

Redmine - Patch #26709

Use correct http status codes

2017-08-17 01:26 - Pavel Rosický

Status:	New	Start date:	
Priority:	Normal	Due date:	
Assignee:		% Done:	0%
Category:	REST API	Estimated time:	0.00 hour
Target version:	Candidate for next major release		

Description

1/ redmine ignores accept headers and jquery dataType attribute

The Accept request-header field can be used to specify certain media types which are acceptable for the response.

If no Accept header field is present, then it is assumed that the client accepts all media types. If an Accept header field is present, and if the server cannot send a response which is acceptable according to the combined Accept field value, then the server SHOULD send a 406 (not acceptable) response.

<http://api.jquery.com/jQuery.ajax/>

The type of data that you're expecting back from the server. If none is specified, jQuery will try to infer it based on the MIME type of the response (an XML MIME type will yield XML, in 1.4 JSON will yield a JavaScript object, in 1.4 script will execute the script, and anything else will be returned as a string). The available types (and the result passed as the first argument to your success callback)

examples:

```
curl -v -H http://demo.redmine.org/issues.json  
-> 200 + json OK!
```

```
but  
curl -v -H "Accept: application/json" http://demo.redmine.org/issues  
-> 500 no builder for format
```

```
expected (with patch)  
-> 200 + json output
```

in some cases html is returned even if json was requested

2/ 406 error raises exception

```
curl -v http://demo.redmine.org/issues.xxx  
-> 406 + exception ActionController::UnknownFormat
```

```
expected (with patch)  
-> 406 no exception
```

3/ csrf protection - useful to avoid exceptions because of site-scanner bots

```
curl -v -H "Accept: text/javascript" http://demo.redmine.org/issues/new
```

```
-> 422 + exception ActionController::InvalidCrossOriginRequest: Security warning: an embedded <script> tag on another site requested protected JavaScript.
```

expected

```
-> 400 - no exception
```

History

#1 - 2017-09-15 12:25 - Toshi MARUYAMA

Could you add tests?

source:trunk/test/integration

#2 - 2017-09-15 23:18 - Pavel Rosický

- *File api_test.rb.patch added*

attachment:builders.rb.patch without a patch fails:

Failure:

Redmine::ApiTest::ApiTest#test_accept_header_on_error:

Expected response to be a <422: Unprocessable Entity>, but was a <500: Internal Server Error>.

Expected: 422

Actual: 500

Failure:

Redmine::ApiTest::ApiTest#test_accept_header_on_show:

Expected response to be a <200: ok>, but was a <500: Internal Server Error>.

Expected: 200

Actual: 500

attachment:application_controller.rb.patch this isn't worth fixing, it affects only logs so I can't detect it in tests anyway

#3 - 2017-10-13 03:59 - Toshi MARUYAMA

- *Target version set to 4.1.0*

#4 - 2019-06-20 15:45 - Jean-Philippe Lang

- *Target version changed from 4.1.0 to Candidate for next major release*

Fixing status codes and changing the behaviour of the API regarding Accept header are different topics. I think these patches need some deeper review.

#5 - 2019-06-20 16:35 - Pavel Rosický

only <http://www.redmine.org/attachments/19034/builders.rb.patch> is relevant.

this is the redmine way how to access an api, the format is determined as an extension

```
curl -v -H http://demo.redmine.org/issues.json
```

but I think that Accept header should be also supported

```
curl -v -H "Accept: application/json" http://demo.redmine.org/issues
```

this is how rails determines the format

What that says is, "if the client wants HTML or JS in response to this action, just respond as we would have before, but if the client wants XML, return them the list of people in XML format." (Rails determines the desired response format from the HTTP Accept header submitted by the client.)

source <https://api.rubyonrails.org/v5.1/classes/ActionController/MimeResponds.html>

right now

```
curl -v -H "Accept: application/json" http://demo.redmine.org/issues
```

raises an internal server error

if this patch isn't accepted I would propose to change the status to

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Status/406>

instead of 500, what do you think?

<https://blog.bigbinary.com/2010/11/23/mime-type-resolution-in-rails.html>

Files

builders.rb.patch	501 Bytes	2017-08-16	Pavel Rosický
application_controller.rb.patch	1.11 KB	2017-08-16	Pavel Rosický
api_test.rb.patch	1.22 KB	2017-09-15	Pavel Rosický