

сигурност с Apache Web Server

Сигурност

- [махане на опцията FollowSymLinks](#)
- [ограничаване на достъпа по IP](#)
- [ограничаване на достъпа по име/парола](#)
- [комбиниране на ограничаването на достъпа по IP и име/парола](#)
- [добавяне на празен index.html файл](#)

[Apache Web Server](#) предлага множество начини да се защити съдържанието на дадена информация на сървъра от натрапници. За да се разрешат за използване повечето от опциите за увеличаване на сигурността в Apache те трябва да са предварително добавени в основния конфигурационен файл на сървъра

httpd.conf

. Имайте предвид, че ако правите промени във този файл трябва да рестартирате сървъра, за да се зареди новата конфигурация. Това става чрез програмата, намираща се в

bin

директорията на сървъра -

apachectl

с опция restart. т.е

```
./apachectl restart
```

Или с командата:

```
killall -HUP httpd
```

Проверка за това дали е правилна конфигурацията можете да направите със следната команда:

```
./apachectl configtest
```

Опциите в зависимост от това къде са написани имат и различен обseg на действие. Ето и някои от по-важните области:

Ако са написани в **.htaccess** файл те са валидни само за директорията, в която се намира файлът и нейните поддиректории

Ако са написани в **httpd.conf** файла, но са заградени с тагове, са валидни само за виртуален хост

Ако са написани в **httpd.conf** файла, но са заградени с тагове, са валидни само за дадена директория

Ако са написани в **httpd.conf** файла и не са заградени с никакви тагове, тогава важат за целият сървър

Да започваме с конфигурирането.

- махане на опцията **FollowSymLinks**

Ако не е абсолютно наложително да присъства тази опция в конфигурацията на вашият сървър я махнете. С нея можете да имате само проблеми. Или по-добре я разрешете само за директорията, за която това е абсолютно наложително.

- ограничаване на достъпа по IP

За да можете да ограничавате достъпа по IP трябва в **httpd.conf** файла да е зададена следната директива:

AllowOverride **Limit**

Ако я заградите в тагове, тя ще важи САМО за конкретния виртуален хост. Ако я

заградите в тя ще важи САМО за директорията, която е посочена в таговете и всички нейни поддиректории. Може би вече се досещате, че ако не я оградите в някакви тагове тя ще важи за целия сървър.

Ако искате да защитите дадена директория да е достъпна само за някое IP добавете файла .htaccess в директорията, която искате да защитите и напишете следното:

```
order deny, allow
deny from all
allow from IP_TO
```

като замените IP_TO с IP адреса, който искате да има достъп до тази директория. Ако искате, например, само IP номер 212.0.0.1 да достъпва директорията, напишете:

```
order deny, allow
deny from all
allow from 212.0.0.1
```

Освен пълен IP адрес, можете да зададете частичен IP адрес. Ако зададете следния IP адрес 212.0.0. -- това значи, че всички IP адреси, които започват с IP 212.0.0. могат да достъпят директорията. Примери за IP адреси, които изпълняват това условие са: 212.0.0.12, 212.0.0.23.

От голяма важност е директивата **order**. Тя инструктира Apache-то за реда, по който трябва да се обработят **deny** и **allow** директивите. Вижте резултатите от следните примери:

```
order deny, allow
deny from all
allow from 212.0.0.1
```

Резултат: само IP адрес 212.0.0.1 има достъп до тази директория,

```
order allow, deny
deny from all
allow from 212.0.0.1
```

Резултат: никое IP няма достъп до тази директория.

Защо се получи така при втория пример? Точно заради директивата **order**. Първо разрешихме на IP адрес 212.0.0.1 да има достъп до директорията, след което забранихме на всички IP-та да имат достъп. В резултат никое IP няма достъп. Не е важна последователността на редовете, започващи с

deny from

и

allow from;

важна е последователността, зададена с директивата **order**.

- ограничаване на достъпа по име/парола

Доста често се случва да искаме да ограничим достъпа до някоя директория с име и парола, а не по IP. За тази цел трябва в конфигурационния файл на Apache сървъра **http.conf**

да е зададена следната директива:

AllowOverride **AuthConfig**

Нека пробваме да защитим нашата директория **data**. Искаме тя да е достъпна само с име и парола. За тази цел в директорията

data

трябва да създадем два файла - **.htaccess** и **.htpasswd**. Във **.htpasswd** файлът ще съхраняваме потребителските имена и паролите. В **.htaccess** файла имаме следните редове:

```
AuthName "Zashtitena Direktoriq"  
AuthType Basic  
AuthUserFile .htpasswd  
require valid-user
```

Нека да разгледаме един примерен .htpasswd файл:

```
test:dsSDvxc32440ztb5vmb  
user:c3244dsSdb5vvx0ztYz
```

Всеки ред представлява име на потребител(test), две точки(:), и криптираната Ви парола(**dsSDvxc32440ztb5vmb**). Този файл е текстови, както и .htaccess файлът, но паролата, която задавате трябва да е криптирана. Коеето значи, че ако напишете следния ред:

```
user1:nopassword
```

потребител **user1** няма да може да влезе с парола **nopassword**. Има и начин да направите така, че Apache-то да не иска паролите да са криптирани, но ние говорим тук за това как да направим системата по-сигурна, а не по-несигурна.

Как да добавите потребител с парола към .htpasswd файл?

Начин 1: Може да го направите с програмката htpasswd която се намира в bin директорията на Apache. Ето и един пример:

```
/www/bin/htpasswd -b /www/htdocs/user1/data/.htpasswd user password
```

Програмата **/www/bin/htpasswd** създава във файла **/www/htdocs/user1/data/.htpasswd** потребител с име

user

и парола

password

.

Начин 2: Друг начин е да използвате стандартната **crypt** функция на вашия Linux. Можете да напишете следното нещо от командния ред:

```
perl -e "print crypt("password","sl")"
```

Резултатът е "sl0N1Oj5JS0pw" - което е криптираната парола **password**. От Вас се изисква да редактирате файла **.htpasswd** и да добавите следния ред:

```
user:sl0N1Oj5JS0pw
```

Сега вече имаме потребител с име **user** и парола **password**

- комбиниране на ограничаването на достъпа по IP и име/парола

Ако искате да ограничите достъпа до дадена директория комбинирано по IP и парола, можете да добавите следното във Вашия **.htaccess** файл:

```
order deny, allow  
deny from all  
allow from 212.0.0.
```

```
AuthName "Zashtitena Direktoriq"  
AuthType Basic  
AuthUserFile .htpasswd  
require valid-user
```

Като преди това във Вашия httpd.conf файл сте добавили следния ред:

AllowOverride **AuthConfig Limit**

По този начин позволявате само на потребители с IP адреси, започващи с 212.0.0. и имащи потребителско име и парола в .htpasswd файла да достъпват защитената директория.

- добавяне на празен **index.html** файл

За да се чувстваме още по-сигурни можем да добавим и файл с име **index.html**, със следното съдържание:

По този начин всеки, който успее да влезе в защитената директория трябва да знае точно името на файла, който иска да види.