Shrine-proxy.war Exploit Fix (v1.25.4 and prior)

This tutorial is intended to provide instructions for applying a configuration-based fix to address a security vulnerability in the SHRINE proxy subsystem.

1. Start tomcat with shrine already installed correctly, started at least once, and can at minimum show ontology terms. shrine-proxy.war must be expanded in tomcat's webapps directory
2. Stop tomcat
3. Edit tomcat/webapps/shrine-proxy/WEB-INF/classes/shrine-proxy-acl.xml to only whitelist URLs for your own shrine (tomcat) host and i2b2 (jboss) host. The following example uses one of our internal QA nodes called shrine-qa3.catalyst:
    a. Remove the following lines:

    ```
    <host>https://</host>
    <host>http://</host>
    ```

    b. Do not add anything to the blacklist section.
    c. Include entries that specify localhost, fully-qualified host names and IP addresses for both the shrine node and i2b2 node as accessed by your tomcat. Here is an example:

    ```
    <lists>
    <whitelist>
           <host>https://shrine-qa3.catalyst:6443</host>
           <host>https://localhost:6443</host>
           <host>https://10.118.12.40:6443</host>
           <host>http://shrine-qa3-i2b2.catalyst:9090</host>
           <host>http://10.118.12.60:9090</host>
    </whitelist>
    </lists>
    ```

4. Start tomcat again. After tomcat has completed its startup confirm the configuration by running a test query. If it does not work, then you will see messages in tomcat/logs/proxy.log that look like this:

    Sample proxy error message

    ```
    2019-Jan-02-16:54:54.480 ERROR [SHRINE][ShrineProxyServlet][http-nio-6443-exec-5] ProxyServlet error:

    net.shrine.proxy.ShrineMessageFormatException: redirectURL not in white list or is in black list:
    http://shrine-qa2-i2b2.catalyst:9090/i2b2/services/PMService/getServices
            at net.shrine.proxy.DefaultShrineProxy.redirect(ShrineProxy.scala:91)
            at net.shrine.proxy.ShrineProxyServlet.doPost(ShrineProxyServlet.scala:56)
            at javax.servlet.http.HttpServlet.service(HttpServlet.java:648)
    ```

    If you encounter an error, add the correct URL(s) into the whitelist and try again.

    5. Please let your hub administrators know that you have made a configuration change so that we can verify from the hub.