Redmine - Defect #40121

InvalidCrossOriginRequest exception raised by automated pentests or malicous user

2024-01-24 12:58 - Liane Hampe

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Resolution:		**Affected version:**	5.1.1

Description

Problem

When an automated pentest or a malicous user requests for example:

```
https://<your-domain>.tld/projects/autocomplete.js
```

the following exception will be raised:

```
An ActionController::InvalidCrossOriginRequest occurred in projects#autocomplete:

  Security warning: an embedded <script> tag on another site requested protected JavaScript. If yo
u know what you're doing, go ahead and disable forgery protection on this action to permit cross-o
rigin JavaScript embedding.
```

Note: Any other url containing *.js will raise this exception.

All currently supported versions of Redmine are affected.

Solution

The solution is to rescue from ActionController::InvalidCrossOriginRequest.

The attached patch file fix_invalid_cross_origin_request_exception.patch gives an example how to do that. A test is also included.

History

#1 - 2024-01-26 15:54 - Holger Just

While this exception is raised internally, it is not actually visible as a 500 to external users. Instead, the exception is rescued by the ActionDispatch::ExceptionWrapper middleware which returns a generic HTTP 422 response to the client (which is also the more correct status than 403).

We have a similar patch in Planio for quite some time which has evolved a bit now. I had it on my backlog to prepare it for redmine.org...

If I remember correctly, this patch alone may also not fully sufficient in all cases, as it can possibly cause double-render errors (depending on the Rails version). These may result because Rails only checks the response type after rendering the response (i.e. it can only check for js responses this after the controller has decided that it actually wants to return js). As the controller's response was already rendered, rendering the error message for the rescued exception again can cause a DoubleRender error. I might have to further dig into this though to fully confirm this.

#2 - 2024-01-29 15:03 - Liane Hampe

Thank you for your feedback, Holger Just!

I run Redmine with an exception notifier which comes as middleware (gem 'exception_notification'). It notifies me about the ActionController::InvalidCrossOriginRequest exception. I did not test the behavior without the gem.

Meanwhile, I can confirm that running Redmine without the notifier would only show a white screen to the user in production. In development mode it shows the typical error page.

My patch will also only show a white screen due to the double render error which will occur when a html page should be rendered.

Changing the HTTP status to 422 is fine for me. But with this further information at hand the patch would not add an improvement to a plain redmine installation.

Whe you already have something what goes beyond, I would be happy when you would share it.

Files

fix_invalid_cross_origin_request_exception.patch	1.75 KB	2024-01-24	Liane Hampe