User Interface - Feature #2342

fix cross-domain cookie for web client on remote launch

07/22/2014 02:06 PM - Marius Gligor

Status:	Closed	**Start date:**	07/22/2014
Priority:	Normal	**Due date:**	
Assignee:	Marius Gligor	**% Done:**	100%
Category:		**Estimated time:**	4.00 hours
Target version:	GUI Support for a Complex ADM2 App		
billable:	No	**vendor_id:**	GCD

Description

Related issues:

Related to User Interface - Feature #1811: implement the AJAX client driver	**Closed**	**11/01/2013**	**03/06/2014**
Related to User Interface - Feature #2308: remote client launch	**Closed**		

History

#1 - 07/23/2014 01:50 AM - Marius Gligor

- Status changed from New to WIP

#2 - 07/23/2014 10:04 AM - Marius Gligor

- % Done changed from 0 to 90

- File mag_upd20140723b.zip added

- Status changed from WIP to Review

When a HTTP redirection is done the GET method is used. A HTTP GET request contains HTTP headers and an URL. No body content is send to server.

In order to send the authorization token we have two ways:

1. Using a HTTP header. On redirection using GET method is not possible to set a header value except setting a cookie which finally is send as a header value by web browser. Cookies does not work over cross domains.

2. Using a query string parameter in URL. In this case the redirection URL looks like:
https://domain:port/?param=<token value> and it works over cross domains.
The problem here is that query string token is visible in browser address bar because is a part of the URL on redirection.
But using the token only once at the redirection time the risk to be stolen and used by another person is reduced, see my implementation bellow.

My changes follow the second way to send the token. The token is send as a query parameter when redirection is made. On the redirected site the token is compared with the expected value. If match a cookie is set using a new random generated token and the first token is no longer valid. If a new request is coming having the first token as a query parameter and the cookie was already set the access is denied. Basically for security reasons the initial token can be used only once when redirection is made.

The cookie is used when the user force a page reload from browser which means also a HTTP GET request and we have to send an authorization token from browser to server. We have again two options HTTP headers or query string. Because the browser have to send token the cookie is used which is send as a HTTP header.
Using a query string is less secure because the query string is always visible in the browser address bar.

#3 - 07/23/2014 10:45 AM - Marius Gligor

- File regression_test.txt added

Here are the results of my regression test. CTRL-C test took 1 hour and 8 minutes and the errors are false negative.
Regarding the MAIN part I'm not sure if the test is completely done.

A severe error occur at one moment:

```
** Shared variable curFac has not yet been created. (392)
```

Comparing results with other results from previous regression tests seems to be completed.
Looking inside the server log I found:

```
07/23/2014 07:05:58 EDT] (com.goldencode.p2j.persist.trigger.DatabaseTriggerManager:INFO) DatabaseTriggerManag
er registered with TransactionManager.
[07/23/2014 07:05:59 EDT] (com.goldencode.p2j.persist.lock.InMemoryLockManager:WARNING) [0000018F:00000506:sym
an] --> local/majic/primary:  cleaning up 2 leaked record lock(s) for exiting context ({purchase_order_item:T=
SHARE [syman:0000018F], temp_sum:T=SHARE [syman:0000018F syman:0000018E deweyw:0000019A deweyw:00000198 syman:
00000189 syman:00000186 syman:00000199]})
[07/23/2014 07:06:00 EDT] (com.goldencode.p2j.persist.lock.InMemoryLockManager:WARNING) [00000198:000004FF:dew
eyw] --> local/majic/primary:  cleaning up 1 leaked record lock(s) for exiting context ({temp_sum:T=SHARE [sym
an:0000018E deweyw:0000019A deweyw:00000198 syman:00000189 syman:00000186 syman:00000199]})
[07/23/2014 07:06:02 EDT] (ErrorManager:SEVERE) {0000019A:00000505:deweyw} ** Shared variable curFac has not y
et been created. (392)
[07/23/2014 07:06:02 EDT] (com.goldencode.p2j.util.ControlFlowOps$ExternalProgramResolver:WARNING) Unable to r
esolve external program.
com.goldencode.p2j.util.ErrorConditionException: ** Shared variable curFac has not yet been created. (392)
        at com.goldencode.p2j.util.ErrorManager.recordOrThrowError(ErrorManager.java:1041)
        at com.goldencode.p2j.util.ErrorManager.recordOrThrowError(ErrorManager.java:934)
        at com.goldencode.p2j.util.ErrorManager.recordOrThrowError(ErrorManager.java:913)
        at com.goldencode.p2j.util.SharedVariableManager.errorHelper(SharedVariableManager.java:766)
        at com.goldencode.p2j.util.SharedVariableManager.lookupWorker(SharedVariableManager.java:742)
        at com.goldencode.p2j.util.SharedVariableManager.lookupVariable(SharedVariableManager.java:337)
        at aero.timco.majic.po.PocoT.<init>(PocoT.java:121)
        at sun.reflect.NativeConstructorAccessorImpl.newInstance0(Native Method)
        at sun.reflect.NativeConstructorAccessorImpl.newInstance(NativeConstructorAccessorImpl.java:57)
        at sun.reflect.DelegatingConstructorAccessorImpl.newInstance(DelegatingConstructorAccessorImpl.java:45
)
        at java.lang.reflect.Constructor.newInstance(Constructor.java:526)
        at java.lang.Class.newInstance(Class.java:374)
```

I started the tests from the beginning with a Majic conversion.
Could be a conversion issue? Should we restart the MAIN part?
Please let me know.

#4 - 07/23/2014 10:50 AM - Marius Gligor

Sorry by mistake I did the post here instead on #2308

#5 - 07/23/2014 10:54 AM - Marius Gligor

- File deleted (regression_test.txt)

#6 - 07/23/2014 11:08 AM - Greg Shah

Code Review 0723b

The changes are fine except for one minor code standards issue. In WebHandler, the public static members should be placed before the private static members.

> The problem here is that query string token is visible in browser address bar because is a part of the URL on redirection.

Yes, this is not optimal. But I think your choice is the best one given the circumstances and limitations of redirection.

The URL may be available in the browser's history. This means it may also be available to plugins, extensions and will probably be stored on the client's hard disk.

On the other hand, it is only useful for a single GET request so I think the danger is limited.

Some questions:

1. Does the query parameter get cleared from the URL when the response is loaded?

2. Have you tested this change in the range of browsers and on both local and remote redirection cases?

#7 - 07/23/2014 11:54 AM - Marius Gligor

1. Yes the query parameter is cleared after form URL when the response is loaded.

2. I tested with Chrome, Firefox on Linux and with Chrome, Firefox, Opera, IE on Windows.
So far I tested only on the same machine using localhost and redirect on an IP like 192.168.1.10
Basically is the same as cross site redirection

3. I tested now running the P2J server on Windows OS and a broker on Linux OS.
Than I tried to connect form Linux to Windows on the main page and it works.
Unfortunately on redirection I found a bug in the broker code regarding the web server address.
When the web client is spawned the address of the embedded server should be the address on which the broker runs not the P2J server address.
The parameter client:web:host should contains the address of the spawned client not the server address.
I have to check and fix this bug and I'll be back with my conclusions.

#8 - 07/23/2014 01:06 PM - Marius Gligor

- File mag_upd20140723c.zip added

WebHandler, the public static members are placed before the private static members.

#9 - 07/23/2014 01:23 PM - Greg Shah

Code Review 0723c

The change looks good. If I understand correctly, this work is done and is tested sufficiently.

You can check it in and distribute it. No regression testing is needed.

#10 - 07/23/2014 01:30 PM - Marius Gligor

Yes this issue is done. I tested also using remote launch using brokers and works.
I have to do the commit, distribute and post the revision number.

#11 - 07/23/2014 01:41 PM - Marius Gligor

- Estimated time set to 4.00

- % Done changed from 90 to 100

no regression tests are mandatory for this changes.
committed revision 10579

#12 - 07/23/2014 02:09 PM - Greg Shah

- Target version set to Milestone 12

- Status changed from Review to Closed

#13 - 11/16/2016 12:13 PM - Greg Shah

- Target version changed from Milestone 12 to GUI Support for a Complex ADM2 App

Files

mag_upd20140723b.zip	6.06 KB	07/23/2014	Marius Gligor
mag_upd20140723c.zip	6.05 KB	07/23/2014	Marius Gligor