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

Witam!

Chcia³em Was zapytaæ o bezpieczeñstwo Joomla!
Chcê zrobiæ stronê ale bojê siê o bezpieczeñstwo takiej strony na Joomli! i proszê o poradê: Jakiej u¿yæ wersji Joomli, jakie dodatki zainstalowaæ ¿eby zwiêkszyæ bezpieczeñstwo?

==========

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

B) Cze¶æ.
B) Bezpieczeñstwo Joomla! to jest bardzo szerokie i ogólne pojêcie. Pytasz o to, czy instaluj±c Joomla na serwerze, nikt Ciê nie zhackuje, nie podkradnie lub podrzuci jakie¶ "lewe" pliki?.

B) To jest tak jak z systemem operacyjnym na komputerze. Jedni bêd± uwa¿aæ, ¿e najlepszym programem antywirusowym jest np. Kaspersky Anti-Virus, a inni ¿e Avast!. I jedni i drudzy maj± racjê. Bo du¿o wolniejszy od Avasta! Kaspersky Anti-Virus przy zaniedbaniu przez Ciebie porz±dku na dyskach twardych komputera, mo¿e byæ prawie bezu¿yteczny (opinie na temat tych programów antywirusowych s± oczywi¶cie moje, i ka¿dy mo¿e siê z nimi nie zgadzaæ). A np. Avast! doskonale radzi sobie nawet przy "zapchanych" i za¶mieconych dyskach. Ale te¿ mo¿e zdarzyæ mu siê "wpadka". Wszystko zale¿ne jest wiêc nie tylko od samych programów, ale i ¶rodowiska, a w³a¶ciwie jego stanu w jakim owe programy pracuj±.
Podobnie jest z Joomla!. Ja mam wersjê Joomla 1.0.7, ale system mam zabezpieczony w ka¿dy mo¿liwy sposób. A to przez pliki .htaccess, a to przez specjalne pliki index.php. Znam wielu ludzi, którzy maj± nowsze wersje Joomla!, i ci±gle maj± jakie¶ wrzutki na serwer, lub wiele innych objawów ingerencji osób niepowo³anych w system plików Joomla!.

:laugh: Generalnie. Jak najwy¿sza wersja Joomla! (obecnie dostêpna jedyna stabilna wersja, to Joomla 1.0.11, lub nieoficjalne wersje, w¶ród których znajdzie siê moja modyfikacja CMS-a, wkrótce :cheer:), i dbanie o bezpieczeñstwo serwera, stosuj±c siê do wielu poradników dostêpnych w internecie. Bo có¿ po tym, ¿e kto¶ ma Joomla 1.0.13 (najbezpieczniejsza wersja, ale z b³êdami!), skoro chmody plików, ze wzglêdu na niedba³o¶æ adminów serwera, lub ma³± profesjonalno¶æ i wiedzê tych¿e ludzi musi ustawiaæ na 777, co zdarza siê czêsto, i to nawet na p³atnych serwerach. Taki niezabezpieczony dodatkowo plik, oczywi¶cie poprzez odpowiednie wpisy, jest dostêpny praktycznie dla ka¿dego z zewn±trz. To samo dotyczy katalogów. Wystarczy wpisaæ frazê w Google "index of/ Joomla" a uzyskasz tysi±ce wyników z niezabezpieczonymi katalogami, oczywi¶cie Joomla!. A przecie¿ mo¿na w prosty sposób uniemo¿liwiæ tego rodzaju listowanie katalogów lub folderów na serwerze.

:laugh: Oczywi¶cie, podstawowym zabezpieczeniem katalogu jest plik index.html, z tak zwanym "pustym body", lub w³asnym (przyk³ad mo¿esz znale¼æ TUTAJ). Ale zdarza siê czasami, ¿e nie mo¿emy tam wstawiæ tego pliku.

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

Options -Indexes

...nic wiêcej. Ten wpis wy¶le polecenie do Apache, aby nie zezwala³ na indeksowanie zawarto¶ci katalogu. I gdzie tylko to jest mo¿liwe, mo¿emy taki plik .htaccess wrzuciæ do katalogów. Przyk³ad dzia³ania pliku .htaccess mo¿esz zobaczyæ na mojej stronie TUTAJ.

:laugh: Jeszcze iny sposób, to specjalny plik index.php, który ma za zadanie przekierowanie w¶cibskiego delikwenta np. na Stronê G³owna serwisu. Robimy to w ten sposób:
Kod 1:

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

Zadzia³anie skryptu spowoduje przekierowanie do katalogu wy¿szego poziomu, o ile plik index.php, ten z cytowanym kodem znajduje siê w podkatalogu root (g³ównym) Joomla!. Mo¿esz zobaczyæ dzia³anie na nastêpnym przyk³adzie, te¿ z mojej strony TUTAJ.
Taki kod:
Kod 2:

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

...te¿ spowoduje przemieszczenie intruza do katalogu wy¿szego poziomu. Mo¿emy zastosowaæ co¶ w rodzaju drzewa, w którym to w katalogu po³o¿onym najg³êbiej umieszczamy index.php z kodu 1 lub 2. Nastêpnie w ka¿dym z katalogów po³o¿onych "wy¿ej" w hierarchii drzewa wrzucamy ten sam plik index.php z kodu 1 lub 2. Spowoduje to przeskoczenie wszystkich katalogów od najg³êbiej po³o¿onego do np. Strony G³ównej. Poni¿ej masz linki, obrazuj±ce strukturê drzewa katalogów. Umie¶ci³em je w znacznikach <code> ze wzglêdu na ich d³ugo¶æ. Ale pod nimi mo¿esz zobaczyæ efekt dzia³ania tej metody. Mo¿emy j± nazwaæ "Drzewiasty Dostêp" lub "Schodowy Dostêp", albo raczej brak dostêpu :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. Sprawd¼ to klikaj±c na poni¿sze linki:
1 - Najg³êbiej po³o¿ony katalog - Zobacz.
2 - Katalog wy¿ej - Zobacz.
3 - Katalog wy¿ej - Zobacz.
4 - Katalog wy¿ej - Zobacz.
5 - Katalog wy¿ej - Zobacz.
6 - Katalog wy¿ej - Zobacz.
7 - Katalog najwy¿ej po³o¿ony - Zobacz.

B) Jeszcze jeden sposób, to ochrona dostêpu do katalogów specjalnym plikiem do autoryzacji o nazwie .htpasswd, oraz plikiem .htaccess.
Zawarto¶æ pliku .htaccess powinna ogólnie wygl±daæ tak jak na poni¿szym 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 przyk³adowa czê¶æ ¶cie¿ki dostêpu do pliku .htpasswd, i oczywi¶cie mo¿emy j± odczytaæ z pliku configuration.php ze zmiennej $mosConfig_absolute_path. Je¶li chcemy dok³adnie znaæ adres po³o¿enia pliku .htpasswd, wpisujemy poni¿szy 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"Â«Â»)) {
$file_htpasswd = '.htpasswd';
echo $path_htpasswd."/.htpasswd";
} else {
$file_htpasswd = '';
echo $path_htpasswd;
}
?>
```

Wrzucamy go do katalogu, który chcemy zabezpieczyæ, i wywo³ujemy z adresu przegl±darki, dodaj±c do naszego adresu strony ¶cie¿kê do owego katalogu, np: administrator, czyli ca³o¶æ mo¿e wygl±daæ tak (link oczywi¶cie przyk³adowy i nie zadzia³a na moim serwerze, ze wzglêdu 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± wpiszemy 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 jakiekolwiek inne istnieja? Je¶li tak to mógbym 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 juz o FTP strony, gdzie nagle nie mia³em dostêpu do FTPa nawet brak mo¿liwo¶ci wpsiania nazwy konta i uzytkowanika (wsyztsko 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 pocztaku 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:(

==========