Kilka porad jak zabezpieczyć stronę opartą o WordPress

Dominik Pietruszko - 2021-02-28 - 1 Comment - in WordPress

Skąd się to wzięło?

WordPress to najpopularniejszy skrypt do tworzenia stron Internetowych. Sprawdza się zarówno dla stron wizytówek, jak i dla dużych sklepów Internetowych. Popularność wiąże się jednak z konsekwencjami, a w przypadku WordPressa są to problemy z jego bezpieczeństwem.

Hakerzy bezustannie czyhają na najmniejszą lukę w którymś z elementów strony i niestety są w stanie szybko wykorzystać ją do wprowadzenia złośliwego kodu. Najczęściej taki kod jest implementowany w plikach strony, może jednak również wystąpić w samej bazie danych.

Czy jesteśmy w stanie się przed tym bronić?

Tak! I wcale nie musi być to skomplikowane. W zasadzie WordPress posiada własne systemy zabezpieczeń, które działają często poza naszą świadomością, a problem jest głównie w liczbie osób, które te zabezpieczenia próbują złamać. Oto co popularność robi z naszymi stronami...

My, jako firma hostingowa również posiadamy całą paletę zabezpieczeń, które chronią strony internetowe na naszych serwerach. Systemy i oprogramowania takie jak WAF (Web Application Firewall), Maldet, BitNinja i wiele innych (o których nie będziemy pisać, właśnie ze względów bezpieczeństwa), zapewniają kompleksową ochronę dla naszych stron, nieustannie przez dzień i noc.

W poniższych punktach przedstawimy metody zabezpieczenia stron opartych na WordPress. Z zastosowaniem większości porad będzie można w łatwy sposób samodzielnie sobie poradzić.

Przechodzimy zatem do zabezpieczenia strony!

Uwaga!

Przed wprowadzeniem zmian sugerujemy wykonać kopię bezpieczeństwa plików strony i

bazy danych do niej podpiętej, aby przy jakichkolwiek problemach w łatwy sposób można było ją odzyskać.

*Eksport bazy danych -> **Eksport bazy danych poprzez phpmyadmin***

*Pliki można pobrać za pośrednictwem połączenia z FTP -> **Konfiguracja połączenia FTP w programie Filezilla***

Uwaga 2!

Nie rekomendujemy instalacji dużych wielofunkcyjnych wtyczek do zabezpieczeń, najczęściej tylko spowalniają stronę i mogą uniemożliwiać skuteczną analizę infekcji wirusowej, gdy do takiej dojdzie.

Podobnie jest z przywróceniem strony z backupu, jeśli były już na niej wirusy, ale strona jeszcze działała, może to zdecydowanie utrudnić wspomnianą już wcześniej analizę.

1. Częste aktualizacje są jedną z najważniejszych kwestii, jeśli chodzi o zabezpieczenie Wodpress'a. Należy aktualizować każdy element, czyli wtyczki, motyw, jak również całego WordPressa, gdy tylko jest to możliwe. W takich aktualizacjach najczęściej znajdują się dodatkowe zabezpieczenia. Dzięki temu będziemy również mogli utrzymać szybkie działanie strony. Zalecamy używanie jak najwyższej wersji PHP dla domeny lub jedną wersję niżej. Zmienić wersję PHP można przy pomocy poniższego poradnika:

Jak zmienić wersję PHP dla domeny

Do wszelkich modyfikacji oraz aktualizacji skryptów zalecamy środowisko testowe(kopia oryginalnej strony pod innym adresem) w którym będziemy dokonywać modyfikacji przed wprowadzeniem ich do życia na głównym adresie.

Po wszelkich modyfikacjach nie zapomnij wyłączyć trybu debugowania jeżeli był uruchomiony. Sprawdzić to możesz z poziomu pliku wp-config.php, jeżeli pojawia się w nim poniższa wartość, oznacza to że tryb jest włączony:

define('WP_DEBUG', true);

Aby dezaktywować tryb, należy zmienić wartość true, na false według poniższego przykładu:

define('WP_DEBUG', false);

2. Redukcja wtyczek,

zarówno tych niepotrzebnych jak i tych, które nie są już rozwijane i są nieaktualne. W przypadku usunięcia nie rozwijanych wtyczek należy rozważyć czy usunięcie ich nie zakłóci kluczowej funkcjonalności strony. Mniejsza ilość wtyczek prawdopodobnie zapewni mniej luk bezpieczeństwa dla strony, a także powinna zwiększyć szybkość jej ładowania. Dodatkowo,

zalecamy sprawdzenie czy wtyczki oraz motyw, z którego korzystamy pochodzą ze sprawdzonego i zaufanego źródła.

3. Wyłączenie możliwości edycji wtyczek/motywu z poziomu Panelu WordPressa. Aby wyłączyć edycję, wystarczy dodać poniższy wpis do pliku wp-config.php, który znajduje się w głównym katalogu strony:

define('DISALLOW_FILE_EDIT', true);

Linijkę tę najlepiej dodać na samym końcu pliku.

4. Uwierzytelnianie dwuskładnikowe jest dobrym rozwiązaniem dla bezpieczeństwa wewnętrznego, jednak wiąże się z tym instalacja odpowiedniej aplikacji na urządzeniu mobilnym > Google Authenticator. Podczas logowania do Panelu Administracyjnego strony, będzie wysyłany specjalny kod na telefon, który będzie należało wpisać w odpowiednie pole. Opcja jest tylko dostępna dla urządzeń mobilnych z systemem Android lub iOS.

Aby skorzystać z tego rozwiązania, należy zainstalować wtyczkę **Two Factor Authentication**.

5. Blokada dla nieautoryzowanych logowań do wp-admin poprzez odpowiedni wpis w .htaccess. Chodzi dokładnie o pozwolenie na logowanie dla konkretnego adresu IP (może być to problematyczne gdy mamy dynamicznie przypisywany adres IP w swojej sieci) i blokadzie wszystkich innych adresów. Oto wpis:

<Files wp-login.php>

order allow,deny

allow from 1.2.3.4

</Files>

Zamiast 1.2.3.4 należy wpisać swój adres IP. Ten adres można sprawdzić po przejściu na poniższy adres:

Adres IP

6. Dobrym pomysłem jest również zablokowanie wykonywania się potencjalnych wirusów w katalogu wp-content/uploads, wystarczy jak w poprzednim punkcie dodać poniższy wpis do pliku .htaccess:

<FilesMatch "\.(?i:php)$">

Order Deny, Allow

Deny From All

</FilesMatch>

i moze dla wp-includes:

wp-includes/.htaccess

<FilesMatch "\.(?i:php)$">

Order Deny, Allow

Deny From All

</FilesMatch>

<Files wp-tinymce.php>

Allow From All

</Files>

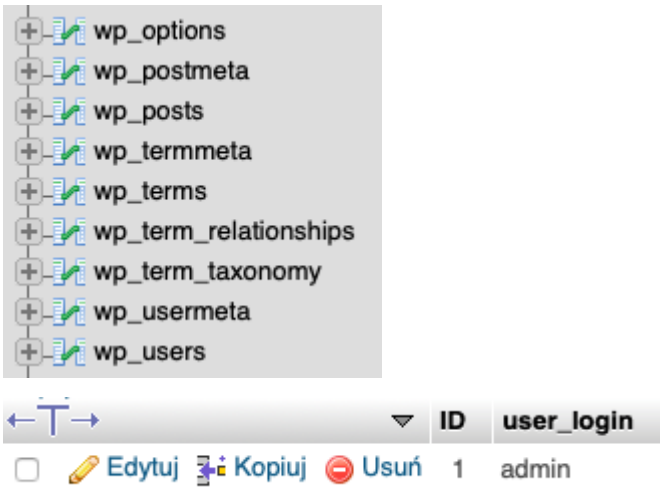
<Files ms-files.php>

Allow From All

</Files>

Po dodaniu wpisu, zalecamy przetestować działanie strony.

7. Nie używaj loginu “admin” dla konta administracyjnego. Jak już wspomnieliśmy wyżej, jest to domyślna nazwa konta administracyjnego podczas instalacji WordPress. Gdy posiadamy swój własny login, dostęp do Panelu Administracyjnego strony będzie znacznie utrudniony. Zalecamy już przy samym tworzeniu strony WWW ustawić swoją własną nazwę. Login możemy również zmienić z poziomu phpmyadmin w bazie danych. Wystarczy przejść do tabeli “_users” i edytować go dla konkretnego użytkownika.

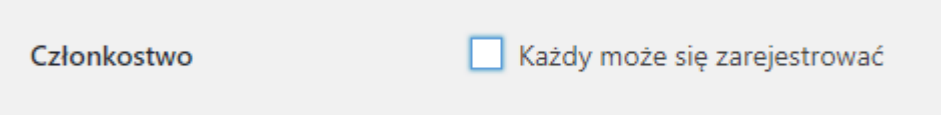


Dodatkowo, proponujemy zmienić również wartość ID na kilku cyfrową np. 12123.

8. Włącz szyfrowanie na stronie poprzez instalację certyfikatu SSL i konfigurację WordPress’a, aby strona była do tego przystosowana. Certyfikat można zakupić z poziomu sklepu, bezpośrednio w Panelu Klienta naszej firmy. Można również skorzystać z bezpłatnego certyfikatu Let’s Encrypt.

Poradnik, który opisuje dostosowanie WordPress’a do połączenia szyfrowanego -> **Jak włączyć protokół HTTPS na WordPress**

9. Jeśli rejestracja nowych użytkowników nie jest wymagana (na przykład dla strony statycznej), można ją wyłączyć. Jest to dobre zabezpieczenie przed tworzeniem nowych kont przez hakerów. Aby tego dokonać należy przejść do Panelu Administracyjnego strony i z menu po lewej stronie kliknąć “Settings” i odznaczyć opcję “Członkostwo Każdy może się zarejestrować”.



10. Używaj jak najmocniejszych haseł składających się z wielu różnych znaków. Hasła są łamane coraz szybciej, ale jakość ustawianych haseł niestety nie idzie z tym w parze.

Proponujemy użyć generator haseł zamieszczony na poniższej stronie:

Generator haseł zenbox

11. Zmień domyślny prefix dla tabel z “wp_” na własny podczas instalacji WordPressa. Dzięki temu osoby, które będą próbowały wstrzykiwać złośliwy kod (SQL Injection), będą miały utrudnione zadanie. Można również zmienić prefix dla tabel w bazie dla już istniejącej strony, wiąże się to jednak z mniej lub bardziej skomplikowaną konfiguracją, która może doprowadzić do problemów z połączeniem strony z bazą danych.

12. Sprawdź uprawnienia do plików i katalogów na koncie FTP dla strony. Prawidłowe uprawnienia dla plików to 644, a dla katalogów 755. Jedynym wyjątkiem jest plik wp-config.php, dla którego uprawnienia powinny być ustawione na 600 lub 640 dla dodatkowej ochrony.

13. Blokowanie dostępu do XML-RCP ze względu na możliwość ataku typu Brute Force. W przypadku gdy nie korzystasz z jego interfejsu, możesz go zablokować dodając w pliku .htaccess odpowiednią regułę:

<files xmlrpc.php>

order deny,allow

deny from all

</files>

Po wprowadzeniu modyfikacji, należy dokonać weryfikacji poprawnego funkcjonowania strony.

14. W przypadku gdy Twoja strona oparta o WordPress, nie wymaga systemu komentowania zachęcamy do ich wyłączenia. Wyłączyć komentarze możesz z poziomu kokpitu WordPressa bez żadnych dodatkowych wtyczek. A zrobisz to w poniższy sposób:

Wyłączenie dla starych materiałów:

a) Zaloguj się do kokpitu WordPressa.

b) Po zalogowaniu do kokpitu, z opcji w menu wybierz Wpisy lub Strony.

c) Podczas dodawania nowego, lub edycji istniejącego wpisu lub strony, odznacz w edytorze z prawego domyślnego menu z sekcji Dyskusja opcję Zezwól na komentarze.

d) Po wprowadzeniu modyfikacji, Zaktualizuj lub Opublikuj zmianę.

Automatyczne wyłączenie dla nowo dodawanych:

a) Zaloguj się do kokpitu WordPressa.

b) W kokpicie, kliknij w menu na pozycję Ustawienia, następnie z rozwiniętych opcji wybierz Dyskusja.

c) W sekcji Domyślne ustawienia nowych artykułów, odznacz pozycję Zezwól na komentowanie nowych artykułów.

d) Zapisz zmianę.

15. Ustaw unikatowe klucze uwierzytelniania. Jeżeli instalowałeś WorPressa ręcznie i nie zadbałeś o te wartości, lub instalowałeś WordPressa z poziomu Installatrona(nasz Installastron generuje unikatowe klucze) - zalecamy wygenerowanie nowych, na poniższej stronie i podmianę ich na nowe w pliku wp-config.php:

Generator unikalnych kluczy

Wspomniane klucze, zabezpieczają dane przechowywane w ciasteczkach.

Comments (1)

Adam Skawiński
21.08.2019
17:08:21

Warto też zablokować w php.ini dyrektywą disable_functions funkcje chmod i chown, a następnie wszystkie domyślne pliki .php WordPressa oraz większość jego folderów pozbawić praw do zapisu nawet dla właściciela. To uniemożliwi zapisanie złośliwych plików lub podmianę kodu z poziomu jakiegoś włamania, jeśli już takie nastąpi.