Redmine - Defect #26296

GET /attachments/download/:id/:filename should deny access

2017-06-28 12:49 - Jess Nielsen

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Attachments	**Estimated time:**	0.00 hour
Target version:			
Resolution:		**Affected version:**	3.3.3

Description

GET /attachments/download/703/android_demo.zip HTTP/1.1
Host: redmine.company.org
Cache-Control: no-cache
X-Redmine-API-Key: INVALID

Returns HTTP Code 200 along with the login page.

It must return HTTP Code 401.
It is an API where login page does not have a relevance.

Redmine version: 3.1.0.stable

History

#1 - 2017-06-28 13:56 - Toshi MARUYAMA

- Status changed from New to Closed

- Resolution set to Invalid

It returns 302.

```
$ curl --head http://localhost:3100/test-3.3-stable/attachments/download/7/new.txt -o /dev/null -w '%{http_cod
e}\n' -s
302
$ curl --head --location http://localhost:3100/test-3.3-stable/attachments/download/7/new.txt -o /dev/null -w
'%{http_code}\n' -s
200
```

#2 - 2017-06-28 14:05 - Jess Nielsen

- Status changed from Closed to Reopened

Toshi MARUYAMA wrote:

> It returns 302.
>
> [...]

1
You are testing on a newer version.
2
It is still not the correct http code to return hence the HTTP response status
code 302 Found is a common way of performing URL redirection.
Signaling a 401 Unauthorized is exactly what is expected due to the fact
that you are not authenticated and you do not want a redirect
when you are accessing the API.

The correct code is 401

401 Unauthorized (RFC 7235)
Similar to 403 Forbidden, but specifically for use when authentication is required and has failed or has not yet been provided.
The response must include a WWW-Authenticate header field containing a challenge applicable to the requested resource.
See Basic access authentication and Digest access authentication.[32]

401 semantically means "unauthenticated",[33] i.e. the user does not have the necessary credentials.
Note: Some sites issue HTTP 401 when an IP address is banned from the website (usually the website domain) and that specific address is refused permission to access a website.

#3 - 2017-06-28 14:45 - Toshi MARUYAMA

- Subject changed from Invalid X-Redmine-API-Key returns http code 200 to GET /attachments/download/:id/:filename should deny access

- Status changed from Reopened to New

Jess Nielsen wrote:

> Toshi MARUYAMA wrote:
>
> > It returns 302.
> >
> > [...]
>
> 1
> You are testing on a newer version.

source:tags/3.1.0/test/integration/api_test/attachments_test.rb#L72

#4 - 2017-06-28 14:45 - Toshi MARUYAMA

- Resolution deleted (Invalid)

#5 - 2017-06-28 14:45 - Toshi MARUYAMA

- Category changed from REST API to Attachments

#6 - 2017-06-28 14:49 - Toshi MARUYAMA

- Affected version changed from 3.1.0 to 3.3.3