

BEZPIECZEŃSTWO

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

Witam!

Chciał³em Was zapyta³ o bezpieczeństwo Joomla!

Chc³e zrobi³æ stron³æ ale boj³æ si³e o bezpieczeństwo takiej strony na Joomla! i prosz³æ o porad³ę: Jakiej uż³y³æ wersji Joomla!, jakie dodatki zainstalowa³æ ż³eby zwi³ększy³æ bezpieczeństwo?

Odp:BEZPIECZEŃSTWO

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

B) Cze³ł³æ.

B) Bezpieczeństwo Joomla! to jest bardzo szerokie i ogólne pojęcie. Pytasz o to, czy instaluj³c Joomla na serwerze, nikt Ci³e nie zhackuje, nie podkradnie lub podrzuci jakie³ś "lewe" pliki?

B) To jest tak jak z systemem operacyjnym na komputerze. Jedni b³ęd³± uważ³æ, ż³e najlepszym programem antywirusowym jest np. Kaspersky Anti-Virus, a inni ż³e Avast!. I jedni i drudzy maj³± racj³ę. Bo duż³o wolniejszy od Avasta! Kaspersky Anti-Virus przy zaniedbaniu przez Ciebie porz³±dku na dyskach twardych komputera, moż³e by³æ prawie bezużyteczny (opinie na temat tych programów antywirusowych s³± oczywi³ł³cie moje, i każ³dy moż³e si³e z nimi nie zgadza³æ). A np. Avast! doskonale radzi sobie nawet przy "zapchanych" i za³ł³mieconych dyskach. Ale też³ moż³e zdarzy³æ mu si³e "wpadka". Wszystko zależ³ne jest wi³ęc nie tylko od samych programów, ale i ł³rodowiska, a w³ał³ciwie jego stanu w jakim owe programy pracuj³±.

Podobnie jest z Joomla!. Ja mam wersj³ę Joomla 1.0.7, ale system mam zabezpieczony w każ³dy moż³liwy spos³ób. A to przez pliki .htaccess, a to przez specjalne pliki index.php. Znam wielu ludzi, którzy maj³± nowsze wersje Joomla!, i ci³±gle maj³± jakie³ś wrzutki na serwer, lub wiele innych objawów ingerencji osób niepowo³anych w system plików Joomla!.

:laugh: Generalnie. Jak najwyż³sza wersja Joomla! (obecnie dost³ępna jedyna stabilna wersja, to Joomla 1.0.11, lub nieoficjalne wersje, wł³ród których znajdzie si³e moja modyfikacja CMS-a, wkrótce :cheer:), i dbanie o bezpieczeństwo serwera, stosuj³c si³e do wielu poradników dost³ępnych w internecie. Bo c³ół po tym, ż³e kto³ś ma Joomla 1.0.13 (najbezpieczniejsza wersja, ale z b³ędami!), skoro chmody plików, ze wzgl³ędu na niedba³oł³æ adminów serwera, lub ma³± profesjonalnoł³æ i wiedz³ę tychż³e ludzi musi ustawia³æ na 777, co zdarza si³e cz³ęsto, i to nawet na p³atnych serwerach. Taki niezabezpieczony dodatkowo plik, oczywi³ł³cie poprzez odpowiednie wpisy, jest dost³ępny praktycznie dla każ³dego z zewn³±trz. To samo dotyczy katalogów. Wystarczy wpisa³æ fraz³ę w Google "index of/ Joomla" a uzyskasz tysi³±ce wyników z niezabezpieczonymi katalogami, oczywi³ł³cie Joomla!. A przecież³ moż³na w prosty spos³ób uniemoż³liwi³æ tego rodzaju listowanie katalogów lub folderów na serwerze.

:laugh: Oczywi³ł³cie, podstawowym zabezpieczeniem katalogu jest plik index.html, z tak zwanym "pustym body", lub w³asnym (przyk³ad moż³esz znaleź³æ TUTAJ). Ale zdarza si³e czasami, ż³e nie moż³emy tam wstawia³æ tego pliku.

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

Options -Indexes

...nic wi³ęcej. Ten wpis wył³le polecenie do Apache, aby nie zezwala³ na indeksowanie zawartoł³ci katalogu. I gdzie tylko to jest moż³liwe, moż³emy taki plik .htaccess wrzuci³æ do katalogów. Przyk³ad dział³ania pliku .htaccess moż³esz zobaczy³æ na mojej stronie TUTAJ.

:laugh: Jeszcze iny spos³ób, to specjalny plik index.php, który ma za zadanie przekierowanie wł³cibskiego delikwenta np. na Stron³ę Gł³ówna serwisu. Robimy to w ten spos³ób:

Kod 1:

```
<?php
header("Location: /"Â«Â»);
die();
?>
```

Zadział³anie skryptu spowoduje przekierowanie do katalogu wyż³szego poziomu, o ile plik index.php, ten z cytowanym kodem znajduje si³e w podkatalogu root (gł³ównym) Joomla!. Moż³esz zobaczy³æ dział³anie na nast³ępnym przyk³adzie, też³ 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 nazwa ścieżki dostępu 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:(

=====