

CONFIGURAZIONE SERVER APACHE (XAMPP): ACCESSO SICURO A DIRECTORY DEL FILE SYSTEM.

A CURA DI ANTONELLA LAURINO

Questa guida permette di configurare il server apache, contenuto nel software xampp, in modo da proteggere alcune directory del nostro file system. La guida è stata scritta operando su Windows 7 e presenta due possibili modalità di configurazione.

[1] - CONFIGURAZIONE DELL' AUTENTICAZIONE HTTP MEDIANTE IL FILE .htaccess

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 – sempre fornita da apache – *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.

- Apriamo una finestra DOS, andando sul pulsante "Start" di Windows: 
Ora, nella casella di ricerca che ci compare davanti, digitiamo: **cmd**.
- Aperta la finestra dos, digitiamo `cd C:\xampp\apache\bin` così entreremo Nella directory bin di apache dove risiede il file *htpasswd*.
- Diamo il comando *htpasswd* in modo che il prompt ci risponda con i vari modi di utilizzo del file che stiamo esaminando. A noi interessano i flag: **-c** e **-b**.

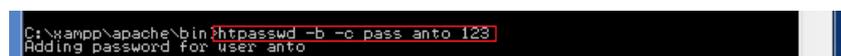


```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versione 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tutti i diritti riservati.
C:\Users\Ant0>cd C:\xampp\apache\bin
C:\xampp\apache\bin>htpasswd
Usage:
  htpasswd [-cmdpsD] passwordfile username
  htpasswd -b[cmdpsD] passwordfile username password
  htpasswd -n[mdps] username
  htpasswd -p[mdps] username password
-c Create a new file.
-n Don't update file; display results on stdout.
-m Force MD5 encryption of the password (default).
-d Force CRYP encryption of the password.
-p Do not encrypt the password (plaintext).
-e 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.
```

Il tag **-c** crea un nuovo file di nome "pass" nella directory in cui ci troviamo e memorizza un record per l'utente "anto" con password annessa ("123" in questo caso). 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.

Il tag **-b** ci permette, invece, di inserire la password direttamente dalla linea di comando, senza che ci venga richiesta successivamente.

- Non ci resta che digitare il comando che crei il nostro file di password:
`htpasswd -b -c pass anto 123`



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

- e) Digitando ora *dir* vedremo l'elenco dei file presenti nella directory, tra cui il nostro file di password, "pass".

```

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

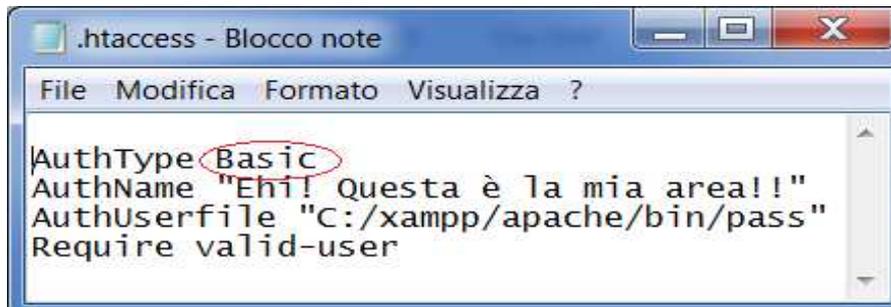
Directory di C:\xampp\apache\bin

21/10/2011 16:10 <DIR> .
21/10/2011 16:10 <DIR> ..
10/09/2011 12:00 700 ab.exe
10/09/2011 11:43 120 ApacheMonitor.exe
10/09/2011 11:50 100 apr_dbd_odbc-1.dll
10/09/2011 11:43 120 apr_ldap-1.dll
10/09/2011 12:11 100 dbmmanage.pl
10/09/2011 11:50 100 htcheckclean.exe
10/09/2011 11:45 100 htdbm.exe
10/09/2011 11:45 100 htdigest.exe
10/09/2011 11:45 100 httpasswd.exe
10/09/2011 11:45 100 httpd.exe
10/09/2011 11:45 100 httpd2dbm.exe
28/09/2011 14:45 <DIR> iconv
10/09/2011 11:31 133 libapr-1.dll
10/09/2011 11:31 170 libapriconv-1.dll
10/09/2011 11:31 170 libaprutil-1.dll
10/09/2011 11:31 100 libexpat-1.dll
10/09/2011 11:34 100 libhttpd.dll
10/09/2011 11:45 100 logresolve.exe
20/12/2009 00:00 37 openssl.cnf
22/10/2011 11:16 372 openssl.exe
21/12/2007 04:00 61 pass
10/09/2011 11:43 48 rotatelogs.exe
10/09/2011 11:43 237 sslau32.dll
10/09/2011 11:43 63 winhttp.dll
25/07/2010 15:20 3,111,601 albi.dll
File 3,111,601 byte
Directory 104,821,374,976 byte disponibili

C:\xampp\apache\bin>

```

- f) Possiamo chiudere il DOS e andare nella directory che vogliamo proteggere; nel mio caso è: *C:/Users/Ant0/Documents/public_html* e creare, con un editor di testo (es Blocco Note), il file *htaccess* con le seguenti direttive:



AuthType: indica il tipo di autenticazione che vogliamo utilizzare. In questo caso abbiamo utilizzato **Basic**, ma non è poi così sicuro come livello di autenticazione poiché trasmette la password in chiaro; successivamente vedremo come utilizzare **Digest** che non trasmette la password in chiaro.

AuthName: E' ciò che comparirà nel popup quando ci sarà richiesto di inserire nome utente e password. Nel tipo di autenticazione Digest, coincide con il *Realm*.

AuthUserfile: Comunica quale file verrà utilizzato per l'autenticazione dell'utente. E' il file di password che abbiamo creato precedentemente; qui bisogna indicare il path.

Require: Inseriamo di default la voce valid-user per permettere l'accesso a tutti gli user del file di password.

Fatto!!

Accedendo tramite browser alla directory che abbiamo voluto proteggere, verrà richiesta l'autenticazione.

Ulteriori direttive e dettagli sono reperibili qui:

<http://httpd.apache.org/docs/2.2/howto/auth.html>

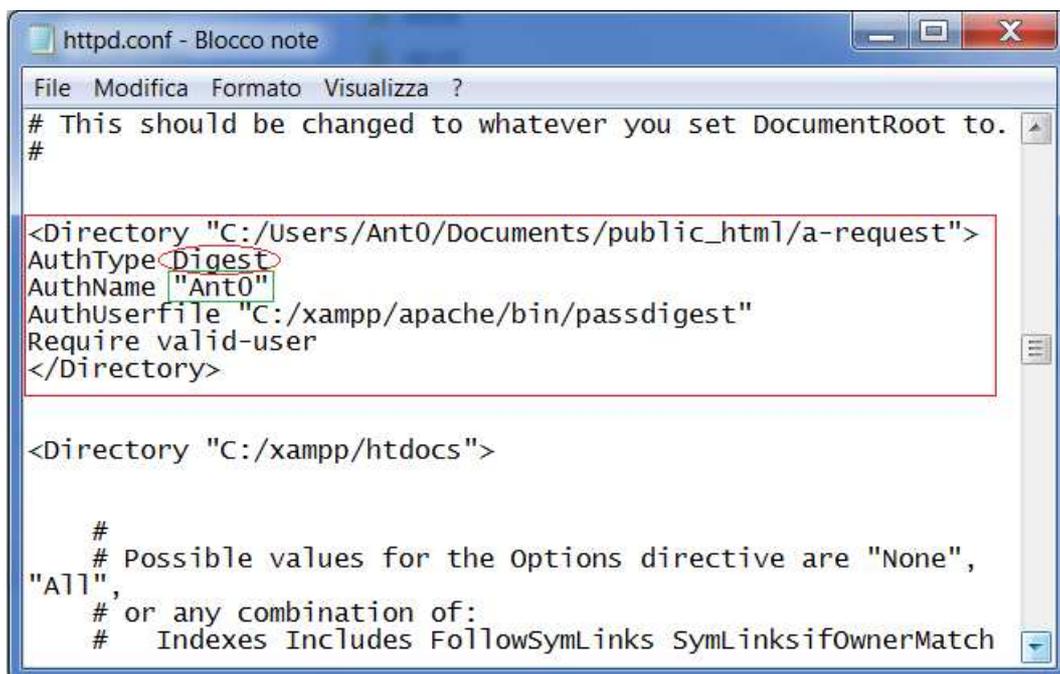
...

[2] - CONFIGURAZIONE DELL' AUTENTICAZIONE HTTP MODIFICANDO IL FILE httpd.conf

Per prima cosa consiglio di effettuare una copia di backup dei file che andremo a modificare in modo da poterli recuperare facilmente in caso di errore. Primo tra tutti, il file: *httpd.conf* presente nella seguente directory: *C:\xampp\apache\conf*.

Diversamente da come fatto in precedenza, questa volta, modificheremo prima il file di configurazione di Apache, quindi creeremo un file di password.

- a) Andiamo nella directory di configurazione del web server (*C:\xampp\apache\conf*) per iniziare la modifica e apriamo il file *httpd.conf* con Blocco Note.



```
httpd.conf - 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
```

Tutto quello che dobbiamo fare è inserire il contenuto del file visto in precedenza (*.htaccess*), con qualche accorgimento, nel file di configurazione di Apache appena aperto.

- b) Impostiamo il tag *<Directory .. >* per indicare ad Apache quale directory proteggere.

AuthType: indica il tipo di autenticazione che vogliamo utilizzare. In questo caso abbiamo utilizzato **Digest**, diversamente da quanto fatto in precedenza; ricordo che **Digest**, che non trasmette la password in chiaro, è più appropriato in quanto fornisce un livello di sicurezza maggiore.

AuthName: E' ciò che comparirà nel popup quando ci sarà richiesto di inserire nome utente e password. Coincide con il *Realm*. Questo campo ci verrà richiesto nella compilazione del file di password.

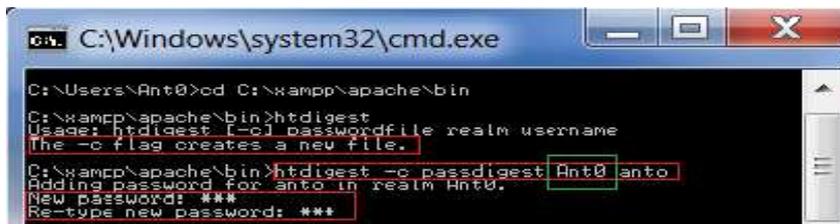
AuthUserfile: Comunica quale file verrà utilizzato per l'autenticazione dell'utente. E' il file di password che creeremo a breve; qui bisogna indicare il path.

Require: Inseriamo di default la voce *valid-user* per permettere l'accesso a tutti gli user del file di password.

Chiudiamo quindi, il tag *</Directory>*.

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

- c) Apriamo una finestra DOS, andando sul pulsante "Start" di Windows: 
Ora, nella casella di ricerca che ci compare davanti, digitiamo: **cmd**.
- d) Aperta la finestra dos, digitiamo `cd C:\xampp\apache\bin` così entreremo nella directory bin di apache dove risiede il file `htdigest`.
- e) Diamo il comando `htdigest` in modo che il prompt ci risponda con i vari modi di utilizzo del file che stiamo esaminando. A noi interessa il flag: **-c**.
- g) Ora dobbiamo digitare il comando che crei il nostro file di password:
`htdigest -c passwdigest Ant0 anto`



```

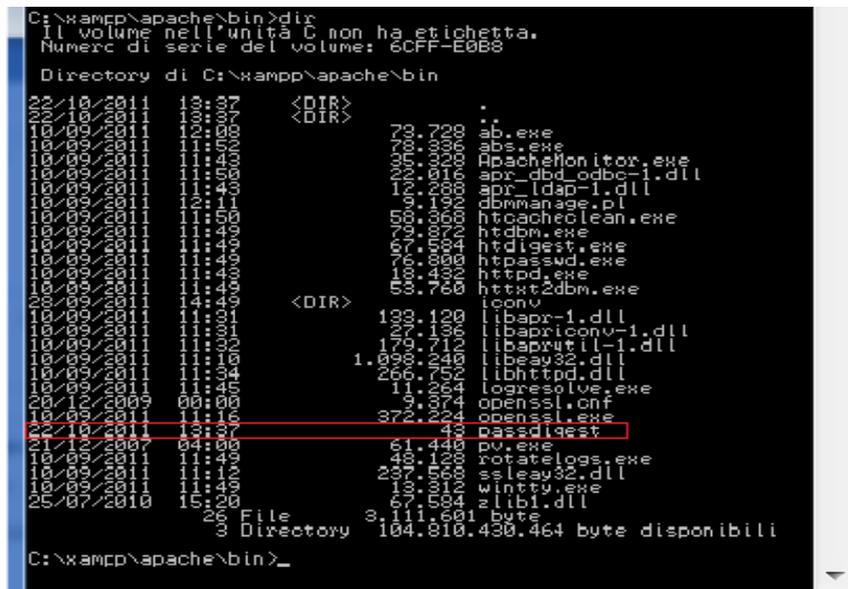
C:\Windows\system32\cmd.exe
C:\Users\Ant0>cd C:\xampp\apache\bin
C:\xampp\apache\bin>htdigest
Usage: htdigest [-c] passwordfile realm username
The -c flag creates a new file.
C:\xampp\apache\bin>htdigest -c passwdigest Ant0 anto
Adding password for anto in realm Ant0.
New password: ***
Re-type new password: ***

```

- h) Ci verrà chiesto di inserire una password per l'utente "anto". Scriviamola, diamo 'invio', quindi inseriamola di nuovo e poi ancora 'invio'.

Il campo che abbiamo aggiunto ("Ant0"), nel riquadro verde, è il *Realm*: l'abbiamo definito in precedenza con *AuthType*; deve essere lo stesso.

- i) Digitando ora `dir` vedremo l'elenco dei file presenti nella directory, tra cui il nostro file di password, "passwdigest".



```

C:\xampp\apache\bin>dir
Il volume nell'unità C: non ha etichetta.
Numero di serie del volume: 0CFF-E0B8

Directory di C:\xampp\apache\bin

22/10/2010 11:00:00 <DIR> .
22/10/2010 11:00:00 <DIR> ..
10/09/2009 11:00:00 abs.exe
10/09/2009 11:00:00 abs.conf
10/09/2009 11:00:00 ApacheMonitor.exe
10/09/2009 11:00:00 apr_dbd_odbc-1.dll
10/09/2009 11:00:00 apr_ldap-1.dll
10/09/2009 11:00:00 dbmmanage.pl
10/09/2009 11:00:00 htcacheclean.exe
10/09/2009 11:00:00 htdbm.exe
10/09/2009 11:00:00 htdigest.exe
10/09/2009 11:00:00 httpasswd.exe
10/09/2009 11:00:00 httpd.exe
10/09/2009 11:00:00 httpd2dbm.exe
10/09/2009 11:00:00 iconv
10/09/2009 11:00:00 libapr-1.dll
10/09/2009 11:00:00 libapriconv-1.dll
10/09/2009 11:00:00 libaprutil-1.dll
10/09/2009 11:00:00 libeay32.dll
10/09/2009 11:00:00 libhttpd.dll
10/09/2009 11:00:00 logresolve.exe
10/09/2009 11:00:00 openssl.cnf
10/09/2009 11:00:00 openssl.exe
22/10/2010 11:00:00 passwdigest
21/10/2010 11:00:00 pv.exe
10/09/2009 11:00:00 rotatelog.exe
10/09/2009 11:00:00 sslay32.dll
10/09/2009 11:00:00 wintty.exe
25/07/2010 15:00:00 zlib1.dll

File 3,111,661 byte
Directory 104,810,430,464 byte disponibili

C:\xampp\apache\bin>

```

Bene, abbiamo finito.

Accedendo tramite browser alla directory che abbiamo voluto proteggere, verrà richiesta l'autenticazione.

Il risultato dei due metodi utilizzati è esattamente lo stesso.

