Runtime Infrastructure - Feature #7418

assess the security of the Jetty web server

06/08/2023 06:45 AM - Constantin Asofiei

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
billable:	No	**version:**	
vendor_id:	GCD		

Description

History

#1 - 06/08/2023 06:54 AM - Constantin Asofiei

The main internet-exposed point of FWD is the Jetty web server. This includes the web server running on the FWD server, and the one running on the FWD client (after logging in).

If Jetty can be exploited (somehow) and gain access to the machine where the FWD client started the web browser, then if this same machine is used for the FWD server, it will expose it. As of trunk rev 14616, FWD is using Jetty version 9.4.22.v20191022.

A first point should be to document all URLs served by Jetty. This includes:

- the Admin Console written in GWT (/admin).
- the /chui, /web, and /embedded URLs for FWD clients
- Hynek, is sheet.war starting another web server? If so, what URL is it using?
- the URLs opened via OPEN-MIME-RESOURCE, with input from the user
- HTML-BROWSER resource, with URLs calculated by the application and/or input from the user

Please add if I missed anything. I think we should document also the JS libraries used in FWD, and in what part (the login page or after login, admin, etc).

#2 - 06/08/2023 07:59 AM - Hynek Cihlar

Constantin Asofiei wrote:

> - Hynek, is sheet.war starting another web server? If so, what URL is it using?

No, it doesn't start new server. It uses GuiWebDriver.websrv by adding new handler to it with the method GuiWebDriver.addHandler.

The exposed endpoints are: https://fwdhost/sheet/&lt;widgetId> and wss://fwdhost/sheet/<widgetId>/push.

#3 - 06/08/2023 08:04 AM - Hynek Cihlar

I think we should also document the full stack for each exposed endpoint including versions. For example for Keikai the enpoints are handled by Servlet API, on top of that is ZK framework (with zul page templating and zk web components) and on top of that is Keikai.

#4 - 06/08/2023 08:09 AM - Greg Shah

And we need to differentiate between FWD server jetty and FWD client jetty.