QFQ - Bug #11702

HTML Special Char makes no sense for 'allbut' if '&' is forbidden

06.12.2020 15:02 - Carsten Rose

Status:	New	**Start date:**	06.12.2020
Priority:	Normal	**Due date:**	
Assignee:	Carsten Rose	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	21.7.0	**Spent time:**	0.00 hour
Discuss:			

Description

- Siehe #5112
- Das '&' sollten wir erlauben, denn mit HTMLSpecialChar wird es kodiert.
- Ist '&' verboten, ist der Nutzen von allbut nicht sehr hoch.
- Ist '&' erlaubt und Encode=none - kann gefaehrliches passieren.

Hier ist eine lange Liste mit Moegelichen Angriffen: https://owasp.org/www-community/xss-filter-evasion-cheatsheet

Waere es sinnvoll bei 'encode=None' eine Warnung anzuzeigen (anstelle der aktuellen sinnlosen)?

Related issues:

Related to QFQ - Feature #5112: FormElement Check Type = allbut nicht kompati...	**Closed**	**14.12.2017**

History

#1 - 06.12.2020 15:02 - Carsten Rose

- Related to Feature #5112: FormElement Check Type = allbut nicht kompatibel mit Encode = Specialchar added

#2 - 07.12.2020 16:24 - Carsten Rose

- Due date set to 18.12.2020

- Assignee changed from Marc Egger to Carsten Rose

Nach Rueckssprache mit Marc: Warnung kann entfernt werden, ist sowieso nicht mehr relevant, da & eingegeben werden kann.

Idee:
1) Aehliche Warnung fuer None + patter|allbut|all
2) auto kann bei 'specialchar' auf 'all' stehen.

#3 - 03.05.2021 20:48 - Carsten Rose

- Tracker changed from Support to Bug

#4 - 05.05.2021 09:12 - Carsten Rose

- Due date changed from 18.12.2020 to 17.05.2021

#5 - 12.06.2021 10:39 - Carsten Rose

- Due date deleted (17.05.2021)

- Target version changed from 21.8.0 to 21.7.0

Files

allbut.png	52.3 KB	06.12.2020	Carsten Rose