

The "Forgot your username?" form offers too much information concerning user accounts

Type:	Bug	Resolution:	Fixed
Priority:	Major	Fix Version/s:	12.10.5, (1)
Affects Version/s:	10.11.9		
Component/s:	None		
Labels:	attack_dataleak attacker_quest security		
Tests:	Integration		
Difficulty:	Unknown		
Documentation:	N/A		
Documentation in	N/A		
Release Notes:			
Similar issues:			

Steps to reproduce:
<ul style="list-style-type: none">Click on "Forgot your username?" on the login screenOpen <a href="http://<server>/xwiki/bin/view/XWiki/ForgotUsername">http://<server>/xwiki/bin/view/XWiki/ForgotUsername and add both a valid email associated to an user and an invalid email
Result: the platform confirms if the user exists or not.
Expected result: a generic message concerning the user without confirming if it exists or not (e.g. "If the account is registered on the application, you will receive a dedicated message").

Attachments
<div><div><p>InvalidUserResult.png 24/Feb/21 16:25 59 kB</p></div><div><p>ValidUserResult.png 24/Feb/21 16:25 48 kB</p></div></div>

Issue Links
is related to
XWIKI-18787 The "Forgot your password?" form offers too much information concerning user accounts CLOSED
relates to
XWIKI-18408 ForgotUsername is not protected against CSRF CLOSED
XWIKI-18787 The "Forgot your password?" 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:

Reporter:

Votes:
0 Vote for this issue
Watchers:
1 Start watching this issue

Dates
Created:
24/Feb/21 16:27
Updated:
07/Jul/22 11:31
Resolved:
09/Mar/21 14:20