



Unauthenticated user can retrieve the list of users through uorgsuggest.vm

Details

Type:	Bug	Resolution:	Fixed
Priority:	Minor	Fix Version/s:	12.10.11, (2)
Affects Version/s:	12.10.8, 13.6-rc-1		
Component/s:	Web - Templates & Resources		
Labels:	attack_dataleak attacker_guest security		
Tests:	Unit		
Difficulty:	Unknown		
Documentation:	N/A		
Documentation in Release Notes:	N/A		
Pull Request Status:	Pull Request accepted		
Similar issues:			

Description

An unauthenticated user can retrieve a list of users and their fullname through a public accessible URL.

Reproducing steps:

Navigate to :

```
http://<server>/bin/login/XWikiLogin?xpage=uorgsuggest&uorg=user&wiki=&media=json
```

Results:

- uorgsuggest gives access to user fullname and reference even if the wiki is private

Expected Results:

- User fullname and documents fullname should not be accessible to anyone who don't have corresponding rights

Issue Links

is related to

- [XWIKI-18851](#) Unauthenticated user can retrieve user information through getdeleteddocuments.vm CLOSED
- [XWIKI-16544](#) Unauthenticated user can retrieve the list of users through getdocuments.vm CLOSED

relates to

- [XWIKI-18849](#) Private user data are accessible through suggest.vm CLOSED
- [XWIKI-20007](#) When sharing a page from a subwiki, global users with restricted access get suggested CLOSED

links to

- [GHSA-97jg-43c9-q6pf](#)

Activity

Newest first

- ▼ [Manuel Leduc](#) added a comment - 13/Oct/21 16:00
<https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-97jg-43c9-q6pf>
- ▼ [Manuel Leduc](#) added a comment - 29/Sep/21 14:36

▼ **Manuel Leduc** added a comment - 28/Sep/21 11:30

Note: The problem is only visible when anonymous users are not allowed to view the pages of the wiki (and in particular the user pages XWiki.Username).

To reproduce, check Prevent unregistered users from viewing pages, regardless of the page rights in the User -> Rights section of the Administration.



Visiting <http://localhost:8080/xwiki/bin/view/XWiki/Admin> redirect the user to the login page but visiting <http://localhost:8080/xwiki/bin/login/XWikiLogin?xpage=uorgsuggest&uorg=user&wiki=&media=json> shows the list of users.

▼ **Guillaume COQUARD** added a comment - 22/Jul/21 18:40

They all concern template doing queries and returning results and not filtering them.

▼ People

Assignee:

 **Manuel Leduc** 

Reporter:

 **Guillaume COQUARD** 

Votes:

0 Vote for this issue

Watchers:

2 Start watching this issue

▼ Dates

Created:

22/Jul/21 18:29

Updated:

26/Jul/22 09:36

Resolved:

13/Oct/21 15:19

Date of First Response:

28/Sep/21 11:30 AM