CVE-2006-1547

CVE-2006-1547: ActionForm in Apache Software Foundation (ASF) Struts before 1.2.9 with BeanUtils 1.7(Commons bean utils) allows remote attackers to cause a denial of service via a multipart/form-data encoded form with a parameter name that references the public getMultipartRequestHandler method, which provides further access to elements in the CommonsMultipartRequestHandler implementation and BeanUtils.

Analysis:

This issue occurs when content type of the form submission is “multipart/form-data"(For Http POST method only) and request parameter “**multipartRequestHandler.servlet.servletContext.attribute(org.apache.struts.action.MODULE)”** is present with any value.

When the above situation occurs then ActionForm properties gets modified and no part of the application will be accessible leading to a denial of service attack.

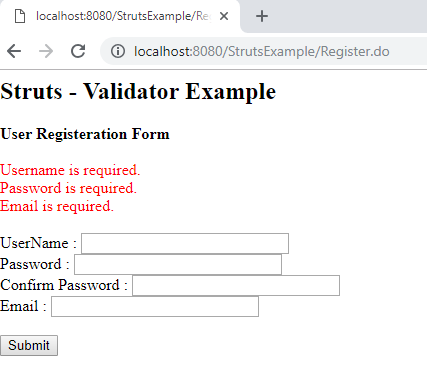
This issue is replicable only in commons-beanutils-1.7.0.jar.

Please follow the below steps to replicate the issue.

1. Unzip and import below project in eclipse.



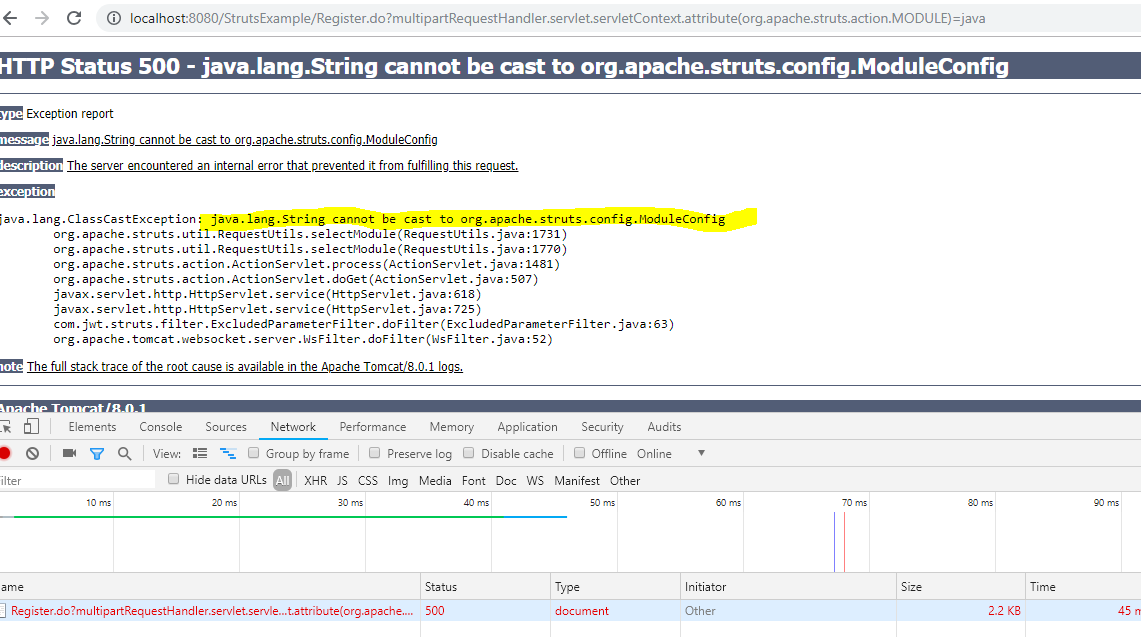
1. Access <http://localhost:8080/StrutsExample/EmployeeRegister.jsp> and click on Submit button without entering any values.



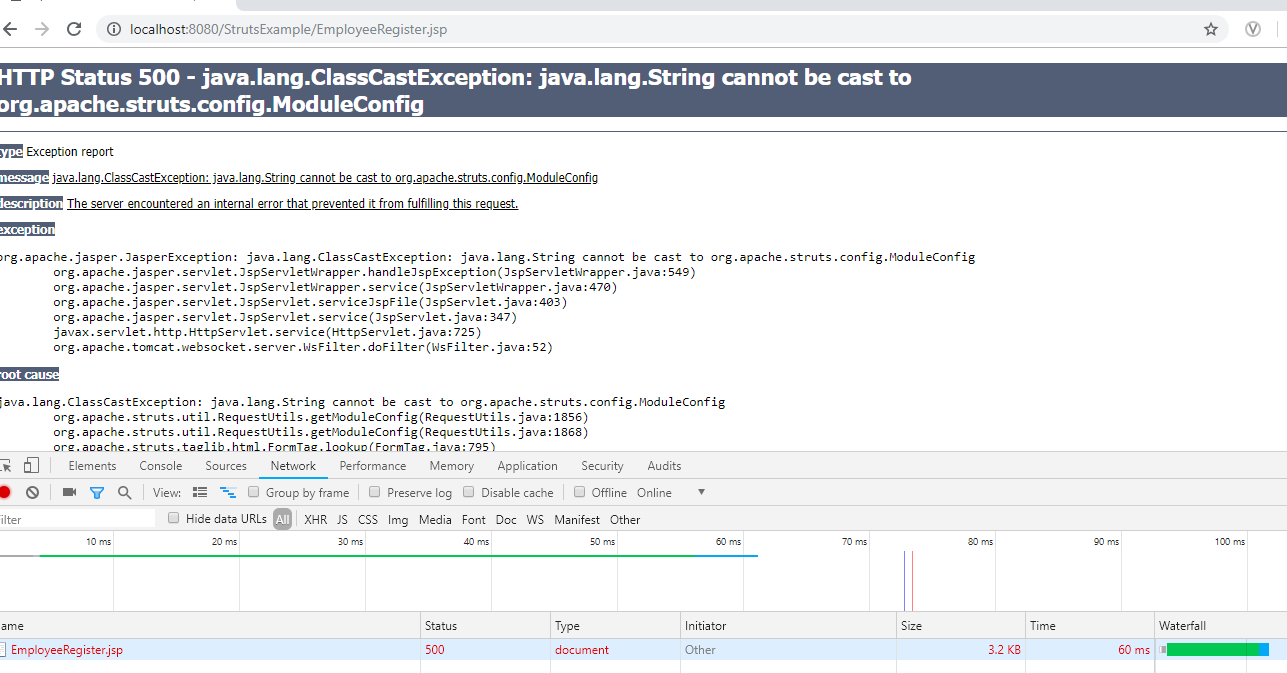
1. Once page reloaded with errors, modify the browser URL as mentioned below,

<http://localhost:8080/StrutsExample/Register.do?multipartRequestHandler.servlet.servletContext.attribute(org.apache.struts.action.MODULE)=java>

1. Once URL is changed in browser, select it and click on enter(Enter it couple of times). Browser page will be reloaded with below error.



1. Now try to access the original URL(<http://localhost:8080/StrutsExample/EmployeeRegister.jsp>) or any other parts of the application.



As shown in the above screen shots, page which was accessible earlier is no longer is accessible and leading to a denial of service attack.

This issue can be exploited when a form tag is present with below options.

<html:form action=*"/Register"* method=*"post"* enctype=*"multipart/form-data"*>

We can check for the highlighted part in Alliance code base to find out if this issue can be exploited.