



Accesso sicuro a directory del filesystem

- Apache fornisce un accesso sicuro a porzioni del file-system, tramite l'utilizzo del file *.htaccess*.
- Per proteggere una directory abbiamo bisogno, insieme al file *.htaccess*, anche di un altro file, creato tramite l'utility *htpasswd*.
- Il comando shell *htpasswd* (su windows è un file eseguibile) permette di creare una password e limitare gli accessi; quindi per usare *.htaccess* bisogna, per prima cosa, creare un file di password.
- Creato il file di password, *.htaccess* ha bisogno di essere configurato.

Autenticazione http mediante il file .htaccess

Creazione file di password

-c : crea un nuovo file e memorizza un record per l'utente "anto" con password annessa.

Questa verrà crittografata dall'utility *htpasswd* usando l'algoritmo MD5.

Se il file esiste e non può essere letto o scritto, viene visualizzato un messaggio di errore.

-b : ci permette di inserire la password direttamente dalla linea di comando, senza che ci venga richiesta successivamente.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versione 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tutti i diritti riservati.

C:\Users\Ant0>cd C:\xampp\apache\bin
C:\xampp\apache\bin>htpasswd
Usage:
    htpasswd [-cmdpsD] passwordfile username
    htpasswd -b[cmdpsD] passwordfile username password
    htpasswd -n[mdps] username
    htpasswd -nb[mdps] username password
-c Create a new file.
-d Don't update file; display results on stdout.
-e Force MD5 encryption of the password (default).
-d Force CRYPT encryption of the password.
-p Do not encrypt the password (plaintext).
-w Force SHA encryption of the password.
-b Use the password from the command line rather than prompting for it.
-D Delete the specified user.
On other systems than Windows, NetWare and TPF the '-p' flag will probably not work.
The SHA algorithm does not use a salt and is less secure than the MD5 algorithm.

C:\xampp\apache\bin>htpasswd -b -c pass anto 123
Adding password for user anto

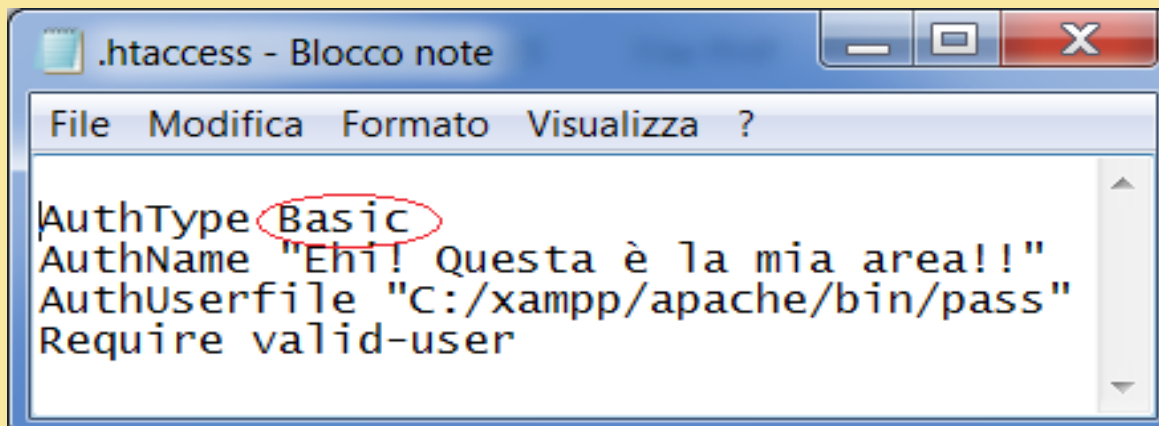
C:\xampp\apache\bin>dir
Il volume nell'unità C non ha etichetta.
Numero di serie del volume: 6CFF-E0B8

Directory di C:\xampp\apache\bin
21/10/2011 16:10 <DIR> .
21/10/2011 16:10 <DIR> ..
10/09/2011 12:00 ab.exe
10/09/2011 11:47 abs.exe
10/09/2011 11:47 ApacheMonitor.exe
10/09/2011 11:47 apr_dbd_odbc-1.dll
10/09/2011 11:47 apr_ldap-1.dll
10/09/2011 12:11 dbmmanage.pl
10/09/2011 11:47 htcacheclean.exe
10/09/2011 11:47 htdbm.exe
10/09/2011 11:47 htdigest.exe
10/09/2011 11:47 htpasswd.exe
10/09/2011 11:47 httpd.exe
10/09/2011 11:47 httpd2dbm.exe
20/09/2011 14:00 <DIR> iconv
10/09/2011 11:47 libapr-1.dll
10/09/2011 11:47 libapriconv-1.dll
10/09/2011 11:47 libaprutil-1.dll
10/09/2011 11:47 libeay32.dll
10/09/2011 11:47 libhttpd.dll
10/09/2011 11:47 logresolve.exe
20/11/2009 00:00 openssl.cnf
10/09/2011 11:16 openssl.exe
22/10/2011 12:21 pass
21/12/2007 04:00 pv.exe
10/09/2011 11:47 rotatelog.exe
10/09/2011 11:17 ssl_eay32.dll
10/09/2011 11:47 winhttp.exe
25/07/2010 15:20 zlib1.dll
26 File 3.111.601 byte
3 Directory 104.821.374.976 byte disponibili

C:\xampp\apache\bin>
```

Autenticazione http mediante il file .htaccess

Ora non ci resta che andare nella directory che vogliamo proteggere (ad esempio "public_html") e creare il file `.htaccess` con le seguenti direttive:



```
.htaccess - Blocco note
File Modifica Formato Visualizza ?
AuthType Basic
AuthName "Ehi! Questa è la mia area!!"
AuthUserfile "C:/xampp/apache/bin/pass"
Require valid-user
```

Ulteriori direttive e dettagli sono reperibili qui:
<http://httpd.apache.org/docs/2.2/howto/auth.html>.

NB: il livello di sicurezza è BASIC.



Autenticazione http modificando il file httpd.conf

Andiamo nelle directory di configurazione di Apache per iniziare la modifica:
C:\xampp\apache\conf
e apriamo il file httpd.conf con Blocco Note.

```
File Modifica Formato Visualizza ?
# This should be changed to whatever you set DocumentRoot to.
#
<Directory "C:/Users/Ant0/Documents/public_html/a-request">
AuthType Digest
AuthName "Ant0"
AuthUserfile "C:/xampp/apache/bin/passdigest"
Require valid-user
</Directory>

<Directory "C:/xampp/htdocs">

#
# Possible values for the Options directive are "None",
"All",
# or any combination of:
#   Indexes Includes FollowSymLinks SymLinksifOwnerMatch
```

Inseriamo lo stesso contenuto del file *.htaccess* che abbiamo visto prima. Diversamente da quanto fatto precedentemente, abbiamo impostato il tag *<Directory .. >* per indicare ad Apache quale directory proteggere. E' cambiato anche il campo **Authtype**, invece che Basic, ora c'è DIGEST.



Autenticazione http modificando il file httpd.conf

Creazione file di password

Siccome abbiamo utilizzato Digest, come livello di sicurezza, questa volta non invocheremo l'utility *htpasswd*, bensì **htdigest**.

Diversamente da quanto fatto con *htpasswd*, *htdigest* ci chiede di inserire un valore per un nuovo campo:

Realm : che è ciò che abbiamo definito con *AuthName*.

DIGEST rispetto a *BASIC* non trasmette la password in chiaro; di conseguenza, è il tipo di autenticazione più sicuro.

```

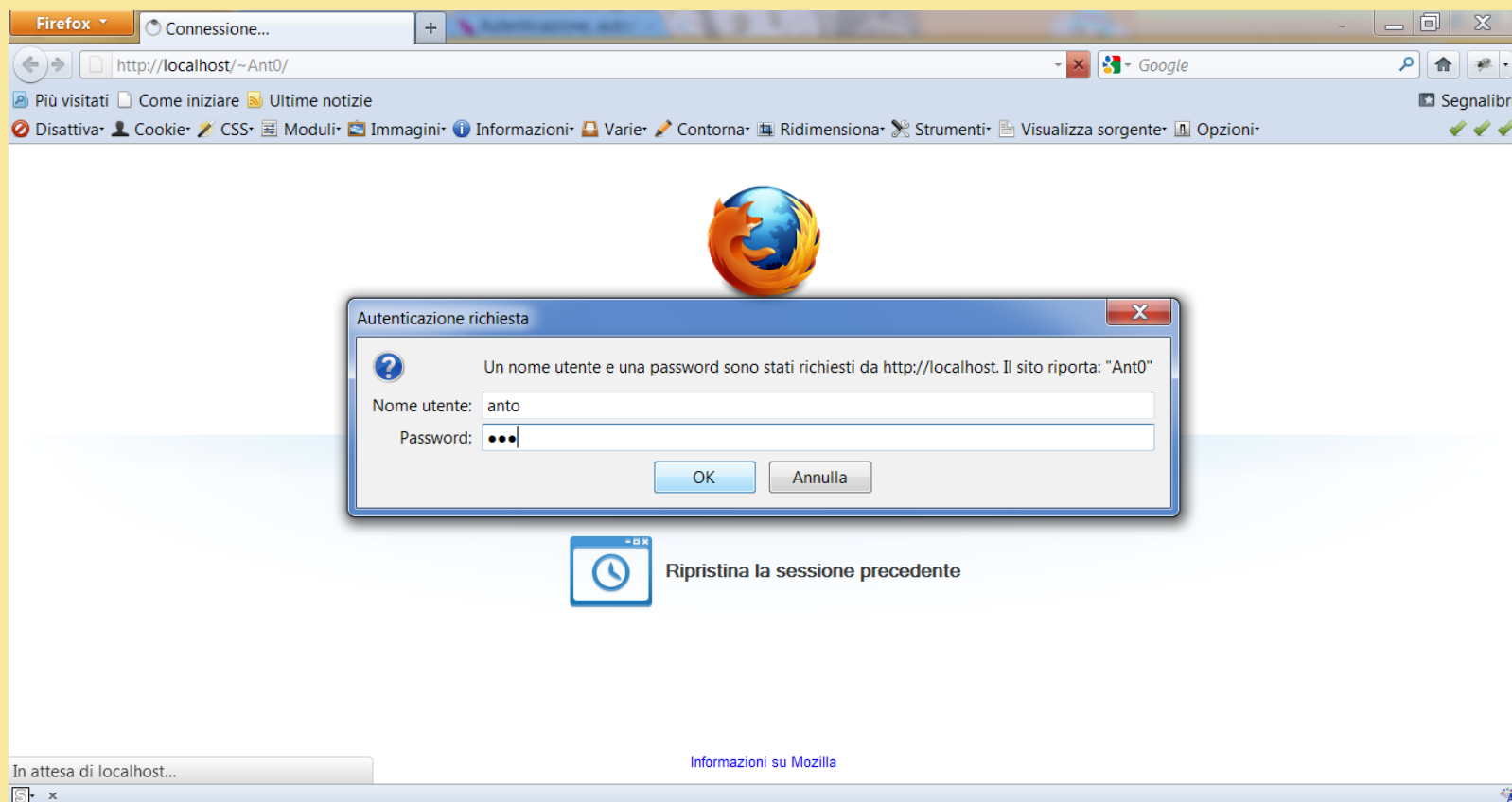
C:\Windows\system32\cmd.exe
C:\Users\Ant0>cd C:\xampp\apache\bin
C:\xampp\apache\bin>htdigest
Usage: htdigest [-c] passwordfile realm username
The -c flag creates a new file.
C:\xampp\apache\bin>htdigest -c passwdigest Ant0 anto
Adding password for anto in realm Ant0.
New password: ***
Re-type new password: ***
C:\xampp\apache\bin>dir
Il volume nell'unità C non ha etichetta.
Numerc di serie del volume: 6CFF-E0B8

Directory di C:\xampp\apache\bin
22/10/2011 13:07 <DIR> .
22/10/2011 13:07 <DIR> ..
10/09/2011 12:00 ab.exe
10/09/2011 11:43 abs.exe
10/09/2011 11:43 ApacheMonitor.exe
10/09/2011 11:50 apr_dbd_odbcc-1.dll
10/09/2011 11:43 apr_ldap-1.dll
10/09/2011 12:11 dbmmanage.pl
10/09/2011 11:50 htcacheclean.exe
10/09/2011 11:43 htdbm.exe
10/09/2011 11:43 htdigest.exe
10/09/2011 11:43 htpasswd.exe
10/09/2011 11:43 httpd.exe
10/09/2011 11:43 httpd2ssl.exe
28/09/2011 14:49 <DIR> iconv
10/09/2011 11:01 libapr-1.dll
10/09/2011 11:01 libapriconv-1.dll
10/09/2011 11:01 libaprutil-1.dll
10/09/2011 11:01 libeay32.dll
10/09/2011 11:34 1.098.246 libhttpd.dll
10/09/2011 11:45 logresolve.exe
20/12/2009 00:00 9.374 openssl.cnf
10/09/2011 11:16 372.224 openssl.exe
22/10/2011 13:37 43 passwdigest
21/12/2007 04:00 61.440 pv.exe
10/09/2011 11:43 48.128 rotatelogs.exe
10/09/2011 11:13 237.568 sslseay32.dll
10/09/2011 11:43 13.312 wintty.exe
25/07/2010 15:20 67.584 zlib1.dll
26 File 3.111.601 byte
3 Directory 104.810.430.464 byte disponibili
C:\xampp\apache\bin>_

```



Il risultato dei due casi esaminati è lo stesso



Inserendo nome utente e password come stabiliti nel file di password si avrà accesso alla cartella che abbiamo voluto proteggere.