redmineorg-copy202205 - Vote #77600

Each HTTP HEAD request renders views and tries to login?

2022/05/09 18:00 - Admin Redmine

ステータス:	Needs feedback	**開始日:**	2022/05/09
優先度:	高め	**期日:**	
担当者:		**進捗率:**	0%
カテゴリ:	Security_51	**予定工数:**	0.00時間
対象バージョン:		**作業時間:**	0.00時間
Redmineorg_URL:	https://www.redmine.org/issues/23240	**status_id:**	10
category_id:	51	**tracker_id:**	1
version_id:	0	**plus1:**	0
issue_org_id:	23240	**affected_version:**	
author_id:	48494	**closed_on:**	
assigned_to_id:	0	**affected_version_id:**	118
comments:	2		

説明

A HTTP HEAD request is supposed to only return the HEADERS of a site to check for availablity or expiry dates and such.
I think it's not supposed to render views and load plugins in order to do so.
But with Redmine 3.2 it does!

This is from my redmine logfile where xxx.xxx.xxx.xxx is a GitLab server checking for ceonnection-availability:

```
Started HEAD "/projects/PROJECT-ID/" for xxx.xxx.xxx.xxx at 2016-07-05 10:24:49 +0200
Processing by ProjectsController#show as */*
  Parameters: {"id"=>"PROJECT-ID"}
  Current user: anonymous
Redirected to https://my-redmine-instance/login?back_url=https%3A%2F%2Fmy-redmine-instance%2Fprojects%2FPROJECT-ID
Filter chain halted as :check_if_login_required rendered or redirected
Completed 302 Found in 4ms (ActiveRecord: 0.5ms)
Started HEAD "login?back_url=https%3A%2F%2Fmy-redmine-instance%2Fprojects%2FPROJECT-ID" for xxx.xxx.xxx.xxx at 2016-0
7-05 10:24:49 +0200
Processing by AccountController#login as */*
  Parameters: {"back_url"=>"https://my-redmine-instance/projects/PROJECT-ID"}
  Current user: anonymous
Failed login for '' from xxx.xxx.xxx.xxx at 2016-07-05 08:24:49 UTC
Completed 200 OK in 356ms (Views: 323.6ms | ActiveRecord: 2.9ms)
```

It's not only loading views, but also the AccountController tries to perform a login?!
I'm not sure that is correct behaviour...

Cheers,
Tobias

journals

> I think it's not supposed to render views and load plugins in order to do so.

The response to a HEAD request is supposed to be the same as the corresponding GET request but without including the response body. There is no expectation on how the server should behave internally to do so.

As far as I can see, this is what happens (even if the application renders the view, only the response headers are sent to the client). If the response to the GET request is a redirect to /login then the response the HEAD request should be the same.

Please, explain how you consider this as a security issue.

Hi Jean-Philippe,

thanks for your explanations.

Sure, the response contains only the HEADER information, but I wasn't sure about whether this was affecting security, whether the redirects and view rendering should happen or not. Still I feel a bit nervous about all the action taking place when sending a HEAD request, but I probably don't know enough Ruby on Rails to draw the perfect picture for me...
anyways, If you think this is the correct way I'm sorry for having bothered you.

Cheers,

Tobias

履歴

#1 - 2022/05/10 17:07 - Admin Redmine

- カテゴリ を Security_51 にセット