KURSY WORDPRESS

WWW.KURSYWORDPRESS.PL

BEZPIECZNA STRONA OPARTA O WORDPRESS

SPIS TREŚCI

Wstęp.

Czytając tego e-booka, dowiemy się, że z Wordpress-a korzystają miliony użytkowników i firm na całym świecie. Jeśli mamy zabezpieczone dobrze komputery, chronimy swoje dane, jesteśmy czujni, to wszystko to może nie wystarczyć. Aby dobrze zabezpieczyć naszą stronę internetową, musimy spojrzeć na temat jej bezpieczeństwa z innej strony.

Nazywam się Radek Rzążewski i w dalszej części przedstawię Ci jak każdy, kto ma dostęp do konta administracyjnego w Wordpress-ie, powinien go zabezpieczyć. Poradnik ten jest przeznaczony dla osób o podstawowych umiejętnościach i nie znajdziesz w nim zaawansowanych technik zabezpieczania Wordpress-a.

INFORMACJA O AUTORZE E-BOOKA

O autorze

Radek Rzążewski. Od 28 lat moim hobby są komputery. Firmę komputerową mam od 2004 roku. Na co dzień zajmuję się administracją serwerów Linux i Windows oraz sieci LAN. Tworzę także strony internetowe dla moich klientów oparte o silnik Wordpress. Właściciel: www.KursyWordpress.pl - zakup kursu: www.arche.edu.pl

Dla kogo jest ten e-book?

Tak jak wspomniałem, e-book jest dla osób, które nie są zaawansowanymi użytkownikami (np. brak wiedzy na temat edycji motywu) oraz nie posiadają dostępu do hostingu (brak dostępu do konta FTP, brak możliwości ustawień PHP).

WordPress jest bardzo popularny, dlatego stwarza to także bardzo ogromną chęć włamań na strony oparte o ten CMS. Rozróżniamy kilka sposobów włamania:

- brak zabezpieczonej wtyczki, motywu lub złe ustawienia na prawa plików/katalogów,
- słabe hasło do konta administracyjnego,
- brak aktualizacji silnika WordPress, wtyczek i motywów.

Zaskakujące jest, że, według serwisu https://w3techs.com/, z WordPress korzysta 60,8% wszystkich stron internetowych, których system zarządzania treścią znamy. To 34,1% wszystkich stron internetowych.

Jednak bardzo smutne jest to, że ze wszystkich 100% stron 41.7% jest w wersji 4.x czyli można to odczytać, że nie są one aktualizowane na bieżąco, a co za tym idzie bardzo podatne na ataki.

W maju 2019 roku podatne na ataki były wtyczki WP Live Chat Support , w listopadzie 2018 WP GDPR Compliance.

Użycie WordPress-a na świecie.

Wiele popularnych stron internetowych, takich jak TechCrunch, The New Yorker, People, Variety i TED, używa WordPress. WordPress.org oferuje ponad 50 000 wtyczek i ponad 3500 motywów na licencji GPL. WordPress jest dostępny w 57 językach.

W momencie pisania tego e-booka wersję WordPress 5.2 został pobrano 39,808,318 razy. Dla porównania 7 maja 2019 r. było to 30,692,479. 11 tygodni, 5 394 404. Tygodniowo ponad 490 tysięcy. Czyli dziennie średnio 70 057.

Źródło: https://wordpress.org/download/counter/

To są dobre wiadomości, bo wliczają się tutaj także aktualizacje z np. 5.1 i starszych wersji. O upgrade wersji opowiem później.

Ilu ludzi czyta blogi? Ponad 409 milionów osób przegląda ponad 20 miliardów stron każdego miesiąca.

Ile jest publikowanych postów? Użytkownicy produkują około 70 milionów nowych postów i 77 milionów nowych komentarzy każdego miesiąca.

Źródło: – https://wordpress.com/activity/

Słowo kluczowe „WordPress" jest wyszukiwane około 2,8 miliona razy w miesiącu. ***Około 19 500 000 stron w całej sieci korzysta z WordPress.***

50-60% to udział WordPress w globalnym rynku CMS – co czyni go najpopularniejszym systemem CMS wśród nich wszystkich już siódmy rok z rzędu.

New York Observer, New York Post, TED, Thought Catalogue, Williams, USA Dzisiaj, CNN, Fortune.com, TIME.com, National Post, Spotify, TechCrunch, CBS Local, NBC i więcej, ***wszyscy używają WordPress.***

WordPress jest najszybciej rozwijającym się systemem CMS, z około 500+ nowymi witrynami tworzonymi codziennie w 10 milionach witryn w sieci (w porównaniu z 60-80 Shopify i Squarespace).

WordPress zasila 14,7% 100 najlepszych stron na świecie.

17 postów publikowanych jest co sekundę na stronach WordPress na całym świecie.

37 milionów globalnych wyszukiwań Google dla „WordPress" odbywa się miesięcznie.

Źródło: https://www.codeinwp.com/blog/wordpress-statistics/

Zaczynamy zabezpieczanie naszego Wordpress-a

I. Wszystko robisz na własną rękę 😉

Warto wspomnieć, że nie biorę odpowiedzialności za Twoje działania. Jednak pamiętaj, że zalecenia opisuję na tej stronie, POWINNY być wykonane na Twojej stronie.

Dodatkowo prezentuję tutaj dużo wtyczek. Warto zaznajomić się z ich funkcjami. Przy okazji wspomnę, że NADMIAR wtyczek zawsze stanowi dłuższe ładowanie strony i często więcej dodatkowego kodu na stronie, czego roboty Google nie lubią! 🙂 Wiadomo, coś za coś 😉

II. Logujemy się do Wordpress-a i sprawdzamy czy mamy konto administracyjne:

Użyj generatora – Link 1:

Generator linków, aby zapewnić szybszy dostęp do omawianego tematu:

Generator do ,, E-BOOK Bezpieczeństwo Wordpress - KursyWordpress_pl''

III. Kopia bezpieczeństwa

Kwestią podstawową, przed wszystkimi poniższymi czynnościami, należy wykonać kopię bezpieczeństwa:

- zrobić koniecznie backup bazy danych i plików (przykład zaczerpnięty z hostingu zenbox):
    - Eksport bazy poprzez phpMyAdmin – http://bit.ly/2TuB2dy

- Konfiguracja połączenia FTP w programie FileZilla – http://bit.ly/2N4b7bd

Backup Wordpressa można zrobić także za pomocą wtyczki: Jak zrobić backup WordPress

Przy okazji ustawić automatyczne ***tworzenie kopii bezpieczeństwa z panelu klienta w swoim hostingu***. Należy się też dowiedzieć ***jaki okres wstecz hosting jest w stanie nam odtworzyć naszą stronę internetową i bazę danych***. Czyli otwieramy e-maila, piszemy do naszego hostingu z pytaniami:

Dzień dobry,

Chciałam/em się dowiedzieć dwóch rzeczy:

1. *Co ile jest wykonywana kopia bezpieczeństwa moich plików?*
2. *Co wchodzi w skład kopii bezpieczeństwa? Pliki poczty? Pliki strony WWW? Pliki bazy danych?*
3. *Jeśli zepsuje mi się poczta e-mail (np. skasuję plik lub katalog z korespondencją) to ile wstecz jest przechowywana kopia bezpieczeństwa u Państwa na serwerach?*
4. *Jeśli zawirusuje mi się moja strona z Wordpress-em, to ile wstecz są przechowywane pliki i baza danych do mojej strony opartej o Wordpress?*
5. *Czy ewentualne odwirusowanie strony jest u Państwa za darmo? Co wtedy robicie, aby mi pomóc?*

Dziękuję bardzo, czekam na odpowiedź.

Pozdrawiam

Możesz sobie skopiować i wkleić tę treść 😋 Piąte pytanie tak dodatkowo 😉

IV. Zmiana nazwy konta administracyjnego.

1. Dla konta administracyjnego ***nie używamy loginu o nazwie ,,admin”***. Utwórz inne konto administracyjne, z nazwą np. ,,30uxHJ78” , a stare ,,admin” skasuj.
2. Oraz ***koniecznie użyj silnego hasła do konta administracyjnego***.

V. Jak utworzyć silne hasło dla konta administracyjnego ?

1. Weź z półki ***swoją ulubioną książkę***
2. Otwórz ją ***na jakiejś konkretnej stronie*** i zacznij czytać:

   ,,Babcia Genowefa bardzo lubiła, kiedy jej wnuczka, lat 3, ciągle się uśmiechała się.’’

3. Hasło: ***BGblkjw,l3,csus***

Dodatkowo warto dodać znak specjalny np. **$** na początku lub końcu – więc ostatecznie hasło wyglądałoby tak: ***BGblkjw,l3,csus$***

Nie używaj polskich liter w hasłach! 🙂

Do zapamiętania hasła, wystarczy Ci nazwa książki i numer strony 😉

VI. Sprawdzanie adresu e-mail dla konta administracyjnego.

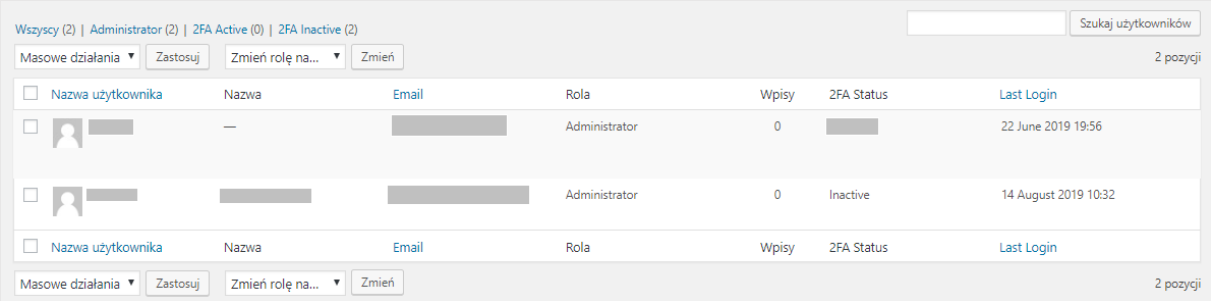
Użyj generatora – Link 2:

Generator linków, aby zapewnić szybszy dostęp do omawianego tematu:

Generator do ,, E-BOOK Bezpieczeństwo Wordpress - KursyWordpress_pl''

Sprawdź, czy Twój adres e-mail do konta administracyjnego jest INNY NIŻ DOMENA na której ,,stoi" strona internetowa. Oraz czy masz dostęp do tego adresu e-mail?

Często zdarza się tak, że może stać się coś z hostingiem, robisz coś z cesją domeny — wtedy warto, aby adres mail do konta administracyjnego był inny niż adres strony internetowej.



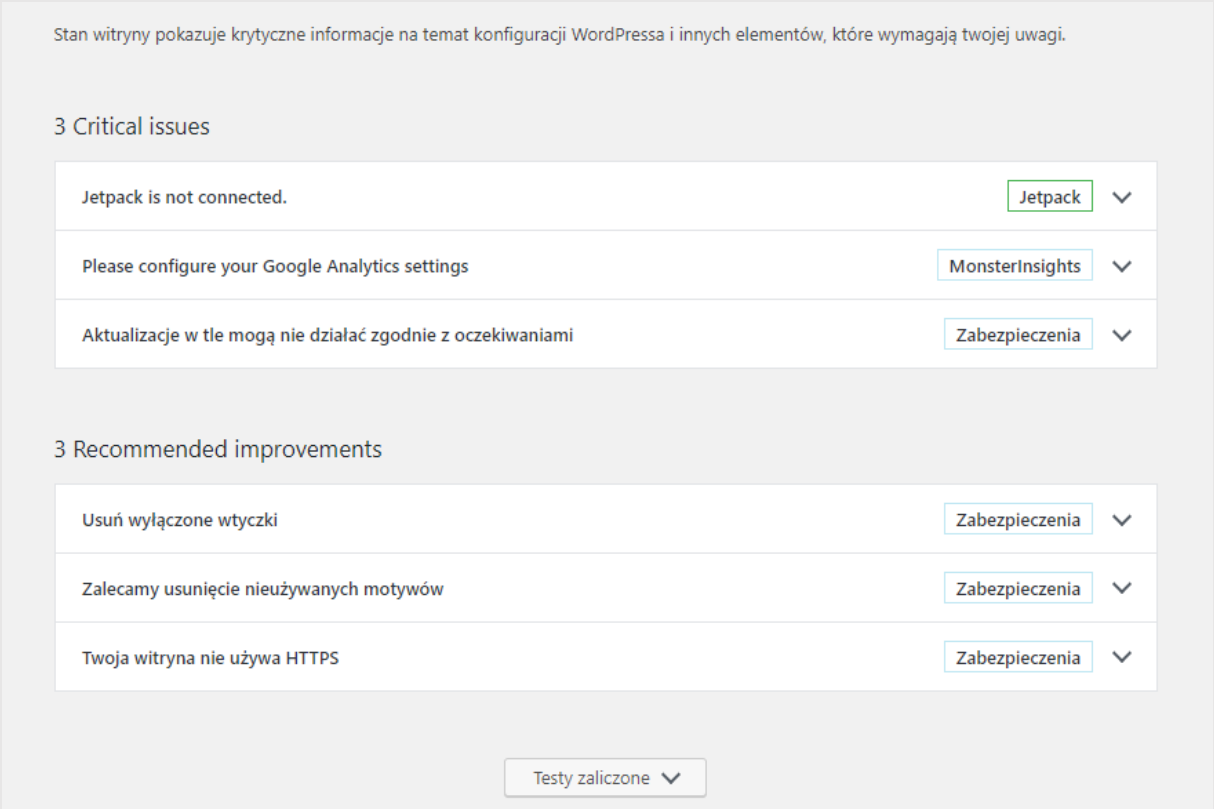
VII. Sprawdź stan Twojej witryny.

Wejdź w Kokpit -> Admin -> Narzędzia -> Stan witryny.

Albo użyj generatora – Link 2:

Generator linków, aby zapewnić szybszy dostęp do omawianego tematu:

Generator do ,, E-BOOK Bezpieczeństwo Wordpress - KursyWordpress_pl''



Generowanie stanu witryny chwilę trwa, więc otrzymasz komunikat:

Sprawdzanie chwilę trwa, więc nie odświeżaj strony.

Wynik powinien być podobny do tego:

Twój WordPress działa poprawnie;

Korzystasz z aktualnych wtyczek i motywów;

Konfiguracja Twojego serwera jest poprawna;

Twój WordPress jest odpowiednio zabezpieczony;

Nie ma żadnych konfliktów na stronie.

Jest to bardzo fajna funkcja do sprawdzenia i rozwiązania problemów na Twojej stronie internetowej.

Ułatwia także sprawdzanie podstawowych parametrów pracy, które wcześniej wymagały specjalistycznej wiedzy lub dodatkowych pluginów.

VIII. Standard https .

Standardem jest użycie HTTPS – to już jest zalecenie Google i strony, które nie mają HTTPS-a, będą rozpoznawane przez algorytmy i mniej punktów w wyszukiwaniach.

- Do użycia HTTPS potrzebny jest Ci certyfikat SSL (najlepiej darmowy Let's Encrypt);
- Sprawdź ustawienia**:**

Generator linków, aby zapewnić szybszy dostęp do omawianego tematu.
Do sprawdzenia poniższych ustawień wykorzystaj link 4:
Generator do ,, E-BOOK Bezpieczeństwo Wordpress - KursyWordpress .pl''

Adres WordPressa (URL)

Adres witryny (URL)

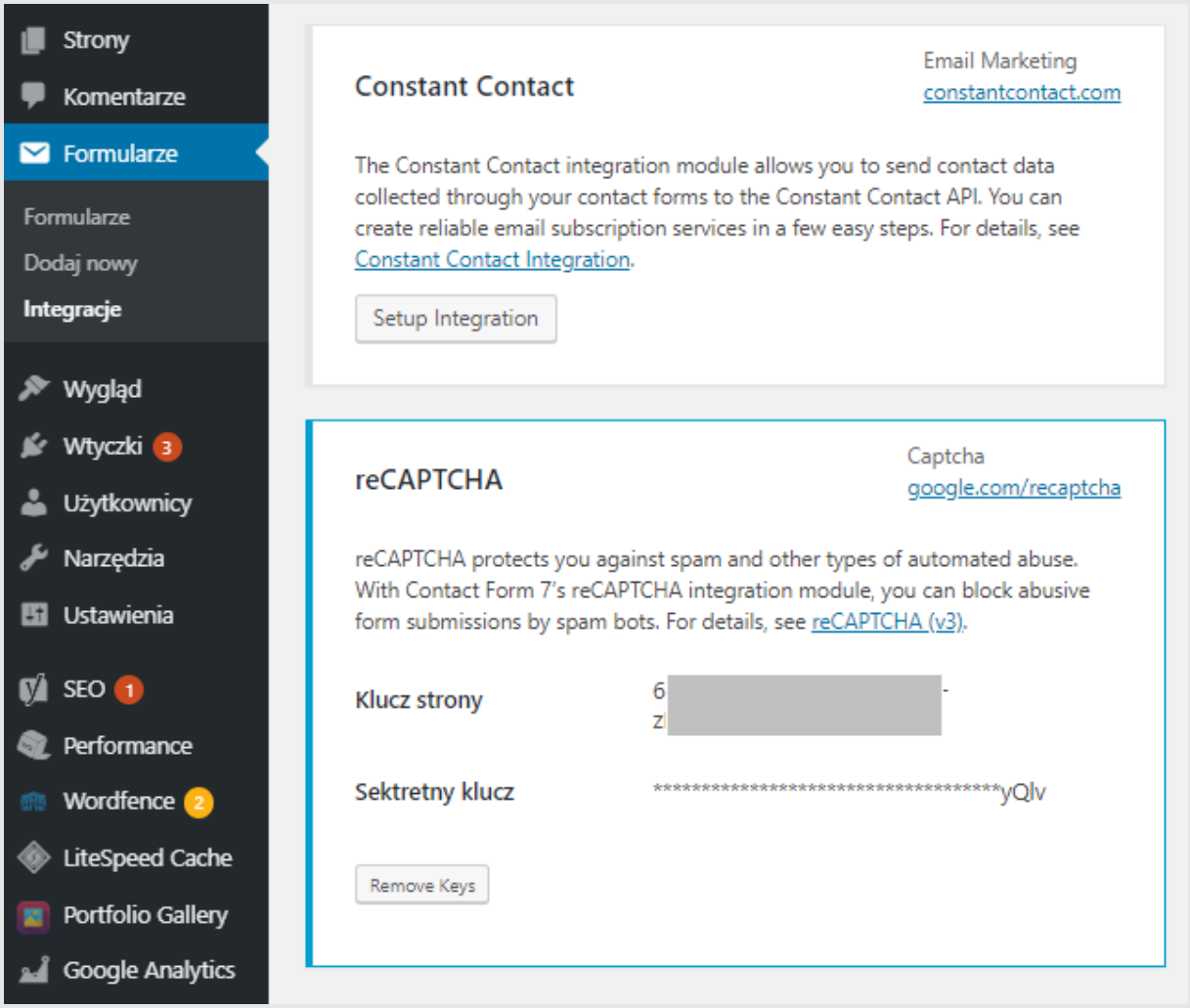
powinny zaczynać się od https, a nie http.

UWAGA: Zmiana ustawień adresu WordPressa i witryny bez dobrze zainstalowanego certyfikatu SSL może spowodować to, że nie dostaniesz się na swoją stronę. Skontaktuj się ze mną lub ze swoim hostingiem.

Dla początkujących włączenie SSL / HTTPS w WordPressie może przydać się wtyczka ***Really Simple SSL***. Na koniec wprowadzania HTTPS dla naszej witryny trzeba dodać nowe adresy stron z przedrostkiem HTTPS w Google Search Console.

IX. Google reCAPTCHA w formularzu.

Użyj koniecznie Google reCAPTCHA w wersji 3 do swojego formularza kontaktowego na stronie.



Jeśli korzystasz z wtyczki Contact Form 7, do wysyłania formularzów, skorzystaj z linku 5:

Do sprawdzenia ustawień Contact Form 7 wykorzystaj link 5:

Generator do ,, E-BOOK Bezpieczeństwo Wordpress - KursyWordpress_pl''

X. Usuwanie zbędnych informacji ze strony.

Usuń informacje o wersji WordPressa ze swojej strony internetowej.

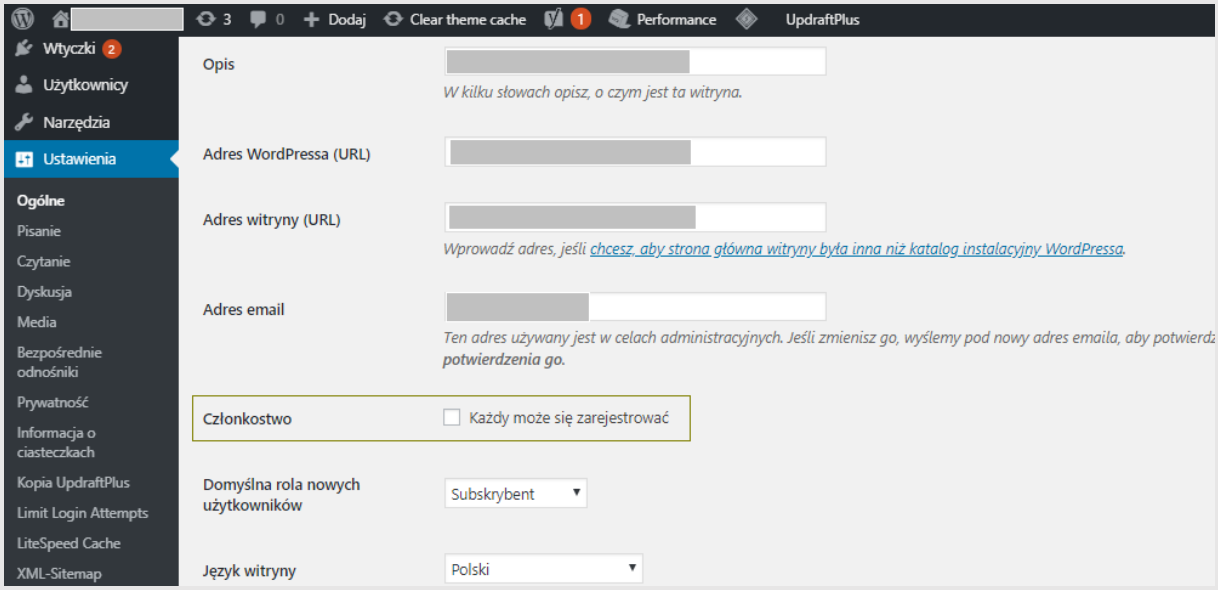
Jeśli znamy się na edycji plików WordPress, możemy usunąć w pliku functions.php linię:

remove_action ('wp_head', 'wp_generator');

XI. Wyłącz rejestrację nowych kont na swojej stronie.

Do sprawdzenia ustawień członkostwa wykorzystaj link 6:

Generator do ,, E-BOOK Bezpieczeństwo Wordpress - KursyWordpress_pl''



Odznacz opcję ,,*Każdy może się zarejestrować*”

XII. Logowanie dwuskładnikowe.

Instalując wtyczkę *Two Factor Authentication*, podniesiemy poziom logowania dwuskładnikowego dla naszej witryny.

Kiedy będziemy próbowali zalogować się do konta administracyjnego, system wyśle na komórkę kod weryfikacji dwuetapowej.

Google Authenticator — zainstalować taką aplikację na telefonie (dostępna na Android i iOS)

Weryfikacja dwuetapowa zapewnia większe bezpieczeństwo Twojego konta Google, ponieważ logowanie obejmuje dwa etapy weryfikacji.

Oprócz hasła trzeba też podać kod wygenerowany przez aplikację Google Authenticator na telefonie.

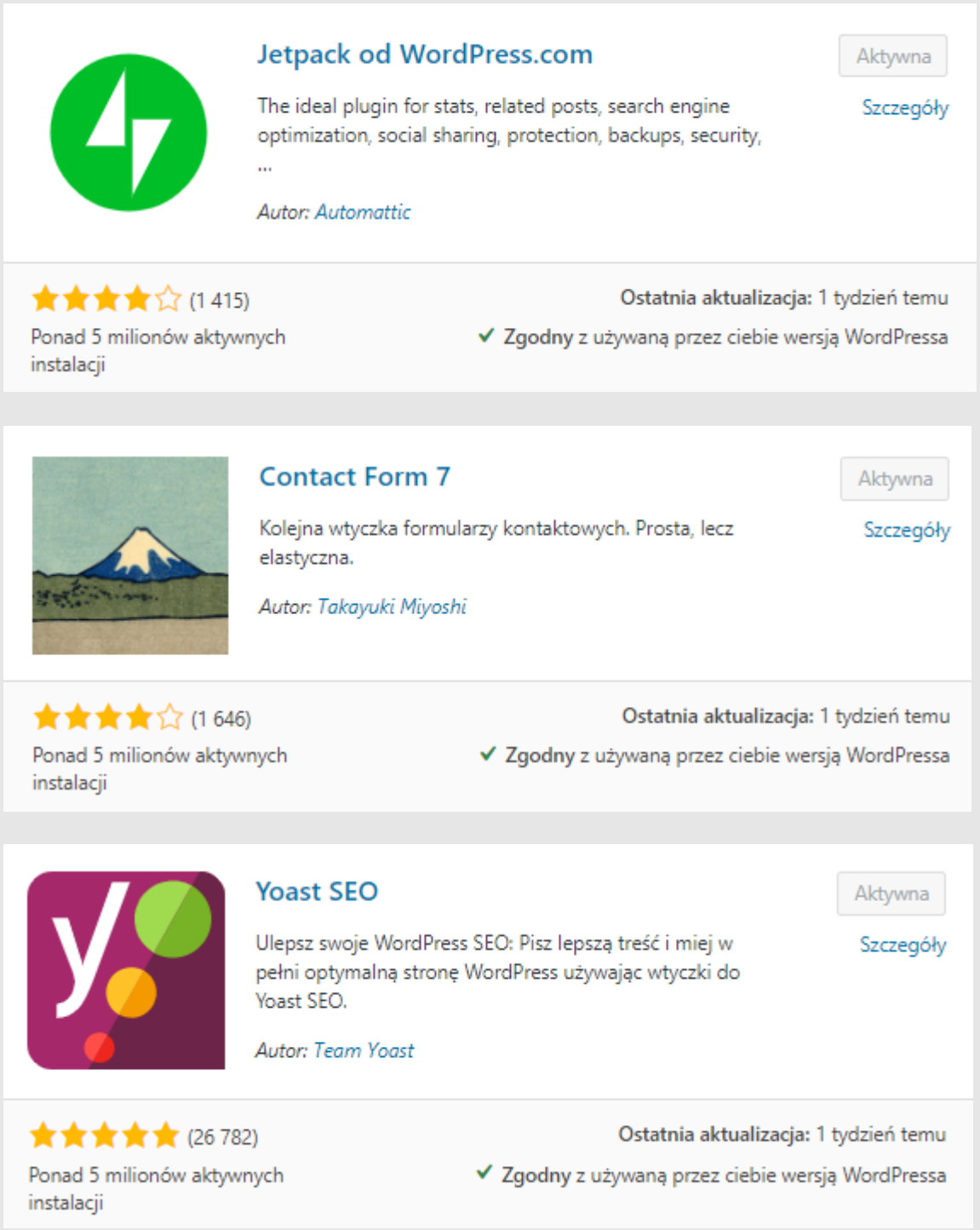
XIII. Ukrywanie autora i motywu.

Za pomocą wtyczki *WP Hide & Security Enhancer* ukryjesz autora tworzonych postów i wersję motywu.

XIV. Wybieraj tylko takie wtyczki, które są ostatnio zaktualizowane.

Osobiście wybieram wtyczki aktualizowane przez wydawcę maksymalnie miesiąc temu i mają dużą liczbę pobrań – Dodatkowo zwracam uwagę, aby miały ponad 100-500tyś pobrań, ponieważ korzystam z popularnych wtyczek. Więcej w artykule: 20 WTYCZEK DO WORDPRESS ,

Przykładowe wtyczki:



XV. Odinstaluj nieużywane wtyczki i motywy.

XVI. Rób częste aktualizacje WordPressa, wtyczek i motywów.

XVII. Wtyczki podnoszące bezpieczeństwo WordPress

Uwaga, wtyczki poniżej stanowią wartościowe funkcje i ustawienia, ale nie znając się zbytnio na nich, możemy zepsuć co nieco na stronie 😉

Oto wtyczki:

- WordFence,
- Cerber,
- Sucuri,

oraz

- WordPresss All-in-one,
- WP Security & Firewall.

Dodatkowo możesz włączyć zaporę sieciową (Firewall). Jedna z poniższych wtyczek zablokuje cały złośliwy ruch, zanim jeszcze dotrze on do Twojej witryny:

- WordPress Simple Security FireWall,
- All In One WP Security & Firewall,
- BulletProof Security.

XVIII. Sprawdzenie atrybutów plików na serwerze.

Na serwerze umieszczone są pliki.

Chodzi o to, że pliki powinny mieć **atrybut 644** (-rw-r--r--) gdzie:

Właściciel: czyta i pisze

Grupa: czyta

Inni: czyta

Więc *nie dopuszczalne są atrybuty na plikach 664 lub 666 !!!*

Katalogi **atrybut 755** (drwxr-xr-x) czyli

r – czytanie

Dostęp do katalogu oznacza, że użytkownik może odczytać zawartość. Użytkownik może spojrzeć na nazwy plików w katalogu.

w – pisanie

Dostęp oznacza, że użytkownik może dodawać lub usuwać pliki z katalogu.

x – wykonywanie

Wykonywanie katalogu naprawdę nie ma sensu, więc pomyśl o tym jako o uprawnieniu do przechodzenia.

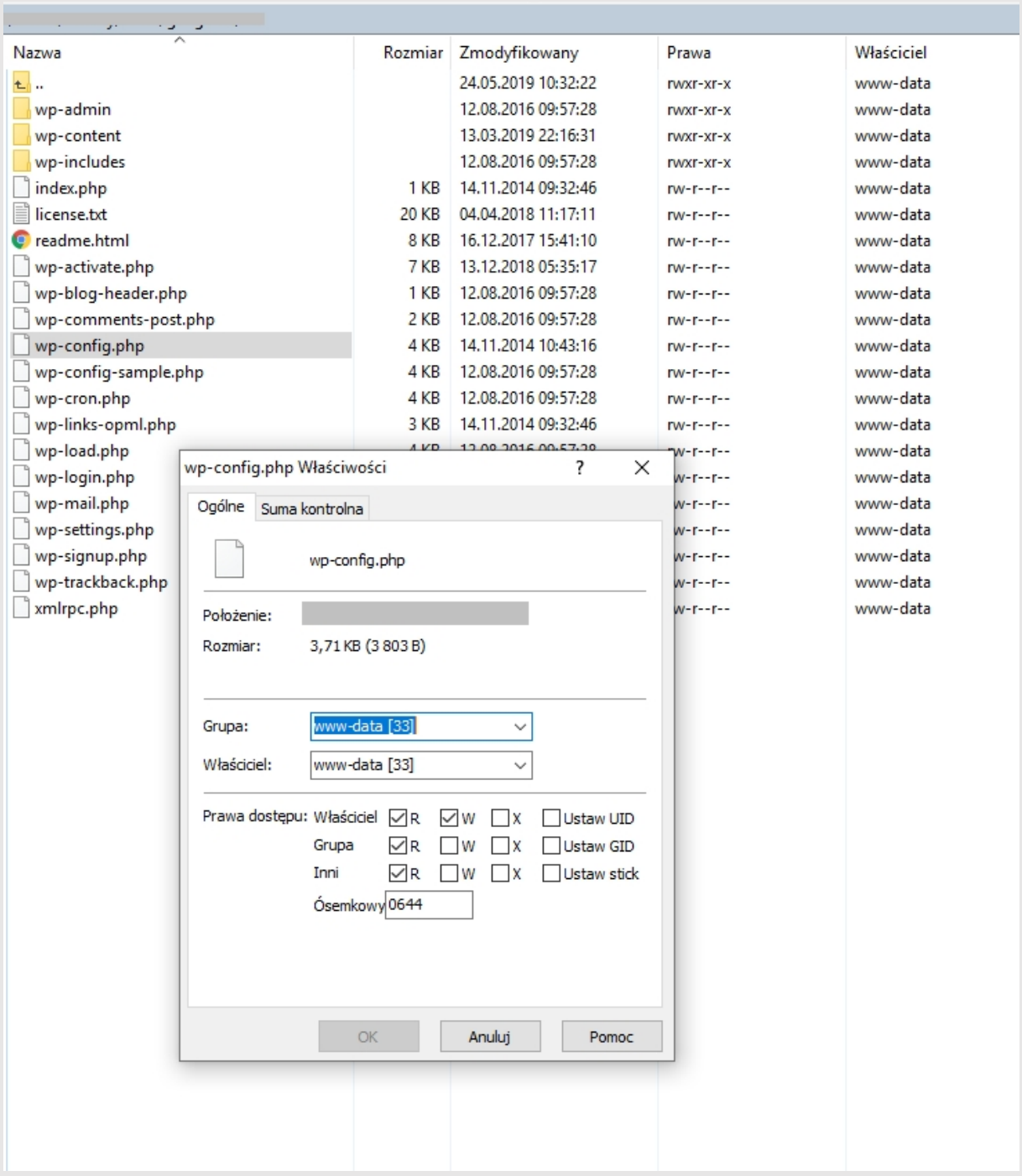
W tym przypadku także *niedopuszczalne jest, aby katalog miał atrybut 775 lub 777*

Koniecznie sprawdź na serwerze swój katalog ,,***uploads'*** w ścieżce:

,, /public_html/wp-content'' lub ,, /private_html/wp-content''

oraz podkatalogi, czy ***nie posiadają one atrybutu 775 lub 777*** **!!!**

Zmiany atrybutów plików i katalogów możesz dokonać (po wcześniejszym backupie!) przez ***WinSCP lub TotalCommander***.



Dziękuję Ci za uwagę, mam nadzieję, że jest to dla Ciebie przydatne. Bardzo cenię Twój czas i jestem otwarty na opinię. Poniżej zapraszam Cię do kontaktu ze mną. Pamiętaj, że to właśnie Twoja opinia pozwoli mi bardziej dopracować poradnik lub stworzyć nowy z nowymi zagadnieniami.

Kontakt do autora:

Radek Rzążewski

Messenger: https://m.me/RadekRzazewskiOfficial

Mail: radek@VIParche.pl

WWW: www.rzazewski.pl

Twoja pierwsza strona WWW za mniej niż 50 zł:

www.arche.edu.pl

Nawet jeśli nie masz do mnie pytań, czy nie chcesz skorzystać z kursu, to proszę Ciebie, polub moją stronę na Facebooku, na której przedstawiam informacje z zakresu bezpieczeństwa, social media i szeroko pojętego IT – będzie mi bardzo miło. Do zobaczenia: http://bit.ly/2TuwMdY