QFQ - Feature #12039

Missing htmlSpecialChar() in pre processing on form submit

18.02.2021 00:09 - Carsten Rose

Status:	New	**Start date:**	18.02.2021
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	21.8.0	**Spent time:**	0.00 hour
Discuss:			

Description

Wird auf Formularelemente mittels '{{notiz:F:allbut}}' zugegriffen, sind dies VERMUTLICH nicht htmlSpecialChar kodiert.

- Check ob dem so ist.

Damit waere das folgende einem potentiellen SQL Inject Angriff ausgeliefert (notiz="1' OR 1")

```
sqlValidate = {{!SELECT n.notiz FROM notiz AS n WHERE  n.gr_id={{gr_id:RS0}} AND n.category=0  AND
 n.file_typ="Uebung" AND n.notiz='{{notiz:F:allbut}}'  AND n.id !=
{{id:R0}} }}
```

- Abhilfe koennte eine neue Escape Klasse sein, die bei Default beim STORE_FORM htmlSpecialChar() anwendet.
- Achtung: was passeirt wenn nicht mit single sondern mit double quotes im SQL Statement gearbeitet wird?
- In der QFQ Doc bei den Bestpractices angeben das immer mit single quotes gearbeitet werden soll.

History

#1 - 18.02.2021 00:09 - Carsten Rose

- Tracker changed from Support to Feature