Redmine - Defect #33029

API POST requests fail with 422 Can't verify CSRF token authenticity. on 3.4.13, 4.0.6 and 4.1.0

2020-02-20 09:23 - casper nielsen

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	REST API	**Estimated time:**	0.00 hour
Target version:			
Resolution:	Invalid	**Affected version:**	4.1.0

Description

I have been tasked with making our main application work with a newer version of redmine than it did before.
The old one was ancient. Our current one is 3.4.13 in a docker container.

I have tried the latest three versions localhost. The behave the same in this regard:
When I make POST requests using HTTParty or even curl, I get a 422 response code with the message "Can't verify CSRF token authenticity"
This is my request:

```
HTTParty.post(
      "http://localhost:3000/issues.json&key=665f63b1c6a66a3a103207c59241ea9aefbe87c4",
      timeout: @options[:timeout],
      headers: {'Content-Type' => 'application/json'},
      body: somehash.to_json
    )
```

In the redmine source code ApplicationController it calls protect_from_forgery. I don't see any exceptions on this like I would expect with api-requests.
I thought CSRF protection was only meant for posted forms and the like. I may be wrong on that. How would I know what to send as a CSRF-token when making api-requests without prior requests?
I read the API reference. I didn't see anything on the matter.

What am I missing?

Another thing:
I have tried putting the key in the body with the json key "key" and as a header with the key name 'X-Redmine-API-Key' like specified. None of those are accepted it seems.
I can only make it accept the key if passed as a query parameter for some reason.

History

#1 - 2020-02-20 13:27 - Holger Just

- Status changed from New to Needs feedback

It's likely that you have forgotten to activated the support for REST API in your local Redmine installation. Make sure to activate the API in **Administration** -> **Settings** -> **API**.

Does this solve your issue?

#2 - 2020-02-20 13:35 - casper nielsen

Enable REST web service is ticked.

I have resorted to disallowing protect_from_forgery by mounting and overwriting the additional_environment.rb containing that setting. This is acceptable but not optimal.
It's an internal system behind a firewall, so I'm not worried about that.

I do not verify the ssl certificate either. This is just until we get a proper certificate on that server. But I doubt that should cause this.

Am I supposed to provide a CSRF-token with an api post request?

#3 - 2022-02-08 17:18 - Arkady Marchenko

- File Screenshot 2022-02-08 231555.png added

- File Screenshot 2022-02-08 231705.png added

Today faced same issue, trying create news with Postman
POST - https://server.domain.com/projects/private/news.json&key=XXXXXXXXXXXXXXXXXXX
Content-Type: application/json

```
{
    "news": {
        "title": "NewsJsonApiTest",
        "summary": "News JSON-API Test",
        "description": "This is the description"
    }
}
```

Keep returning 422 Unprocessable entity (Screenshot 2022-02-08 231555)
And in the server log I found that error (Screenshot 2022-02-08 231705)

#4 - 2022-02-08 18:02 - Pavel Rosický

you have an error in the URL, it should be
https://server.domain.com/projects/private/news.json?key=XXXXXXXXXXXXXXXXXXX
instead of
https://server.domain.com/projects/private/news.json&key=XXXXXXXXXXXXXXXXXXX

also, note that news have Rest-API since Redmine 4.1, it won't work on previous versions https://redmine.org/issues/13468

#5 - 2022-03-22 07:38 - Go MAEDA

- Status changed from Needs feedback to Closed

- Resolution set to Invalid

#6 - 2022-06-23 12:45 - Yasuhiro Oguro

Today faced same issue, (on version 5.0.2) tring webhook with GitLab
https://server.domain.com/sys/fetch_changesets?key=pKOYjqfbuQpHtfML8b1i&id=8

Keep returning 422 Unprocessable entity

You have endpoint as " /sys/ ".
Can you disable CSRF on it?
Or add settings for "X-Gitlab-Token" header handing with OAuth2.

#7 - 2022-06-23 18:28 - Holger Just

The sys endpoint requires a different key (not your user's API key) and must be enabled separately from the "normal" REST API. You can enable this at **Admin** -> **Settings** -> **Repositories** -> **Enable WS for repository management** and configure the static key below that.

The httpr eply you got there is entirely unrelated to the CSRF validation.

#8 - 2022-08-09 07:43 - r okui

I am facing the same issue(5.0.0.stable).
GitLab's WebHook POSTs to /sys/fetch_changesets/key=...
There is no problem if you GET the same URL with a browser, but POST will result in a 422 error.

#9 - 2022-08-09 08:25 - Go MAEDA

The report #33029#note-6 by Yasuhiro Oguro and #33029#note-8 are different from this issue and are specific to Redmine 5.0, due to #36317.

I have opened a new issue #37562.

Files

Screenshot 2022-02-08 231555.png	50.6 KB	2022-02-08	Arkady Marchenko
Screenshot 2022-02-08 231705.png	21.1 KB	2022-02-08	Arkady Marchenko