QFQ - Support #11953

überall absolue anstatt relative pfade verwenden für Filesystem pfade

05.02.2021 12:14 - Marc Egger

Status:	Closed	**Start date:**	05.02.2021
Priority:	Normal	**Due date:**	
Assignee:	Marc Egger	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	21.3.0	**Spent time:**	0.00 hour
Discuss:			

Description

anstatt cwdToApp zu setzen bei jedem Entrypoint, setzen wir absolutApp in Path:setMainPaths
Somit sind wir nicht mehr abhängig von dem CWD oder der art und weise wie ein Entrypoint aufgerufen wird.
Speziell für Unittests sollte dies eine grosse erleichterung sein.

Related issues:

Related to QFQ - Support #11926: Anmerkungen zu FormAsFile	**Closed**	**31.01.2021**

Associated revisions

Revision ad87c16e - 08.02.2021 10:54 - Marc Egger

Refs #11953 Logger.php: replace makePathAbsolute with Path functions

Revision 86697ebb - 08.02.2021 14:43 - Marc Egger

Refs #11953 Path.php: add function which detects double dot. Function is not in use.

History

#1 - 05.02.2021 12:15 - Marc Egger

- Related to Support #11926: Anmerkungen zu FormAsFile added

#2 - 08.02.2021 11:38 - Marc Egger

Security Check realpath : to prevent certain attacks we could use the PHP function realpath() on all absolute paths before accessing the file and make sure that the path is inside our App directory.

Problem: the file must exist, otherwise realpath() returns false. In many places in our code we construct an absolute path to a file or folder which might not exist and if it doesn't, it is created. Therefore we cannot use this simple check here.

Out of all 47 places where an absolute path is computed most of them are concatenations of path constants which do not pose a security risk. There is only one dynamic path where we access a file which must exist: When we execute a script using the _script column. But the realpath check would only give a small security benefit here, since the path to the script is never user generated.

A much simpler security feature would be to disallow double dots /../ in user generated paths. Of the 47 places where absolute paths are computed there is not one which would need to allow /../

#3 - 08.02.2021 11:57 - Carsten Rose

- Gerade bei den Scripts koennte es gewuenscht sein sowohl mit '..' als auch ausserhalb des App Dirs zu arbeiten.
- Auf den I-MATH Server liegen viele Scripts, die von QFQ getriggert werden, unter `/etc/scripts` - das ist sinnvoll da man so nicht identische Scripts an mehreren Stellen hat. Also Einschraekung auf 'App Dir' ist keine gute Ueberlegung.
- Andere Admins setzen ihr System anders auf. Ggfs. benoetigen Sie '..' - wenn realpath() 'on the fly' die Pfade anpasst, haette ich noch wenig Sorgen, aber '..' zu verbieten laesst bei uns das Telefon klingeln ...

D.h. wir koennen diese Sicherheits Intitiative vermutlich abbrechen.

#4 - 08.02.2021 14:35 - Marc Egger

ok, lassen wirs.

Habe schon eine Funktion geschrieben, die testet ob '..' vorkommt in einem Pfad. Lasse die mal drin. vielleicht brauchen wir sie mal. siehe commit 86697ebb

#5 - 09.02.2021 11:40 - Marc Egger

- Status changed from New to In Progress

#6 - 08.03.2021 00:08 - Carsten Rose

- Target version changed from 22.4.0 to 21.3.0

Kann das Ticket geschlossen werden?

#7 - 16.03.2021 17:10 - Marc Egger

- Status changed from In Progress to Closed

ja