Nirva Application Platform - Feature #68

HTTP command filter for security.

07/11/2012 11:50 AM - Pierre Marc

Status:	Closed	**Start date:**	07/11/2012
Priority:	Normal	**Due date:**	
Assignee:	Pierre Marc	**% Done:**	100%
Category:	Application Platform	**Estimated time:**	0.00 hour
Target version:	4.7.005		
Operating System:	Any	**Tested:**	Yes
Version:			

Description

Many Nirva commands are directly accessible from an HTTP client (web browser for example). Even if sensible commands are not available from web and the server files are not accessible, this can be a security issue. We suggest to add a filter to authorise only some commands from HTTP clients. In a first time this filter could be a very simple one that authorises only MISC:NOP and OBJECT:GET commands from distant HTTP clients with a possibility to enable/disable the filter by a security permission. This filter is at application level.

History

#1 - 07/11/2012 12:26 PM - Lionel Martin

I suppose you mean that the filter would forbid any SYSTEM:* command except for SYSTEM:MISC:NOP and SYSTEM:OBJECT:GET.

In deed, I think that all services should implement their own web security (easy thing to add with a simple check for current services), especially to allow Renderers for web access.

Otherwise, I vote for this feature, that will greatly help us control the operations made to our application.

#2 - 08/10/2012 10:12 AM - Pierre Marc

- Status changed from New to In Progress

#3 - 09/17/2012 03:48 PM - Pierre Marc

- Target version set to 4.7.005

- % Done changed from 0 to 100

- Tested changed from No to Yes

#4 - 09/17/2012 03:48 PM - Pierre Marc

- Status changed from In Progress to Closed