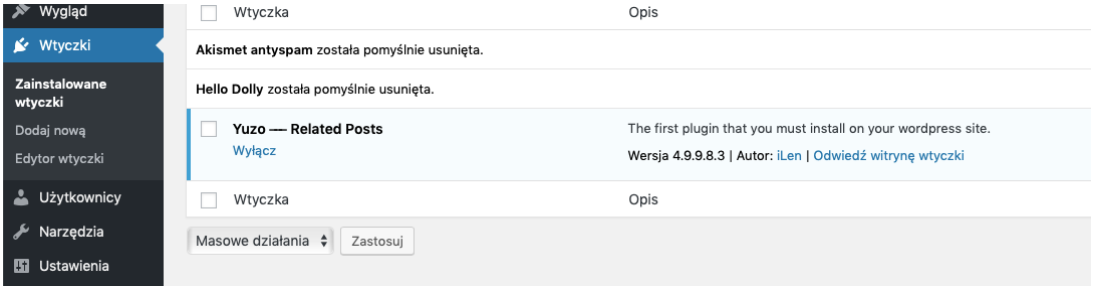
Usunięcie podatnej na infekcje wersji wtyczki Yuzo Related Posts oraz jej pozostałości.

Dominik Pietruszko - 2019-04-12 - 0 Comments - in WordPress

W celu usunięcia podatnej na infekcję wersji wtyczki z naszego WordPress a także jej przykrych następstw z bazy danych, niezbędne jest wykonanie poniższych kroków.

1. W pierwszej kolejności zaloguj się do swojego WordPressa i z sekcji **Wtyczki**, przy problematycznej wtyczce kliknij **Wyłącz**, następnie **Usuń**.



2. Kolejnym krokiem jest operacja na bazie danych, w celu dostania się do niej niezbędne jest uzyskanie danych dostępowych.

2.1 Aby tego dokonać, zaloguj się do swojego konta FTP według poniższej instrukcji:

Konfiguracja połączenia FTP w programie FileZilla.

2.2 Gdy zalogujesz się do konta FTP, przejdź do ścieżki ze swoim WordPressem, klikając kolejno:

domains > Adres_domeny.pl > public_html

Pobieramy z obecnej lokalizacji plik wp-config.php, dane dostępowe powinny być zadeklarowane w stałych z wartościami, gdzie:

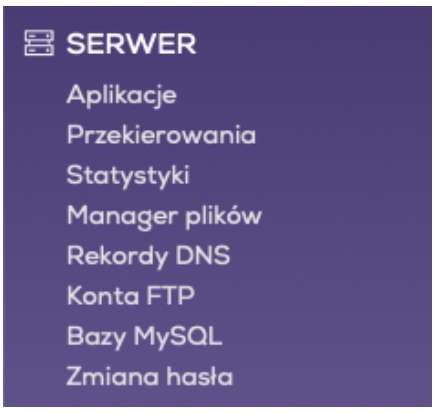
DB_NAME - Nazwa bazy danych

DB_USER - Nazwa użytkownika

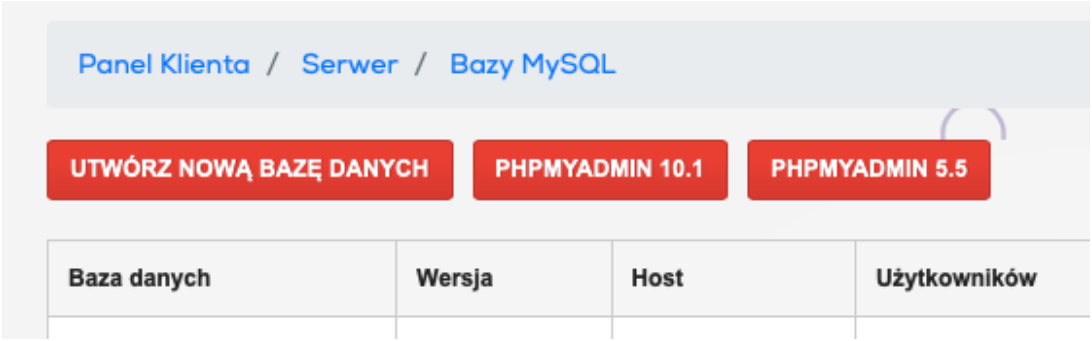
DB_PASSWORD - Hasło do bazy danych.

3.1 Gdy już posiadasz dane dostępowe do bazy danych, zaloguj się do **panelu Klienta** zenbox.

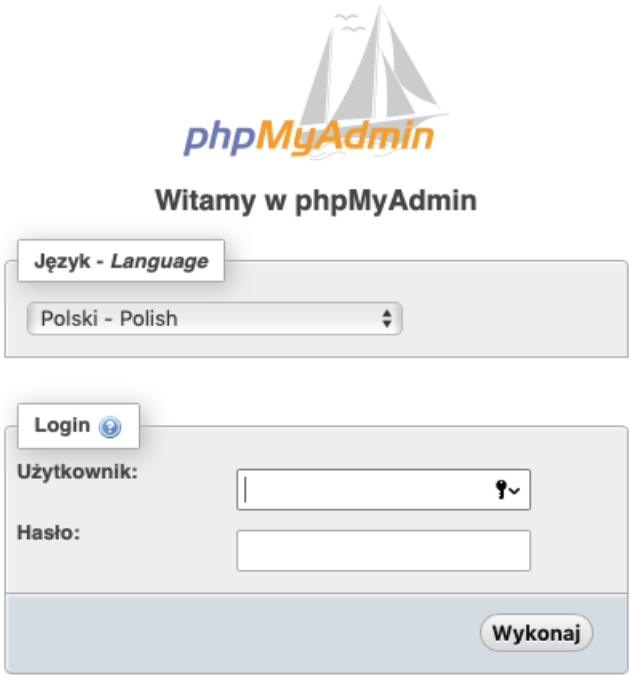
Następnie z sekcji **SERWER** wybierz pozycję **Bazy MySQL**.



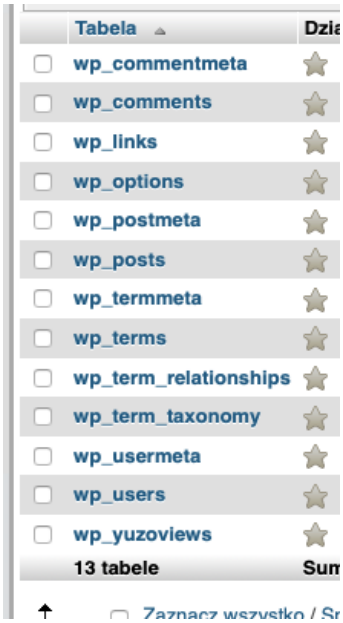
3.2 W wyświetlonej liście baz danych w kolumnie **Wersja** zweryfikuj jaką wersję bazy danych posiadasz i kliknij w przycisk odpowiadający **PHPMYADMIN** z Twojej bazy.



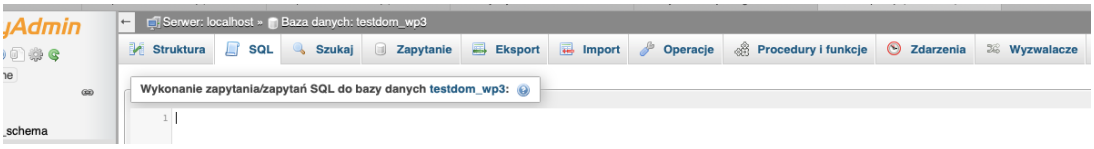
3.3 Przekierowanie przeniesie cię w miejsce logowania do **PHPMYADMIN** w które wprowadzasz uzyskane dane.



3.4 Z listy baz po lewej stronie ekranu, wybieramy naszą bazę danych i weryfikujemy prefiks jej tabel. W tym przypadku to **wp**.



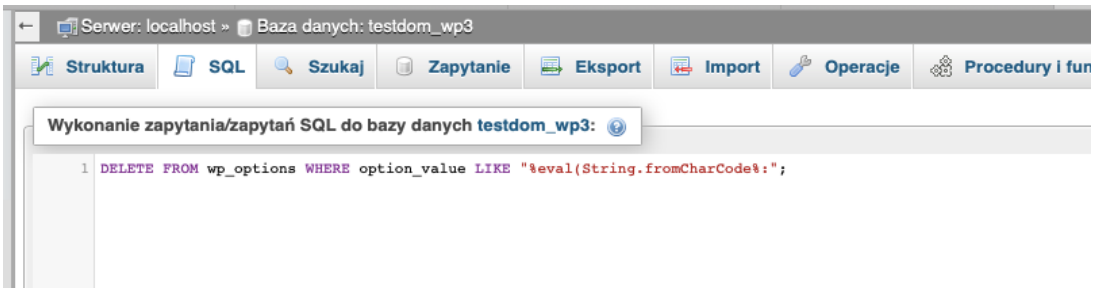
3.5 W celu ostatecznego wyczyszczenia infekcji spowodowanej wtyczką, niezbędne jest wprowadzenie zapytania które to wykona. W związku z powyższym z górnego menu wybieramy pozycję **SQL**.



Następnie wprowadzamy poniższe zapytanie:

```
DELETE FROM PREFIX_options WHERE option_value LIKE
"%eval(String.fromCharCode%:";
```

Gdzie **PREFIX** to prefiks naszych tabel, w tym przypadku to **wp**.



3.6 Zatwierdzamy zapytanie przyciskiem **Wykonaj** i potwierdzamy nasze działanie przyciskiem **Ok**.

3.7 Gdy zapytanie wykona się na całej tabeli, otrzymamy informujący nas o tym komunikat.

Powyższa procedura usunęła wtyczkę oraz jej szkodliwe pozostałości.