XWiki Platform XWIKI-19155

# Simple users can create global SSX/JSX without specific rights

## Details

| | | | |
|---|---|---|---|
| Type: | Bug | Resolution: | Fixed |
| Priority: | Major | Fix Version/s: | 12.10.11, (2) |
| Affects Version/s: | 3.1 M1 | | |
| Component/s: | Skin - Skinx | | |
| Labels: | attack_impersonation, attacker_edit, security | | |
| Difficulty: | Unknown | | |
| Documentation: | N/A | | |
| Documentation in Release Notes: | N/A | | |
| Similar issues: | | | |

## Description

The PR rights for adding an "always used" Skinx extension (be it SSX or JSX) is currently checked against the content of the document, instead of being checked against the metadata author. It means that any document with a content edited by a user with PR rights can be edited by a standard user to add a JSX that will be executed everywhere in the wiki.

Reproduction steps:

- Create a document with Admin user (who has PR rights)
- Login with a user with edit rights (no need for script rights)
- Edit the previously created document to add a Javascript object containing only `console.log("Hello hello");` and set this object to be used on the whole wiki
- Log out and navigate

Expected result:

- the console log should not be output since the user doesn't have PR rights

Obtained result:

- the console log is displayed everywhere

## Issue Links

**relates to**

XSKINX-8 Implement always used extensions — CLOSED

**links to**

Github Security advisory

## Activity

There are no comments yet on this issue.

## People

Assignee:

Simon Urli

Reporter:

Simon Urli

Votes:

0 Vote for this issue

Watchers:

1 Start watching this issue

## Dates

Created:

19/Nov/21 10:58

Updated:

07/Jul/22 11:30

Resolved:

19/Nov/21 16:05