Kontrola dostępu

Spis treści

Krótki wstęp

Powrót do góry

Czasami istnieje konieczność zabezpieczenia całości lub chociażby fragmentów naszej strony internetowej przed dostępem osób do tego nieuprawnionych. W tym celu udostępniliśmy Państwu wiele technik pozwalających na pełną kontrolę nad przeglądaniem witryny WWW.

Sposoby autoryzacji dostpne w naszym hostingu

Powrót do góry

Poniżej znajduję się opis sposobów autoryzacji dostępnych w dhosting.

Autoryzacja osób przy pomocy nazwy użytkownika i hasła

Powrót do góry

Pierwszy z opisywanych trybów uwierzytelniania jest w Internecie najbardziej powszechny. Przy próbie dostępu do chronionego folderu wyświetli się nam okienko z miejscem na nazwę użytkownika i hasło.

Aby skorzystać z tego rodzaju autentykacji wymagane będzie wykonanie dwóch kroków. Pierwszy z nich to utworzenie pliku z bazą danych uprawnionych osób przy pomocy narzędzia htpasswd.exe.

programy/htpasswd.exe

Po pobraniu tego programu otwieramy wiersz poleceń (w systemach Microsoft Windows robimy to poprzez Start -> Wszystkie programy -> Akcesoria -> Wiersz polecenia) i przechodzimy do katalogu z plikiem htpasswd.exe.

Następnie wpisujemy:

```
htpasswd.exe -c .htpasswd nazwa_uzytkownika [ENTER]
```

W odpowiedzi system zapyta nas o hasło dla użytkownika.

Kolejnych użytkowników dodajemy poprzez pominięcie parametru "-c"
htpasswd.exe .htpasswd nazwa_uzytkownika [ENTER]
Jeśli nazwa użytkownika zawiera spację, należy wtedy ją umieścić w cudzysłowie.

Utworzony został plik o nazwie .htpasswd zawierający informacje o uprawnieniach.

Następnie należy utworzyć plik o nazwie .htaccess z następującą treścią:

```
AuthType basic
AuthName "Ograniczony dostep"
AuthBasicProvider file
AuthUserFile /home/klient.dhosting.pl/nazwa_uzytkownika/chroniony_katalog/.htpasswd
Require valid-user
```

Opcja AuthUserFile wymaga podania bezwzględnej ścieżki dostępu do pliku .htpasswd

Następnie oba pliki (.htaccess i .htpasswd) umieszczamy w chronionym katalogu poprzez klienta FTP. Od tej pory po wejściu na stronę widzimy prośbę o zalogowanie się.

Autoryzacja określonych komputerów przy pomocy adresu IP

Powrót do góry

Każdy komputer będący podłączony do Internetu posiada unikalny adres, zwany adresem IP. Jeśli firma posiada komputery podłączone do Internetu i posiadające stałe, unikalne adresy IP, to możliwe jest utworzenie ograniczeń dostępu tylko do sieci wewnętrznej.

Aby to zrobić, tworzymy plik o nazwie ".htaccess" (bez cudzysłowów) i wpisujemy do niego:

```
Deny from all
Allow from 111.222.222.0-111.222.222.255
```

(111.222.222.0-111.222.222.255 to adresy IP komputerów w sieci firmowej).

Możemy także wykluczyć niektóre osoby (np. internetowych wandali) z grona odwiedzających poprzez blokadę dostępu do strony WWW dla określonych adresów IP.

W tym celu plik .htaccess powinien wyglądać następująco:

```
Deny from 111.222.222.123
Deny from 111.232.232.210
```

(111.222.222.123 i 111.232.232.210 to adresy komputerów, które chcemy zablokować).

Wówczas osoby, które nie mają przypisanych uprawnień dostępu, zobaczą komunikat błędu o kodzie 403 - Dostęp zabroniony.

Ograniczanie pojedynczych plików

Powrót do góry

Podane reguły domyślnie dotyczą wszystkich plików i podfolderów katalogu, w którym umieściliśmy plik .htaccess. Aby ustawić limit tylko dla określonych typów (np. tylko dla obrazów o rozszerzeniu JPG lub programów .exe) należy rozbudować regułę dostępu o nazwy plików do których wymagana jest autoryzacja. Dozwolone jest także stosowanie wyrażeń regularnych zgodnych ze składnią języka Perl.

Aby zilustrować praktyczne zastosowanie omówionych komend, przerobimy przykład z podpunktu 2.3. Zezwoliliśmy w nim na dostęp do witryny tylko dla pracowników znajdujących się w sieci korporacyjnej o adresach IP z klasy 111.222.222.0 - 111.222.222.255.

Modyfikacja polegać będzie na ograniczeniu dostępu do plików wykonywalnych (rozszerzenie .exe) i dokumentów programu Microsoft Word (rozszerzenie .doc) tylko wewnątrz sieci korporacyjnej. Reszta witryny będzie dostępna dla każdej osoby.

W tym celu istniejącą regułę:

```
Deny from all
Allow from 111.222.222.0-111.222.222.255
```

modyfikujemy do postaci:

```
<FilesMatch ".(exe|doc)$">
      Deny from all
      Allow from 111.222.222.0-111.222.222.255
</FilesMatch>
```

Jeśli natomiast chcemy ograniczyć dostęp jedynie do jednego pliku o określonej nazwie (np. raport.doc), nie musimy budować wyrażenia regularnego. Stosujemy wtedy

```
<Files raport.doc>
      Deny from all
      Allow from 111.222.222.10
</Files>
```

Zapoznaj się z:

Kontrola dostępu

Krótki kurs języka PHP

Moduł mod_rewrite

Plik .htaccess