

Monarch - Bug #953

lock down security issues

01/15/2003 02:59 PM - Chad Berkley

Status:	Resolved	Start date:	01/15/2003
Priority:	Immediate	Due date:	
Assignee:	Chad Berkley	% Done:	0%
Category:	monarch - general bugs	Estimated time:	0.00 hour
Target version:	2.0.0Alpha2	Spent time:	0.00 hour
Bugzilla-Id:	953		

Description

monarch is able to execute arbitrary code on so the security issues need to be looked into. at a minimum, we need to make sure that absolute paths are not allowed in step code so that the filesystem can't be accessed outside the temp directory. also need to make sure that certain commands are not executed in different plugins. and example of this is the xterm command in sas that gives a user a command line terminal into the system. the original perl script that was monarch looked for any x* commands and threw an exception if they existed in submitted code.

History

#1 - 02/06/2003 02:36 PM - Matt Jones

Add a filter interface to AEPlugin that can be implented to filter out insecure pipelines and produce an exception when one is encountered. Use the perl SAS X command to initially try it out.

#2 - 03/17/2003 11:36 AM - Chad Berkley

There is now an interface in the AEPlugin code that allows each plugin to implement a filter for illegal code. I've implemented the filter for SAS and Matlab. It is the responsibility of the plugin itself to make sure it is not executing any dangerous code. see SASPlugin.checkForIllegalCode() to see an example of the filter

#3 - 03/27/2013 02:15 PM - Redmine Admin

Original Bugzilla ID was 953