



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

Details

Type:	Bug	Resolution:	Fixed
Priority:	Minor	Fix Version/s:	12.10.11, (2)
Affects Version/s:	8.4.5, 10.11.8, 11.3.1, 13.6-rc-1		
Component/s:	Like, (2)		
Labels:	attack_dataleak attacker_guest security		
Tests:	Unit		
Development Priority:	Low		
Difficulty:	Hard		
Documentation:	N/A		
Documentation in	N/A		
Release Notes:			
Similar issues:			

Description

An unauthenticated user can retrieve the list of users through a public accessible URL

Note: the dataleak is only true in case of a closed wiki, with specific rights to allow the usage of ForgotUsername/ResetPassword pages.

Note: a "closed wiki" is when "Prevent unregistered users from viewing pages, regardless of the page rights in the User" is checked in the admin (XWiki.XWikiPreference.authenticate_view = true)

To reproduce this access one of the following:

```
<server>/xwiki/bin/get/XWiki/ForgotUsername?
xpage=getdocuments&childrenOf=XWiki&exclude=XWiki.ForgotUsername&queryFilters=unique,hidden&offset=1&limit=100&reqNo=2
```

```
<server>/xwiki/bin/get/XWiki/ResetPassword?
xpage=getdocuments&childrenOf=XWiki&exclude=XWiki.ResetPassword&queryFilters=unique,hidden&offset=1&limit=100&reqNo=2
```

```
<server>/xwiki/bin/login/XWikiLogin?xpage=getdocuments&limit=10000
```

Note: ForgotUsername/ResetPassword are not accessible anymore, but the issue is still true for XWikiLogin, and needs to be solved in a general way.

It managed to make them inaccessible by removing the XwikiGuest user from objects of these pages:

- <server>/xwiki/bin/edit/XWiki/ResetPassword
 - <server>/xwiki/bin/edit/XWiki/ForgotUsername
- But this makes the Reset password / username unusable.

Note that this issue is not directly related to ResetPassword / ForgotUsername pages: it exists for any page of the wiki available for guest user.

In addition to getdocuments from the examples above, the following templates could also be used in the same way, and have been fixed accordingly:

- getdeleteddocuments.vm
- getgroupmembers.vm
- getgroups.vm
- getusers.vm

Issue Links

causes



XWIKI-19755 Changing the pagination page when all the results are already fetched empties the livetable



CLOSED

depends on

is related to

❏ [XWIKI-18851](#) Unauthenticated user can retrieve user information through getdeleteddocuments.vm

🔒 CLOSED

❏ [XWIKI-16610](#) Forgot Username and Reset Password are not available in closed wiki

🔒 CLOSED

relates to

❏ [XWIKI-18849](#) Private user data are accessible through suggest.vm

🔒 CLOSED

[Show 5 more links](#) (4 relates to, 1 links to)

▼ Activity

Newest first

▼ [Manuel Leduc](#) added a comment - 15/Oct/21 11:25

<https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-qpp2-2mcp-2wm5>

▼ [Guillaume COQUARD](#) added a comment - 22/Jun/21 11:40 - edited

I proposed a fix [here](#).

The rationale is to not provide non-viewable document reference but in order to fix an offset problem, provide the overall checked rows number in the response. In that way it allows to make it work with something like a pagination that depends on getdocuments.

▼ [Anca Luca](#) added a comment - 08/Apr/21 16:18

Note that since XWiki 13.1RC1 and with [XWIKI-11205](#) being fixed, it's now possible to remove the ForgotUsername/ResetPassword pages (kept for backward compatibility reasons) which should be enough in most cases to protect against this issue. Now as I mentioned in my latest comment, nothing prevents to have the issue again because of another page, so we should properly fix this for any page.

So, what I understand from here is that starting with XWiki 13.1 RC1 we can get rid of the problem described by this issue for part of the usecases, those that had view rights for unauthenticated users only because there was no other way to allow Forgot Username / Reset password actions.

But, indeed, the problem remains for all the other cases when view rights for unauthenticated users is given for other reasons...

▼ [Simon Urli](#) added a comment - 05/Mar/21 10:05

Discussion on that topic with Anca Luca shows that the issue might be wider than just ForgotUsername/ResetPassword page we might fix it only by not disclosing the full name of a page in getdocuments.vm (see: <https://github.com/xwiki/xwiki-platform/blame/master/xwiki-platform-core/xwiki-platform-web/src/main/webapp/templates/getdocuments.vm#L145>).

I think that fix would also be related with [XWIKI-9649](#) and the proposal I made in the comments of [XWIKI-17943](#). Note that the discussion we had with [luca](#) pushed towards a solution for checking scripts rights of users (at wiki level) at this specific line to only disclose the page names for those users. The rationale behind that is that:

1. users without script rights which cannot view a page won't get leaked data about those pages
2. users with script rights at wiki level, will always be able to get this info by using the API even if they don't have rights on those pages, so it's ok to display that info to them
3. users with script rights on subspace might be able to get that info too if they really want by creating a script in the space they have the proper right, but it's better for perf to not have to check the rights everywhere and it's not harmful to be a bit more restrictive in the UI.

▼ [Thomas Mortagne](#) added a comment - 03/Mar/21 10:45

Well we can keep ForgotUsername/ResetPassword but the special right setup on them (which is the real problem here) should be removed.

▼ [Simon Urli](#) added a comment - 01/Mar/21 18:18

Note that since XWiki 13.1RC1 and with [XWiki-11205](#) being fixed, it's now possible to remove the ForgotUsername/ResetPassword pages (kept for backward compatibility reasons) which should be enough in most cases to protect against this issue. Now as I mentioned in my latest comment, nothing prevents to have the issue again because of another page, so we should properly fix this for any page.

Simon Urli added a comment - 03/Nov/20 17:27

Discussion on that topic with [luca](#) shows that the issue might be wider than just ForgotUsername/ResetPassword page we might fix it only by not disclosing the full name of a page in getdocuments.vm (see: <https://github.com/xwiki/xwiki-platform/blame/master/xwiki-platform-core/xwiki-platform-web/src/main/webapp/templates/getdocuments.vm#L145>).

Camelia Andrei added a comment - 02/Nov/20 11:34 - edited

Also the list of pages can be retrieved.

```
<server>/xwiki/bin/get/XWiki/ForgotUsername?  
queryFilters=unique&exclude=XWiki.ForgotUsername&childrenOf=&xpage=getdocuments&offset=0&limit=1000
```

This issue is even more critical for instance with Google Apps installed, because a workaround this issue is to check: "Prevent unregistered users from viewing pages, regardless of the page rights" . But a the Google Apps extensions doesn't worked with that option checked:

<https://github.com/xwikisas/application-googleapps/issues/42> .

Also [XWiki-1661](#) si fixed.

Simon Urli added a comment - 25/Jul/19 15:19

This issue will become more critical when [XWiki-16610](#) will be fixed, but the changes made on [XWiki-16610](#) might also impact this.



Simon Urli added a comment - 25/Jul/19 14:24

This is actually a specific usecase: the dataleak is only true in case of a closed wiki, with specific rights to allow the usage of ForgotUsername/ResetPassword pages.



On an open wiki, the user profiles pages are publicly available, so it's not a dataleak IMO to be able to get access to them. And on a close wiki for unregistered users those pages are not even available, which is a bug IMO (cf <https://forum.xwiki.org/t/enable-forgot-password-forgot-username-in-xwiki-login/2262/5>).

People

Assignee:

 Manuel Leduc 

Reporter:

 Camelia Andrei 

Votes:

0 Vote for this issue

Watchers:

6 Start watching this issue

Dates

Created:

28/Jun/19 12:13

Updated:

12/Jul/22 16:34

Resolved:

15/Oct/21 10:55

Date of First Response:

25/Jul/19 2:24 PM