How to set securest permissions on my MyBB based forum's files?

Have you a MyBB based forum on your site?

Author: imei Addmimistrator
Contact: Addmimistrator@Gmail.com
Web: http://myimei.com/security
Published: Dec-06-2006

MyBB had become one of most well-known and powerful forum web softwares and it is going to became better. If you have a MyBB based site, you may like to know about how to have secure configured file permissions on your host. Also hackers will not always come from your public root files, but they sometimes abuse other ways of your site. For example there are some exploits published for some files that never call in usual state. So it is better to take some of unnecessary permissions to prevent such abuses.

Please note that this recommendation will not guarantee your board against hackers, but it makes doing some stuff (i.e. editing your MyBB files for making backdoors or collecting your board's configuration) much harder or even impossible.

Now we're going to review an ideal permission setting for your boards.
Please note that these configurations are for a usual board and if you have some specification in configuration or you have a modification on MyBB, Maybe these advices don’t help you. If so, you may contact me to find your site's special solution for a little cost.

Scope	R	W	E	G	P	Description
/	+	-	+	+	+	Root folder
/*.*	+	-	-	+	+	Files of root
/global.php	+	-	-	-	-	Global file should not call
/admin	+	-	+	+	+	Even better if pass protected
/admin/*.*	+	-	-	+	+	Global.php should be as root
/archive	+	-	+	+	-	
/archive/*.*	+	-	-	+	-	Global.php should be as root
/css	+	+	+	+	-	If themes are file based.
/css	+	+	-	+	-	If themes are file based.
/images	+	-	+	+	-	
/images/*.*	+	-	-	+	-	
/inc	+	-	+	-	-	

/inc/languages/*.*	+	+	-	-	-	If admin likes edit lang terms
/inc/cache	+	+	+	-	-	If cache is file based cache
/install	-	-	-	-	-	Should be renamed
/inc/config.php	+	-	-	-	-	Config.php is not usable more than upgrade or install time.
/inc/settings.php	+	+	-	-	-	Should be writable for editing settings.
/jscripts	+	-	+	+	-	
/jscripts/*.*						
/[uploads]	+	+	+	-	-	Depend with your configuration this location may be different
/[uploads]/*.*	+	+	-	-	-	
/[avatars]	+	+	+	+	-	Depend with your configuration this location may be different
/[avatars]/*.*	+	+	-	+	-	

Legend:
+ (granting relevant permission (i.e. +R means access to read)
- (prevention of relevant permission (i.e. –R means not allowed for read)

[NIX File system permission]
Directories for directories and subdirectories; files for files and subdirectories' files

W: Write (access for writing on file or folder in NIX file system or Win if possible)
R: Read (access for reading content of a file or directory in NIX file system or Win if possible)
E: Execute/List (access of executing a file or Listing contents of a directory in NIX file system (Win Incompatible). Note that some of NIX distributions make differences between allowing listing and allowing reading in manner with directories, so you have to allow both reading and listing if you'd like to i.e. include some file.

[Apache permissions; directories for directories and subdirectories and all files in them]

G: Get (access of getting a specified file as a URL and make apache to pass it to its handler. If a file has not Get permission apache will not allow users to call them via their browser.
P: Post (access of sending data to a file via HTTP POST Method)

If you don’t know how to set these permissions on your site, please contact your hosting provider or keep waiting for next guidelines about this topic. I'll provide some `.htaccess` directive for more security in your site.