Redmine - Defect #37517
User disclosure vulnerability via "Forgot password" functionality

2022-07-28 10:12 - Alberto Guerrero

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Security	**Estimated time:**	0.00 hour
Target version:			
Resolution:	Duplicate	**Affected version:**	

Description

The redmine application reveals the existing users in the system database and their current status by using the "forgot password" functionality, as different messages will appear when entering your email to recover your password if the user in the email is pending approval, does not correspond to any user or is assigned to an active user.

This could therefore help attackers to perform more sophisticated and targeted brute force attacks.

Solution: Display the same message when executing this functionality, without differentiating whether the user exists, is pending approval or is incorrect.

Related issues:

Duplicates Redmine - Defect # 6254: Remove 'invalid user' notification on pas...	**New**	**2010-08-31**

History

#1 - 2022-08-11 00:43 - Mischa The Evil

- Duplicates Defect #6254: Remove 'invalid user' notification on password request with invalid e-mailadress added

#2 - 2022-08-11 00:46 - Mischa The Evil

- Status changed from New to Closed

- Resolution set to Duplicate

Thanks for filing this issue. Though, a similar request is already being tracked as issue #6254. As such I am closing this issue as a duplicate of it.