CoColi / 2019-04-02 09:51:00 / 浏览数 3694 安全技术 漏洞分析 顶(0) 踩(0)

## S2-045 调试学习

#### 漏洞版本

2.3.31-2.3.5 2.5-2.5.10

#### 漏洞成因

content-type里有multipart/form-data就会走JakartaMultiPartRequest,捕捉了异常信息(里面带有payload),后又OGNL解析了

## payload

%{(#dm=@ognl.OgnlContext@DEFAULT\_MEMBER\_ACCESS).(#\_memberAccess?(#\_memberAccess=#dm):((#container=#context['com.opensymphony.x

### 从burp里面导的curl command

```
curl -i -s -k -X $'POST' \
   -H $'Host: 192.168.95.1:8081' -H $'User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Geo
   $'http://192.168.95.1:8081/S2_045_war_exploded/'
```

### 调试

```
修复地方 我把断点也下在这里了
```

```
🛾 $2-045 🕽 🖿 web 🗎 WEB-INF 🗎 IIb 🕽 📗 IIb 🐧 struts2-core-2.3.20.1.jar ) 🖿 org ) 🖿 apache 🖰 struts2 ) 🖻 struts2 ) 🖿 dispatcher 🗀 multipart 🖰 🔞 JakartaMultiPartRequest
                                                                                                                                                                                   Tomcat 8.5.34
                                                              Decompiled .class file, bytecode version: 49.0 (Java 5)
                                                                                                                                                                                                     Download
            ▶ Ilog4j-1.2.17.jar
             ▶ ¶ myfaces-api-1.1.2.jar
            ▶ | myfaces-impl-1.1.2.jar
                                                                                                  protected void setLocale(HttpServletRequest request) {
                                                                                                      if (this.defaultLocale == null) {
   this.defaultLocale = request.getLocale();
             ▶ | sitemesh-2.4.2.jar
             sslext-1.2-0.jar
               struts2-config-browser-plugin-2.3.20.1.jar
                                                                                                 protected String buildErrorMessage(Throwable e, Object[] args) {
   String errorKey = "struts.messages.upload.error." + e.getClass().getSimpleName();
   if (LOG.isDebugEnabled()) {
      LOG.debug( s: "Preparing error message for key: [#0]", new String[]{errorKey});
}
             ▶ 📗 struts2-convention-plugin-2.3.20.1.jar
               struts2-core-2.3.20.1.jar
                ► META-INF
                                                                                                                             Preparing error message for key: [#0]", new String[]{errorKey});
                  org.apache.struts2
                   ▶ tomponents
                                                                                                      return LocalizedTextUtil.findText(this.getClass(), errorKey, this.defaultLocale, e.getMe
                   ► config
                   ▼ dispatcher
                                                                                                 protected void processUpload(HttpServletRequest request, String saveDir) throws FileUploadEx
    Iterator i$ = this.parseRequest(request, saveDir).iterator();
                      ▶ mapper
                      ▼ 🛅 multipart
                                                                                                                                                                                    JakartaMultiPartRequest
                                                                                                      while(i$.hasNext()) {
```

## 都先经过web.xml 拦截 Struts2PrepareAndExecutefilter

```
处理请求
          its2-core-2.3.20.1.jar 🕽 🖿 org 🕽 🖿 apache 🕽 🖿 struts2 🕽 🗖 dispatcher 🕽 🖿 ng 🕽 📵 PrepareOperations
                                Q JakartaMultiPartRequest.class × Q Throwable.java >
                                                                                       MultiPartRequestWrapper.class ×
Q PrepareOperations.class ×
Q TextParseUtil.class ×
Q OgnlValueStack.class
                                Decompiled .class file, bytecode version: 49.0 (Java 5)
pi-1.1.jar
 1.3.1.iar
                                              public void assignDispatcherToThread() { Dispatcher.setInstance(this.dispatcher); }
                                              public void setEncodingAndLocale(HttpServletRequest request, HttpServletResponse response) {
                                                    this.dispatcher.prepare(request, response)
                                               public HttpServletRequest wrapRequest(HttpServletRequest oldRequest) throws ServletException {    oldRequest: RequestFacade@4177
    HttpServletRequest request = oldRequest;    request: RequestFacade@4177    oldRequest: RequestFacade@4177
                                                        request = this.dispatcher.wrapRequest(request);
                                                   return request;
} catch (IOException var4) {
                                                        throw new ServletException("Could not wrap servlet request with MultipartRequestWrapper!", var4);
 ser-plugin-2.3.20.1.jar
-plugin-2.3.20.1.jar
```

```
Stricts2-core-2.3.20.1jar (and stricts2) images and stricts2 image
```

### 这个地方 获取ContentType

2-045的POC—般都有(#nike='multipart/form-data')这样一句,就是使content\_type.contains("multipart/form-data")判断为true

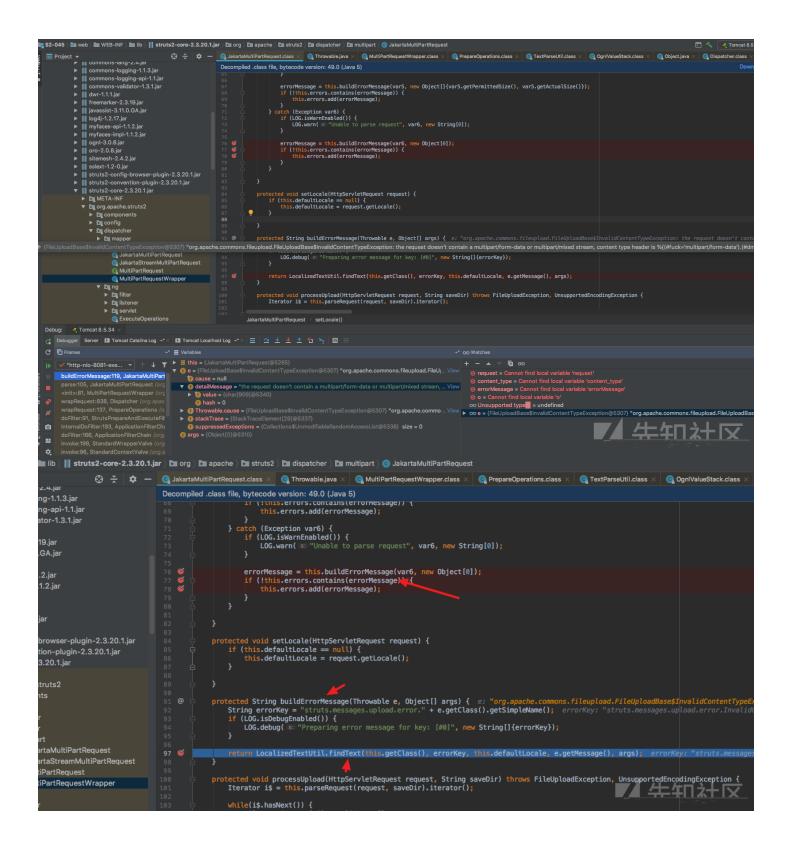
继续追踪getMultiPartRequest方法。通过配置struts.multipart.parser属性,可以指定不同的解析类,而默认就是org.apache.struts2.dispatcher.multipart.JakartaMultil

```
try {
    this.multi.parse(request, saveDir); multi: JakartaMultiPartRequest@4935 request: Requestive Iterator i$ = this.multi.getErrors().iterator();

    while(i$.hasNext()) {
        String error = (String)i$.next();
        this.addError(error);
    }
} catch (IOException var7) {
    if (LOG.isWarnEnabled()) {
        LOG.warn(var7.getMessage(), var7, new String[0]);
    }

    this.addError(this.buildErrorMessage(var7, new Object[]{var7.getMessage()}));
}
```

这里已经可以看到是用JakartaMultiPartReques解析了

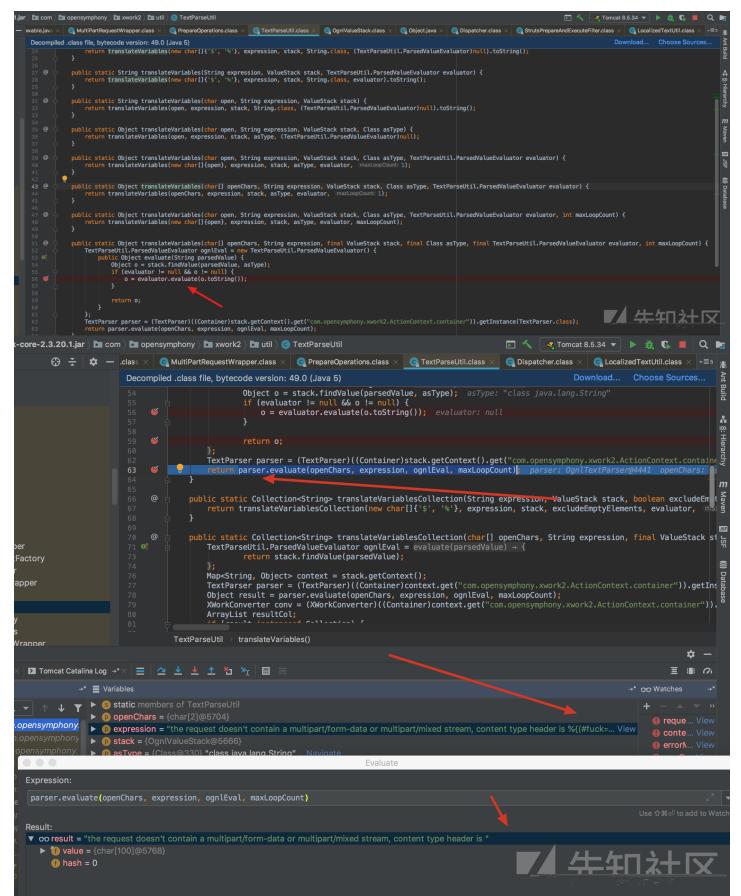


```
wable_java × 🧠 MultiPartRequestWrapper.class × 🗠 PrepareOperations.class × 🗠 TextParseUtil.class × 🗠 Ogn|ValueStack.class × 🗠 Object.java × 🗠 Dispatcher.class ×
      Decompiled .class file, bytecode version: 49.0 (Java 5)
                                                             uctassivauci(ctassivauci ctassivauci) (
                                       zed(bundlesMap) {
                                 delegatedClassLoaderMap.put(getCurrentThreadContextClassLoader().hashCode(), classLoader);
                       public static void clearBundle(String bundleName) {
   bundlesMap.remove( key: getCurrentThreadContextClassLoader().hashCode() + bundleName);
                       private static String createMissesKey(String prefix, String aBundleName, Locale locale) {
    return prefix + aBundleName + "_" + locale.toString();
                       public static String findText(Class aClass, String aTextName, Locale locale) {
    return findText(aClass, aTextName, locale, aTextName, new Object[0]);
                        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);
                                                                                                                                                                 ▼無知計区
再继续findText
                                       } catch (Exception var15) {
   LOG.debug( s: "unable to find property " + prop, var15, new String[0]);
                              LocalizedTextUtil.GetDefaultMessageReturnArg result;
                             if (indexedTextName == null) {
    result = getDefaultMessage(aTextName, locale, valueStack, args, defaultMessage);
                                  result = getDefaultMessage(aTextName, locale, valueStack, args, (String)null);
if (result != null && result.message != null) {
                                        return result.message;
                                  result = getDefaultMessage(indexedTextName, locale, valueStack, args, defaultMessage);
                             if (unableToFindTextForKey(result) && LOG.isDebugEnabled()) {
                                  prop = "Unable to find text for key '" + aTextName + "' ";
if (indexedTextName != null) {
   prop = prop + " or indexed key '" + indexedTextName + "' ";
                                  prop = prop + "in class '" + aClass.getName() + "' and locale '" + locale + "'";
LOG.debug(prop, new String[0]);
                              return result != null ? result.message : null;
               LocalizedTextUtil > findText()
                                                                                                                                                        nost Log → * X 😑 🔼 🛨 🛨 🏦 🧤 🖼 🗒
                LocalizedTextUtil.GetDefaultMessageReturnArg result = null;
                boolean found = true;
if (key != null) {
                     String message = findDefaultText(key, locale);
                     if (message == null) {
                          message = defaultMessage;
                     if (message != null) {
    MessageFormat mf = buildMessageFormat(TextParseUtil.translateVariables(message, valueStack), locale);
                          String msg = formatWithNullDetection(mf, args);
result = new LocalizedTextUtil.GetDefaultMessageReturnArg(msg, found);
       ♀ ▼ }
                return result;
                                                                                                                                                                         com.opensymphony.xwork2.util.TextParseUtil.translateVariables(String, ValueStack) 方法主要用于扩展字符串中由 ${} 或 %{} 包裹的 OGNL
```

1.jar > 🖿 com > 🖿 opensymphony > 🖿 xwork2 > 🖿 util > 🜀 LocalizedTextUtil

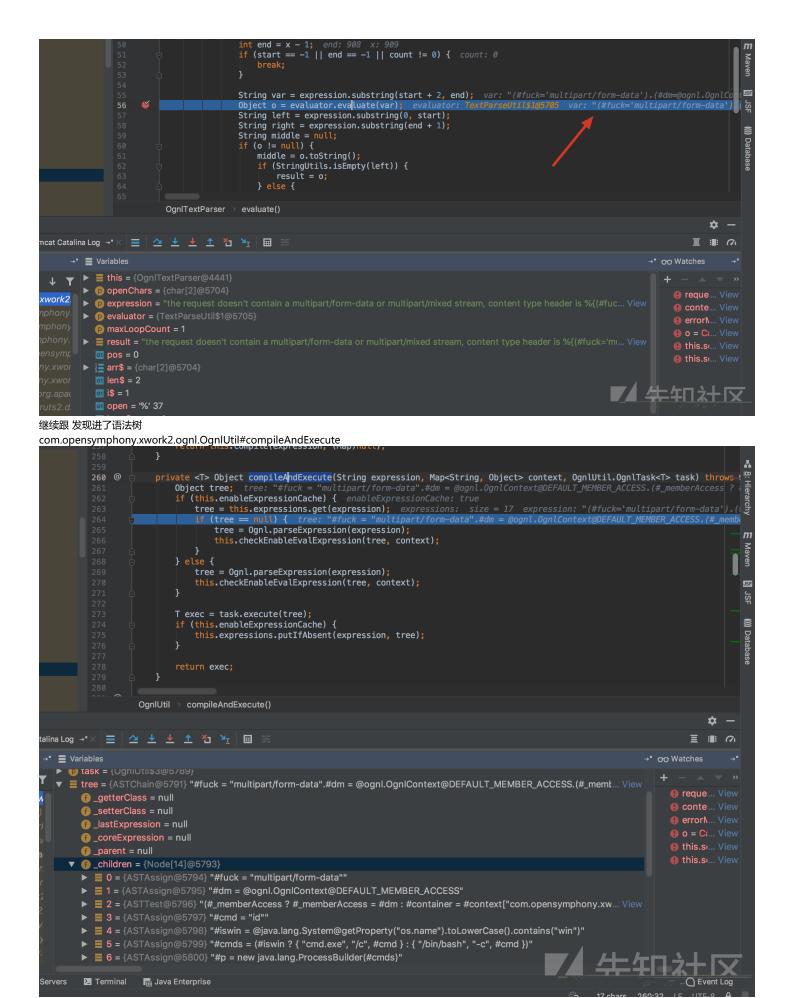
com.opensymphony.xworkz.util.TextParseUtil.translateVariables(String, ValueStack) 万法主要用于扩展字符串中由 \${} 或 %{} 包裹的 OGNL 表达式,这里也就是 OGNL 的入口,随后 action message 将进入 OGNL 的处理流程,漏洞被触发。

```
public TextParseUtil() {
    public static String translateVariables(String expression, ValueStack stack) {
    return translateVariables(new char[]{'$', '%'}, expression, stack, String.class, (TextParseUtil.ParsedValueEvaluator)null).toString();
    return translateVariables(new char[]{'$', '%'}, expression, stack, String.class, (TextParseUtil.ParsedValueEvaluator)null).toString();
    public static String translateVariables(String expression, ValueStack stack, TextParseUtil.ParsedValueEvaluator evaluator) {
```



下一步 又继续 解析

com. open symphony. xwork 2. util. Text Parse Util. Parsed Value Evaluator #evaluate Parse Util. Parsed Value Evaluator #evaluator #eval



```
protected void setValueBody(OgnlContext context, Object target, Object value) throws OgnlException { context
       context.put(this._name, value); context:
   public Object put(Object key, Object value) {
       Object result;
       if (RESERVED_KEYS.containsKey(key)) {
           if (key.equals("this")) {
               result = this.getCurrentObject();
               this.setCurrentObject(value);
           } else if (key.equals("root")) {
               result = this.getRoot();
               this.setRoot(value);
           } else {
               if (key.equals("context")) {
                   throw new IllegalArgumentException("can't change context in context");
               if (key.equals("_traceEvaluations")) {
                   result = this.getTraceEvaluations() ? Boolean.TRUE : Boolean.FALSE;
                   this.setTraceEvaluations(OgnlOps.booleanValue(value));
               } else if (key.equals("_lastEvaluation")) {
                   result = this.getLastEvaluation();
               this._lastEvaluation = (Evaluation)value;
} else if (key.equals("_keepLastEvaluation")) {
                   result = this.getKeepLastEvaluation() ? Boolean.TRUE : Boolean.FALSE;
                   this.setKeepLastEvaluation(OgnlOps.booleanValue(value));
               } else if (key.equals("_classResolver")) {
                   result = this.getClassResolver();
                   this.setClassResolver((ClassResolver)value);
               } else if (key.equals("_typeConverter")) {
                   result = this.getTypeConverter();
                   this.setTypeConverter((TypeConverter)value);
               } else {
                   if (!key.equals("_memberAccess")) {
                       throw new IllegalArgumentException("unknown reserved key '" + key + "'");
                   result = this.getMemberAccess();
                   this.setMemberAccess((MemberAccess)value);
       } else {
           result = this._values.put(key, value);
OgnlContext → put()
                                                                       学
```

```
this.setValueBody(context, target, value);
                                            public final Object getValue(OgnlContext context, Object source) throws OgnlException {
                                                 Object result = null; result:
                                                      EvaluationPool pool = OgnlRuntime.getEvaluationPool();
                                                      Throwable evalException = null;
                                                      Evaluation evaluation = pool.create( node: this, source);
                                                      context.pushEvaluation(evaluation);
ory
                                                      boolean var13 = false;
                                                          var13 = true;
                                                           result = this.evaluateGetValueBody(context, source);
                                                           var13 = false:
                                                      } catch (OgnlException var14) {
                                        SimpleNode > getValue()
 屇
     →" oo Watches
        ▼ 

this = {ASTStaticMethod@6984} "@java.lang.System@getProperty("os.name")"
              _className = "java.lang.System"
                                                                                                                request = Cannot find local variable
              _methodName = "getProperty"
                                                                                                                content_type = Cannot find local va
              _getterClass = null
                                                                                                                errorMessage = Cannot find local v
              parent = {ASTChain@7023} "@java.lang.System@getProperty("os.name").toLowe
                                                                                                                  o = Cannot find local variable 'o'
              f _children = {Node[1]@7024}
                                                                                                                  this.securityMemberAccess = No
这个地方执行 OGNL 表达式
                                                                                                                                  Choose Sources...
               Decompiled .class file, bytecode version: 49.0 (Java 5)
                           public static Object translateVariables(char[] openChars, String expression, ValueStack stack, Class asType, TextParseUt
                            public static Object translateVariables(char open, String expression, ValueStack stack, Class asType, TextParseUtil.Pars
    return translateVariables(new char[]{open}, expression, stack, asType, evaluator, maxLoopCount);
}
                            public static Object translateVariables(char[] openChars, String expression, final ValueStack stack, final Class asTyr
    TextParseUtil.ParsedValueEvaluator ognlEval = new TextParseUtil.ParsedValueEvaluator() {
                                    public Object evaluate(String parsedValue) {
                                                                                                                                                       Mayen
                                        Object o = stack.findValue(parsedValue, asType);
                                           (evaluator != null && o != null) {
                                            o = evaluator.evaluate(o.toString());
                                                                                                                                                      IE JSF
                                        return o:
                                TextParser parser = (TextParser)((Container)stack.getContext().get("com.opensymphony.xwork2.ActionContext.container
                                return parser.evaluate(openChars, expression, ognlEval, maxLoopCount);
                           public static Collection<String> translateVariablesCollection(String expression. ValueStack stack. boolean excludeEmptvl
                        TextParseUtil > translateVariables()
                                                                                                                                               ø
at Catalina Log →"× | ☰ | 🏄 👲 👲 🛕 🧤 🔭
                                                                                                                                           I :■: 0
 ■ Variables
                                                                                    →" oo Watches
                                                                                                    <u> </u> ∞
    ► foot = {CompoundRoot@5796} size = 1
      f context = {Ogn|Context@5797} size = 25
                                                                                         • request = Cannot find local variable 'request'
          \equiv 0 = \{ HashMap\$Node@5814 \} \ "com.opensymphony.xwork2.ActionContext.locale \} 
         = 1 = {HashMap$Node@5815} "request" -> " size = 1"
                                                                                         errorMessage = Cannot find local variable 'errorMessage'
         2 = {HashMap$Node@5816} "session" -> " size = 0"
         3 = {HashMap$Node@5817} "fuck" -> "multipart/form-data"
                                                                                         • this.securityMemberAccess = 'this' is not available
                                                                                         this.securityMemberAccess.excludedClasses = 'this' is not available
         ■ 5 = {HashMap$Node@5819} "com.opensymphony.xwork2.ActionContext.conta

    ((OgnlUtil)this).excludedClasses = Inconvertible types; ca... View
    ((OgnlUtil)this).container = Inconvertible types; cannot ca... View

         ■ 6 = {HashMap$Node@5820} "com.opensymphony.xwork2.dispatcher.HttpServ
         7 = {HashMap$Node@5821} "last.property.accessed" -> "null"
         ■ 8 = {HashMap$Node@5822} "iswin" -> "false"
                                                                                                           ▶ ■ value = {Boolean@5852} false
         9 = {HashMap$Node@5823} "com.opensymphony.xwork2.ActionContext.applic
```

在mac上调试的 payload里

#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win')) 执行之后就是false

当请求到来的时候,一个ActionContext对象被createActionContext方法创建。
OgnlValueStack 的setOgnlUtil函数被调用,以用来初始化OgnlValueStack 的securityMemberAccess ,这样就获得OgnlUtil的全局实例 这就意味着全局OgnlUtil 实例都共享相同的SET:excludedClasses, excludedPackageNames 和 excludedPackageNamePatterns作为\_memberAccess,所以清除这些之后也会清除与\_memberAccess相匹配的SET。 在那之后,OGNL 就可以自由的访问DEFAULT\_MEMBER\_ACCESS对象并且 OgnlContext 的 setMemberAccess 代替了\_memberAccess和DEFAULT\_MEMBER\_ACCESS,这样就可以执行任意代码了

## 参考文章

### 参考文章

作为武器的CVE-2018-11776:绕过Apache Struts 2.5.16 OGNL 沙箱 Struts2 架构图

可能有的地方说的不对,希望师傅们指正(萌新瑟瑟发抖)

点击收藏 | 1 关注 | 1

<u>上一篇:OSINT Primer:组织(第...下一篇:详解变形金刚</u>

- 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

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板