Open Medical Record System

OpenMRS
MEDICAL RECORD SYSTEM

ČVUT FEL - OSP

Kamil Procházka

Work Assignment

- „Introductory Tickets“

- Lack of HTTPOnly flag on JSESSIONID cookies
  - Securing client HTTP Cookie, exacly user JSESSIONID which is used for user session

- HSODAO.saveObject should set auditable fields before serializing
  - Propagation of auditable object attributes before persistence

- Log Errors that are being captured on screen
  - Propagate error messages from UI framework to server log

Lack of HTTPOnly flag on JSESSIONID cookies

- Security risk caused by exploit of user session id (JSESSIONID) by script (https://www.owasp.org/index.php/HttpOnly)

- OpenMRS build upon Servlet 2.5 Specification
- Portable solution would be migration to Servlet 3.0 specification which provides mechanism for setting this directly in web.xml file

```
<web-app>
        <session-config>
         <cookie-config>
<!-- Specifies whether any session tracking cookies created by this web application will be marked as HttpOnly -->
                     <http-only>true</http-only>
         </cookie-config>
        </session-config>
</web-app>
```

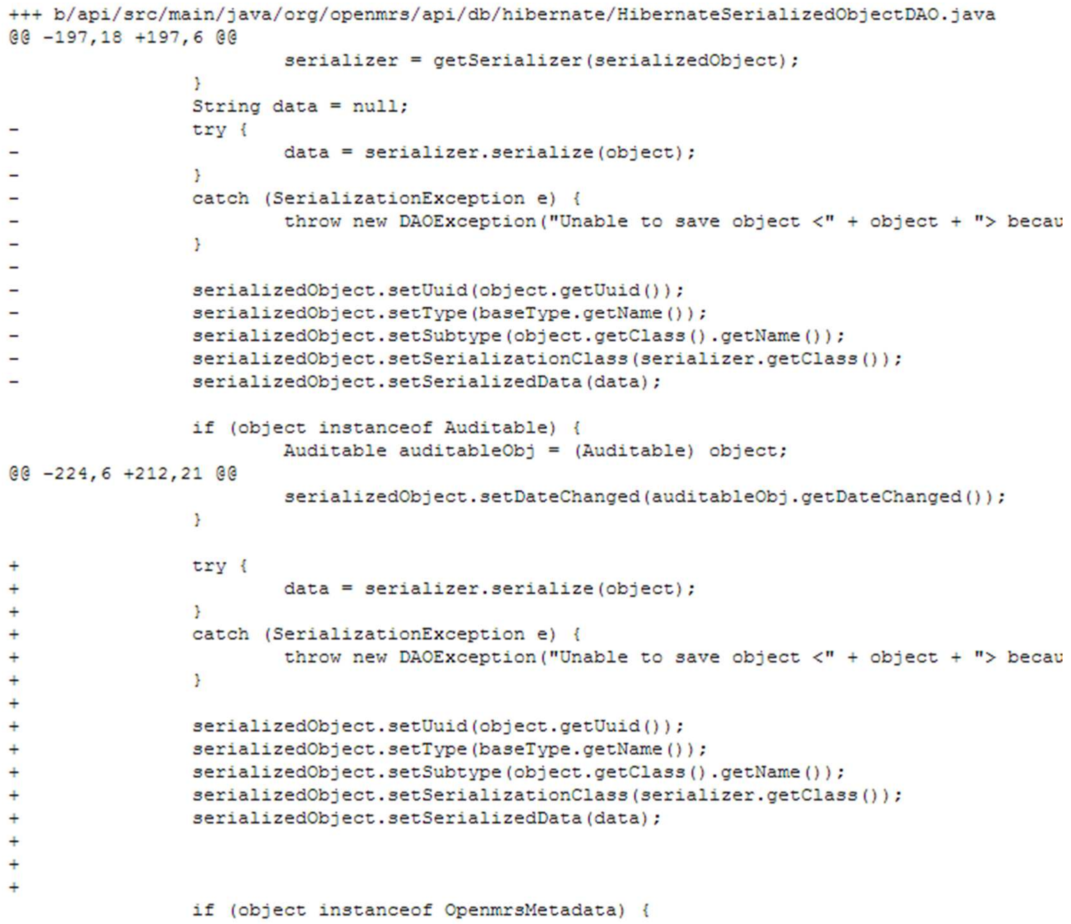
- Acceptable solution without any coding is to is configuration of default used application serveru (Tomcat 6,7)
  - Tomcat 6 (http://tomcat.apache.org/tomcat-6.0-doc/config/context.html)
  - Tomcat 7 (http://tomcat.apache.org/migration-7.html) = default setting

HSODAO.saveObject should set auditable fields before serializing

- In HibernateSerializedObjectDAO.saveObject(T object, OpenmrsSerializer serializer)), the Auditable (creator, dateCreated, changedBy, dateChanged) fields should be set before calling serializer.serialize(definition); instead of after serialization.

Solution is proposed as a part of assignment. Proposed change moves block of code which takes care of propagation of serializable object

With respect of test migration and that the code is deprecated in favor of never API and application version, this task will not be merged and will be closed based on IRC communication



```
+++ b/api/src/main/java/org/openmrs/api/db/hibernate/HibernateSerializedObjectDAO.java
@@ -197,18 +197,6 @@
                        serializer = getSerializer(serializedObject);
                }
                String data = null;
-               try {
-                       data = serializer.serialize(object);
-               }
-               catch (SerializationException e) {
-                       throw new DAOException("Unable to save object <" + object + "> becau
-               }
-
-               serializedObject.setUuid(object.getUuid());
-               serializedObject.setType(baseType.getName());
-               serializedObject.setSubtype(object.getClass().getName());
-               serializedObject.setSerializationClass(serializer.getClass());
-               serializedObject.setSerializedData(data);

                if (object instanceof Auditable) {
                        Auditable auditableObj = (Auditable) object;
@@ -224,6 +212,21 @@
                        serializedObject.setDateChanged(auditableObj.getDateChanged());
                }

+               try {
+                       data = serializer.serialize(object);
+               }
+               catch (SerializationException e) {
+                       throw new DAOException("Unable to save object <" + object + "> becau
+               }
+
+               serializedObject.setUuid(object.getUuid());
+               serializedObject.setType(baseType.getName());
+               serializedObject.setSubtype(object.getClass().getName());
+               serializedObject.setSerializationClass(serializer.getClass());
+               serializedObject.setSerializedData(data);
+
+
+
                if (object instanceof OpenmrsMetadata) {
```

Results

- Community is very friendly and open for new contributors
  - I contributed to this project some time ago (not part of my school assignment)
- JIRA communication might be a problem, preferred way is to use IRC, or mailing list
- Underestimated project plan from my side which lead to unfinished issue from assignment ...