Authenticating Web Users via HTACCESS

Mu Beta Psi, National Honorary Musical Fraternity

Webmaster Resources Series

FIRST RELEASE
OCTOBER 11, 2005

TABLE OF CONTENTS

Introduction to User Authentication

User Authentication is the process of verifying a person's identity in order to grant special privileges, such as viewing protected documents, sending email, etc. User authentication can be done on an individual basis (*"I am Joe Jones"*), or on a group level (*"I am a member of Team 5"*).

Within Mu Beta Psi, the Information Technology Policy provides for the need to perform user authentication before granting access to certain information, termed "Restricted Content". Restricted Content may include Brothers personal information, pledge policies, and discussion of Fraternity business, among others.

Beyond the requirements of policy, it is often desirable to create "Brothers Only" areas of a Chapter website for the purposes of coordinating internal social or pledging events, collaborating on works-in-progress, or storing Chapter records. User authentication is the key to creating such areas.

Introduction to HTACCESS

The most basic form of user authentication for the web is called HTACCESS.

With HTACCESS, a file (named, appropriately enough, ***.htaccess***) is placed in the folder to be protected. This file typically contains information about who is permitted to view the files contained in the directory and its subdirectories, the method of authentication, and the location of the user information. A separate file, called **htpasswd** contains the actual usernames and passwords.

HTACCESS is great for simple authentication. It's not ideal for situations where you have a large number of users, or where passwords change frequently, due to the need to manually update encrypted passwords in the HTPASSWD file.

Beyond user authentication, there are some other advanced features of HTACCESS, such as handling redirects and setting up environment variables. Although this goes beyond the scope of this document, you can find references to more information about HTACCESS in the last section of this guide.

The HTACCESS File

A simple htaccess file is below:

```
AuthName "Brothers Only"
AuthType Basic
AuthUserFile /full/path/to/.htpasswd
Require valid_user
```

The first line defines the name of the protected area. This text will appear on the prompt box where users will enter their username/password. The second line defines the method of authentication ("Basic" authentication is fine in most cases).

The third line identifies the location of the HTPASSWD file, which contains valid username/password combinations. We will discuss the contents of this file in more detail later, but for now you should be aware of the following:

- For security reasons, this file should not be stored in any directory that is accessible from the internet. In other words, if the files that make up your homepage are located in the */home/usr/mbpsi/www/* directory, your HTPASSWD file should not be. Store it in */home/usr/mbpsi/secure* instead.
- The file path for this file should be listed as an *absolute* path, not relative to your home directory. If you have any questions about this, please contact the Mu Beta Psi webmaster, who can assist you.

TIP
The filename .htaccess may look strange, but it's really pretty simple. It consists of an empty filename, and the extension "htaccess".

The last line in the example above is the list of valid usernames (as stored in the htpasswd file) that are permitted to access this directory. In this way, you can have multiple htaccess files that share one htpasswd file. In the example shown, the user "valid_user" is permitted to view the files.

Save the file in the directory you want to protect with the name *.htaccess*. If you wish to protect subdirectories using a different authentication scheme, put a separate htaccess file in each subdirectory.

The HTPASSWD File

The HTPASSWD file, as mentioned earlier, contains the list of established usernames and passwords. The structure of this file is very simple. An example is shown below:

```
valid_user:yDPtSBMJfPGrU
joe_jones:hqrIMzCnZzgm
```

This example shows two users, **valid_user** and **joe_jones**. From our previous example, we see that only **valid_user** is permitted to view our particular directory. In this way, you can set up an htpasswd file to protect multiple directories based on the username.

The username is separated from the password by a colon. The password itself is encrypted, to prevent anyone viewing the text file from seeing the password. There are several web scripts available to help you generate your passwords. A few of these are listed in the next section.

Again, store the htpasswd file in a directory separate from your web folder, if at all possible. Even though the passwords in the file are encrypted (and can't be decrypted), storing the file separately will prevent anyone from learning what valid usernames are enabled for your site, which makes hacking monumentally more difficult.

For More Information

For more information about htaccess, try one of the following websites. If you have questions or get stuck, contact the Mu Beta Psi webmaster for assistance, at webmaster@mubetapsi.org. Happy coding!

- HTACCESS information at Free Webmaster Help (Basic):
  www.freewebmasterhelp.com/tutorials/htaccess
- Password Encryption Script at KXS:
  www.kxs.net/support/htaccess_pw.html
- More advanced HTACCESS tutorial:
  www.javascriptkit.com/howto/htacess.shtml


MBΨ
Mu Beta Psi
National Honorary Musical Fraternity
http://www.mubetapsi.org
webmaster@mubetapsi.org