Indexscan 2.03 released - Modules

NEWS_PDF_AUTHOR: culex

NEWS_PDF_DATE: 2010/1/18 21:50:27

The modules scans your webfolders for missing index.html files. It skips folders where there are already indexfiles (index.php, index.html, index.html). If you find folders without you can automaticly create these by pressing \"create index files\". **New in 2.03** - Check web files against checkfile with xoops file names and filter with allowed extensions in config. Red colored showing files not equal to the settings allow manuel delete using ajax+jquery to prevent page reload. - Create backup containing only empty folders, index.html files and download as zip. **Why use index.html files ?** Unless the webmaster disallows casual folder browsing on the web server, most of the contents of each folder can be listed in a browser pointing to that Internet address. This concept is easily demonstrable by typing most any website address into the address bar of an Internet browser and simply adding a forward-slash and this folder name to the address: If the folder of the website navigated to is not protected, a listing of all the files in the folder will be displayed. Any of the files in the resulting display may be right-clicked on and the \'save as\' option taken in order to save that file to a hard drive. In most cases websites will have an images folder, and this folder will not ususually be protected from casual browsing. If so, the entire contents of the images folder will be accessible to the public at large. Depending upon file types, the files in an unprotected web folder may or may not be accessible; .php, .asp, and .aspx files are not accessible although .gif, .jpg, .bmp, .png, and other image files are fully accessible. Additionally, without folder protection in place, a hacker can make use of configuration files as well, such as config.inc and that could be where the websites database connection strings are held! Therefore, the database itself could become compromised. Source:Easy Website Security The module looks through the txt in your index.php, index.html, index.htm, mainfile.php, headers and footers for the words iframe or code indicating encoded javascript etc wich is commonly used in coded javascript inserts. Should it find some occurencies of these words you can yourself check the source code by clicking the red bar emmerging at the line for the file. Do not check the files just because the module finds these words in your pages. Not all uses of iframe and javascript is equal to damaging code and therefor better to check and if in doubt ask for help about what to do with these files. **Changes in 2.03** - Added possibility to check files in webfolders against xoops check file and filter from Config. Filter separates extensions of files presumed to be ok. - Files found in check files marked red are presumed not to be part of Xoops, and can be deleted by the \'delete icon\' using ajax + jquery avoid reloading the page. - Added the PclZip.Class to create zip file on the fly for users not having php > 5.20. - Scan to create back up from the folders residing in the admin/folder2backup. The scan creates a copy of the empty folders, existing index.html, index.php, index.htm files, delete all other files, creates new indexfiles, and create link to download as zip. Handy when working with developing and want to create a zip with nothing but index files. I tested with htdoc from Xoops 2.4.4 in a Wamp, creation time is aprox. 2 minutes. Not tested in real server yet, but time must be considerble. - New language defines are **(modinfo.php)**

```
//Added in 2.03

define ("_MI_INDEXSCAN_ILLEGALFILETYPES", "Skip file types.");
define(
"_MI_INDEXSCAN_ILLEGALFILETYPES_DE
SC","Add files you wish to skip while 'checking files'.
These files will be considered 'safe'
if they also are listed in the file 'admin/filecheck.txt'.");
define("_MI_INDEXSCAN_FROMBACKUP", "Create file zip");
define (
"_MI_INDEXSCAN_FROMBACKUP_DESC",
"Creates a zip archieve with same folder structure from the folder you ftp to folder2backup.
The zip contains nothing but the folders and,
index.html files where missing from
your uploaded folder.

The folder name is the name of the folder in your folder2backup folder, for instance 'testing'.
You can delete 'testing' this folder is only for example.");
```

(admin.php) // Added in 2.03

```
 define ("_AM_INDEXSCAN_CHECKILLEGALFILES","Check files");
define ("_AM_INDEXSCAN_SCANNING4ILLEGALFILES", "Scanning web files");
define("_AM_INDEXSCAN_MAYBEOK", "Looks to be ok");
define ("_AM_INDEXSCAN_NOTINXOOPSINSTALL", "Not Xoops file");
define ("_AM_INDEXSCAN_FINISDILLEGAL",
" files found that are not Xoops files. Total files scanned: ");
define ("_AM_INDEXSCAN_ILLEGAL_DESC",
"The file found Not to be Xoops files, are checked against checkfile.txt in admin folder, and agai
ns files in config defined as allowed file types.
These files could be unwanted tmp, thumbs.db, or info files.
If you you dont need these files add them to automaticly delete in config and they will be deleted
 when you run this scan next time.");
define ("_AM_INDEXSCAN_REALLYDELETE", "Are you sure ?, delete file.: ");
define("_AM_INDEXSCAN_CREATEZIP", "Create zip file for download");
define("_AM_INDEXSCAN_CREATINGZIP", "Creating backup with empty folders
plus index files.
");
define(
"_AM_INDEXSCAN_BACKEDUPD
ELETEDFROMBACKUP", "Deleted files in folder from backup except index.html files");
define("_AM_INDEXSCAN_BACKEDUP2", "Backed up folder.: ");
define("_AM_INDEXSCAN_DOWNLOADZIP", "Download index files zip");
define("_AM_INDEXSCAN_CREATINGZIPFORDOWNLOAD", "Creating zip file for download");
define(
"_AM_INDEXSCAN_CREATEDINDEXINBACKUP", "Created index file in backup folder");
define("_AM_INDEXSCAN_CLEANUPDONE", "Cleaning up...Done!");
define("_AM_INDEXSCAN_FILESARECOPIED", " Files were copied to backup folder");
```

```
define("_AM_INDEXSCAN_FILESDELETED", " Files were deleted from backup folder again");
define("_AM_INDEXSCAN_FILESCREATED",
" Index.html files were created in backupfolder");
```

Indexscan 2.03 released

The modules scans your webfolders for missing index.html files. It skips folders where there are already indexfiles (index.php, index.html, index.html). If you find folders without you can automaticly create these by pressing \"create index files\". **New in 2.03** - Check web files against checkfile with xoops file names and filter with allowed extensions in config. Red colored showing files not equal to the settings allow manuel delete using ajax+jquery to prevent page reload. - Create backup containing only empty folders, index.html files and download as zip. **Why use index.html files ?** Unless the webmaster disallows casual folder browsing on the web server, most of the contents of each folder can be listed in a browser pointing to that Internet address. This concept is easily demonstrable by typing most any website address into the address bar of an Internet browser and simply adding a forward-slash and this folder name to the address: If the folder of the website navigated to is not protected, a listing of all the files in the folder will be displayed. Any of the files in the resulting display may be right-clicked on and the \'save as\' option taken in order to save that file to a hard drive. In most cases websites will have an images folder, and this folder will not ususually be protected from casual browsing. If so, the entire contents of the images folder will be accessible to the public at large. Depending upon file types, the files in an unprotected web folder may or may not be accessible; .php, .asp, and .aspx files are not accessible although .gif, .jpg, .bmp, .png, and other image files are fully accessible. Additionally, without folder protection in place, a hacker can make use of configuration files as well, such as config.inc and that could be where the websites database connection strings are held! Therefore, the database itself could become compromised. Source:Easy Website Security The module looks through the txt in your index.php, index.html, index.htm, mainfile.php, headers and footers for the words iframe or code indicating encoded javascript etc wich is commonly used in coded javascript inserts. Should it find some occurencies of these words you can yourself check the source code by clicking the red bar emmerging at the line for the file. Do not check the files just because the module finds these words in your pages. Not all uses of iframe and javascript is equal to damaging code and therefor better to check and if in doubt ask for help about what to do with these files. **Changes in 2.03** - Added possibility to check files in webfolders against xoops check file and filter from Config. Filter separates extensions of files presumed to be ok. - Files found in check files marked red are presumed not to be part of Xoops, and can be deleted by the \'delete icon\' using ajax + jquery avoid reloading the page. - Added the PclZip.Class to create zip file on the fly for users not having php > 5.20. - Scan to create back up from the folders residing in the admin/folder2backup. The scan creates a copy of the empty folders, existing index.html, index.php, index.htm files, delete all other files, creates new indexfiles, and create link to download as zip. Handy when working with developing and want to create a zip with nothing but index files. I tested with htdoc from Xoops 2.4.4 in a Wamp, creation time is aprox. 2 minutes. Not tested in real server yet, but time must be considerble. - New language defines are **(modinfo.php)**

```
//Added in 2.03

define ("_MI_INDEXSCAN_ILLEGALFILETYPES", "Skip file types.");
define(
"_MI_INDEXSCAN_ILLEGALFILETYPES_DE
SC","Add files you wish to skip while 'checking files'.
These files will be considered 'safe'
if they also are listed in the file 'admin/filecheck.txt'.");
```

```
define("_MI_INDEXSCAN_FROMBACKUP", "Create file zip");
define (
"_MI_INDEXSCAN_FROMBACKUP_DESC",
"Creates a zip archieve with same folder structure from the folder you ftp to folder2backup.
The zip contains nothing but the folders and,
index.html files where missing from
your uploaded folder.

The folder name is the name of the folder in your folder2backup folder, for instance 'testing'.
You can delete 'testing' this folder is only for example.");
```

(admin.php) // Added in 2.03

```
 define ("_AM_INDEXSCAN_CHECKILLEGALFILES","Check files");
define ("_AM_INDEXSCAN_SCANNING4ILLEGALFILES", "Scanning web files");
define("_AM_INDEXSCAN_MAYBEOK", "Looks to be ok");
define ("_AM_INDEXSCAN_NOTINXOOPSINSTALL", "Not Xoops file");
define ("_AM_INDEXSCAN_FINISDILLEGAL",
" files found that are not Xoops files. Total files scanned: ");
define ("_AM_INDEXSCAN_ILLEGAL_DESC",
"The file found Not to be Xoops files, are checked against checkfile.txt in admin folder, and agai
ns files in config defined as allowed file types.
These files could be unwanted tmp, thumbs.db, or info files.
If you you dont need these files add them to automaticly delete in config and they will be deleted
 when you run this scan next time.");
define ("_AM_INDEXSCAN_REALLYDELETE", "Are you sure ?, delete file.: ");
define("_AM_INDEXSCAN_CREATEZIP", "Create zip file for download");
define("_AM_INDEXSCAN_CREATINGZIP", "Creating backup with empty folders
plus index files.
");
define(
"_AM_INDEXSCAN_BACKEDUPD
ELETEDFROMBACKUP", "Deleted files in folder from backup except index.html files");
define("_AM_INDEXSCAN_BACKEDUP2", "Backed up folder.: ");
define("_AM_INDEXSCAN_DOWNLOADZIP", "Download index files zip");
define("_AM_INDEXSCAN_CREATINGZIPFORDOWNLOAD", "Creating zip file for download");
define(
"_AM_INDEXSCAN_CREATEDINDEXINBACKUP", "Created index file in backup folder");
define("_AM_INDEXSCAN_CLEANUPDONE", "Cleaning up...Done!");
define("_AM_INDEXSCAN_FILESARECOPIED", " Files were copied to backup folder");
define("_AM_INDEXSCAN_FILESDELETED", " Files were deleted from backup folder again");
define("_AM_INDEXSCAN_FILESCREATED",
" Index.html files were created in backupfolder");
```

Indexscan 2.03 released