note: these vulns were added to JPetstore to try this out

The payload injection on TLDs depends on what they do:

for example, in a JSP:

```
<%
        String payload ="\"><h1>payload</h1>";
%>

<html:form action="<%=payload%>" method="post">
</html:form>
```

is not exploitable, because the TLD throws an error

root cause

```
javax.servlet.jsp.JspException: Cannot retrieve mapping for action /"<h1>payload</h1>
        org.apache.struts.taglib.html.FormTag.lookup(FormTag.java:753)
        org.apache.struts.taglib.html.FormTag.doStartTag(FormTag.java:443)
        org.apache.jsp.account.SignonForm_jsp._jspService(SignonForm_jsp.java:295)
        org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
        org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:393)
        org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:320)
        org.apache.jasper.servlet.JspServlet.service(JspServlet.java:266)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
        org.apache.struts.action.RequestProcessor.doForward(RequestProcessor.java:1063)
        org.apache.struts.action.RequestProcessor.processForwardConfig(RequestProcessor.java:3
        org.apache.struts.action.RequestProcessor.process(RequestProcessor.java:229)
        org.apache.struts.action.ActionServlet.process(ActionServlet.java:1194)
        org.apache.struts.action.ActionServlet.doGet(ActionServlet.java:414)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:690)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
```

but

```
<%
        String payload =" \"><h1>payload</h1>";
%>

<html:form action="/shop/signon" target="<%=payload%>" method="post">
</html:form>
```

is exploitable because the 'target' attribute of the html:form tag lib, just outputs it out:

<html:form target="<%=payload%>" styleId="UploadActionForm<%=payload%>" action="/shop/signon" method="post" name="<%=payload%>">
</html:form>

note in the above screenshot how the action was resolved

this is using the Ibatis JpetStore example with struts