

BEZPIECZEŃSTWO

Autor: szymo93 - 2007/12/21 23:10

Witam!

Chciałbym Was zapytać o bezpieczeństwo Joomla!

Chcę zrobić stronę ale boję się o bezpieczeństwo takiej strony na Joomla! i proszę o poradę: Jakiej użyć wersji Joomla!, jakie dodatki zainstalować żeby zwiększyć bezpieczeństwo?

Odp:BEZPIECZEŃSTWO

Autor: Jokris - 2007/12/23 08:38

B) Cześć.

B) Bezpieczeństwo Joomla! to jest bardzo szerokie i ogólne pojęcie. Pytasz o to, czy instalując Joomla na serwerze, nikt Cię nie zhackuje, nie podkradnie lub podrzuci jakieś "lewe" pliki?.

B) To jest tak jak z systemem operacyjnym na komputerze. Jedni będą uważać, że najlepszym programem antywirusowym jest np. Kaspersky Anti-Virus, a inni że Avast!. I jedni i drudzy mają rację. Bo dużo wolniejszy od Avasta! Kaspersky Anti-Virus przy zaniedbaniu przez Ciebie porządku na dyskach twardych komputera, może być prawie bezużyteczny (opinie na temat tych programów antywirusowych są oczywiście moje, i każdy może się z nimi nie zgadzać). A np. Avast! doskonale radzi sobie nawet przy "zapchanych" i zaśmieconych dyskach. Ale też może zdarzyć mu się "wpadka". Wszystko zależy więc nie tylko od samych programów, ale i środowiska, a właściwie jego stanu w jakim owe programy pracują.

Podobnie jest z Joomla!. Ja mam wersję Joomla 1.0.7, ale system mam zabezpieczony w każdy możliwy sposób. A to przez pliki .htaccess, a to przez specjalne pliki index.php. Znam wielu ludzi, którzy mają nowsze wersje Joomla!, i cięgle mają jakieś wrzutki na serwer, lub wiele innych objawów ingerencji osób niepowołanych w system plików Joomla!.

:laugh: Generalnie. Jak najwyższa wersja Joomla! (obecnie dostępna jedyna stabilna wersja, to Joomla 1.0.11, lub nieoficjalne wersje, wśród których znajdzie się moja modyfikacja CMS-a, wkrótce :cheer:), i dbanie o bezpieczeństwo serwera, stosując się do wielu poradników dostępnych w internecie. Bo cóż po tym, że ktoś ma Joomla 1.0.13 (najbezpieczniejsza wersja, ale z błędami!), skoro chmody plików, ze względu na niedbałość adminów serwera, lub może profesjonalność i wiedzę tych ludzi musi ustawiać na 777, co zdarza się często, i to nawet na poważnych serwerach. Taki niezabezpieczony dodatkowo plik, oczywiście poprzez odpowiednie wpisy, jest dostępny praktycznie dla każdego z zewnątrz. To samo dotyczy katalogów. Wystarczy wpisać frazę w Google "index of/ Joomla" a uzyskasz tysiące wyników z niezabezpieczonymi katalogami, oczywiście Joomla!. A przecież można w prosty sposób uniemożliwić tego rodzaju listowanie katalogów lub folderów na serwerze.

:laugh: Oczywiście, podstawowym zabezpieczeniem katalogu jest plik index.html, z tak zwanym "pustym body", lub własnym (przykład możesz znaleźć TUTAJ). Ale zdarza się czasami, że nie możemy tam wstawić tego pliku.

:laugh: Tworzymy wówczas plik .htaccess i dodajemy do niego tylko jeden wpis:

Options -Indexes

...nic więcej. Ten wpis wyśle polecenie do Apache, aby nie zezwalał na indeksowanie zawartości katalogu. I gdzie tylko to jest możliwe, możemy taki plik .htaccess wrzucić do katalogów. Przykład działania pliku .htaccess możesz zobaczyć na mojej stronie TUTAJ.

:laugh: Jeszcze inny sposób, to specjalny plik index.php, który ma za zadanie przekierowanie właścicielskiego delikwenta np. na Stronę Główną serwisu. Robimy to w ten sposób:

Kod 1:

```
<?php
header("Location: /" . $url);
die();
?>
```

Zadziałanie skryptu spowoduje przekierowanie do katalogu wyższego poziomu, o ile plik index.php, ten z cytowanym kodem znajduje się w podkatalogu root (głównym) Joomla!. Możesz zobaczyć działanie na następnym przykładzie, też z mojej strony TUTAJ.

Taki kod:

Kod 2:

```
<?php
header("Location: ../" . $url);
die();
?>
```

...też spowoduje przemieszczenie intruza do katalogu wyższego poziomu. Możemy zastosować coś w rodzaju drzewa, w którym to w katalogu poziomym najgłębiej umieszczamy index.php z kodu 1 lub 2. Następnie w każdym z katalogów poziomych "wyżej" w hierarchii drzewa wrzucamy ten sam plik index.php z kodu 1 lub 2. Spowoduje to przeskoczenie wszystkich katalogów od najgłębiej pożądanego do np. Strony Główniej. Poniżej masz linki, obrazujące strukturę drzewa katalogów. Umieściłem je w znacznikach <code> ze względu na ich długość. Ale pod nimi możesz zobaczyć efekt działania tej metody. Możemy ją nazwać "Drzewiasty Dostęp" lub "Schodowy Dostęp", albo raczej brak dostępu :P :

```
http://www.jokris.info/foldernajwyzej/foldernizej/foldernizej/foldernizej/foldernizej/foldernizej/foldernajnizej/
http://www.jokris.info/foldernajwyzej/foldernizej/foldernizej/foldernizej/foldernizej/foldernizej/
http://www.jokris.info/foldernajwyzej/foldernizej/foldernizej/foldernizej/foldernizej/
http://www.jokris.info/foldernajwyzej/foldernizej/foldernizej/foldernizej/
http://www.jokris.info/foldernajwyzej/foldernizej/foldernizej/
http://www.jokris.info/foldernajwyzej/foldernizej/
http://www.jokris.info/foldernajwyzej/
```

...co da efekt przeskoku. Sprawdź to klikając na poniższe linki:

- 1 - Najgłębiej pożąany katalog - Zobacz.
- 2 - Katalog wyżej - Zobacz.
- 3 - Katalog wyżej - Zobacz.
- 4 - Katalog wyżej - Zobacz.
- 5 - Katalog wyżej - Zobacz.
- 6 - Katalog wyżej - Zobacz.
- 7 - Katalog najwyższej pożąany - Zobacz.

B) Jeszcze jeden sposób, to ochrona dostępu do katalogów specjalnym plikiem do autoryzacji o nazwie .htpasswd, oraz plikiem .htaccess.

Zawartość pliku .htaccess powinna ogólnie wyglądać tak jak na poniższym kodzie:

```
AuthType Basic
AuthName "Katalogu"
AuthUserFile /home/x/x/x/user/www/katalog/.htpasswd
require valid-user
```

/home/x/x/x/user/www - jest to przykładowa ścieżka do pliku .htpasswd, i oczywiście możemy ją odczytać z pliku configuration.php ze zmiennej \$mosConfig_absolute_path. Jeśli chcemy dokładnie znać adres pożądanego pliku .htpasswd, wpisujemy poniższy kod do dowolnego Notatnika (najlepiej Notatnik SP), i zapisujemy go np. jako pathinfo.php.

Oto kod pliku pathinfo.php:

```
<?php
function dirnamepath(){
    $path_dirname = pathinfo(__FILE__);
    return $path_dirname;
}
$path_htpasswd = dirnamepath();
if (file_exists($path_htpasswd."/htpasswd")) {
    $file_htpasswd = 'htpasswd';
    echo $path_htpasswd."/htpasswd";
} else {
    $file_htpasswd = "";
    echo $path_htpasswd;
}
?>
```

Wrzucamy go do katalogu, który chcemy zabezpieczyć, i wywołujemy z adresu przeglądarki, dodając do naszego adresu strony ścieżkę do owego katalogu, np: administrator, czyli całość może wyglądać tak (link oczywiście przykładowy i nie zadziała na moim serwerze, ze względu na brak owego pliku pod tym adresem):

<http://www.jokris.info/pathinfo.php>

Wynikiem zadzia³ania skryptu bêdzie nasza ¶cie¿ka do katalogu, lub je¶li mamy plik .htpasswd, ca³a ¶cie¿ka któr± wpisujemy do pliku .htaccess. Poni¿ej ju¿ kod wynikowy pliku .htaccess wykorzystuj±cy pe³n± ¶cie¿kê z pliku pathinfo.php :

```
AuthType Basic
AuthName "Panel administratora Joomla"
AuthUserFile /home/x/x/x/user/www/administrator/.htpasswd
require valid-user
```

B) Teraz jak powinien wygl±daæ plik .htpasswd. Oto przyk³ad pliku .htpasswd:

Ksywausera:MQiTxpPIF/neI

Has³o jest zakodowane (zaszyfrowane!), wiêc mo¿esz skorzystaæ z "Generatora Has³a dla .htpasswd".

:laugh: Na koniec kilka uwag. Plik .htaccess z autoryzacj± dostêpu mo¿e znajdowaæ siê w dowolnym katalogu, czyli np. "/administrator/.htaccess", z tym ¿e musi byæ w nim okre¶lona w sposób opisywany powy¿ej ¶cie¿ka do pliku .htpasswd. Ten ostatni mo¿e znajdowaæ siê w innym katalogu ni¿ plik .htaccess. Wa¿ne aby trzymaæ siê opisanych przeze mnie zasad. To tyle. My¶lê ¿e ju¿ trochê wiesz o bezpieczeñstwie Joomla!. To naprawdê porz±dny CMS.

B) Pozdrawiam. Jokris.

=====

Odp:BEZPIECZEÑSTWO

Autor: szymo93 - 2007/12/23 19:11

Wielkie dziêki Jokris!! Bardzo mi pomog³e¶! :laugh: Super jest ten sposób "schodkowy" :cheer:

Mam jeszcze jedno pytanko, czyta³em gdzie¶ na forum jest komponent do zmiany nazwy, lokalizacji pliku konfiguracyjnego. Czy wiesz mo¿e jak siê on nazywa? Ja szuka³em i nie znalaz³em:blink:

=====

Odp:BEZPIECZEÑSTWO

Autor: ryantaylor - 2008/03/21 17:21

Czy oprócz powy¿szych rad jakie¶ inne zabezpieczenia s± porz±dane? Czy wogóle jakiegokolwiek inne istnieja? Je¶li tak to móg³bym prosiæ o jakie¶ porady? z tego powodu ze za³o¿ona przeze mnei strona w Joomla od pewnego momentu sta³a siê dla mnie niedostêpna nie mówi±c ju¿ o FTP strony, gdzie nagle nie mia³em dostêpu do FTPa nawet brak mo¿liwo¶ci wpisania nazwy konta i u¿ytkownika (wszystko za³o¿one na 60free), postanowi³em zadbaæ o bezpieczeñstwo strony, co mog³oby siê tak¿e innym u¿ytkownikom przydaæ, st±d moje pytanie :)

Pozdrawiam

=====

Odp:BEZPIECZEÑSTWO

Autor: ryantaylor - 2008/03/25 15:45

No ok. Ale nie rozumiem jednej rzeczy. Czy pliki .htaccess i index.php to maja byc pliki textowe? A dlaczego przed htaccess jest kopka? utworzenie takiego pliku z kropka na pocztku jest niemozliwe? Z tego wlasnie tego nie rozumiem i tkwie w tym matrwym punkcie

pozdrawiam

=====

Odp:BEZPIECZEÑSTWO

Autor: wespaz - 2008/04/06 11:53

No i stworzy³em taki plik .htaccess i wpisa³em Options -Indexes ale potem niestety moj± stronê wywali³o w powietrze:(
nie mogê siê do nie dostaæ a jak próbuje siê usun±æ za pomoc± joomla explorera ten plik z poziomu innej strony to mi
wyskakuje ¿e nie mam uprawnieñ:(

=====