Redmine - Defect #8166

Firebug can enable a disabled field and thus allow a change

2011-04-15 18:55 - Charles Monteiro

Status:	Closed	**Start date:**	2011-04-15
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Resolution:	Invalid	**Affected version:**	

Description

A developer of ours proved that he could use Firebug to enable a field that the system had disabled. In this case, the estimated time field and enter a new value. Thus bypassing the system's constraints.

I don't understand what is fully exposed to a tool like Firebug. It seems to me that the individual would have to be logged in to the system and even though he would be able to enable the field and submit the update that at the very least that update would be tracked as part of the issue's history.

Anyhow, of course, we would prefer that the capability was not there but this might just part of the nature of the beast i.e. a JS driven app.

Are there any other security risks that a tool like Firebug opens up ?

thanks in advance,

-Charles

History

#1 - 2011-04-15 19:04 - Jean-Philippe Lang

Where was this disabled 'estimated time' field? On a parent issue?

#2 - 2011-04-15 19:05 - Jean-Philippe Lang

And please give your Redmine version.

#3 - 2011-04-15 19:14 - Charles Monteiro

current version: Redmine 1.0.4.stable (MySQL)

#4 - 2011-04-15 19:17 - Charles Monteiro

sorry, yes it is.

#5 - 2011-04-15 19:34 - Jean-Philippe Lang

I've just had a look at the 1.0.4 code and it should not allow the change. I'll see if it can reproduce.
Do you have any plugins installed?

#6 - 2011-04-15 19:40 - Jean-Philippe Lang

I can not reproduce with current trunk. The value submitted after enabling the field is ignored.

#7 - 2011-04-15 19:53 - Charles Monteiro

thank you and sorry for the waste of time, the developer did not include that last piece of info.

#8 - 2011-04-17 17:20 - Jean-Philippe Lang

Charles Monteiro wrote:

> thank you and sorry for the waste of time, the developer did not include that last piece of info.

What is "that last piece of info"?

#9 - 2011-04-18 05:19 - Charles Monteiro

That the "value submitted after enabling the field is ignored". In other words he stopped short and just reported that the firebug was able to enable a disabled field and that subsequently the value of the field could be changed. I have not tested the impact of this in different scenarios but in this case there is no real impact as you have pointed out.

To be complete I also should answer your question, no I don't have any plugins installed although that is also irrelevant at this point.

thank you for your attention to this.

#10 - 2011-04-18 09:57 - Etienne Massip

Could you ask him for more details ?

#11 - 2011-04-18 18:03 - Charles Monteiro

I'm not sure what further detail you want. He simply used firebug to enable a disabled field, he then changed the value but never submitted the form. Had he done so he would have realized that his change would not be submitted.

#12 - 2011-04-18 18:08 - Etienne Massip

- Status changed from New to Closed

- Resolution set to Invalid

Ok, sorry, I misunderstood, thought he eventually submitted the value.