E.g. why is there an error suddenly, has somebody files modified / hacked or was there an update from outside, what has a programmer / supplier modified, have you been hacked etc. Solution a Web File Checker / Detector or a Web Hacked Checker / Detector. Check your webstore on or detect modifications and configuration settings.

I created a module for Magento and because I am too busy I created 1 program for all other webshops that can be run as an cronjob. When I have extra time, I will create a module for the settings of this cronjob and to view the modifications log. If somebody else want to do this job I will update this download and put his/her name on this page. Currently you find all the settings in the beginning of this cronjob like your email address to set. The installation asks for minimal technical skills (or ask your programmer).

For this cronjob, cronjobs must (already) set up at your provider and you must have enough time from your provider to run for at least 5 minutes (this varies for customers from 1 to 5 minutes on a slow server).

This program may run every day 2x as cronjob at 07.00 and 15.00 (can be changed in your cron panel of course with your own schedule, e.g. 0 7,15 * * *).

It checks always which VirtueMart/Joomla files are modified since the last run. It also checks for changed configuration settings.

If modified you will receive a report per email, otherwise an empty email with subject. After the first run you receive all filenames and configuration settings (not really, more a link to the log the first time). I send always 2 emails, because 1 email with an attachment can be considered as spam sometimes. But you can remove this email from the script of course.

So you can check always what have been modified (by someone or an update) e.g. to solve errors.

In the protected directory you can find the webfilechecks log with modifications on date. Or e.g. to clean this log after a long period.

If you create a backup from these few files and later restore, you can determine the changes always again since your last backup! There are only 3 files in the protected wfc-cronjob directory: 1) oa_wfc_ref.log (reference log files) 2) ooa_wfc_ref_conf.log (reference log configuration variables) 3) ooa_wfc_mod.log (changes compared to both reference logs). Through restoring 1) and 2) changes can be determined again. If you for example have been hacked, you can easily see which files have been modified!

Please don't touch the reference logs, these logs are necessary for comparisons in a next run.

Language English.

Installation:

- download .zip file and unpack

- install the directory wfc-cronjob in your admin directory

- protect your wfc-cronjob directory (always better)

- define your cronjob running /wfc-cronjob/wfc_cron.php running 2x at e.g. 07.00 and 15.00 (0 7,15 * * *)

Extension support:

No support (too busy), but a few questions will be answered here.

Only bugs will be fixed later concerning the extension itself.

Questions will be NEVER answered per email!

Extension history:

Such a script was there already for OsCommerce (but more extensive). I tried then in 2013 to find such scripts for other webshops but nothing found. Then I found a snippet on the internet how you could easily determine if programs (files) were changed and used this for the WebFileChecker.