Redmine - Defect #25296

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

2017-03-09 16:53 - Sgargel Sgargel

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	REST API	**Estimated time:**	0.00 hour
Target version:			
Resolution:		**Affected version:**	2.5.2

Description

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
```

History

#1 - 2017-04-07 10:07 - Toshi MARUYAMA

- Category set to REST API

#2 - 2021-05-10 04:21 - Ko Nagase

- File settings_self-registration_except_disabled.png added

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": "ZZZZZZ", "mail": "XXXXX@example.com", "pas
sword": "************"}}'

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

<html><body>You are being <a href="http://localhost:3000/my/account">redirected</a>.</body></html>
```

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>
<html lang="en">
<head>
  <meta charset="utf-8" />
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <title>Action Controller: Exception caught</title>
  :
```

Files

settings_self-registration_except_disabled.png	62.2 KB	2021-05-10	Ko Nagase