Open Medical Record System

ČVUT FEL - OSP

Kamil Procházka

Zadání práce

- „Introductory Tickets“

- Lack of HTTPOnly flag on JSESSIONID cookies
  - Zabezpečení HTTP Cookie identifikátoru uživatelské session

- HSODAO.saveObject should set auditable fields before serializing
  - Propagace auditovaných položek před uložením záznamu

- Log Errors that are being captured on screen
  - Propagace errorových hlášek do logu serveru v UI

Lack of HTTPOnly flag on JSESSIONID cookies

- Bezpečnostní riziko zneužití identifikátoru JSESSIONID klientským skriptem (https://www.owasp.org/index.php/HttpOnly)

- OpenMRS staví nad specifikací Servlet 2.5
- Přenositelným řešením by byla migrace na specifikaci Servlet 3.0, která umožňuje nastavení tohoto atributu přímo ve web.xml

```
<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>
```

- Přijatelné řešení, bez zbytečného psaní vlastního kódu je konfigurace používaného aplikačního 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) = využívá defaultně

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.

Řešení je součástí zadání, kdy se jedná o přesun bloku kódu stararající se o propagaci atributů do serializovaného objektu.

S ohledem na migraci testů a aktuální nevyužívání kódu je to waitting stavu po IRC dohodě.

```
+++ 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) {
```

Zhodnocení

- Komunita je přátelská a otevřená
  - již dříve jsem přispíval
- Může být problém delší odezva členu, nejlepší komunikovat přímo přes IRC, či mailing list

- Nepovedl se project management na mé straně ...