

ForgotUsername is not protected against CSRF

Details

Type:	Bug	Resolution:	Fixed
Priority:	Major	Fix Version/s:	12.10.5, (1)
Affects Version/s:	12.10.4, 13.1-rc-1		
Component/s:	Administration		
Labels:	attacker_quest csrf security		
Difficulty:	Unknown		
Documentation:	N/A		
Documentation in	N/A		
Release Notes:			
Similar issues:			

Description


It's possible to perform a ForgotUsername request without needing a CSRF token:

<http://127.0.0.1:8080/xwiki/bin/view/XWiki/ForgotUsername?e=aaa%22bbb%27ccc%3Eddd%3Ceee> (before XWiki 13.1)

<http://127.0.0.1:8080/xwiki/bin/view/Main/WebHome?e=aaa%22bbb%27ccc%3Eddd%3Ceee&vm=forgotusername.vm&skin=default&xpage=xpart&language=en> (since XWiki 13.1)

Issue Links

is related to

 [XWIKI-18384](#) The "Forgot your username?" form offers too much information concerning user accounts

 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:

09/Mar/21 10:14

Updated:

07/Jul/22 10:20

Resolved:

09/Mar/21 14:20