

Zabezpieczenie Joomla przed atakiem SQLInjection

Wpisany przez Jan Jackowicz-Korczyński
poniedziałek, 28 lutego 2011 03:20

Warto uzupełnić swój serwis oparty na CMS Joomla dodatkiem zabezpieczającym przed włamaniem za pomocą metody SQL Injection. (Dla mniej zorientowanych co to jest, zobacz: pl.wikipedia.org/wiki/SQL_injection).

Ciekawe rozwiązanie zaproponowała Jola Surma tworząc dodatek, zgrabnie nazwany: SPADAJ. Dostępny on jest do pobrania w serwisie: joomla.pl

Zainstalowany i opublikowany dodatek powoduje, że natręt, zamiast oryginalnego hasła, widzi dokładnie to, co chcemy mu pokazać np. komunikat "Spadaj na drzewo".

Wersja 1.5.1 oferuje:

- wyświetlanie zamiast hasła
- własnego tekstu
- zaszyfrowanego fałszywego hasła

- wybór, czyje hasła mają być chronione
- superadministratorów
- wszystkich mających dostęp do zaplecza
- wszystkich zarejestrowanych

- wybór powiadamiania o próbie ataku
- zapis do pliku - Data, IP, Referer (strona, na której użytkownik został przekierowany za pomocą odnośnika),
- Metoda (np. get), Przeglądarka i Połączenie.
- dodanie informacji do wiadomości administratora (panel administratora)
- zapis do pliku i wiadomość do administratora
- id administratora powiadamianego i id użytkownika traktowanego jako nadawcę do ustawienia w konfiguracji dodatku.

Zabezpieczenie Joomla przed atakiem SQLinjection

Wpisany przez Jan Jackowicz-Korczyński
poniedziałek, 28 lutego 2011 03:20

Po zainstalowaniu skonfigurować, włączyć i zapisać dodatek.

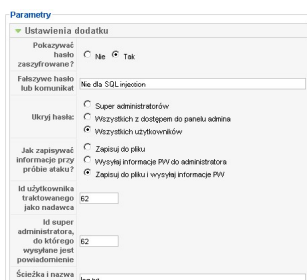
Aktualizacja polega na nadpisaniu plików, ustawieniu wybranych opcji i zapisaniu.

Dodatek Spadaj został przetestowany przez @trzepiza w "trudnych" warunkach i spisał się dobrze.

Testowanie może polegać na umieszczeniu w dowolnej części strony - kodu, który będzie uśiłował wyświetlać hasło pobrane z bazy danych.

(informacja cytowana z serwisu: pliki.joomla.pl/)

Poniżej opcje ustawienia dodatku:



The screenshot shows the 'Parametry' (Parameters) section for the 'Ustawienia dodatku' (Plugin Settings). The options are as follows:

- Pokazywać hasło zaszyfrowane?** (Show encrypted password?) - Radio buttons for 'Nie' (No) and 'Tak' (Yes). 'Nie' is selected.
- Falszywe hasło lub komunikat** (False password or message) - Text input field containing 'Nie do SQL injection'.
- Ukryj hasła:** (Hide passwords) - Radio buttons for 'Super administratorów' (Super administrators), 'Wszystkich z dostępem do panelu admina' (All with access to the admin panel), and 'Wszystkich użytkowników' (All users). 'Wszystkich użytkowników' is selected.
- Jak zapisywać informacje przy próbie ataku?** (How to save information on attack attempt?) - Radio buttons for 'Zapisuj do pliku' (Save to file), 'Wysyłaj informacje PIV do administratora' (Send PIV information to administrator), and 'Zapisuj do pliku i wysyłaj informacje PIV' (Save to file and send PIV information). 'Zapisuj do pliku i wysyłaj informacje PIV' is selected.
- Id użytkownika traktowanego jako nadzwyczajny** (ID of user treated as special) - Text input field containing '62'.
- Id super administratora, do którego wysyłane jest powiadomienie** (ID of super administrator to whom notification is sent) - Text input field containing '62'.
- Ścieżka i nazwa logów** (Log path and name) - Text input field.