redmineorg-copy202205 - Vote #78746

HTTP code 401 on login failure

2022/05/09 18:21 - Admin Redmine

ステータス:	New	**開始日:**	2022/05/09
優先度:	通常	**期日:**	
担当者:		**進捗率:**	0%
カテゴリ:	Accounts / authentication_7	**予定工数:**	0.00時間
対象バージョン:		**作業時間:**	0.00時間
Redmineorg_URL:	https://www.redmine.org/issues/26677	**status_id:**	1
category_id:	7	**tracker_id:**	2
version_id:	0	**plus1:**	0
issue_org_id:	26677	**affected_version:**	
author_id:	306539	**closed_on:**	
assigned_to_id:	0	**affected_version_id:**	
comments:	2		

説明

When purposely causing a login error on Redmine, I can see (using web inspector and/or logfiles) that the HTTP return code is 200, i.e. "everything is ok", for the page that presents the error to the user.

It would be great if Redmine would return a 401 ("Unauthorized", see here: https://en.wikipedia.org/wiki/List_of_HTTP_status_codes#4xx_Client_errors).

Indeed, I think a 401 code in the webserver logs has great security value, and makes it easy to integrate with solutions such as Fail2Ban and others.

If this change were made, there should be absolutely no impact on the user.

journals

The 401 status code is specifically used for Basic or Digest authentication. It has no value when using form authentication as done with Redmine.

If Redmine would return a 401 here, your browser would ask for authentication with a Basic-Auth form, similar to

!https://i.stack.imgur.com/5C6Pp.png!

This not what we want. As such, returning a 200 is okay here for the user. When querying the API, we do already return a 401 if the user did not provide any credentials along with their request. API clients are equipped to deal with this.

This is not what I obtain with other services (e.g. with Jenkins CI instances), where a 401 code is returned, and presents the usual HTML login form (not through the browser, as the authentication is made through the application, not the web server).

履歴

#1 - 2022/05/10 17:05 - Admin Redmine

- カテゴリ を Accounts / authentication_7 にセット