

QFQ - Bug #5030

Dokumentation: Code-Beispiel enthält Sicherheitsproblem

30.11.2017 11:44 - Nicola Chiapolini

Status:	Closed	Start date:	30.11.2017
Priority:	High	Due date:	
Assignee:	Carsten Rose	% Done:	0%
Category:		Estimated time:	0.00 hour
Target version:	18.4	Spent time:	0.00 hour
Discuss:			

Description

<https://docs.typo3.org/typo3cms/drafts/github/T3DocumentationStarter/Public-Info-053/Manual.html#person-search-form>

Die Sanitizer in den Variablen ist falsch (all statt alnumx).

Im Bereich HTML erlaubt das Cross-Site Scripting.

Suche zum Beispiel nach:

```
'><h1>Hallo Welt</h1><br style='
```

SQL Injection scheint dank dem Default Escape blockiert, wäre sonst aber wohl auch möglich.

Associated revisions

Revision bd12dc86 - 21.01.2018 10:09 - Carsten Rose

#5030, Manual.rst: Fixed example with XSS vulnerability.

History

#1 - 01.12.2017 11:07 - Nicola Chiapolini

- *Tracker changed from Support to Bug*

#2 - 21.01.2018 10:11 - Carsten Rose

- *Status changed from New to Closed*

Hallo Nicola

vielen Dank, ist in der naechsten Version gefixt.

CU

Carsten

#3 - 21.01.2018 10:15 - Carsten Rose

- *Assignee set to Carsten Rose*

- *Target version set to next*

#4 - 30.04.2018 18:00 - Carsten Rose

- *Target version changed from next to 18.4*