

redmineorg-copy202205 - Vote #78308

RestAPI doesn't allow anonymous account registration but web interface does.

2022/05/09 18:13 - 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:	REST API_32	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/25296	status_id:	1
category_id:	32	tracker_id:	1
version_id:	0	plus1:	0
issue_org_id:	25296	affected_version:	
author_id:	220250	closed_on:	
assigned_to_id:	0	affected_version_id:	84
comments:	2		

説明

Rest API [Rest Users](#) doesn't allow a the creation of a new user if no admin rights are provided but is it possible for non authenticated user to registers through web interface at <http://redmine/account/register>

Environment:

Redmine version 2.5.2.devel
Ruby version 2.1.5-p273 (2014-11-13) [x86_64-linux-gnu]
Rails version 4.1.8
Environment production
Database adapter Mysql2

SCM:

Git 2.1.4
Filesystem

Redmine plugins:

no plugin installed

journals

When @Self-registration@ value is not "disabled", the following Rest API POST request creates the account with locked or activated status as @text/html@ format.

!settings_self-registration_except_disabled.png!

```
$ curl -i -H "Content-Type: application/json" -X POST http://localhost:3000/account/register.json \
-d '{"user": {"login": "XXXXX", "firstname": "YY", "lastname": "ZZZZZ", "mail": "XXXXX@example.com", "password":
*}}'
```

```
HTTP/1.1 302 Found
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Download-Options: noopen
X-Permitted-Cross-Domain-Policies: none
Referrer-Policy: strict-origin-when-cross-origin
Location: http://localhost:3000/my/account
Content-Type: text/html; charset=utf-8
Cache-Control: no-cache
Set-Cookie: _redmine_session=***** ...; path=/; HttpOnly
X-Request-Id: ***** ...
X-Runtime: 0.027633
Content-Length: 98
```

You are being [redirected](#).

The following GET request also returns error message as @text/html@ format, so I think that both should return JSON format when specifying /account/register.json.

```
$ curl -i -H "Content-Type: application/json" http://localhost:3000/account/register.json
```

HTTP/1.1 406 Not Acceptable

Content-Type: text/html; charset=utf-8

X-Request-Id: e0c96a76-32c6-44ce-afe7-066c86e218de

X-Runtime: 0.144548

Content-Length: 105021

<!DOCTYPE html>

Action Controller: Exception caught

:

履歴

#1 - 2022/05/10 17:06 - Admin Redmine

- カテゴリ を REST API_32 にセット