# Jak zabezpieczyć stronę opartą na silniku WordPress?

Coraz więcej serwisów używa WordPressa, gdyż twierdzą, że jest szybciej, bardziej intuicyjny, ale samo korzystanie z niego nie jest w 100% do końca bezpiecznie, ponieważ hakerzy bardzo polują na ten silnik i zawiera w sobie dziury – dlatego dziś tu opisuję jak uniknąć nieprzewidzianych problemów.

1. Wybór hostingu

To jeden z najważniejszych punktów jeśli chodzi o zabezpieczenie. Większość właścicieli, administratorów stron internetowych sugeruje się bowiem ceną a przede wszystkim jego parametrami – gdyż w głównej mierze zależy od tego czy strona jest w stanie się chronić przed atakami hakerskimi.

A przede wszystkim warto zwrócić uwagę na to czy:

- posiada najnowszą wersję PHP - obecnie 8.0,
- czy wykonywane są kopie bazy danych, plików oraz czy mamy do nich bezpłatny dostęp,
- czy ma ochronę przeciwko atakom DDoS.

2. Aktualizacja silnika WordPress

Najlepiej co jakiś czas sprawdzać w swoim panelu czy nie ma dostępnych nowych łatek, jeśli są, to najlepiej je wszystkie zaktualizować, ponieważ dzięki temu możesz uchronić się przed nieprzewidzianymi problemami.

3. Zmiana strony logowania do panelu

Najczęściej na stronach spotykamy się z tego typu odnośnikami:

- twojastrona.pl/wp-login.php
- twojastrona.pl/wp-admin/

Musisz to zmienić!

Dlatego też, aby zmniejszyć ilość ataków typu brute-force za pomocą wtyczki Limit Login Attempts możemy ograniczyć liczbę logowań i zablokować użytkownika na określony czas.

Jeśli jednak chcemy całkowicie zabezpieczyć formularz logowania możemy zmienić jej lokalizację za pomocą wtyczki WPS Hide Login.

4. Nie ujawnianie wersji WordPressa i wtyczek w kodzie źródłowym strony

To kolejny czynnik, dzięki któremu osoby nieuprawnione mogą w zależności od wersji silnika (CMS), wtyczki wykorzystać to.

WordPress domyślnie wyświetla wersję w źródle strony dodając tag w sekcji HEAD:

<meta name="generator" content="WordPress 5.8.7" />

W przypadku wtyczek WordPress dopisuje do URL plików CSS i JS ?ver=X.X

```
t/block-library/style.min.css?ver=5.6.4' type='text/css' media='all'/>
t-form-7/includes/css/styles.css?ver=5.3.2' type='text/css' media='all'/>
ookie-notice/css/front.min.css?ver=5.6.4' type='text/css' media='all'/>
-multilingual-cms/templates/language-switchers/menu-item/style.css?ver=1' type=
A400%2C500%2C600%2C700%2C300%2C100%2C800%2C900%7COpen+Sans%3A400%2C300%2C300ita
ess/assets/css/animate.min.css?ver=33.5.9' type='text/css' media='all'/>
ssets/css/font-awesome.min.css?ver=4.7.0' type='text/css' media='all'/>
press/assets/css/bootstrap.min.css?ver=33.5.9' type='text/css' media='all'/>
s/style.css?ver=5.6.4' type='text/css' media='all'/>
```

Za pomocą informacji, o jakich wersjach używamy poszczególnych komponentów na stronie ułatwiamy pracę atakującym naszą stronę.

Wyświetlanie wersji można zablokować dodając poniższy kod do pliku functions.php znajdujący się w szablonie.

```
remove_action('wp_head', 'wp_generator');
add_filter('the_generator', '__return_empty_string');
function shapeSpace_remove_version_scripts_styles($src) {
    if (strpos($src, 'ver=')) {
        $src = remove_query_arg('ver', $src);
```

```
    }
    return $src;
}
add_filter('style_loader_src', 'shapeSpace_remove_version_scripts_styles', 9999);
add_filter('script_loader_src', 'shapeSpace_remove_version_scripts_styles', 9999);
```

## 5. Blokowanie dostępu do plików

Dzięki odpowiednim regułom w pliku .htaccess możemy zabezpieczyć dostęp do niektórych plików, folderów jakich chcemy. W tym punkcie skupimy się na dwóch plikach – najczęściej wykorzystywanymi przez hakerów.

W głównym folderze WP znajduje się plik xmlrpc.php i wp-config.php, który przechowuje dane do bazy danych MySQL, dlatego też warto dodatkowo zabezpieczyć te pliki dodając poniższą regułę w pliku.htaccess, który znajduje się w tym samym folderze.

```
<files wp-config.php>
order allow,deny
deny from all
</files>
<files xmlrpc.php>
    order allow,deny
    deny from all
</files>
```

Dodatkowo w katalogu /wp-content/uploads/ jeśli nie ma to tworzymy plik .htaccess i dodajemy poniższą regułę, która zablokuje wykonywania się niektórych wirusów:

```
<Files ~ "\.ph(?:p[345]?|t|tml)$">
   deny from all
</Files>
```

## 6. Zmiana danych logowania do panelu

Sposób I:

- zaloguj się do bazy danych poprzez phpMyAdmin,
- poszukaj tabelę wp_users,
- znajdź swoje konto, kliknij edytuj,
- w kolumnie user_login zmień stary login na nowy.

Sposób II:

- w panelu WP dodaj nowego użytkownika z uprawnieniami administratora,
- zaloguj się na nowe konto,
- usuń stare konto.

Pomyśl sobie o tym, że raz na kilka miesięcy zmieniasz hasła dla wszystkich administratorów swojej domeny. Szczególnie gdy Twoim loginem jest: adm, admin, administrator bądź nazwa strony.

7. Certyfikat SSL

Certyfikat SSL szyfruje wszelkie informacje wysyłane między przeglądarką użytkownika a stroną internetową. Każda profesjonalna firma hostingowa w swoich ofertach posiada płatne i darmowe certyfikaty SSL (np. Let's Encrypt) – dlatego takie istotne jest posiadanie takowego certyfikatu.

8. WAF czyli Web Application Firewall na stronę

Dobrym rozwiązaniem jest też zainstalowanie wtyczki do WP o nazwie „Web Application Firewall – website security". WAF/firewall śledzi ruch HTTP, który dociera do Twojej witryny/aplikacji internetowej. Zasadniczo monitoruje wszystkie żądania przychodzące do Twojej aplikacji internetowej/strony internetowej.

Jeśli WAF uzna, że przychodzące żądania są podejrzane, tj. jeśli przychodzące żądanie może zaszkodzić Twojej witrynie (np. żądanie może zawierać kod, który może wprowadzić pewne zmiany w Twojej bazie danych lub nieupoważniona osoba/haker mógłby uzyskać dostęp do Twojej aplikacja internetowa) WAF blokuje te żądania i zapobiega niechcianym atakom na Twoją witrynę internetową. Zasadniczo WAF filtruje i blokuje podejrzany lub niechciany ruch HTTP do aplikacji internetowej.

9.Odinstalowanie niepotrzebnych wtyczek i szablonów

Jeśli nie używasz niektórych wtyczek lub są Ci potrzebne sporadycznie – odinstaluj!

Masz zainstalowane więcej szablonów - odinstaluj, są Ci niepotrzebne. Do poprawnego działania potrzebny Ci jest ten, którego aktualnie używasz.

Należy zmniejszać ryzyko wszędzie tam, gdzie jest to możliwe. Nie ułatwiajmy życia hakerom i robotom!

## 10. Włącz dwustopniowe uwierzytelnianie

Dodatkowy poziom zabezpieczeń przy logowaniu jeszcze nikomu nie zaszkodził. Dzięki wtyczce Two Factor Authentication skonfigurujesz podwójne logowanie do panelu polegające na podaniu loginu z hasłem, a następnie unikalnego kodu, który zostanie przesłany na Twój smartfon.

Pamiętaj jednak, że to rozwiązanie wymaga również instalacji na smartfonie aplikacji Google Authenticator, dostępnej na Androidzie oraz iOS.

Jeżeli więc posiadasz telefon starszej generacji lub z innym systemem operacyjnym – dwustopniowe uwierzytelnianie nie będzie dla Ciebie dostępne.