Опити за Влизане (Login) и в резултат ще бъде Разкрит и Блокиран 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 Обръщания (Request-a).

Ето защо, при отсъствие на изрична нужда, 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.

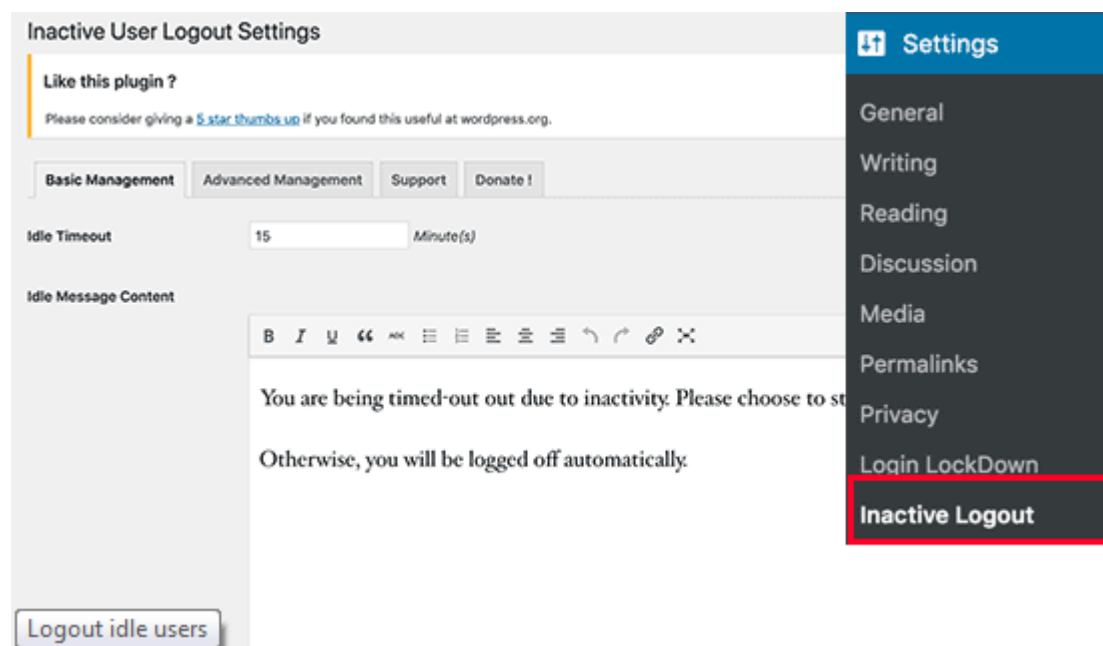
Ако ползваме вече споменатата Защитна стена на Ниво „Web-Приложение“, за същото ще разчитаме на Защитната стена (Firewall).

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

Log-натите Потребители понякога се отвлечат с нещо друго в страни, а това поражда Рискове в Безопасността. Някой друг може да седне зад Компютъра им, да СМЕНЯ Пароли или да ПРОМЕНЯ Настройки в техния Account.

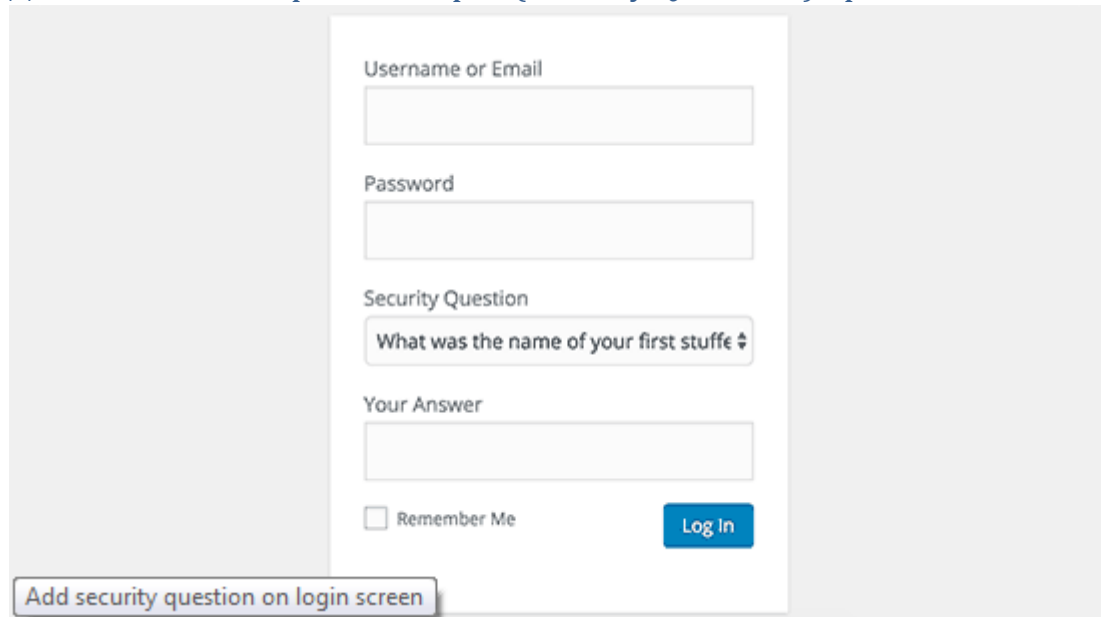
По същата Причина, множество Банкови и Финансови Сайтове АВТОМАТИЧНО „изхвърлят“ (Log out) Неактивен потребител. Подобна Функционалност можем да заложим и ние, в нашия WordPress-Сайт.

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 Запазваме Настройките с Избиране на Бутон: „Съхранение“.

Добавяне на Контролен въпрос (Security Questions) при WordPress Login



The image shows a WordPress login form with the following fields and elements:

- Username or Email input field
- Password input field
- Security Question dropdown menu with the text "What was the name of your first stuff" and a double arrow icon.
- Your Answer input field
- ☐ Remember Me checkbox
- Log In button
- A button at the bottom left labeled "Add security question on login screen".

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

Контролни въпроси можем да добавим, като Инсталираме [WP Security Questions](#) Plugin. При Активирането му, отиваме на Страница: **Settings » Security Questions** и там Указваме конкретни Настройки.

По-детайлни Инструкции можем да почерпим от 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 Слив в Трафика на Web-Сайта/изоставане в Класацията на Търсещите машини ([Search Rankings](#)), резонно провеждаме Сканиране.

Можем да ползваме нашия WordPress Security Plugin или някой измежду изброените на: [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, БЕЗ ДА МОГАТ да Премахнат Нерегламентирания код, нито да Възстановят WordPress-Сайт от Зловредни изменения.

Ето как закономерно стигаме до следващия Раздел за Почистване на Зловреден софтуер и Ликвидиране последствията от Външна намеса във WordPress Сайтове.

Ликвидиране на Зловредни изменения вследствие Външна намеса във WordPress Сайт

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

Профилактиката на един WordPress Сайт може да бъде изключително трудна и времеемка. Непредубеденият съвет 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](#) за Възстановяване нашия Web-Сайт, гарантира текущо изрядното му състояние. Можем да разчитаме на Превенция и при последващи Атаки.

За по-авантюристично настроените и за Ползватели „Направи си сам“, сме предоставили Ръководство „Стъпка по стъпка“, на: [fixing a hacked WordPress site](#).

Толкова по темата. Надяваме се Ръководството да ви е запознало с НАЙ-Добрите Практики на WordPress Информационната безопасност и да ви насочи към НАЙ-Удачните WordPress Security Plugin-и в конкретна ситуация.

Ако Материалът ви е бил от полза, 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 1,300,000 читатели в глобален мащаб.

Разяснителни бележки

Повече Информация за Sucuri Security WordPress plugin, ще намерим в Базата-знания [ТУК](#).

Що е Security Activity Auditing?

Проследяването на Дейностите по Защита на безопасността е може би най-подценяваната Функция на Безопасността. Това е Дейността по Проследяване (Monitoring) на ВСЯКАКВИ Събития, свързани с Безопасността в рамките на нашата WordPress-Инсталация. Въпросът е: Що е Събитие, свързано с Безопасността? В очите на Sucuri, всяка последвала Промяна в Приложението може да бъде категоризирана като: Събитие, касаещо Безопасността и поради това, WordPress полагат усилия то да бъде Журнализирано.

Това е важно, защото предоставя на Собственика на Web-Сайт възможност щателно да следи всякакви Изменения в съответната Среда. Кой го Посещава? Какво произтича?

Процедурата включва представяне на всички Дейности в Журнализиран вид на Sucuri Облака, с предохранителна цел. Това лишава Злонамерен субект от възможност да достъпи наши Квалифицирани данни и да осуети предприемането на Ответни мерки по отношение на Пробива в Сигурността. Ако Злонамерен субект съумее да байпасира нашите Предохранителни мерки, Журналите ни по Безопасността (Security Logs) ще бъдат надеждно съхранени в Sucuri Центъра за мерки по Безопасността/Sucuri Security Operations Center (SOC).

Конкретната Функционална възможност касае особено силно Уебсайт/Системни администратори и Експертите по безопасност, следящи ситуацията с/поведението на своя Сайт и кога възникват Проблеми.

Що е [File Integrity Monitoring](#)?

Проследяването на Файловия Интегритет с оглед Информационна безопасност е от ключов приоритет за Безопасността. Това е Процесът на Съотнасяне на Текущото състояние спрямо предварително установен Критерий. Несъответствие между Текущото състояние и Установен критерий предвещава Проблем. Принципът е залегнал в голяма част от Системите за Предпазване от Неправомерен достъп при Доставчиците на Hosting-Услуги. Именно това е заложено в Sucuri Security Plugin.

Критерий „Препоръчително състояние“ се създава при Инсталиране на Plugin-а. Той включва ВСИЧКИ Директории от Главната Root-Директория на Инсталацията, в т.ч. Plugin-и, Theme-и и Файлове на Ядрото (Core Files).

Що е [Remote Malware Scanning](#)?

Във въпросната Функционална възможност е Заложена т.нар. Scanning Engine (Машина за Сканиране) на Sucuri – вградена в техния Свободен Free Security Scanner – [SiteCheck](#). Препоръчително е да отделим време и да проучим [как работи въпросното Сканиране](#).

Що е [Blacklist Monitoring](#)?

Друга, изключително полезна Функционална възможност на Security Malware Scanner е, че Проверява в най-различни Blacklist Engines, в т.ч.:

- [Sucuri Labs](#)
- [Google Safe Browsing](#)
- [Norton](#) (Вж. [тук](#) и [Symantec Web Application Firewall](#))
- [AVG](#)
- [Phish Tank](#)
- [ESET](#)
- [McAfee Site Advisor](#)
- [Yandex](#)
- [SpamHaus](#)
- [Bitdefender](#)

Това са някои от най-големите Оператори, поддържащи Черни списъци; всека може непосредствено да повлияе Online-Репутацията ни. Бидейки в Синхрон с техните Environments (Среди), Sucuri могат да съобщят на своите Ползватели, вследствие Сканиране, дали някоя измежду Операторите не ги причислява към Категория „Съмнителни Сайтове“. В подобен случай можем да разчитаме, че с помощта своя Продукт за Web-Сайт Security, те ще ни помогнат да излезем от Security „Черния списък“.

Що е [Effective Security Hardening](#)?

Лесно е да се изгубим в света на Подобряване на Информационната безопасност. Sucuri Възстановяват стотици Web-Сайтове всеки ден, най-вече с помощта на многообразие от Конфигурации за Засилване на Информационната безопасност, каквито срещаме в изобилие от WordPress Security Презентации. В настоящия Раздел сме включили тези, които считаме, че най-ефикасно допълват Комплекса Продукти на Sucuri в неговата цялост.

Какво включват [Post-Hack Security Actions](#)?

Дори и най-добрият в сферата на Безопасността понякога може да не съумее да предотврати неизбежното. Именно с оглед подобна ситуация, Sucuri са включили Раздел, представящ трите Ключови мерки, които следва да бъдат предприети в случай на Компрометиране.

Що са [Security Notifications](#)?

Всички споменати Функционални възможности във връзка с Безопасността биха били безполезни, ако не сме УВЕДОМЕНИ за Проблемите. Именно с такава цел, Sucuri са ИНТЕГРИРАЛИ Набор Security Alerts. Разширявайки кръга Събития, свързани с Безопасността, осигуряват на Web-Сайт Владелците повече Гъвкавост по отношение на това, което желаят да им бъде разяснено. Като Владелец на Web-Сайт, можем да бъдем Информирани така дискретно или на толкова висок глас, колкото желаем

Що е [Website Firewall \(premium\)](#)?

Разглеждаме най-ценната към момента Функционална възможност по Безопасността, предлагана от Sucuri на Владелците на Web-Сайтове. Става дума за Защитна стена на Ниво „Web-Сайт на Стопанска организация“ (enterprise grade Website Firewall), проектирана да предоставя ВЪЗМОЖНО НАЙ-Добра Защита на Информационната безопасност. Защитава ни от всякакви Web-Сайт Атаки, в т.ч.:

- Възпрепятстване Достъпа до ценна Информация или даден Сайт/Denial of Service (DoS/DDoS) Attacks
- Възползване от Уязвими места в Софтуера/Exploitation of Software Vulnerabilities
- [Zero-Day](#) Disclosure Patch-ове (вж. и Responsible Disclosure [тук](#))
- Нерегламентирани Атаки/Brute Force Attacks по нашите Системи за Контрол над Достъпа/Access Control Mechanisms

В допълнение, предоставя и следните Функционални възможности

- Оптимизиране на Производителността/Performance Optimization
- Засилени Мерки за Контрол над Достъпа/Advanced Access Control Features
- Надеждни Съхранение и Пренос на Данни и Интегритет на Данните/Failover and Redundancy

Последните **не са включени в Свободната (Free)** Опция на Plugin-а, но са Интегрирани, така че при Закупуване от наша страна, МОЖЕМ да ги Активираме. Ако желаем самите ние да участваме в подобряването на Sucuri Firewall като такъв, можем да вложим свой принос в Доработката на [Website Firewall WordPress Security](#) в Standalone Mode.

Sucuri WordPress Security plugin е Разработен от Екип, известен с Проактивния си подход към Безопасността. Изграден е на база Опит, натрупан в хиляди случаи на

„Излекуване“, милиони специфични Сканирания на Домейни и 10-ки милиони Блокирани Атаки по Web-Сайтове.

Кое е [това](#) , което нашият Plugin прави, а другите Security Plugin-и - не?

И други Security Plugin-и притежават Възможности за Проследяване Действията на Потребителите ([Activity Monitoring](#)), но единици се справят задоволително. Уникално при Activity Monitoring-а на нашия Plugin е това, че Безопасността и Надеждността са ГАРАНТИРАНИ от Sucuri Security Operations Center (SOC).

Функциите в Security Plugin-а ни са организирани Йерархически, като считаното от нас за недотам нужно на Масовия потребител е с по-нисък Приоритет. Фиксирали НАЙ-Уместни за един Владелец на Web-Сайт Функционални възможности и сме ги Интегрирали в съответния Plugin.

[Ако Инсталираме Sucuri Security Plugin, имаме ли право на Sucuri Account?](#)

НЕ, коментираният Plugin е Свободно (Free) Разширение. От нас НЕ СЕ ИЗИСКВА Допълнително заплащане, което обаче не означава, че се ползваме и със Свободен (Free) Account.

[Ако имаме Premium Plugin-а, ще ни трябва ли Свободният \(Free\) Plugin?](#)

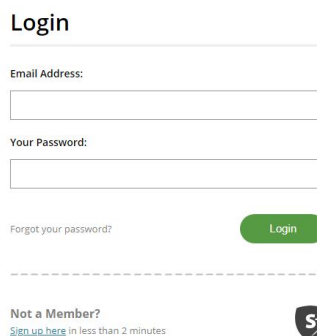
Поддръжката на Premium Plugin-а бе Преустановена още през 2014г. Всички Главни Функционални възможности са Добавяни към Free Plugin-а. Ако все още ползваме Стария (Old) Premium Plugin, от Sucuri ни МОЛЯТ да пристъпим към негово Изтриване и да си Инсталираме Новия (New) Free Plugin от WordPress Plugin Market. Припомним, че ще трябва и да Генерираме Нов API Key, защото Новата API Service НЕ Поддържа Старите API-Ключове.

[Ще ни трябват ли други Sucuri-Продукти, ако имаме Sucuri Security Plugin?](#)

Да. Plugin-ът ДОПЪЛВА вече наличния ни Арсенал с Инструменти по Безопасността. НЕ Е Замислен с като Заместител на Sucuri Website Security или Firewall Продуктите.

[Откъде получаваме Поддръжка за въпросния Plugin?](#)

Най-удачно е да се обърнем към Sucuri, от: [Support Forum](#). Ако сме Клиент, можем да



Изпратим наш/-а Ticket/Идентификация [оттук](#) ().

[В КОНФЛИКТ ли е Plugin-ът ни с WordFence?](#)

Plugin-ът ни НЕ, но са ВЪЗМОЖНИ Колизии със „Скенерите“ на Sucuri. Ако ни се извежда Грешка: “Unable to Properly Scan Your Site”, най-вероятно WordFence Plugin-ът БЛОКИРА нашия Scanner като НЕРЕГЛАМЕНТИРАН [Crawler](#) (Програма за Web-Обхождане/Spider/Spiderbot, от типа на: [Jeeves](#)). Трябва да „Разрешим“ (включим във

White List/„Белия списък“ с Разрешени Адреси) IP-Адресите на Sucuri от WordFence Dashboard (Контролния Екран на WordFence).

Какви са Ограниченията на Remote Malware Scanner при Отдалечено Сканиране за Зловреден софтуер?

Security Malware Scanner-ът е ОТДАЛЕЧЕН и поради това, няма как да „види“ неща на Сървъра, които Browser-ът НЕ Извежда. Ако Казусът ни интригува, Sucuri с готовност очакват наши Коментари относно техния Website Security Продукт – неща, от типа на: Phishing-Страници, Backdoors/„Задни врати“, Mailer Scripts/[Скриптове за Разпращане на Съобщения](#) и др.

Plugin-ът ни НЕ ИДЕНТИФИЦИРА Зловреден софтуер

При подобен случай, Правим СПРАВКА в [гореспоменатите](#) Remote Scanner Limitations. Проблема НЕ ТРЯБВА да отдаваме на Website Security Product-ите на Автора. В случай, че в качеството на Клиент на Sucuri, ни Порази Malware (Зловреден софтуер), Съветът е да изпратим Ticket (Нотация), за да може [да ни Помогне да се Избавим](#).

Ако НЕ СМЕ Клиент, но желаем да Споделим нещо интересно за нас, можем да го сторим на Адрес: labs@sucuri.net.

Plugin-ът НЕ ИЗВЪРШВА Сканиране за Malware/Security на Ниво „Приложение“ (Application Level), така че споменатото НЕ Е Необичайна практика.

Свободно ли е Активирането на Защитната стена?

НЕ, не е. Ще можем да я Активираме, АКО се Абонираме за Услуга: [Website Firewall Service](#).

Ще Повлияе ли Plugin-ът на Поведението и Производителността (Performance) на нашия Web-Сайт?

С всяка следваща Версия, Sucuri подобрява Поведението и Производителността на Кода. Поради Несъответствия при Hosting Provider-ите обаче, Plugin-ът може да повлияе Поведението (Responsiveness) на Web-Сайта при Инсталиране. Неща, като: HTTP-Заявки (Requests), Проверки на SSL-Сертификати (SSL Certificate Verifications) и DNS Lookups (вж. [тук](#)), са сред малкото неща, които, според Конфигурацията на нашият Web-Сървър, може да забавят Web-Сайта ни.

Log-овете в моята База-данни ли се Съхраняват?

Не, не се Съхраняват в нея.

Възможни ли са Проблеми с Инсталирането на Plugin-и при някои Host-ове?

Не, доколкото [WordPress България](#) са запознати с Въпроса.

Нужен ли ни е този Plugin, за да ползваме Услуга Website Firewall?

НЕ, не е необходим. Website Firewall-ът работи в Облака, без да трябва да Инсталираме каквото и да е при нас. Plugin-ът се грижи ЕДИНСТВЕНО да можем да виждаме и Управляваме Услугата от WordPress Dashboard Контролния панел.

Каква Информация събира Sucuri?

Sucuri стриктно съблюдават Поверителността на нашите Данни. За Ползвателите на Свободен (Free) , Plugin, неразполагащи с API-Ключ, Sucuri НЕ Събира Информация. Когато Активираме API-Ключ, Sucuri ЩЕ Запомни ОПРЕДЕЛЕНА Информация, от типа на: Log-ове. Съветват да се запознаем с техните [Правила за използване](#) и [Правила за Поверителност на Данните](#). Всякакви въпроси относно Поверителността на нашите Данни, можем да изпращаме по Електронна поща, на Адрес: gdpr@sucuri.net.