Apache2: Basic autentikacija s pojedinim i grupama korisnika

O zaštiti dijela sadržaja vašeg weba preko Radiusa i LDAP-a smo već u nekoliko navrata pisali. No, Apache ima i vlastite načine autentikacije, koje još uvijek mogu dobro doći, primjerice kada želite omogućiti pristup suradnicima koji nisu u AAI@EduHr sustavu. Radi se o ***Basic*** autentikaciji preko .htpasswd datoteka. Da se tekst ne ponavlja i ne bude suhoparan, dodat ćemo i rješenje upita sa Helpdeska za sistemce povezan uz ovaj način autentikacije.

Za početak, potrebno je generirati **.htpasswd** datoteku sa svim korisnicima koji trebaju imati pristup tom određenom dijelu weba (ili cijelom virtualnom hostu). Svaki korisnik može imati svoju zaporku, ili se može napraviti više grupa korisnika, ukoliko za time postoji potreba.

Datoteku .htpasswd stavite negdje gdje nije dostupna s weba, ali jest korisniku www-data. Korisnici upisani u ovu datoteku nemaju nikakve veze s /etc/passwd, niti korisnicima na sustavu.

Datoteka sa zaporkama ne mora nužno imati ime .htpasswd, već je ono proizvoljno. To ime je standardno ako želite datoteku staviti negdje direktno stabla weba koji želite zaštititi (postoje interna pravila koja štite datoteku od čitanja web korisnicima). Za stavljanje izvan DOCUMENT_ROOT direktorija, ime može biti i drugačije, primjerice "webpasswords". Bez obzira na ime, datoteka se kreira preko naredbe **htpasswd**:

```
# htpasswd -c /etc/apache2/webpasswords webkorisnik
New password: zaporka
Re-type new password: zaporka
Adding password for user webkorisnik
```

Opcija "**-c**" se rabi samo kod inicijalizacije datoteke sa zaporkama, odnosno briše i kreira datoteku ispočetka. Kod dodavanja novih web korisnika nije nužna, dapače, obrisat će sve korisnike. Dodavanje novog korisnika je identično kao i dodavanje inicijalnog korisnika (osim što nemojte staviti opciju "-c"):

```
# htpasswd /etc/apache2/webpasswords webkorisnik2
New password: zaporka
Re-type new password: zaporka
Adding password for user webkorisnik2
```

Uz pretpostavku da želite zaštititi direktorij /var/www/tajna, u odgovarajućem virtualnom hostu (primjerice /etc/apache2/sites-enabled/001-www.domena.hr) unesite sljedeće:

```
AuthType Basic
AuthName "Privatne datoteke"
AuthUserFile /etc/apache2/webpasswords
Require user webkorisnik webkorisnik2
```

Ove retke morate upisati unutar tagova **<Directory></Directory>**, odnosno **<Location></Location>**. Značenje je prilično samorazumljivo, no objasnit ćemo ih sve.

AuthType određuje tip autentikacije. Svi *browseri* podržavaju **Basic** način autentikacije, ali je on

vrlo nesiguran, odnosno moguće je zlorabiti zaporku ukoliko je netko presretne. Postoji i tip **Digest** (koji dolazi s modulom **mod_auth_digest**), no on se još uvijek smatra eksperimentalnim i podržavaju ga samo najnovije inačice browsera (što vjerujemo, neće još dugo biti problem). Više o Digest tipu možete pročitati na http://httpd.apache.org/docs/2.2/mod/mod_auth_digest.html [1].

Direktiva **AuthName** određuje *realm*, odnosno jednostavno taj će se natpis pojaviti u iskočnom prozoru kod pokušaja autentikacije, pa tu upišite prikladan opis, kako bi izbjegli zabunu ukoliko imate više zaštićenih dijelova.

Direktiva **AuthUserFile** samo određuje lokaciju datoteke sa zaporkama.

Direktiva "**Require user**" određuje korisnike kojima je dopušteno pristupiti ovom dijelu weba. Može ih biti i nekoliko, a svi moraju biti unutar datoteke sa zaporkama. No, neće svima navedenima u webpasswords (ili .htpasswd) datoteci dopušten pristup. Za to se možete poslužiti drugačijim oblikom direktive:

```
Require valid-user
```

Uporabom opcije **valid-user** omogućujemo da svatko iz webpasswords datoteke može pristupiti zaštićenom dijelu weba, uz uvjet da su točno otkucali odgovarajuću zaporku.

Ovakav, grupni pristup, se može podesiti i na drugi način, s nešto finijom kontrolom. Kao i na samom sustavu putem datoteke /etc/group, potrebno je kreirati novu datoteku s imenima grupa i imenima korisnika u njima. Neka datoteka bude /etc/apache2/webgroups, a njen oblik je:

```
grupa1: webkorisnik1 webkorisnik2
grupa2: pero marko
```

I unos u virtualnom hostu treba malo modificirati:

```
AuthType Basic
AuthName "Privatne datoteke"
AuthUserFile    /etc/apache2/webpasswords
AuthGroupFile    /etc/apache2/webgroups
Require group    grupa1
```

Ovakva konfiguracija omogućava da pojedini ljudi (skupljeni u grupe) imaju pristup zaštićenim webovima, ali ne i svi iz webpasswords datoteke.

Ovime smo završili s opisom konfiguracije web poslužitelja, a kako smo i obećali na početku, dodat ćemo i kuharicu (iako ih baš ne volimo, jer ljude učine lijenima i nevoljnima za daljnje istraživanje!) kako da ta ista grupa ljudi može ftp-om postavljati datoteke i na ovaj način razmjenjivati podatke. Ukratko, upit je bio kako da skupina ljudi/suradnika može preko weba institucije razmjenjivati određene podatke.

Zbog lakšeg snalaženja, bilo bi poželjno da korisnici imaju iste korisničke oznake i na sustavu i u webpasswords datoteci. Ovo se naravno ne odnosi na zaporke, koje ne bi smjele biti iste (sjetimo se, Basic autentikacija je slaba i lako je doći do zaporke!).

Prvo trebamo kreirati grupu s korisnicima koji žele razmjenjivati podatke, nazovimo je "razmjena":

```
# groupadd razmjena
```

Potom je potrebno dodati željene korisnike u tu grupu, a to æete najbrže napraviti tako da ruèno otvorite /etc/group datoteku i upišete:

```
# vim /etc/group
razmjena:x:4:marko,pero,ivo,www-data
```

Zatim kreirajte (ako već ne postoji) direktorij /var/www/tajna, te mu dodijelite ove atribute:

```
# chown root:razmjena /var/www/tajna
# chmod 770 /var/www/tajna
# ls -ld /var/www/tajna
drwxrwx---  4 root razmjena    4096 Dec 18  2002 /var/www/tajna
```

Drugim riječima, u ovaj direktorij (osim naravno korisnika root) mogu pisati samo članovi grupe "razmjena", a to naravno uključuje i pravo čitanja podataka u njemu. Da bi dodatno olakšali uporabu, možete postaviti simboličke linkove u $HOME direktorije svih članova grupe:

```
# for dir in marko pero ivo
do
    cd /home/$dir
    ln -s /var/www/tajna tajna
done
```

Na ovaj će način korisnici jednostavno nakon prijave ftp-om moći doći do direktorija za razmjenu, tako da jednostavno naprave:

```
ftp> cd tajna
```

U daljnjem radu se rabe standardne ftp naredbe "get" i "put", te naravno i sve ostale koje vam zatrebaju. Samim načinom uporabe alata ftp se ovdje nećemo baviti.

Nadamo se da smo u potpunosti odgovorili na vaša pitanja, i zaokružili najčešće načine autenticiranja preko weba, izuzimajući naravno CMS-ove i druge tehnologije koje u se u međuvremenu pojavile.

čet, 2009-10-15 07:58 - Željko Borš**Kuharice:** Linux [2]
Kategorije: Software [3]
Servisi [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr./node/645

Links
[1] http://httpd.apache.org/docs/2.2/mod/mod_auth_digest.html
[2] https://sysportal.carnet.hr./taxonomy/term/17
[3] https://sysportal.carnet.hr./taxonomy/term/25

[4] https://sysportal.carnet.hr./taxonomy/term/28