koelnerwasser.de
Java, .Net and other parts of my life

« Ausflug ins “Ländle” Programme immer im Vordergrund halten »

HowTo renew the Session id in Tomcat or JBoss after a login

...or: HowTo prevent a session fixation attack. Most Security Papers (eg. the Security White Paper of the BSI) suggest to renew the given Session id after a successful login. To archive this goal, you need to create a Valve which manipulates the session. According to the BSI paper there a four steps to renew the session id:

» store the old session

» invalidate the old session

» generate a new session

» copy the data of the old session into the new session

A valve is a special filter that operate outside of a web application. It intercepts all requests before they are subsequently processed. You can find out more about valves at the Tomcat documentation.

And here is the code for the valve:

```
public class RenewSessionValve implements Valve{

 public void invoke(Request request, Response response)
    throws IOException, ServletException {

        // check for the login URI, only after a login
        // we want to renew the session
        if (req.getRequestURI().
                contains("/portal/j_security_check")) {

          // step 1: save old session
          Session oldSession = req.getSessionInternal(true);
          SavedRequest saved = (SavedRequest) oldSession.
                                getNote(Constants.FORM_REQUEST_NOTE);

          // step 2: invalidate old session
          req.getSession(true).invalidate();
          req.setRequestedSessionId(null);
          req.clearCookies();

          // step 3: create a new session and set it to the request
          Session newSession = req.getSessionInternal(true);
          req.setRequestedSessionId(newSession.getId());

          // step 4: copy data pointer from the old session
          // to the new one
          if (saved != null) {
            newSession.setNote(Constants.FORM_REQUEST_NOTE, saved);
          }

        }

 }

}
```

To make the Valve work, you need to declare it in the server.xml.

The reason why the session id is not renewed if you call
request.getSessionInternal(true)
is because of the way how the catalina request class creates a new session.
If the old session id was stored in a cookie it creates a new session
using the old session id:

```
if (connector.getEmptySessionPath() && isRequestedSessionIdFromCookie()) {
            session = manager.createSession(getRequestedSessionId());
        }
```

The only way to prevent this is to call
request.RequestedSessionId(null) befor calling
req.getSessionInternal(true)
This causes a manager.createSession(null) call in the request.doGetSession(), which generates a new session ID.
The JBoss Web 2.1.3 (which is a pimped Tomcat 6.0) has fixed this problem.

I would like to thank Thomas Schmidt who
developed this solution with me.

> This entry was posted on Tuesday, November 6th, 2007 at 13:00 and is filed under JBoss. You can follow any responses to this entry through the RSS 2.0 feed. You can leave a response, or trackback from your own site.

13 Responses to “HowTo renew the Session id in Tomcat or JBoss after a login”

Anjum Rizwi says:
December 10, 2007 at 5:30

Thanks,
Very good article, I am googling this type of article for long time today suddenly found in your article.

HowTo renew the Session id in asp as well as asp.net after a login.

Krawunke says:

December 10, 2007 at 18:43

In C# maybe it could be done in the Global.asax.cs. The technique should be nearly the same like in Java. I will write an article about it soon.

Cres? says:
March 15, 2009 at 19:52

Hi

Could you please explain what entry has to be given in the server.xml?

Daniel Wasser says:
March 16, 2009 at 9:33

just declare the valve as subnode of the <Host> entry:

```
<Host name=”localhost” autoDeploy=”false” deployOnStartup=”false” deployXML=”false”>
….
<Valve className=”de.koelnerwasser.RenewSessionValve ” />
….
</Host>
```

Cres says:
March 16, 2009 at 15:38

Hi Daniel,

I’ve implemented my valve. I’m using the valve along with a login filter. I’m getting the request in the valve, but it is not proceeding from there. ie, its not reaching my login servlet. What could be the problem?

Regards
Cres

Shriniwas says:
June 10, 2010 at 6:21

which jars would i need to compile and deploy this valve ? I’m using tomcat Apache Tomcat/5.5.28.

Thanks!

Daniel Wasser says:
June 10, 2010 at 11:20

Hello Shriniwas,

Just compile your valve and jar it. To compile your jar you need to look in which jar the valve interface is located in your Tomcat. Just search the lib folders of your Tomcat.

Regards,
Daniel

Jenny says:
June 15, 2010 at 12:19

Hi Danial,

Can you please elaborate the implementation of Valve? what I understand is this that:
1. We have to make a class… say RenewSessionValve.
2. We have to declare the valve as subnode in our tomcat server.xml file.
3. Compile the Valve and jar it.
4. Compile your jar….. What is the point of search the lib folders of Tomcat?
5. What changes we have to do in LoginFilter?
6. How this RenewSessionValve is going to be read from LoginFilter?
7. Whats next we have to do to accomplish this task?

Regards,
Jennifer

Daniel Wasser says:
June 15, 2010 at 12:49

Hello Jenny,
Point 1 to 3 is OK. To compile your Jar, the compiler needs the valve interface which is
a apache class (org.apache.catalina.valves.ValveBase) – so you need to add the tomcat server jars to your buildpath.

5. What changes we have to do in LoginFilter?
>> None, the valve exist beside the filters. A valve is a part of the server pipline (as filters too)
and is called before the filters
6. How this RenewSessionValve is going to be read from LoginFilter?
>> he does not need to read something from the login filter. As he is called
before the filter, there is nothing he could read from the filter
7. Whats next we have to do to accomplish this task?
>> i don't understand the question. If your valve is compiled, jared,
added to the servers lib file and declared in the server.xml it should be invoked by the server and do his work.

Regards,
Daniel

Jenny says:
June 15, 2010 at 18:03

Hi Daniel

I was writing a new class say RenewSessionValve, it says that The type RenewSessionValve must implement the inherited abstract method Valve.invoke(Request, Response, ValveContext)

I have imported the org.apache.catalina.Valve file.

Regards,
Jennifer

Daniel Wasser says:
June 17, 2010 at 7:51

Hello Jenny,
that’s OK. Did you get the valve to work now?

Regards,
Daniel

Jey says:
October 6, 2010 at 14:43

Hi Daniel,
Thank you so much for this solution. I have implemented your Valve and added in server.xml. I’m getting the request in the valve, but it is not proceeding from there. It is not going to my login servlets from Value. what should i do here so request would proceed to my Login Servlet ? Appreciate your response.

regards
Jey

Jey says:
October 6, 2010 at 14:49

ok just figured it out…
getNext().invoke(request, response);
Adding this line made the request to proceed to my Login servlet.

Leave a Reply

Name (required)

Mail (will not be published) (required)

Website

Submit Comment

CAPTCHA Code