XWiki Platform XWIKI-18315

No CSRF protection on the password change form

Details

Type:	Bug	Resolution:	Fixed
Priority:	Major	Fix Version/s:	12.10.5, (1)
Affects Version/s:	1.3 M2		
Component/s:	Web - Templates & Resources		
Labels:	attacker_quest csrf security		
Difficulty:	Easy		
Documentation:	N/A		
Documentation in Release Notes:	N/A		
Similar issues:			

Description

There is no protection against CSRF type attacks on the password change form. The **form_token** parameter **is not checked** on the server side. It is possible to create a request without this parameter, and the password will be changed.

It is therefore very easy, under the condition of tricking an administrator, to be able to change the password of any user of the Wiki.

Here is an example of a query that allows you to change a password (user toto) on the current stable version of XWiki (POST and GET methods are possible):

GET /xwiki/bin/view/XWiki/toto?**xpage**=passwd&**xwikipassword**=**aaaaaaaa**&**xwikipassword2**=**aaaaaaaa** HTTP/1.1
Host: 127.0.0.1:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,**/**;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Origin: http://127.0.0.1:8080
Connection: close
Referer: http://127.0.0.1:8080/xwiki/bin/view/XWiki/toto?xpage=passwd
Cookie: JSESSIONID=1AC1B58E461B85FBE5E1C980197C5A64; username="**XXX**"; password="**XXX**"; rememberme="false"; validation="**XXX**"

Issue Links

links to

Github security advisory

Activity

Newest first

Simon Urli added a comment - 08/Nov/21 17:07

Note that this ticket is not about being able to change the password of the currently logged-in user, but about any other user: there's a protection when changing its own password by checking the old password.

So the reproduction steps are:
1. create a user, e.g. Foo
2. login with an Admin user (since admin can change password of other users)
3. Go to a forged URL (such as the one shown in description or in the previous comment for previous versions)

Simon Urli added a comment - 19/Mar/21 15:04 - edited

AFAICS the passwd.vm was introduced as part of ~~XWIKI-2114~~ so the issue exist since 1.3M2 probably.

Simon Urli added a comment - 19/Mar/21 14:58

Investigating on when exactly the issue sarted, note that before 11.9 (and ~~XWIKI-16623~~) the issue was already existing but the password reset was done with different parameters. The way to reproduce is with using an URL such as:

> http://localhost:8080/xwiki/bin/view/XWiki/Foo?xpage=passwd&password=totototo&password2=totototo

Simon Urli added a comment - 15/Mar/21 14:52

> I made a mistake and I actually fixed the ResetPassword page

So to be a bit more clear, I thought first this issue was related to ResetPassword so I bulletproof it a bit in my first commit, before realizing that it wasn't related to it, but to the usage of the register macros. I properly fixed those afterwards. What's provided in the description (not related to ResetPassword) is accurate.

Simon Urli added a comment - 03/Mar/21 15:22

Reopening: I made a mistake and I actually fixed the ResetPassword page, but not the passwd xpage...

People

Assignee:
Simon Urli

Reporter:
Pierrick Vuillemin

Votes:
0 Vote for this issue

Watchers:
2 Start watching this issue

Dates

Created:
07/Feb/21 18:34

Updated:
07/Jul/22 10:20

Resolved:
03/Mar/21 17:20

Date of First Response:
03/Mar/21 3:22 PM