Redmine - Feature #25140
[API] authentication with JSON Web Tokens

2017-02-21 15:51 - Vincent Robert

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

Description

Currently, the API only accepts two ways to authenticate users:
- HTTP Basic authentication (logins and passwords are sent with each request)
- API key

We could secure this process and make it easier to use.
Allowing JWT (JSON web token) authentication could be a great improvement.

History

#1 - 2017-02-22 13:36 - Serguei Okladnikov

Vincent Robert wrote:

> *We could secure this process and make it easier to use.*

Whoud you like to secure api calls?
Or You want to rewrite front panel working process too?

#2 - 2017-03-06 10:33 - Vincent Robert

Hi Serguei,
I am just talking about API calls here. I could work on this feature, but I would like to know the opinion of core contributors first.
Thanks

#3 - 2018-05-08 14:26 - Jaap de Haan

Good point. I would go so far and also allow this not only for API calls but also for normal UI as well (enabling SSO use cases via JWT for example)

#4 - 2018-08-01 08:36 - Enziin System

I think JWT is necessary.

Using the API key will require more actions, which is to force the user to create a key, then copy the API key into their application.

JWT authentication is simply using username/password

When we embed Redmine API into the mobile app, then JWT must be used.

If you use Redmine core in multi-million users application, then each request from the client on the mobile or the desktop and it will cause Redmine to query the Token table in the DB.

It is not effective and it will overload.