



Java EE Security Explained - examples lab

MUNI, Brno 2013

JBoss by Red Hat

Peter Škopek, pskopek@redhat.com, twitter: @pskopek

Mar 25, 2013

Abstract

This lecture will guide you through various aspects of security in Java Enterprise Edition Applications. It will start with plain JAAS and continue with JEE security concepts and explanation of their usage in your application. Next comes JAAS and its usage in JBoss AS7. Then we will finish with login modules in JBoss AS7

Agenda

1 Introduction

2 Examples

- JAAS
- JEE web container examples



Section 1

Introduction

Project

- Project location: <https://github.com/qa/pv243>
- Directory: lesson04-security
- tags beginning security-01
- download: <http://download.jboss.org/jbossas/7.1/jboss-as-7.1.1.Final/jboss-as-7.1.1.Final.zip>



Section 2

Examples

Task 1: Plain JAAS Example

- 1 Explore all parts of jaas-example project (lesson04-security/jaas-example/)
- 2 Run example under JBDS (use `-Djava.security.auth.login.config==sample_jaas.config` as VM parameter)
- 3 Modify “Sample” JAAS configuration which will include `sample.module.CardLoginModule` with following characteristics:
 - Try to use “card” authentication if it fails use provided `SampleLoginModule`.
 - “Card” authentication can fail and `SampleLoginModule` has to be enough to authenticate user.
 - Use provided `sample.module.CardLoginModule` class.

Hint: change login `MyCallbackHandler` to include “Card” login module callback. Change config file.

Task 2: Secure access to servlet using annotations

- Secure SecuredServlet using annotations (programmatic way) using security domain “test” configured with UsersRoles login module.
- Only user with role “gooduser” can have access to it using all HTTP methods (verbs).
- The new domain has to use users.properties and roles.properties located at WEB-INF/classes directory of webapp01.war.
- **Hint:** modify manually standalone/config/standalone.xml to add desired domain.

Task 3: Secure static content of the web application

- Secure static content of the webapp01 at `/static/secured/`. All pages there must be readable for “superuser” only.
- All pages located at `/static/` should be readable by any authenticated user.
- SecuredServlet from previous task has to stay secured as it was.
- **Hint:** For details see Java Servlet 3.0 specification.

Task 4: Override security annotations using deployment descriptor

- Modify security constraint attached to the SecuredServlet so that only members of “superuser” group can run it.
- Act as application assembler, therefore you are not allowed to change code of `web.security.SecuredServlet.java`.
- Still using `webapp01` project.
- **Hint:** the hit is already show at title of this task. You have to define servlet in `web.xml`.

Task 5: Identity propagation

- Application has added application logic layer in form of EJB called TestBean.
- Modify security settings using annotations to allow users in roles “gooduser” and “superuser” to SecuredServlet.
- Set security constraints on each method TestBean method to allow users in following roles to call them.
echo - all users, goodUserEcho - “gooduser” members,
superUserEcho - “superuser” members
- **Hint:** Do not forget to add SecurityDomain to TestBean.

Task 6: Programmatic Security

- At the beginning of doGet SecuredServlet method display following information:
 - remote user name
 - user principal
 - information if the user is in “superuser” role
- Create new method in TestBean which displays following information:
 - user principal
 - information if the user is in “gooduser” role
- Call the method at the end of SecuredServlet doGet method.
- **Hint:** Use @Resource annotation and HttpServletRequest.