Making your setup more secure

When configuring the access control for your server, you will want to make sure you do not give any unauthorized access to anyone. Please follow these guidelines to ensure that your server is not compromised.

- A word of caution on DNS based access control and user authentication

  The access control by hostname and Basic user authentication facilities provided by HTTPd are relatively safe, but *not bulletproof*. The user authentication sends passwords across the network in plaintext, making them easily readable. The DNS based access control is only as safe as DNS, so you should keep that in mind when using it. Bottom line: If it absolutely positively cannot be seen by outside people, you probably should not use HTTPd to protect it.

- Disable Server−side includes wherever possible

  Whenever you can, use the Options[1] directive to disable server−side includes[2]. At the very least, you should disable the exec[3] feature. Note that because the default value of Options is All, you should include an Options directive in every Directory[4] clause in your global ACF and in every .htaccess file you write.

- Use AllowOverride[5] None wherever possible

  Use this directive to prevent any "untrusted" directories (such as users' home directories) from overriding your settings (and thus allowing their friends to execute xterms as nobody with a server−side include or other such horrors). You also gain a bonus in performance.

- Protect your users' home directories

  Protect your users' home directories with `Directory` directives. If your users all have their home directories in one physical location (such as `/home`), then this is easy:

  ```
  <Directory /home>
  AllowOverride None
  Options Indexes
  </Directory>
  ```

  If they are not all in one location such as /home, then you should use this wildcard pattern[6] to secure them (assuming your UserDir[7] is set to `public_html`):

  ```
  <Directory /*/public_html*>
  AllowOverride None
  Options Indexes
  </Directory>
  ```

1 ../setup/access/Options.html
2 includes.html
3 includes.html#exec
4 ../setup/access/Directory.html
5 ../setup/access/AllowOverride.html
6 ../setup/MatchExp.html
7 ../setup/srm/UserDir.html

In addition, if you wish to give your users the ability to create symbolic links to things only they own, use the Option `SymLinksIfOwnerMatch`.

Return to tutorial overview[8]

NCSA HTTPd Development Team / httpd@ncsa.uiuc.edu[9] / 9–11–95

[8] index.html
[9] ../FeedBack.html