NAME

htdbm – Manipulate DBM password databases

SYNOPSIS

htdbm [-**T***DBTYPE*] [**-i**] [**-c**] [**-m** | **-B** | **-d** | **-s** | **-p**] [**-C** *cost*] [**-t**] [**-v**] *filename username*

htdbm **-b** [-**T***DBTYPE*] [**-c**] [**-m** | **-B** | **-d** | **-s** | **-p**] [**-C** *cost*] [**-t**] [**-v**] *filename username password*

htdbm **-n** [**-i**] [**-c**] [**-m** | **-B** | **-d** | **-s** | **-p**] [**-C** *cost*] [**-t**] [**-v**] *username*

htdbm **-nb** [**-c**] [**-m** | **-B** | **-d** | **-s** | **-p**] [**-C** *cost*] [**-t**] [**-v**] *username password*

htdbm **-v** [-**T***DBTYPE*] [**-i**] [**-c**] [**-m** | **-B** | **-d** | **-s** | **-p**] [**-C** *cost*] [**-t**] [**-v**] *filename username*

htdbm **-vb** [-**T***DBTYPE*] [**-c**] [**-m** | **-B** | **-d** | **-s** | **-p**] [**-C** *cost*] [**-t**] [**-v**] *filename username password*

htdbm **-x** [-**T***DBTYPE*] *filename username*

htdbm **-l** [-**T***DBTYPE*]

SUMMARY

htdbm is used to manipulate the DBM format files used to store usernames and password for basic authentication of HTTP users via mod_authn_dbm. See the dbmmanage documentation for more information about these DBM files.

OPTIONS

-b Use batch mode; *i.e.*, get the password from the command line rather than prompting for it. This option should be used with extreme care, since **the password is clearly visible** on the command line. For script use see the **-i** option.

-i Read the password from stdin without verification (for script usage).

-c Create the *passwdfile*. If *passwdfile* already exists, it is rewritten and truncated. This option cannot be combined with the **-n** option.

-n Display the results on standard output rather than updating a database. This option changes the syntax of the command line, since the *passwdfile* argument (usually the first one) is omitted. It cannot be combined with the **-c** option.

-m Use MD5 encryption for passwords. On Windows and Netware, this is the default.

-B Use bcrypt encryption for passwords. This is currently considered to be very secure.

-C This flag is only allowed in combination with **-B** (bcrypt encryption). It sets the computing time used for the bcrypt algorithm (higher is more secure but slower, default: 5, valid: 4 to 31).

-d Use **crypt()** encryption for passwords. The default on all platforms but Windows and Netware. Though possibly supported by **htdbm** on all platforms, it is not supported by the httpd server on Windows and Netware. This algorithm is **insecure** by today's standards.

-s Use SHA encryption for passwords. Facilitates migration from/to Netscape servers using the LDAP Directory Interchange Format (ldif). This algorithm is **insecure** by today's standards.

-p Use plaintext passwords. Though **htdbm** will support creation on all platforms, the httpd daemon will only accept plain text passwords on Windows and Netware.

-l Print each of the usernames and comments from the database on stdout.

-v Verify the username and password. The program will print a message indicating whether the supplied password is valid. If the password is invalid, the program exits with error code 3.

-x Delete user. If the username exists in the specified DBM file, it will be deleted.

-t Interpret the final parameter as a comment. When this option is specified, an additional string can be appended to the command line; this string will be stored in the "Comment" field of the database, associated with the specified username.

filename

The filename of the DBM format file. Usually without the extension **.db**, **.pag**, or **.dir**. If **-c** is given, the DBM file is created if it does not already exist, or updated if it does exist.

username

The username to create or update in *passwdfile*. If *username* does not exist in this file, an entry is added. If it does exist, the password is changed.

password

The plaintext password to be encrypted and stored in the DBM file. Used only with the **-b** flag.

-T*DBTYPE*

Type of DBM file (SDBM, GDBM, DB, or "default").

BUGS

One should be aware that there are a number of different DBM file formats in existence, and with all likelihood, libraries for more than one format may exist on your system. The three primary examples are SDBM, NDBM, GNU GDBM, and Berkeley/Sleepycat DB 2/3/4. Unfortunately, all these libraries use different file formats, and you must make sure that the file format used by *filename* is the same format that **htdbm** expects to see. **htdbm** currently has no way of determining what type of DBM file it is looking at. If used against the wrong format, will simply return nothing, or may create a different DBM file with a different name, or at worst, it may corrupt the DBM file if you were attempting to write to it.

One can usually use the **file** program supplied with most Unix systems to see what format a DBM file is in.

EXIT STATUS

htdbm returns a zero status ("true") if the username and password have been successfully added or updated in the DBM File. **htdbm** returns **1** if it encounters some problem accessing files, **2** if there was a syntax problem with the command line, **3** if the password was entered interactively and the verification entry didn't match, **4** if its operation was interrupted, **5** if a value is too long (username, filename, password, or final computed record), **6** if the username contains illegal characters (see the Restrictions section), and **7** if the file is not a valid DBM password file.

EXAMPLES

```
htdbm /usr/local/etc/apache/.htdbm-users jsmith
```

Adds or modifies the password for user **jsmith**. The user is prompted for the password. If executed on a Windows system, the password will be encrypted using the modified Apache MD5 algorithm; otherwise, the system's **crypt()** routine will be used. If the file does not exist, **htdbm** will do nothing except return an error.

```
htdbm -c /home/doe/public_html/.htdbm jane
```

Creates a new file and stores a record in it for user **jane**. The user is prompted for the password. If the file exists and cannot be read, or cannot be written, it is not altered and **htdbm** will display a message and return an error status.

```
htdbm -mb /usr/web/.htdbm-all jones Pwd4Steve
```

Encrypts the password from the command line (**Pwd4Steve**) using the MD5 algorithm, and stores it in the specified file.

SECURITY CONSIDERATIONS

Web password files such as those managed by **htdbm** should *not* be within the Web server's URI space -- that is, they should not be fetchable with a browser.

The use of the **-b** option is discouraged, since when it is used the unencrypted password appears on the command line.

When using the **crypt()** algorithm, note that only the first 8 characters of the password are used to form the password. If the supplied password is longer, the extra characters will be silently discarded.

The SHA encryption format does not use salting: for a given password, there is only one encrypted representation. The **crypt()** and MD5 formats permute the representation by prepending a random salt string, to make dictionary attacks against the passwords more difficult.

The SHA and **crypt()** formats are insecure by today's standards.

RESTRICTIONS

On the Windows platform, passwords encrypted with **htdbm** are limited to no more than **255** characters in length. Longer passwords will be truncated to 255 characters.

The MD5 algorithm used by **htdbm** is specific to the Apache software; passwords encrypted using it will not be usable with other Web servers.

Usernames are limited to **255** bytes and may not include the character **:**.