Dane aktualne na dzień: 20-05-2024 09:45

Link do produktu: https://follow.pl/wp-craft-box-50-gb-p-34.html

WP Craft BOX 50 GB

Cena brutto	**500,00 zł**
Cena netto	**406,50 zł**
Dostępność	**Dostępny**

Opis produktu

WP Craft BOX 50 GB

- Powierzchnia 50 GB SSD nVME
- Certyfikat Let’s Encrypt DV
- Protokół HTTP/2.0
- Kompresja .gzip
- PHP 7.1 – 8.0+
- Kopia zapasowa 28 dni
- Nielimitowane konta e-mai
- Baza danych MariaDB, v10.3.27
- Brak limitu transferu
- Dedykowane narzędzia do WordPress

Aplikacje dedykowane dla WordPress:

- Zarządzanie bezpieczeństwem WP Toolkit
- Zarządzanie klonowaniem WP Toolkit
- Zarządzanie synchronizacją WP Toolkit
- Inteligentna aktualizacja PHP w WP Toolkit

Zarządzanie bezpieczeństwem WP Toolkit

Możesz zastosować następujące środki w celu poprawy bezpieczeństwa stron internetowych WordPress. Należy pamiętać, że niektóre środki bezpieczeństwa można cofnąć, a niektóre nie. Zalecamy wykonaj kopię zapasową swojej witryny przed zabezpieczeniem witryny WordPress.

- Blokowanie nieautoryzowanego dostępu do xmlrpc.php
- Ograniczenie dostęp do plików i katalogów
- Skonfigurowanie klucza bezpieczeństwa
- Blokowanie przeglądanie katalogów
- Blokada wykonywania skryptów PHP w katalogu wp-includes
- Blokada wykonywania skryptów PHP w katalogu wp-content/uploads

- Blokada nieautoryzowanego dostępu do wp-config.php
- Wyłączenie łączenia skryptów dla panelu administracyjnego WordPress
- Wyłączenie pingbacki
- Wyłączenie wykonywania PHP w katalogach pamięci podręcznej
- Wyłączenie edycji plików w Panelu WordPress
- Zmiana domyślna prefiks tabeli bazy danych
- Włączenie ochrony przed botami
- Blokada dostęp do poufnych plików
- Blokada dostęp do potencjalnie wrażliwych plików
- Blokada dostęp do plików .htaccess i .htpasswd
- Blokada skanowanie autora
- Zmiana domyślna nazwy użytkownika administratora
- Ochrona przed hotlinkowaniem

Zarządzanie klonowaniem WP Toolkit

- Umożliwia klonowanie stron internetowych WordPres

Zarządzanie synchronizacją WP Toolkit

- Pozwala kopiować pliki i bazy danych między stronami WordPress

Inteligentna aktualizacja PHP w WP Toolkit

- Pozwala korzystać z funkcji Smart PHP Update w WP Toolkit.

WP Toolkit - szczegóły funkcji

Zarządzanie bezpieczeństwem WP Toolkit

Możesz zastosować następujące środki w celu poprawy bezpieczeństwa stron internetowych WordPress. Należy pamiętać, że niektóre środki bezpieczeństwa można cofnąć, a niektóre nie. Zalecamy wykonaj kopię zapasową swojej witryny przed zabezpieczeniem witryny WordPress.

Blokowanie nieautoryzowanego dostępu do xmlrpc.php

- Ten środek bezpieczeństwa zapobiega nieautoryzowanemu dostępowi do pliku xmlrpc.php. Ten środek modyfikuje plik konfiguracyjny serwera (Apache, nginx dla systemu Linux lub web.config dla systemu Windows). Pamiętaj, że niestandardowe dyrektywy w plikach .htaccess lub web.config mogą to zastąpić.

Ograniczenie dostęp do plików i katalogów

- Jeśli uprawnienia dostępu do plików i katalogów nie są wystarczająco bezpieczne, hakerzy mogą uzyskać dostęp do tych plików i wykorzystać je do złamania zabezpieczeń witryny. Ten środek bezpieczeństwa ustawia uprawnienia dla pliku wp-config na 600, dla innych plików na 644, a dla katalogów na 755.

Skonfigurowanie klucza bezpieczeństwa

- WordPress używa kluczy bezpieczeństwa (AUTH_KEY, SECURE_AUTH_KEY, LOGGED_IN_KEY oraz NONCE_KEY), aby zapewnić lepsze szyfrowanie informacji przechowywanych w plikach cookie użytkownika. Dobry klucz bezpieczeństwa powinien być długi (60 znaków lub więcej), losowy i złożony. Kontrola bezpieczeństwa powinna sprawdzić, czy klucze bezpieczeństwa są skonfigurowane i czy zawierają co najmniej znaki alfabetyczne i numeryczne.

Blokowanie przeglądanie katalogów

- Jeśli przeglądanie katalogów jest włączone, hakerzy mogą uzyskać różne informacje o Twojej witrynie, które mogą potencjalnie zagrozić jej bezpieczeństwu. Przeglądanie katalogów jest zwykle domyślnie wyłączone, ale jeśli jest

włączone, ten środek bezpieczeństwa może je zablokować. Środek ten modyfikuje plik konfiguracyjny serwera (Apache, nginx w systemie Linux lub web.config w systemie Windows). Zauważ, że niestandardowe dyrektywy w plikach .htaccess lub web.config mogą to zastąpić.

Blokada wykonywania skryptów PHP w katalogu wp-includes

- Katalog wp-includes może zawierać niezabezpieczone pliki PHP, które można wykonać w celu przejęcia i wykorzystania witryny. Ten środek bezpieczeństwa uniemożliwia wykonanie plików PHP w katalogu wp-includes. Ta zmiana modyfikuje plik konfiguracyjny serwera (Apache, nginx dla Linux lub web.config dla Windows). Pamiętaj, że spersonalizowane dyrektywy w plikach .htaccess lub web.config mogą to napisać.

Blokada wykonywania skryptów PHP w katalogu wp-content/uploads

- Katalog wp-content/uploads może zawierać niezabezpieczone pliki PHP, które można wykonać w celu przejęcia i wykorzystania witryny. Ten środek bezpieczeństwa uniemożliwia wykonanie plików PHP w katalogu wp-content/uploads. Ta zmiana modyfikuje plik konfiguracyjny serwera (Apache, nginx dla Linux lub web.config dla Windows). Pamiętaj, że spersonalizowane dyrektywy w plikach .htaccess lub web.config mogą to napisać.

Blokada nieautoryzowanego dostępu do wp-config.php

- Plik wp-config.php zawiera poufne informacje, takie jak poświadczenia dostępu do bazy danych i tym podobne. Jeśli z jakiegoś powodu przetwarzanie plików PHP przez serwer WWW jest wyłączone, hakerzy mogą uzyskać dostęp do zawartości pliku wp-config.php. Ten środek bezpieczeństwa zapobiega nieautoryzowanemu dostępowi do pliku wp-config.php. Ta zmiana modyfikuje plik konfiguracyjny serwera (Apache, nginx dla Linux lub web.config dla Windows). Pamiętaj, że spersonalizowane dyrektywy w plikach .htaccess lub web.config mogą to napisać.

Wyłączenie łączenia skryptów dla panelu administracyjnego WordPress

- Ten proces bezpieczeństwa wyłącza łączenie skryptów uruchomionych w panelu administracyjnym WordPress, zapobiegając atakom DoS na Twoją witrynę. Wyłączenie łączenia skryptów może nieznacznie wpłynąć na wydajność panelu administracyjnego WordPress, ale nie powinno to wpłynąć na twoją witrynę WordPress z punktu widzenia odwiedzających.

Wyłączenie pingbacki

- Pingbacki pozwalają innym stronom WordPress automatycznie zostawiać komentarze pod twoimi postami, gdy te strony linkują do tych postów. Pingbacki mogą być używane do uruchamiania ataków DDoS ukierunkowanych na Twoją stronę internetową. Ten środek bezpieczeństwa wyłącza pingbacki XML-RPC dla całej witryny, a także wyłącza pingbacki dla wcześniej utworzonych postów z włączoną funkcją pingback.

Wyłączenie wykonywania PHP w katalogach pamięci podręcznej

- Jeśli zainfekowany plik PHP trafi do jednego z katalogów pamięci podręcznej Twojej witryny, wykonanie go może doprowadzić do naruszenia bezpieczeństwa całej witryny. Ta miara bezpieczeństwa wyłącza wykonywanie plików PHP w katalogach pamięci podręcznej, uniemożliwiając takie exploity. Zauważ, że niektóre wtyczki lub motywy mogą ignorować zalecenia bezpieczeństwa z zespołu bezpieczeństwa WordPress i przechowywać poprawne pliki PHP w ich katalogu pamięci podręcznej. Może być konieczne wyłączenie tego środka bezpieczeństwa, jeśli chcesz, aby takie wtyczki lub motywy działały.

Wyłączenie edycji plików w Panelu WordPress

- Wyłączenie edytowania plików w WordPress usuwa możliwość bezpośredniej edycji źródeł wtyczek i plików motywów w interfejsie WordPress. Ta miara dodaje dodatkową warstwę ochrony dla witryny WordPress w przypadku naruszenia bezpieczeństwa jednego z kont administratora WordPress. W szczególności zapobiega to łatwemu dodawaniu złośliwego kodu wykonywalnego do wtyczek lub kompozycji.

Zmiana domyślna prefiks tabeli bazy danych

- Tabele bazy danych WordPress mają takie same standardowe nazwy na wszystkich instalacjach WordPress. Gdy standardowy prefiks wp_ jest używany dla nazw tabel bazy danych, cała struktura bazy danych WordPress jest przejrzysta, co ułatwia szkodliwym skryptom uzyskiwanie z niej danych. Ten środek bezpieczeństwa zmienia prefiks nazwy tabeli bazy danych na coś innego niż domyślny prefiks wp_. Należy pamiętać, że zmiana prefiksu bazy danych na stronie internetowej z danymi produkcyjnymi może być niebezpieczna, dlatego zaleca się wykonanie kopii zapasowej witryny przed zastosowaniem tej miary.

Włączenie ochrony przed botami

- Ten środek chroni twoją stronę przed nieużytecznymi, złośliwymi lub w inny sposób szkodliwymi botami. Blokuje boty, które skanują Twoją witrynę pod kątem luk w zabezpieczeniach i przeciążają Twoją witrynę niepożądanymi żądaniami, co powoduje nadużywanie zasobów. Zauważ, że możesz tymczasowo wyłączyć tę miarę, jeśli zamierzasz użyć usługi online do skanowania witryny pod kątem luk, ponieważ te usługi mogą również używać takich botów.

Blokada dostęp do poufnych plików

- Ten środek bezpieczeństwa uniemożliwia publiczny dostęp do niektórych plików, które mogą zawierać poufne informacje, takie jak poświadczenia połączenia lub różne informacje, które mogą być wykorzystane do określenia, które znane exploity mają zastosowanie do Twojej witryny WordPress.

Blokada dostęp do potencjalnie wrażliwych plików

- Ten środek bezpieczeństwa uniemożliwia publiczny dostęp do niektórych plików (na przykład plików dziennika, skryptów powłoki i innych plików wykonywalnych), które mogą funkcjonować na stronie internetowej WordPress. Publiczny dostęp do tych plików może potencjalnie zagrozić bezpieczeństwu Twojej witryny WordPress.

Blokada dostęp do plików .htaccess i .htpasswd

- Uzyskanie dostępu do plików .htaccess i .htpasswd pozwala atakującym na poddanie Twojej witryny różnym exploitom i naruszeniom bezpieczeństwa. Ten środek bezpieczeństwa gwarantuje, że pliki .htaccess i .htpasswd nie będą dostępne dla osób niepowołanych.

Blokada skanowanie autora

- Skany autorów szukają nazw użytkowników zarejestrowanych (zwłaszcza administratorów WordPressa) i atakują metodą brute-force stronę logowania Twojej witryny, aby uzyskać do niej dostęp. Ten środek bezpieczeństwa uniemożliwia takim skanom poznanie tych nazw użytkowników. Pamiętaj, że w zależności od konfiguracji permalinków w Twojej witrynie, ten środek może uniemożliwić odwiedzającym dostęp do stron zawierających listę wszystkich artykułów napisanych przez określonego autora.

Zmiana domyślna nazwy użytkownika administratora

- Podczas instalacji WordPress tworzy użytkownika z uprawnieniami administracyjnymi i nazwą użytkownika „admin”. Ponieważ nazwy użytkowników w WordPressie nie mogą być zmieniane, możliwe jest wprowadzenie hasła tego użytkownika za pomocą metody "brute force", aby uzyskać dostęp do WordPressa jako administratora. Ten środek bezpieczeństwa tworzy konto administratora WordPress z losową nazwą użytkownika i zapewnia, że nie ma użytkownika z uprawnieniami administracyjnymi i nazwą użytkownika „admin”. Jeśli zostanie znaleziony użytkownik „admin”, cała zawartość należąca do tego użytkownika zostanie ponownie przypisana do nowego konta administratora, a konto użytkownika „admin” zostanie usunięte.

Ochrona przed hotlinkowaniem

- Ochrona typu Hotlink uniemożliwia innym witrynom wyświetlanie, łączenie lub osadzanie Twoich plików (zwykle obrazów). Ta praktyka nazywana jest hotlinkingiem i może szybko wyczerpać przepustowość i uniemożliwić dostęp do witryny.

Zarządzanie klonowaniem WP Toolkit

- Umożliwia klonowanie stron internetowych WordPres

Zarządzanie synchronizacją WP Toolkit

- Pozwala kopiować pliki i bazy danych między stronami WordPress

---

Inteligentna aktualizacja PHP w WP Toolkit

- Pozwala korzystać z funkcji Smart PHP Update w WP Toolkit.